LABORATORIO

ENUMERACIÓN ACTIVA DEL OBJETIVO

ANTES DE COMENZAR

Antes de comenzar con las tareas de enumeración del objetivo, deberemos crear un entorno de pruebas para poder hacer las prácticas. Un entorno de prueba proporciona un **lugar seguro** para realizar pruebas de penetración e investigaciones de seguridad. Para construir este entorno necesitaremos las siguientes herramientas:

- **Un software de virtualización:** el cual utilizaremos para crear y correr las máquinas virtuales donde haremos las pruebas. Podemos utilizar vmware Player (free), vmware Workstation (requiere licencia) o VirtualBox (free).

- **Una máquina atacante:** podemos utilizar Kali o ParrotOS. Ambas, son distribuciones de linux, basadas en Debian, específicamente creadas para ser utilizadas para efectuar tareas de seguridad.

- **Una máquina víctima:** utilizaremos **Metasploitable2**, que es una máquina virtual linux intencionalmente vulnerable y especialmente diseñada para realizar capacitaciones en seguridad, probar herramientas de seguridad y practicar técnicas comunes de pruebas de penetración y explotación. Esta máquina virtual (VM) es compatible con **VMWare**, **VirtualBox**.

NOTA: Nunca exponga a la máquina virtual **metasploitable2** a una red que no sea de confianza y mucho menos a internet. En su defecto se sugiere utilizar únicamente los modos de red `NAT` o `HOST-ONLY`.

PERO… ¿CÓMO INSTALO TODO ESTO?

Si tenés dudas de como instalar y configurar el entorno recordá que google te puede ayudar. Existen múltiples artículos y videos en línea donde podés investigar el paso a paso de como hacerlo.

El primer paso para convertirte en un verdadero atacante es no darte por vencido ante la adversidad y ser muy curioso. ¡Buena suerte!

ENUMERACIÓN ACTIVA

INTRODUCCIÓN

Para poder efectuar las tareas de enumeración activa del objetivo necesitaremos:

1. La máquina víctima Metasploitable2 configurada encendida.

2. La máquina atacante (Kali o ParrotOS) configurada y encendida.

3. La herramienta **nmap** para efectuar el escaneo de puertos y enumeración de servicios.

4. **Nessus** u **OpenVAS** instalado y configurado como para efectuar un escaneo.

5. Instalar **metasploit** para efectuar las explotaciones de las vulnerabilidades.

VALIDAR LA DIRECCIÓN IP DE METASPLOITABLE2

Antes de comenzar deberemos validar que ambas máquinas virtuales se encuentran dentro de la misma red. Asimismo necesitaremos conocer cuál es la dirección ip de la máquina metasploitable. Para ellos deberemos:

1. Iniciar sesión en metasploitable2 utilizando las credenciales default: Usuario **`msfadmin`** y contraseña **`msfadmin`**

2. Una vez dentro del sistema, ejecutar el comando **`ifconfig`** como se indica a continuación:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:de:35:be
          inet addr:172.16.214.141  Bcast:172.16.214.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fede:35be/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4251 (4.1 KB)  TX bytes:11121 (10.8 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:118 errors:0 dropped:0 overruns:0 frame:0
          TX packets:118 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31841 (31.0 KB)  TX bytes:31841 (31.0 KB)
```

Ahora sabemos que la dirección IP de metasploitable2 es la **`172.16.214.141`**

Utilizaremos esta dirección IP como objetivo de nuestros escaneos de puertos, de servicios y de vulnerabilidades.

NOTA: Tu dirección IP probablemente sea diferente. No te preocupes, no tiene que ser la misma. Lo importante es que esté en el mismo rango de red que tu máquina atacante y que se vean entre sí.

LISTADO DE LINKS ÚTILES

A continuación se listan una serie de links útiles que nos ayudarán a resolver problemas y/o aprender como hacer algunas tareas en las herramientas que tenemos que utilizar.

- Nessus Command Line Reference: donde encontraremos cómo actualizar el sistema Nessus y gestionar usuarios, entre otros.
- Metasploit Unleashed: un curso de metasploit completo.
- Nmap: el libro oficial de nmap.

TAREAS

Una vez que tenemos configurado y corriendo nuestro entorno se pide:

1. Validar que la dirección IP de metasploitable2 responde.

2. Utilizar nmap para:
    a. Realizar un escaneo `TCP SYN` de todos los puertos.
    b. Realizar un fingerprint del sistema operativo.
    c. Efectuar una enumeración de todos los puertos que se encuentren abiertos.

3. Escanear vulnerabilidades de forma completa con Nessus u OpenVAS.

4. Explotar todas las vulnerabilidades que puedas utilizando las técnicas y herramientas vistas en clase. (metasploit, exploit-db, google, etc.)

5. Generar un reporte completo (con al menos 10 vulnerabilidades detalladas) utilizando el template.