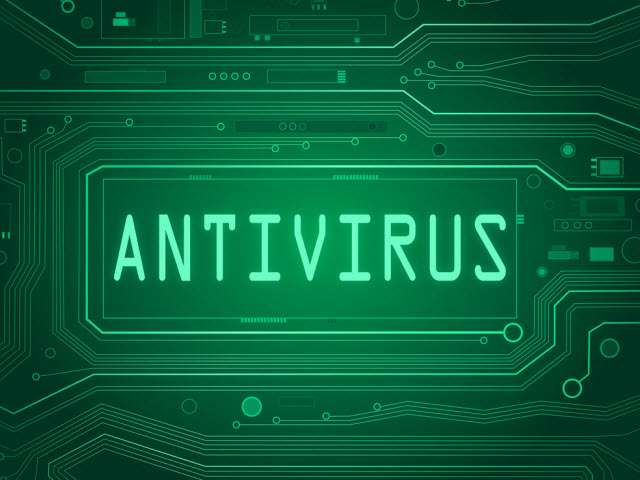
1 ASIX

**MÒDUL 16: CIBERSEGURETAT I HACKING ÈTIC**

ACTIVITAT 1.13: Payloads avançats i evasió d’antivirus

línea horizontal

# 



**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Sergi Andrés

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

**ÍNDEX**

[**Exercici 1 – Payload dins d’un fitxer .exe existent 3**](#_gfqyynffb1n3)

[a. Genera el payload dins d’un executable existent, que es connecti al port 4444. Fes-lo 2 cops, un amb encriptació ShikataGaNai i l’altre sense encriptació 3](#_d9566e5ezz3t)

[b. Posa la màquina atacant en escolta seguint els passos: 4](#_9xaz1bjacd0j)

[c. Passa-li el payload a la víctima i executa’l. 5](#_klk47lcwqfc8)

[d. Comprova que es crea una connexió reversa cap a l’atacant. 7](#_adkfwqi1e77i)

[e. Has pogut esquivar l’antivirus i/o Windows Defender? Raona la resposta 8](#_p0f71xa4clcl)

[Amb el que no esta codificat he pogut esquivar el firewall i el windows defender, en canvi, amb el encriptat no funciona. 8](#_vfkonb1hm1d8)

[**Exercici 2 – Antivirus 9**](#_b42u55fg0e5)

[Busca informació de com funciona un antivirus i quines tècniques utilitza per a detectar virus, malware, troians, payloads... 9](#_tlq94el1v3cf)

[**Exercici 3 – Defeat Defender 10**](#_c13p70a2rpyi)

[a. Explica per a què serveix la eina Defeat-Defender que pots trobat a Github 10](#_2w5qltvvlul7)

[b. Prova el seu funcionament en una màquina Windows 10](#_velvrurhhsuj)

[**Exercici 4 – Camuflar un payload amb DarkArmour 13**](#_i6escj8luc6c)

[a. Actualitza repositoris —> apt update 13](#_nm2npwetk9ho)

[b. Descarrega’t git —> apt install git 13](#_km2bpr316ftw)

[c. Busca a google —> github DarkArmour, i trobaràs l’enllaç a la plana del projecte 13](#_ar0r0lsh2eu)

[d. Clona’l —> git clone adreça\_del\_projecte.git 14](#_ecmsyu4h8xgp)

[e. DarkArmour necessita que també tinguem instal·lats diversos paquets auxiliars, executa la següent sentència per a instal·lar-los: apt install mingw-w64-tools mingw-w64-common g++-mingw-w64 gcc-mingww64 upx-ucl osslsigncode 14](#_38pxq955vm5)

[f. Un cop instal·lat tot, entra a la carpeta darkarmour —> cd darkarmour 15](#_eyb9k37a2sz6)

[g. Per posar una armadura al teu fitxer maliciós 15](#_xcz13rlxom9t)

[h. Posa la màquina atacant en escolta (revisa els passos de l’exercici 1) 16](#_kx8o4rslnun)

[i. Passa el malware a la víctima i executa’l. 17](#_cc4iotm9zr2z)

[j. Comprova que es crea una connexió reversa cap a l’atacant. 18](#_8hcki4u77s14)

[k. Has pogut esquivar l’antivirus i/o Windows Defender? Raona la resposta 18](#_7g07a077it6b)

[**Exercici 5 – Altres eines d’ofuscació 19**](#_g7xozsg7mwf7)

[Explica breument què ofereixen els següents projectes que pots trobar a GitHub: 19](#_6p739hr0vjsb)

[– RedNeuron 19](#_snejp1izg36b)

[– Villain 19](#_if5qrv7vpcq4)

[– Hyperion 19](#_bazw10l88mll)

[– Fud payload generator 20](#_xdisz5h948ss)

[– MSFMania 20](#_aapkunl96tdh)

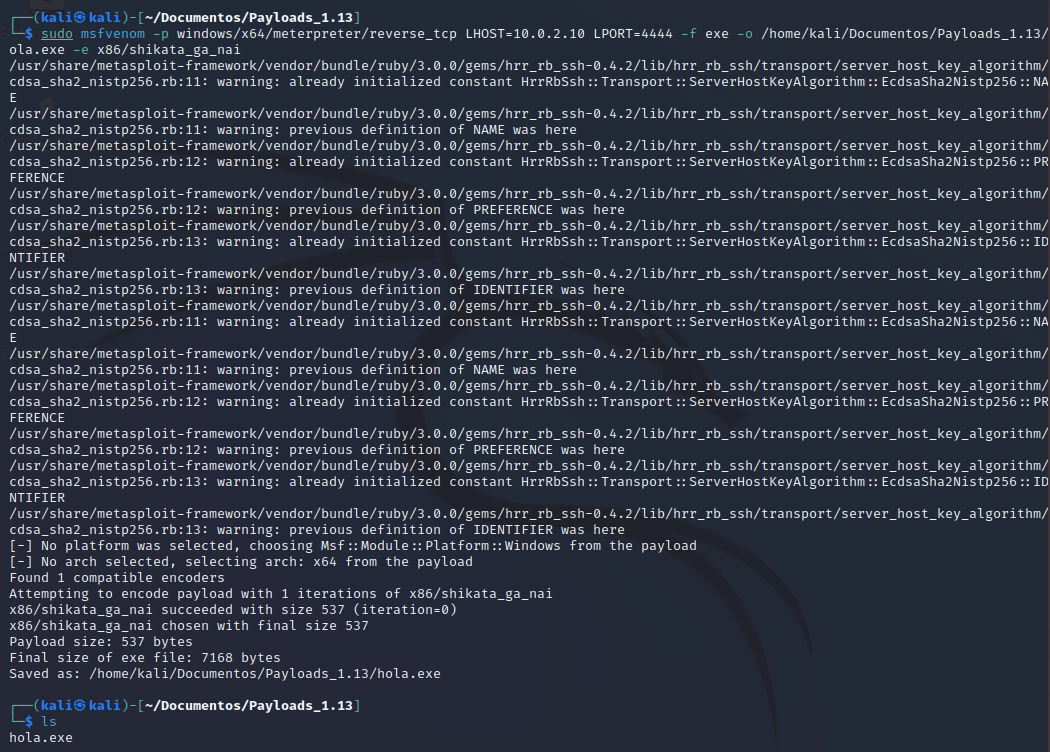
[– Python Obfuscator 21](#_k4he17im1afo)

