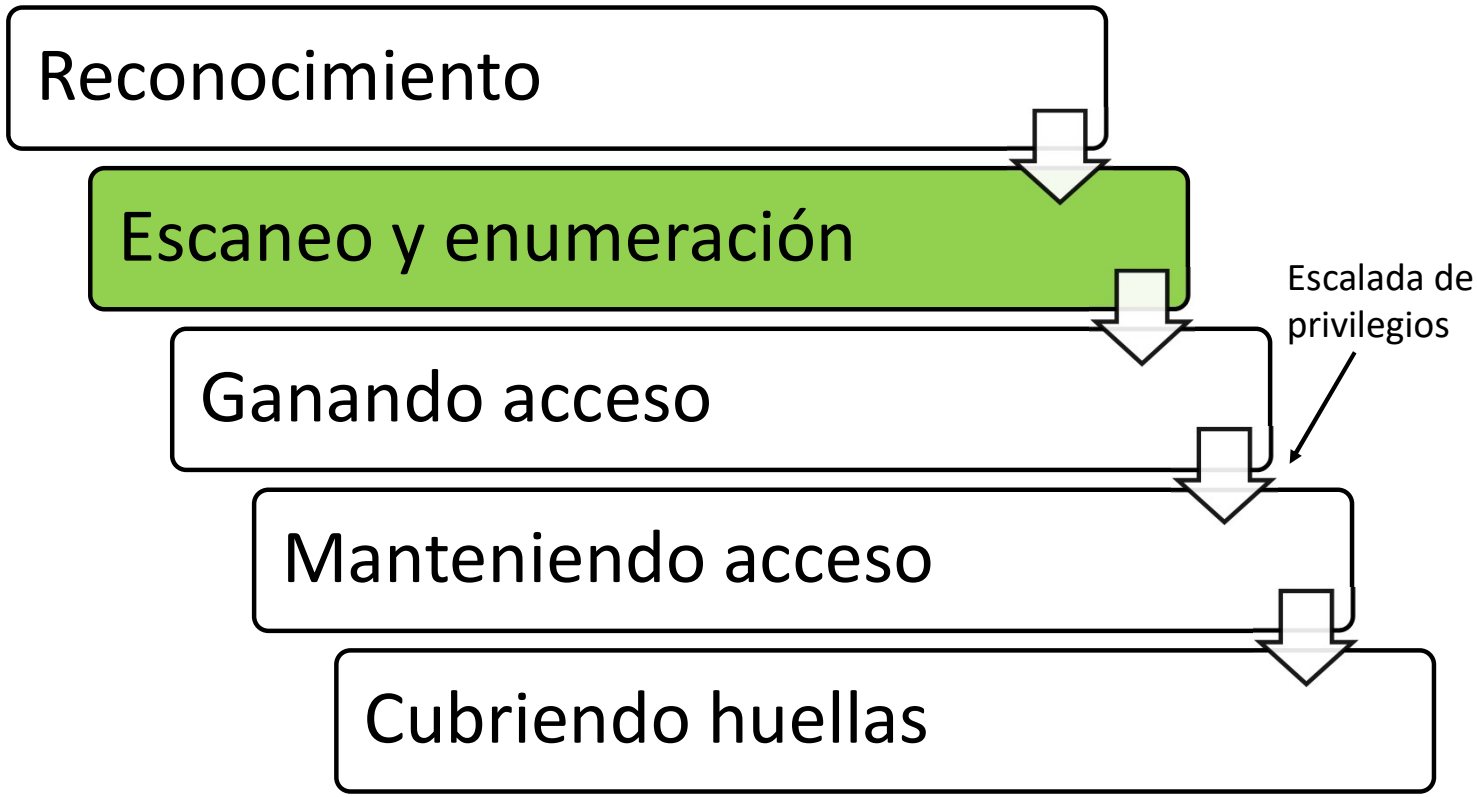
DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Laboratorio 2: Escaneo y análisis de vulnerabilidades

# Fundamentos de ciberseguridad

Profesor
Juan Ignacio Iturbe A.

# Fases del Hacking



# Introducción

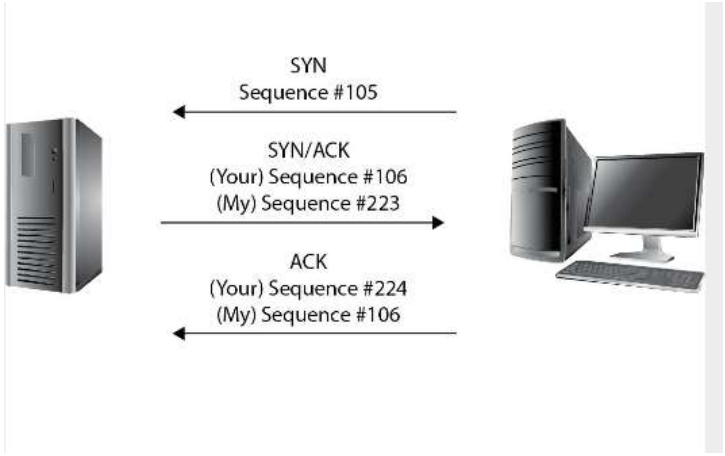

- En la etapa de reconocimiento se obtiene un montón de información públicamente disponible.
- En el escaneo y enumeración el esfuerzo será mucho más focalizado.
- Por ejemplo:
  - El reconocimiento pudo entregar el rango de direcciones IP de una organización.
  - El escaneo mostrará cuales de todas esas direcciones se está utilizando.

