Capítulo 3
Auditar Active Directory

1. Metodología

Antes de adentrarnos en los aspectos técnicos de la auditoría de un Active Directory, es fundamental situar el proceso en un marco metodológico claro. Una auditoría seria no se limita a la ejecución de unas cuantas herramientas o a la búsqueda oportunista de vulnerabilidades; se trata de un proceso estructurado, concebido para ser a la vez exhaustivo, reproducible y comprensible para todas las partes interesadas, ya sean equipos técnicos o direcciones estratégicas.

Por ello, en primer lugar, presentaremos las principales metodologías que sirven de hilo conductor para las pruebas de intrusión y las auditorías de seguridad. Estos marcos aportan una lógica a la evaluación, permiten trazar sus etapas y establecen un lenguaje común entre auditores y auditados.

1.1 El PTES: un estándar de referencia

El PTES (*Penetration Testing Execution Standard*) es, sin duda, uno de los marcos más conocidos en el ámbito del pentest. Define un conjunto de etapas que estructuran la realización de una auditoría de seguridad, desde la preparación hasta la restitución.

El PTES se articula en varias fases:

– **Pre-compromiso**: definición del alcance, los objetivos y las reglas de la auditoría.
– **Recopilación de información**: fase de reconocimiento en la que se recopila el máximo de datos disponibles sobre el entorno objetivo (mapeo de la red, inventario de equipos, descubrimiento de Active Directory).
– **Modelización de amenazas**: identificación de los vectores de ataque más relevantes en función del contexto.
– **Análisis de vulnerabilidades**: detección de debilidades técnicas u organizativas que puedan ser explotadas.
– **Explotación**: intento de aprovechar las vulnerabilidades descubiertas para obtener acceso o elevar privilegios.
– **Post-explotación**: consolidación de los accesos, búsqueda de movimientos laterales y extracción de información sensible.
– **Informes**: presentación clara y documentada de los hallazgos, con recomendaciones adecuadas.

En el contexto de un Active Directory, el PTES encuentra una aplicación especialmente relevante. La fase de recolección de información incluye, en particular, la enumeración de cuentas, grupos, relaciones de confianza y directivas de seguridad. La modelización de amenazas se centrará en los posibles abusos de configuraciones inadecuadas, fallos en la gestión de contraseñas o delegaciones mal controladas. La fase de post-explotación consiste entonces en aplicar técnicas como el Pass-the-Hash, la extracción de tickets de Kerberos o el uso indebido de los nombres principales de servicio (SPN) para avanzar en el entorno.

1.2 La Cyber Kill Chain: pensar como un atacante

Desarrollada por Lockheed Martin, la Cyber Kill Chain es un modelo que describe las etapas de un ataque dirigido. A diferencia del PTES, que está concebido como una guía de buenas prácticas para el auditor, la Kill Chain se sitúa más bien desde el punto de vista del atacante.

© Editions ENI - All rights reserved

Consta de siete etapas sucesivas:

- **Reconocimiento**: identificación de los objetivos y recopilación de información.
- **Weaponización**: preparación del ataque (explotación, payload).
- **Delivery**: envío de la carga maliciosa (phishing, explotación de la red, etc.).
- **Explotación**: ejecución del código o aprovechamiento de una vulnerabilidad.
- **Instalación**: implantación de puertas traseras o herramientas de persistencia.
- **Command & control (C2)**: establecimiento de un canal de comunicación entre el atacante y el entorno comprometido.
- **Actions on Objectives**: consecución de los objetivos (robo de datos, elevación de privilegios, sabotaje).

En el marco de una auditoría de Red Team, la Cyber Kill Chain resulta especialmente útil, ya que permite simular paso a paso las tácticas reales del adversario y evaluar la capacidad de detección y reacción de la organización ante un ataque completo.