# Exercici 1 – Payload dins d’un fitxer .exe existent

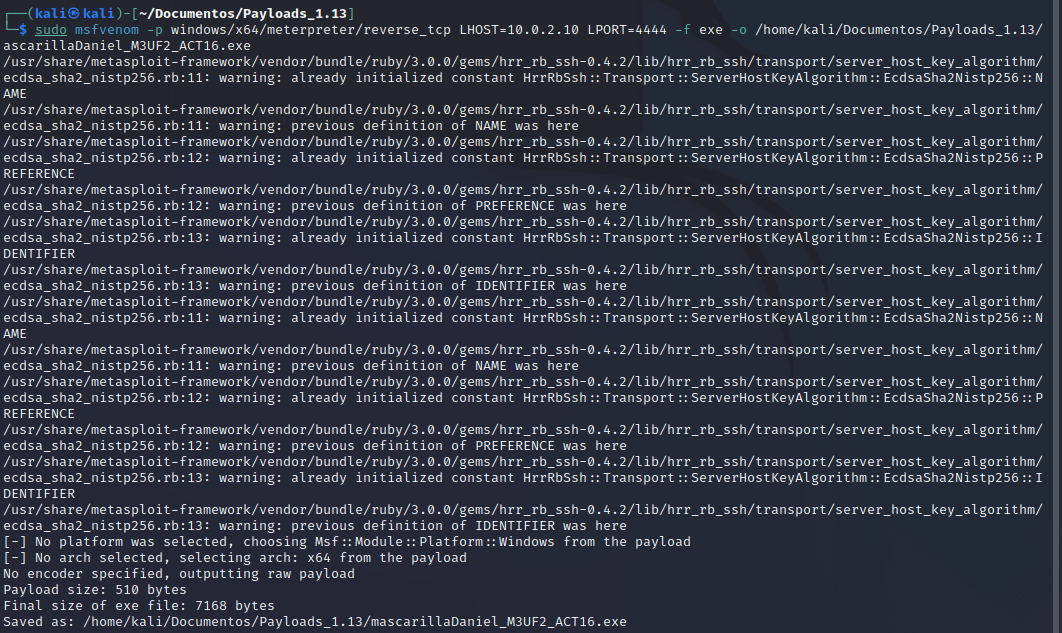
### a. Genera el payload dins d’un executable existent, que es connecti al port 4444. Fes-lo 2 cops, un amb encriptació ShikataGaNai i l’altre sense encriptació

