2. Pasos de un Ataque a la Ciberseguridad

3. Enumeración

3.1 Introducción

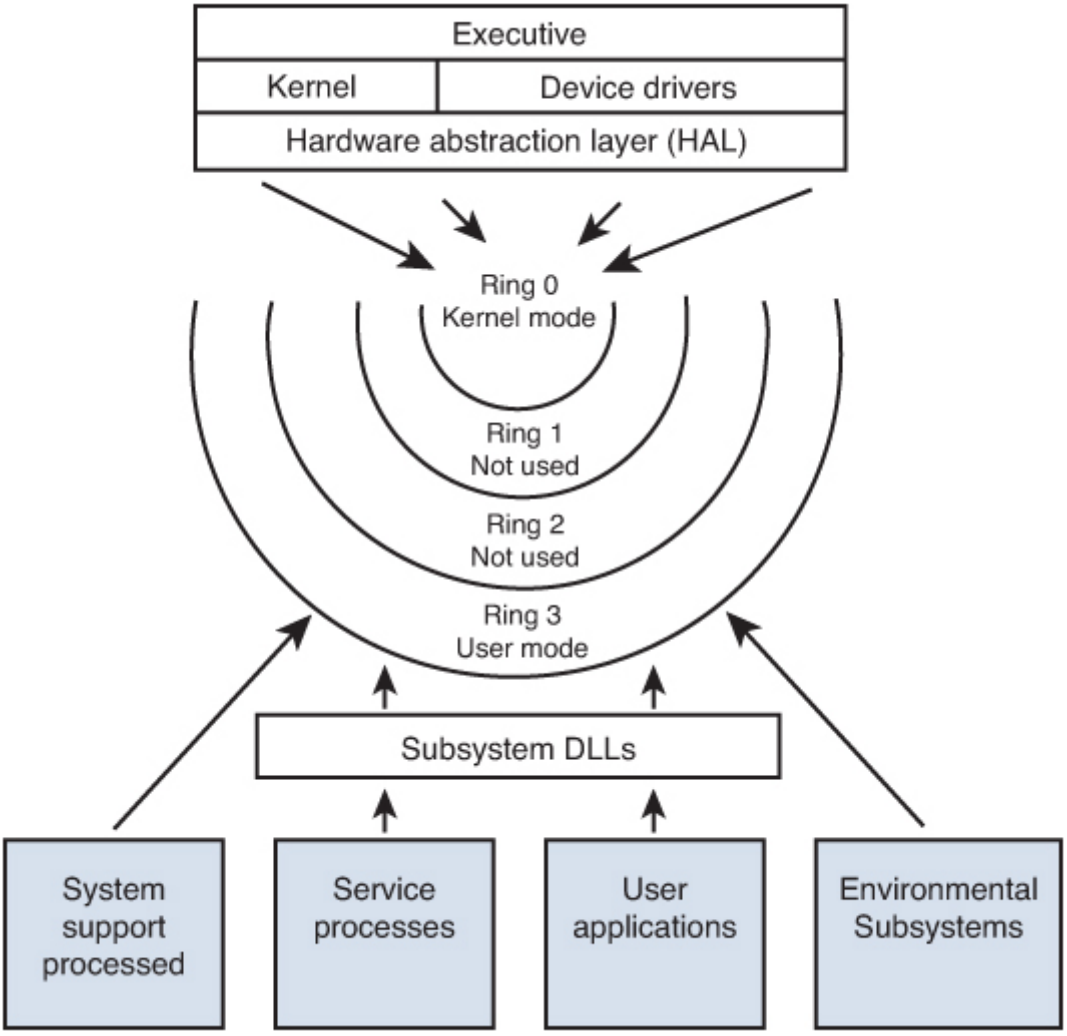
La enumeración puede ser descrita como un análisis en profundidad de los equipos de destino. La enumeración se realiza mediante la conexión activa a cada sistema para identificar las cuentas de usuario, cuentas de sistema, servicios y otros detalles del sistema. Es el proceso de consulta activa o la conexión a un sistema de destino para adquirir información sobre: NetBIOS/LDAP, SNMP, operación UNIX/Linux, servidores NTP, servidores SMTP y servidores DNS. Estos temas se discuten a continuación.

