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

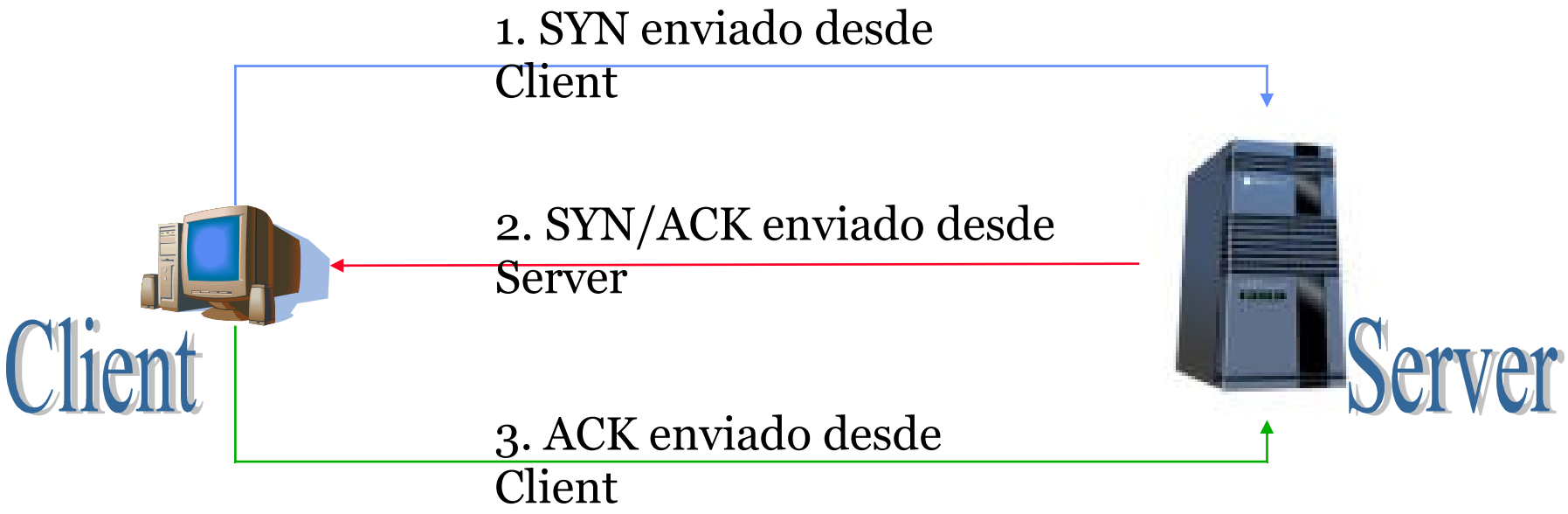
Detecting Ping Sweeps

- ¿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)
  - Enviarlo al buzón de tareas.

