
4. Enumeración
Julio Javier Iglesias Pérez
C|EH Julio Iglesias Pérez

¿Qué es la enumeración?

La enumeración es definida como la extracción de nombres de usuario, equipos, recursos de redes, recursos compartidos y servicios.

Las técnicas de enumeración son conducidas en una ambiente Intranet.

La enumeración involucra conexiones activas a sistemas y consultas dirigidas.

¿Qué es la enumeración?

La información que es enumerada por los intrusos:

- Recursos de redes, recursos compartidos.
- Usuarios y grupos.
- Aplicaciones y banderas.
- Configuraciones de auditoría.

Técnicas para la enumeración

- Extraer nombres de usuario utilizando enumeración Win2k
- Extraer nombres de usuario utilizando SNMP
- Extraer nombres de usuario utilizando IDs (números de identificación) de correo electrónico.
- Extraer información utilizando contraseñas por defecto.
- Fuerza bruta Active Directory.

Sesiones nulas Netbios

La sesión nula es también conocida como la Biblia de Windows hacking. Las sesiones nulas toman ventaja en los Sistemas de Archivos Comunes de Internet o CIFS (Common Internet File System/Server Messaging Block) y en los bloques de mensaje de servidor SMB (Server Messaging Block).

Sesiones Nulas

net view (muestra info de la red)

net use \\victum\ipc$ "" /u:""

- Crea la sesión nula

net view \\victim

- Muestra el contenido

Sesiones Nulas

Podemos utilizar herramientas para sesiones nulas como el getacct. En esta herramienta podemos enumerar las cuentas de usuario. Tener en cuenta que el USER 500 será del administrador y el 501 del Guest.

Enumeración SNMP

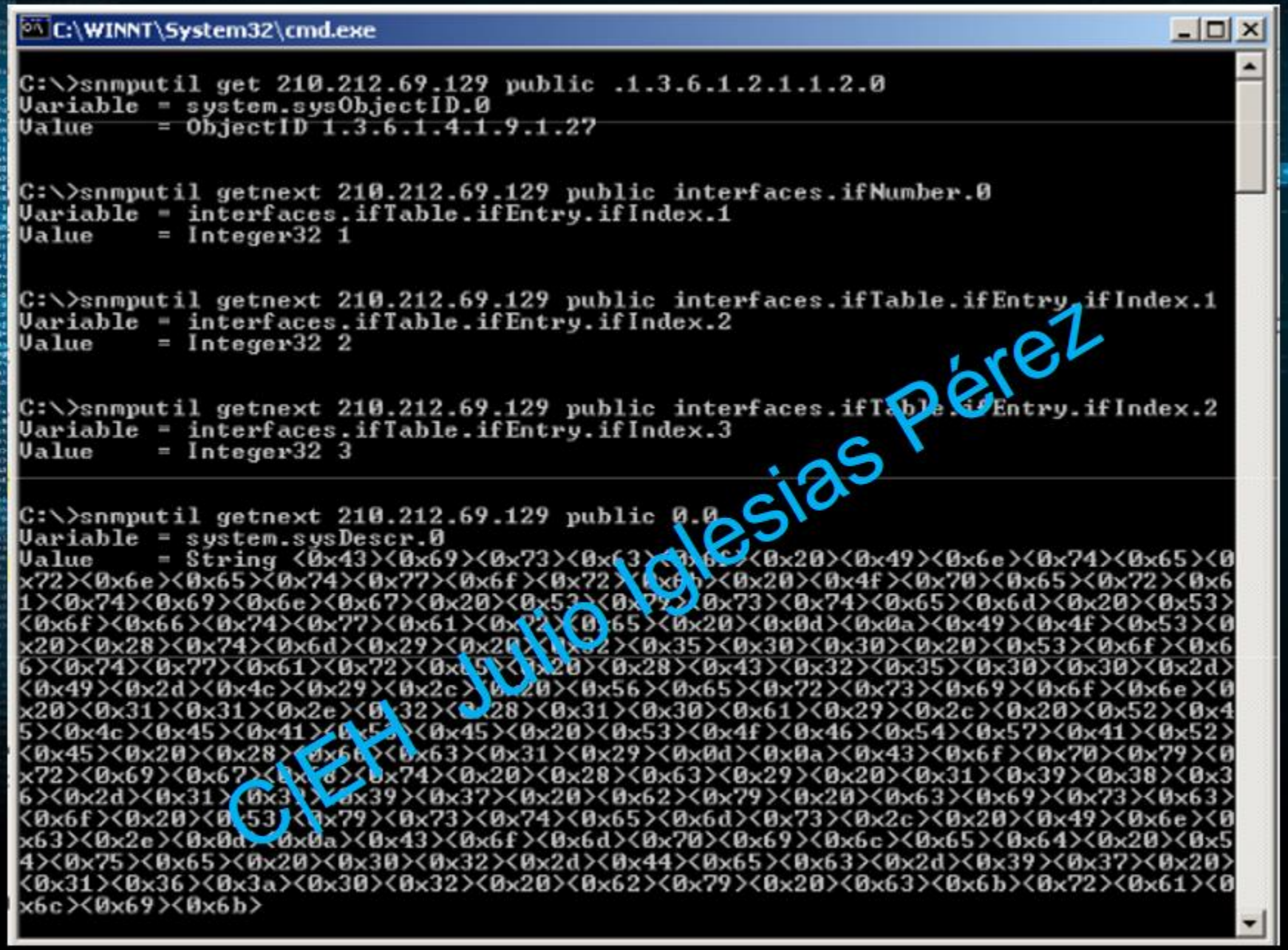
SNMP (Simple Network Management Protocol)

