Hacking ético

Módulo III

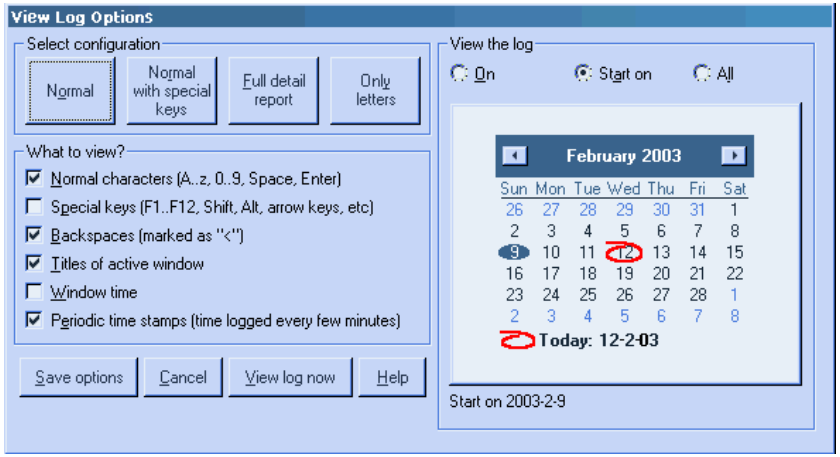
Hacking del sistema (2ª parte)

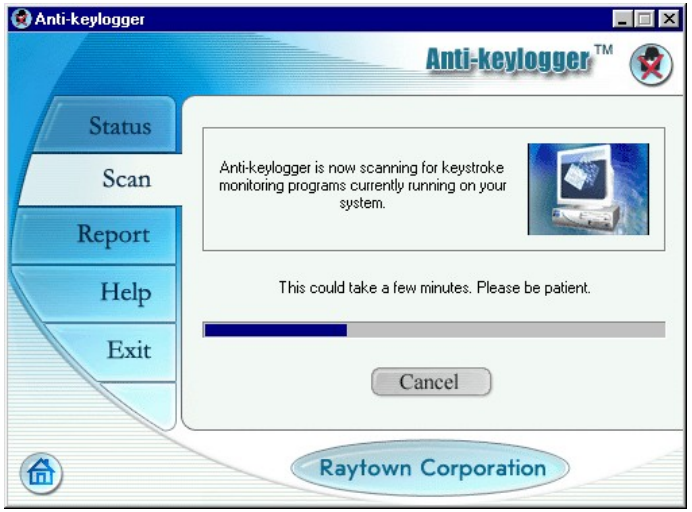
Objectivo del módulo

- Esto es lo que veremos en este módulo:
  - Adivinación de contraseñas remotas
  - Craqueo de contraseñas (cont)
  - Keyloggers
  - Escalada de privilegios
  - Denegación de servicio (DoS)
  - Buffer overflows
  - Sniffers
  - Control remoto y puertas traseras
  - Redirección de puertos
  - Borrado de huellas
  - Ocultar ficheros

Keystroke Loggers

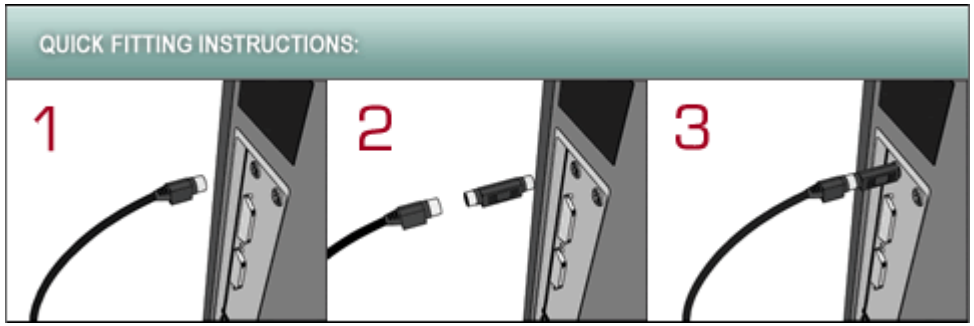
- Si todos los intentos anteriores fallan, entonces un *keystroke logger* es la solución.
- Keyloggers son programas que registran cada pulsación de teclas en el teclado.
- Hay dos tipos:
  - 1.Basados en Software
  - 2.Basados en Hardware





Hacking Tool: Hardware Key Logger (www.keyghost.com)

- Un Key Logger por hardware se debe conectar entre el teclado y el equipo.



LKL Linux KeyLogger

- **Lab: Usando un keylogger**
- Se puede descargar de Sourceforge, o mejor,
  - sudo apt-get install lkl
  - sudo lkl -l -k /usr/share/lkl/keymaps/it_km -o log.file

Spy ware: Spector (www.spector.com)

- Spector es un spy ware (programa espía) que registra todo lo que hace un usuario (o tu novi@) en un equipo (sitios web, conversaciones msn,...)
- Spector toma automáticamente cientos de snapshots (captura de pantalla) cada hora, de forma que se puede ver qué está haciendo exactamente un usuario.
- Cada captura la guarda en un directorio oculto del disco duro.

Hacking Tool: eBlaster (www.spector.com)

- eBlaster permite conocer exactamente qué está haciendo un usuario en el equipo objetivo (de forma remota).
- eBlaster registra sus emails, chats, mensajes instantáneos del msn, sitios web visitados y teclas pulsadas y te manda esta información por email.
- Nada más mandar o recibir un correo ese usuario te llegará a ti una copia.

Anti Spector (www.antispector.de)

- Herramienta que es capaz de detectar si Spector está instalado en el sistema.

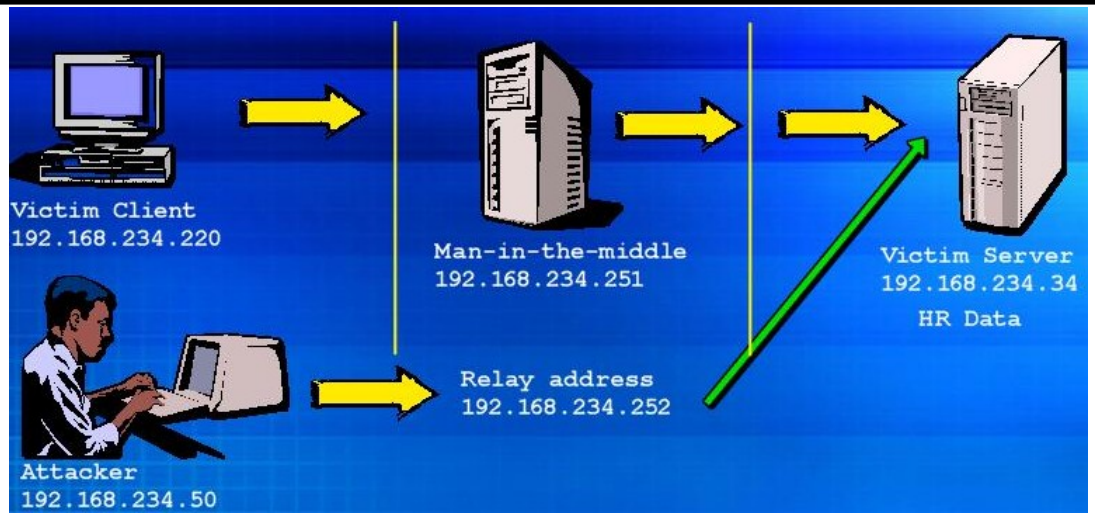
Redirigir una autenticación SMB al atacante

- Escuchar las conversaciones de la red puede ser mucho más fácil si el atacante puede engañar a la víctima haciendo que intente una autenticación Windows contra un sistema puesto por el atacante.
- Un truco típico es enviar un email a la víctima (incluso como si fuéramos administrador, es decir, desde su cuenta SMTP) con un hiperenlace que apunte a un servidor SMB fraudulento.
- Cuando hace click en el hiperenlace, el usuario manda sin darse cuenta sus credenciales (cuenta de usuario)

Hacking Tool: SMBRelay

- SMBRelay es esencialmente un servidor SMB que puede capturar usernames y hashes de contraseñas a partir del tráfico SMB que le llega.
- Puede realizar también ataques man-in-the-middle (MITM).
- Se debería deshabilitar NetBIOS sobre TCP/IP y bloquear los puertos 139 y 445.
- Arrancar el servidor SMBRelay y escuchar para capturar los paquetes SMB:
  - c:\>smbrelay /e
  - c:\>smbrelay /IL 2 /IR 2
- Un atacante puede acceder a la máquina cliente simplemente conectándose a él vía “relay address” mediante la orden net use * \\<capture _ip>\c$

Escenario SMBRelay man-in-the-middle



- El atacante configura un servidor fraudulento con la IP 192.168.234.251, una dirección de reenvío (relay address) 192.168.234.252 usando /R, y un servidor objetivo con IP 192.168.234.34 con /T.

c:\> smbrelay /IL 2 /IR /R 192.168.234.252 /T 192.168.234.34

- Cuando un cliente víctima se conecta con el servidor fraudulento pensando que está hablando con el servidor real que yo le mandé, un servidor man-in-the-middle (MITM) intercepta la llamada, recoge el hash de la password del usuario y pasa la conexión al equipo del atacante (que se conecta como si fuese la víctima inicial)

Debilidades SMBRelay

- El problema es convencer a la víctima para que se autentique contra el servidor
- En vez de mandar el mail malicioso se podría realizar un ataque de envenenamiento de la tabla ARP contra todos los equipos de la subred para que todos se autentiquen contra el servidor fraudulento MITM.