Técnicas de escaneo de puertos

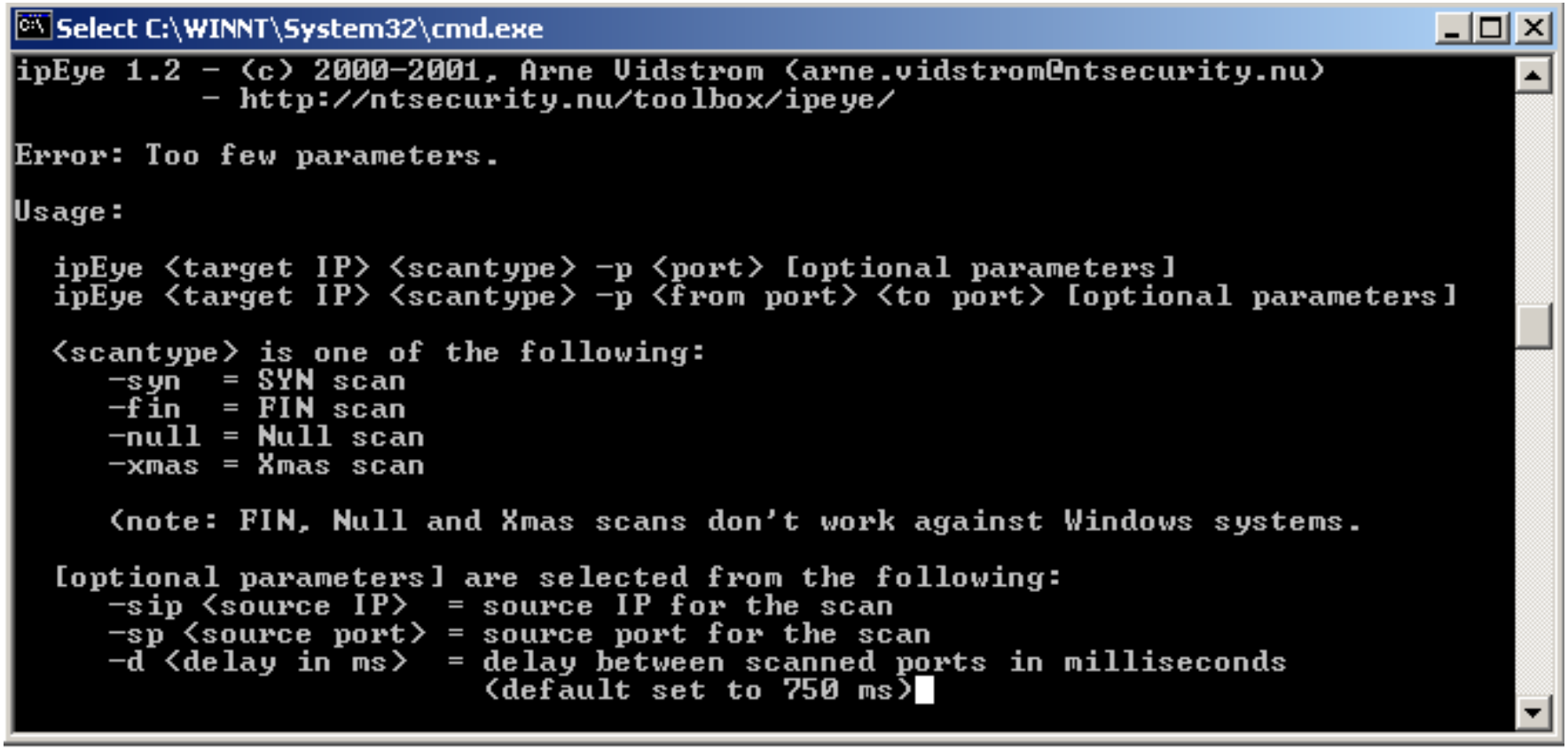
- El escaneo de puertos es una de las técnicas más usadas por un hacker para descubrir servicios que puedan ser comprometidos.
- Un potencial objetivo puede ejecutar muchos servicios que escuchan en puertos conocidos.
- Escaneando estos puertos podemos encontrar vulnerabilidades potenciales (por ejemplo 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

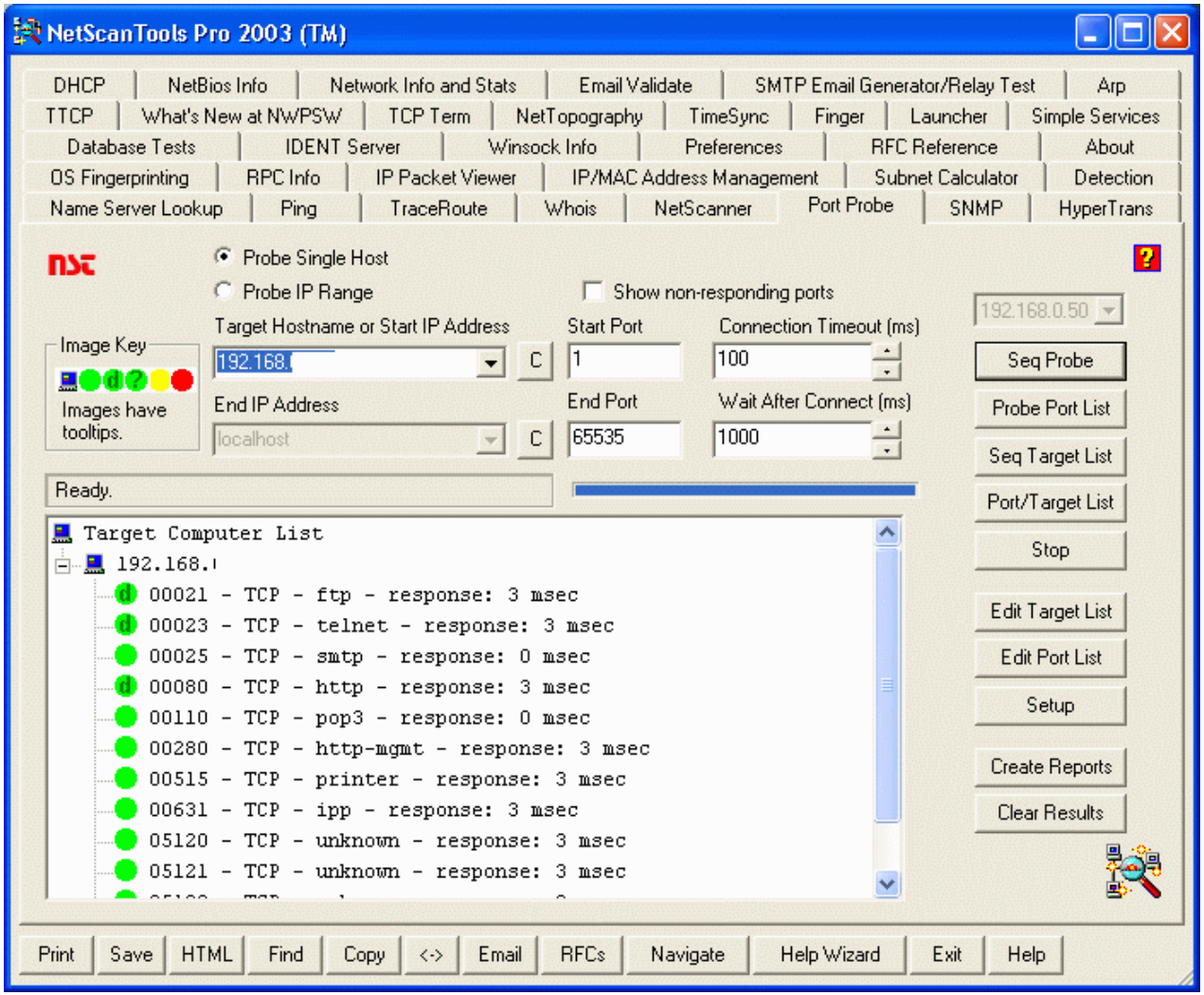
Las técnicas de escaneo pueden clasificarse en:

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

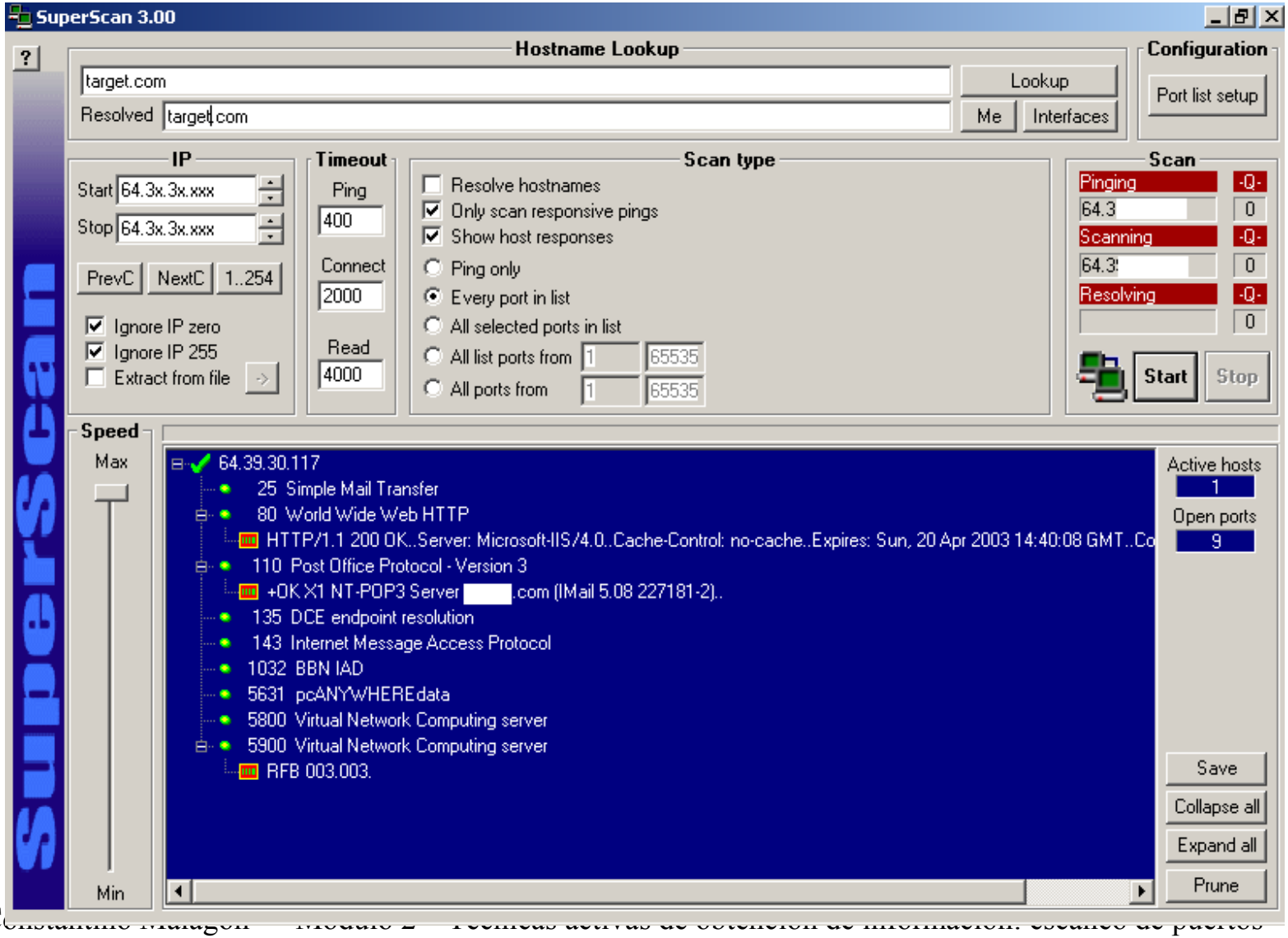
Tool: ipEye, IPSecScan



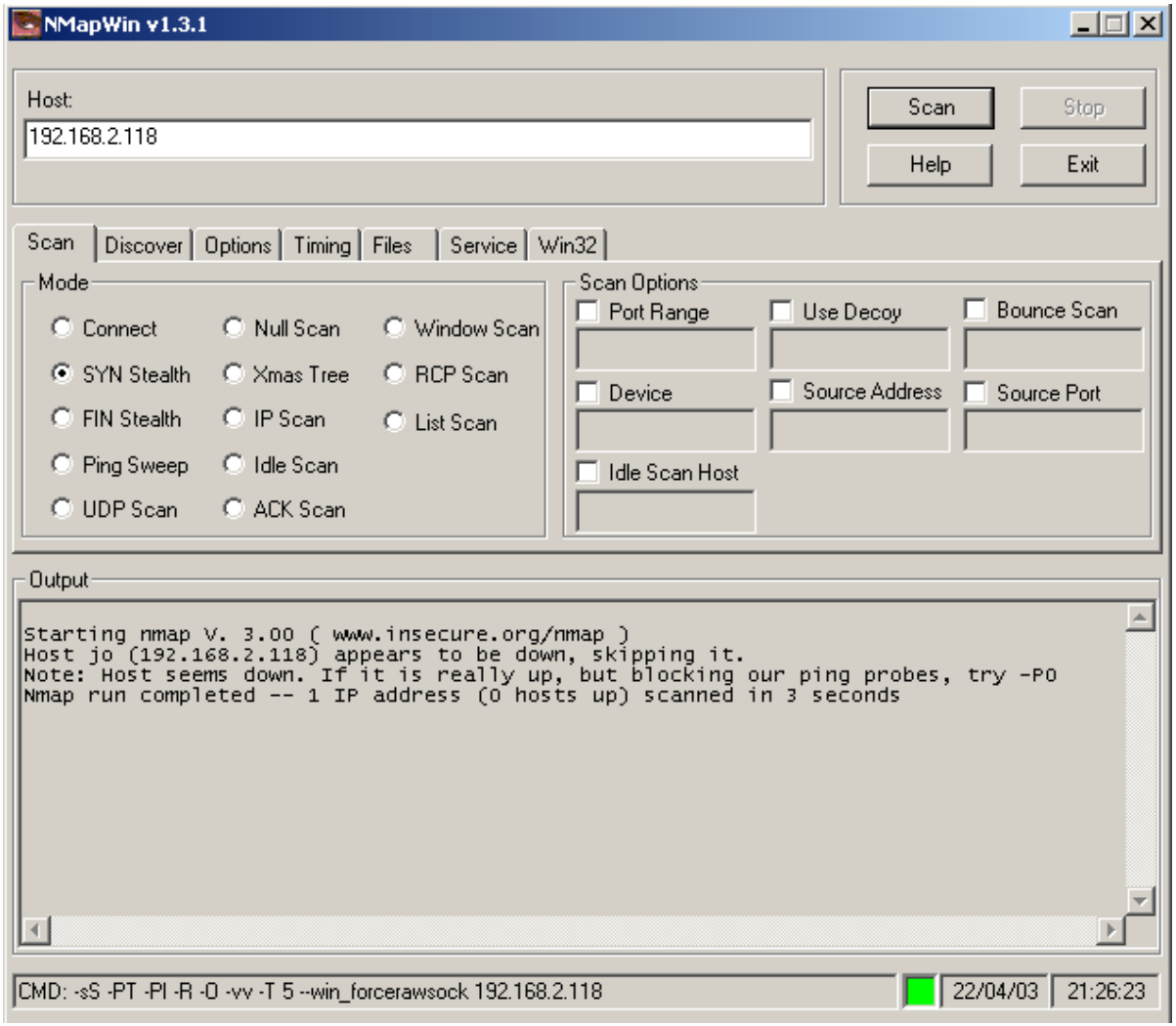
Tool: NetScan Tools Pro 2003



Tool: SuperScan



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