

Seguridad de Sistemas

Clase 3: Reconocimiento activo

Contenidos



- Conocer las principales técnicas de reconocimiento activo
- Conocer las diferentes técnicas de scan de puertos y su aplicación
- Conocer la técnica del Banner Grabbing y sus contramedidas

Introducción

- En este módulo, avanzaremos más allá de la recopilación pasiva de información y exploraremos técnicas que implican una interacción directa con los servicios de destino.
- Echaremos un vistazo a algunas técnicas fundamentales, pero tenga en cuenta que hay innumerables servicios a los que se puede dirigir en el campo. Esto incluye Active Directory, por ejemplo, que cubrimos con más detalle en un módulo separado. Sin embargo, veremos algunas de las técnicas de recopilación de información activa más comunes en este módulo, incluido el escaneo de puertos y la enumeración de DNS, SMB, NFS, SMTP y SNMP.

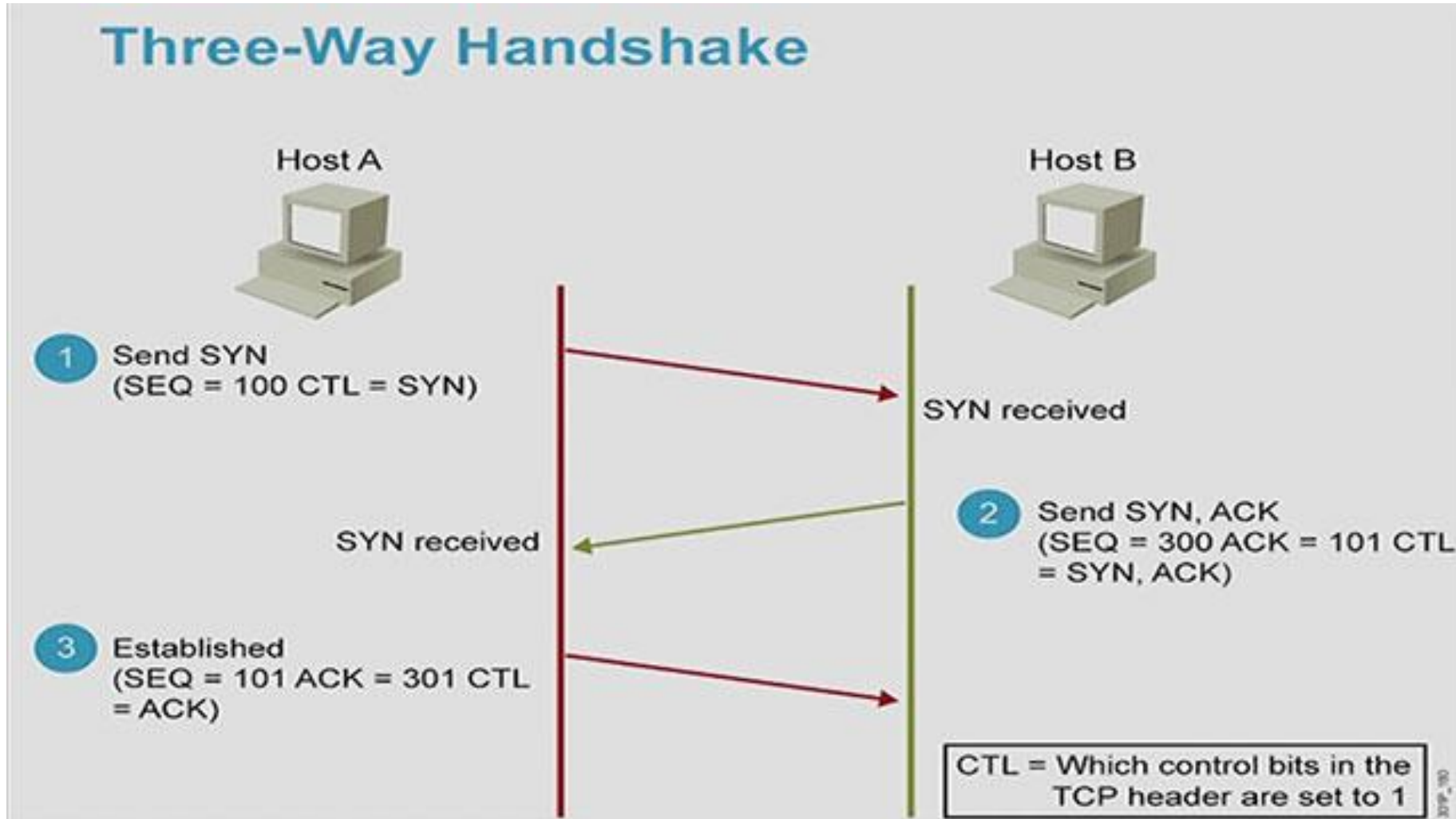
Scan de puertos

- El escaneo de puertos es el proceso de inspeccionar puertos TCP o UDP en una máquina remota con la intención de detectar qué servicios se están ejecutando en el objetivo y qué posibles vectores de ataque pueden existir.
- Es esencial comprender las implicaciones del escaneo de puertos, así como el impacto que pueden tener los escaneos de puertos específicos. Debido a la cantidad de tráfico que pueden generar algunos análisis, junto con su naturaleza intrusiva, ejecutar análisis de puertos a ciegas puede tener efectos adversos en los sistemas de destino o en la red del cliente, como sobrecargar servidores y enlaces de red o activar IDS. Ejecutar el escaneo incorrecto podría resultar en tiempo de inactividad para el cliente.

Scan de puertos

0		1				2			3		
Source Port						Destination Port					
Sequence Number											
Acknowledgment Number											
Data offset	Reserved 0 0 0	N S	C W R	E C E	U R G	A C K	P S H	R S T	S Y N	F I N	Window Size
Checksum						Urgent Pointer					

Scan de puertos

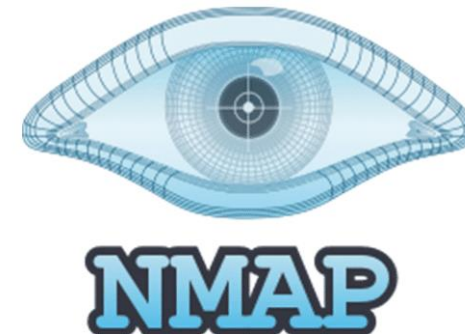


Scan de puertos

- La técnica de escaneo de puertos TCP más simple, generalmente llamada escaneo CONNECT, se basa en el mecanismo de protocolo de enlace TCP de tres vías. Este mecanismo está diseñado para que dos hosts que intenten comunicarse puedan negociar los parámetros de la conexión del socket TCP de la red antes de transmitir cualquier dato. En términos básicos, un host envía un paquete TCP SYN a un servidor en un puerto de destino. Si el puerto de destino está abierto, el servidor responde con un paquete SYN-ACK y el host del cliente envía un paquete ACK para completar el protocolo de enlace.

Scan de puertos

- Nmap
- Es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon y cuyo desarrollo se encuentra hoy a cargo de una comunidad. Fue creado originalmente para Linux aunque actualmente es multiplataforma. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas.