1.3 Más allá de los modelos: hacia un enfoque estructurado

Si bien el PTES y la Cyber Kill Chain constituyen marcos de referencia sólidos, pueden complementarse de forma útil con otros enfoques. La norma NIST SP 800-115 ofrece una guía metódica para la realización de pruebas de seguridad, mientras que la base de conocimientos MITRE ATT&CK traza un mapa de las tácticas y técnicas empleadas por los atacantes, lo cual resulta especialmente relevante para anticipar e ilustrar escenarios de intrusión en un Active Directory. Más allá de su contenido, estos marcos de referencia aportan una estructura y una visión de conjunto que refuerzan el alcance de la auditoría. La adopción de este enfoque metodológico no debe percibirse como una limitación; por el contrario, constituye una garantía de rigor y coherencia. Asegura una cobertura completa de las pruebas, evita un enfoque fragmentado limitado a los aspectos puramente técnicos y facilita la comunicación con los responsables de la toma de decisiones, al transformar las observaciones operativas en elementos comprensibles desde el punto de vista estratégico.

La auditoría de un Active Directory va, por tanto, más allá del mero uso de herramientas para integrarse en una evaluación global y estructurada de la seguridad de la organización.

2. Recopilación de información

En cualquier proceso de auditoría, el reconocimiento constituye el primer paso y, sin duda, uno de los más decisivos. Se sitúa en el centro de las metodologías presentadas anteriormente: es la fase inicial del PTES y de la Cyber Kill Chain. En esta fase, el auditor aún no busca explotar vulnerabilidades, sino recopilar la máxima información posible sobre el entorno objetivo. Estos datos brutos, a menudo obtenidos de forma pasiva o anónima, servirán de base para todas las etapas posteriores. Cuanto más riguroso y completo sea el reconocimiento, mayor será la eficacia de la auditoría.

2.1 Descubrimiento de la red e identificación de los servicios

2.1.1 Descubrimiento

La primera tarea suele consistir en **realizar un mapeo de la red** para identificar los sistemas conectados y los servicios expuestos. Las herramientas de código abierto como **Nmap**, **Masscan** o **Rustscan** permiten escanear los rangos de direcciones IP incluidos en el perímetro de la auditoría. El objetivo es detectar los servidores críticos y, en particular, los **controladores de dominio de Active Directory**, reconocibles por la presencia de servicios característicos como **LDAP** (389/TCP, 636/TCP), **Kerberos** (88/TCP, 88/UDP), **DNS** (53/TCP, 53/UDP), **Global Catalog** (3268/TCP, 3269/TCP) o incluso **ADWS**(9389/TCP).

Estas herramientas también pueden ayudar a detectar servicios inesperados o mal protegidos, que a menudo constituyen puntos de entrada interesantes.

© Editions ENI - All rights reserved

Entre las numerosas herramientas de mapeo de redes, **Nmap** se erige como una referencia imprescindible. Su popularidad no se debe únicamente a su larga trayectoria, sino a la riqueza de sus funcionalidades, su portabilidad (Linux, Windows, macOS) y su activa comunidad. Permite descubrir hosts, identificar los servicios en escucha, reconocer las versiones de software e incluso ejecutar scripts de auditoría automatizados.

Entre sus numerosas opciones, algunas merecen una atención especial, ya que cubren la mayoría de las necesidades de reconocimiento:

`-n`: desactiva la resolución DNS para acelerar el escaneo y evitar consultas innecesarias.

`-sn`: ejecuta únicamente una detección de hosts (ping scan), sin escanear los puertos.

`-Pn`: considera el host como activo sin enviar un ping previo, lo cual resulta útil cuando se filtra el ICMP.

`-T5`: ajusta el nivel de agresividad del escaneo (T3 es el comportamiento por defecto; `T5` es mucho más rápido, pero más detectable).

Para el escaneo de puertos:

`-sS`: realiza un escaneo SYN sigiloso, rápido y discreto, muy utilizado en auditorías.

`-p-`: escanea los 65 535 puertos TCP, para una cobertura completa.

`--top-ports <N>`: se limita a los N puertos más utilizados (por defecto, 1 000).

`--open`: muestra únicamente los puertos abiertos, lo que facilita la lectura de los resultados.

Para la identificación de servicios:

`-sV`: activa la detección de versiones de software.

