ETHICAL HACKING POST EXPLOITATION - EHPX

DESCRIÇÃO

(Nível Intermediário)

Carga Horária: 40hrs

O curso Ethical Hacking Post Exploitation (EHPX) apresenta técnicas ofensivas de pós-exploração, com a análise das etapas de um ataque e suas principais características, utilizando como base *frameworks* e metodologias consagradas como MITRE ATT&CK e o *Cyber Kill Chain*.

As ameaças cibernéticas estão cada vez mais avançadas ao ponto de grandes empresas e nações serem vítimas constantes de ataques mais elaborados. Isso nos leva a dura realidade de que, mais cedo ou mais tarde, sua organização será atacada e comprometida em algum nível.

Uma vez que um atacante explora alguma vulnerabilidade e consegue entrar numa rede, o que acontece depois ? Como ele se instala ? Como ele escala privilégios ? Como ele coleta informações sem ser notado ? Como ele se comunica com seu servidor de Comando e Controle ? Como ele exfiltra dados relevantes ? Como ele cobre seus rastros ? Essas e outros perguntas serão respondidas nesse treinamento que possui uma abordagem 100% prática, conduzido por uma bateria de exercícios e laboratórios.

O curso trabalha técnicas atuais de pós-exploração em um ambiente composto por aplicações reais e com sistemas operacionais modernos (Windows e Linux). Serão apresentadas técnicas, táticas e procedimentos (TTP) de ataques, dos mais simples aos mais avançados (APT), pontos fundamentais tanto para atividades ofensivas (Pentesters, Red Team) quanto para as atividades de defesa (Blue Team, Threat Hunting, CSIRT, SOC).

Diversos temas serão abordados, tais como: Coleta de Informações (*Pillaging*), Escalada de Privilégios, Manutenção do Acesso (*Backdoor*), Persistência, Mapeamento Interno da Rede, Pivoteamento, Captura de Credenciais, Quebra de Senhas, Pass-The-Hash, PowerShell Ofensivo, Ataques a Infraestrutura do Active Directory, Exploração do Protocolo Kerberos, Movimentação Lateral, Canal de Comando e Controle (C2/C&C), Exfiltração de Dados, entre outros.

MÓDULO 1

1. Visão Geral sobre Teste de Invasão (*Pentesting*), Exploração (*Exploitation*), Pós-Exploração (*Post-Exploitation*), *Red Team Operation* e *Purple Team Activities*

2. Cyber Kill Chain Framework
   - Análise das etapas de um ataque
   - Outros frameworks equivalentes

3. Mitre ATT&CK Framework
   - Visão Geral
   - Guia para atividades de Pós-Exploração

4. Introdução a Pós-Exploração (*Post-Exploitation*)
   - Visão Geral: Coleta de Informações, Escalada de Privilégios, Manutenção do Acesso (Backdoor), Persistência, Mapeamento Interno da Rede, Pivoteamento, Captura de Credenciais, Quebra de Senhas, Pass-The-Hash, PowerShell, Ataques a Infraestrutura do Active Directory, Movimentação Lateral, Canal de Comando e Controle (C2), Extração/Exfiltração de Dados

MÓDULO 2

1. Preparação e Configuração Inicial
   - Acesso ao Portal do Aluno – GoHacking Academy
   - Acesso ao ambiente dos Laboratórios Online

2. Acesso inicial ao alvo
   - Comprometimento de aplicação vulnerável no Windows
   - Acesso não privilegiado (*reverse shell*)
   - Laboratório

3. Coleta de Informações do Alvo Comprometido (*Pillaging*) – Windows
   - Comandos do cmd.exe (systeminfo, netstat, tasklist, net user, net localgroup, net session, net use, netsh, reg, sc, schtasks, certutil, bitsadmin etc) utilizados em atividades ofensivas
   - Ataques *Living Off The Land* (LOLBAS)
   - Transferência de arquivos entre atacante e alvo
   - WMI – principais comandos para um Pentester
   - Coleta de informações com o WMIC
   - Laboratório

4. Metasploit e Meterpreter Shell
   - Módulos de Pós-Exploração do Metasploit
   - Principais características e plugins/scritps do Meterpreter para Pós-Exploração
   - Laboratório

5. Técnicas de Escalada de Privilégios no Windows
   - Enumeração e verificação de vulnerabilidades locais
   - ExploitDB (*searchsploit*), serviços privilegiados, Meterpreter
   - Laboratório

6. Captura de Credenciais e Ataque de Senhas
    - Meterpreter Token Impersonation/Incognito
    - Mimikatz
    - Meterpreter (Hashdump, Mimikatz, Kiwi)
    - Dump de memória do processo LSASS
    - Quebra de hash *offline* com ataque de dicionário
    - Utilização das ferramentas John The Ripper e Hashcat
    - Laboratório

7. Manutenção de Acesso e Persistência
    - Utilização de Credenciais Privilegiadas
    - Mecanismos de persistência
    - Criação e Instalação de *Backdoor*
    - Laboratório

