Universidad del Istmo

Campus Tehuantepec

Materia: Redes de Computadoras II

Docente: Ing. Carlos Mijangos Jiménez

Alumna: Valery Rodríguez Trejo

Carrera: Ingeniería en Computación

Semestre: Séptimo semestre

Actividad 1

Índice

1 Introducción

1.1 Descripción de conceptos

1.1.1 Sandbox

Entorno aislado y controlado que permite realizar pruebas, escaneos y análisis sin poner en riesgo la red real. Es ideal para prácticas de ciberseguridad, ya que evita impactos en sistemas de producción.

1.1.2 Nmap

Herramienta de escaneo utilizada para descubrir hosts activos, identificar puertos abiertos, servicios ejecutándose y posibles vulnerabilidades dentro de una red. Es una de las herramientas más utilizadas en auditorías de seguridad y pruebas de penetración.

1.1.3 Wireshark

Analizador de tráfico de red que permite capturar, visualizar y estudiar paquetes en tiempo real. Resulta útil para identificar comportamientos sospechosos, analizar protocolos y comprender la actividad generada durante un escaneo.

1.1.4 Máquina virtual

Software que permite emular un sistema operativo dentro de otro, creando un entorno independiente donde se pueden realizar pruebas sin afectar el equipo físico. Facilita la creación de sandbox o laboratorios de práctica.

1.1.5 Escaneos seguros y evasión de detección

Técnicas aplicadas para reducir la probabilidad de que un escaneo sea detectado por sistemas de defensa (IDS/IPS). Entre estas técnicas se encuentran el uso de SYN Scan (escaneo sigiloso), el control del ritmo de envío de paquetes, la fragmentación de paquetes, y la aleatorización de tiempos.

1.1.6 Relación entre ataque y defensa

Nmap se utiliza desde la perspectiva ofensiva para descubrir debilidades en un sistema, mientras que Wireshark permite monitorear y detectar estos escaneos desde una perspectiva defensiva. En conjunto ofrecen una visión integral del proceso de auditoría de seguridad.

1.2 Detalle de herramientas

En esta práctica se utilizaron dos herramientas principales:

Nmap

Se empleó para realizar diferentes tipos de escaneos a una máquina virtual objetivo. Con esta herramienta se identificaron puertos abiertos, servicios activos, el sistema operativo probable y otros datos relevantes para una auditoría de seguridad.

Wireshark

Se utilizó para monitorear el tráfico de red durante los escaneos efectuados con Nmap. Esto permitió observar cómo viajan los paquetes, identificar patrones propios de cada tipo de escaneo y reconocer indicios que un administrador podría utilizar para detectar un ataque.

1.3 Requisitos

Para esta práctica, además de contar con las herramientas Nmap y Wireshark instaladas en la máquina anfitriona (Windows), fue necesario disponer de una máquina virtual que funcionara como entorno de pruebas o "víctima". En este caso se utilizó Oracle VirtualBox con el sistema operativo Elementary OS.

Tanto la laptop anfitriona como la máquina virtual debían estar conectadas a la misma red, lo que permite la comunicación entre ambas y hace posible la ejecución de los escaneos. Para ello, fue indispensable configurar adecuadamente la red en adaptador puente de la máquina virtual, este modo de red hace accesible para Nmap y observable desde Wireshark.

Esta configuración garantizó que la máquina virtual pudiera ser detectada, escaneada y monitoreada sin afectar la red real, manteniendo un entorno seguro y controlado.

2 Monitoreo y escaneo de vulnerabilidades con las herramientas nmap y wireshark

2.1 Escaneos con Nmap

Primero verifico cual es la dirección IP de mi maquina virtual que en este caso es la víctima.

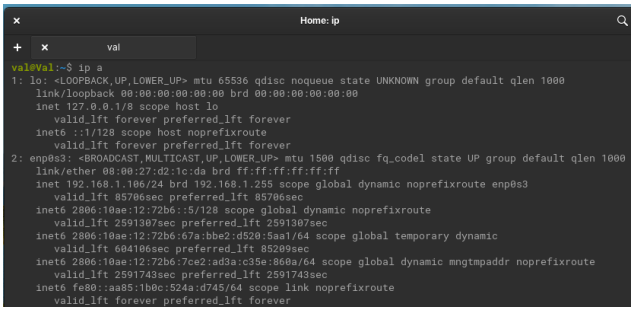

Figura 1: Obtención de la dirección IP de la máquina víctima

Una vez que la obtengo, hago un ping desde la máquina atacante para verificar la conectividad entre ambas máquinas.