`--version-intensity <0-9>`: ajusta el nivel de profundidad de esta detección (7 por defecto, siendo 9 el más agresivo).

`-sC`: ejecuta los scripts predeterminados de Nmap (NSE), que comprueban configuraciones o vulnerabilidades comunes.

`--script <nombre>`: permite ejecutar scripts específicos (por ejemplo, relacionados con SMB, LDAP o DNS).

Por último, para los informes:

`-oG <ARCHIVO>`: exporta los resultados a un formato compatible con grep, muy práctico para su reutilización por otras herramientas.

`-oX <ARCHIVO>`: exporta los resultados en XML, un formato práctico para integrarlos en un informe.

Estas opciones, combinadas adecuadamente, permiten adaptar **Nmap** a la mayoría de los contextos que se dan en una auditoría: desde el descubrimiento inicial rápido hasta el análisis en profundidad de servicios críticos.

Nmap admite una gran variedad de objetivos: una dirección IP única, varias direcciones separadas por espacios, un rango de IP (p. ej., 192.168.1.1-50), una CIDR (p. ej., 192.168.1.0/24) o incluso un archivo que contenga una lista de hosts (-iL <ARCHIVO>).

– Detección de hosts activos:

```
nmap -sn <ip>
```

– Detección automatizada y exportación de hosts:

```
nmap -sn <subred> -oG - | awk '/Up$/{print $2}' > hosts.txt
```

– Detección de Active Directory:

```
nmap -sS -Pn -p 53,88,389,636,3268,3269,9389 --open -iL hosts.txt
```

– Identificación rápida de los servicios expuestos:

```
nmap -sS -Pn -sV --top-ports 50 --open -iL hosts.txt
```

– Escaneo TCP completo:

```
nmap -sS -Pn -sC -sV -p- --open -iL hosts.txt
```

– Escaneo UDP específico:

```
nmap -sU -Pn -sV --top-ports 50 --open -iL hosts.txt
```

© Editions ENI - All rights reserved

La salida sin procesar de Nmap, aunque es muy completa, a veces puede resultar difícil de leer cuando muestra un gran número de hosts y servicios. Para mejorar la legibilidad, se puede utilizar **grc** (*Generic Colouriser*), una sencilla herramienta que añade color y hace que la interpretación de los resultados resulte mucho más agradable. Este programa no se limita a Nmap: también se puede aplicar a muchas otras utilidades de línea de comandos, lo que hace que la experiencia de auditoría resulte más cómoda.

```
apt install grc
grc nmap -sn <ip>
```

2.1.2 Análisis de DNS y búsqueda de información relacionada

En un entorno de Active Directory, el DNS desempeña un papel fundamental, ya que se encarga de la resolución de los nombres de los equipos y de los servicios vinculados al dominio. Por lo tanto, el auditor debe recurrir a este servicio para extraer información adicional. Tras identificar los controladores de dominio mediante escaneos y análisis de servicios, es esencial configurar correctamente la resolución DNS en el equipo de auditoría. En una distribución como Kali Linux, esto suele consistir en añadir la dirección IP de un controlador de dominio al archivo /etc/resolv.conf. Esta configuración permite resolver los nombres internos del dominio e interactuar de forma fiable con los distintos servicios de Active Directory, lo cual es una condición indispensable para continuar con la evaluación.

Una vez completado este paso, el auditor puede profundizar en su análisis comprobando la configuración del servicio DNS. En algunos casos, un error puede permitir una **transferencia de zona**, lo que ofrece una visibilidad casi completa de los registros disponibles y, por tanto, de la estructura interna del dominio. Aunque esta configuración incorrecta es poco frecuente en entornos debidamente protegidos, sigue siendo un ejemplo elocuente de lo que puede revelar un reconocimiento minucioso. La prueba se realiza fácilmente con la herramienta **dig**, por ejemplo, con el comando:

```
grc dig axfr <dominio> @<servidor_dns>
```