Scan de puertos

Ejemplo de scan de puertos utilizando la herramienta NMAP

```
Nmap scan report for 10.0.2.17
Host is up (0.0014s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
```



USM

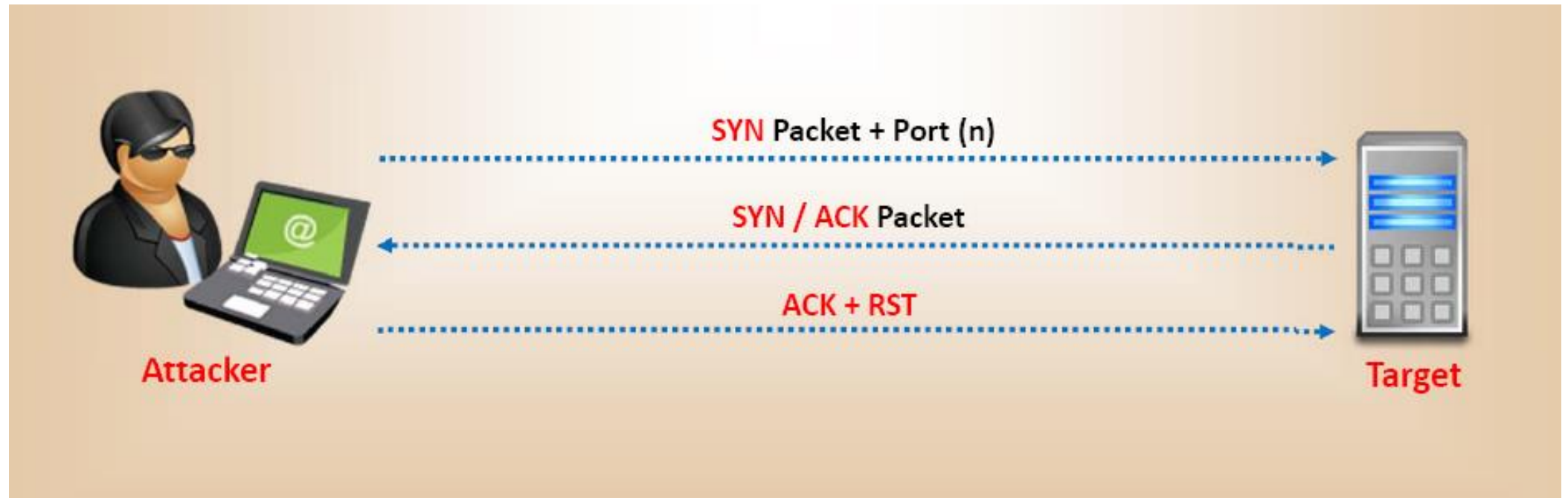
UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Scan de puertos

- **TCP Connect Scanning**
- Cuando un usuario que ejecuta nmap no tiene privilegios de socket sin formato, Nmap utilizará por defecto la técnica TCP connect scan descrita anteriormente. Dado que un escaneo de conexión TCP de Nmap utiliza la API de sockets de Berkeley para realizar el protocolo de enlace de tres vías, no requiere privilegios elevados.
- Sin embargo, debido a que Nmap tiene que esperar a que se complete la conexión antes de que la API devuelva el estado de la conexión, un escaneo de conexión tarda mucho más en completarse que un escaneo SYN.

Scan de puertos

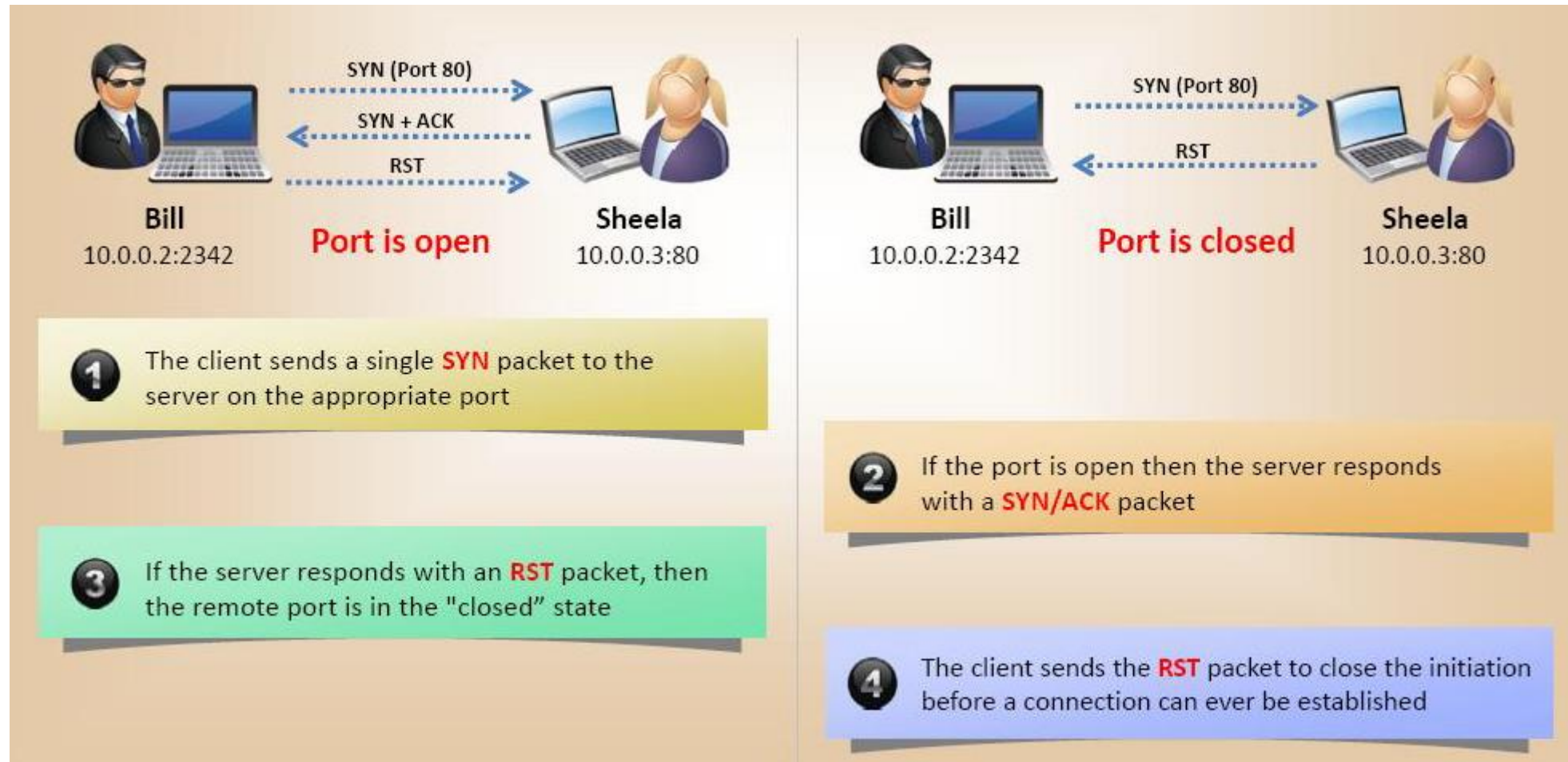
- TCP Connect Scanning



Scan de puertos

- **Stealth / SYN Scanning**
- La técnica de escaneo preferida de Nmap es un SYN, o escaneo “sigiloso”. El uso de un escaneo SYN tiene muchos beneficios y, como tal, es la técnica de escaneo predeterminada que se usa cuando no se especifica ninguna técnica de escaneo en un comando nmap y el usuario tiene la privilegios de sockets sin formato necesarios.
- El escaneo SYN es un método de escaneo de puertos TCP que implica el envío de paquetes SYN a varios puertos en una máquina de destino sin completar un protocolo de enlace TCP. Si un puerto TCP está abierto, se debe enviar un SYN-ACK desde la máquina de destino, informándonos que el puerto está abierto

