ETHICAL HACKING PENETRATION TESTING (EHPT)

DESCRIÇÃO

(Nível Básico/Intermediário)

Carga Horária: 40 hrs

O Ethical Hacking Penetration Testing (EHPT) é o nosso curso de entrada na trilha de Segurança Ofensiva. O curso tem início com uma abordagem das técnicas e procedimentos adotados em Ataques Cibernéticos, explorando alguns casos reais como forma de identificar as etapas da Cyber Kill Chain e outras metodologias de ataque.

Em seguida, são abordadas metodologias para execução de um Teste de Invasão (Pentest), as implicações legais e formais da realização deste tipo de atividade e um rápido *overview* sobre Pentest, Red Team e Blue Team.

Finalizando a 1ª parte (cujo conteúdo é disponibilizado por aulas gravadas), falamos sobre como produzir um relatório do teste executado e como classificar as vulnerabilidades encontradas de acordo com os padrões estabelecidos e seus respectivos impactos.

Na 2ª parte do curso, são abordadas, de forma prática, as fases de um teste de invasão: Reconhecimento, Escaneamento/Enumeração, Exploração e Pós Exploração. Em cada uma das fases são demonstradas as técnicas e ferramentas que permitem alcançar os objetivos desejados em cada etapa do teste e os conhecimentos são aplicados nos laboratórios de cada módulo. Além das fases de um Pentest, são abordados assuntos como Engenharia Social e Pentest Físico.

No ultimo laboratório do curso, os alunos poderão realizar um Pentest Simulado na rede de uma organização fictícia, com escopo e regras de engajamento definidos.

O curso possui mais de 30 laboratórios práticos de nível Básico/Intermediário e é indicado para os alunos que estão iniciando os estudos na área de Segurança Ofensiva ou que estejam se preparando para certificações como a OSCP.

MÓDULO 1 – ATAQUES CIBERNÉTICOS

1. Entendendo a dinâmica de ataques cibernéticos com estudos de casos;
2. Cyber Kill Chain Framework;
3. Advanced Persistent Threat;
4. ATT&CK Matrix for Enterprise;

MÓDULO 2 – ETHICAL HACKING AND PENETRATION TESTING

1. Fundamentos de Ethical Hacking;
2. Penetration Test (Teste de Invasão)
3. Mindset de um Pen Tester;
4. Tipos de Teste de Invasão;
5. Metodologias de Teste de Invasão;
6. Mercado de trabalho e certificações;
7. Aspectos Legais;
8. Termo de responsabilidade e confidencialidade;
9. Fases de um Teste de Invasão;

MÓDULO 3 – PRÁTICA COM SISTEMAS LINUX, WINDOWS E VIRTUALIZADORES

1. Configuração do ambiente e instalação das Vms;
2. Lab 1 – Linux com Kali Linux;
3. Lab 2 – Windows Essentials;
4. Lab 3 – Netcat, Socat e Powercat (Binds and Reverse Shells)

MÓDULO 4 – REPORTING (RELATÓRIO)

1. Dicas para elaboração de um relatório de qualidade;
2. Classificação e scoring de vulnerabilidades;
3. CVE, CWE e CVSS;
4. Sugestões de formato do relatório;
5. Links e Dicas;

MÓDULO 5 – RECONNAISSANCE (RECONHECIMENTO)

1. Conceitos e objetivos da fase Reconhecimento;
2. Reconhecimento Passivo x Ativo;
3. Ferramentas e técnicas;
4. Lab 4: Google Hacking, Shodan and Censys;
5. Lab 5: Extraindo informações de Metadados;
6. Lab 6: Recon-ng;
7. Lab 7: Open AWS S3 buckets;

MÓDULO 6 – SCANNING AND ENUMERATION (ESCANEAMENTO E ENUMERAÇÃO)

1. Conceitos e objetivos da fase Escaneamento e Enumeração;
2. Ferramentas e técnicas;
3. Lab 8: Nmap Scan;
4. Lab 9: Nmap Script Engine e Enumeração;
5. Lab 10: Scan com OpenVas;
6. Lab 11: Enumeração com SNMP;

MÓDULO 7 – EXPLOITATION (EXPLORAÇÃO)

1. Conceitos e objetivos da fase Exploração;
2. Ferramentas e técnicas;
3. Lab 12: Exp 1 - Vuln de SO, Metasploit e Meterpreter;
4. Lab 13: Exp 2 - Brute Force, Remote Desktop, CVE-2020-0796 e Jenkins;
5. Lab 14: Exp 3 - Falha em aplicações;
6. Lab 15: Exp 4 - Desafio Rorscharck;
7. Lab 16: Exp 5 - Vuln Struts CVE-2018-11776;
8. Lab 17: Exp 6 - Desafio Homeland;

MÓDULO 8 – EXPLORAÇÃO DE VULNERABILIDADES EM APLICAÇÕES WEB

1. Conceitos, ferramentas e técnicas;
2. Metodologia OWASP;
3. Top 10 OWASP;
4. Técnicas Comuns Web Application Hacking;

5. Programas de Bug Bounty;
6. Plataformas para treinamento de habilidades;
7. Lab 18: OWASP Top 10 - A1;
8. Lab 19: Exp 7 - Falhas em CMS (Desafio DareDevil);
9. Lab 20: Exp 8 - Falha em Aplicações (GLPI);

MÓDULO 9 – POST EXPLOITATION (PÓS EXPLORAÇÃO)

1. Escalação de Privilégios;
2. Manutenção do Acesso;
3. Cracking Passwords;
4. Pivoteamento e Movimento Lateral;
5. Lab 21: Escalação de Privilégios Ubuntu-18;
6. Lab 22: Escalação de Privilégios DareDevil;
7. Lab 23: Cracking password Linux/Windows;
8. Lab 24: Meterpreter Post Exploitation;
9. Lab 25: Pivoteamento com SSH;

MÓDULO 10 – SOCIAL ENGINEERING (ENGENHARIA SOCIAL)

1. Engenharia Social: conceitos, técnicas e ferramentas;
2. Como incluir Engenharia Social em Testes de Invasão;
3. Lab 26: SET – Social Engineering Toolkit;
4. Lab 27: Evil PDF;
5. Lab 28: Evil Android App;
6. Lab 29: GoPhish;

MÓDULO 11 – PENTEST SIMULATION (TESTE DE INVASÃO SIMULADO)

1. Escopo e Regras de Engajamento;
2. Reconhecimento e Enumeração;
3. Acesso vpn;
4. Exploração e confecção do Relatório;
5. Lab 30: Pentst Simulation;

LAB EXTRA – EXPLORAÇÃO E PÓS-EXPLORAÇÃO EM VM WINDOWS

PRÉ-REQUISITOS

- Conhecimentos básicos em Sistema Operacional Windows
- Estrutura de diretórios, comandos básicos do prompt, configuração de rede, verificação de serviços e processos, gerenciamento de usuários locais
- Estrutura de diretórios, comandos básicos do shell, 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
- Familiaridade com a distribuição Kali Linux
- 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 até 03 (três) Máquinas Virtuais (VM) simultaneamente.
- Configuração mínima de 8GB de RAM, 50 GB de espaço livre em disco, porta USB e placa de rede (RJ45 ou *wireless*) para acesso à Internet.
- Desejável 02 (dois) monitores para incremento na produtividade.
- Software de Virtualização: VMWare ou VirtualBox, preferencialmente, a versão mais atualizada.

MATERIAL RECEBIDO

- As Máquinas Virtuais com as aplicações utilizadas nos exercícios
- Slides do Curso no formato PDF
- Acesso ao ambiente GoHacking Academy
- 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 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 Teste de Invasão (Pentest)
- Planejar um Teste de Invasão (Pentest)
- Adotar metodologia para testes de segurança
- Realizar um pentest e produzir relatório
- Identificar e explorar vulnerabilidades em sistemas windows
- Identificar e explorar vulnerabilidades em sistemas linux
- Identificar e explorar vulnerabilidades em aplicações web
- Realizar ações de Engenharia Social
- Planejar atividades para Pentest Físico

BRUNO CORTES