# 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.

### [L2] 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: Permite evitar el envío de ping
  - Sondeo de lista (-sL)
  - Deshabilitación de ping (-Pn)
  - Enviando combinaciones arbitrarias de sondas

- Metasploit
  - Escaneo y Explotación de vulnerabilidades con Metasploit
  - [Intrusión Extra] Metasploit para dummies

> Las herramientas utilizadas en esta capa están limitadas debido a que las solicitudes ARP no atraviesan los routers y solo detectan sistemas de la misma subred

## [L3] Capa de red

El descubrimiento en capa 3 se basa en ICMP.

- fping: versión de ping optimizada para escaneos simultáneos. En ligar de enviar paquetes a un solo objetivo hasta que pase cierto período de tiempo, envia un paquete ping y pasa al siguiente objetivo.
  - El flag "-a" muestra los sistemas activos
  - El flag "-g" genera una lista desde la máscara de red IP proporcionada o una IP de inicio y otra de fin.
  - Si se define una red con máscara de red, las direcciones de red y broadcast serán excluidas.
- hping3: Además de paquetes ICMP, también puede enviar TCP, UDP y RAW-IP.

```
#Permite trazar rutas de conexión y evadir reglas de firewalls
hping3 udc.gal -t 1 --traceroute

#Permite realizar ataques DDOS y DOS:
hping3 --rand-source 192.168.56.6
hping3 --rand-source --flood 192.168.56.4
```

- NMAP: se puede realizar escaneo de red mediante flag "-sn". Para evitar el uso de ARP se inserta el flag "–disable-arp-ping"

## [L4] Capa de transporte

Basado en TCP/UDP. Hay que distinguir entre descubrimiento (Detectar máquinas) y enumeración (escaneo de puertos). En este tipo de descubrimiento se suelen utilizar los puertos conocidos para saber si una máquina está apagada.

- hping3

```
#Se escanean puertos conocidos con el flag SYN de TCP
hping3 --udp 192.168.56.4 -p 53

#Se escanean puertos conocidos por UDP (Si devielve flag SA, el puerto está
abierto, si devuelve RA, entonces está filtrado o cerrado.)
hping3 -S udc.gal -p 80

#Se puede ver cuanto tiempo lleva la máquina arrancada
```

```
hping3 -p 443 -S --tcp-timestamp udc.gal
```

- NMAP

```
#Escaneo de puertos conocidos usando flag SYN de TCP
nmap 192.168.56.4 -PS80 -sn

#Escaneo de puertos conocidos usando flacg ACK de TCP
nmap 192.168.56.4 -PA80 -sn

#Escaneo de puertos conocidos por UDO
nmap udc.gal -PU53 -sn
```

# Enumeración

Tras realizar el descubrimiento y tener identificada la topología de la red local,se procede a escanerar en profundidad para obtener la información para diseñar un vector de ataque:

- Rangos IP, registros DNS y subdominios
- Puertos abiertos y filtrados
- Servicios en escucha y en uso
- Sistema operativo
- IDS o IPS activos
- Firewall activos.

## DNS

Se implementa como una base de datos distribuida. Usa una arquitectura de cliente servidor:

- Servidor DNS: contienen información sobre una porción del espacio de nombres
- Cliente DNS: Realizan preguntas a los servidores para conocer la correspondencia entre nombre y dirección IP.

## nslookup

```
#Búsqueda de servidor de nombres
nslookup udc.gal
nslookup -querytype=mx udc.gal
```

Tipos de registro de recurso DNS:

- A: Puntos para alojar la IP
- MX: pintos para el servidor de correo electrónico
- NS: Puntos al servidor de nombres de host
- CNAME: Nombramiento canónico que permite que los alias se alojen
- SOA: Indica autoridad para el dominio
- SRV: Registro de servicio
- PTR: Mapa las direcciones IP al nombre de host

- INFO: Información del host.

Verificación SPF: un registro SPF es un registro TXT que forma parte del archivo de zona DNS de un dominio, el propósito de este es evitar que los spammers envíen mensajes con direcciones falsificadas en su dominio:

```
nslookup -querytype=txt udc.gal
```

## Zonas de transferencia DNS

Con el comando “dig” se pueden obtener los name servers:

```
dig udc.gal
```

Con el mismo comando se puede realizar una transferencia de zonas sobre uno de los Name Servers

```
dig axfr @nsztm2.operadora.es zonetransfer.me
```

## DNSRECON

```
dnsrecon -d url.com -D /usr/share/wordlist/dnsmap.txt -t std --xml
dnsrecon.xml
```

- -d: indica el dominio
- -D: indica el diccionario de busqueda para fuerza bruta
- -t: se indica la salida
- -xml: se indica el fichero de salida del reconocimiento

```
dnsrecon -d example.com -a
```

- -a: modo completo

## Google Hacking

Se utilizan opreadores avanzados de google:

- filetype: - Permite restrigir la búsqueda por tipo de documento
- site: - Permite restringir la búsqueda a un sitio determinado
- inurl: - Restringe la búsqueda a páginas que contienen varias palabras
- intext: - Restringe la búsqueda a una palabra determinada en el texto
- allintext: - Restringe la búsqueda a páginas que contengan todos los términos especificados
- intitle: - Restringe la búesqueda a una palabra o frase en el título de la página
- inanchor: - Restringe la búesqueda a páginas que contengan en texto surayado la palabra indicada
- related: - Debe ir continuado de un sitio web, permite ampliar la búsqueda a páginas similares.
- info: - Permite saber si la página es conocida por google
- link: - Permite obtener una muestra de páginas que vinculen a la web indicada
- cache: - Permite ver una versión anterior de la web guardada en cache.