OpenLearning

3.2 Enumeración Windows

El objeto de la enumeración de Windows es identificar una cuenta de usuario o cuenta del sistema para su uso potencial. Puede que no tengamos que encontrar una cuenta de administrador del sistema, porque puede ser posible llevar a cabo un escalado de privilegios. En este punto, simplemente estamos buscando el conocimiento para lograr cierto nivel de acceso.

Para atacar mejor las computadoras Microsoft Windows, debemos entender cómo funcionan. Windows incluye versiones tanto de cliente como de servidor. Los sistemas cliente que aún están tienen soporte mientras escribimos este curso son: Windows XP, Vista, 7, y 8. En el lado del servidor, Microsoft tiene soporte para Windows 2003, 2008, y 2012. Cada uno de estos sistemas operativos comparte un kernel similar en algunos aspectos. El núcleo es la parte más confiable del sistema operativo. ¿Cómo sabe el sistema operativo en quién y qué confiar? La respuesta es mediante la implementación de anillos de protección. El modelo de anillos de protección proporciona al sistema operativo diferentes niveles en los que ejecutar código o restringir su acceso. Proporciona así un nivel de control de acceso y granularidad. A medida que avanzamos hacia los límites exteriores del modelo, los números aumentan, y el nivel de confianza disminuye. La figura muestra el modelo básico que utiliza Windows para anillos de protección.



En la arquitectura de Windows, se puede ver que hay dos modos básicos: modo de usuario (anillo 3) y modo kernel (anillo 0). El modo de usuario tiene restricciones, mientras que el modo de núcleo permite un acceso completo a todos los recursos. Este es un concepto importante a

contemplar en la seguridad informática ya que las herramientas antivirus y de análisis pueden detectar herramientas de hacking y el código que se ejecuta en modo de usuario. Sin embargo, si el código se implementa en un sistema Windows para ejecutarse en modo kernel, puede evitarse la detección y será más difícil de erradicar. Todo el código que se ejecuta en un equipo con Windows se debe ejecutar en el contexto de una cuenta. La cuenta del sistema tiene la capacidad de realizar actividades de modo de núcleo. El nivel de la cuenta determina su capacidad para ejecutar código en un sistema. Los atacantes siempre quieren ejecutar código en el nivel más alto de privilegio. Windows utiliza los siguientes dos elementos para ayudar a mantener un registro de los privilegios de seguridad de un usuario y su identidad:

- Identificadores de seguridad (SID)
- Identificadores relativos (RID)

Los SID son una estructura de datos de longitud variable que identifica las cuentas de usuario, grupo y equipo. Por ejemplo, un SID de S -1 -1-0 indica un grupo que incluye a todos los usuarios. Estrechamente vinculados a los SID están los RID. Un RID es una parte del SID que identifica a un usuario o grupo en relación con la autoridad que el usuario tiene. Veamos un ejemplo:

```
S-1-5-21-1607980848-492894223-1202660629-500
    S for security id
    1 Revision level
    5 Identifier Authority (48 bit) 5 = logon id
    21 Sub-authority (21 = nt non unique)
    1607980848      SA
    492894223       SA domain id
    1202660629      SA
    500             User  id
```

Centremos nuestra atención en la última línea del texto en este ejemplo. El ID de usuario especifica el usuario específico, como se muestra en la Tabla:

User ID	Code
Admin	500
Guest	501
Kerberos	502
First user	1000
Second user	1001

Esta tabla muestra que la cuenta de administrador tiene un RID de 500 de forma predeterminada, el cliente tiene un RID 501, y la primera cuenta de usuario tiene un RID de 1000. Cada nuevo usuario recibe el siguiente RID disponible. Esta información es importante porque simplemente cambiar el nombre de una cuenta no va a evitar que alguien descubra cuentas clave. Esto es similar a la forma en que Linux controla el acceso para los usuarios y los procesos del sistema a través de un ID de usuario asignado (UID) y un ID de grupo (GID) que se encuentra en el archivo /etc/passwd.

En un equipo Windows independiente (no en dominio), la información de usuario y las contraseñas se almacenan en la base de datos Security Account Manager (SAM). Si el sistema

forma parte de un dominio, el controlador de dominio almacena la información crítica en Active Directory (AD). La SAM contiene los usuarios y grupos locales definidos, junto con sus contraseñas y otros atributos. La base de datos SAM se almacena en la carpeta Windows/System32/config en un área protegida del Registro en HKLM\SAM.

AD es un servicio de directorio, que contiene una base de datos que almacena información acerca de los objetos en un dominio. AD mantiene la información de contraseña y privilegios para los usuarios y grupos del dominio que antes se guardaban en la SAM. A diferencia del viejo modelo de confianza NT, un dominio es una colección de computadoras y sus grupos de seguridad asociados que se gestionan como una sola entidad. AD fue diseñado para ser compatible con Lightweight Directory Access Protocol (LDAP).

Otro importante mecanismo de seguridad de Windows es Local Security Authority Subsystem (LSASS. Lsass es lo que el gusano Sasser explotaba por desbordamiento de búfer en el año 2004. Lsass es un proceso de modo de usuario que es el responsable de la política de seguridad del sistema local. Esto incluye el control de acceso, las políticas de gestión de contraseñas, la autenticación de usuarios y el envío de mensajes de auditoría de seguridad para el registro de eventos.

3.2.1 Enumeración NetBIOS y LDAP

NetBIOS fue una creación de IBM. Se considera un protocolo anticuado hoy, pero todavía se puede encontrar en algunos sistemas antiguos. En las redes de área local (LAN), los sistemas de NetBIOS normalmente se identifican mediante el uso de un nombre único de 15 caracteres. Debido a que NetBIOS no es enrutable de forma predeterminada, Microsoft lo adaptó para ejecutarse sobre TCP/IP. NetBIOS se usa en conjunto con Server Message Blocks (SMB). SMB permite el acceso remoto a directorios y archivos compartidos. Estos servicios se prestan a través de los puertos que se muestran en la Tabla:

Port	Protocol	Service
135	TCP	MS-RPC endpoint mapper
137	UDP	NetBIOS name service
138	UDP	NetBIOS datagram service
139	TCP	NetBIOS session service
445	TCP	SMB over TCP

Esta tabla muestra los principales puertos y protocolos que utilizan los sistemas de Microsoft. Al realizar un escaneo de puertos o el intento de identificar un sistema, encontrar estos puertos abiertos nos indicará que posiblemente estamos tratando con un sistema de Microsoft. Después de identificar estos puertos, podemos comenzar a enumerar cada sistema.

SMB fue diseñado para hacer posible que los usuarios compartan archivos y carpetas, aunque InterProcess Communication (IPC) ofrece un recurso por defecto en los sistemas Windows.

Una sesión nula se produce cuando se inicia sesión en un sistema sin ID de usuario ni contraseña. En versiones antiguas de Windows 2000, XP y Windows 2003, se podía establecer una sesión nula mediante el comando net.

Hay toda una serie de comandos net. Unos pocos se discuten aquí, pero para una lista más completa, sólo tenemos que escribir net desde la línea de comandos y la opción /? después de cualquiera de los comandos sobre los que nos gustaría obtener más información.

Aunque no podamos ver el recurso compartido de IPC$ en la búsqueda de unidades y carpetas compartidas, eso no significa que no está allí. Por ejemplo, si hemos identificado los puertos abiertos de 135, 139 y 445 en algunos sistemas específicos, es posible intentar el comando net view /domain:

```
C:\>net view /domain
Domain
SALES
MARKETING
ACCOUNTING
The command completed successfully.
```

Podemos echar un vistazo más detallado a cualquier sistema utilizando el comando net view \\system_name:

```
C:\net view \\donald
Shared resources at \\DONALD
Sharename    Type         Comment
-------------------------------------------------------
CDRW         Disk
D            Disk
Payroll      Disk
Printer      Disk
Temp         Disk
The command was completed successfully.
```

