

Capítulo 1 - Kali Linux 2020

1. Pentesting con Kali

1.1. Introducción, descarga e instalación

1.2. Visión de Kali y políticas

1.3. Aplicaciones en Kali

Capítulo 2 - Information Gathering

2. Introducción

2.1 Footprinting activo

2.2 Descubrimiento DNS

2.3 Banner grabbing

2.3.1 Maltego

2.3.2 Fingerprint web

2.3.2.1 SMB

2.3.2.2 SMTP

2.3.2.3 SNMP

2.3.2.4 VoIP

2.3.2.5 IDS/IPS

2.3.3 Footprinting pasivo

2.3.1 Whois

2.3.2 Google / Bing

2.3.3 Shodan

2.3.4 Robtex

2.3.5 Information leakage

2.3.6 Social engineering

Capítulo 3 - Análisis de vulnerabilidades y ataques a contraseñas

3.1 Introducción

3.2 Análisis de vulnerabilidades (PTES)

3.2.1 Pruebas

3.2.2 Validación

3.2.3 Investigación

3.3 Análisis con Kali

3.3.1 Nmap + NSE

3.3.2 OpenVAS

3.3.3 Nessus

3.3.4 Nikto

3.3.4 Faraday

3.4 Ataques a contraseñas

3.4.1 Métodos de ataque

3.4.2 Tipos de ataque

3.4.2.1 Ataques sin conexión

3.4.2.2 Ataques con conexión

3.4.2.3 Pass the Hash

Capítulo 4 - Explotación

4.1 Introducción

4.2 Tipos de payloads

4.3 Explotación en Kali

4.3.1 Searchsploit

4.3.2 Metasploit

4.3.2 POC: Pivote + 0Day

4.3.2.1 POC: Exploiting e ingeniería inversa

4.3.2.2 Network exploitation

4.3.2.3 MSF Payload creator

4.3.2.4 Termineter

4.3.2.5 JBoss-Autopwn

4.3.3 SE Toolkit

4.3.3.1 Vectores de ataque

4.3.3.2 POC: Powershell y la puerta de atrás

Capítulo 5 - Auditoría de aplicaciones web

5.1 Introducción

5.2 Explotación de vulnerabilidades web comunes

5.2.1 XSS

5.2.1.1 XSS reflejado

5.2.1.2 XSS persistente

5.2.1.3 CSRF

5.2.1.4 SQL injection

5.2.1.5 LFI / Path transversal

5.2.1.6 RFI

5.3 Aplicaciones de seguridad web en Kali

5.3.1 Aplicaciones proxy

5.3.2 Aplicaciones para fuzzing

5.3.3 Escáner de vulnerabilidades web

5.3.4 Explotación de bases de datos

5.3.5 Identificación de CMS

5.3.6 Identificación de IDS/IPS

5.3.7 Indexadores web

Capítulo 6 - Ataques wireless

6.1 Introducción

6.2 Tipos de ataques inalámbricos

6.3 Herramientas wireless en Kali

6.3.1 Suite air*

6.3.1.1 Airodump-ng

6.3.1.2 Aireplay-ng

6.3.2 Evasión de configuraciones básicas de seguridad

6.3.3 POC: Bypass MAC + Bypass DHCP + SSID oculto

6.3.4 Captura e interpretación de tráfico abierto

6.3.4.1 POC: MITM en el aire y Hijacking de sesión

6.3.5 Hacking WEP

6.3.6 Hacking WPA & WPS

6.3.6.1 POC: Hacking WPA/WPA2

6.3.6.2 POC: Hacking WPA2 con WPS

Capítulo 7 - Forense con Kali

7.1 Introducción

7.2 Captura de evidencias

7.3 Tratamiento

7.3.1 POC: Análisis de una imagen

7.4 Forense de red

7.4.1 Captura de evidencias en red

7.4.2 Fingerprint

7.4.3 POC: Forense de red

7.5 Forense de RAM

7.5.1 POC: Forense de red

Capítulo 8 - Ataques a redes

8.1 Introducción

8.1.1 Herramientas en Kali

8.2 Envenenamiento de redes

8.2.1 Ataques a IPv4

8.2.2 Ataques a IPv6

8.2.3 VoIP

8.3 MITM

8.3.1 ARP spoofing

8.3.2 POC: arpspoof

8.3.3 POC: ettercap

8.3.4 POC: mitmproxy

8.3.4 POC: hijacking

8.4 DNS spoofing

8.4.1 POC: dns spoofing

8.5 Bettercap

8.5.1 POC: Bettercap