1 ASIX

**MÒDUL 16: CIBERSEGURETAT I HACKING ÈTIC**

ACTIVITAT 1.5: Scanning de ports

línea horizontal

# 

**Alumne**: Daniel Mascarilla del Olmo

**Professor**:Sergi Andrés

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

**ÍNDEX**

[**Exercici 1 – Ports TCP/UDP**](#_npr0sbtyc7op) **4**

[a. Quins són els 2 protocols que actuen a nivell de transport?](#_ygnbwzrkivjx) 4

[b. Quins són els Well-Known ports més habituals?](#_bm4zhpdq1k2h) 4

[c. Què significa que un port estigui obert?](#_9ccgxe5peb6u) 4

[d. Què significa que un port estigui tancat?](#_tf9gfyu7a32j) 4

[e. Què significa que un port estigui filtrat?](#_67gxy9dver3t) 4

[f. Quina és la eina més famosa per saber l’estat d’un port remot?](#_dgco337wy8et) 4

[**Exercici 2 – Scanner de ports Nmap**](#_l6x1581h936) **5**

[a. Troba tots els hosts (alive) de la teva xarxa RedNat amb un Nmap de tipus ICMP. (Raona la resposta).](#_da4zf6pnbam7) 5

[b. Busca tots els ports oberts de la teva màquina Windows amb un escaneig que sigui el més ràpid possible.](#_48hni1vlkerv) 5

[c. Si no has trobat res abans, apaga el Firewall i torna-ho a provar](#_1r0v8xz2xuvx) 6

[d. Busca tots els ports oberts de cada una de les màquines de la teva xarxa RedNat.](#_bhov3625pd0v) 6

[e. Busca els ports oberts i la versió de servei que s’executa en aquell port, de totes les màquines de la teva xarxa RedNat.](#_vpp1mhwoj3bi) 6

[**Exercici 3 – Scanner de ports Nmap a servidor extern**](#_v16882e8pzqh) **8**

[a. Utilitzant nmap mira quins ports té oberts el servidor scanme.nmap.org](#_idex9m8elmds) 8

[b. Podries dir quina versió de software s’està executant en cada port obert de scanme.nmap.org](#_gm5yq7k6jbw2) 9

[**Exercici 4 – TCP three-way handshake**](#_rrefjjeomm9m) **10**

[a. Executar un nmap de tipus Half-scan, per a trobar tots els ports oberts de la teva xarxa RedNat.](#_sxpg2j661kmq) 10

[→ Si no trobes ports oberts, canvia la víctima i fes-ho sobre scanme.nmap.org](#_p0lee7p95pkp) 10

[b. Capturar amb el Wireshark els paquets](#_fdhbdrb77fb9) 10

[c. Comentar els paquets del three-way handshake capturats (SYN, SYN+ACK, RST)](#_ydyo091cpngi) 11

[**Exercici 5 – Funcions avançades de nmap**](#_65x8wdy35hxk) **12**

[a. Scan d’un rang de ports d’una adreça IP concreta](#_yqh3v2i1f92l) 12

[b. Scan del port 80 de totes les IPs d’una xarxa](#_lt4admuq1mjf) 12

[c. Buscar amb nmap la versió de servei que s’executa en un port](#_c289923yzsda) 12

[**Exercici 6 – Hping3**](#_a0rtfw51uy8u) **14**

[a. Busca per a que serveix la eina hping3](#_jmq60l5stm4t) 14

[b. Mostra diversos exemples on es vegi el seu funcionament](#_7lv6fm5hd8lc) 14

[c. Comprova que funciona llistant els ports oberts de les teves màquines de la xarxa RedNat](#_nvn1x9myau3a) 15

[**Exercici 7 – Netcat**](#_24itgqzeairl) **16**

[a. En una màquina Windows 10 instal·la Netcat (Recorda que segons el sistema, també pot rebre el nom de ncat o nc) (Netcat es considera una eina de hacking i segurament Windows posarà problemes per a instal·lar-la, caldrà deshabilitar Windows Defender i el Firewall).](#_tshyj1b3yaz8) 16