### 

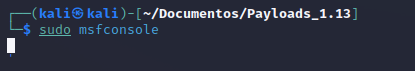
Payload amb encode ShikataGaNai

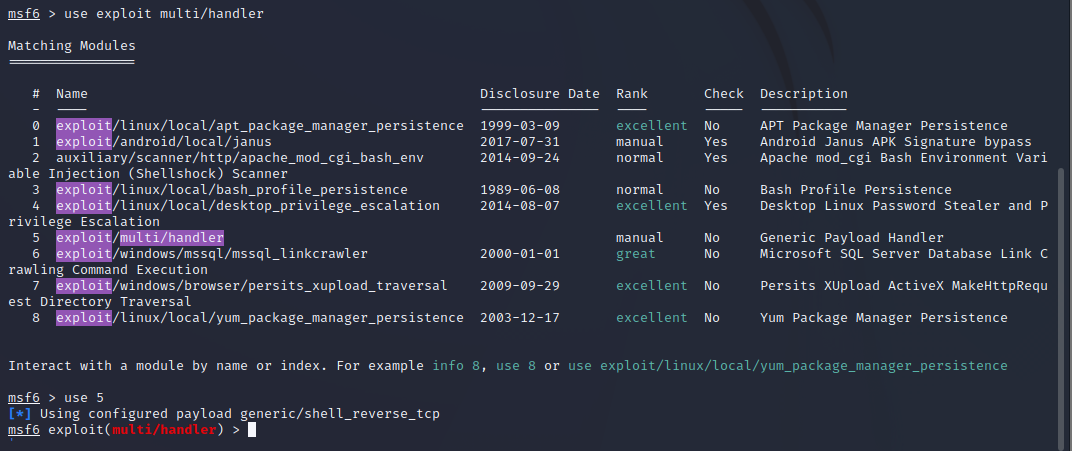


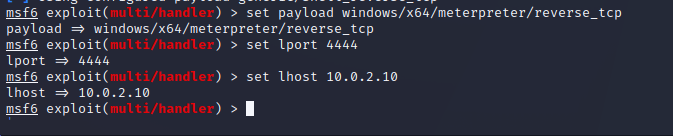
Payload sense encoder



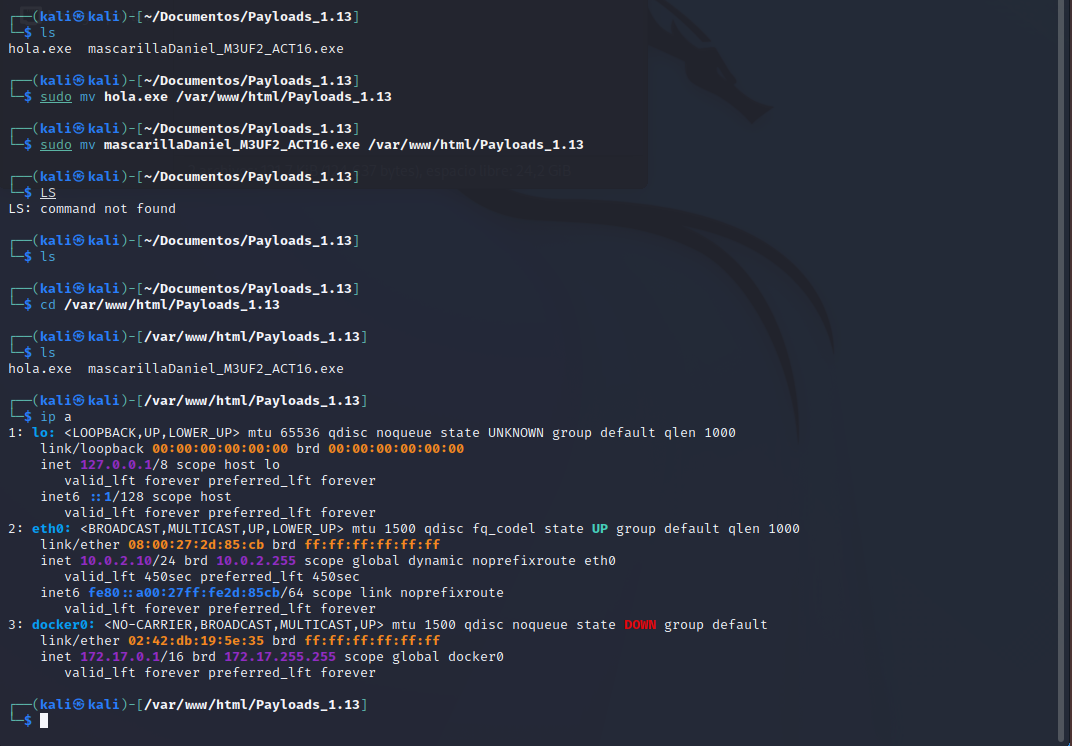
### b. Posa la màquina atacant en escolta seguint els passos:

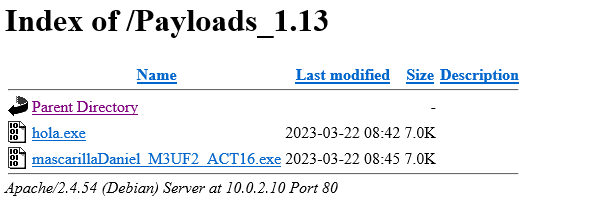


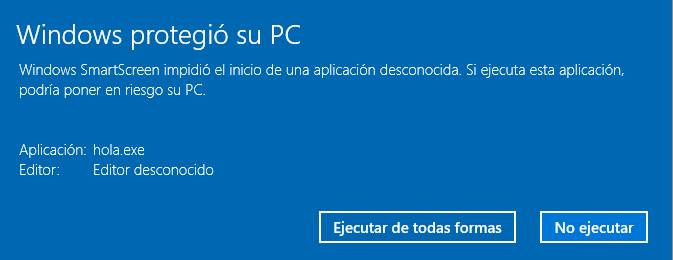


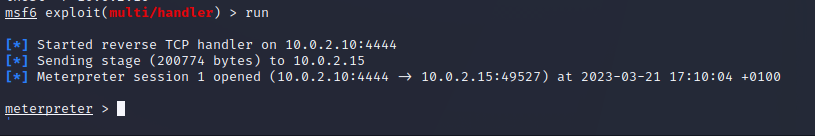


### c. Passa-li el payload a la víctima i executa’l.

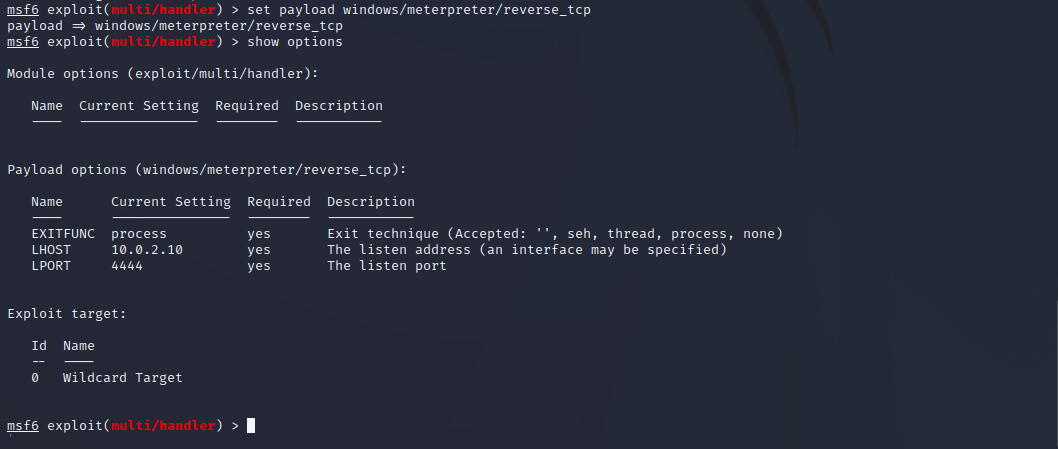


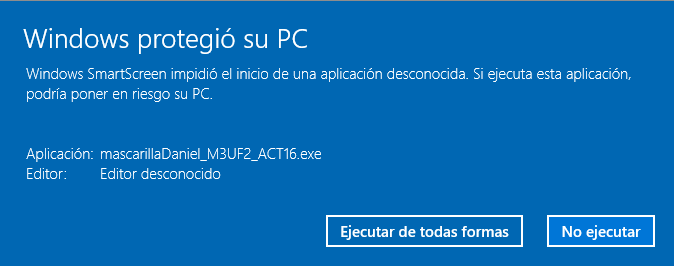


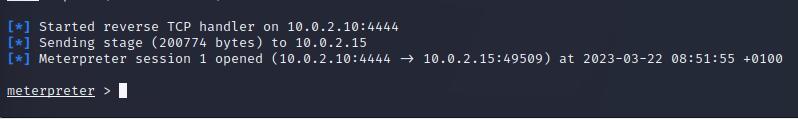




Ara ho faré amb el encoder

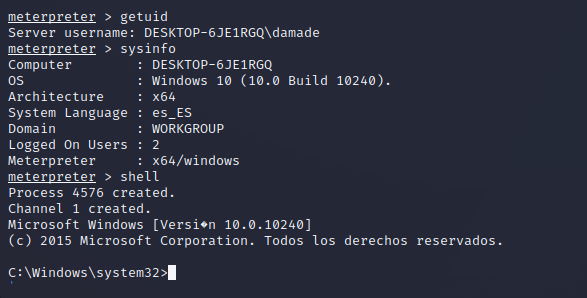






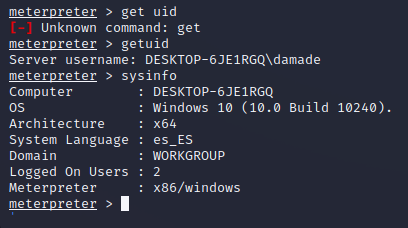
### d. Comprova que es crea una connexió reversa cap a l’atacant.

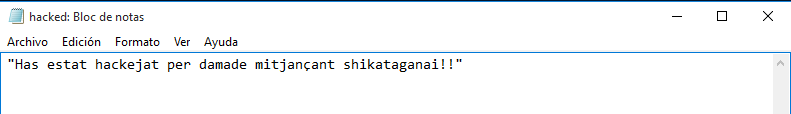
Amb el sense encoder:



Amb el encoder:







### e. Has pogut esquivar l’antivirus i/o Windows Defender? Raona la resposta

### Amb el que no esta codificat he pogut esquivar el firewall i el windows defender, en canvi, amb el encriptat no funciona.

# Exercici 2 – Antivirus

### Busca informació de com funciona un antivirus i quines tècniques utilitza per a detectar virus, malware, troians, payloads...

Un antivirus és un programa dissenyat per detectar, prevenir i eliminar virus informàtics, malware, troians, i altres amenaces informàtiques. A grans trets, un antivirus funciona mitjançant lús de diverses tècniques de detecció i anàlisi darxius i programes.

Les tècniques que els antivirus utilitzen per detectar virus i malware inclouen:

* Signatures de virus: Els antivirus mantenen una base de dades de firmes de virus conegudes. Quan un fitxer és escanejat, l'antivirus compara el contingut amb les signatures de virus conegudes a la base de dades per veure si hi ha una coincidència.
* Anàlisi heurística: Aquesta tècnica s'utilitza per detectar virus desconeguts. L'antivirus analitza el comportament del fitxer i cerca patrons sospitosos que puguin indicar la presència d'un virus.
* Anàlisi de comportament: L'antivirus monitoritza contínuament el comportament del sistema per detectar qualsevol activitat inusual que pugui indicar la presència d'un virus.
* Anàlisi de signatures digitals: Els programes maliciosos solen estar signats digitalment per semblar legítims. L'antivirus pot comprovar si una signatura digital és autèntica o no per determinar si un fitxer és segur o no.
* Anàlisi de codi: Els antivirus també poden analitzar el codi font d'un fitxer per detectar qualsevol activitat sospitosa.
* Anàlisi de sandbox: Aquesta tècnica implica executar un fitxer en un entorn virtual aïllat per veure com es comporta. Si es detecta una activitat maliciosa, l'antivirus pot bloquejar el fitxer.

# Exercici 3 – Defeat Defender

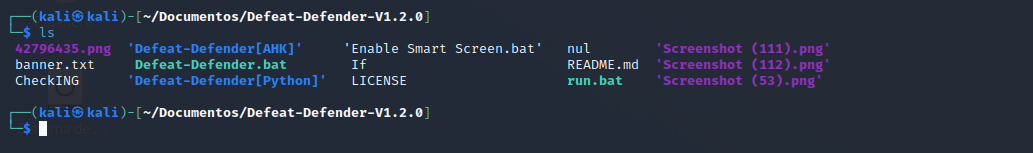
### a. Explica per a què serveix la eina Defeat-Defender que pots trobat a Github

Potent script per lots per desmuntar la protecció completa de Windows Defender i fins i tot evitar la protecció contra manipulacions

Desactivar Windows-Defender permanentment....

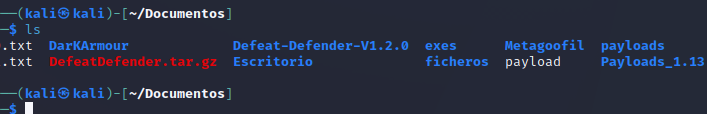
Piratejar finestres. POC

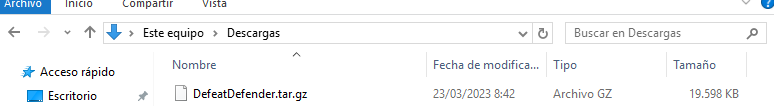
### b. Prova el seu funcionament en una màquina Windows