8. Exploração dos Protocolos SMB e RDP
    - Exploração do protocolo SMB
    - Exploração do protocolo de acesso remoto RDP
    - Utilização da ferramenta CrackMapExec
    - Ataque *Pass-The-Hash* (PTH)
    - Laboratório

MÓDULO 3

1. Acesso inicial ao alvo
    - Comprometimento de aplicação vulnerável no Linux
    - Exploração de aplicação web para acesso inicial ao alvo
    - Acesso não privilegiado (*reverse shell*)
    - Técnicas de melhoria e customização de shell remoto
    - Utilização de ferramentas nativas para estabelecer de um shell remoto cifrado
    - Laboratório

2. Coleta de Informações do Alvo Comprometido (*Pillaging*) – Linux
    - Principais comandos do bash utilizados em atividades ofensivas, verificação de arquivos chaves do sistema, verificar arquivos com SUID/SGID
    - Enumeração e verificação de vulnerabilidades locais
    - Transferência de arquivos entre atacante e alvo
    - Laboratório

3. Manutenção de Acesso
    - Instalação de *Backdoor*
    - Instalação e configuração de *Webshell*
    - Laboratório

4. Técnicas de Escalada de Privilégios no Linux
    - ExploitDB (*searchsploit*)
    - Kernel Exploits
    - Serviços privilegiados vulneráveis
    - Binários customizados com SUID/SGID
    - Laboratório

5. Captura de Credenciais
    - Utilização de Credenciais
    - Manipulação do serviço *Secure Shell* (SSH)
    - SSH *Hijacking*
    - Laboratório

MÓDULO 4

1. PowerShell Kung-Fu para Pentesters and Red Team
    - Fundamentos, estrutura e principais comandos do PowerShell
    - Execução de scripts em PowerShell
    - Execução de scripts em memória (*fileless*)
    - Laboratório

2. Scripts Ofensivos
    - Técnicas Ofensivas e Utilização de Scripts específicos para realização de ataques diversos
    - Utilização de frameworks como o Nishang e PowerSploit
    - Customização e execução de scripts em memória
    - Laboratório

3. Ofuscação de Scripts
    - Técnicas de ofuscar a execução de scripts ofensivos em PowerShell
    - Laboratório

4. Persistência com WMI
    - Manipulação de comandos WMI via PowerShell
    - Configuração de tarefas WMI maliciosas via PowerShell
    - Laboratório

MÓDULO 5

1. Infraestrutura de Comando e Controle – C2
    - Arquitetura e Características de um Canal de C2
    - Mapeamento dos Frameworks de C2 disponíveis

2. Empire
    - Estrutura, módulos e funcionalidades
    - Estabelecimento de um canal de C2
    - Explorar mecanismos de persistência
    - Laboratório

3. Covenant
    - Estrutura, módulos e funcionalidades
    - Estabelecimento de um canal de C2
    - Exfiltrar dados do alvo
    - Laboratório

4. Sliver
    - Estrutura, módulos e funcionalidades
    - Estabelecimento de um canal de C2
    - *Bypass* de AV
    - *Dump* de processo em memória
    - Laboratório

MÓDULO 6

1. Pivot e Movimento Lateral
    - Aproveitamento do acesso inicial como *pivot*
    - Técnicas de movimento lateral

2. Pivoteamento com SSH
    - Sistema Linux como *Pivot*
    - Tunelamento via SSH
    - *Port Forwarding* – Local e Remoto / Estático e Dinâmico
    - SOCKS Proxy e Proxychains com SSH
    - SSH + Manipulação do IPTables
    - VPN com SSH
    - Configuração de um Jump Box
    - Como trabalhar com múltiplas camadas de pivoteamento
    - Laboratório

3. Windows Pivot
    - Manipulação do Windows como *Pivot*
    - Módulos de Roteamento e Port Forwarding do Metasploit
    - Encaminhamento de portas via Meterpreter
    - SOCKS Proxy e Proxychains com Metasploit
    - Utilização de ferramentas de terceiros como Chisel e Plink
    - *Port Fowarding* via "*netsh interface portproxy*" (LOLBAS)
    - Laboratório

4. Exfiltração de Dados
    - Técnicas de extração/exfiltração de dados
    - Protocolos de rede utilizados para exfiltração (HTTP, HTTPS, DNS, ICMP)
    - Exfiltração via ICMP (ping)
    - Laboratório

MÓDULO 7

1. Introdução a ataques a Infraestrutura de Active Directory (AD)
   - Fundamentos de Windows Domain e AD
   - Nomenclatura, serviços e principais componentes

2. Mapeamento da estrutura do AD
   - Utilização da Ferramenta CrackMapExec em ambiente de AD
   - Utilização da Ferramenta BloodHound
   - Mapeamento das entidades e relações de um AD
   - Laboratório

3. Ataques ao Protocolo de Autenticação Kerberos
   - Entendimento do protocolo Kerberos (*Windows Domain*)
   - Visão geral dos principais ataques ao Kerberos (Kerberosating, ASREPRoast, Pass-The-Ticket, Over-Pass-The-Hash, Silver Ticket, Golden Ticket)
   - Execução do ataque Golden Ticket
   - Laboratório

4. Ataque em estrutura com múltiplas camadas de proteção
   - Cenário Final
   - Manipulação do alvo inicial (*pivot*)
   - Mapeamento da Topologia
   - Preparação e Execução do Ataque
   - Laboratório

CAPTURE THE FLAG – CTF

1. Desafio Final – CTF
   - Ambiente Simulado da Infraestrutura de um Organização a ser atacada
   - Emprego das táticas, técnicas, procedimentos e ferramentas de pós-exploração

PRÉ-REQUISITOS

- Conhecimentos básicos em Sistema Operacional Windows
  - Estrutura de diretórios, comandos básicos do prompt (cmd.exe), configuração de rede, verificação de serviços e processos, gerenciamento de usuários locais
- Conhecimentos básicos em Sistema Operacional Linux
  - Estrutura de diretórios, comandos básicos do shell (bash), configuração de rede, verificação de serviços e processos, gerenciamento de usuários locais, permissão de arquivos
- Conhecimentos básicos de Rede de Computadores e Serviços de Rede
  - Protocolo TCP/IP, FTP, HTTP, HTTPS, SMB, SSH, DNS, ICMP
- Conhecimentos básicos de Penetration Testing – Metodologia e Procedimentos
- Familiaridade com a distribuição Kali Linux
- Familiaridade com ferramentas de Pentesting – Metasploit, Meterpreter
- Familiaridade com ferramentas de Virtualização – VMWare

PÚBLICO ALVO

- Especialistas em Segurança da Informação
- Analista de Segurança da Informação
- Pentesters
- Membros de Red Team / Blue Team
- Membros de CSIRT
- Analista de SOC
- Gestor de Segurança da Informação
- Profissionais de TI com interesse e afinidade na área de Segurança da Informação

MATERIAL NECESSÁRIO

- Os alunos devem utilizar suas próprias estações de trabalho (Windows, Linux ou Mac OS), com a capacidade de executar de 02 a 03 Máquinas Virtuais (VM) simultaneamente.
- Configuração mínima de 8GB de RAM, 60 GB de espaço livre em disco, porta USB e placa de rede (RJ45 ou *wireless*) para acesso à Internet.
- Software de Virtualização: VMWare, versão mais atualizada, de preferência *Workstation* (para hosts Windows ou Linux) ou *Fusion* (para host Mac OS). É possível utilizar a versão de avaliação (*trial*). O VMWare *Player* também é capaz de executar as VMs do curso (não possui a capacidade de realizar *snapshots*, importante mas não imprescindível para o curso).
- Será disponibilizado uma VM Kali Linux customizada para o treinamento (empregada como a máquina atacante). O aluno está livre para utilizar qualquer outra distribuição ou mesmo um Kali próprio, contudo, é aconselhável utilizar a VM Kali oferecida no curso.

MATERIAL RECEBIDO

- Acesso ao Portal do Aluno – GoHacking Academy, que concentra o material do curso
- Apostila do Curso no formato PDF
- Gravações das sessões ao vivo
- Certificado de Conclusão do Curso no formato PDF (com a carga horária e ementa)

CAPACIDADES ALCANÇADAS

No final do curso, o aluno estará apto a:

- Diferenciar as atividades de *Pentesting*, *Red Team* e *Purple Team*
- Entender aspectos fundamentais da Segurança Ofensiva
- Compreender modelos e frameworks como *Cyber Kill Chain* e MITRE ATT&CK
- Entender a metodologia de um ataque cibernético
- Compreender a importância das atividades de Pós-Exploração em Segurança da Informação
- Mapear as atividades de Pós-Exploração na infraestrutura de uma organização
- Executar atividades de Pós-Exploração na infraestrutura de uma organização
- Identificar falhas e vulnerabilidades internas da infraestrutura de uma organização
- Utilizar de ferramentas nativas do Sistema Operacional (Linux e Windows) para executar atividades ofensivas (*Living Off The Land* – LOLBAS)
- Utilizar o Metasploit/Meterpreter para atividades de Pós-Exploração
- Escalar privilégios em sistemas Windows e Linux
- Extrair credencias de acesso em memória
- Aproveitar o PowerShell para atividades ofensivas
- Estabelecer mecanismos de persistência em uma infraestrutura comprometida
- Entender a arquitetura e características de Sistemas de Comando e Controle (C2)
- Utilizar ferramentas de C2 e estabelecer Canal de C2
- Extrair (exfiltrar) dados e informações de um sistema ou infraestrutura comprometida
- Realizar atividades de movimento lateral e pivoteamento em uma infraestrutura de uma organização
- Mapear a estrutura de ambientes de *Windows Domain* e *Active Directory* (AD) e identificar fraquezas
- Realizar ataques a ambientes de AD
- Entender e realizar ataques ao protocolo de autenticação Kerberos
- Realizar atividades de Pós-Exploração utilizando técnicas furtivas (*stealthy*)
- Proteger, detectar e responder a atividades ofensivas de Pós-Exploração

LAIOS FELIPE BARBOSA