[b. Des de la màquina Windows 10, utilitzant Netcat, obre el port 333 i fes que estigui en espera un cmd de Windows. Per a aconseguir-ho, executa la següent comanda des d’un terminal de Windows 10 à nc -lvp 333 -e cmd](#_avela4ajr4zw) 17

[c. Des de la màquina atacant Kali Linux, connecta’t a la víctima al port 333 (suposem que la víctima té la IP 10.0.2.200). Per a aconseguir-ho, executa la següent comanda à nc 10.0.2.200 333](#_dpgw44rw1z94) 17

[d. Automàticament podrem executar comandes a través de cmd des de Kali Linux sobre la màquina Windows 10. Per exemple, des de Kali, a través del cmd obert, ves a l’escriptori de Windows i posa-hi un fitxer anomenat à Hacked.txt Per fer-ho, pots teclejar: echo Aquest sistema ha estat hackejat! > Hacked.txt](#_cpi3gkbjyvtq) 17

[e. Comprova des de la màquina Windows 10 que en l’escriptori s’ha creat aquest fitxer i que per tant la màquina ha estat hackejada remotament.](#_cso5uoi3btn6) 17

# Exercici 1 – Ports TCP/UDP

## a. Quins són els 2 protocols que actuen a nivell de transport?

El UDP (Protocol de datagrama del usuari) i el TCP (protocol de control de transmisió)

## b. Quins són els Well-Known ports més habituals?

HTTP (port 80), HTTPS (port 443), FTP (port 21), FTPS/SSH (port 22) POP3 (port 110), POP3 SSL (port 995), IMAP (port 143), IMAP SSL (port 993), SMTP (port 25), SMTP SSL (port 587), MySQL (port 3306), CPanel (port 2082), CPanel SSL (port 2083), WHM (port 2086), WHM SSL (port 2087), WebDAV/WebDisk (port 2077), WebDAV/WebDisk SSL (port 2078)

## c. Què significa que un port estigui obert?

Es considera que un port està obert quan hi ha una aplicació o servei que està allotjat en aquell port, és a dir, està “escoltant” i per tant és accesible des de fora de la seva xarxa

## d. Què significa que un port estigui tancat?

Que un port estigui tancat vol dir que el servidor o la xarxa ha rebut la petició de sol·licitud, però no hi ha cap aplicació o servei escoltant en aquell port

## e. Què significa que un port estigui filtrat?

Vol dir que un Firewall ha denegat l’accés al port on està escoltant la aplicació o servei.

## f. Quina és la eina més famosa per saber l’estat d’un port remot?

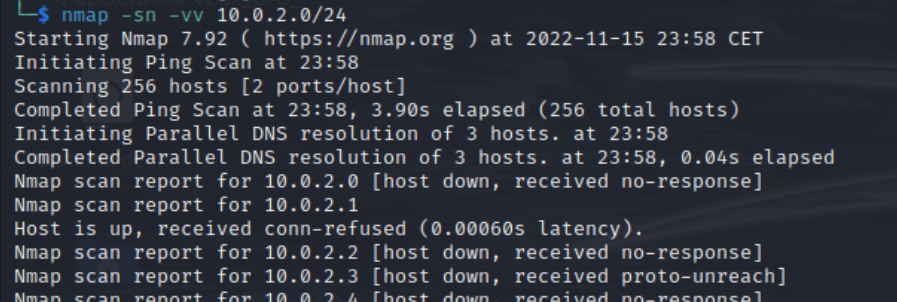
NMap

# Exercici 2 – Scanner de ports Nmap

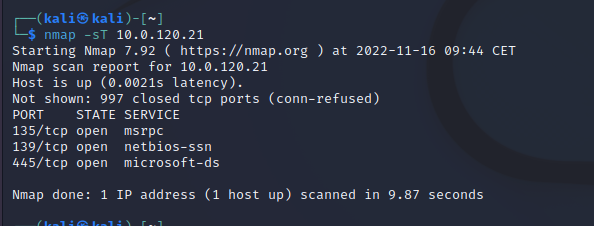
Utilitzant la eina Nmap executa les següents operacions per a trobar els hosts que hi ha connectats a la teva xarxa Red Nat.

