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

2.3Banner grabbing

2.3.1 Maltego

2.3.2Fingerprint 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

8.5 Bettercap

8.5.1 POC: Bettercap