EJERCICIOS INTRODUCCIÓN A LA ELEVACIÓN DE PRIVILEGIOS Y TRANSFERENCIA DE FICHEROS

Prerrequisitos

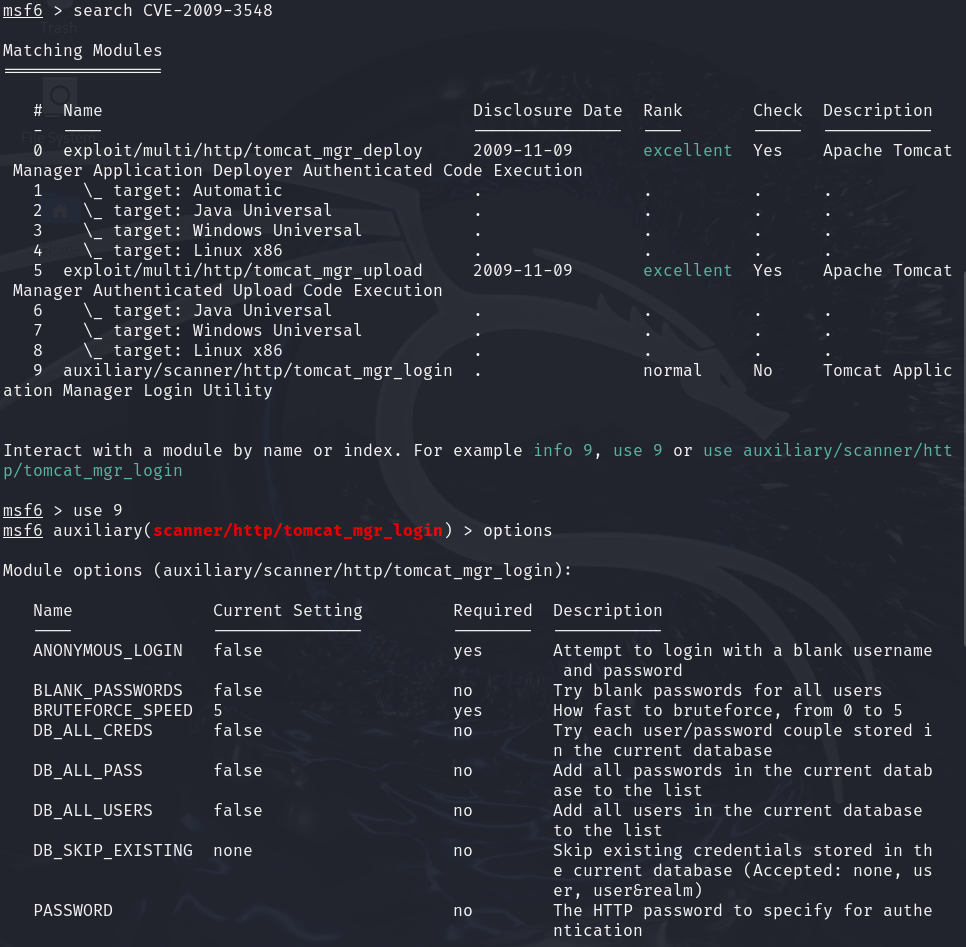
Kali Linux

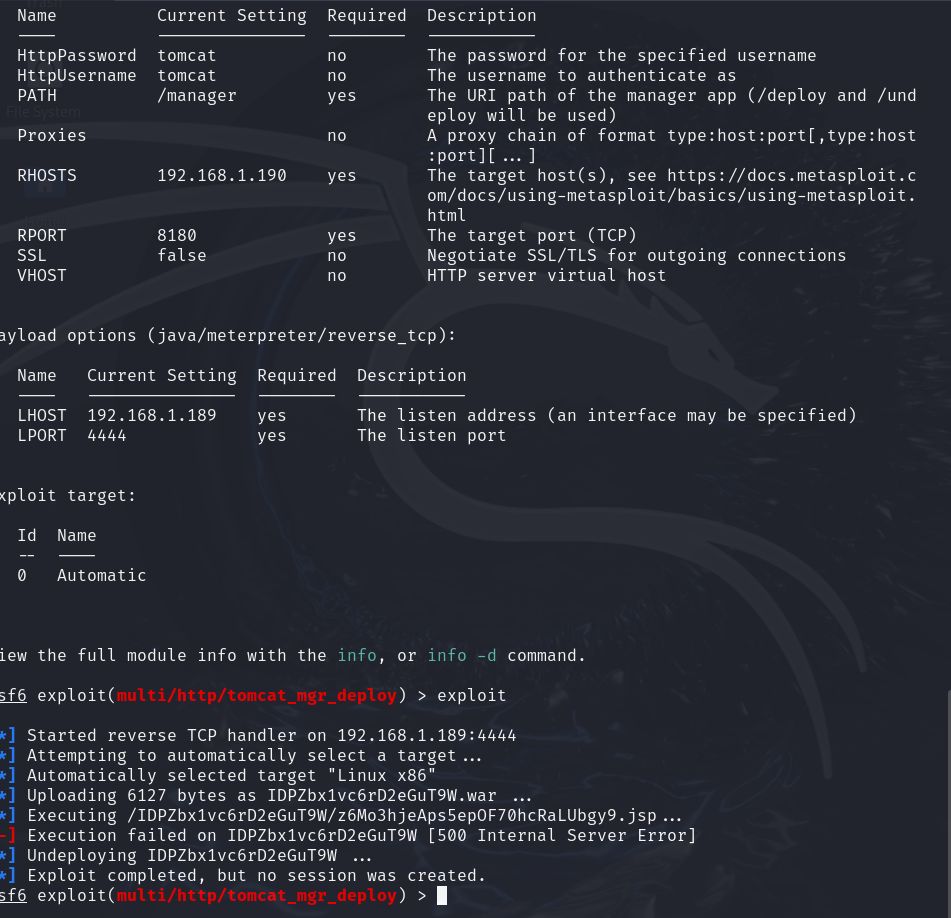