Para obtener todos los registros IPv4, se puede filtrar el resultado del comando anterior de la siguiente manera:

```
grc dig axfr <dominio> @<servidor_dns>| awk '/IN[[:space:]]+A/
{print $1, "->", $NF}'
```

2.1.3 Vulnerabilidades: Quick Compromise

Una vulnerabilidad es una debilidad o fallo en un sistema informático, una aplicación o una red, generalmente debido a un error de diseño, configuración o implementación. Numerosas organizaciones recopilan y publican estas vulnerabilidades: CERT, GitHub, CNVD y muchas otras. Para facilitar la centralización de esta información procedente de múltiples fuentes, la herramienta **Vulnerability Lookup** permite correlacionar rápidamente las vulnerabilidades, incluso cuando estas no tienen el mismo identificador. Su objetivo es simplificar la gestión del CVD (*Coordinated Vulnerability Disclosure*) y hacer más accesible el análisis de las vulnerabilidades procedentes de repositorios heterogéneos. En la siguiente dirección se puede consultar una lista reciente de vulnerabilidades procedentes de diferentes fuentes:
https://vulnerability.circl.lu/recent#cvelistv5

Entre todas estas fuentes, los **CVE** (*Common Vulnerabilities and Exposures*) son los identificadores más conocidos por el público en general y constituyen una referencia mundial para catalogar las fallas de seguridad. En algunos sitios web es posible realizar una búsqueda por producto de forma más intuitiva, por ejemplo, para **Windows 10**:
https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-32238/Microsoft-Windows-10.html

En esta fase de la auditoría, es fundamental catalogar las vulnerabilidades sin intentar explotarlas de inmediato. Existen varias herramientas que permiten buscar CVE y evaluar el nivel de riesgo asociado a los sistemas y servicios identificados. Entre las soluciones de código abierto se encuentran **Nuclei**, adecuada para la detección automatizada de vulnerabilidades en aplicaciones web, así como **GVM/OpenVAS**, que ofrece análisis completos de redes y aplicaciones. Soluciones comerciales como **Nessus**, **QualysGuard**, **Acunetix** o **Nexpose** ofrecen bases de datos que se actualizan periódicamente y capacidades de análisis exhaustivas.

© Editions ENI - All rights reserved

▶Para instalar GVM, ejecuta los siguientes comandos:

```
curl -f -O -L https://greenbone.github.io/docs/latest/_static/
docker-compose.yml
docker compose up -d
```

Este proyecto ilustra la creciente adopción de las tecnologías de contenerización para simplificar el despliegue de herramientas y aplicaciones en general, evitando los problemas de dependencias y preservando así la integridad del sistema anfitrión.

Existen numerosas herramientas que permiten probar y explotar las vulnerabilidades de los distintos sistemas y plataformas. Entre ellas, una de las más conocidas es el marco **Metasploit (MSF)**. Este marco integra un amplio catálogo de **exploits** (programas destinados a aprovechar una vulnerabilidad) y de **payloads**, entre los que se encuentra el famoso **Meterpreter**, que permite interactuar de forma avanzada con un sistema comprometido. Pero **Metasploit** no se limita a la explotación; también ofrece numerosos **módulos auxiliares** dedicados al reconocimiento y al inventario de servicios.

Por ejemplo, el módulo **auxiliary/scanner/smb/smb_version** permite escanear los servicios SMB de un host para identificar la versión y la firma del protocolo utilizado.

Para utilizar Metasploit y ejecutar el módulo **auxiliary/scanner/smb/smb_version**, puedes seguir estos pasos:

– Iniciar Metasploit: abre tu terminal y escribe **msfconsole** para iniciar la interfaz de línea de comandos de Metasploit.
– Buscar el módulo: utiliza el comando `search smb_version` para localizar el módulo específico que deseas utilizar.
– Consultar las opciones: una vez seleccionado el módulo con **use auxiliary/scanner/smb/smb_version**, escribe **show options** para mostrar los parámetros configurables, como **RHOSTS**, que especifica la dirección IP del objetivo.
– **Ejecutar el módulo**: tras configurar las opciones necesarias, utiliza el comando `run` para iniciar el escaneo.