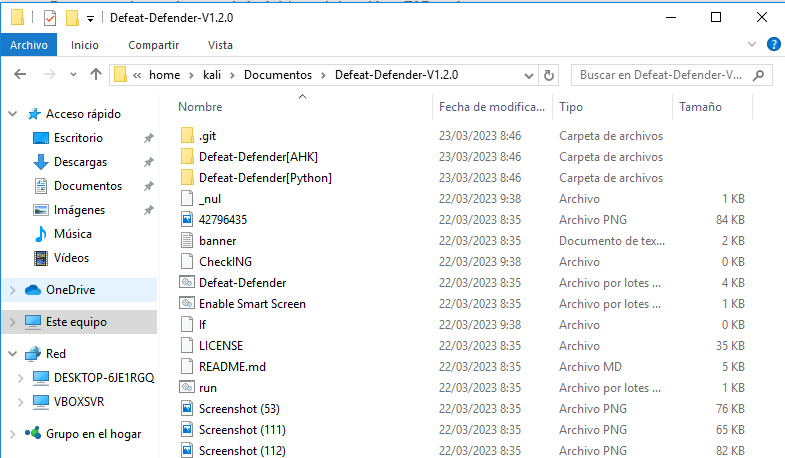


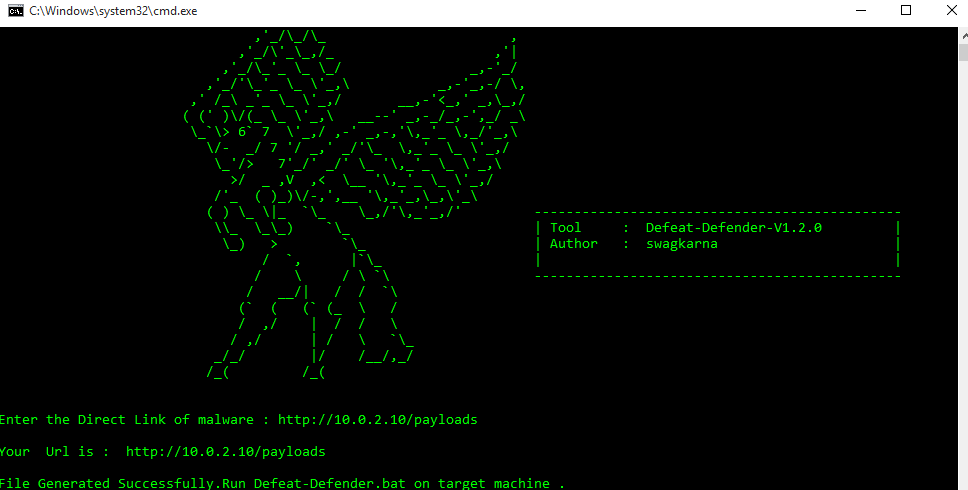
Pasarem la carpeta de Defeat Defender al windows:

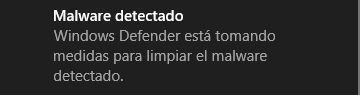


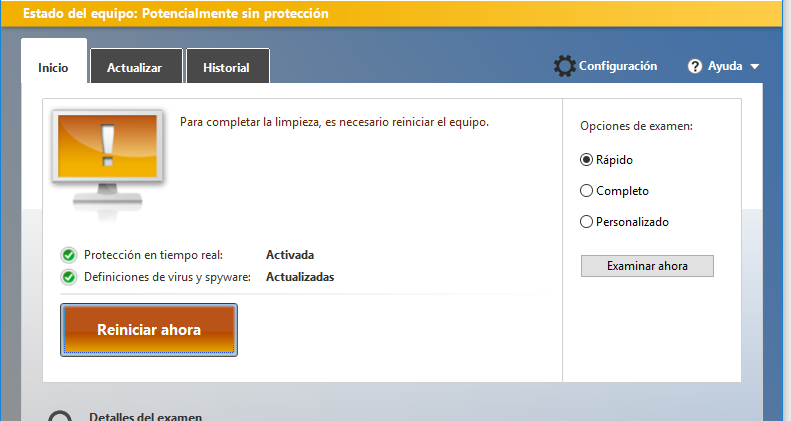












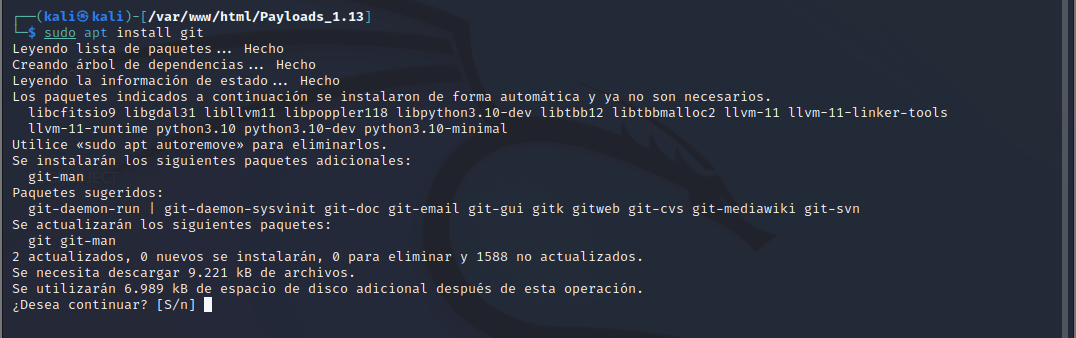
Ens posa després de executar el run que el windows defender esta potencialmente sense protecció, així que podem dir que ha funcionat el programa.

# Exercici 4 – Camuflar un payload amb DarkArmour

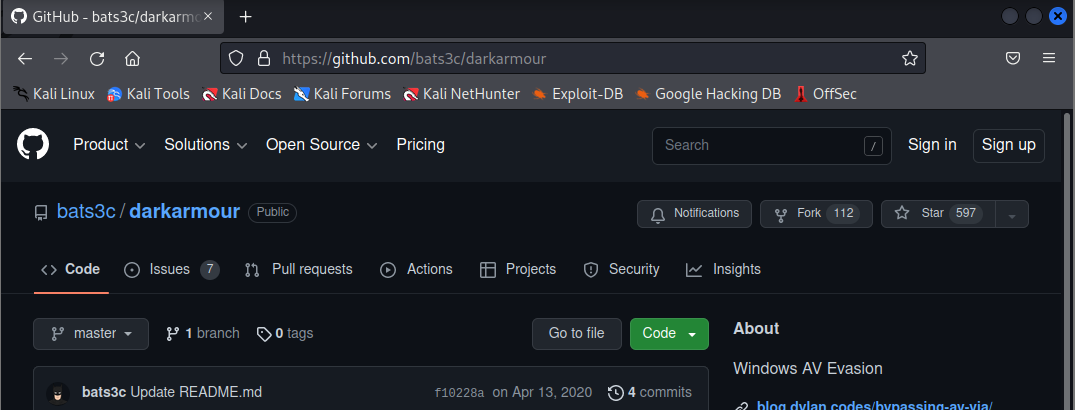
### a. Actualitza repositoris —> apt update