Metasploitable2

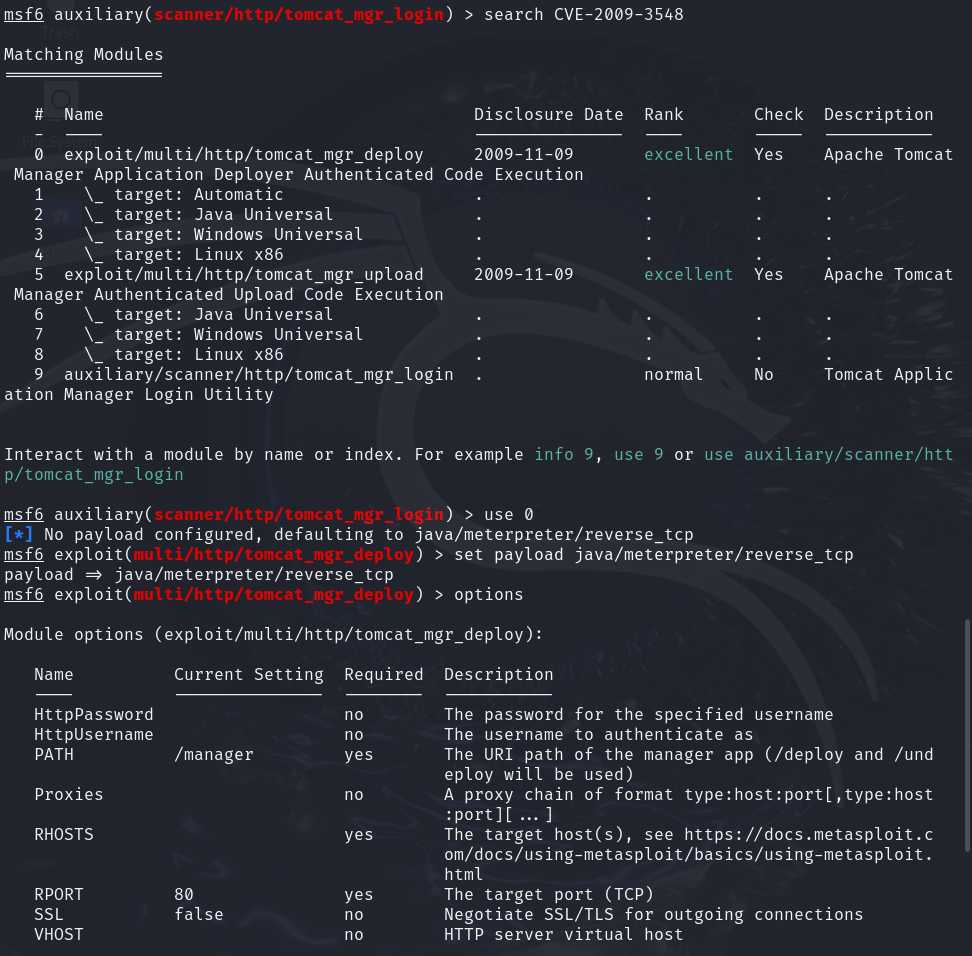
Windowsploitable LPE

Ejercicio 1 - Metasploit

Explotación de la vulnerabilidad CVE-2009-3548 para acceso con usuario limitado.







