Laboratorio 2: Evaluación de Vulnerabilidades en una Red

Enunciado para el Campista

Objetivo del laboratorio:
Desarrollar habilidades para identificar vulnerabilidades en una red mediante el uso de herramientas básicas como **Nmap** y **Zenmap**, analizar servicios expuestos, buscar vulnerabilidades conocidas y generar un informe detallado con hallazgos y recomendaciones.

Herramientas necesarias

1. **Nmap:** Herramienta de línea de comandos para el escaneo de red.
2. **Zenmap:** Interfaz gráfica para Nmap (opcional, pero recomendada para principiantes).
3. **Máquina virtual objetivo:** Un sistema operativo configurado con servicios básicos activos (servidor web y FTP).
4. **Documentación de vulnerabilidades:** Uso de bases de datos públicas como **CVE Details** o **Exploit-DB**.

Configuraciones previas al laboratorio

1. Instalación de herramientas

- Descarga e instala **Nmap** y **Zenmap** desde nmap.org.

  Asegúrate de que estén correctamente instalados ejecutando:
  ```
  nmap --version
  ```

- Si se muestran la versión y los detalles, Nmap está listo para usarse.

2. Configuración de la máquina virtual objetivo

1. Descargar imagen de máquina virtual preconfigurada: Utiliza una imagen de Ubuntu Server o Windows Server.
2. Configurar servicios activos:
   - En Ubuntu Server:

Instala y habilita Apache con los comandos:
sudo apt update
sudo apt install apache2
sudo systemctl start apache2

luego:

Instala y habilita un servidor FTP como **vsftpd**:
sudo apt install vsftpd
sudo systemctl start vsftpd

- **En Windows Server:** Activa IIS desde el Panel de Control y habilita el servicio FTP en la misma consola.

3. Configura el adaptador de red de la máquina virtual en modo **Red Interna** o **NAT**, asegurándote de que la máquina del analista (tu equipo) esté en la misma red.

3. Obtener la IP de la máquina objetivo

- En Linux: Ejecuta `ifconfig` o `ip a` para ver la dirección IP.
- En Windows: Ejecuta `ipconfig` en la línea de comandos.

  Anota la dirección IP, ya que será necesaria para el escaneo.

Instrucciones Paso a Paso

Parte 1: Escaneo de red con Nmap

1. **Descubre dispositivos en la red:**
   - Abre una terminal o Zenmap en tu máquina.

     Usa el siguiente comando para identificar dispositivos conectados al rango de IP:
     nmap -sn 192.168.1.0/24

   - Observa los dispositivos detectados y anota la IP de la máquina virtual objetivo.
2. **Escaneo de puertos abiertos en la máquina objetivo:**
   - Realiza un escaneo rápido para detectar puertos abiertos:
     nmap -sS <IP_objetivo>

- El indicador `-sS` realiza un escaneo TCP SYN rápido.
- Documenta los puertos abiertos y los servicios que los ocupan (puerto 80 para HTTP, puerto 21 para FTP, etc.).

3. **Escaneo detallado de servicios y versiones:**
   - Realiza un escaneo para obtener más información sobre los servicios y sus versiones:
     nmap -sV -p- <IP_objetivo>
     - `-sV` permite detectar versiones de los servicios.
     - `-p-` escanea todos los puertos (0-65535).
4. **Usando Zenmap:**
   - Abre Zenmap, selecciona el perfil **"Escaneo intenso"** e introduce la IP de la máquina objetivo.
   - Genera y guarda un reporte en formato HTML.

Parte 2: Análisis de servicios expuestos

1. Revisa los resultados del escaneo y localiza:
   - Puertos abiertos.
   - Servicios activos (HTTP, FTP, etc.).
   - Versiones detectadas (por ejemplo, Apache 2.4.49).
2. Analiza posibles implicaciones de cada servicio:
   - ¿Por qué podría ser vulnerable?
   - ¿Es necesario que este puerto esté abierto?

Parte 3: Identificación de vulnerabilidades conocidas

1. Usa bases de datos en línea como:
   - **CVE Details**: https://www.cvedetails.com.
   - **Exploit-DB**: https://www.exploit-db.com.
2. Busca vulnerabilidades para las versiones de servicios detectados.
   - Ejemplo: Si el escaneo detectó "Apache 2.4.49", busca CVEs asociados con esta versión.
3. Documenta:
   - **Identificador de la vulnerabilidad** (CVE-ID).
   - **Descripción del problema**.
   - **Impacto** (confidencialidad, integridad, disponibilidad).

Parte 4: Generación de informes de vulnerabilidades

1. El informe debe incluir:
    - **Resumen del escaneo:**
        - Dispositivos encontrados.
        - Puertos abiertos.
        - Servicios detectados y versiones.
    - **Vulnerabilidades identificadas:** Detalle de cada vulnerabilidad, su CVE-ID y recomendaciones.
    - **Capturas de pantalla:** Evidencia de los escaneos realizados (Nmap/Zenmap).
2. Sugerencias de mitigación:
    - Actualizar servicios a versiones más seguras.
    - Cerrar puertos innecesarios.

Resultados de aprendizaje

Criterios:

1. **Configuración del entorno:** Configuración de herramientas y máquinas virtuales correctamente.
2. **Escaneo de red:** Habilidad para realizar escaneos básicos y avanzados con Nmap/Zenmap.
3. **Análisis de resultados:** Capacidad para interpretar servicios detectados y buscar vulnerabilidades.
4. **Informe:** Claridad, detalle y organización del informe generado.

Este laboratorio te brindará las habilidades iniciales para evaluar vulnerabilidades en entornos controlados, una de las tareas fundamentales en ciberseguridad. ¡Buena suerte!