Scan de puertos



Scan de puertos

- **Xmas Scan**
- Los escaneos Xmas obtienen su nombre del conjunto de indicadores que se encienden dentro de un paquete. Estos escaneos están diseñados para manipular los indicadores PSH, URG y FIN del encabezado TCP. Cuando se ve dentro de Wireshark, podemos ver que los bits alternos están habilitados, o "Parpadeando", como si se iluminara un árbol de Navidad.
- Este tipo de scan, solo aplica a Sistemas Operativos que cumplen el RFC 793, es decir sólo sistemas Linux y OSx

Scan de puertos

- Xmas Scan

```
root@kali:/home/kali# nmap -sX -p 445 192.168.0.156
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-03 18:41 EDT
Nmap scan report for 192.168.0.156
Host is up (0.00042s latency).
PORT      STATE SERVICE
445/tcp    closed microsoft-ds
MAC Address: 08:00:27:AD:64:B0 (Oracle VirtualBox virtual NIC)
```

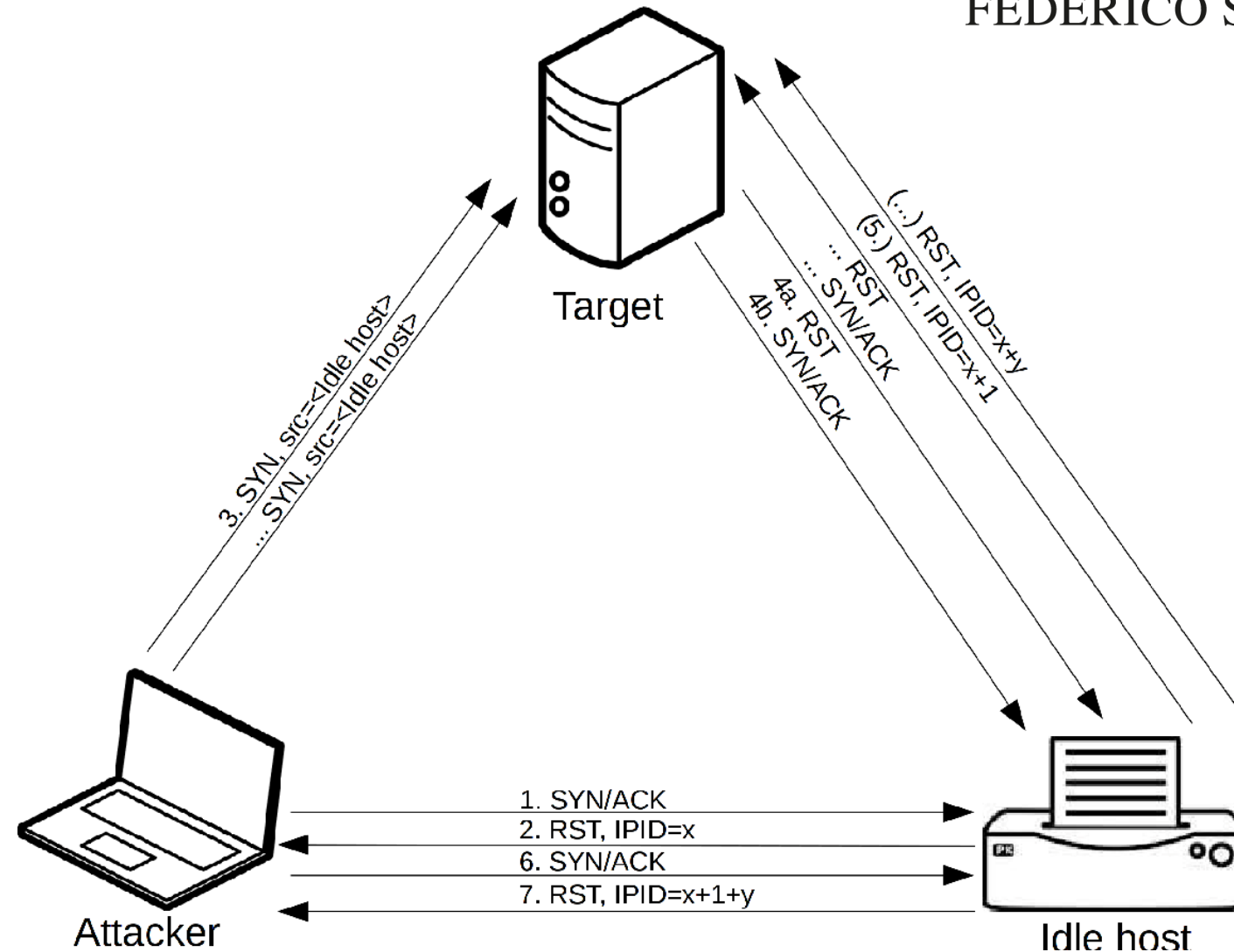
ip.addr==192.168.0.156						
No.	Time	Source	Destination	Protocol	Length	Info
12	2.545376296	192.168.0.155	192.168.0.156	TCP	54	35185 → 445 [FIN, PSH, URG] Seq=1 Win=1024 Ur...
15	2.546088814	192.168.0.156	192.168.0.155	TCP	60	445 → 35185 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

Scan de puertos

- **Idle Scan**
- Es el nombre con el que se conoce a la técnica de escaneo que haciendo uso de hosts zombies oculta completamente la IP origen del escaneo. No ofusca la IP origen de la conexión, sino que ni siquiera envía un sólo paquete al destino.
- El ataque consiste básicamente en forjar el escudo o dispositivo intermedio. Es importante resaltar que el paso más importante en este tipo de ataque no es llevarlo a cabo contra el objetivo sino encontrar el dispositivo zombie.
- Esta técnica es una de las mejores para saltarnos firewall's e IDS.

Scan de puertos

- Idle Scan



Scan de puertos

- **UDP Scanning**

- Al realizar un escaneo UDP, Nmap utilizará una combinación de dos métodos diferentes para determinar si un puerto está abierto o cerrado. Para la mayoría de los puertos, utilizará el método estándar de "puerto ICMP inalcanzable" descrito anteriormente enviando un paquete vacío a un puerto determinado. Sin embargo, para los puertos comunes, como el puerto 161, que es utilizado por SNMP, enviará un paquete SNMP específico del protocolo en un intento de obtener una respuesta de una aplicación vinculada a ese puerto.