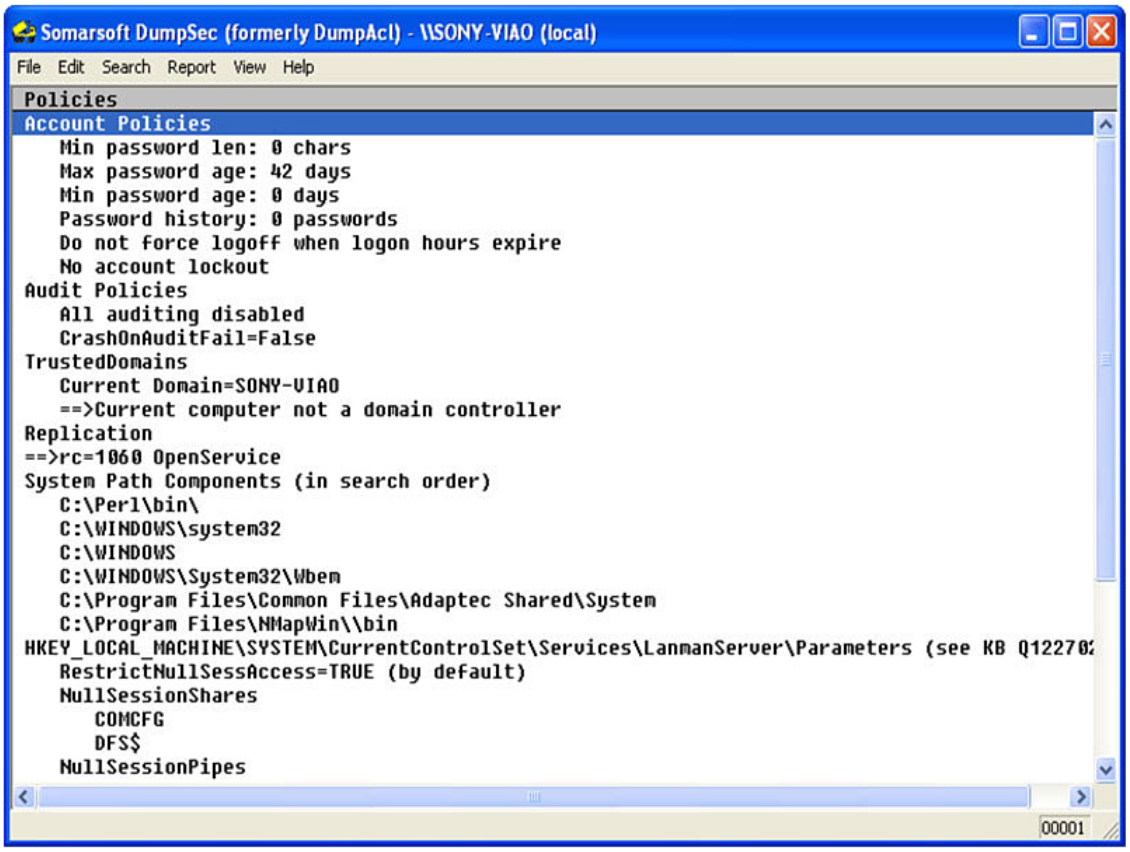
Ahora que hemos completado alguna tarea básica, vamos a pasar a enumerar los detalles de usuario, la información de cuenta, contraseñas débiles, y más. IPC$ se explota aún más para estas actividades. En concreto, tendremos que establecer una sesión nula. Podemos hacerlo de forma manual con el comando net:

```
C:\net use \\donald\ipc$ "" /u:""
```

Configurar una sesión nula para aprovecharse de los protocolos de comunicación de Windows subyacentes es algo que ya ha sido protegido en los sistemas operativos más recientes como Server 2012, Windows 7 y Windows 8, pero aún se pueden encontrar algunos viejos sistemas en los que esto sea posible.

Veamos algunas herramientas que nos pueden ayudar a automatizar este proceso de enumeración sobre máquinas Windows.

DumpSec revela recursos compartidos sobre una sesión nula con el ordenador objetivo:

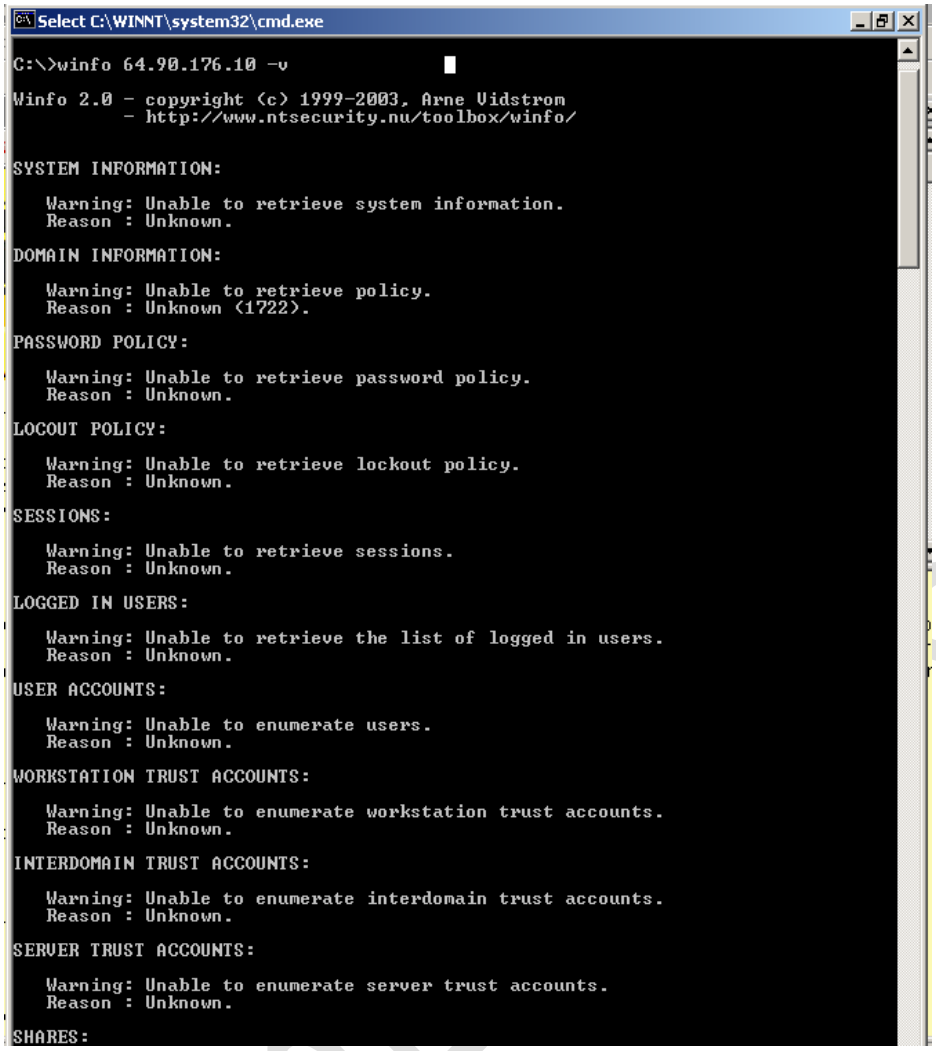


Winfo usa sesiones nulas para recopilar información de forma remota sobre el sistema objetivo.

Winfo da información detallada sobre lo siguiente:

- Información del Sistema
- Información del Dominio
- Política de Passwords
- Política de Logout
- Sesiones
- Usuarios logeados
- Cuentas de Usuario

OpenLearning

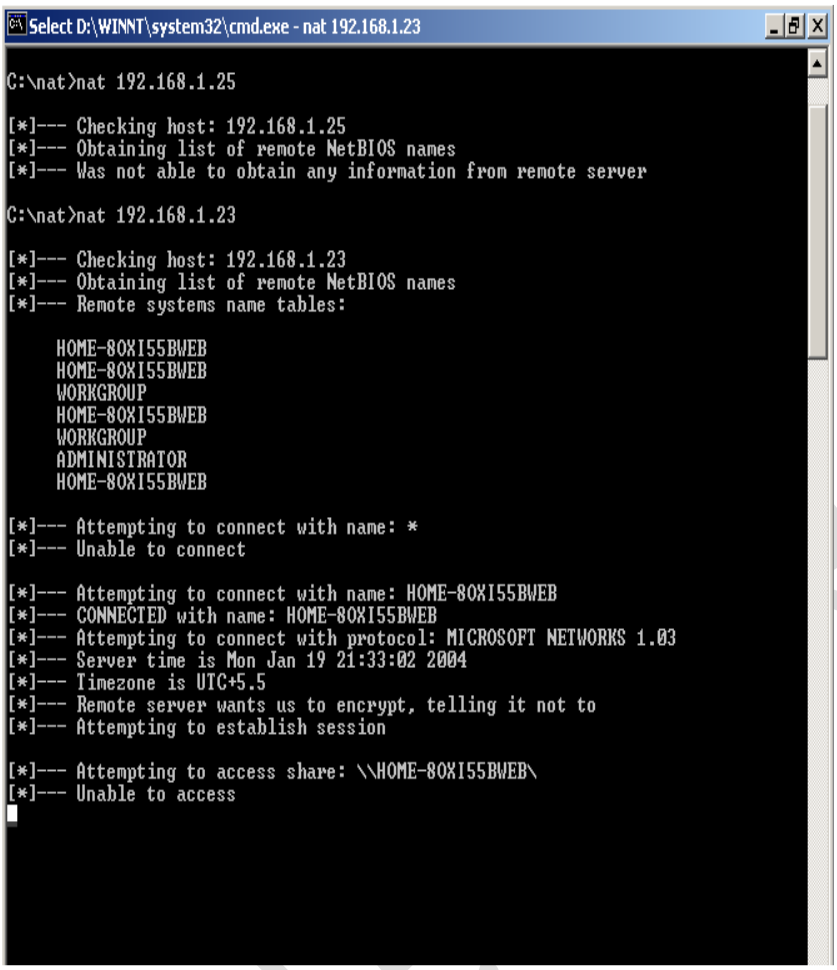


NetBIOS Auditing Herramienta (NAT) está diseñada para explorar los servicios de compartición de archivos de NetBIOS ofrecidos por el sistema objetivo.

Implementa una aproximación por etapas a la recopilación de información e intenta obtener acceso a nivel del sistema de archivos como si fuera un cliente local legítimo.

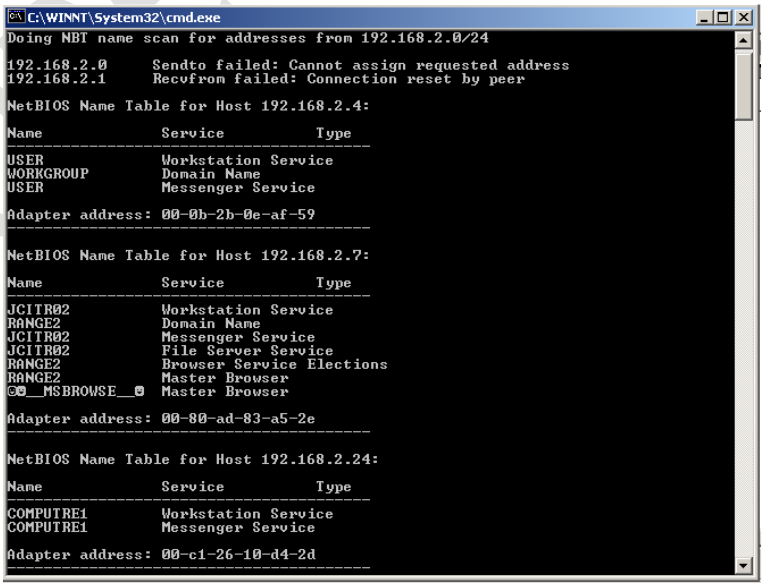
Si se puede establecer una sesión NetBIOS a través del puerto 139, el objetivo se declara “vulnerable”.

Una vez que se establece la sesión, se realizan transacciones para recoger más información sobre el servidor incluyendo cualquier sistema de archivos compartido que ofrezca.



NBTscan es un programa para escanear redes IP en búsqueda de información de nombres NetBIOS.

Para cada host que responde lista su dirección IP, nombre de ordenador NetBIOS, usuario logueado y dirección MAC.



Contramedidas para Null Session:

Las Null sessions requieren acceso a los puertos TCP 139 y/o 445. Podemos deshabilitar los servicios SMB completamente en hosts individuales desasociando el cliente TCP/IP WINS del interfaz.

También podemos editar el registro para restringir el usuario anónimo.