# Escaneo


"El escaneo es el proceso de descubrir sistemas en la red y observar qué puertos abiertos y aplicaciones pueden estar ejecutándose" [1].

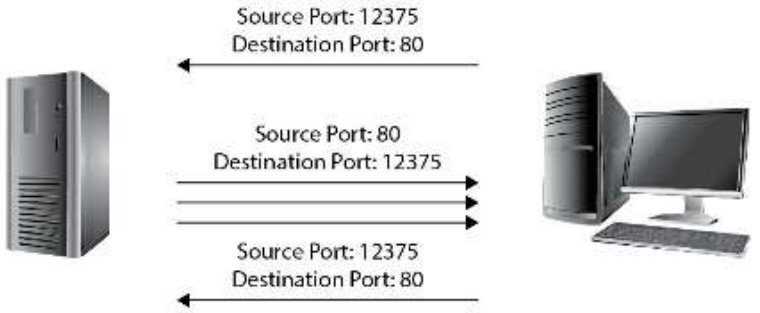
# Importante

- En esta etapa se requiere el conocimiento obtenido en redes computacionales. Especialmente lo relacionado en TCP/IP.
- Repasar funcionamiento y parámetros de:
  - Protocolos de nivel de aplicación (ej. HTTP, DNS, SSH)
  - TCP (ej: handshake, flags)
  - UDP (ej: puertos)
  - IP (ej: subnetting, flags)
  - Ethernet (ej: direccionamientos Checksum, etc)



# Numeración de puertos

- La IANA mantiene el Registro de Número de Puerto de Nombre de Servicio del Protocolo de Transporte, que es la lista oficial para todas las reservas de números de puerto.
- Los números de puerto van de 0 a 65,535 y se dividen en tres grupos diferentes:
  - Puertos conocidos 0 – 1.023
  - Puertos registrados 1.024 - 49.151
  - Puertos dinámicos 49.152 -65.535



# Números de puerto importantes

| Port Number | Protocol | Transport Protocol | Port Number | Protocol | Transport Protocol |
|---|---|---|---|---|---|
| 20/21 | FTP | TCP | 110 | POP3 | TCP |
| 22 | SSH | TCP | 135 | RPC | TCP |
| 23 | Telnet | TCP | 137–139 | NetBIOS | TCP and UDP |
| 25 | SMTP | TCP | 143 | IMAP | TCP |
| 53 | DNS | TCP and UDP | 161/162 | SNMP | UDP |
| 67 | DHCP | UDP | 389 | LDAP | TCP and UDP |
| 69 | TFTP | UDP | 443 | HTTPS | TCP |
| 80 | HTTP | TCP | 445 | SMB | TCP |

**Utilice:**

**> netstat <opción>**

`-an:` se muestran todas las conexiones y puertos de escucha, con las direcciones y los números de puerto en forma numérica

`-b :` puede ver el ejecutable vinculado al puerto abierto

# Metodología de escaneo

- Las fases de la metodología de exploración del EC-Council incluyen los siguientes pasos:
  1. Comprobar si hay sistemas vivos.
  2. Comprobar si hay puertos abiertos.
  3. Escanear más allá del IDS.
  4. Realice la captura de banners.
  5. Escanear en busca de vulnerabilidades.
  6. Dibuja diagramas de red.
  7. Preparar proxies.