Recorda que com a mínim hauries de tenir enceses una màquina Kali Linux i una màquina virtual Windows. A més d’aquests Virtual Box també crea el Gateway i potser el servidor DHCP (segons si el tens activat o no).

## a. Troba tots els hosts (alive) de la teva xarxa RedNat amb un Nmap de tipus ICMP. (Raona la resposta).



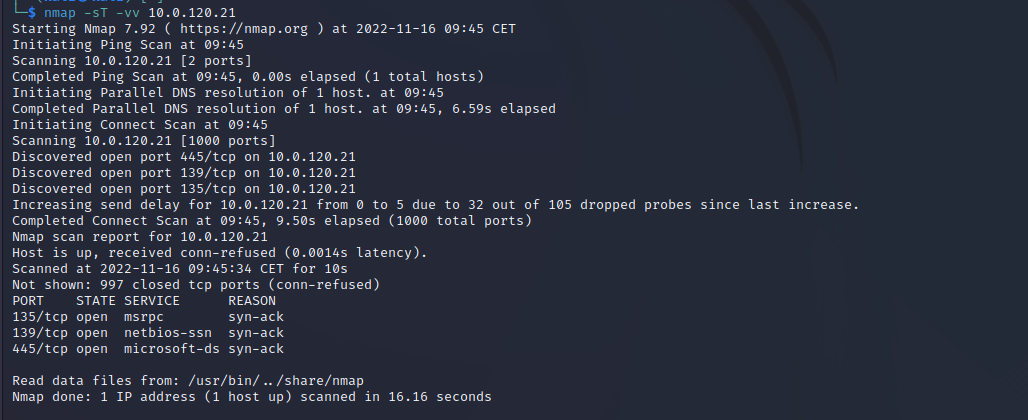
## b. Busca tots els ports oberts de la teva màquina Windows amb un escaneig que sigui el més ràpid possible.



## c. Si no has trobat res abans, apaga el Firewall i torna-ho a provar

Ja ha trobat coses abans perquè el firewall estava apagat.

## d. Busca tots els ports oberts de cada una de les màquines de la teva xarxa RedNat.



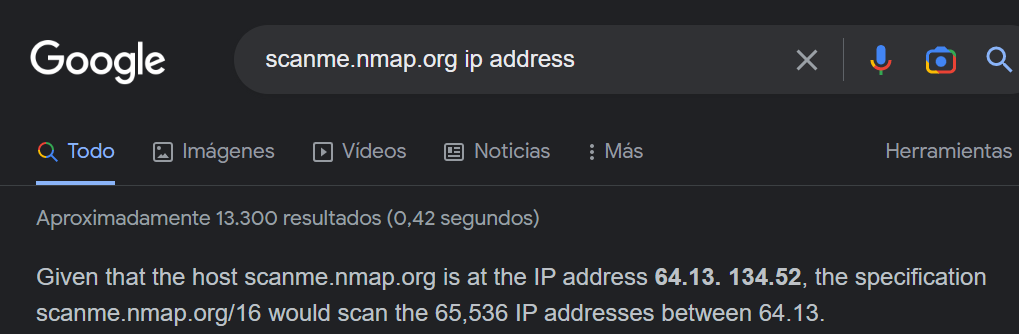
## e. Busca els ports oberts i la versió de servei que s’executa en aquell port, de totes les màquines de la teva xarxa RedNat.

