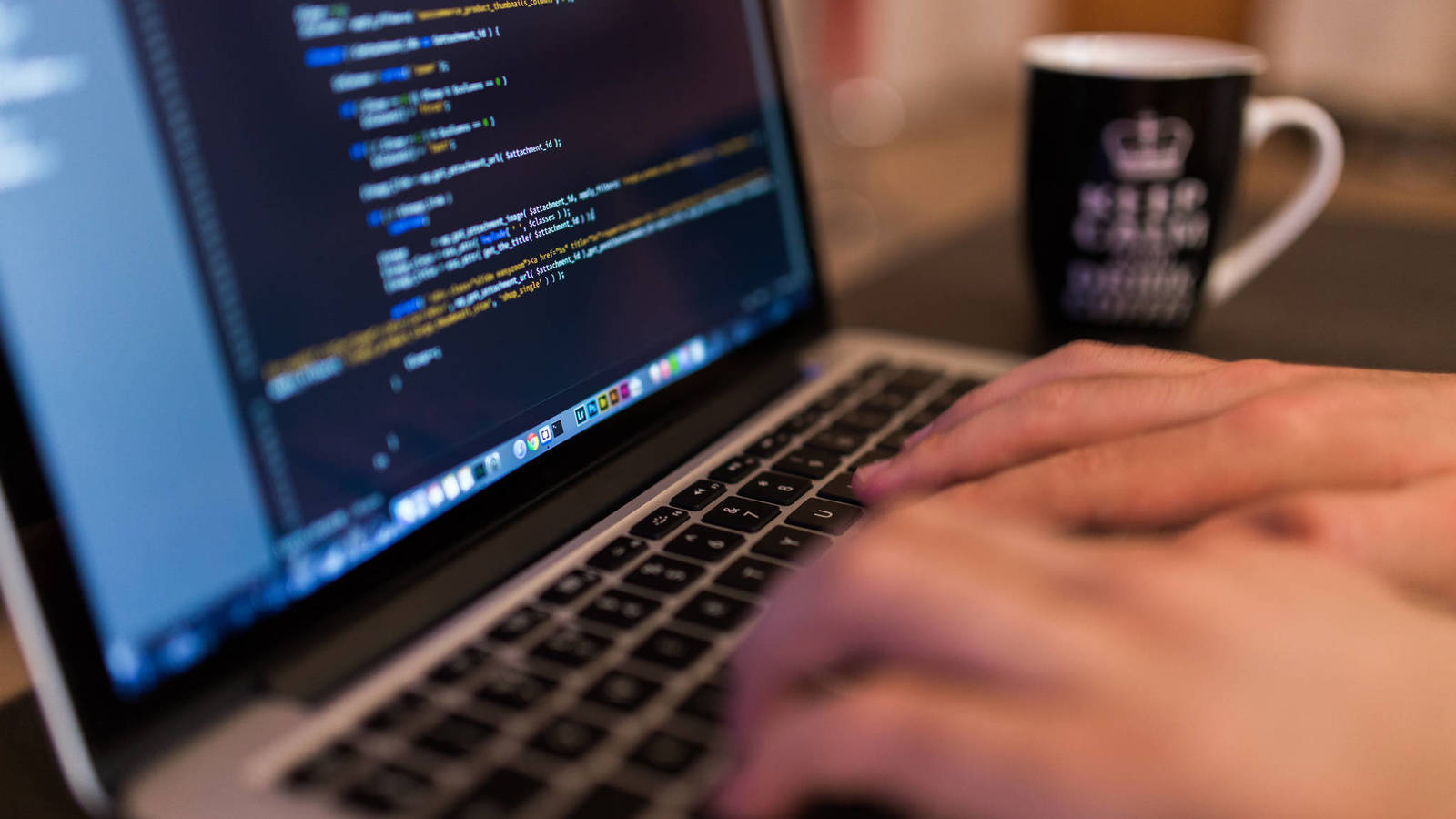
1 ASIX

**MÒDUL 16: CIBERSEGURETAT I HACKING ÈTIC**

ACTIVITAT 1.11: Explotació 3

línea horizontal

# 



**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Sergi Andrés

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

**ÍNDEX**

[**Exercici 1 – Explotar vulnerabilitat SMB/SAMBA de Metasploitable 2**](#_91dfsc6gigpz) **3**

[a. Posa la Màquina Metasploitable 2 en la mateixa Red Nat que Kali Linux i executa Netdiscover per a saber quina és la seva IP](#_4w0le0uf55tb) 3

[b. Executa Nmap sobre la màquina víctima Metasploitable 2 per a veure quins ports té oberts.](#_k31bq0lyqrkj) 3

[c. Per quins ports s’està executant el servei Samba o SMB?](#_pcil3cn8q23) 4

[d. Quina versió de Samba hi ha instal·lada?](#_lpcd0ex19xoe) 4

[e. Executa algun script de Nmap (possiblement el millor és vulners) per a comprovar si hi ha alguna vulnerabilitat relacionada amb aquesta versió de SMB/SAMBA, i indica els seus CVE en cas que els trobis.](#_v3s5syp096r6) 4

[f. Amb els resultats obtinguts en els apartats anteriors, intenta explotar la màquina a través de les vulnerabilitats que presenta el servei SMB que hi ha en execució.](#_otuxp2lhqjis) 5

[**Exercici 2 – Explotar vulnerabilitat FTP de Metasploitable 2**](#_1drzc4b5dn5f) **8**

[a. Executa Nmap sobre la màquina víctima Metasploitable 2 per a veure quins ports té oberts.](#_80hx7q7t01y0) 8

[b. Quants serveis de FTP hi ha en execució? I per quins ports estan escoltant?](#_tramufn99wl7) 8

[c. Com es diuen els programes de FTP i quines versions són?](#_yytw8txkawuw) 8

[d. Amb els resultats obtinguts en els apartats anteriors, intenta ara explotar la màquina a través de les vulnerabilitats que presenta algun dels serveis de FTP que hi ha en execució.](#_hxned8th09ue) 9

[**Exercici 3 – Altres vulnerabilitats de Metasploitable 2**](#_dobuyewf3utc) **12**

[a. Executa Nessus, Nexpose o OpenVas contra Metasploitable 2 i comenta els resultats obtinguts.](#_uhlcn4zi957z) 12

[b. Prova d’explotar alguna de les vulnerabilitats trobades ja sigui a través d’algún exploit o a través de força bruta.](#_uwz4lmid8p1h) 14

[**Exercici 4 – Explotar vulnerabilitat màquina BasicPentesting 1**](#_k5g9m09k8zpf) **18**

[a. Executa Netdiscover per a trobar quina és la IP d’aquesta màquina.](#_iim6zckt1115) 18

[b. Executa Nmap sobre aquesta màquina per a saber quina versió de FTP hi ha en execució i per quin port està escoltant.](#_9pz7aeopgxxt) 19

[c. Busca dins de Metasploit si aquesta versió de FTP és explotable](#_a3jr6465gg9z) 20

[d. Explota-la](#_vrfxzzmjacuj) 20

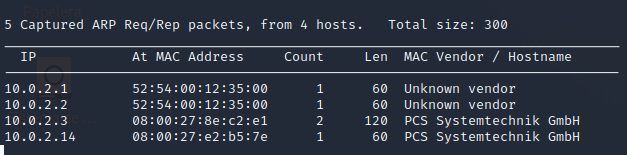
# Exercici 1 – Explotar vulnerabilitat SMB/SAMBA de Metasploitable 2

### a. Posa la Màquina Metasploitable 2 en la mateixa Red Nat que Kali Linux i executa Netdiscover per a saber quina és la seva IP



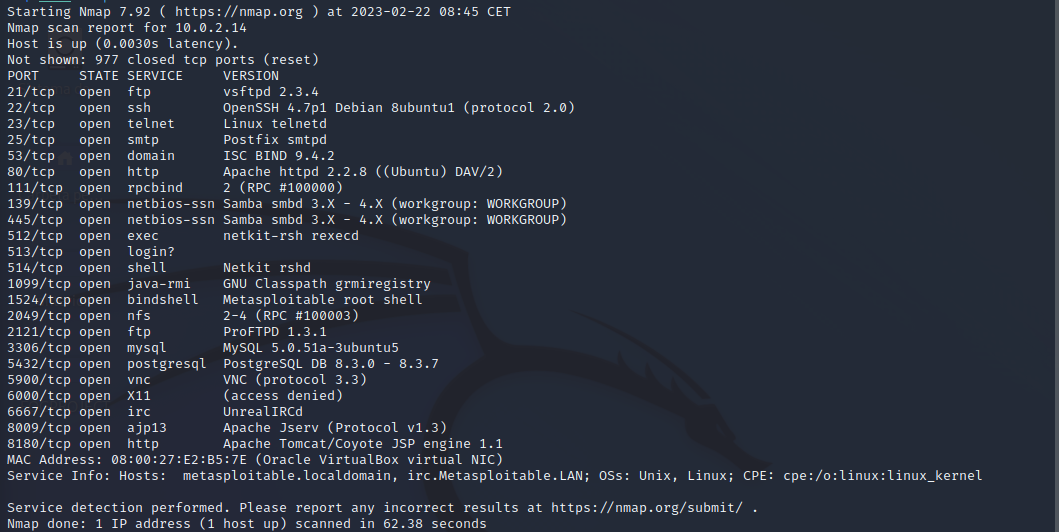
Des de Kali Linux farem un netdiscover de la xarxa per descobrir la ip de metasploitable 2:





### b. Executa Nmap sobre la màquina víctima Metasploitable 2 per a veure quins ports té oberts.





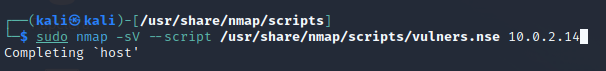
### c. Per quins ports s’està executant el servei Samba o SMB?

El servei samba o SMB s’està executant en els ports 139 i 445.

### d. Quina versió de Samba hi ha instal·lada?

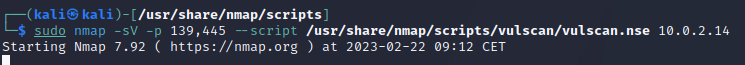
La versió instal·lada és la 3.X - 4.X (Esta en el rang d’aquestes dues versions)

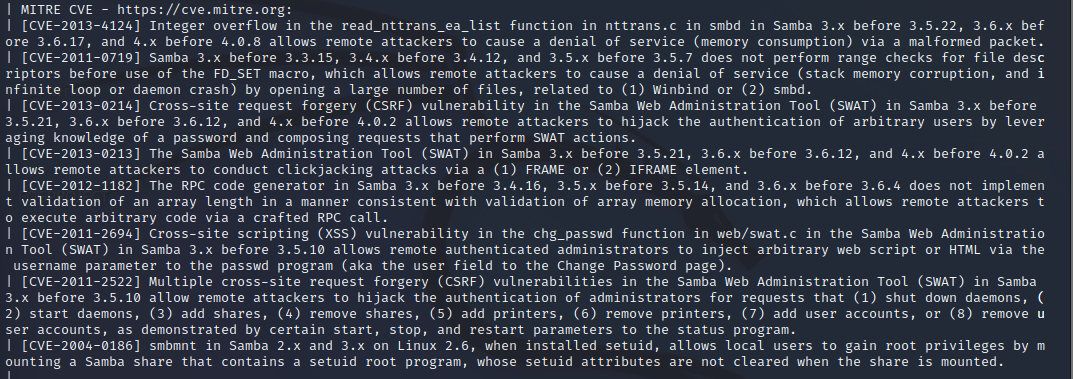
### e. Executa algun script de Nmap (possiblement el millor és vulners) per a comprovar si hi ha alguna vulnerabilitat relacionada amb aquesta versió de SMB/SAMBA, i indica els seus CVE en cas que els trobis.





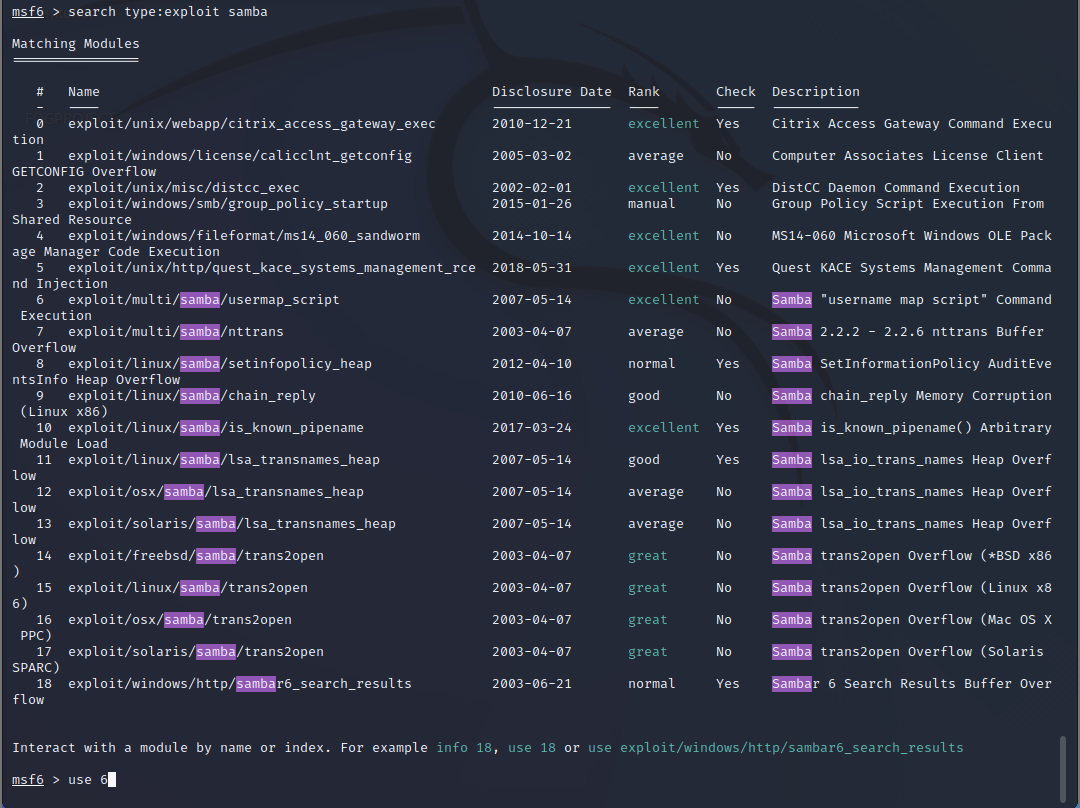
No surt cap vulnerabilitat, només la versió. Provarem amb el vulscan:



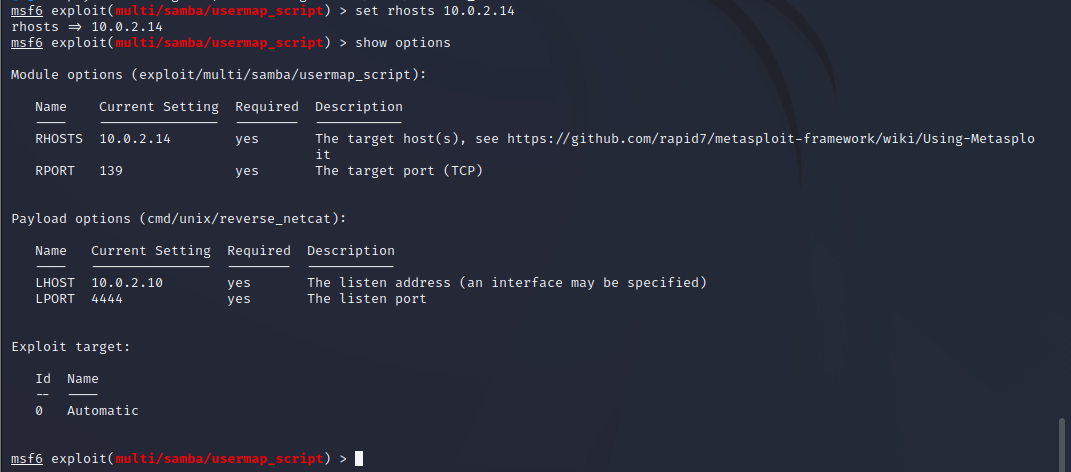


Ens ha trobat aquestes vulnerabilitats.

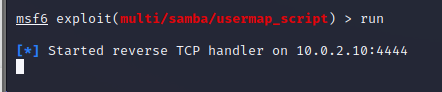
### f. Amb els resultats obtinguts en els apartats anteriors, intenta explotar la màquina a través de les vulnerabilitats que presenta el servei SMB que hi ha en execució.



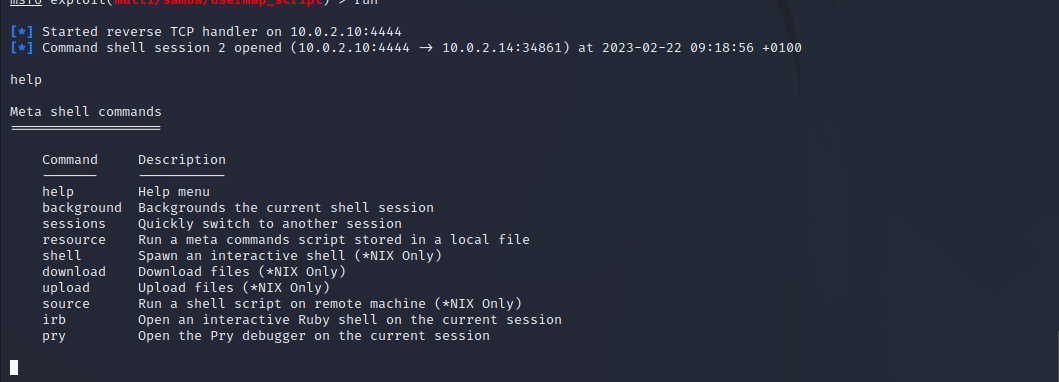
Farem un search exploit de samba i utilitzarem el 6.



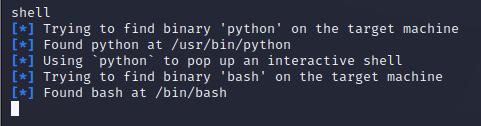
Posarem el host i farem un run:



Estarem dins de la màquina:



Farem un shell per entrar a la shell de metasploitable 2





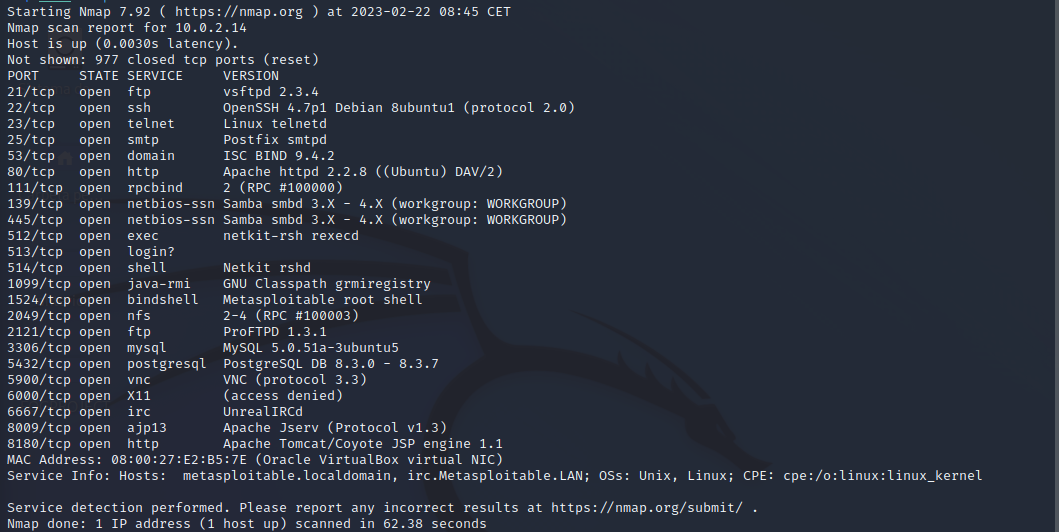
Ja som dins.

# 

# Exercici 2 – Explotar vulnerabilitat FTP de Metasploitable 2

### a. Executa Nmap sobre la màquina víctima Metasploitable 2 per a veure quins ports té oberts.





### b. Quants serveis de FTP hi ha en execució? I per quins ports estan escoltant?

Hi han dos serveis FTP, un al port 21 i l’altre al port 2121

### c. Com es diuen els programes de FTP i quines versions són?

Els programes es vsftpd i la versió es la 2.3.4

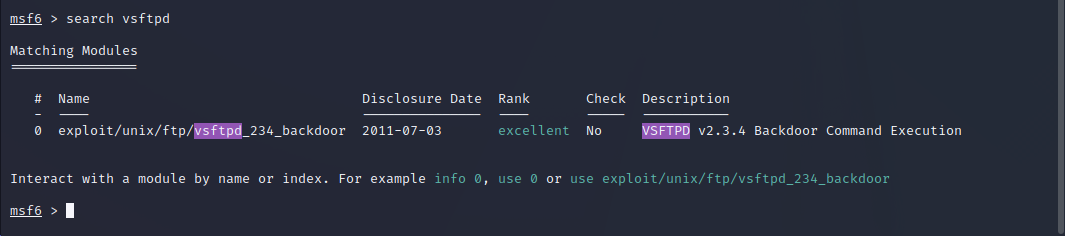
L’altre es el ProFTPD i la seva versió es la 1.3.1

### d. Amb els resultats obtinguts en els apartats anteriors, intenta ara explotar la màquina a través de les vulnerabilitats que presenta algun dels serveis de FTP que hi ha en execució.



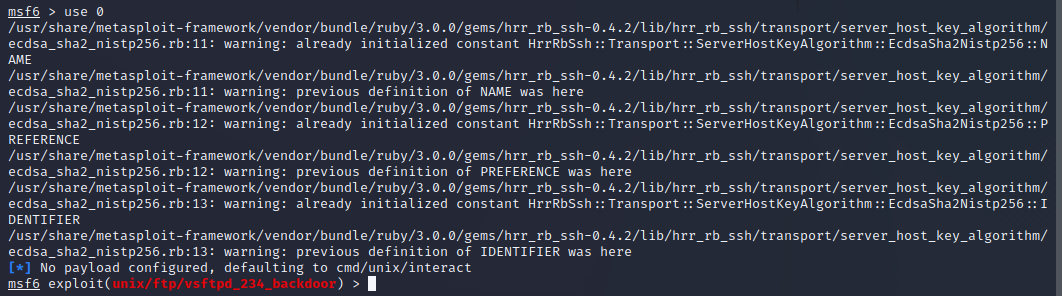
Entrarem al msfconsole.

Buscarem el vsftpd per exemple:

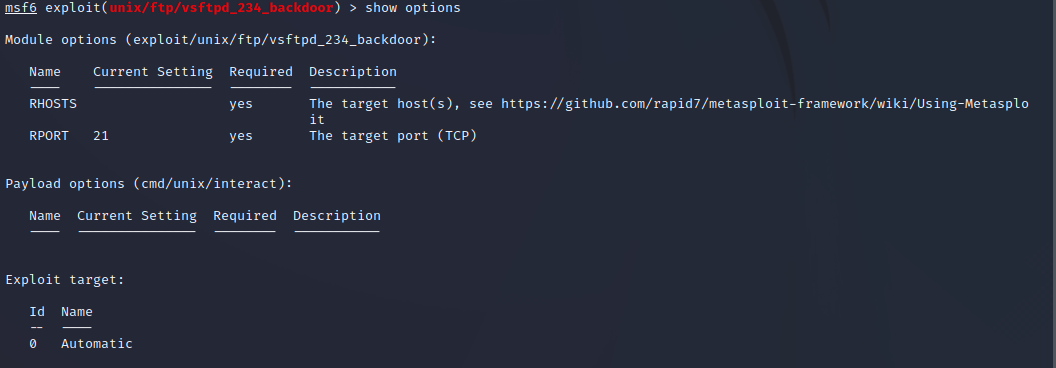


Podem veure l’exploit i també la versió que cuadra.

Farem un use 0:

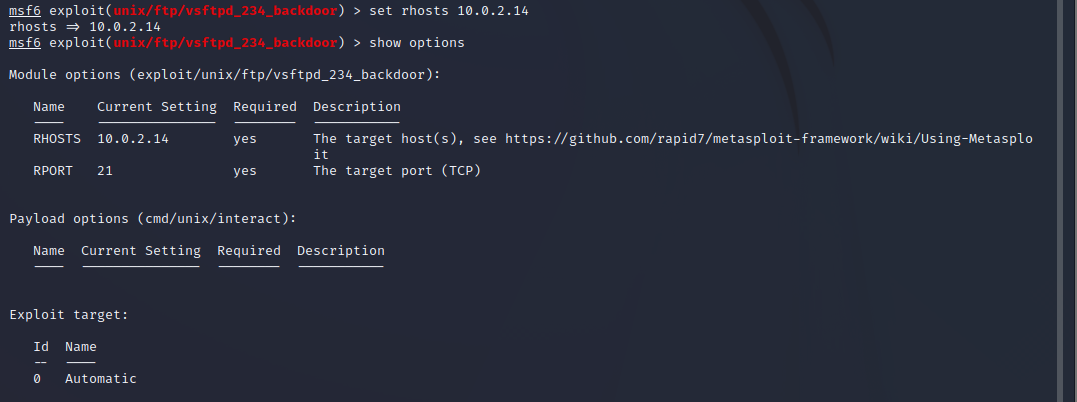


Ara configurarem el host i el port, però abans farem un show options:



El port es el correcte, així que no fa falta canviar-ho.

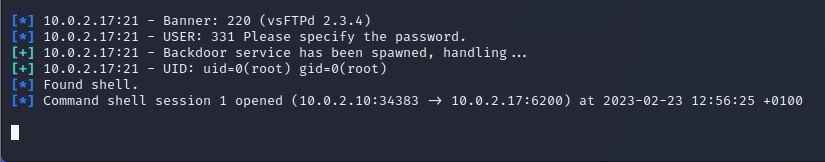
Haurem de seleccionar el host:



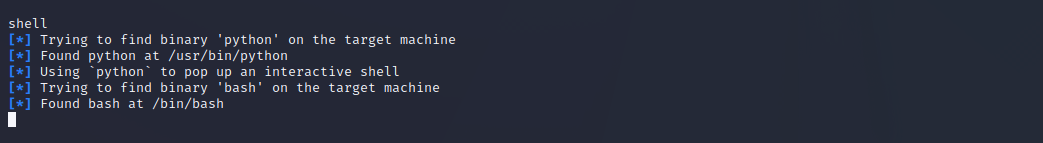
Ara podrem executar el run.

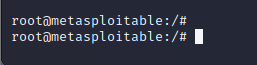


(La ip de la màquina metasploitable 2 ha canviat ja que he hagut de reinstalar-la)



Per exemple entrarem a la shell:

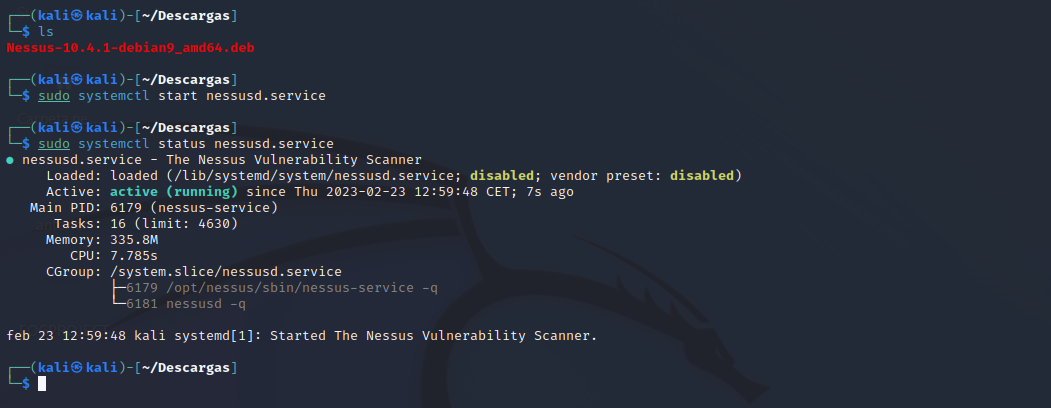




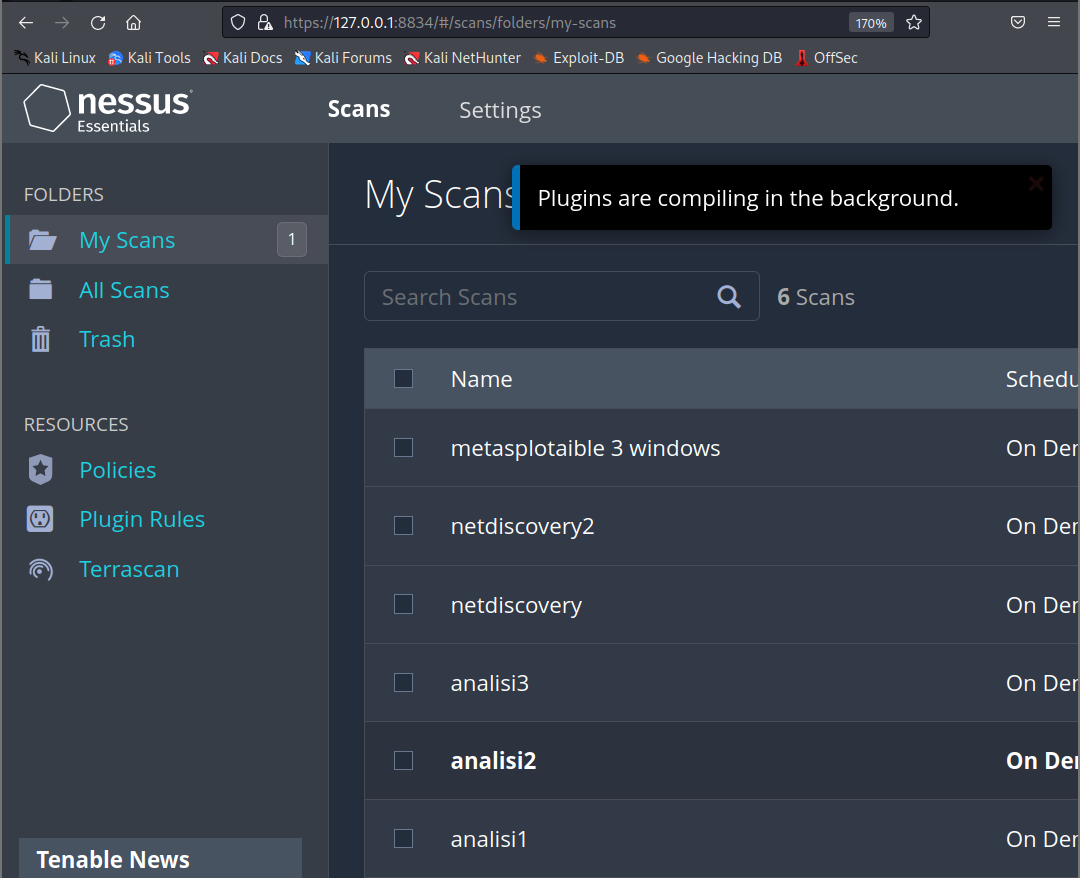
Ja som dins de la shell.

# Exercici 3 – Altres vulnerabilitats de Metasploitable 2

### a. Executa Nessus, Nexpose o OpenVas contra Metasploitable 2 i comenta els resultats obtinguts.

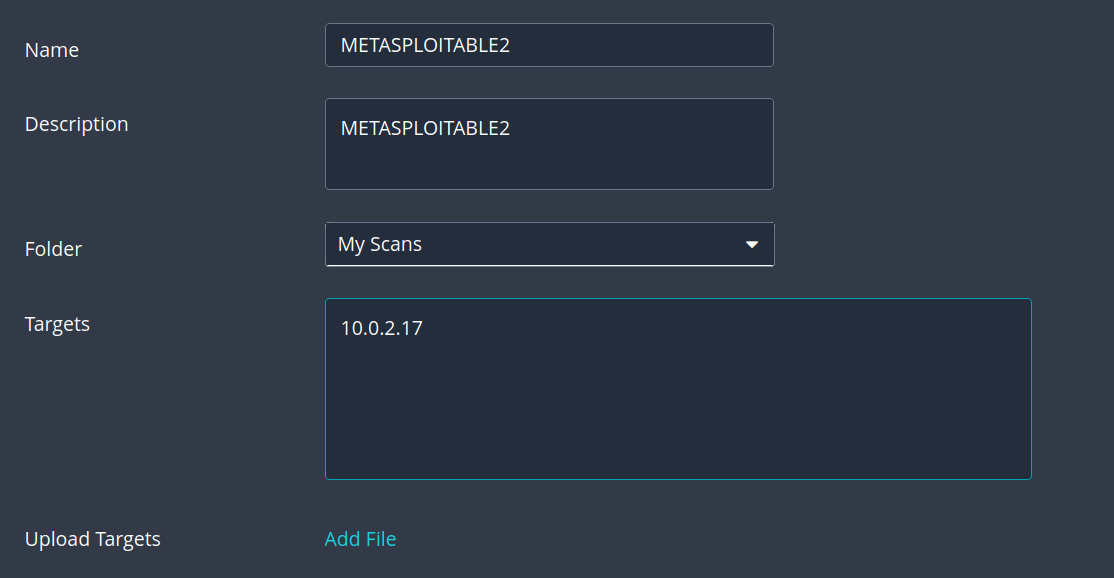


Posarem el nessus actiu.

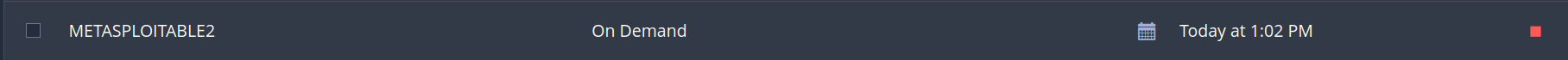


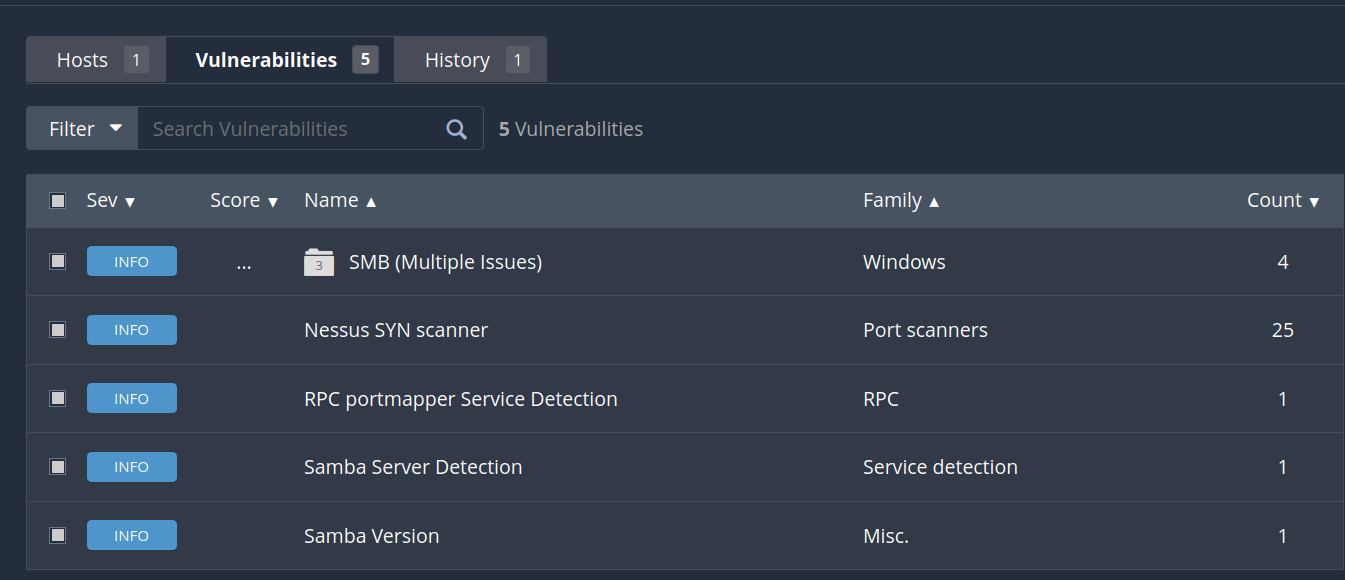
Posarem la ip i el port i ja som dins de nessus.

Farem un nou basic scan:

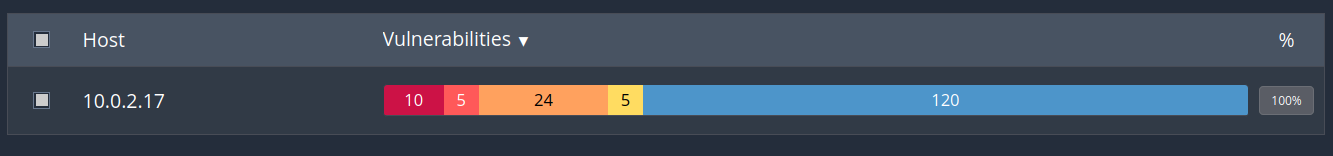


Executarem el scan:





Aqui un cop acabat podrem veure totes les vulnerabilitats.



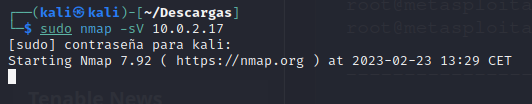
Ja ha cabat, mirarem alguna vulnerabilitat i la explotarem.

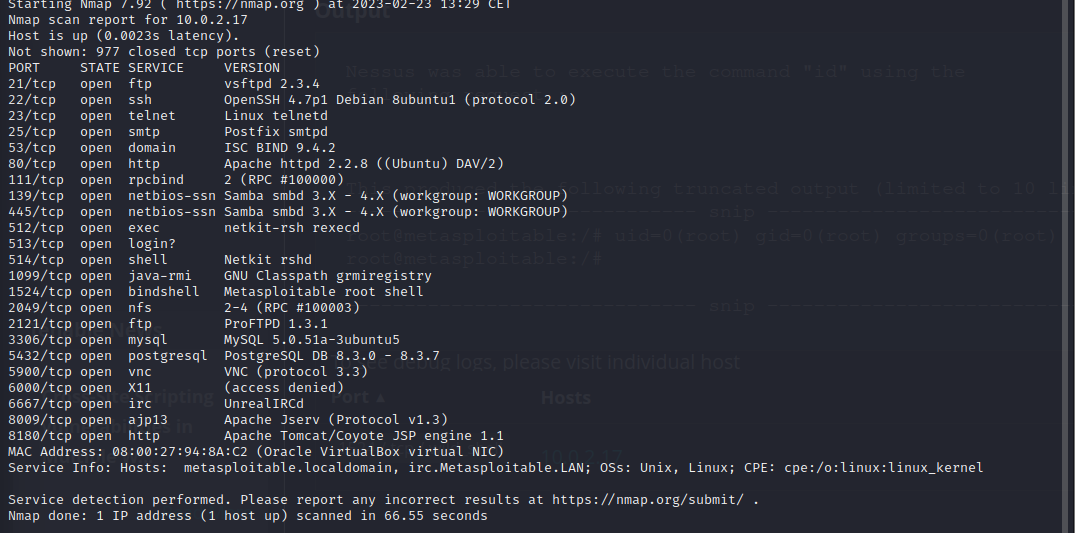
### b. Prova d’explotar alguna de les vulnerabilitats trobades ja sigui a través d’algún exploit o a través de força bruta.



Per exemple, aquesta ens diu que s’allotja en el port 21, intentarem explotar aquesta.

Farem un nmap amb -sV per determinar la versió de la vulnerabilitat:



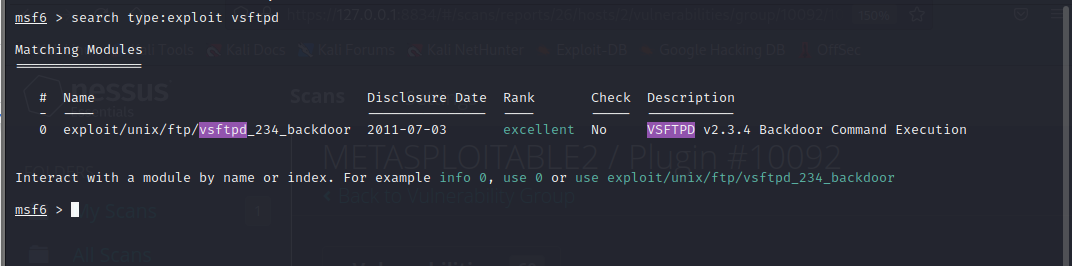


Podem observar que es el vsftpd versió 2.3.4

Entrarem al msfconsole:



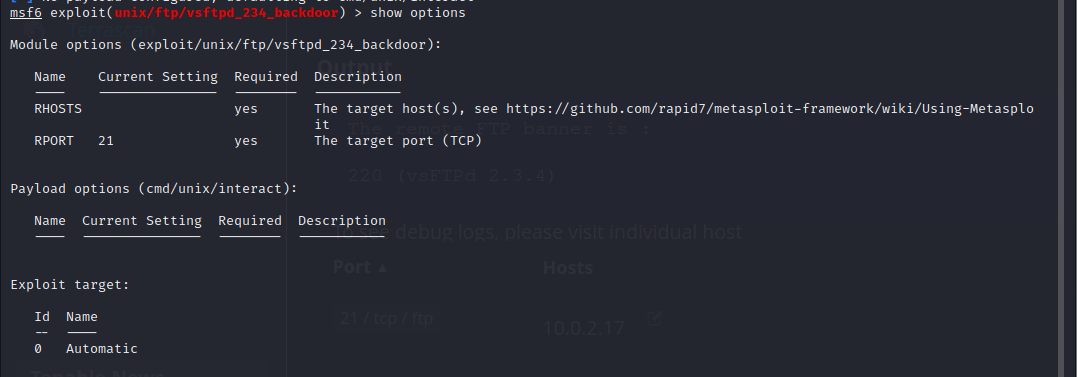
Buscarem el exploit vsftpd:



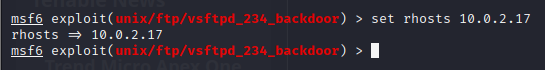
Farem un use 0 per utilitzar el unic exploit.

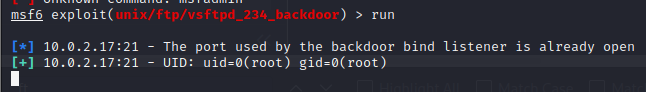


Farem un show options:

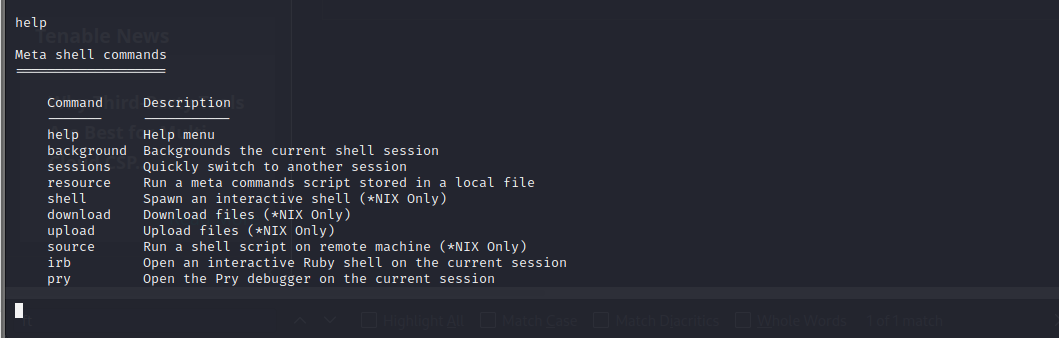


Farem un set rhosts per determinar la màquina victima.

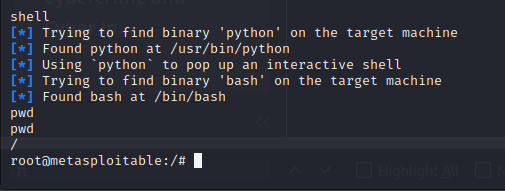




Un cop dins farem un help:



Farem un shell

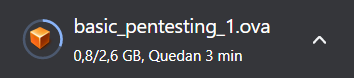


I ja serem dins de la màquina metasploitable 2.

# Exercici 4 – Explotar vulnerabilitat màquina BasicPentesting 1

### a. Executa Netdiscover per a trobar quina és la IP d’aquesta màquina.

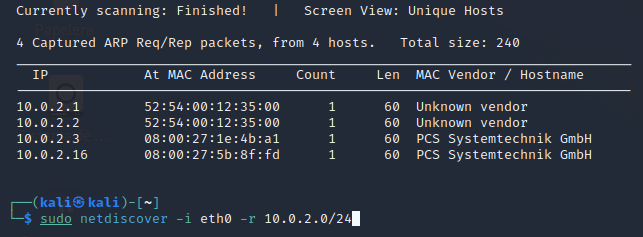
Descarregarem la ova d’internet:



Quan estigui llesta executarem la màquina:

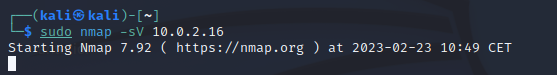


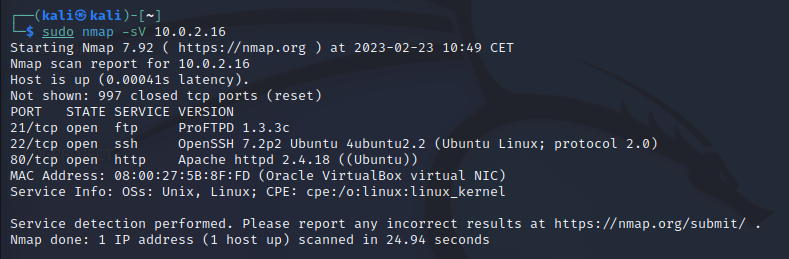
Entrarem dins i un cop dins pasarem al Kali Linux i farem un netdiscover sobre la xarxa per descobrir la ip d’aquesta nova màquina:



### b. Executa Nmap sobre aquesta màquina per a saber quina versió de FTP hi ha en execució i per quin port està escoltant.

Executarem nmap amb el sV:

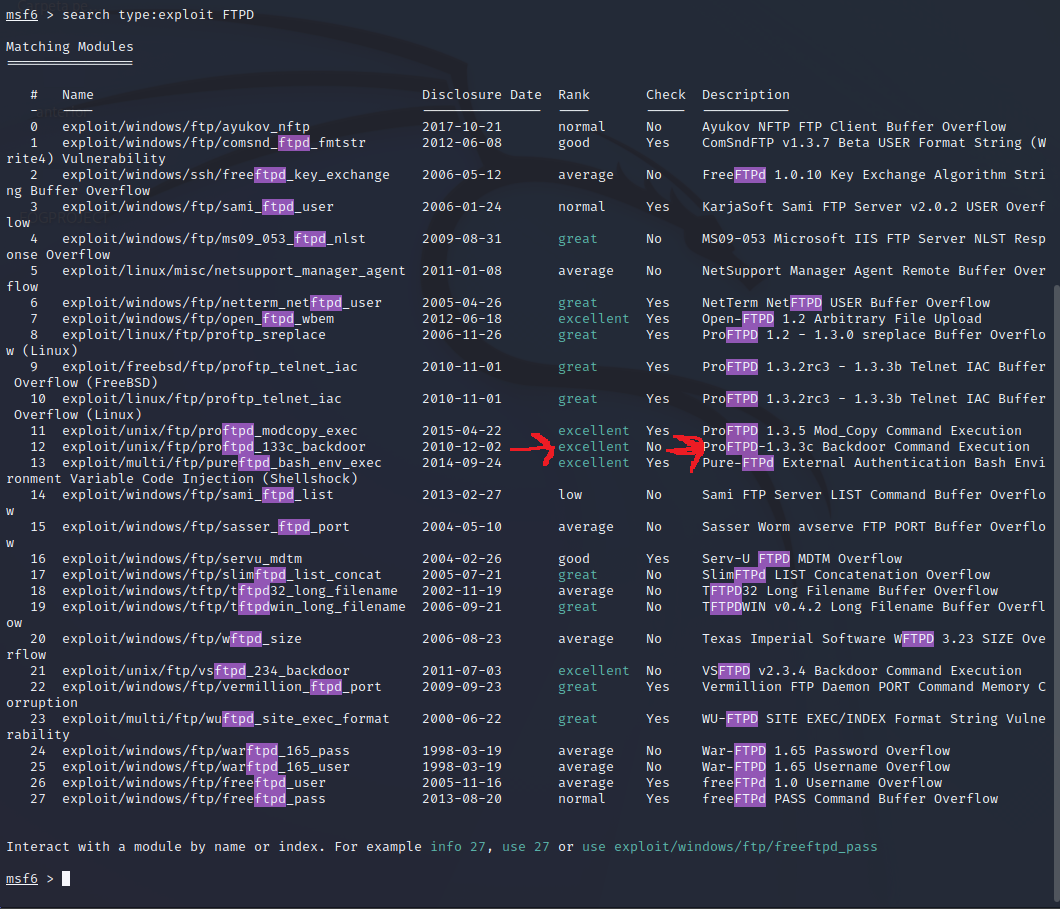




En el port 21 tenim una versio de FTPD que es la 1.3.3c

### 

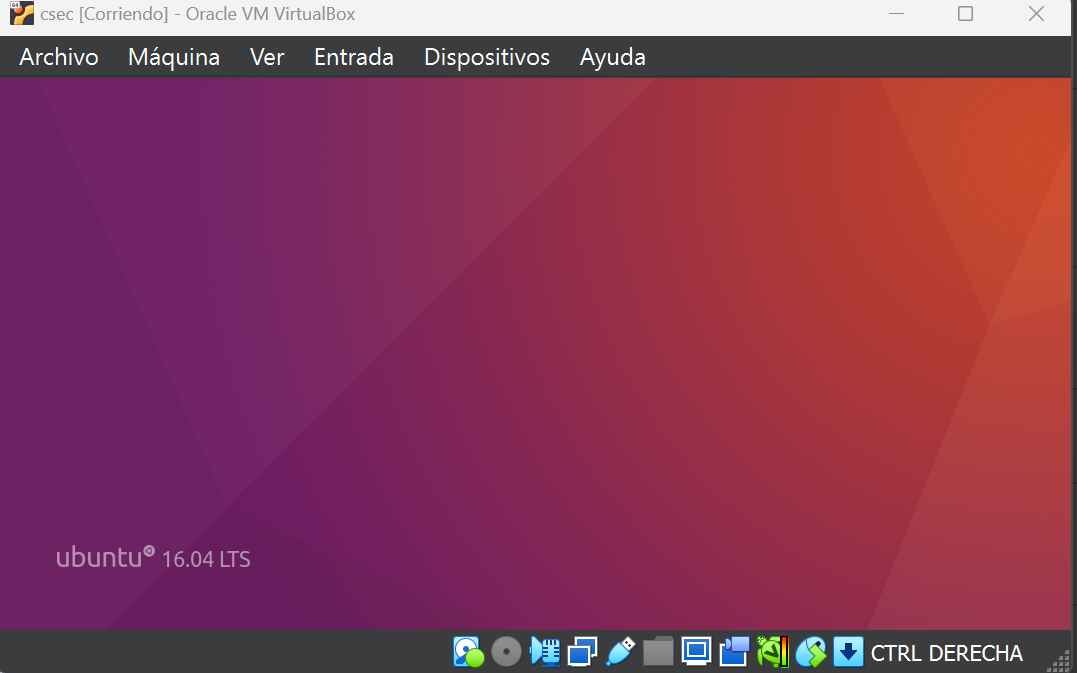
### c. Busca dins de Metasploit si aquesta versió de FTP és explotable



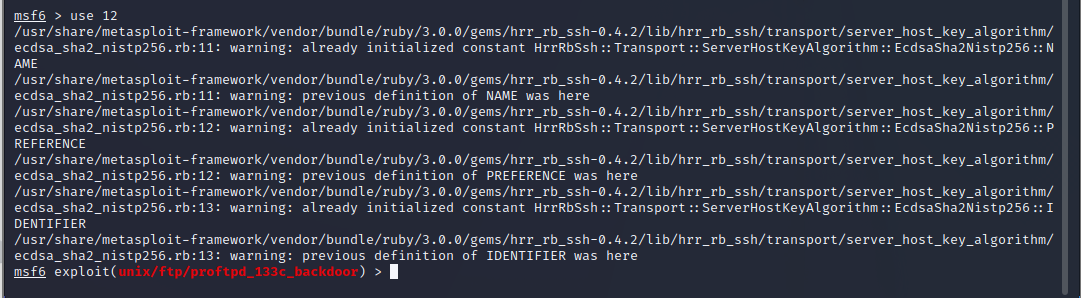
Podem observar que si que es pot explotar

### d. Explota-la

Per explotarla, iniciarem un altre cop la màquina basicpentesting1.



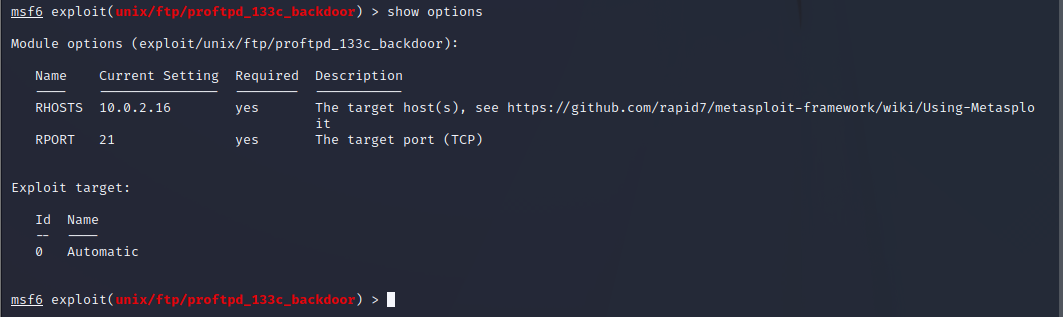
Un cop encesa, farem un use 12 ja que es el de la versió que volem explotar:



Farem un set rhosts a la màquina:

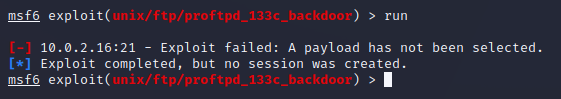


Ara farem un showoptions:



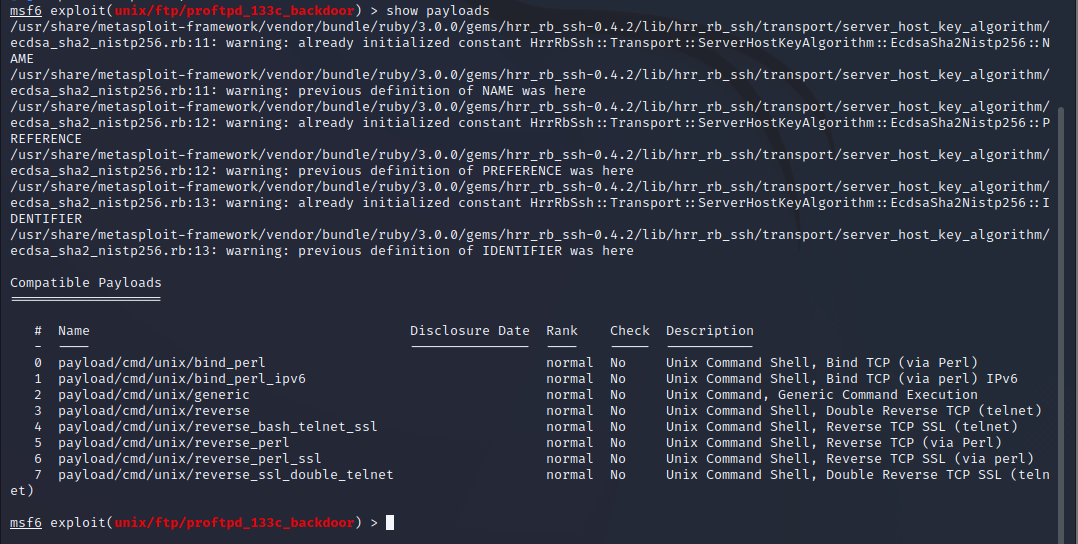
El port es el correcte, el 21, per tant anem bé.

Ara el que executarem es un run:

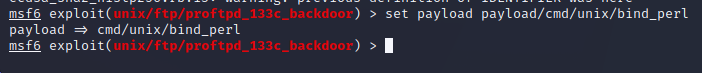


Hem de posar el payload:

Farem show options dels payloads



Escollirem per exemple el 0:



Executarem el run:

