Fundamentos de Auditoría y Reconocimiento de Seguridad: Guía de Comandos Esenciales

En el ámbito de la ciberseguridad, la fase de **reconocimiento y enumeración** es crítica. Antes de proteger un sistema, debemos entender qué estamos protegiendo. La auditoría local permite identificar configuraciones erróneas, privilegios excesivos y vectores de ataque potenciales que un actor malintencionado podría explotar.

A continuación, detallamos las herramientas y comandos nativos de Windows necesarios para realizar una evaluación de seguridad profunda sin necesidad de instalar software de terceros.

1. Mapeo de la Superficie del Sistema

El primer paso es conocer el terreno. La información del sistema nos indica el nivel de parches y la arquitectura base.

- **Comando:** systeminfo
    - **Utilidad técnica:** Proporciona el nombre del host, la versión exacta del SO y, lo más importante, los **Hotfixes (parches de seguridad)** instalados.
    - **Enfoque de seguridad:** La ausencia de ciertos parches puede indicar vulnerabilidades conocidas (CVEs) que permiten la escalada de privilegios.
- **Comando:** wmic logicaldisk get name, size, freespace
    - **Enfoque de seguridad:** Identifica unidades montadas, incluyendo particiones ocultas o dispositivos USB no autorizados que podrían contener herramientas de ataque o exfiltración de datos.

2. Auditoría de Red y Conectividad

La red es el vector de entrada más común. Entender cómo se comunica el equipo es vital para detectar intrusiones.

- **Comando:** ipconfig /all
    - **Utilidad:** Revela la configuración de DNS, puertas de enlace y la dirección física (MAC). Un servidor DNS

desconocido podría indicar un ataque de **DNS Hijacking**.

- **Comando:** arp -a
    - **Enfoque de seguridad:** Muestra la tabla de resolución de direcciones. Si ves dos direcciones IP diferentes con la misma dirección MAC, podrías estar siendo víctima de un ataque de **ARP Spoofing** (Man-in-the-Middle).

3. Análisis de Servicios y Puertos Activos

Un puerto abierto es una puerta potencial. Saber qué proceso lo controla es la diferencia entre un servicio legítimo y una *backdoor*.

- **Comando:** netstat -ano
    - **Detalle:** El parámetro -o es crucial porque muestra el **PID (Process ID)**. Esto nos permite rastrear qué programa específico está escuchando en un puerto sospechoso.
- **Comando:** tasklist /v
    - **Utilidad:** Lista todos los procesos con el nombre de usuario que los ejecuta. Permite identificar procesos maliciosos camuflados con nombres genéricos (como svchost.exe) pero ejecutados por usuarios no sistémicos.

4. Evaluación de Privilegios y Usuarios

El principio de **menor privilegio** es la base de la seguridad. Estos comandos ayudan a verificar si un usuario tiene más poder del que debería.

- **Comando:** whoami /priv
    - **Enfoque de seguridad:** Muestra los tokens de privilegio. Privilegios como SeBackupPrivilege o SeImpersonatePrivilege son críticos, ya que pueden ser explotados para elevarse a nivel de SYSTEM.
- **Comando:** Get-ExecutionPolicy (PowerShell)

    - **Detalle:** Si la política es Bypass o Unrestricted, el sistema es vulnerable a la ejecución de scripts maliciosos de PowerShell que evaden las restricciones estándar.

5. Estado de las Defensas Perimetrales y Activas

No basta con tener defensas; hay que comprobar que estén activas y correctamente configuradas.

- **Comando:** netsh firewall show state (o el moderno netsh advfirewall show allprofiles)
    - **Utilidad:** Indica si el firewall está activo en perfiles públicos, privados o de dominio. Un firewall desactivado en el perfil "Domain" es una bandera roja inmediata.
- **Comando:** Get-MpComputerStatus (PowerShell)
    - **Enfoque de seguridad:** Es la forma más rápida de verificar si **Windows Defender** está actualizado, si el escaneo en tiempo real está activo y cuándo fue la última vez que se detectó una amenaza.

Conclusión y Buenas Prácticas

La seguridad no es un estado estático, sino un proceso continuo. El uso regular de estos comandos permite a los administradores:

1. **Detectar anomalías** antes de que se conviertan en brechas.
2. **Prepararse para auditorías** externas manteniendo un inventario limpio.
3. **Fortalecer (Hardening)** el sistema cerrando vectores innecesarios.


Fundamentos de Auditoría y Reconocimiento de Seguridad: Herramientas y Comandos Clave
1 Información del Sistema
systeminfo
Muestra información detallada sobre el sistema operativo, hardware, y posibles vulnerabilidades de seguridad.
2 Configuración de Red
ipconfig /all
arp -a
Vista completa de red, IP, DNS, MAC; tabla ARP para identificar dispositivos.
3 Estado de los Procesos y Puertos Abiertos
netstat -ano
tasklist /v
Lista puertos abiertos y procesos activos, ideal para detectar intrusos.
4 Estado del Firewall y Seguridad en el Sistema
netsh firewall show state
Consulta el estado del firewall y las reglas activas, crucial para asegurar puertos.
5 Seguridad de Usuario y Privilegios
whoami /priv
Get-ExecutionPolicy
Privilegios de usuario actual; políticas de ejecución de scripts en PowerShell.
6 Estado de Protección Contra Amenazas
Get-MpComputerStatus
Revisa el estado de Windows Defender y las amenazas activas.
7 Inventario del Sistema de Almacenamiento
wmic logicaldisk get name
Muestra discos duros y particiones, útil para identificar cambios no autorizados.
#AuditoríaDigital #Ciberseguridad #HerramientasClave