



Nebrija
Universidad MADRID

Hacking Ético

Módulo II

Fase 2: Técnicas activas de
obtención de información:
Escaneo

Objetivos

- Detectar sistemas “vivos” en la red.
- Descubrir servicios que se están ejecutando o que están escuchando en los sistemas objetivos.
- Entender las técnicas de escaneo de puertos.
- Identificar servicios TCP y UDP ejecutándose en la red objetivo.
- Descubrir los sistemas operativos que hay
- Herramientas de descubrimiento automáticas.

Descubrir equipos “vivos”

■ ¿Por qué?

- Para determinar la arquitectura de la red objetivo.
- Para construir un inventario de sistemas accesibles en la red objetivo.

■ Tools

- Ping Utilities
- War Dialers

Ping

- Ping envía un paquete ICMP Echo Request y espera un mensaje ICMP Echo Reply proveniente de una máquina activa.
- Alternativamente, se pueden enviar paquetes TCP/UDP si los mensajes ICMP están bloqueados por un firewall (lo que suele ser normal)

Ping

- Ping también ayuda a estimar el tráfico de la red y la capacidad de cada equipo variando el tamaño del paquete y viendo el tiempo de respuesta.
- Ping también puede ser usado para resolver nombres (-a)
- Tools – *Ping*, *fpinger* (*ping a varios hosts*), *nmap*.

Ping

■ Opciones del ping

- `-c 4` : número de mensajes mandados
- `-i 0.01`: tiempo entre mensajes (sólo root <0.2)
- `-t 200`: ttl (por defecto a 64 en el request)
Cada router disminuye en 1.

■ Monitorizarlo con ethereal:

- Resolución arp
- ICMP:
 - request / reply

Detecting Ping Sweeps

- ¿Cómo detectar los ping sweeps?
- Ping Utilities:
 - Nmap (ya lo veremos)
 - Hping: `apt-get install hping3`.
- Ping Sweep Detection Utilities:
 - Network based IDS (www.snort.org)
 - Genius (www.indiesoft.com)
 - BlackICE (www.networkice.com)
 - Scanlogd (www.openwall.com/scanlogd)
- Ya veremos también los IDS.

Descubrir servicios corriendo / escuchando

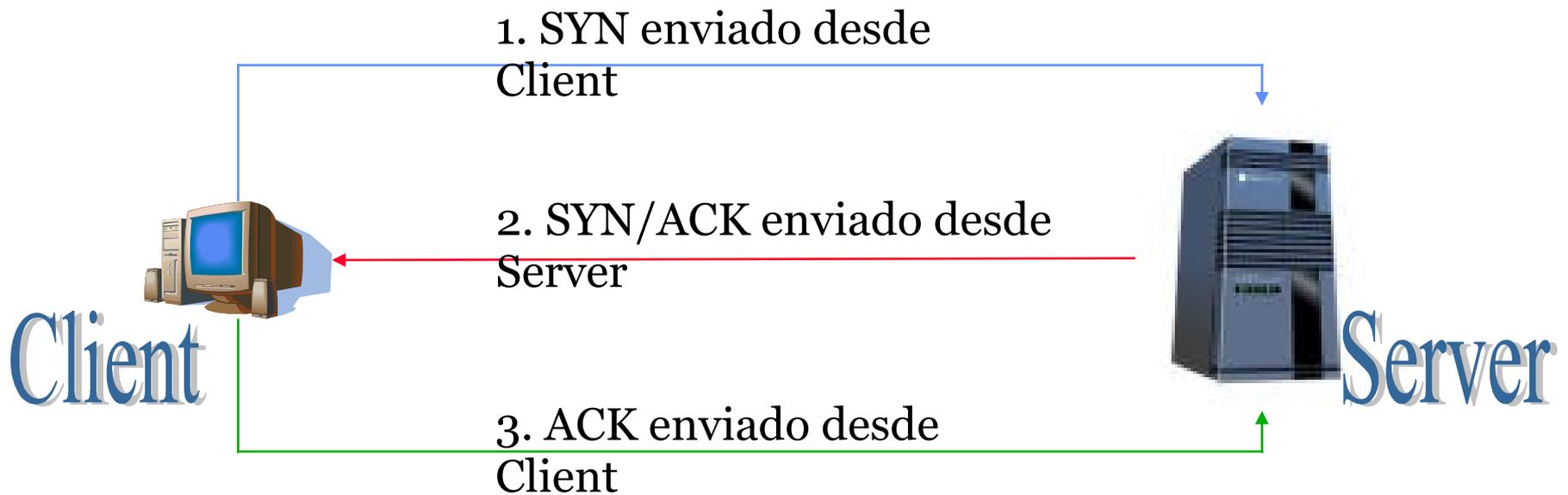
■ ¿Por qué?