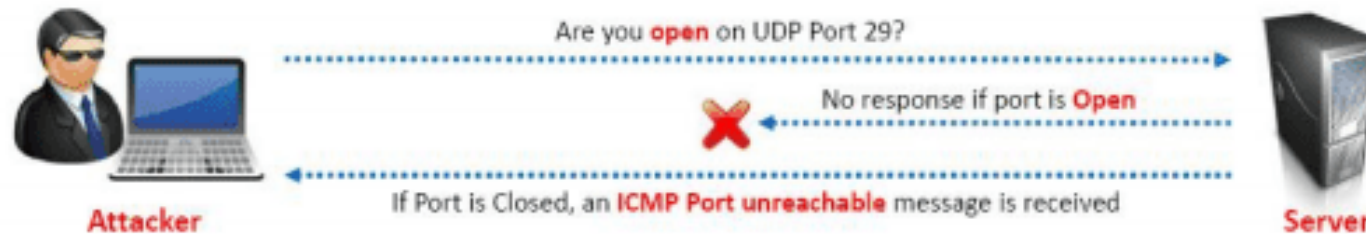
Scan de puertos



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

UDP Scanning



UDP Port Open

- There is no **three-way TCP handshake** for UDP scan
- The system does not respond with a message when the port is **open**

UDP Port Closed

- If a UDP packet is sent to open port, the system responds with **ICMP port unreachable message**
- Spywares, Trojan horses, and other malicious applications use **UDP** ports

Scan de hosts

- **Network Sweeping**
- Para tratar con grandes volúmenes de hosts, o para tratar de conservar el tráfico de red, podemos intentar sondear los objetivos utilizando técnicas de barrido de red, en las que comenzamos con escaneos amplios y usamos escaneos más específicos contra hosts de interés.
- Al realizar un barrido de red con Nmap usando la opción -sn, el proceso de descubrimiento de host consiste en algo más que enviar una solicitud de eco ICMP. Se utilizan varias otras sondas además de la solicitud ICMP. Nmap también envía un paquete TCP SYN al puerto 443, un paquete TCP ACK al puerto 80 y una solicitud de marca de tiempo ICMP para verificar si un host está disponible o no.

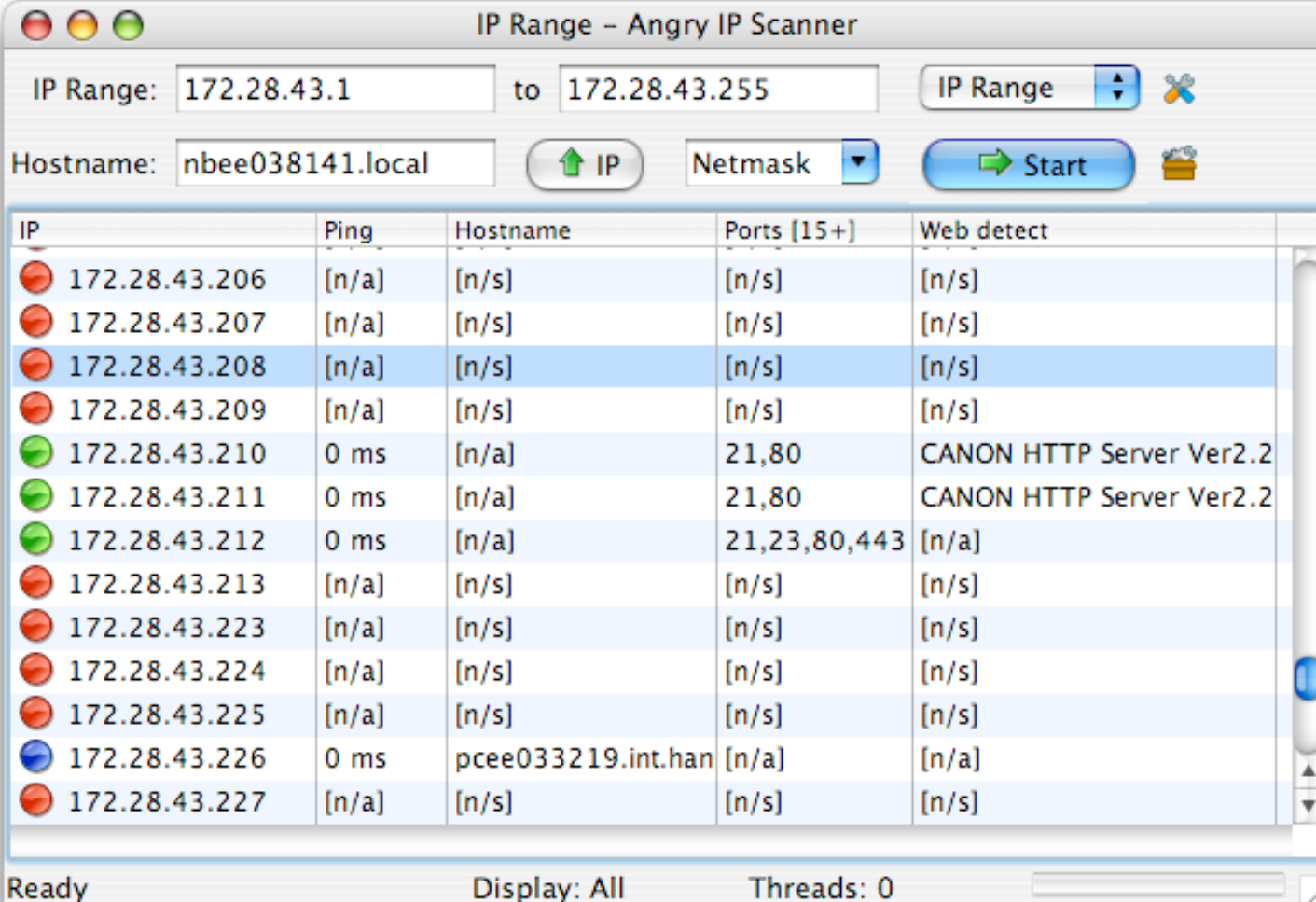
Scan de hosts

- Network Sweeping

```
root@kali:/home/kali# nmap -sn 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-03 16:39 EDT
Nmap scan report for 192.168.0.1
Host is up (0.033s latency).
MAC Address: E8:DE:27:3E:D4:92 (Tp-link Technologies)
Nmap scan report for 192.168.0.152
Host is up (0.45s latency).
MAC Address: 94:EE:9F:8C:A0:A6 (HMD Global Oy)
Nmap scan report for 192.168.0.154
Host is up (0.0027s latency).
MAC Address: 70:1C:E7:E1:D0:5C (Intel Corporate)
Nmap scan report for 192.168.0.155
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 5.43 seconds
```

Scan de hosts

- Angry IP



IP	Ping	Hostname	Ports [15+]	Web detect
172.28.43.206	[n/a]	[n/s]	[n/s]	[n/s]
172.28.43.207	[n/a]	[n/s]	[n/s]	[n/s]
172.28.43.208	[n/a]	[n/s]	[n/s]	[n/s]
172.28.43.209	[n/a]	[n/s]	[n/s]	[n/s]
172.28.43.210	0 ms	[n/a]	21,80	CANON HTTP Server Ver2.2
172.28.43.211	0 ms	[n/a]	21,80	CANON HTTP Server Ver2.2
172.28.43.212	0 ms	[n/a]	21,23,80,443	[n/a]
172.28.43.213	[n/a]	[n/s]	[n/s]	[n/s]
172.28.43.223	[n/a]	[n/s]	[n/s]	[n/s]
172.28.43.224	[n/a]	[n/s]	[n/s]	[n/s]
172.28.43.225	[n/a]	[n/s]	[n/s]	[n/s]
172.28.43.226	0 ms	pcee033219.int.han	[n/a]	[n/a]
172.28.43.227	[n/a]	[n/s]	[n/s]	[n/s]

Ready Display: All Threads: 0

OS Fingerprinting

- Nmap tiene una función incorporada llamada huella digital del sistema operativo, que se puede habilitar con la opción -O.
- Esta función intenta adivinar el sistema operativo del objetivo mediante la inspección de los paquetes devueltos. Esto es posible porque los sistemas operativos a menudo tienen implementaciones ligeramente diferentes de la pila TCP/IP (como la variación de los valores TTL predeterminados y los tamaños de las ventanas TCP) y estas ligeras variaciones crean una huella digital que Nmap a menudo puede identificar.