## 

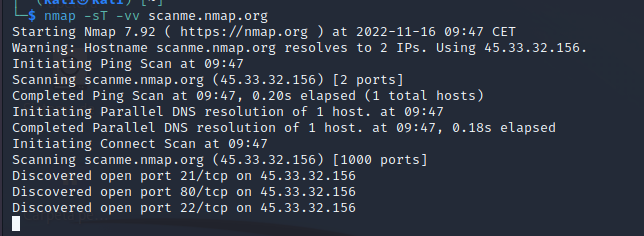
## 

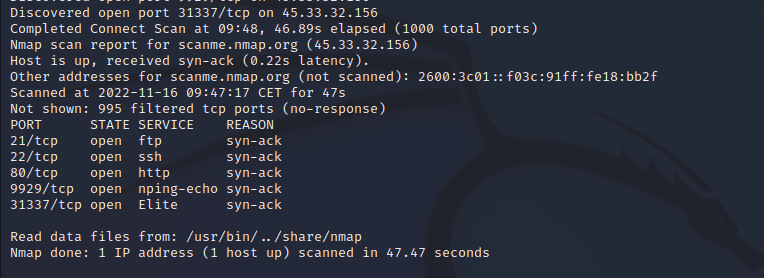
# Exercici 3 – Scanner de ports Nmap a servidor extern

En aquest exercici utilitzarem Nmap per obtenir la màxima informació d’un servidor remot: scanme.nmap.org



## a. Utilitzant nmap mira quins ports té oberts el servidor scanme.nmap.org





## b. Podries dir quina versió de software s’està executant en cada port obert de scanme.nmap.org

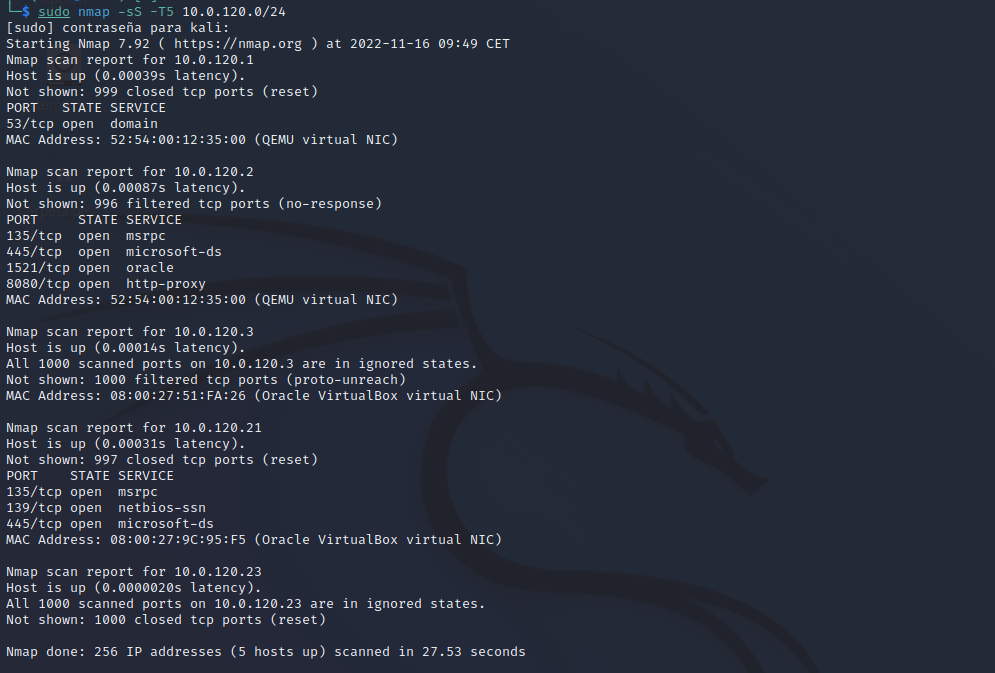
Podem deduïr que la versió de software que s’està executant en els ports és la TCP.

# Exercici 4 – TCP three-way handshake

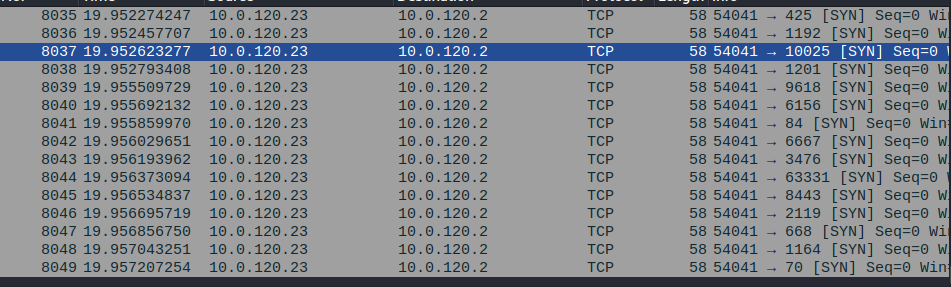
Utilitzant la eina Wireshark demostra com Nmap troba els ports oberts de les màquines d’una xarxa en el procés de three-way handshake de TCP. Concretament has de fer

## a. Executar un nmap de tipus Half-scan, per a trobar tots els ports oberts de la teva xarxa RedNat.

### → Si no trobes ports oberts, canvia la víctima i fes-ho sobre scanme.nmap.org



## b. Capturar amb el Wireshark els paquets



## c. Comentar els paquets del three-way handshake capturats (SYN, SYN+ACK, RST)

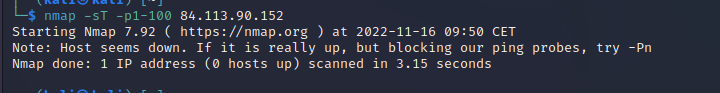
Observem que Kali envia paquets a la 10.0.120.2 mitjançant una eina anomenada sync, aquesta envia un sync a kali i kali envia un restabliment per evitar establir la connexió entre “victima” i “hacker”.

## 

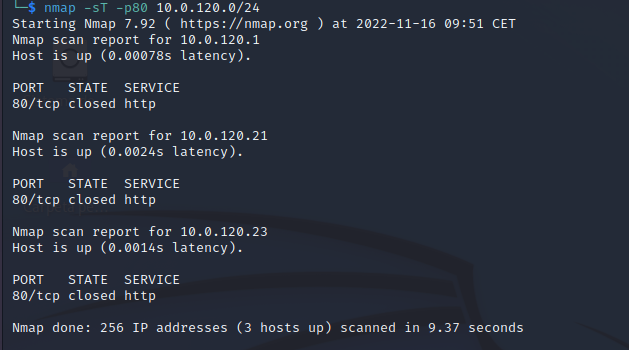
# Exercici 5 – Funcions avançades de nmap

Busca com fer les següents operacions amb nmap:

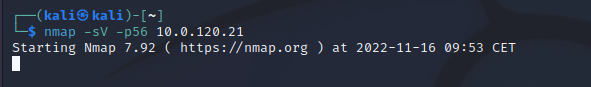
## a. Scan d’un rang de ports d’una adreça IP concreta