1. Abrir regedt32, navegar a HKLM\SYSTEM\CurrentControlSet\LSA

2. Elegir editar | añadir valor

- nombre valor: RestrictAnonymous
- Tipo de Dato: REG_WORD
- Valor: 2

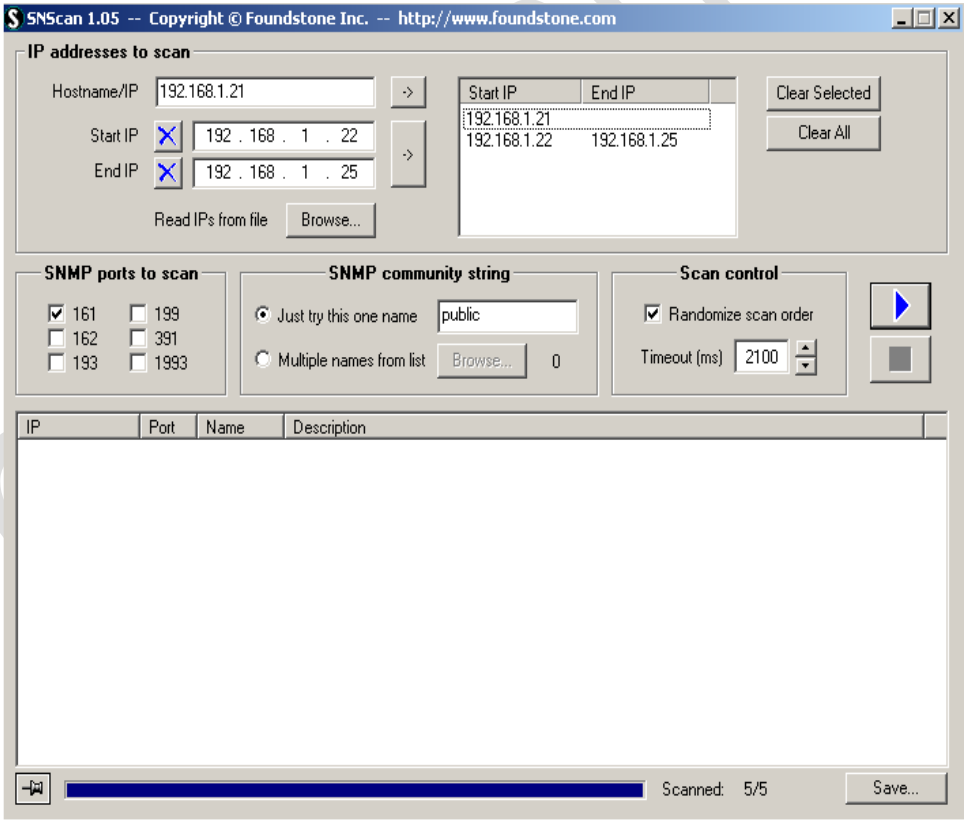
OpenLearning

3.3 Enumeración SNMP

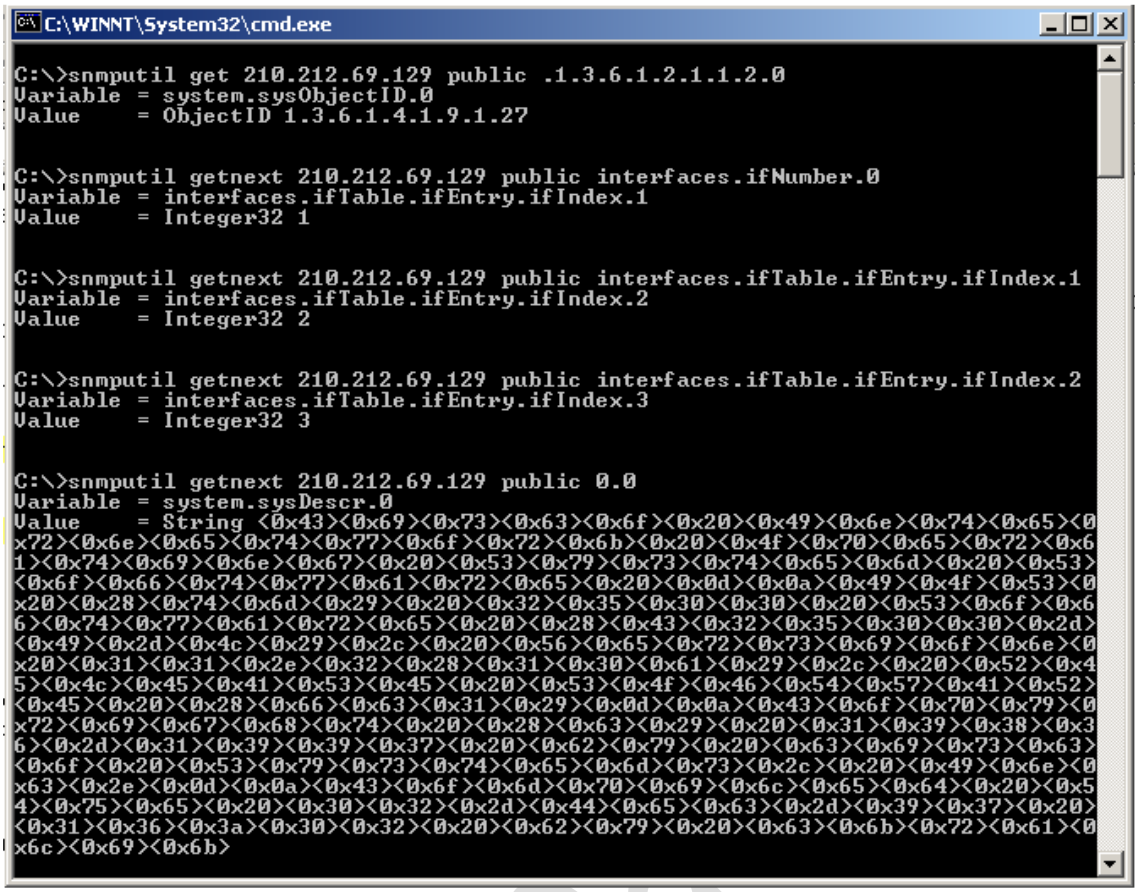
Simple Network Management Protocol (SNMP) es un estándar TCP/IP popular para la monitorización remota y la gestión de los hosts, routers y otros nodos y dispositivos de una red. Funciona a través de un sistema de agentes y nodos. SNMP está diseñado para que las solicitudes se envíen a los agentes, y los agentes envían respuestas de vuelta. Las peticiones y las respuestas se refieren a la configuración de variables accesibles por el software de agente. Los traps se utilizan para significar un evento, como por ejemplo un reinicio o el fallo de la interfaz. SNMP hace uso de la Base de información de administración (MIB). El MIB es la base de datos de las variables de configuración que reside en el dispositivo de red.