- Los administradores envían a los agentes y estos devuelven respuestas.
- Las solicitudes y respuestas se refieren a las variables de acceso al software agente.
- Los administradores también pueden enviar solicitudes para establecer determinadas variables.
- Las trampas hacen que el administrador note que algo significativo que ha ocurrido:
  - Un reinicio
  - Una falla de la interfaz
  - O bien, otra cosa potencialmente mala se ha producido
- La enumeración a usuarios NT vía protocolo SNMP es fácil utilizando snmputil.

Management Information Base

La base de la información de gestión MIB (Management Information Base) provee una representación estándar de la información disponible del agente SNMP y donde está almacenado.

Es el elemento más básico de la administración de red.

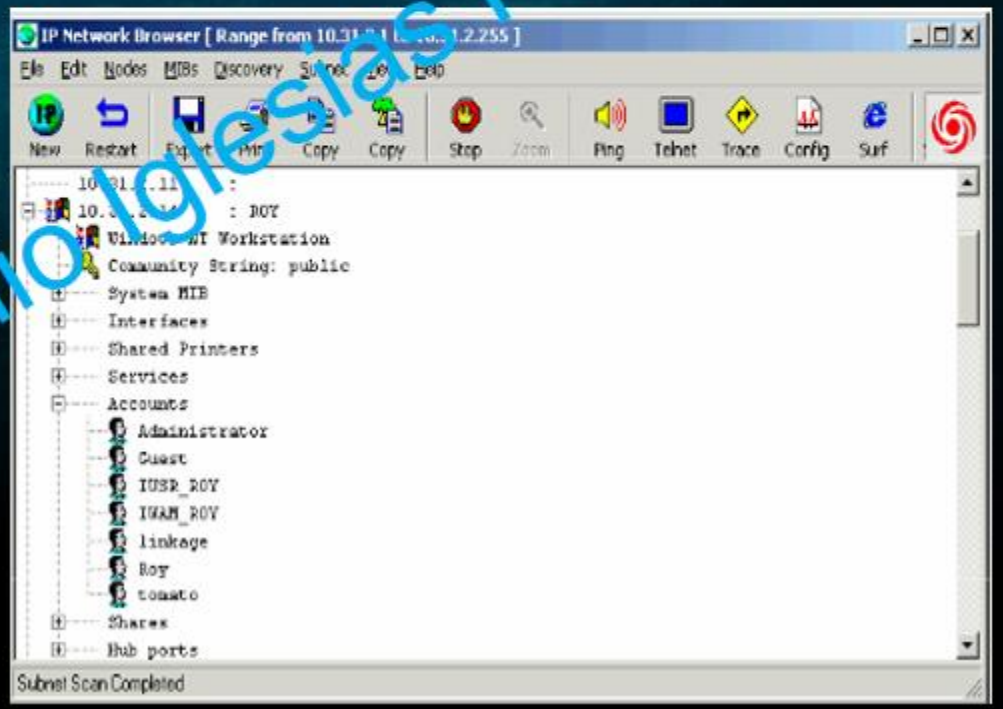

C:\WINNT\System32\cmd.exe
C:\>snmputil get 210.212.69.129 public .1.3.6.1.2.1.1.2.0
Variable = system.sysObjectID.0
Value = ObjectID 1.3.6.1.4.1.9.1.27
C:\>snmputil getnext 210.212.69.129 public interfaces.ifNumber.0
Variable = interfaces.ifTable.ifEntry.ifIndex.1
Value = Integer32 1
C:\>snmputil getnext 210.212.69.129 public interfaces.ifTable.ifEntry.ifIndex.1
Variable = interfaces.ifTable.ifEntry.ifIndex.2
Value = Integer32 2
C:\>snmputil getnext 210.212.69.129 public interfaces.ifTable.ifEntry.ifIndex.2
Variable = interfaces.ifTable.ifEntry.ifIndex.3
Value = Integer32 3
C:\>snmputil getnext 210.212.69.129 public 0.0
Variable = system.sysDescr.0
Value = String
CEH Julio Iglesias Pérez

Herramienta de enumeración SolarWinds

- Es un conjunto de herramientas de administración de redes.

El conjunto consiste en:

- Administración de direcciones.
- Descubrimiento.
- Herramientas Cisco.
- Herramientas ping.
- Monitoreo.
- Navegador MIB.
- Seguridad.
- Miscelanea.



Herramientas de enumeración SNMP

- Herramientas de enumeración SNMP
- Getif SNMP MIB Browser
- OidView SNMP MIB Browser
- iReasoning MIB Browser
- SNScan
- Etc.

Enumeración UNIX/Linux

showmount -e 192.168.1.x

Encuentra directorios compartidos en el equipo

finger -l @target.hackme.coom

Enumera el usuario y host, muestra el directorio del usuario, tiempo de login, idle times, office location y la última vez que recibió o leyó un mail.

Enumeración UNIX/Linux

rpcclient $> netshareenum

Enumera los usernames de Linux y OSX

rpcinfo -p 192.168.1.x

Ayuda a enumerar el protocolo Procedure Call Protocol, el RPC permite a las aplicaciones comunicarse en la red.

Enumeración LDAP

El Protocolo Ligero de Acceso a Directorio es un protocolo utilizado para acceder al listado del directorio Active Directory u otros servicios de directorio.

Tiende a estar vinculado al servicio DNS para permitir una integración.

Trabaja en el puerto TCP 389

Herramientas: Jxplorer, Symlabs LDAP Browser, LDAP Admin Tool, LDAP Account Manager, etc.

Enumeración NTP

El protocolo NTP está diseñado para sincronizar los relojes de los en equipos en una red. Utiliza el puerto UDP 123.

Para enumerar los servidores NTP simplemente se busca el puerto mencionado o también se puede utilizar la herramienta NTP Server Scanner.

Para enumeración del protocolo SMTP(y otros) se pueden utilizar las herramientas: NTP Server Scanner, PresenTense Time Server, etc.

Enumeración SMTP

El Protocolo simple de transferencia de correos SMTP (Simple Mail Transport Protocol) es utilizado para enviar mensajes de correo al contrario que POP3 o MMAP que son enviados para recibir correos.

Generalmente utiliza servidores Intercambio de correos MX (Mail Exchange) que dirigen los correos vía servicio de nombre de dominio DNS.

Opera sobre el puerto TCP 25.

Una herramienta de enumeración SMTP es: NetScanTools Pro

- Es posible interactuar directamente con un SMPT vía telnet:

```
telnet 192.168.0.1 25
220 uk03.cak.uk ESMTP Sendmail 8.9.3; Wed, 9 Nov 2005 15:29:50 GMT
EXPN ROOT
250 <root@uk03.nu.cak.uk>
250 <smith.j@uk03.nu.cak.uk>
EXPN BIN
250 <bin@uk03.nu.cak.uk>
VRFY NOBODY VRFY NOBODY
250 <nobody@uk03.nu.cak.uk>
EXPN NOBODY
250 /dev/null@uk03.nu.cak.uk>
VRFY ORACLE
550 ORACLE... User unknown
QUIT
```

Enumeración DNS

Ejemplo de enumeración DNS

nslookup

> ls -d nombre_de_la_zona

Si la transferencia de zonas está habilitada, mostrará el resultado completo de dicha zona

Enumerando Sistemas utilizando contraseñas por defecto

Muchos dispositivos como routers, switches, hubs llegan con contraseñas por defecto.

Muchas veces se pueden acceder a estos dispositivos utilizando estas contraseñas por defecto.

Buscar en google acerca de default password para ver las contraseñas por defecto de routers, modems, etc.

Contramedidas

SNMP

- Quitar el agente SNMP o apagarlo.
- Actualizar a SNMP3.
- Implementar la directiva de grupo "Additional Restrictions for anonymous connections"

Contramedidas

DNS

- Deshabilitar la transferencia de zonas a hosts no confiados.
- Asegurarse que los nombres de host no públicos no estén accesibles desde fuera.
- Asegurarse que los registros HINFO y otros no aparezcan en los archivos de la zona DNS.
- Proveer detalles estándar sobre el administrador de la red.

Contramedidas

SMTP

- Configurar los servidores SMTP para ignorar mensajes de correo hacia destinatarios desconocidos.
- Configurar los servidores SMTP para que ignore correos desde destinatarios desconocidos.

Contramedidas

LDAP

- Utilizar autenticación básica o NTLM para limitar el acceso a usuarios conocidos solamente.
- Utilizar tecnología SSL para cifrar el tráfico.
- Habilitar el bloqueo de cuentas.

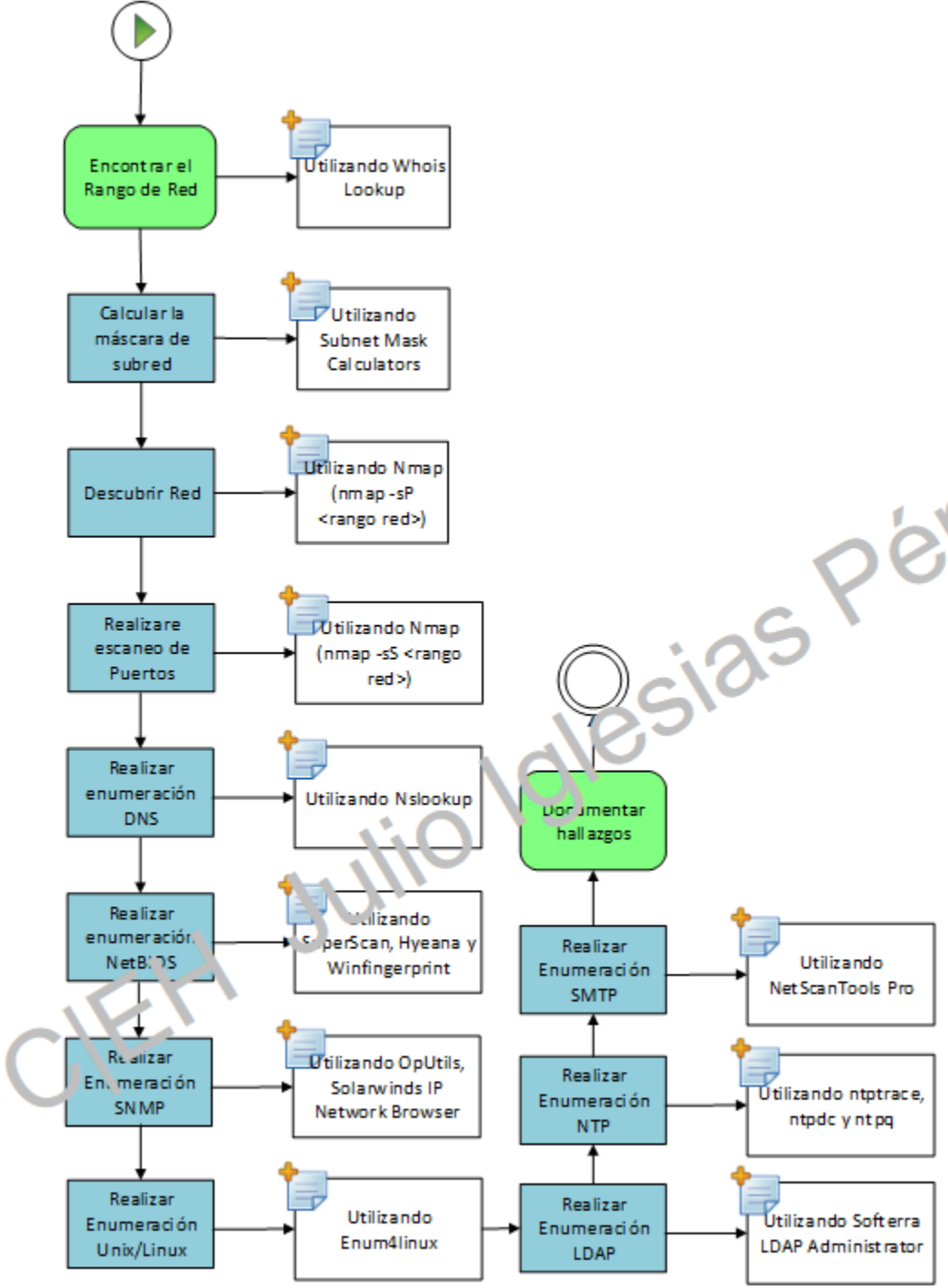
Contramedidas

SMB

- Deshabilitar las opciones de Client For Microsoft Networks, y File and Printer Sharing for Microsoft Networks. Desinstalarlas de las propiedades de Conexion de área local.

Test de Intrusión de Enumeración

Se utiliza para identificar cuentas de usuario válidas o recursos de red pobremente compartidos utilizando conexiones activas a los sistemas.




¡Muchas Gracias!
C|EH Julio Iglesias Perez