- define: - Permite obtener diferentes definiciones desde distintos glosarios

También se pueden suar caracteres especiales:

- [+]: Fuerza la inclusión de un término
- [-]: Excluye un término de búsqueda
- [“]: Coincidencia exacta con la frase entre comilas
- [.]: Sustitye a un solo caracter
- [*]: Sustituye una palabra
- [|]: Operación OR

## Shodan

Buscador para buscar en los banners de las webs. Puede importar muchos protocolos. Opreadores importantes:

- after:dd/mm/yyyy - Muestra servidores actualizados tras la fecha especificada
- before:dd/mm/yyy - Muestra servidores actualizados antes de la fecha especificada
- os:<Sistema_Operativo> - Se filtra la búsqueda por sistema operativo.
- port:<puerto> - Se filtran servidores por el servicio
- net: - busca en un rango de IPS
- hostname:<dominio> - Filtra los resultados por nombre de dominio

Ejemplos de dorks en shodan:

- lis/7.5 200 - Busca dominios con servidor IIS 7.5 y que devuelva mensaje indicando que está disponible
- os:cisco after:01/01/2011 - Buscara sistemas operativos cisco tras la fecha indicada.
- server:SQ-WEBCAM: Permite encontrar cámaras web

## Estado de los puertos

Los puertos pueden estar en los siguientes estados:

- Abierto: disponible
- Cerrado: Puerto cerrado pero disponible, no está en uso
- Filtrado: No accesible al estar filtrado por un dispositivo intermedio
- No-Filtrado: Puerto accesible pero no se sabe si está en uso o no
- Abierto | Filtrado: No se puede determinar si está abierto
- Cerrado | Filtrado: No se puede determinar si está cerrado.

Para determinar el estado se realizan escaneos de puertos

```
# Escaneo ICMP, inutil si el tráfico ICMP está deshabiltiado en el firewall
nmap -PP 192.168.56.4
nmap -PE 192.168.56.4

# Escaneo UDP, muy lento
nmap -sU 192.168.56.4
nmap -sU 192.168.56.4 -p 53
```

```
# Escaneo TCP, puede dejar rastro en los logs y es detectable por los IDS
nmap -sT 192.168.56.4 -p 80

# Escaneo stealth TCP, requiere permisos de admin, realiza una conexión TCP incompleta, por lo que algunos logs no la registran al no completarse la conexión.
#    - De los escaneos más rápidos para redes grandes
#    - No da Falsos positivos
#    - Puede ser detectado por IDS bien configurados
nmap -sS 192.168.56.4 -p 21,80,443

# Escaneo XMAS, basado en el uso de flags PSH, FIN y URG.
#     - Si el puerto está abierto no habrá respuesta
#     - Si el puerto devuelve un paquete RST, está cerrado
#     - Si devuelve un paquetea ICMP unreachable, está filtrado
#     - Fácil de filtrar y detectar
nmap -sX 192.168.56.4

# Escaneo Zombie, se realiza a través de una máquina que tenga IPID secuencial incremental, acceso a la máquina atacada y no tenga a penas tráfico
#    - La máquina escaneada cree que el paquete tiene su origen en la máquina zombie
#    - Se utiliza para identificar reglas del firewall intermedio
#    - La opción -P0 previene que se envíe un ping inicial
#    - La opción -p- se usa para escanear todos los puertos, pero el escaneo es lento
nmap -P0 -p- -sl <IP-maquina-zombie> <IP-objetivo>

# Para realizar un escaneo exhaustivo de la red se puede usar un comando como el siguiente:
nmap -PE -PP -PS80,443 -PA3389 -PU40125 192.168.56.0/24
```

## Fingerprinting de servicios

- Banner Grabbing: cuando se realiza una petición a un servidor, este puede devolver paquetes que contienen información suficiente como para indentificar el tiepo de servicio o si versión, con esta información se pueden identificar vulnerabilidades en el servicio.
- Existen herramientas que permiten ver tanto las tecnologías como los plugins de un servicio

```
whatweb udc.es
```

- Se puede obtener información de los servicios disponibles a través de los banners:

```
nmap 192.168.56.6 -p 22 -sV
nc -vn 192.168.56.4 22
lynx -head -dump http://www.udc.es
```

- También se pueden obtener las versiones de todos los servicios con el siguiente comando:

```
nmap -sV -T4 -F -version-all 192.168.56.4
nmap -sV -T1 -F -version-light 192.168.56.4
```