### 

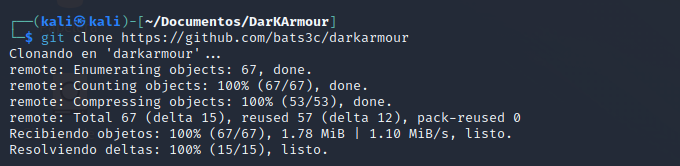
### b. Descarrega’t git —> apt install git



### c. Busca a google —> github DarkArmour, i trobaràs l’enllaç a la plana del projecte

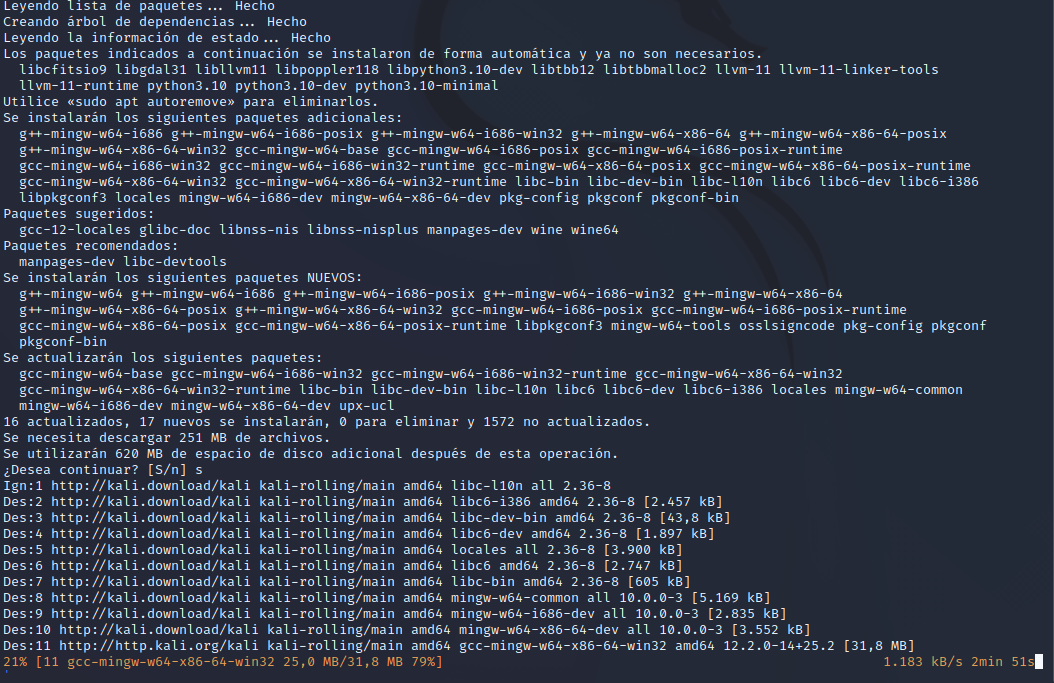


### d. Clona’l —> git clone adreça\_del\_projecte.git



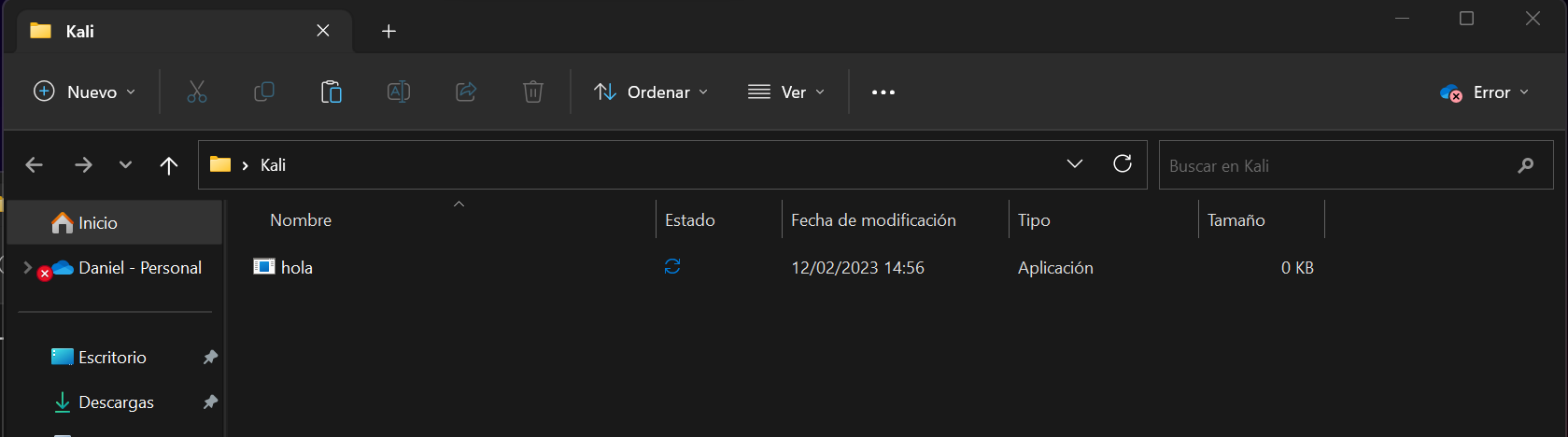
### e. DarkArmour necessita que també tinguem instal·lats diversos paquets auxiliars, executa la següent sentència per a instal·lar-los: apt install mingw-w64-tools mingw-w64-common g++-mingw-w64 gcc-mingww64 upx-ucl osslsigncode