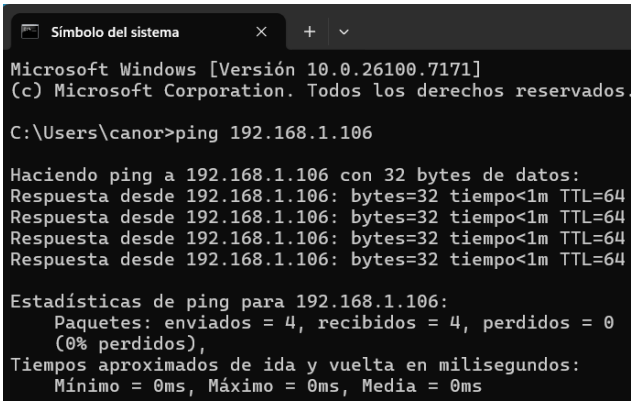

Figura 2: Escaneo de la máquina atacante a la víctima

Y en esa misma máquina realizo un escaneo. Sin embargo, debido a que mi laptop ya no soporta más carga (de hecho, ya ni siquiera me permite compilar la máquina virtual) únicamente podré incluir teoría al respecto.

Como mencioné anteriormente, el siguiente paso consiste en realizar un escaneo con Nmap para identificar qué servicios están activos en la máquina víctima, qué puertos abiertos tienen en común y cuál es el estado de cada uno.

Para comenzar, se ejecuta un escaneo básico:

- Comando: nmap 192.168.1.106

Posteriormente, se realiza un escaneo sigiloso, el cual permite evadir en cierta medida firewalls o sistemas de detección de intrusos (IDS), ya que utiliza el método SYN para no establecer una conexión completa con los puertos.

- Comando: nmap -sS 192.168.56.10

Después, se lleva a cabo un escaneo enfocado en la detección de versiones, lo que permite identificar el software, la versión exacta del servicio y, con ello, posibles vulnerabilidades públicas asociadas.

- Comando: nmap -sV 192.168.56.10

A continuación, se ejecuta un escaneo agresivo, que proporciona información más detallada como la detección del sistema operativo, ejecución de traceroute y el uso de scripts básicos del motor NSE.

- Comando: nmap -A 192.168.56.10

Finalmente, se utiliza el conjunto de scripts orientados a la detección de vulnerabilidades con el fin de identificar servicios desactualizados, configuraciones inseguras y CVEs conocidas que puedan representar un riesgo.

- Comando: nmap –script vuln 192.168.56.10

2.2 Monitoreo con Wireshark

En la máquina víctima (y también posible en la atacante), se ejecuta Wireshark seleccionando la interfaz de red que usa la VM.

Durante el escaneo de Nmap se observa en tiempo real:

- Paquetes SYN enviados repetidamente a distintos puertos
- Paquetes TCP RST
- Tráfico ICMP del ping inicial
- Se detectaron [mencionar servicios específicos] ejecutándose
- Distintos patrones de escaneo, según el tipo ejecutado

Esto demuestra cómo un administrador puede detectar actividad sospechosa, incluso si el escaneo es sigiloso.

Los filtros usados en Wireshark fueron:

- Filtrar tráfico del atacante: ip.addr == 192.168.1.100
- Ver solo tráfico de escaneo: tcp.flags.syn == 1
- Filtrar paquetes ICMP: icmp

3 Conclusiones

3.1 Resultados obtenidos

- Se identificaron x puertos abiertos en la máquina objetivo
- El escaneo SYN demostró ser menos detectable que el escaneo TCP Connect
- Wireshark permitió visualizar claramente los diferentes tipos de tráfico generado
- Se detectaron [mencionar servicios específicos] ejecutándose
- El uso de timing (-T2) redujo significativamente la posibilidad de detección

3.2 Recomendaciones

3.2.1 Desde la perspectiva ofensiva

- Utilizar escaneos SYN en lugar de TCP Connect
- Emplear timing lento (-T1 o -T2) para evadir IDS/IPS
- Fragmentar paquetes cuando sea posible
- Aleatorizar el orden de escaneo de puertos

3.2.2 Desde la perspectiva defensiva

- Implementar monitoreo continuo con herramientas como Wireshark o Zeek
- Configurar alertas para patrones de escaneo (múltiples SYN a diferentes puertos)
- Mantener un inventario actualizado de servicios expuestos
- Cerrar puertos innecesarios y actualizar servicios vulnerables
- Implementar sistemas IDS/IPS que detecten escaneos lentos

3.3 Conclusión general

La práctica demostró la importancia de conocer tanto las herramientas de ataque como las de defensa. Nmap es una herramienta poderosa para auditorías de seguridad, pero su uso puede ser detectado si no se emplean técnicas de evasión. Por otro lado, Wireshark resulta fundamental para el análisis de tráfico y la detección de actividades sospechosas. Ambas herramientas son complementarias y esenciales en cualquier proceso de auditoría de seguridad.