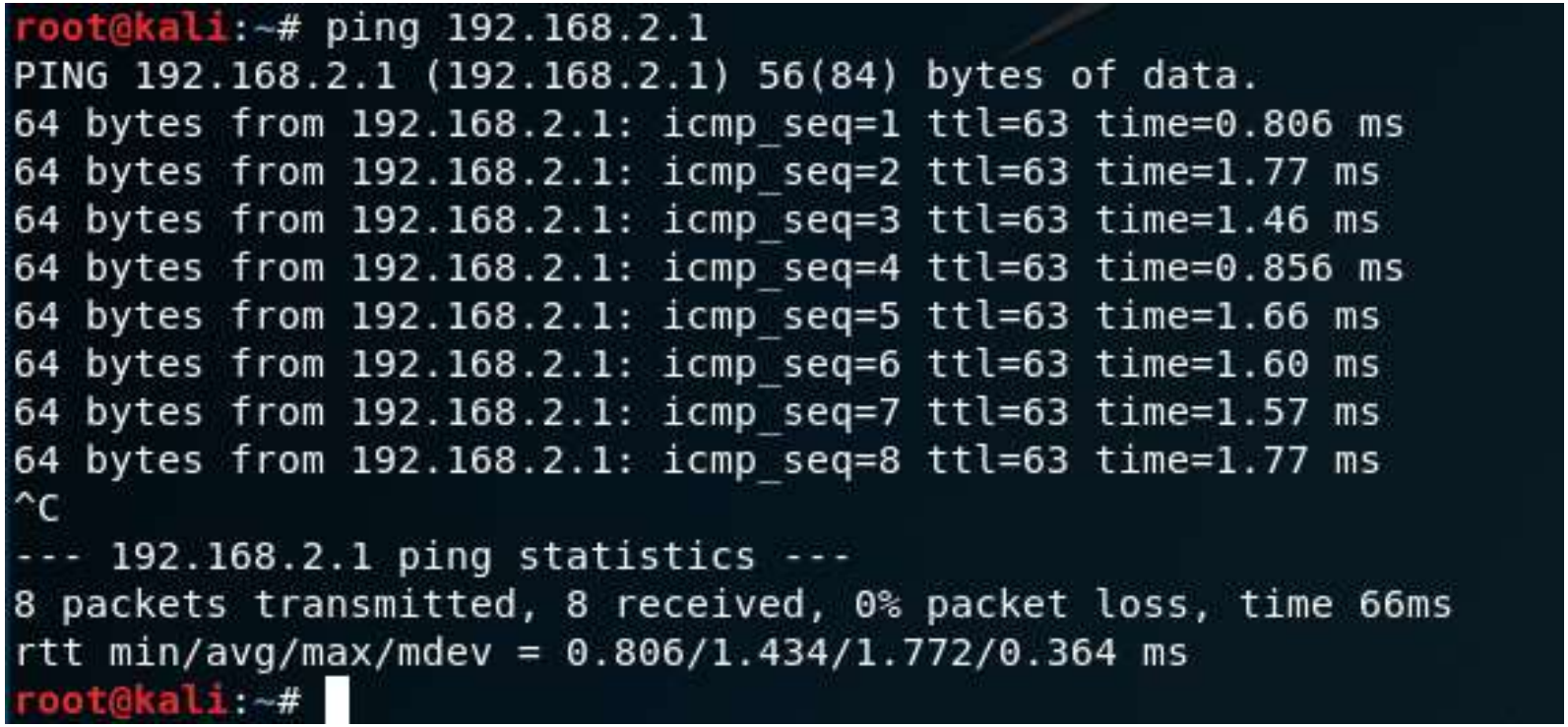
# Comprobar sistemas vivos

- La primera opción es utilizar el protocolo ICMP.
- Este permite el envío de mensajes de error en la capa de red y presenta la información al remitente en uno de varios tipos de mensaje ICMP.
- ICMP está integrado en cada dispositivo TCP/IP y sus respuestas proporcionan información detallada sobre el host.
- El comando *ping* utiliza el protocolo ICMP.

# Tipos de mensajes relevantes ICMP

| ICMP Message Type | Description and Important Codes |
|---|---|
| 0: Echo Reply | Answer to a Type 8 Echo Request |
| 3: Destination Unreachable | Error message indicating the host or network cannot be reached. The codes follow:<br>**0**—Destination network unreachable<br>**1**—Destination host unreachable<br>**6**—Network unknown<br>**7**—Host unknown<br>**9**—Network administratively prohibited<br>**10**—Host administratively prohibited<br>**13**—Communication administratively prohibited |
| 4: Source Quench | A congestion control message |
| 5: Redirect | Sent when there are two or more gateways available for the sender to use and the best route available to the destination is not the configured default gateway. The codes follow:<br>**0**—Redirect datagram for the network<br>**1**—Redirect datagram for the host |
| 8: Echo Request | A ping message, requesting an Echo reply |
| 11: Time Exceeded | The packet took too long to be routed to the destination (code 0 is TTL expired) |

# Comando ping



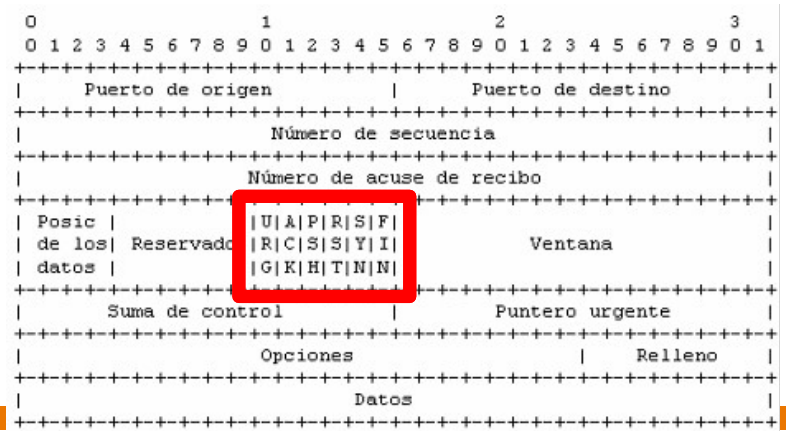

**Notas:**

1. ¿Es posible utilizar canales encubiertos (*Covert channel)* utilizando ICMP?
2. Tenga en cuenta que si no hay respuesta de ICMP no implica que el host no esté vivo.