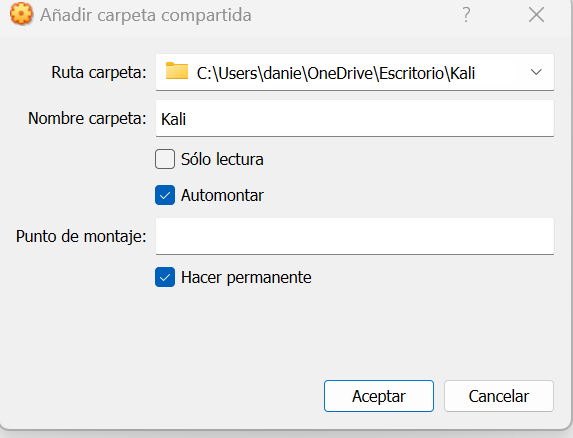


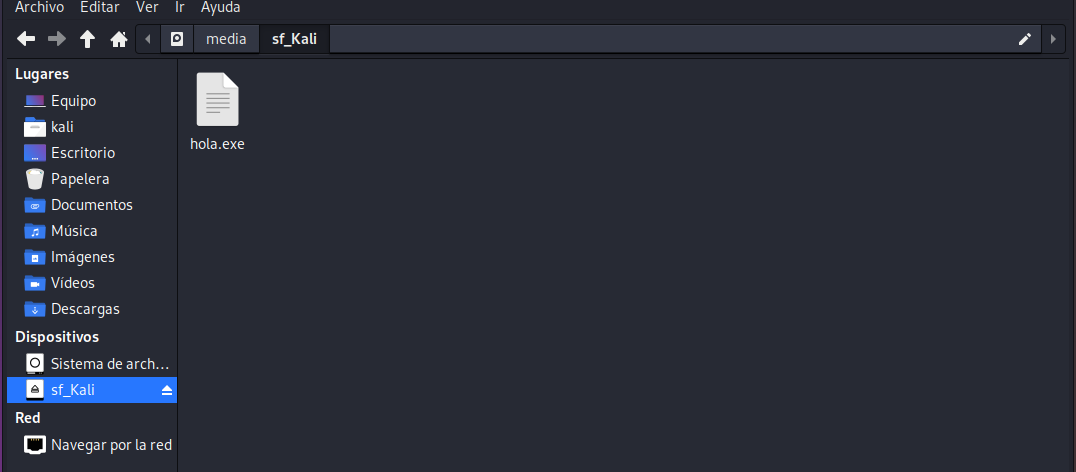


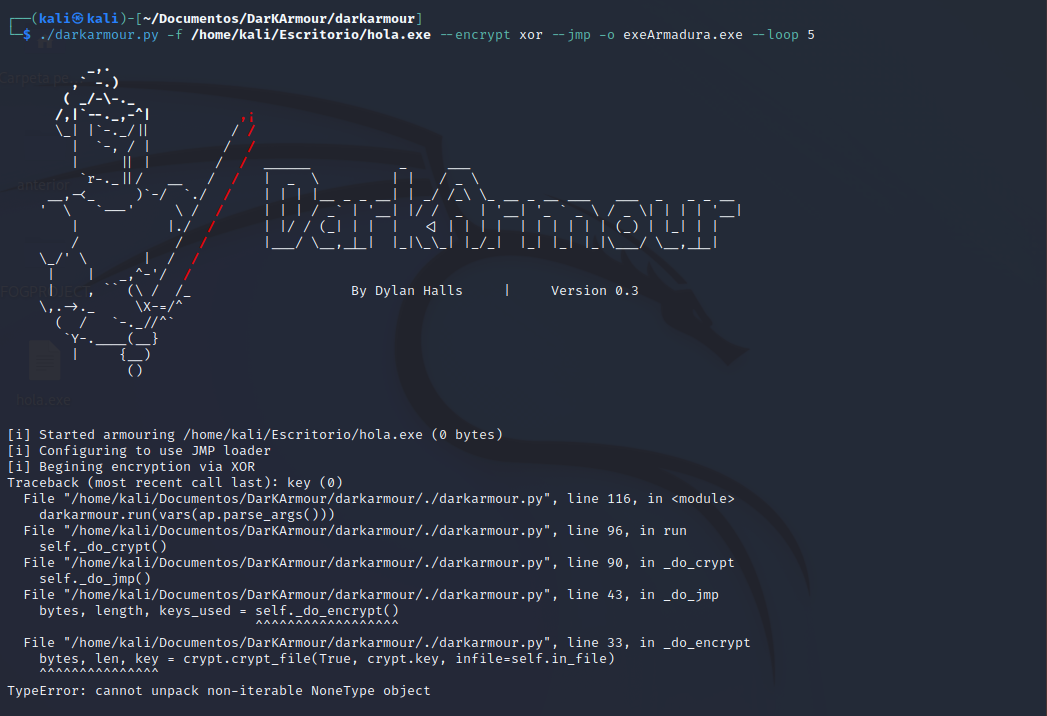
### f. Un cop instal·lat tot, entra a la carpeta darkarmour —> cd darkarmour

### g. Per posar una armadura al teu fitxer maliciós

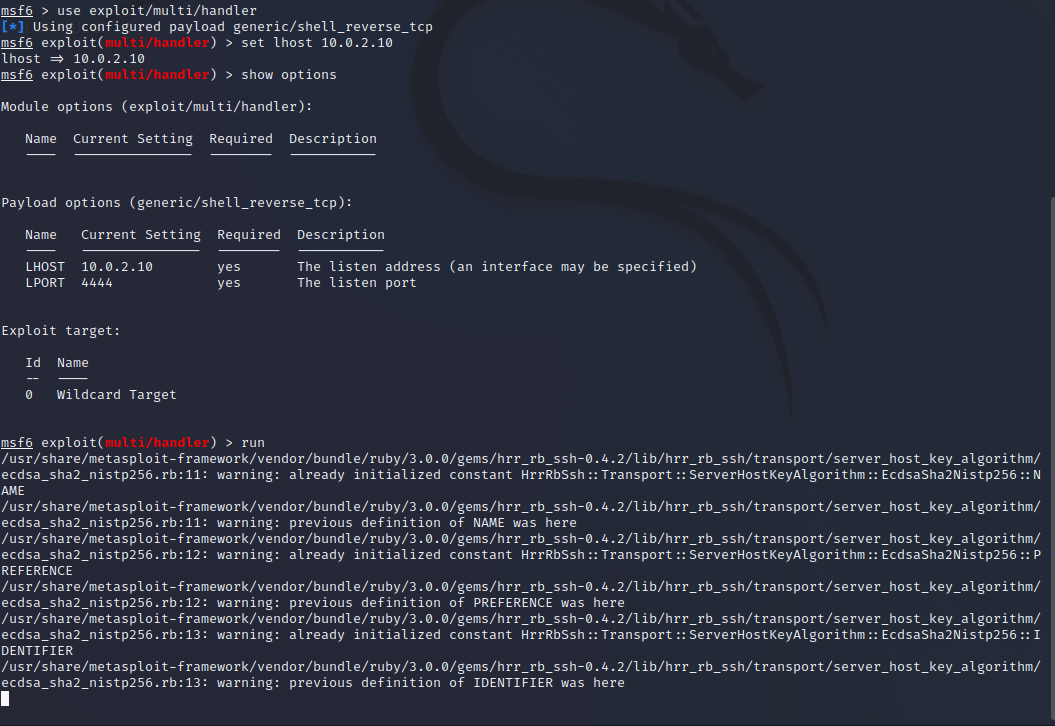


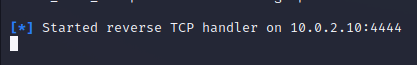






### h. Posa la màquina atacant en escolta (revisa els passos de l’exercici 1)





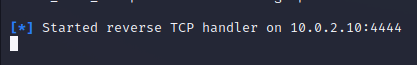
### i. Passa el malware a la víctima i executa’l.

### 

### 

### 

### j. Comprova que es crea una connexió reversa cap a l’atacant.



No es crea una connexió reversa cap a l’atacant.

### k. Has pogut esquivar l’antivirus i/o Windows Defender? Raona la resposta

A l’hora de descarregar el arxiu amb el windows defender i el firewall l’esquiva, però no funciona a l’hora de fer la connexió reversa.

# Exercici 5 – Altres eines d’ofuscació

### Explica breument què ofereixen els següents projectes que pots trobar a GitHub:

### – RedNeuron

Ofereix una biblioteca de xarxes neuronals artificials per a Python amb una varietat d'algorismes d'aprenentatge profund i tècniques d'entrenament, fet que el converteix en una eina útil per a la construcció de models personalitzats en aplicacions de visió per ordinador, processament de llenguatge natural i altres camps .

### – Villain

Escaneig de ports: Villain permet fer escaneigs de ports en una xarxa o sistema per identificar possibles punts d'entrada.

Detecció de vulnerabilitats: El projecte inclou una varietat d'eines per detectar vulnerabilitats a aplicacions web i servidors.

Creació d'exploits: Villain proporciona eines per crear exploits personalitzats i aprofitar vulnerabilitats identificades.

Força bruta: El projecte inclou eines per fer atacs de força bruta en contrasenyes i credencials.

Anonimat: Villain inclou eines per mantenir l'anonimat de l'atacant durant els atacs.

### – Hyperion

Sincronització amb el contingut de pantalla: Hyperion utilitza maquinari de captura de vídeo per analitzar el contingut d'una pantalla i sincronitzar-ne els efectes.

Personalització d'efectes d'il·luminació: Hyperion permet crear efectes d'il·luminació personalitzats que es poden ajustar segons les preferències de l'usuari.

Integració amb plataformes d'entreteniment: El projecte s'integra amb plataformes d'entreteniment populars, com Kodi, per proporcionar una experiència d'il·luminació ambiental en temps real.

Compatibilitat amb maquinari: Hyperion és compatible amb una àmplia varietat de maquinari, inclosos dispositius de captura de vídeo, plaques de LED i altres components d'il·luminació.

Comunitat activa: El projecte compta amb una comunitat activa de desenvolupadors i usuaris que contribueixen al desenvolupament i suport continu de l'eina.

### – Fud payload generator

Generació de diferents tipus de payloads: PayGen permet generar diferents tipus de payloads, incloent backdoors, codi maliciós (malware), scripts maliciosos, i més.

Personalització de payloads: L'eina permet personalitzar els payloads generats per adaptar-se als requisits específics de l'atac o la prova de penetració.

Compatibilitat amb diferents sistemes operatius: PayGen és compatible amb diferents sistemes operatius, incloent Windows, Linux i MacOS.

Fàcil d'usar: La interfície d'usuari de PayGen és intuïtiva i fàcil d'usar, cosa que fa que la generació de payloads personalitzats sigui accessible fins i tot per a aquells que no tenen experiència en programació.

Llicència de codi obert: El projecte és de codi obert, cosa que significa que qualsevol persona pot contribuir al desenvolupament de l'eina o modificar-la segons les necessitats.

### – MSFMania

Automatització de tasques: MsfMania automatitza tasques comunes de Metasploit, com ara la selecció d'exploits, l'elecció d'objectius, la configuració de payloads i l'execució de mòduls.

Interfície de línia d'ordres simplificada: L'eina proporciona una interfície de línia d'ordres més fàcil d'usar i amigable per a l'usuari que la interfície de línia d'ordres de Metasploit.

Compatibilitat amb diferents sistemes operatius: MsfMania és compatible amb diferents sistemes operatius, incloent Windows, Linux i MacOS.

Llicència de codi obert: El projecte és de codi obert, cosa que significa que qualsevol persona pot contribuir al desenvolupament de l'eina o modificar-la segons les necessitats.

Millora de la productivitat: MsfMania ajuda a millorar la productivitat dels usuaris en simplificar l'ús de Metasploit Framework, cosa que pot estalviar temps i esforç.

### – Python Obfuscator

Ofuscació del codi: El projecte ofereix diferents eines i biblioteques d'ofuscació de codi per a Python, que permeten als usuaris protegir el codi de l'enginyeria inversa i la còpia no autoritzada.

Compatibilitat amb diferents versions de Python: La majoria de les eines i biblioteques d'ofuscació són compatibles amb diferents versions de Python, incloent-hi Python 2.x i Python 3.x.

Fàcil de fer servir: Moltes de les eines ofertes són fàcils dusar i es poden integrar fàcilment en els fluxos de treball existents de desenvolupament de Python.

Llicència de codi obert: El projecte és de codi obert, cosa que significa que qualsevol persona pot contribuir al desenvolupament de les eines o biblioteques o modificar-les segons les necessitats.

– ...

—> Si t’atreveixes... prova’n algun!