Computer Assisted Audit Techniques - Ejemplos de uso

Demo: uso de la herramienta nmap

Introducción

Se trata de una herramienta que suele usarse para escanear y auditar una serie de *hosts* en una red o uno de ellos en particular. Para hacer esto realiza envíos de paquetes TCP / UDP / ICMP al objetivo y analiza sus respuestas para comparar contra su base de conocimiento y en función de la misma generar una respuesta al usuario.

Para usarla existen dos opciones, puede ser en forma local (instrucciones de instalación) o desde algún servicio *online* por ejemplo: acá y acá.

Se *recomienda* usar la herramienta con cuidado ya que existen reglas que pueden ser implementadas en ciertos dispositivos de red (routers por ejemplo) que ante la detección de un escaneo como el que realiza la herramienta lo consideran un ataque y podrían pasar la IP de origen a una lista negra bloqueando su acceso. En este sentido, antes de ejecutar un análisis así en un lugar externo se deberá consultar sobre estas restricciones a fin de evitar problemas.

Sintaxis básica

Si bien existen alternativas con una UI como Zenmap se va a usar el modo CLI de la herramienta que será posiblemente el escenario más común.

La forma general del comando es:

```
nmap [Tipo de escaneo] [Opciones] {especificación de objetivos}
```

Analizando por partes el comando se puede ir trabajando de la siguiente manera:

- Para descubrimiento de hosts:
    - Si es una IP en particular: `nmap 192.168.0.50`.
    - Si es un rango de IPs: `nmap 192.168.0.0/24` (usando notación CIDR) o sino especificando el rango manualmente con `nmap 192.168.0.1-254`.
    - Puede usarse directo una URL: `nmap www.scanme.org`
- Para identificar a los hosts que se encuentran online:
    - Se puede usar el modificador *-PS* que verifica a través del envío de un paquete TCP SYN al puerto 80. Comando: `nmap 192.168.01.1-20 -PS`
    - Se puede usar el modificador *-sL* para solo listar aquellos hosts encendidos (puede dar resultados diferentes al anterior). Comando: `nmap 192.168.0.1-20 -sL`

    - En caso de que esté bloqueado poder realizar un ping a los hosts se puede usar la opción *-PN*. Comando: `nmap 192.168.0.1-20 -PN`

- Para evaluar un subconjunto de puertos:

    - Se puede optar por analizar solo aquellos con mayor utilización: `nmap 192.168.0.20 --top-ports 100` (en este caso los 100 más comunes)
    - Si se requiere analizar un puerto en especial: `nmap 192.168.0.1 -p 80`
    - Un subrango específico: `nmap 192.168.0.1 -p 80-100`
    - Un conjunto específico: `nmap 192.168.0.1 -p 80,443,22,23,25,145,53`

- Para especificar el tipo de configuración del escaneo se pueden usar (entre otros):

    - *-sS* hace un análisis de puertos enviando paquetes TCP SYN (no completa la conexión, pero necesita permisos de root / administrador para ejecutarse)
    - *-sT* hace un análisis de puertos enviando paquetes TCP CONNECT (intenta completar la conexión pudiendo dejar un registro en el log del host analizado, no necesita permisos de root / administrador para ejecutarse)
    - *-O* para intentar obtener el tipo de sistema operativo que se está ejecutando en el host (esta operación incrementa el tiempo del análisis). Comando: `nmap -O 192.168.0.8`
    - *-sV* para obtener (en caso de que sea posible) la versión del servicio que se está ejecutando en cada puerto analizado. Comando: `nmap -sV 192.168.0.8`
    - *-A* para hacer una detección más agresiva, sería equivalente a -O -sV -sC (que ejecuta los scripts integrados a la herramienta por defecto para la detección) y -traceroute (que trata de trazar la ruta al host). Comando: `nmap -A 192.168.0.8`

A partir de estas variantes se puede construir un conjunto de versiones del comando que permitan analizar diferentes hosts según la importancia que pueden tener para la auditoría que se esté realizando.

Por ejemplo:

- Obtener todos los puertos de un servidor junto a las versiones de servicio que estén ejecutando.
- Intentar detectar de forma rudimentaria la topología de la red.
- Detectar puertos abiertos en las terminales de usuario de una subred.
- Entre otros.

Referencias

Fuente 1
Fuente 2
Fuente 3