Nebrija Universidad MADRID

Hacking Ético

Módulo II_b

Fase 2: Enumeración y detección de vulnerabilidades

Objetivos

- Comprender la enumeración de Windows
- Cómo conectarse mediante una sesiój nula (null session)
- Cómo evitar la enumeracion NetBIOS
- Cómo robar información del DNS en Windows 2000 usando transferencia de zone
- Aprender cómo enumerar usuarios CIFS/SMB
- Enumeración del Active Directory

Qué es la enumeración

- Es el proceso de obtener las cuentas de usuarios y vulnerabilidades (recursos mal protegidos)
- La Enumeración incluye conexiones activas a sistemas y consultas directas.

Net Bios Null Sessions

- Null Sessions se aprovecha de un defecto en los protocolos CIFS/SMB (Common Internet File System/ Server Messaging Block).
- Se puede establecer una sesión nula (Null Session) en un Windows (NT/2000/XP) iniciando sesión con un nombre de usuario y contraseña vacíos.
- Gracias a esto vamos a poder obtener la siguiente información del equipo:
  - Lista de usuarios y grupos
  - Lista de máquinas
  - Lista de recursos compartidos
  - SIDs (Security Identifiers) de usuarios y equipos

Net Bios Null Sessions

- net use \\192.34.34.2 \IPC$ "" /u: ""
- Mediante esta orden se puede abrir una conexión al recurso compartido oculto IPC$ (Process Communication) en la dirección IP 192.34.34.2 con el usuario anónimo predeterminado (/u:"") con password vacía ("")

Contramedidas

- Null sessions requiere acceso a los puertos TCP 139 y/o TCP 445.
- Se podrían deshabilitar los servicios SMB por completo en determinados equipos eliminando el cliente Wins TCP/IP de la conexión de red.
- O editar el registro para restringir el acceso anónimo.
  - 1. Ejecutar regedt32, ir a HKLM\SYSTEM\CurrentControlSet\LSA
  - 2. Elegir edit | add value
    - value name: ResticAnonymous
    - Data Type: REG_WORD
    - Value: 2

Hacking Tool: Nessus

- Arquitectura cliente-servidor
- El servidor se puede instalar desde la página o con apt.
- El cliente sólo desde la página
- Servidor
  - Crear una cuenta inicial nessusd
    - nessus-adduser
  - Crear reglas para restringir (opcional)
    - deny 10.163.156.1
    - accept 10.163.156.0/24
    - default deny

Hacking Tool: Nessus

- Iniciar Nessus (en /etc/init.d si se instaló con apt-get o en /opt si se hizo desde la web)
  - sudo nessusd -D
  - sudo /etc/init.d/nessusd start
- Iniciar el cliente:
  - /usr/X11R6/bin/NessusClient
  - Conectarse al servidor (en teoría nuestra máquina)
- Elegir el objetivo y las opciones (si acaso deshabilitar DoS)

Hacking Tool: Nessus

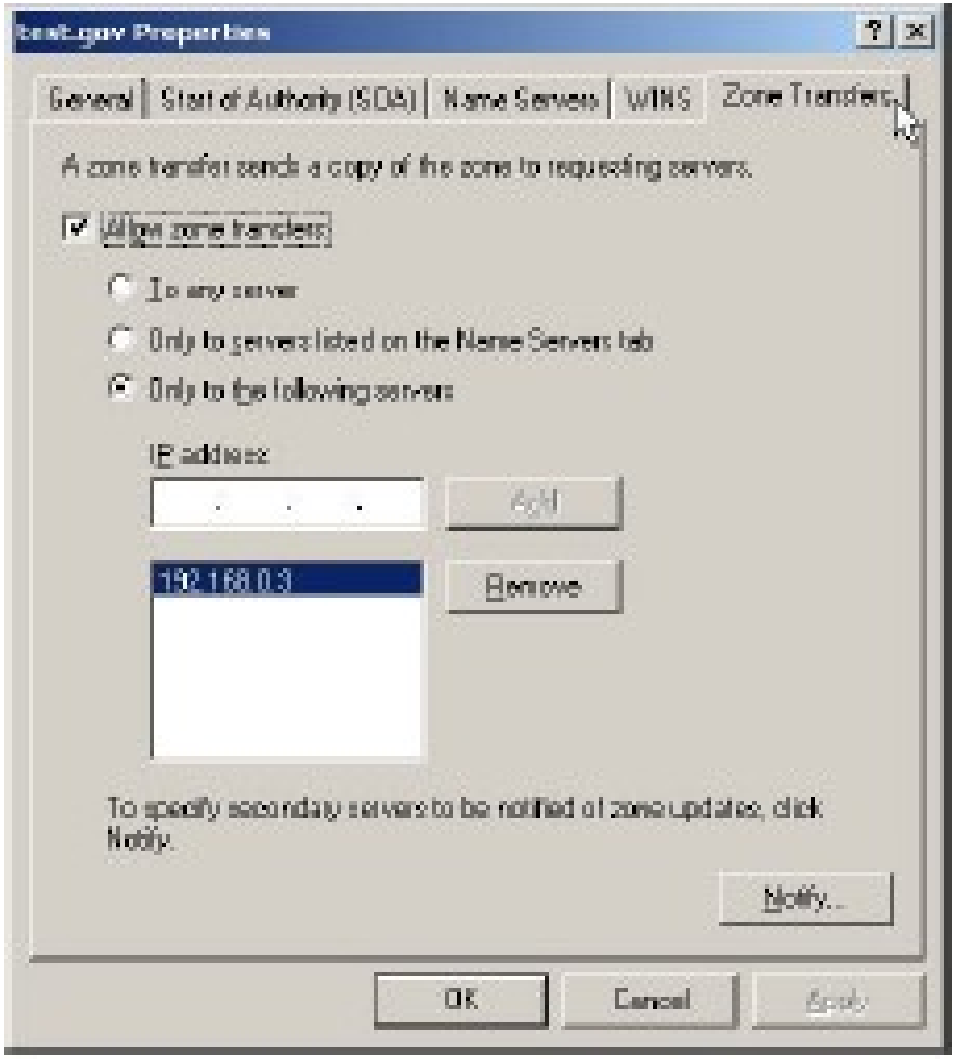
- Informe (exportado a html):
  - http://www.nessus.org/demo/report.html
- Puntos importantes:
  - Ver los security holes (vulnerabilidades)
    - Posiblemente SMB/Netbios
  - Ver los warnings
    - Posibilidad de null sessions
    - Usuarios y SIDs
    - Directivas de seguridad
    - ...

Windows 2000 DNS Zone transfer

- Para que lo clientes puedan encontrar servicios de dominios Win 2k como el Directorio Activo (AD) y kerberos, Win 2k necesita los registros SRV.
- La transferencia de zona (nslookup, ls -d <domainname>) puede enumerar un montón de información interesante.
- Un atacante miraría los siguientes registros:
  - 1. Global Catalog Service (_gc._tcp_)
  - 2. Domain Controllers (_ldap._tcp)
  - 3. Kerberos Authentication (_kerberos._tcp)

Bloquear la transferenca de zona en Win2k

Se puede bloquear fácilmente la transferencia de zona especificando los servidores que pueden pedir dicha operación.



Enumeración del Active Directory

- Todos los usuarios y grupos pueden ser obtenidos mediante una simple consulta LDAP.
- Lo único que hay que hacer es crear una sesión autentificada vía LDAP.
- Conectar a cualquier servidor AD usando ldp.exe port 389 (o cualquier cliente LDAP)
- Autentícate usando Guest (invitado) o cualquier cuenta del dominio
- Obtendremos todas las cuentas del dominio:usuarios, grupos y equipos.

Medidas para evitar la enumeración AD

- Cómo es posible hacer esto con una cuenta de invitado?
- Al hacer el dcpromo (construir el dominio) se puede elegir entre:

  1.Permisos compatibles con pre-Win2k

  2.Permisos compatibles sólo con Win2k
- Elegir la opción 2 en la instalación del AD.

Resumen

- La enumeración implica conexiones activas a sistemas y consultas o queries directas.
- El tipo de información obtenida incluye recursos compartidos de la red, usuarios, grupos y aplicaciones.
- Null sessions son usadas por los crackers para conectarse a los sistemas objetivo.
- Enumeraciones NetBIOS y SNMP se pueden realizar con herramientas como el Nessus.
- Herramientas como user2sid, sid2user y userinfo se pueden usar para identificar cuentas del sistema (aunque esto ya lo hace el Nessus).