NO SE HA PODIDO CREAR LA SESION DE METERPRETER

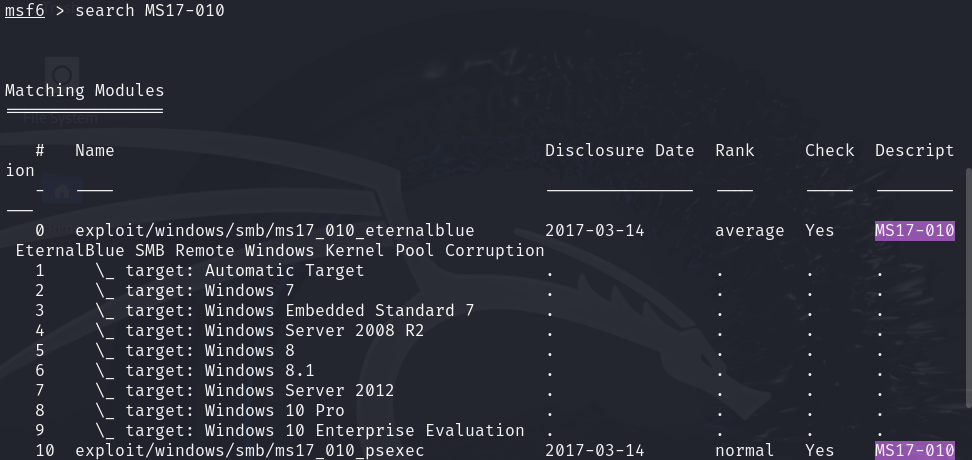
Enumeración básica y recopilación de información del sistema utilizando comandos y módulos de metasploit.