- Para descubrir hosts vivos en el caso de que esté bloqueado el ICMP request.
- Para identificar potenciales puertos para un ataque.
- Para detectar aplicaciones específicas o diferentes versiones de un servicio.
- Para detectar sistemas operativos.

■ Tools

- Port Scanners

TCP three-way handshake



Ejemplo: el servidor ftp

■ Servidor ftp

- Explicar el servicio y sesión.
- Instalar el servidor ftp
- El cliente ftp

■ Ejercicio:

- Monitorizar una sesión ftp e identificar los paquetes involucrados en la sesión.
 - Three way handshake
 - Números de secuencia
 - Autenticación (username y password)
- Enviarlos al buzón de tareas.

Técnicas de escaneo de puertos

- El escaneo de puertos es una de las técnicas más usadas por un hacker para descubrir servicios que puedan ser comprometidos.
- Un potencial objetivo puede ejecutar muchos servicios que escuchan en puertos conocidos.
- Escaneando estos puertos podemos encontrar vulnerabilidades potenciales (por ejemplo por bugs conocidos de ese servicio)
- Las tácticas de escaneo pueden clasificarse entre Vanilla, Strobe, Stealth, FTP Bounce, Fragmented Packets, Sweep y UDP Scans.

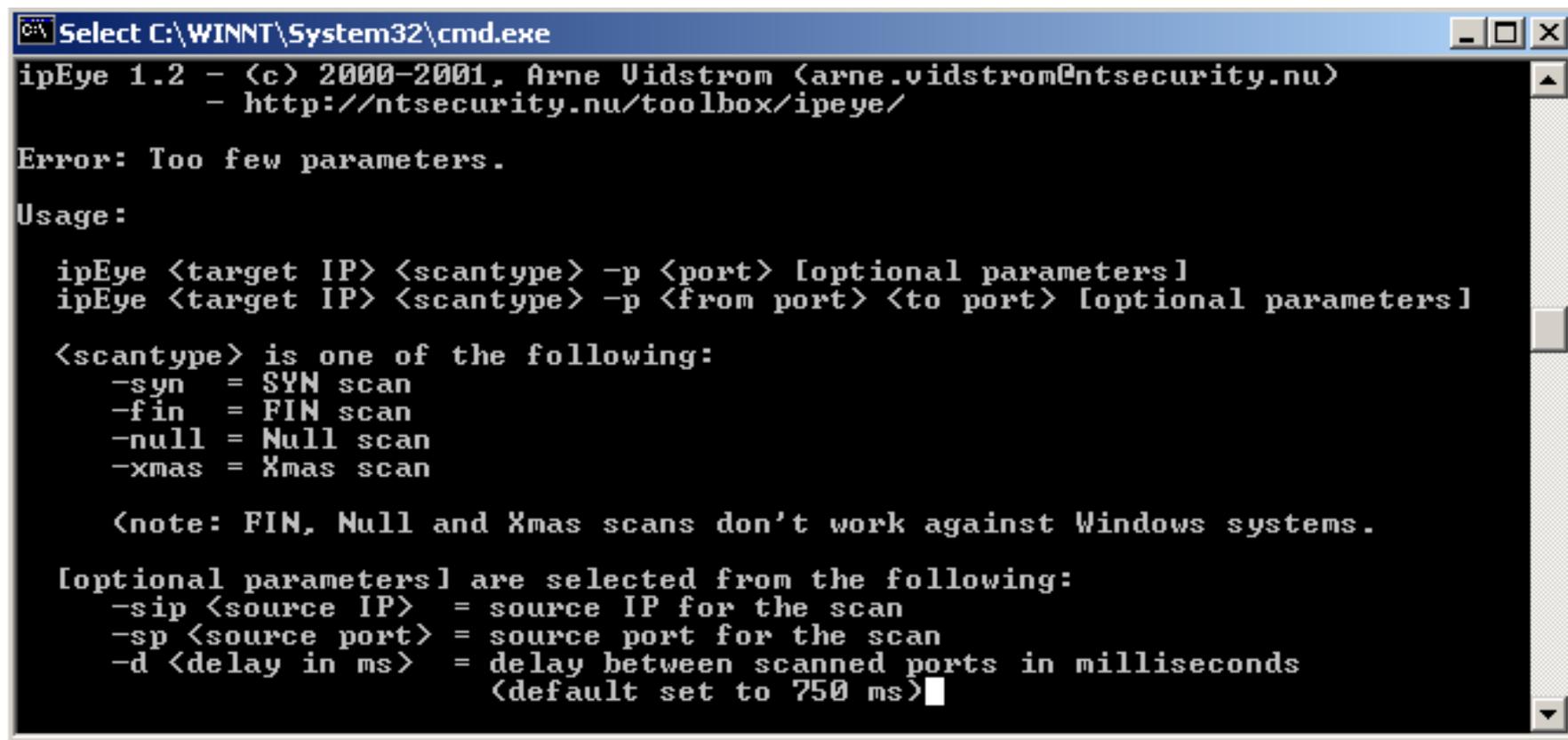
Port Scanning Techniques



Las técnicas de escaneo pueden clasificarse en:

- 1 Open scan
 - Half- open scan
 - Stealth scan
 - Sweeps
 - Misc

Tool: ipEye, IPsecScan



```
C:\WINNT\System32\cmd.exe
ipEye 1.2 - (c) 2000-2001, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
          - http://ntsecurity.nu/toolbox/ipeye/

Error: Too few parameters.

Usage:

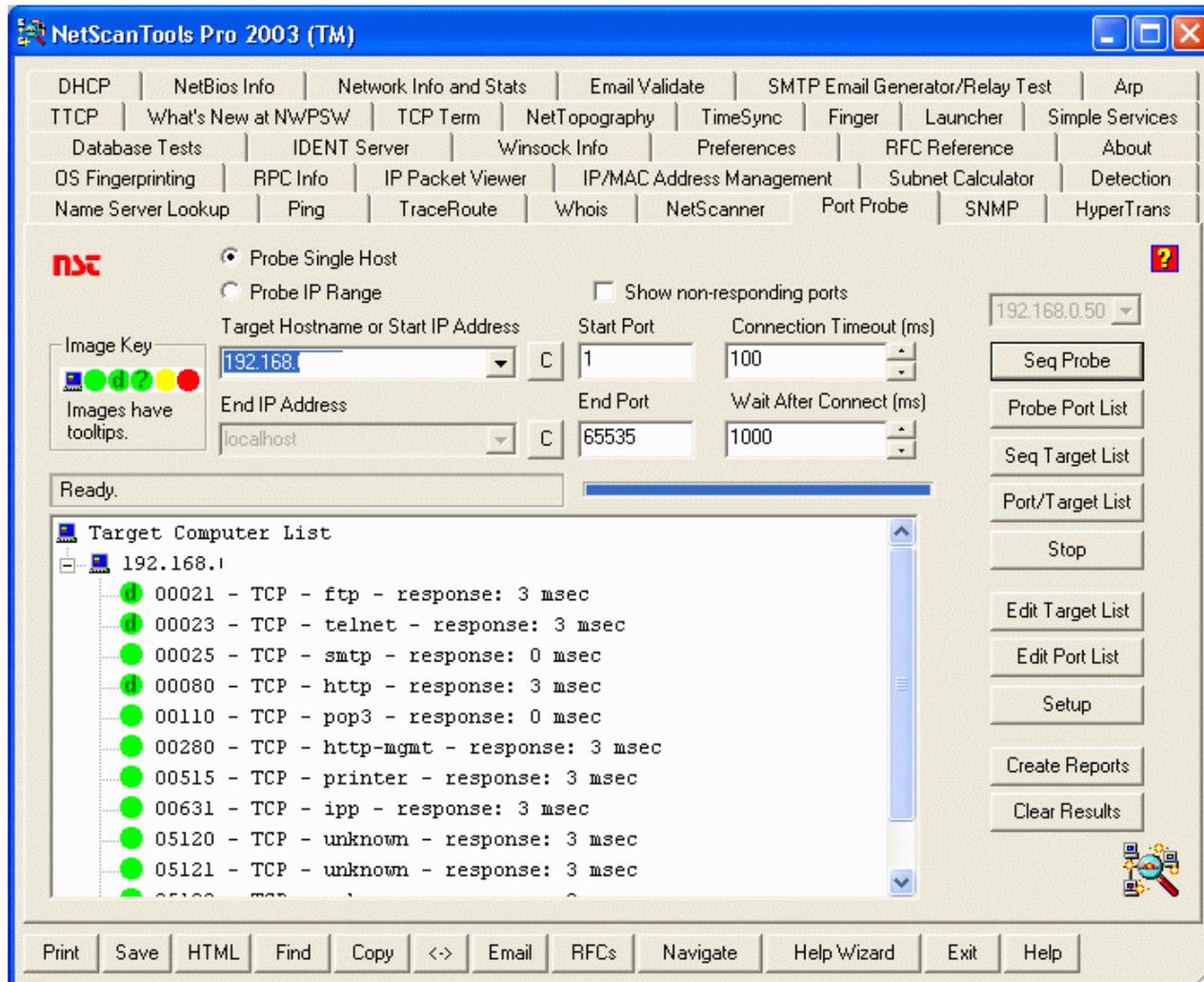
ipEye <target IP> <scantype> -p <port> [optional parameters]
ipEye <target IP> <scantype> -p <from port> <to port> [optional parameters]

<scantype> is one of the following:
  -syn  = SYN scan
  -fin  = FIN scan
  -null = Null scan
  -xmas = Xmas scan

<note: FIN, Null and Xmas scans don't work against Windows systems.

[optional parameters] are selected from the following:
  -sip <source IP> = source IP for the scan
  -sp <source port> = source port for the scan
  -d <delay in ms> = delay between scanned ports in milliseconds
                    (default set to 750 ms)
```

Tool: NetScan Tools Pro 2003



Tool: SuperScan

The screenshot displays the SuperScan 3.00 application window. The main area is titled "Hostname Lookup" and shows the target "target.com" with its resolved IP address "64.39.30.117". The "Scan type" section is configured with "Only scan responsive pings" and "Show host responses" checked, and "Every port in list" selected. The "Scan" section shows the progress of the scan, with "Pinging", "Scanning", and "Resolving" all completed. The "Speed" section shows a slider set to "Max". The "Active hosts" section shows 1 active host and 9 open ports. The "Configuration" section includes a "Port list setup" button. The "IP" section includes "Start" and "Stop" IP addresses, "PrevC", "NextC", and "1..254" buttons, and checkboxes for "Ignore IP zero", "Ignore IP 255", and "Extract from file". The "Timeout" section includes "Ping", "Connect", and "Read" time values. The "Scan type" section includes checkboxes for "Resolve hostnames", "Only scan responsive pings", and "Show host responses", and radio buttons for "Ping only", "Every port in list", "All selected ports in list", "All list ports from", and "All ports from". The "Scan" section includes a table showing the progress of the scan:

Scan	Progress
Pinging	-Q-
64.3	0
Scanning	-Q-
64.3	0
Resolving	-Q-
	0

The "Active hosts" section shows:

Active hosts	Open ports
1	9

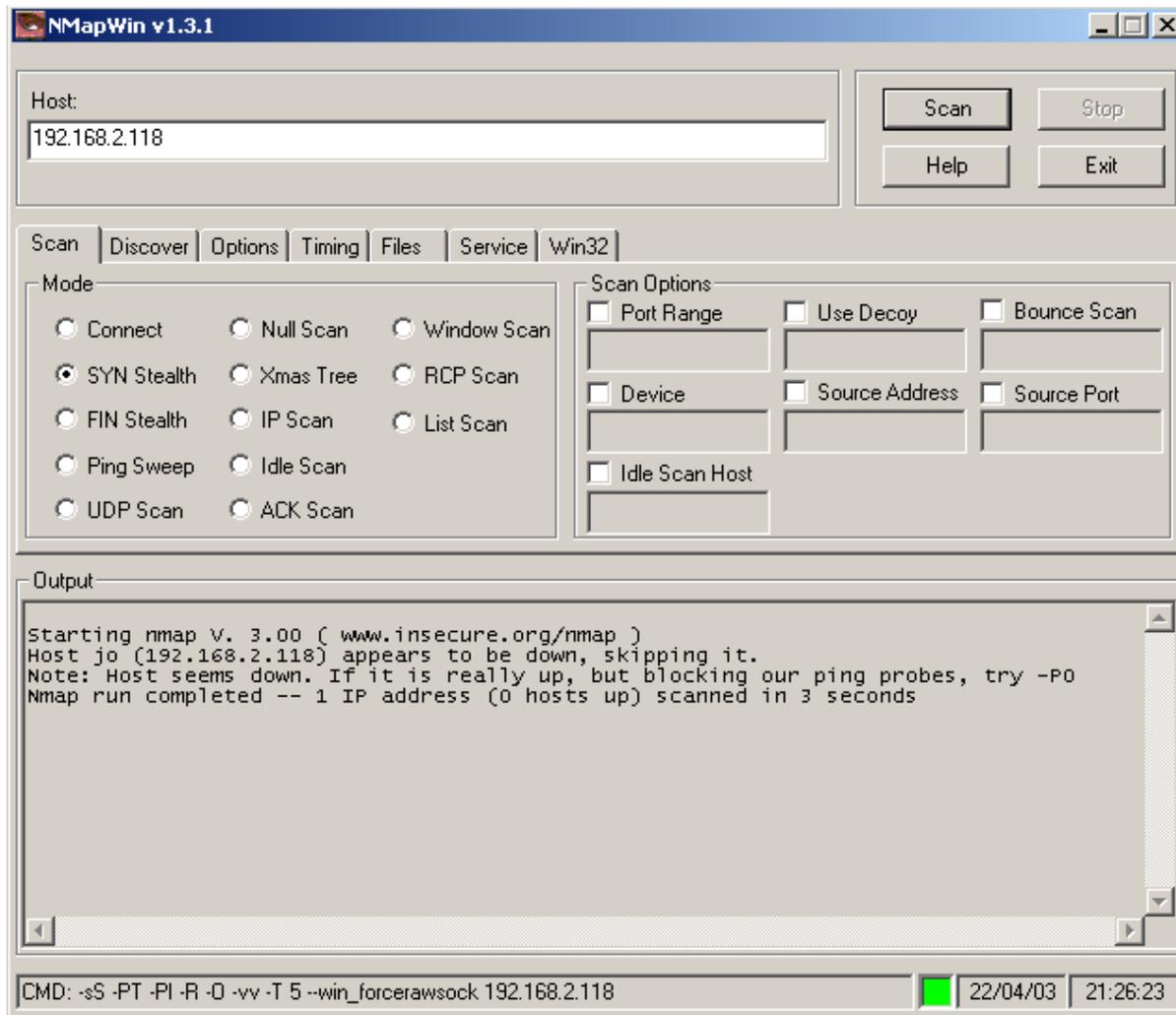
The "Speed" section shows a slider set to "Max". The "Configuration" section includes a "Port list setup" button. The "IP" section includes "Start" and "Stop" IP addresses, "PrevC", "NextC", and "1..254" buttons, and checkboxes for "Ignore IP zero", "Ignore IP 255", and "Extract from file". The "Timeout" section includes "Ping", "Connect", and "Read" time values. The "Scan type" section includes checkboxes for "Resolve hostnames", "Only scan responsive pings", and "Show host responses", and radio buttons for "Ping only", "Every port in list", "All selected ports in list", "All list ports from", and "All ports from".

The main scan results are displayed in a list:

- 64.39.30.117
 - 25 Simple Mail Transfer
 - 80 World Wide Web HTTP
 - 110 Post Office Protocol - Version 3
 - +OK X1 NT-POP3 Server [redacted].com (IMail 5.08 227181-2).
 - 135 DCE endpoint resolution
 - 143 Internet Message Access Protocol
 - 1032 BBN IAD
 - 5631 pcANYWHEREdata
 - 5800 Virtual Network Computing server
 - 5900 Virtual Network Computing server
 - RFB 003.003.

The "Active hosts" section shows 1 active host and 9 open ports. The "Speed" section shows a slider set to "Max". The "Configuration" section includes a "Port list setup" button. The "IP" section includes "Start" and "Stop" IP addresses, "PrevC", "NextC", and "1..254" buttons, and checkboxes for "Ignore IP zero", "Ignore IP 255", and "Extract from file". The "Timeout" section includes "Ping", "Connect", and "Read" time values. The "Scan type" section includes checkboxes for "Resolve hostnames", "Only scan responsive pings", and "Show host responses", and radio buttons for "Ping only", "Every port in list", "All selected ports in list", "All list ports from", and "All ports from".

Tool: NMap (Network Mapper)



Uso del nmap

- Web
- Tipos de escaneo con nmap
- ¡Ojo! Hay que entender qué es lo que estamos haciendo.
- Artículo de hackxtrack 9.

Tipos de escaneo

- **TCP connect (-sT)** – se intenta crear una conexión mediante la llamada a connect()
 - Es la llamada normal que se hace en cualquier aplicación.
 - Muy fácilmente detectable (se guarda en el syslog que no se han mandado datos después del connect)
- **TCP syn (-sS)**
 - Se envía un paquete con el flag SYN, el otro envía un SYN+ACK y en lugar de aceptarlo se manda un RST (reset)
 - También se le llama half-open scanning
 - Es difícil de detectar.

Tipos de escaneo

- UDP connect (-sU) – se intenta crear una conexión mediante la llamada a connect()
 - DNS, DHCP y SNMP son algunos ejemplos.
 - Se puede combinar con -sS
- Otros:
 - Null scan – paquetes sin banderas
 - Xmas scan – con todos los flags levantados
- El resto de opciones en la web de nmap