1 ASIX

**MÒDUL 16: CIBERSEGURETAT I HACKING ÈTIC**

ACTIVITAT 1.9: Explotació bàsica

línea horizontal

# 



**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Sergi Andrés

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

**ÍNDEX**

[**Exercici 1: Explotació bàsica amb Netcat (Bind Shell)**](#_eztcwy3l3plv) **3**

[**Exercici 2: Explotació amb Reverse Shell a través de Netcat**](#_r1cqv2ki88ce) **5**

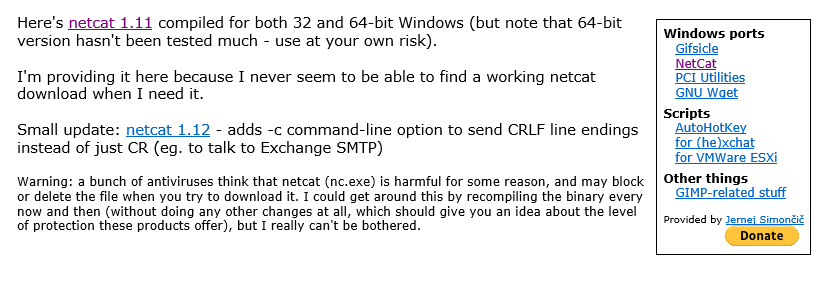
[**Exercici 3: Explotar una vulnerabilitat amb Metasploit**](#_5wo46bslrrxr) **7**

[**Exercici 4: Meterpreter**](#_d04tdh4dygdp) **14**

[**Exercici 5: Explotar altres vulnerabilitats**](#_upqjy1ye822g) **18**

# Exercici 1: Explotació bàsica amb Netcat (Bind Shell)

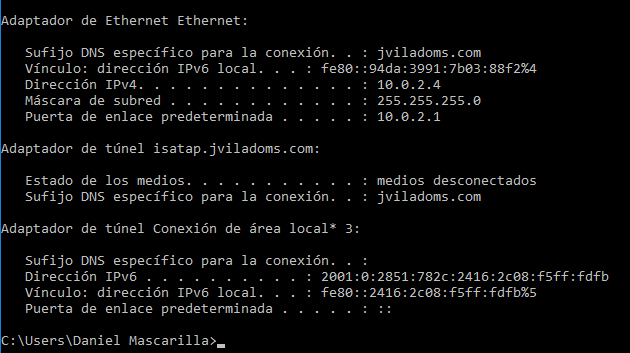
Descarregarem netcat:



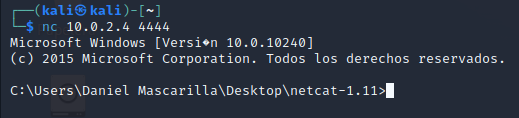
Obrirem el cmd dins de la màquina Windows 10 i executarem la següent comanda (amb netcat executat):



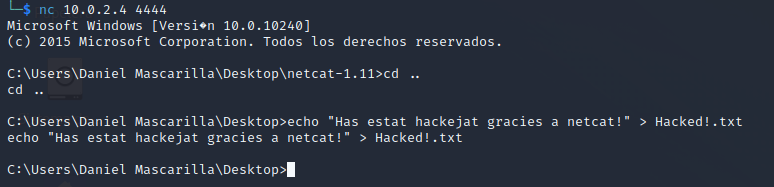
Agafarem la ip de la màquina win10:



Ara anirem al kali Linux i executarem un nc:



Ara posarem un missatge amb echo i el guardarem al escriptori:



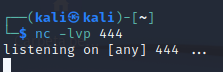
Anirem al windows 10 i mirarem el escriptori:



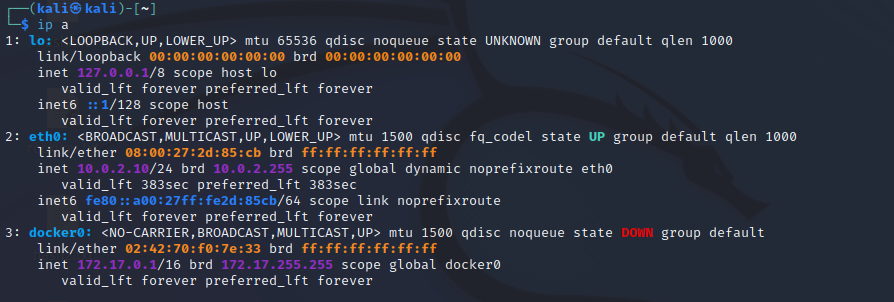


# Exercici 2: Explotació amb Reverse Shell a través de Netcat

Desde el Kali Linux executarem la següent comanda:

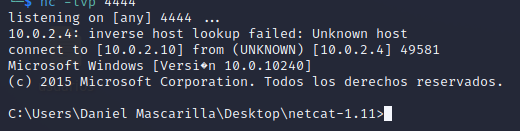


Agafarem la ip del Kali:



Ara des del Windows 10 executarem això:





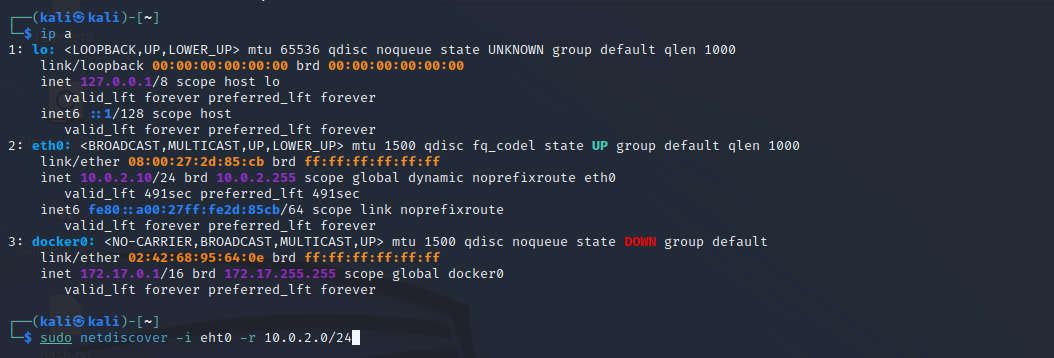
Ara farem el mateix que l’exercici anterior per comprovar:

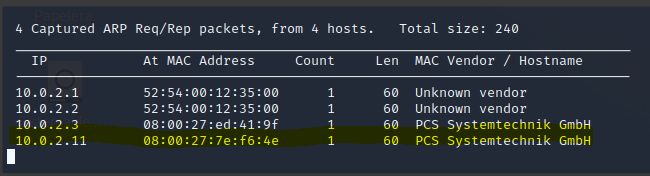




# Exercici 3: Explotar una vulnerabilitat amb Metasploit

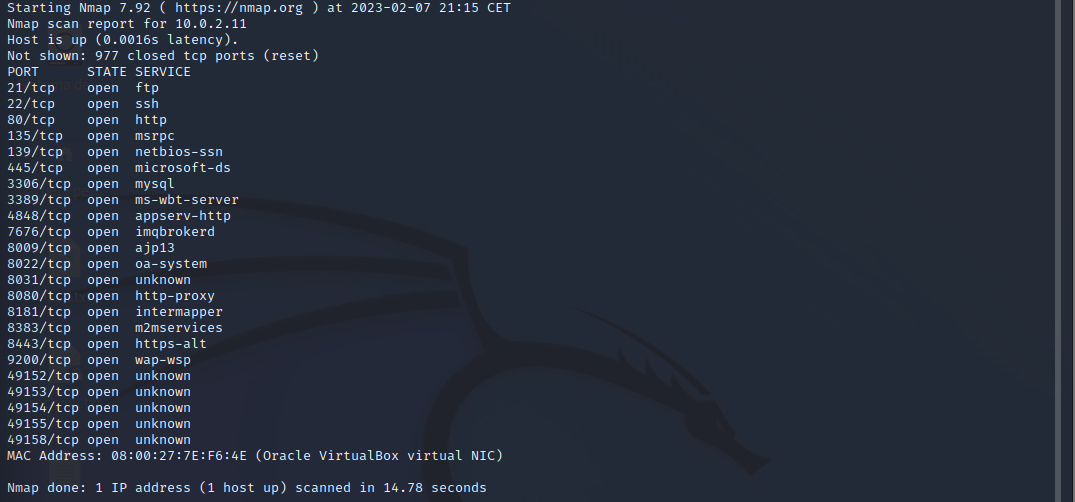
Descobrirem la ip de Metasploit:



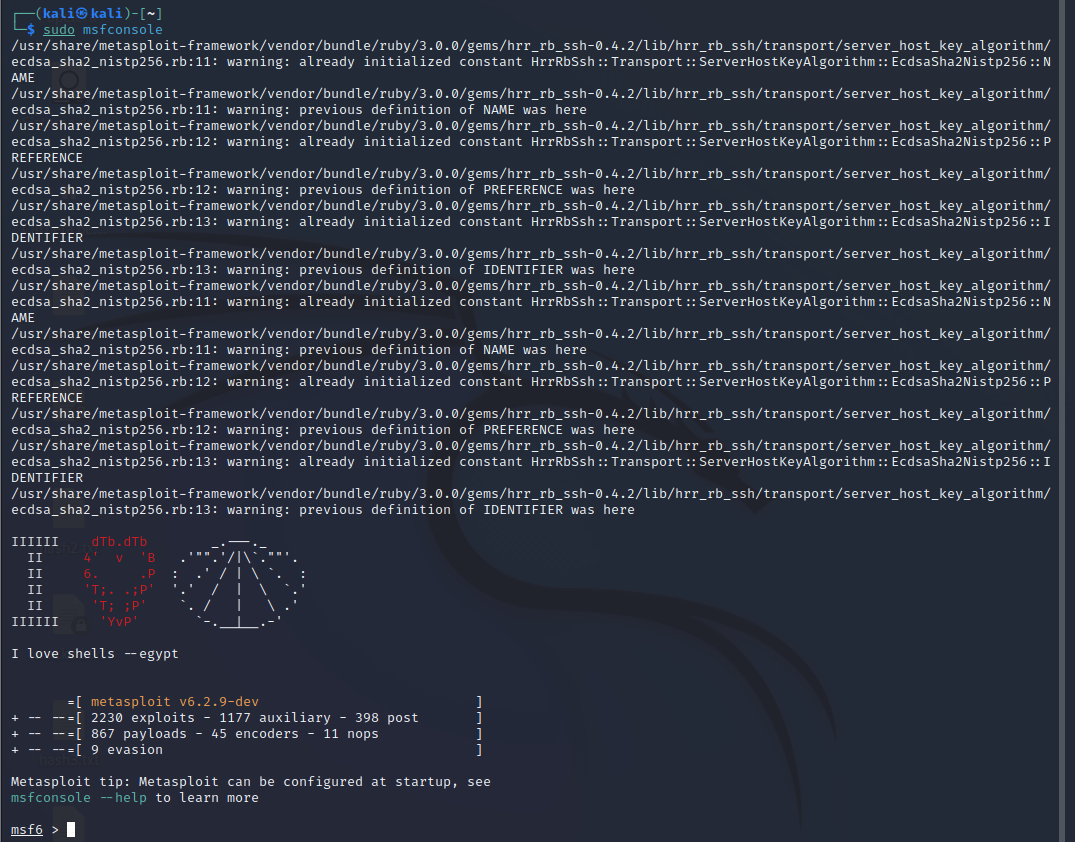


Un cop trobada farem un nmap de la màquina:



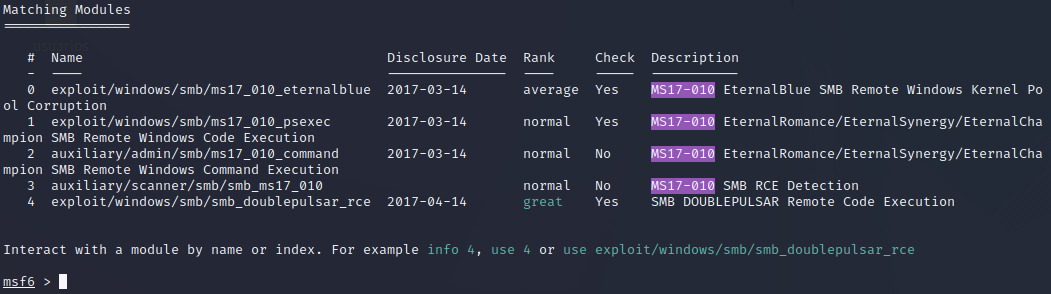


Ara executarem la següent comanda:



Dins executarem això:





Per buscar més info sobre EternalBlue executarem això:



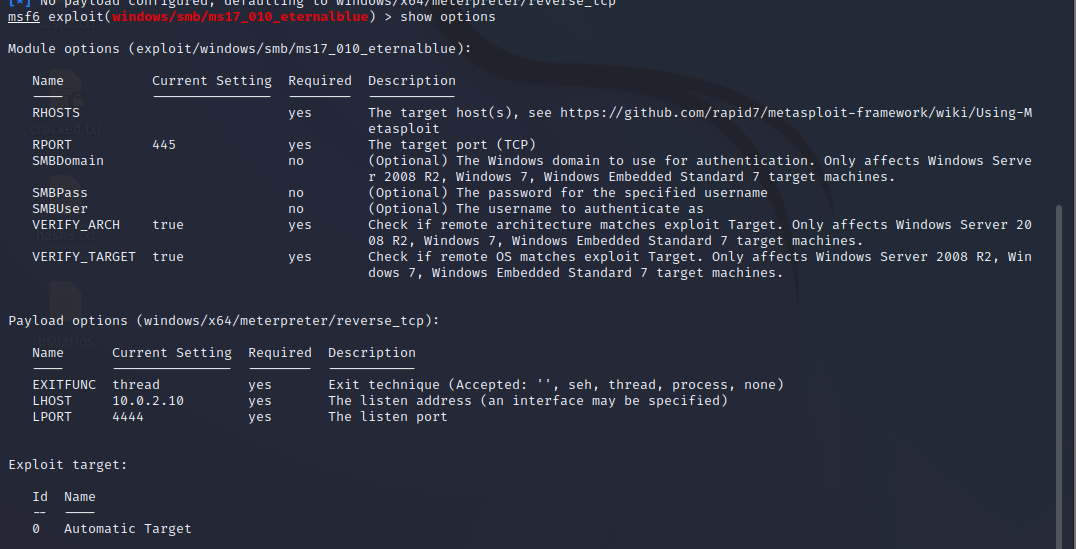


Ara carregarem el sploit amb la següent comanda:





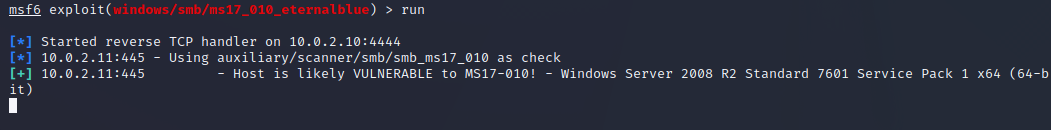
Ara farem un show options

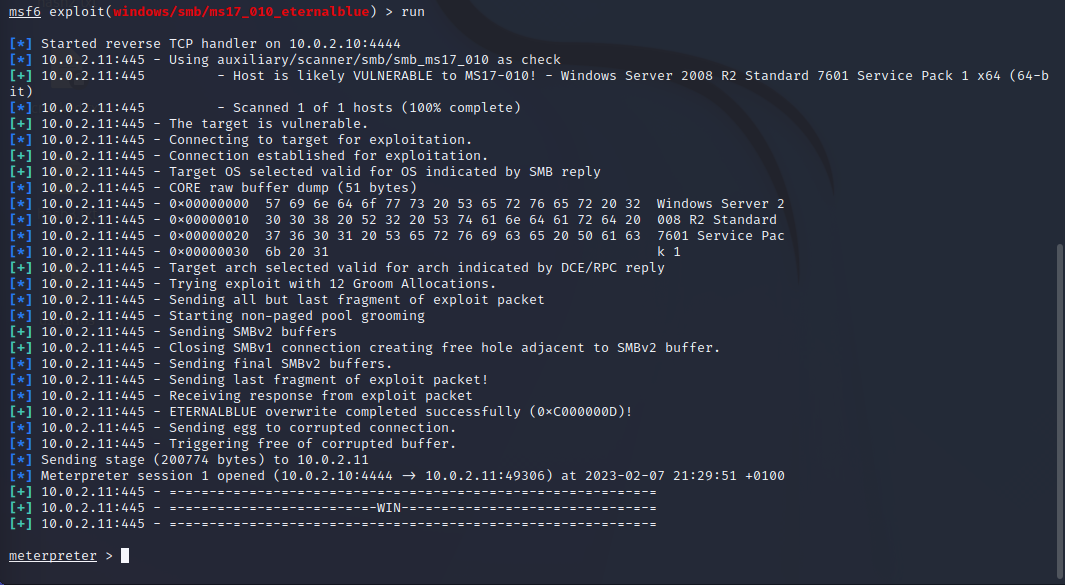


Seguidament executarem la següent comanda:

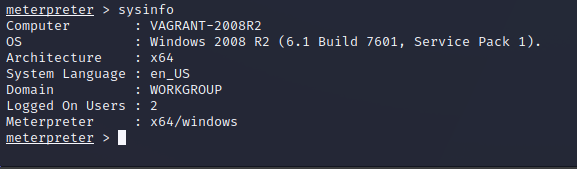


Executarem un run

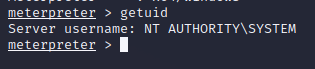




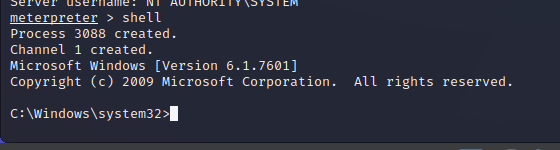
Haurem entrat a meterpreter. Ara executarem un sysinfo



Ara farem un getuid:

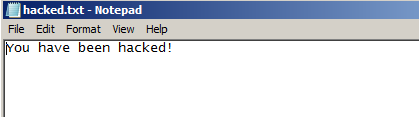


Ara si executem shell podrem entrar a la shell de vagrant:



Farem un echo i guardarem el echo en un document al escriptori.





S’ha completat correctament.

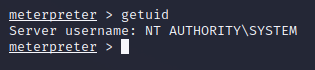
# 

# Exercici 4: Meterpreter

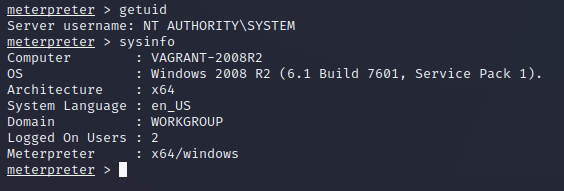
Dins del meterpreter haurem de fer un help.



Seguidament farem un getuid:



Farem un sysinfo:



Ara farem un getwd:



Després un getlwd:

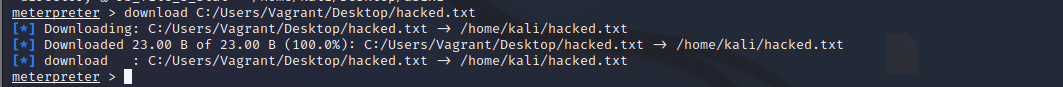


Ara farem aquesta comanda:

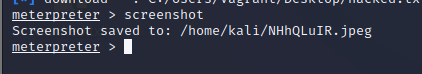




Ara descarregarem l’arxiu hacked.txt del meta:

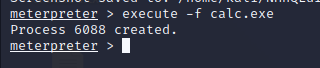


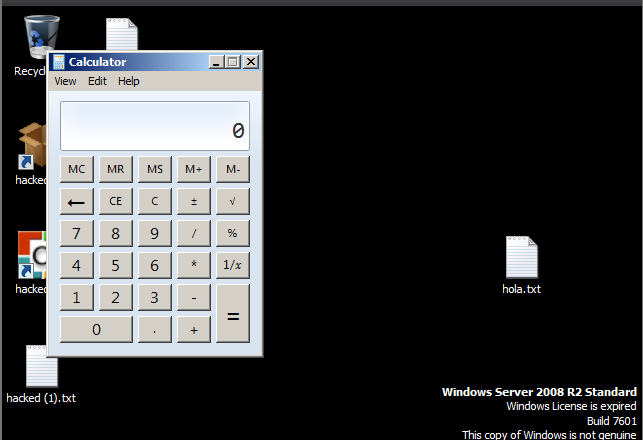
Ara farem una captura del que s’esta fent ara mateix en la màquina meta:



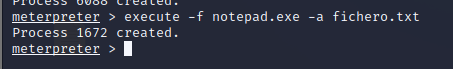


Seguidament obrirem la calculadora a distància:





També crearem un fitxer a distància:



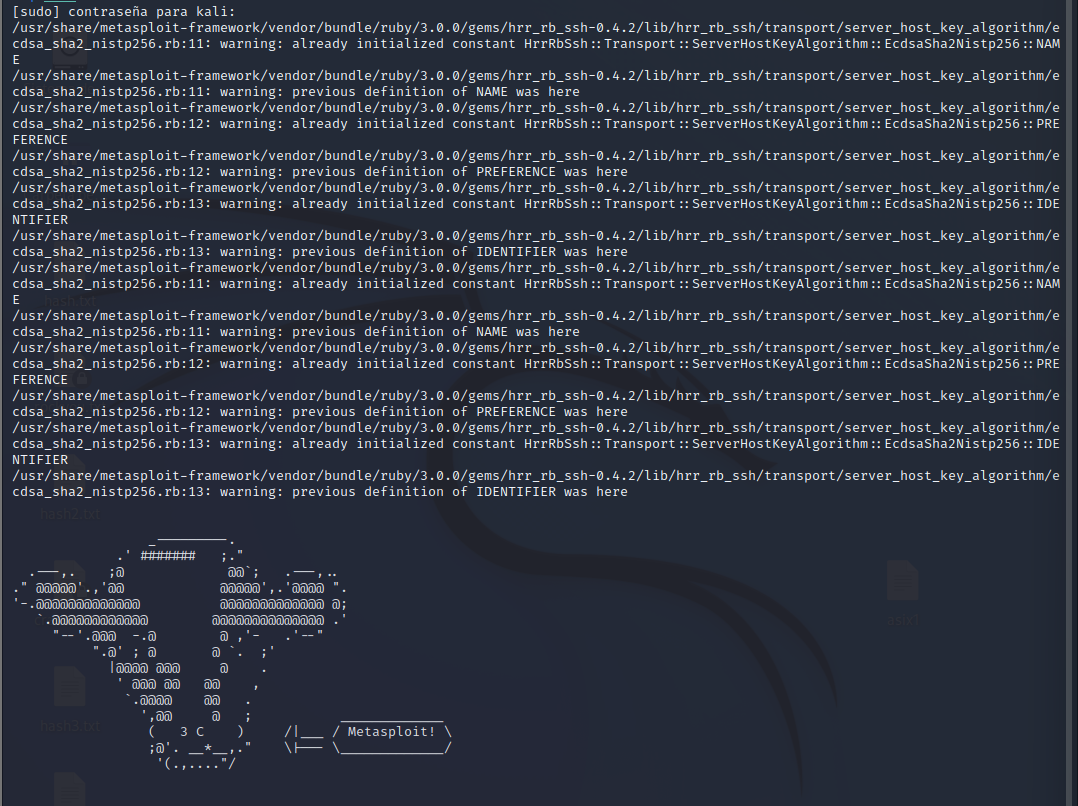


# 

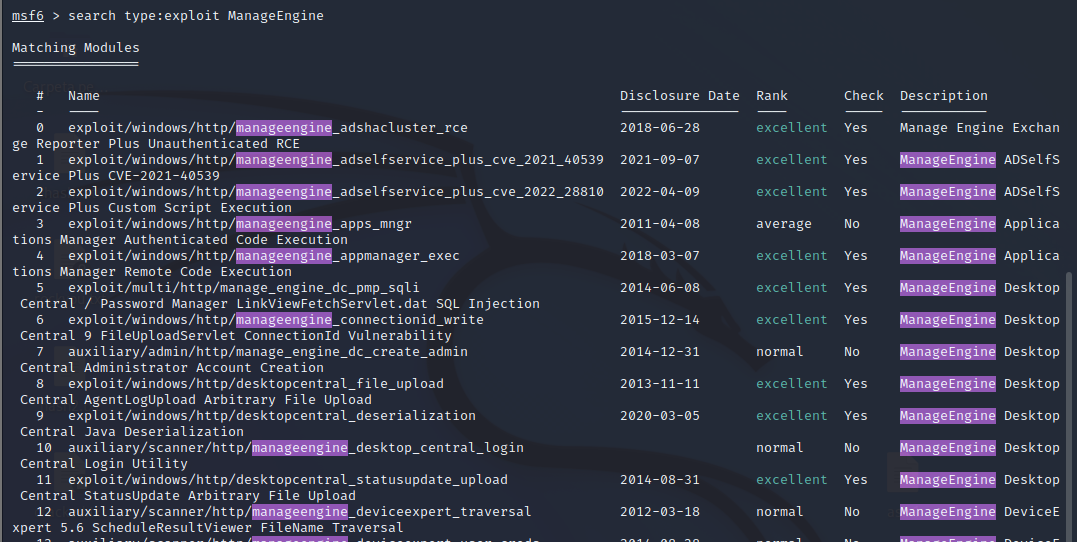
# Exercici 5: Explotar altres vulnerabilitats

Primer de tot executarem la consola a la terminal:





Executarem aquesta comanda per cercar exploits de ManageEngine



Probarem amb el 6:

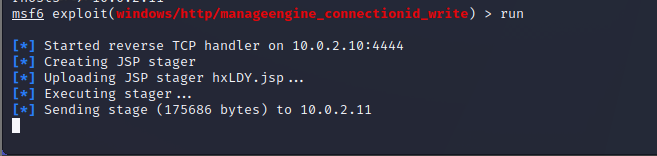


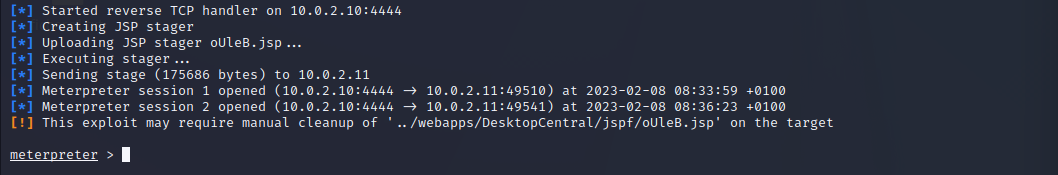


Farem un rhosts de la màquina meta:

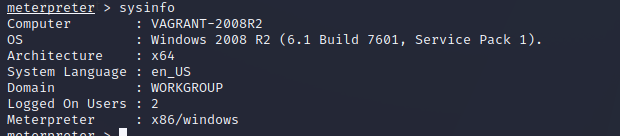


I executarem un run:





Farem un sysinfo dins del meterpreter:

I ara farem un shell per entrar a la terminal del meta a través del ManageEngine:

