Footprinting: reconocimiento de información pública de sistemas

RECONNAISSANCE PHASE (Step 1 of Ethical Hacking)

EXTERNAL FOOTPRINTING
(Outside the Network)

INTERNET / PUBLIC SOURCES

CONCEPTS / METHODS

OSINT
(Open Source Intelligence)

- Search Engines (Google Hacking)
- Social Media Analysis
- WHOIS Lookups
- DNS Interrogation
- Email Harvesting

TOOLS

COMMON TOOLS

Google, Shodan, Maltego

`whois`

`nslookup`, `dig`

`theHarvester`

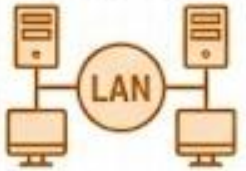
GOALS / INFO GATHERED

TARGET INFORMATION

- Domain Names & Subdomains
- Public IP Ranges
- Employee Names & emails
- Technology Stack Details
- Physical Locations

NETWORK PERIMETER / FIREWALL

INTERNAL FOOTPRINTING
(Inside the Network)



INTERNAL NETWORK

CONCEPTS / METHODS

ACTIVE SCANNING & ENUMERATION

- Network Scanning (Ping Sweep)
- Port Scanning
- Service & Version Detection
- User & Share Enumeration
- Packet Sniffing

TOOLS

COMMON TOOLS

`nmap`

`Wireshark`, `tcpdump`

`netcat`

`enum4linux`, PowerShell

GOALS / INFO GATHERED

NETWORK MAPPING & ASSETS

- Live Hosts & Topologies
- Open Ports & Services
- OS Versions & Patches
- User Accounts & Groups
- Network Shares & Permissions

Disclaimer: Footprinting should only be conducted ethically and legally with proper authorization.

Instalación de Herramientas

Comandos

```
sudo apt-get install nmap

sudo apt-get install whois

sudo apt-get install amass

sudo apt-get install nuclei

sudo apt-get install sniper
```

NMAP

Función Principal: Envía paquetes a una red o dirección IP específica y analiza las respuestas para determinar qué hosts están activos, qué puertos están abiertos y qué servicios (y versiones) se están ejecutando en esos puertos.

Para qué sirve en Footprinting: Te permite crear un "mapa" de la red del objetivo. No solo te dice "la puerta está abierta", sino que te dice "la puerta está abierta y detrás hay un servidor web Apache versión 2.4.49 corriendo en un sistema Linux".

Comando típico: nmap -sV -sC <ip> (Escanea versiones y usa scripts por defecto).

WHOIS

Función Principal: Busca información administrativa sobre quién es el propietario de un nombre de dominio o un bloque de direcciones IP.

Para qué sirve en Footprinting: Revela información "burocrática" valiosa: nombres de las personas de contacto, correos electrónicos, números de teléfono, direcciones físicas y servidores DNS autoritativos.

Esta información es crucial para ataques de Ingeniería Social o para ampliar la superficie de ataque buscando otros dominios registrados por la misma persona.

AMASS

Función Principal: Realiza una enumeración de DNS (Nombres de Dominio) extremadamente profunda. Utiliza múltiples técnicas: scraping de fuentes abiertas (OSINT), fuerza bruta de subdominios, transferencias de zona, etc.

Para qué sirve en Footprinting: Es, probablemente, la mejor herramienta actual para encontrar subdominios ocultos u olvidados (ej: dev.empresa.com, test.empresa.com). Cuantos más subdominios encuentres, más grande es tu superficie de ataque y más probabilidades tienes de hallar un fallo.

NUCLEI

Función Principal: Envía peticiones a los objetivos basándose en una lista enorme de plantillas YAML creadas por la comunidad. Cada plantilla busca una vulnerabilidad específica o una mala configuración.

Para qué sirve en Footprinting/Escaneo: A diferencia de Nmap (que busca puertos), Nuclei busca fallos web específicos. Por ejemplo, si sale una vulnerabilidad nueva hoy, la comunidad crea una plantilla en horas y tú puedes usar Nuclei para escanear miles de dominios buscando solo ese fallo específico. Es excelente para detectar tecnologías expuestas o CVEs (vulnerabilidades conocidas) recientes.

SN1PER

Función Principal: Ejecuta automáticamente Nmap, Whois, Amass, Nuclei y muchas otras herramientas en secuencia contra un objetivo y te genera un reporte unificado.

Para qué sirve en Footprinting/Escaneo: Ahorra tiempo. Es ideal para la fase inicial cuando quieres lanzar un reconocimiento masivo "sin manos". Lanzas Sn1per contra un dominio y él se encarga de recolectar toda la información posible (puertos, subdominios, vulnerabilidades básicas) mientras tú te enfocas en analizar los resultados.