OS Fingerprinting

```
kali@kali:~$ sudo nmap -O 10.11.1.220
```

```
...
```

```
Device type: general purpose
```

```
Running: Microsoft Windows 2008|7
```

```
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7
```

```
OS details: Microsoft Windows 7 or Windows Server 2008 R2
```

```
Network Distance: 1 hop
```


Banner Grabbing

- También podemos identificar los servicios que se ejecutan en puertos específicos inspeccionando los banners de servicio (-sV) y ejecutando varios scripts de enumeración de sistemas y servicios (-A) contra el objetivo.
- Es importante tener en cuenta que los administradores del sistema pueden modificar los banners. Como tal, estos pueden configurarse intencionalmente como nombres de servicios falsos para engañar a un atacante potencial.
- La captura de banners tiene un impacto significativo en la cantidad de tráfico utilizado, así como en la velocidad del escaneo.

Banner Grabbing

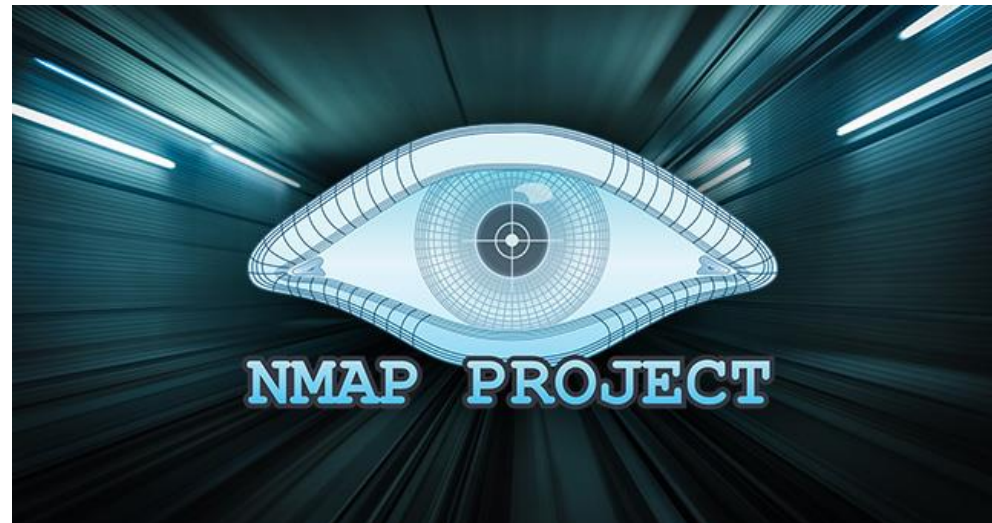
```
root@kali:/home/kali# nmap -sV 192.168.0.158
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-03 17:13 EDT
Nmap scan report for 192.168.0.158
Host is up (0.00036s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp          CUPS 1.7
3306/tcp  open  mysql        MySQL (unauthorized)
6667/tcp  open  irc          UnrealIRCd
8080/tcp  open  http         Jetty 8.1.7.v20120910
8181/tcp  open  http         WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
MAC Address: 08:00:27:9A:E5:14 (Oracle VirtualBox virtual NIC)
```

Banner Grabbing

```
root@kali:/home/kali# nmap -A 192.168.0.158
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-03 17:14 EDT
Nmap scan report for 192.168.0.158
Host is up (0.00054s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 0a:34:3c:32:8a:a9:4e:c5:db:8b:64:77:f8:65:0b:7d (DSA)
|   2048 1b:75:8d:f0:8b:10:b1:99:9c:6a:6a:44:d6:66:a8:1b (RSA)
|   256  f7:db:02:1d:e7:4b:3d:0b:69:eb:6a:f0:29:f5:e5:f4 (ECDSA)
|_  256  bc:4b:63:fa:ae:7d:f0:5b:d3:69:45:a3:d0:5e:98:9d (ED25519)
```

Nmap Scripting Engine (NSE)

- Podemos usar Nmap Scripting Engine (NSE) para lanzar scripts creados por el usuario para automatizar varias tareas de escaneo. Estos scripts realizan una amplia gama de funciones que incluyen enumeración de DNS, ataques de fuerza bruta e incluso identificación de vulnerabilidades. Los scripts de NSE se encuentran en el directorio **`/usr/share/nmap/scripts`**.





USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Nmap Scripting Engine (NSE)

```
root@kali:/home/kali# nmap --script=smb-os-discovery 192.168.0.156
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-03 17:27 EDT
Nmap scan report for 192.168.0.156
Host is up (0.00040s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
1026/tcp   open  LSA-or-nterm
1027/tcp   open  IIS
1053/tcp   open  remote-as
1068/tcp   open  instl_bootc
1216/tcp   open  etebac5
3389/tcp   open  ms-wbt-server
5357/tcp   open  wsapi
MAC Address: 08:00:27:AD:64:B0 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Victima-PC
|   NetBIOS computer name: VICTIMA-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-09-03T17:27:56-04:00
```

Masscan

- Masscan es posiblemente el escáner de puertos más rápido; Puede escanear toda la Internet en aproximadamente 6 minutos, ¡transmitiendo la asombrosa cantidad de 10 millones de paquetes por segundo! Si bien fue diseñado originalmente para escanear todo Internet, puede manejar fácilmente una subred de clase A o B, que es un rango objetivo más adecuado durante una prueba de penetración.
- Masscan no está instalado en Kali por defecto; debe instalarse usando apt install:
 - **apt install masscan**

Masscan

```
root@kali:~# masscan 172.217.0.0/16 -p 80,443 --rate=1000
Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2017-03-02 17:48:47 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 65536 hosts [2 ports/host]
Discovered open port 80/tcp on 172.217.25.207
Discovered open port 80/tcp on 172.217.24.100
Discovered open port 443/tcp on 172.217.24.233
Discovered open port 80/tcp on 172.217.4.181
Discovered open port 80/tcp on 172.217.4.150
Discovered open port 443/tcp on 172.217.11.18
Discovered open port 443/tcp on 172.217.9.46
Discovered open port 443/tcp on 172.217.1.100
Discovered open port 443/tcp on 172.217.17.187
Discovered open port 80/tcp on 172.217.26.220
Discovered open port 80/tcp on 172.217.28.126
Discovered open port 80/tcp on 172.217.25.126
Discovered open port 80/tcp on 172.217.23.52
Discovered open port 443/tcp on 172.217.20.218
Discovered open port 443/tcp on 172.217.25.218
Discovered open port 80/tcp on 172.217.29.160
Discovered open port 443/tcp on 172.217.12.5
Discovered open port 80/tcp on 172.217.20.196
Discovered open port 443/tcp on 172.217.1.48
Discovered open port 443/tcp on 172.217.16.59
Discovered open port 80/tcp on 172.217.22.6
Discovered open port 443/tcp on 172.217.22.52
Discovered open port 80/tcp on 172.217.8.10
Discovered open port 443/tcp on 172.217.17.244
Discovered open port 80/tcp on 172.217.0.179
Discovered open port 443/tcp on 172.217.26.2
```

Hping

- Es un analizador/ensamblador de paquetes TCP/IP orientado a la línea de comandos. La interfaz está inspirada en el comando ping (8) de Unix, pero hping no solo puede enviar solicitudes de eco ICMP. Es compatible con los protocolos TCP, UDP, ICMP y RAW-IP, tiene un modo de ruta de seguimiento, la capacidad de enviar archivos entre un canal cubierto y muchas otras funciones.
- Si bien hping se utilizó principalmente como herramienta de seguridad en el pasado, puede ser utilizado de muchas formas por personas que no se preocupan por la seguridad para probar redes y hosts.