# Comprobar si hay puertos abiertos

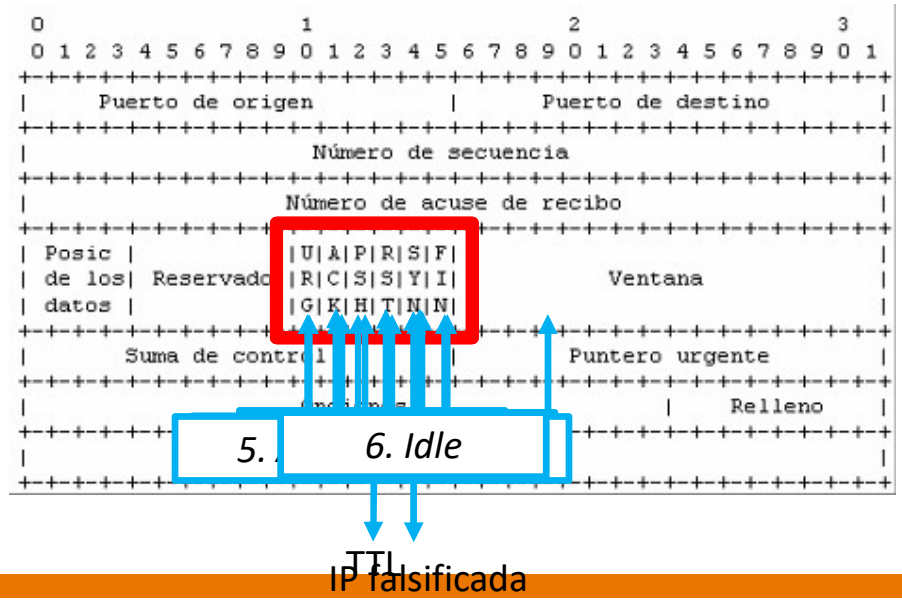
## Escaneo de puertos

- La mayoría de los escáneres de puertos funcionan mediante la manipulación de las flags del protocolo de la capa de transporte.
- Esto permite la identificación de hosts activos y analizar sus puertos.



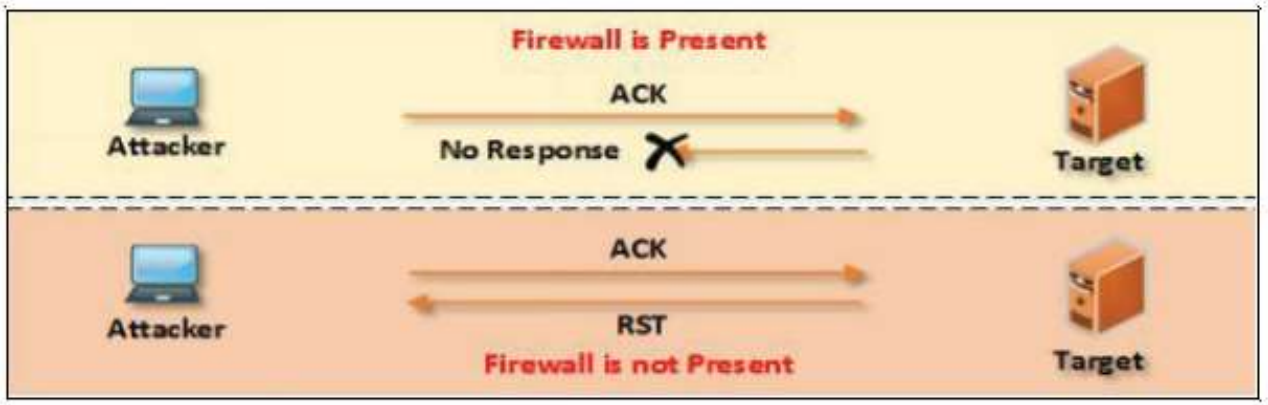
# Tipos de escaneo de puertos

- Existen varios tipos de escaneos de puertos:
  1. Full connect / TCP connect / Full open connect
  2. Stealth / Half-open scan / Syn scan
  3. Inverse TCP flag
  4. XMAS
  5. Ack flag probe
  6. Idle

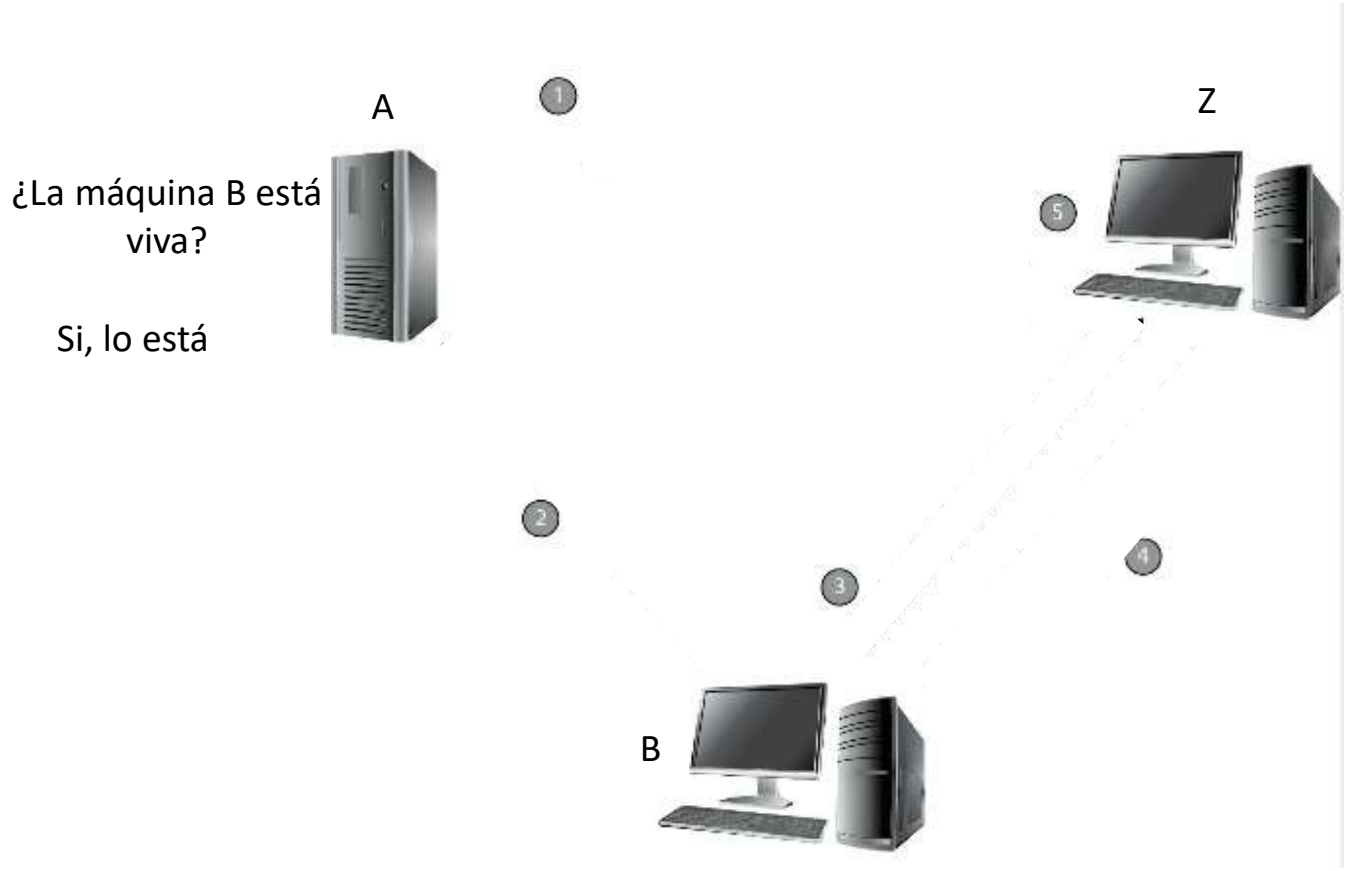


# Escaneo de puertos: XMAS

# Escaneo de puertos: Ack flag probe



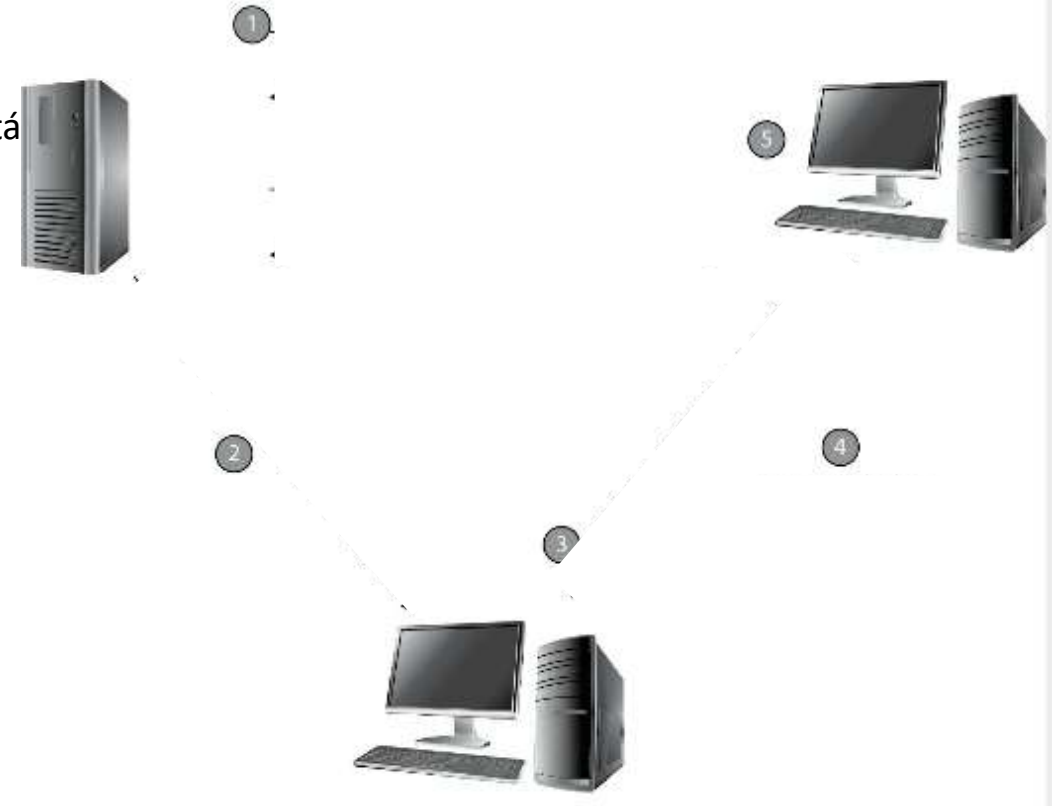
# Escaneo de puertos: Idle (1/2)



# Escaneo de puertos: Idle (2/2)

¿La máquina B está viva?

No, no lo está



# Comparación

| Scan Type | Initial Flags Set | Open Port Response | Closed Port Response | Notes |
|---|---|---|---|---|
| Full (TCP connect) | SYN | SYN/ACK | RST | Noisiest but most reliable.* |
| Stealth | SYN | SYN/ACK | RST | No completion of three-way handshake; designed for stealth but may be picked up on IDS sensors. |
| XMAS | FIN, URG, or PSH | No response | RST | Doesn't work on Windows machines. |
| Inverse TCP | FIN, URG, or PSH (or no flags at all) | No response | RST/ACK | Doesn't work on Windows machines. |

# Nmap

- Es la herramienta de escaneo y enumeración mas utilizada en el planeta.
- Este puede realizar muchos tipos de análisis (incluidos los descrito anteriormente).
- Puede controlarse la velocidad del análisis (lento es mejor).
- Puede desarrollar escaneos sobre TCP y UDP.
- Se requieren permisos de administrador para los sondeos.



https://nmap.org/

# Nmap


- La sintaxis de nmap es la siguiente:

```
# nmap <opciones del scan> <host objetivo>
```

- Ej, para escanear solamente un host y con opciones por defecto:

```
# nmap 192.168.2.1
```

- Ej, para escanear varias IP

```
# nmap 192.168.2.3 192.168.2.20 192.168.3.45
```

- Ej, para escanear todo un segmento de red

```
# nmap 192.168.2.0/24
```

Sitios con mayor detalle:
- https://svn.nmap.org/nmap/docs/nmap.usage.txt
- http://nmap.org/docs.html

# Opciones Nmap

| Nmap Switch | Description | Nmap Switch | Description |
|---|---|---|---|
| -sA | ACK scan | -PI | ICMP ping |
| -sF | FIN scan | -Po | No ping |
| -sI | IDLE scan | -PS | SYN ping |
| -sL | DNS scan (a.k.a. list scan) | -PT | TCP ping |
| -sN | NULL scan | -oN | Normal output |
| -sO | Protocol scan | -oX | XML output |
| -sP | Ping scan | -T0 | Serial, slowest scan |
| -sR | RPC scan | -T1 | Serial, slowest scan |
| -sS | SYN scan | -T2 | Serial, normal speed scan |
| -sT | TCP connect scan | -T3 | Parallel, normal speed scan |
| -sW | Window scan | -T4 | Parallel, fast scan |
| -sX | XMAS scan | | |

Las opciones se puede combinar. Por ejemplo, para ser lo mas silencio posible en un segmento de red:

```
# nmap 192.168.2.0/24 -sS -T0
```

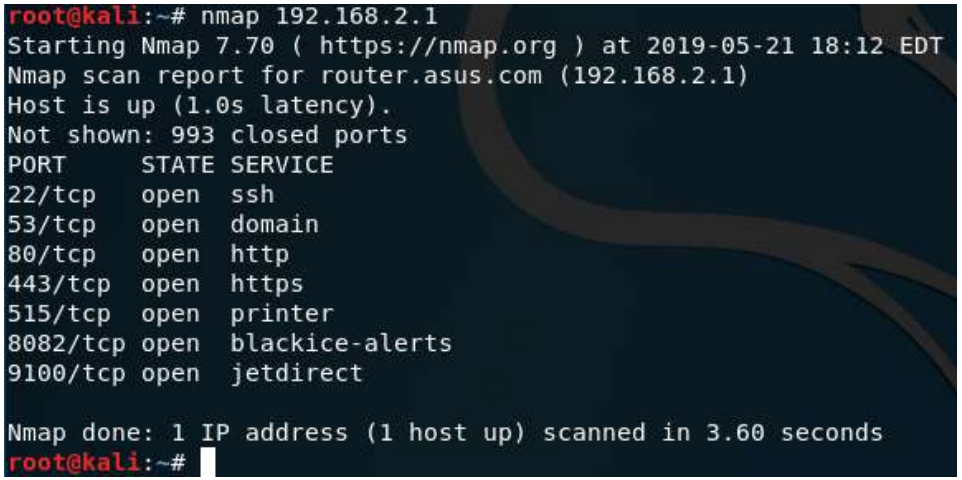
También puedes ser muy agresivo:

```
# nmap 192.168.2.0/24 -sX -T4
```

Sitios con mayor detalle:

- https://nmap.org/man/es/man-port-scanning-techniques.html

# Salida de nmap



# Advertencia

¡No escanear ni analizar vulnerabilidades de hosts en producción, del gobierno o militares sin su autorización por escrito!

# 3. Escanear más allá del IDS.


## Evasión

- El sigilo siempre es importante.
- Ocultar las actividades del hacking es importante para conseguir el objetivo.
- Un firewall o un dispositivo de monitoreo puede detectar los escaneos de puertos o vulnerabilidades.
- Lo que implicará disfrazar la actividad y al ejecutante.
- Para lograr el sigilo suficiente se puede, por ej:
  - Fragmentar paquetes
  - Falsificar un dirección IP
  - Enrutamiento de origen
  - Proxies

# Evasión con fragmentación de Paquetes


- Uno de los métodos más comunes para evadir a los IDS es la fragmentación de paquetes.
- Si se divide el encabezado TCP en varios paquetes, todo lo que ve el IDS en una charla inútil.
- Hay que ser cuidadoso con no inundar el segmento de red con demasiados paquetes, para que no se note el escaneo (*timming y performance*).
- Por ejemplo:

```
# nmap -sS -A -f scanme.nmap.org
```

**Recordar:**
-sS: SYN scan
-A : Detección del sistema operativo
-f : fragmentar paquetes

Otras opciones de evasión para firewalls/IDS, timming y performance en https://svn.nmap.org/nmap/docs/nmap.usage.txt

```
root@kali:~# nmap -sS -A -f scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-21 20:48 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 18 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT       ADDRESS
1   0.20 ms   10.0.2.2
2   0.86 ms   router.asus.com (192.168.2.1)
3   35.42 ms  10.50.1.121
4   35.51 ms  10.50.1.114
5   35.92 ms  176.52.253.114
6   149.05 ms 94.142.118.221
7   123.00 ms 94.142.120.28
8   123.45 ms 213.140.37.13
9   153.38 ms ix-ae-15-0.tcore1.mln-miami.as6453.net (63.243.152.141)
10  198.30 ms if-ae-1-2.tcore2.mln-miami.as6453.net (63.243.152.62)
11  200.68 ms if-ae-3-2.tcore2.dt8-dallas.as6453.net (66.110.72.6)
12  198.15 ms if-ae-34-2.tcore1.lvw-los-angeles.as6453.net (66.110.57.21)
13  236.90 ms if-ae-8-2.tcore1.sv1-santa-clara.as6453.net (66.110.59.9)
14  197.92 ms if-ae-0-2.tcore2.sv1-santa-clara.as6453.net (63.243.251.2)
15  198.28 ms if-ae-38-2.tcore1.sqn-san-jose.as6453.net (63.243.205.74)
16  204.42 ms 216.6.33.114
17  204.46 ms 173.230.159.69
18  198.06 ms scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 220.75 seconds
root@kali:~#
```

# Evasión con suplantación de IP


- Se utiliza una herramienta para la creación de paquetes para ocultar la dirección IP de origen.
- Existen varias herramientas disponibles para ello, por ej: Nmap, Hping, Scapy y Komodia.
- Otras herramientas de sniffing también poseen esta capacidad, por ej.:Ettercap y Cain.
- Ejemplo:

```
# nmap -S 111.222.111.222 -e eth0 -Pn scanme.nmap.org
```

**Recordar:**
-S IP_source: Suplantar IP origen (IP_source)
-e iface: Usar interfaz especificada (iface)
-Pn: Tratar a todos los hosts como en línea (omitir el descubrimiento de host)

# Evasión con enrutamiento desde el origen


- El enrutamiento de origen proporciona otro medio para disfrazar la identidad en una red.
- Fue diseñado para que las aplicaciones especifiquen la ruta que un paquete lleva a un destino. Actualmente en desuso.
- Un atacante podría usar una dirección IP de otra máquina en la subred y recibir todo el tráfico de retorno, independientemente de qué enrutadores estén en tránsito.
- Las protecciones contra los ataques de enrutamiento de origen (en firewalls y routers) son frecuentes y efectivas, por lo que esto no funcionará en redes modernas.

# Evasión con proxies (1/2)


- Se pueden utilizar proxies para esconderse detrás.
- Este se configura para actuar como intermediario entre el equipo atacante y los objetivos.
- Cualquier persona que esté monitoreando la subred ve al proxy intentando todas las acciones, no al hacker.
- Se pueden realizar proxies desde una única ubicación o se pueden distribuir a través de múltiples proxies para disimular aún más la fuente original

# Evasión con proxies (2/2)


- Si desea configurar cadenas de proxy, donde varios proxies ocultan aún más sus actividades, puede usar herramientas como:
  - Proxy Switcher (proxyswitcher.com)
  - Proxy Workbench (proxyworkbench.com)
  - ProxyChains (http://proxychains.sourceforge.net)),
  - Proxy Chain Builder de SoftCab (www.softcab.com/download.php)
  - CyberGhost (cyberghostvpn.com)
  - Proxifier (www.proxifier.com).

# Escaneo de vulnerabilidades


- Es ejecutar una herramienta contra un objetivo para ver qué vulnerabilidades puede contener.
- El escáner en sí mismo debe ser realmente bueno para mantenerse al día con las vulnerabilidades conocidas y realmente bueno para no afectar negativamente a los sistemas a los que apunta.
- Algunos ejemplos:
  - Retina CS (beyondtrust.com)
  - Microsoft Baseline Security Analyzer (MBSA), orientado a tareas específicas. Solamente para Windows.
  - Nessus (tenable.com)

# Escaneo de vulnerabilidades


- Otros escáneres fácilmente disponibles y populares incluyen:
  - GFI LanGuard (www.gfi.com) ofrece vulnerabilidades de calidad y escaneo de cumplimiento, así como administración de parches incorporados.
  - Qualys FreeScan (www.qualsys.com) para probar sitios web y aplicaciones para detectar los principales riesgos y malware de OWASP.
  - OpenVAS (www.openvas.com) es probablemente el mejor de todos, aunque es posible que nunca haya oído hablar de él.

# OpenVas


```
root@kali:~# apt-get update
root@kali:~# apt-get dist-upgrade
...
root@kali:~# apt-get install openvas
...
root@kali:~# openvas-setup
/var/lib/openvas/private/CA created
/var/lib/openvas/CA created

[i] This script synchronizes an NVT collection with the 'OpenVAS NVT
Feed'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-
nvt-feed
...
sent 1143 bytes received 681741238 bytes 1736923.26 bytes/sec
total size is 681654050 speedup is 1.00
[i] Initializing scap database
[i] Updating CPEs
[i] Updating /var/lib/openvas/scap-data/nvdcve-2.0-2002.xml
[i] Updating /var/lib/openvas/scap-data/nvdcve-2.0-2003.xml
...
Write out database with 1 new entries
Data Base Updated
Restarting Greenbone Security Assistant: gsad.
User created with password '6062d074-0a4c-4de1-a26a-5f9f055b7c88'.
```

# Construye tu propio laboratorio de prácticas


Construya su propio laboratorio en casa y aislado

- Levante una red inalámbrica (ej. Con su celular, un Access point viejo, etc)
- Utilice equipos viejos, raspberry pi, etc.
- Levante servicios (web, mail, etc)
- Observe el tráfico de la red (wireshark)
- Existen ataques para engañar el switch y que el tráfico se redirija a su máquina (ej. ettercap).
- Realice escaneo de puertos (ej. nmap)
- Investigue y aplique herramientas (ej. Kali).
- Realice escaneo de vulnerabilidades (ej. Nessus, openvas)

# Herramientas


- Colasoft Packet Builder (Editor de paquetes), www.colasoft.com/download/products/download_packet_builder.php
- CurrPorts (Mis puertos abiertos y aplicaciones asociadas), https://www.nirsoft.net/utils/cports.html
- Wireshark (Revisión del tráfico de red en tiempo real), https://www.wireshark.org/
- Nmap, https://nmap.org/
- Hping, https://www.hping.org
- Otras herramientas Mcafee, https://www.mcafee.com/enterprise/en-us/downloads/free-tools.html

**Nota:** Algunas herramientas necesitan permiso de administrador.

# Herramientas de escaneo para uso móvil


- IP Scanner (10base-t.com),
- Fing (www.fing.io),
- Hackode (play.google.com),
- zANTi (www.zimperium.com),
- PortDroid Network Analysis (play.google.com)

# Herramientas de evasión para uso móvil

Evasión

- Proxydroid (github.com)
- Servers ultimate (www.icecoldapps.com)
- NetShade (www.raynersw.com).
- Shadowsocks (shadowsocks.org) Proxy encriptado nacido en China para eludir la censura. No es un VPN.
- Orbot (guardianproject.info). Librerías de desarrollo y otros, para proteger la identidad y las comunicaciones.
- Psiphon (psiphon.ca). VPN, anonimozador y mas. Para ambientes adversos.
- OpenDoor (itunes.apple.com)

Anonimizador

- Guardster (guardster.com),
- Ultrasurf (ultrasurf.us),
- Psiphon (psiphon.ca)
- Tails (tails.boum.org). Sistema operativo que se ejecuta desde un USB.

# Bibliografía


1. Walker, Matt. CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition. McGraw-Hill Education.
2. Nastase, Ramon. Hacking with Kali Linux: A Step by Step Guide for you to Learn the Basics of CyberSecurity and Hacking.
3. Marsh, Nicholas. Nmap 6 Cookbook: The Fat-Free Guide to Network Security Scanning (p. 214). Fat Free Publishing.
4. Oriyano, Sean. Passing the CEH 10: Learning the Certified Ethical Hacker 10 .

# Anexo A: Cabecera IP


https://www.rfc-es.org/rfc/rfc0791-es.txt