Medidas de prevención

Contramedidas

- Configurar Windows 2000 para usar firmas SMB.
- Las comunicaciones entre el cliente y servidor se firmarán criptográficamente (cada bloque de comunicaciones SMB se firma con una clave privada)
- Se configura en Directivas de seguridad /Opciones de seguridad

Escalada de privilegios

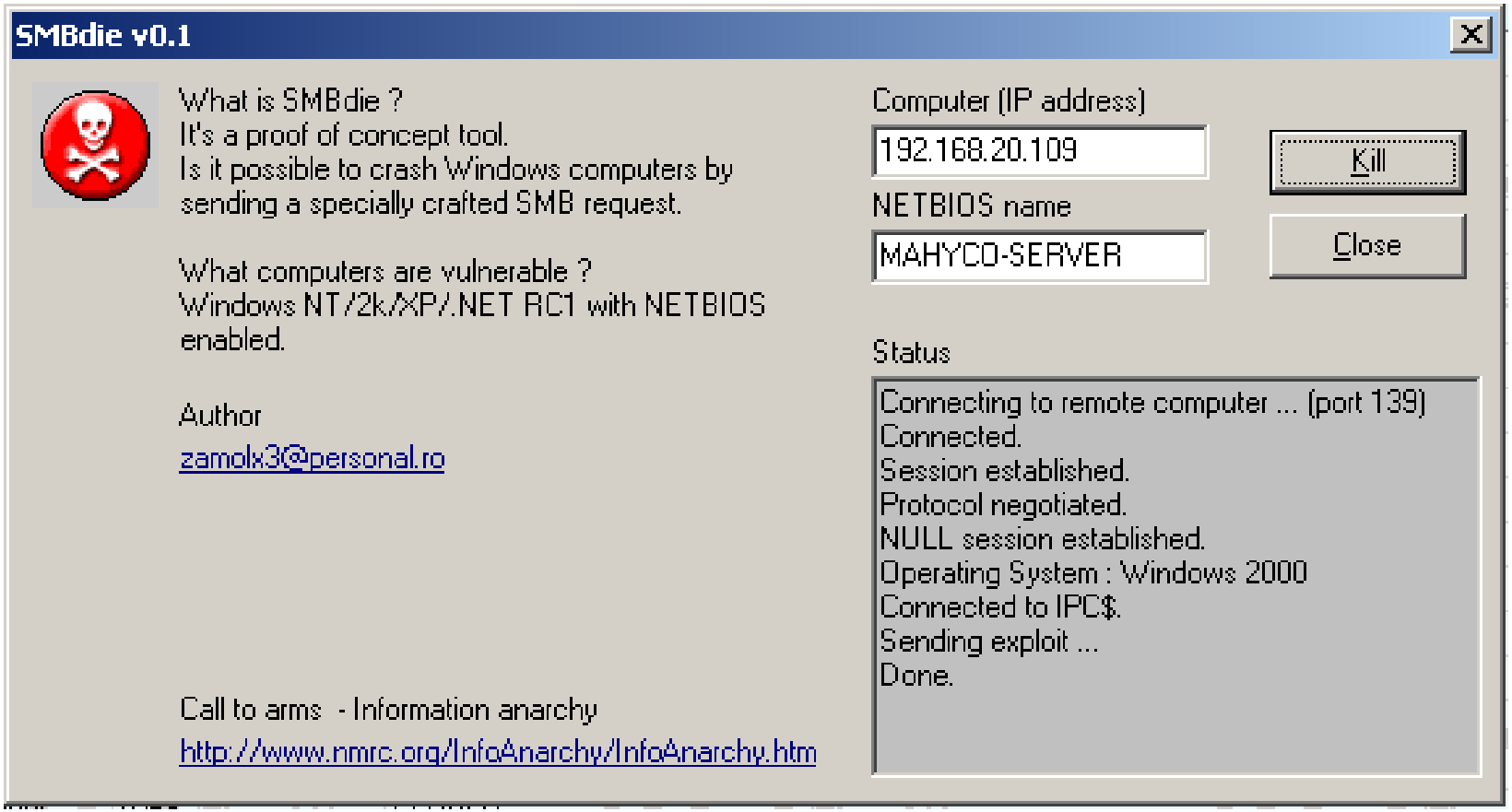
- Si un atacante consigue obtener acceso a la red o a una máquina mediante una cuenta que no es Administrador, el siguiente paso es obtener mayores privilegios (si puede ser de administrador)
- Llamaremos a esto escalar privilegios.

Tool: GetAdmin

- GetAdmin.exe es un pequeño programa que permite añadir un usuario al grupo de Administradores locales.
- El GetAdmin.exe se ejecuta desde un terminal o desde un navegador.
- Sólo funciona con Nt 4.0 Service pack 3.
- Otras herramientas: Win32 Create Local Admin User.

Hacking Tool: SMBDie

- SMBDie es capaz de echar abajo un equipo Windows 2000/XP/NT enviando peticiones SMB.



Ataque DoS NeBIOS

- Si se manda un mensaje 'NetBIOS Name Release' al Servicio de nombres NetBIOS Name Service (NBNS, UDP 137) a una equipo NT/2000 se le notifica a éste que su nombre está repetido y hay un conflicto, de forma que el sistema se desactiva.
- Esto desactivará el cliente de red del equipo.
- Tool: nbname
  - NBName puede deshabilitar LANs completas y hacer que no puedan volver a reengancharse los equipos..
  - Los equipos infectados en la red NetBIOS networkpor la herramienta pensarán que sus nombres están siendo usados por otras máquinas.