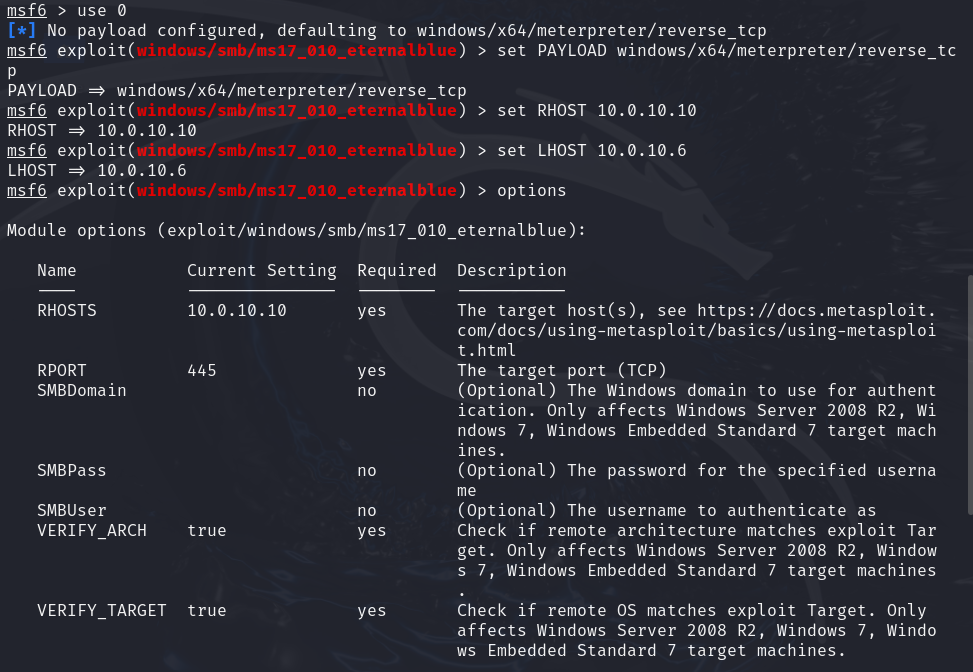
Transferencia al sistema utilizando comando upload de meterpreter del script linux-exploit-suggester-2.pl para recopilar posibles vulnerabilidades locales. Explotar alguna de las vulnerabilidades locales recopiladas para conseguir elevar privilegios. De no tener éxito, utilizar el módulo de post-explotación suggester para recopilar otros exploits de elevación de privilegios.

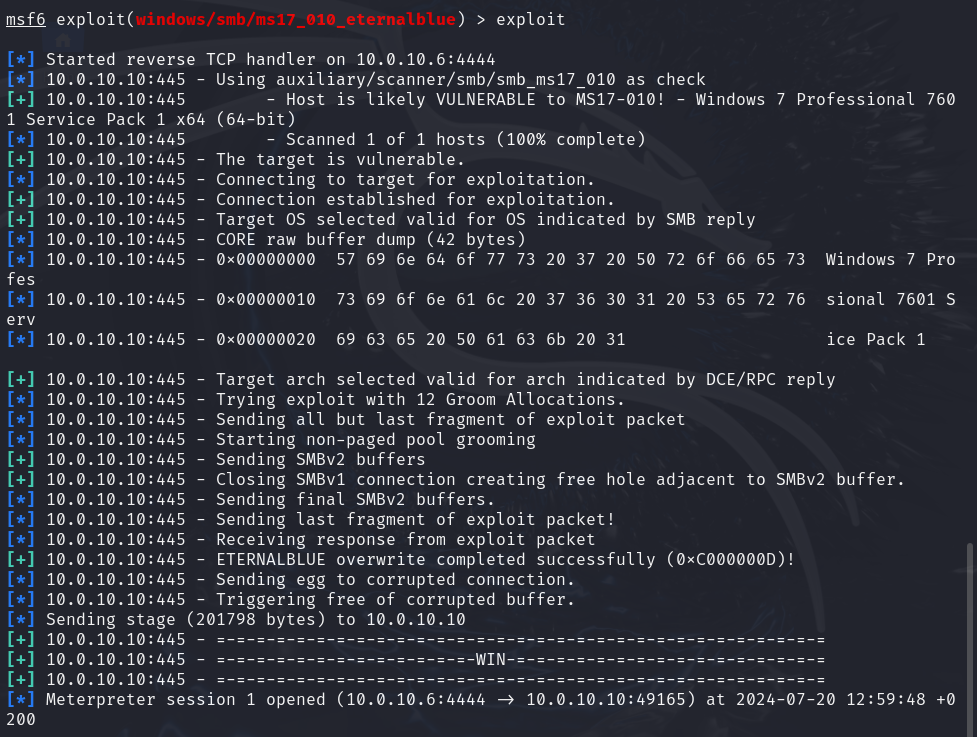
Conseguir meterpreter con usuario privilegiado.

Ejercicio 2 - Metasploit y Netcat

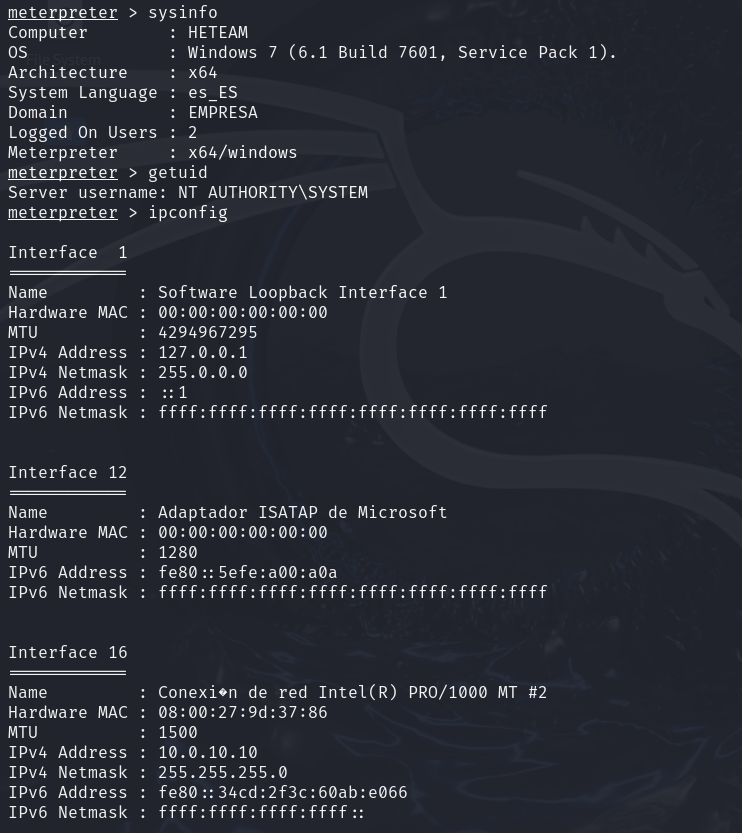
Explotación de la vulnerabilidad del boletín MS17-010 para acceso con usuario privilegiado.



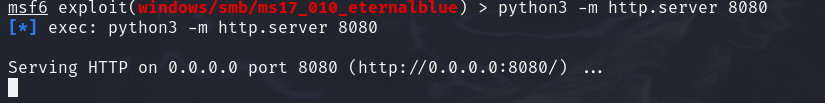


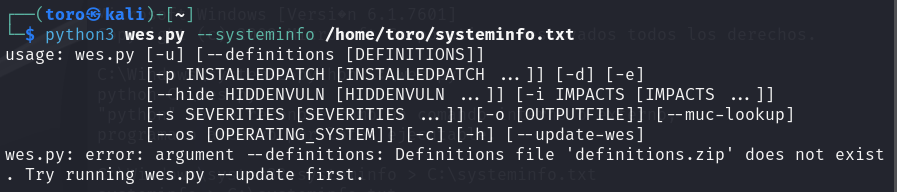


Enumeración básica y recopilación de información del sistema utilizando comandos y módulos de metasploit.



Transferencia al sistema utilizando netcat del script wes.py para recopilar posibles vulnerabilidades locales. En caso de error en la ejecución del script descargar con el comando download de meterpreter el archivo systeminfo.txt y ejecutar wes.py en Kali Linux.





NO SE HA PODIDO EXECUTAR EL WES.PY

Explotar alguna de las vulnerabilidades locales recopiladas. De no tener éxito, utilizar el módulo de post-explotación suggester para recopilar otros exploits de elevación de privilegios.

Probar exploit de elevación de privilegios.