Hping

```
root@kali:/home/kali# hping3 --rand-source 192.168.0.156  
HPING 192.168.0.156 (eth0 192.168.0.156): NO FLAGS are set, 40 headers + 0 data bytes
```

ip.dst==192.168.0.156					
No.	Time	Source	Destination	Protocol	
57	21.621763842	128.231.66.25	192.168.0.156	TCP	
60	22.623514564	119.221.140.98	192.168.0.156	TCP	
61	23.623706136	133.170.234.237	192.168.0.156	TCP	
63	24.624477303	226.167.133.167	192.168.0.156	TCP	
66	25.625002942	165.56.57.248	192.168.0.156	TCP	
67	26.625756924	128.109.33.167	192.168.0.156	TCP	
69	27.625971462	130.248.66.25	192.168.0.156	TCP	
71	28.626903451	116.56.24.30	192.168.0.156	TCP	
72	29.627203733	217.66.109.123	192.168.0.156	TCP	
81	30.627390115	83.40.33.67	192.168.0.156	TCP	
90	31.627529958	194.233.216.142	192.168.0.156	TCP	

Hping

- Ataque SYN Flood

```
root@kali:/home/kali# hping3 -S 192.168.0.156 -p 445 --fast
HPING 192.168.0.156 (eth0 192.168.0.156): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.156 ttl=128 DF id=2565 sport=445 flags=SA seq=0 win=8192 rtt=4.3 ms
len=46 ip=192.168.0.156 ttl=128 DF id=2576 sport=445 flags=SA seq=1 win=8192 rtt=9.8 ms
```

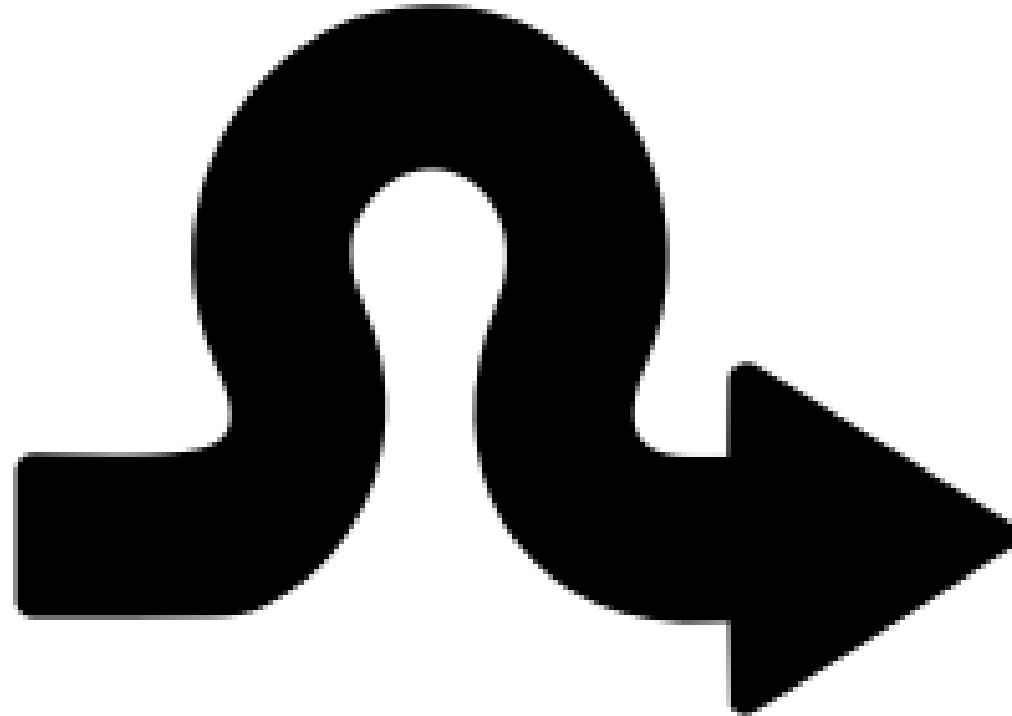
ip.addr==192.168.0.156						
No.	Time	Source	Destination	Protocol	Length	Info
169	5.612850725	192.168.0.156	192.168.0.155	TCP	60	445 → 2619 [SYN, ACK] Seq=0 Ack=1 Win=8192 Le...
170	5.612885128	192.168.0.155	192.168.0.156	TCP	54	2619 → 445 [RST] Seq=1 Win=0 Len=0
171	5.720548362	192.168.0.155	192.168.0.156	TCP	54	2620 → 445 [SYN] Seq=0 Win=512 Len=0
172	5.721125299	192.168.0.156	192.168.0.155	TCP	60	445 → 2620 [SYN, ACK] Seq=0 Ack=1 Win=8192 Le...
173	5.721149335	192.168.0.155	192.168.0.156	TCP	54	2620 → 445 [RST] Seq=1 Win=0 Len=0
174	5.826222726	192.168.0.155	192.168.0.156	TCP	54	2621 → 445 [SYN] Seq=0 Win=512 Len=0
175	5.826563684	192.168.0.156	192.168.0.155	TCP	60	445 → 2621 [SYN, ACK] Seq=0 Ack=1 Win=8192 Le...
176	5.826617850	192.168.0.155	192.168.0.156	TCP	54	2621 → 445 [RST] Seq=1 Win=0 Len=0
177	5.935321131	192.168.0.155	192.168.0.156	TCP	54	2622 → 445 [SYN] Seq=0 Win=512 Len=0
178	5.935845699	192.168.0.156	192.168.0.155	TCP	60	445 → 2622 [SYN, ACK] Seq=0 Ack=1 Win=8192 Le...
179	5.935870272	192.168.0.155	192.168.0.156	TCP	54	2622 → 445 [RST] Seq=1 Win=0 Len=0

Contramedidas

- Bloquear scan de puertos a través de firewall e IDS
- Actualizar los sistemas operativos de firewalls e IDS
- Filtrar el protocolo ICMP, sólo permitir los hosts autorizados
- Realizar pruebas de scanning periódicas
- Ocultar los banners de las aplicaciones o versiones de Sistema Operativo
- Configurar las alertas de detección de scan de puertos
- Configurar reglas anti-scanning, si se tienen