SNMP versión 3 ofrece encriptación de datos y autenticación, pero la versión 1 y 2 se encuentran todavía en uso. Tanto la versión 1 como la 2 son los protocolos en texto plano que proporcionan sólo seguridad débil mediante el uso de cadenas de comunidad. Las cadenas de comunidad predeterminadas son public y private y se transmiten en texto plano. Si las cadenas de comunidad no se han cambiado o si alguien puede esnifar las cadenas de comunidad, esa persona tiene entonces más que suficiente para enumerar los dispositivos vulnerables.

SNScan es un escáner SNMP basado en Windows que puede detectar de forma efectiva dispositivos SNMP en la red. Puede escanear los puertos y de uso público de SNMP, los definidos por el usuario, los nombres de comunidades SNMP. Es una útil herramienta para recogida de información.



Otra herramienta es SNMPutil:



Contramedidas para Enumeración SNMP

La forma más simple de evitar esta actividad es pasar a la versión 3 o eliminar el agente SNMP o apagar el servicio.

Si apagar SNMP no es una opción, cambiar el nombre por defecto de la comunidad “public”.

Implementar la opción de seguridad de la Política de Grupo llamada Restricciones Adicionales para Conexiones Anónimas.

El acceso a tuberías de null sessions, recursos compartidos de null sessions y el filtrado IPSec también debería estar restringido.

OpenLearning

3.4 Enumeración DNS

La enumeración DNS es el proceso de localizar toda la información sobre DNS. Esto puede incluir la identificación de los servidores DNS internos y externos, y realizar búsquedas de registros DNS de información, como nombres de usuario, nombres de equipos y direcciones IP de los sistemas de destino potenciales y las transferencias de zona. La forma más sencilla es utilizar Nslookup, pero también se pueden utilizar otras herramientas.

- DigDug
- WhereIsIP
- NetInspector
- Men and Mice Management Console

OpenLearning

3.5 Enumeración SMTP

Simple Mail Transfer Protocol (SMTP) se utiliza para la transmisión de mensajes de correo electrónico. SMTP funciona en el puerto TCP 25. SMTP es algo que a un hacker le interesará porque potencialmente puede ser utilizado para realizar la enumeración de nombres de usuario a través de los comandos EXPN, RCPT, y VRFY. Las pruebas de penetración también pueden aprovechar los nombres de usuario que se han obtenido a partir de esta enumeración para realizar nuevos ataques contra otros sistemas. La enumeración SMTP se puede realizar con utilidades como Netcat. Desde la línea de comandos, escribimos lo siguiente:

```
nc –v –z –w 2 Dirección IP 1-1024
```

Otras herramientas de enumeración SMTP comunes incluyen los siguientes:

- Herramientas NetScan Pro
- Nmap
- Telnet

OpenLearning