Test de Intrusión: Reconocimiento y Enumeración

1. Footprinting: Se obtiene una “instantanea” de los elementos observables en la red local (IP activas, protocolos usados, topología, si hay IDS/IPS…)
2. Fingerprinting: Una vez identificadas las máquinas en la red, se escanean para obtener información de estas (Sistema operativo y su versión, servicios activos y sus versiones, Info del IDS o firewall desplegado)

Reconocimiento

- Activo: Interacción directa con el objetivo, se tiene interacción directa con la organización victima. Hay un alto riesgo de detección, se usan barridos de ping o conexiones de puertos de alguna aplicación.
- Pasivo: No se tiene interacción con el objetivo. Se obtiene mediante google, IP o puertos abiertos. Se usa Sniffing.

Capa de enlace

Se suele realizar el descubrimiento de esta capa medainte el uso del protocolo ARP para descubrir servicios sin ser detectado, para ello se usan las siguientes herramientas:

- ARPing
  - Envía una trama ARP en la capa de enlace como si fuera un ping en la capa de red
  - Útil en máquinas con el ping deshabilitado
  - Evita detección por firewalls básicos

```
arping 192.168.56.6 -c 1
```

- Netdiscover: similar a a ARPing

```
#Para una interfaz
netdiscover -i eth0

#Ficheros de entrada
netdiscover -l lista_ips.txt

#Ragos de IP
netdiscover -r 192.168.56.0/24

#Modo pasivo (Muy lento)
netdiscover -p
```

- NMAP
- Metasploit