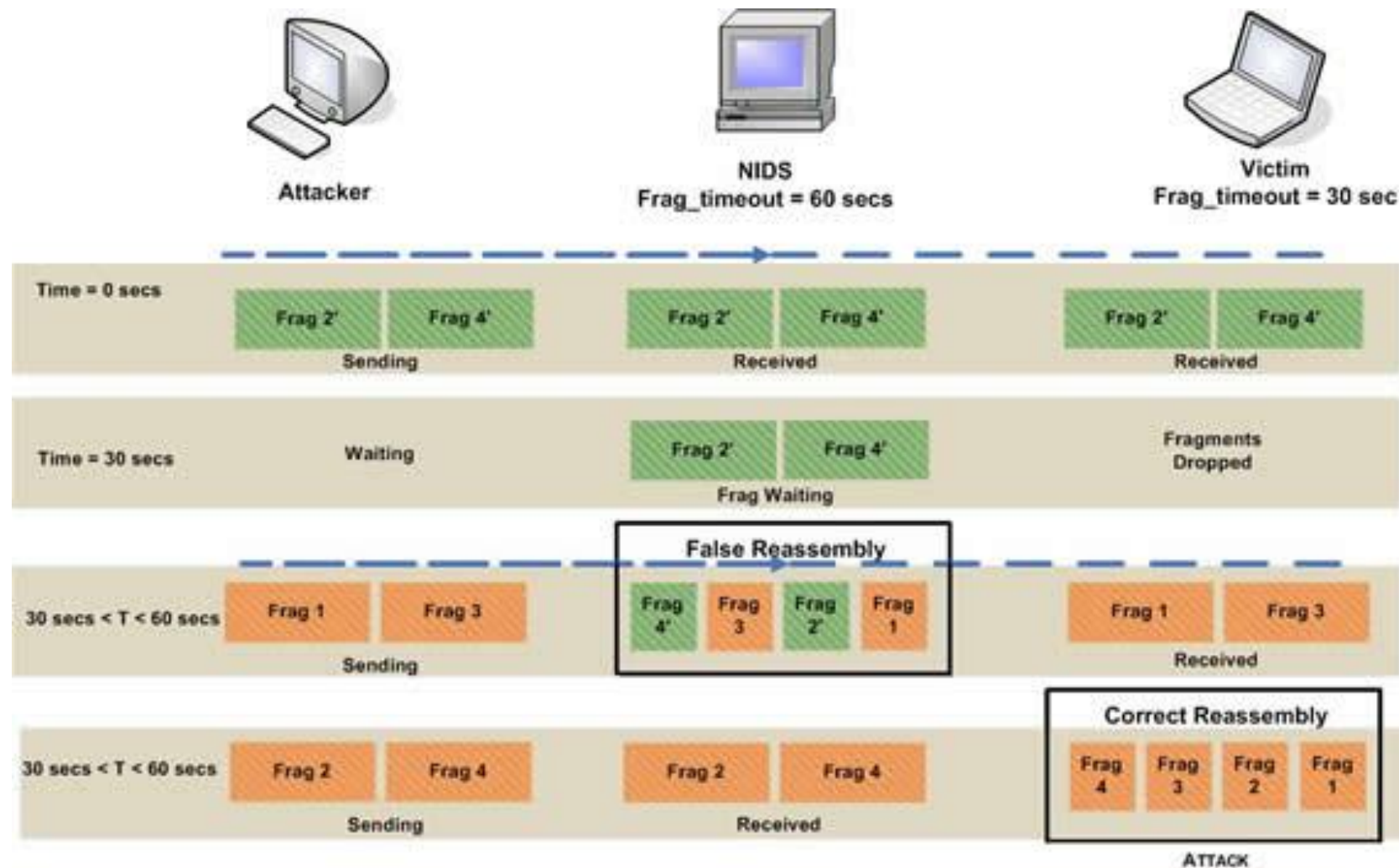
Técnicas de evasión

- Fragmentación
- IP Spoofing
- Cadena de proxys
- Source routing



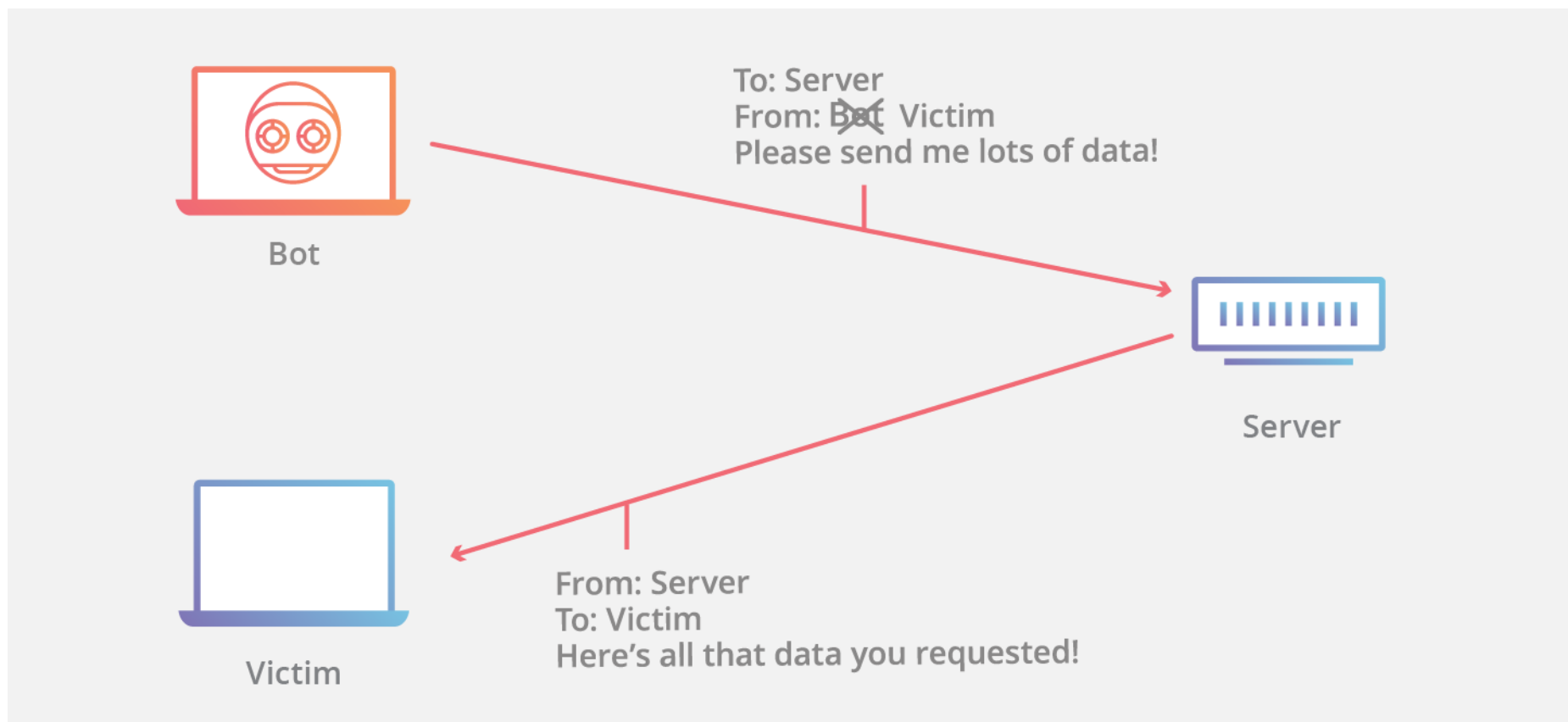
Técnicas de evasión

Fragmentación



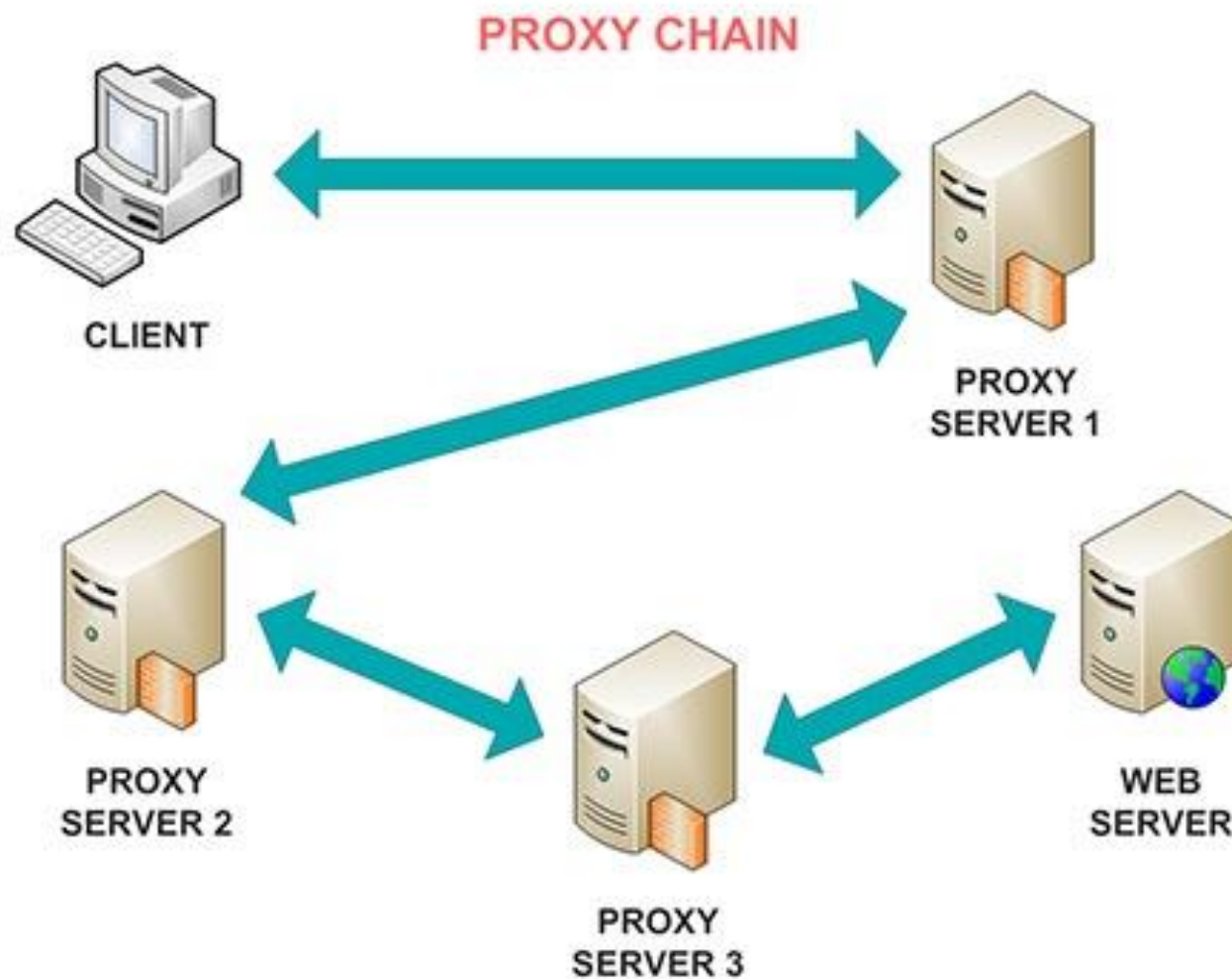
Técnicas de evasión

- IP Spoofing



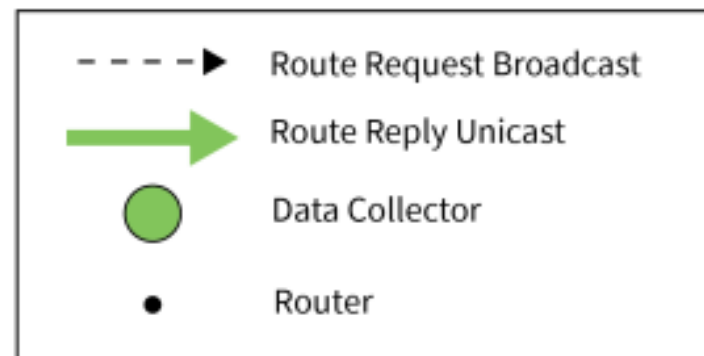
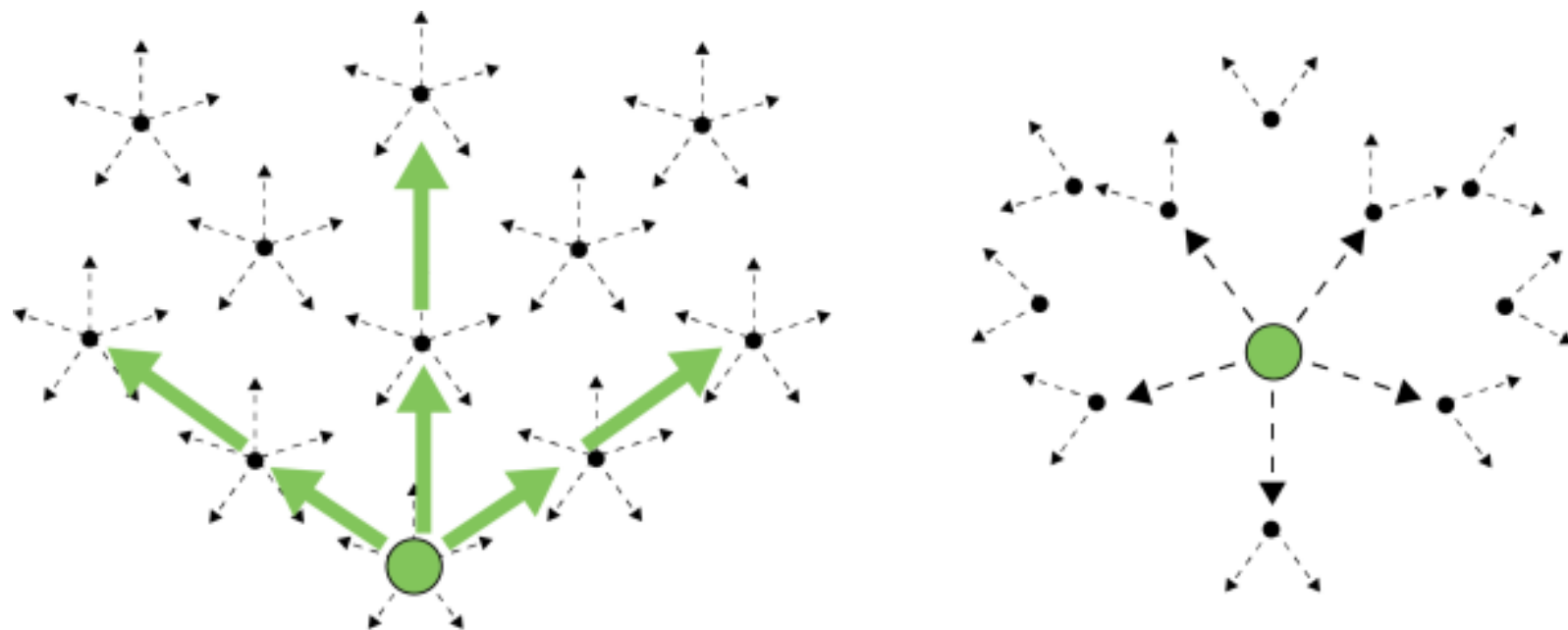
Técnicas de evasión

- Cadena de proxy



Técnicas de evasión

- Source routing



Resumen

- Scan de puertos
- NMAP
- tipos de scan
 - TCP Connect
 - Stealth
 - Xmas Scan
 - Idle Scan
 - UDP Scan
- Network Sweeping
- Banner Grabbing
- Hping
- Contramedidas
- Técnicas de evasión





USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA