ETHICAL HACKING WIFI PENTESTING (EHWP)

DESCRIÇÃO

Instrutor: Nelson Murilo

Nível: Básico

Carga Horária: 32hrs

O curso Ethical Hacking WiFi Pentesting (EHWP) apresenta técnicas ofensivas de exploração de redes sem-fio (WiFi), trabalhando os conceitos, características, ferramentas e métodos dos ataques a redes corporativas.

As redes WiFi são uma realidade não somente nas casas das pessoas como em empresas de todos os tamanhos e que podem ser vítimas dos mais variados tipos de ataque. Isso nos leva a supor que, mais cedo ou mais tarde, sua organização será atacada e comprometida em algum nível.

Quais são as principais vulnerabilidades para as redes WiFi? Que características podem afetar a segurança o facilitar ataques? Que ferramentas e técnicas poderiam nos auxiliar a identificar vulnerabilidades em ambientes WiFi? Essas e outros perguntas serão respondidas nesse treinamento que possui uma abordagem 100% prática, conduzido por uma bateria de demonstrações e exercícios.

O curso trabalha técnicas clássicas e atuais de exploração, utilizando uma série de ferramentas passando pelos conceitos e entendimento de cada ataque descrito.

MÓDULO 1 – Visão Geral

1. Tipos de rede
   - Frequência, dispositivos, potência, sensibilidade, etc.
2. Modos
   - Ad-Hoc, Gerenciado, Promiscuo e Monitor

3. Limitações
   - Hardware, Sistemas Operacionais, Drivers, Virtualização, Legislação
   - Possíveis hacks

MÓDULO 2 – Ataques Passivos

1. Portal
   - Conceitos, Ferramentas, Demos/Exercícios

2. Evil Twin
   - Conceitos, Ferramentas, Demos/Exercícios

3. Redes preferenciais
   - Conceitos, Ferramentas, Demos/Exercícios

MÓDULO 3 – Ataques Clássicos

1. WPS
   - Conceitos, Definição, Ferramentas, Demo/Exercícios

2. WEP
   - Conceitos, Definição, Ferramentas, Demo/Exercícios

3. WPA/2
   - Conceitos, Definição, Ferramentas, Demo/Exercícios

4. WPA Enterprise
   - Conceitos, Definição, Ferramentas, Demo/Exercícios

5. WPA 3
   - Ataques básicos

MÓDULO 4 - Medidas de proteção

1. WPA 3.0
2. Métodos de autenticação
3. Eficácia
4. Limitações

FERRAMENTAS UTILIZADAS NO CURSO

1. Aircrack-ng suíte (Aircrack-ng, Airmon-ng, Airbase-ng, Airodump-ng, etc.)
2. Bettercap
3. Bully
4. Cowpatty
5. Freeradius
6. HashCat e HCX Tools (Hcxdumptool, Hcxpcapngtoolstool, etc.)
7. Hostapd
8. Kismet
9. Reaver
10. Tcpdump, Tshark, Wireshark
11. Ferramentas e scripts desenvolvidos pelo autor com foco no conteúdo do curso

PRÉ-REQUISITOS

- Conhecimentos básicos em Sistema Operacional Linux
  - Estrutura de diretórios, comandos básicos do shell (bash), configuração de rede e processos
- Conhecimentos básicos de Rede de Computadores e Serviços de Rede
  - Protocolo TCP/IP, HTTP, HTTPS, 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
- 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 01 Máquina Virtual (VM).
- Configuração mínima de 8GB de RAM, 60 GB de espaço livre em disco, porta USB e interface *wireless*.
- Software de Virtualização: VMWare, versão mais atualizada, de preferência Pro *Workstation* (para hosts Windows ou Linux) ou Pro *Fusion* (para host Mac OS).

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:

- Entender os fundamentos de operação de rede sem-fio (WiFi)
- Executar as atividades de *Pentesting* em ambiente WiFi
- Entender aspectos fundamentais da Segurança Ofensiva em redes WiFi
- Compreender a importância das atividades de exploração de redes sem-fio em Segurança da Informação
- Identificar falhas e vulnerabilidades internas da infraestrutura WiFi de uma organização
- Utilizar de ferramentas do Sistema Operacional Linux para executar atividades ofensivas em WiFi
- Proteger, detectar e responder a atividades ofensivas de exploração de redes sem-fio

NELSON MURILO