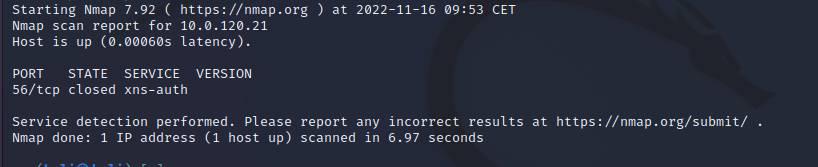


## b. Scan del port 80 de totes les IPs d’una xarxa



## c. Buscar amb nmap la versió de servei que s’executa en un port



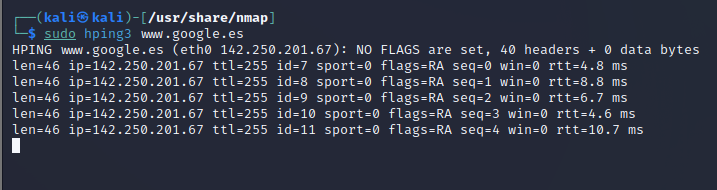


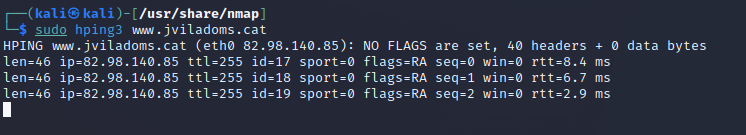
# Exercici 6 – Hping3

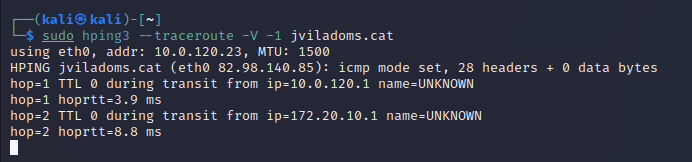
## a. Busca per a que serveix la eina hping3

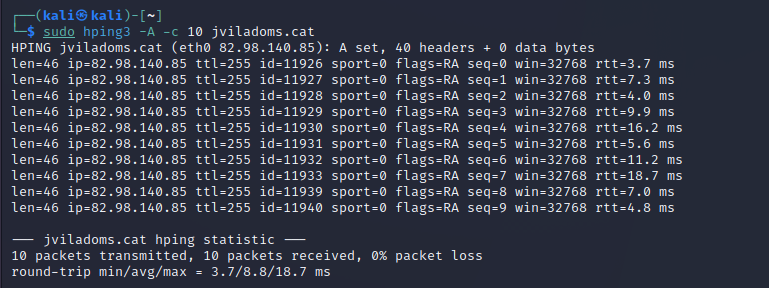
L’eina hping3 és una aplicació que s’executa a través de linia de comandes que ens permet analitzar i ensamblar paquets del tipus TCP/IP d’una manera senzilla.

## b. Mostra diversos exemples on es vegi el seu funcionament







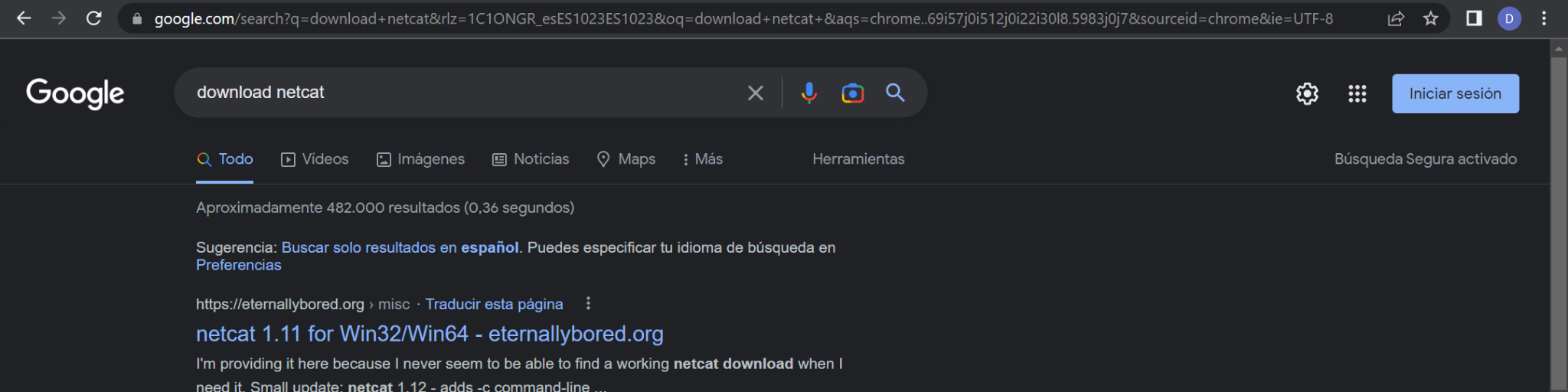


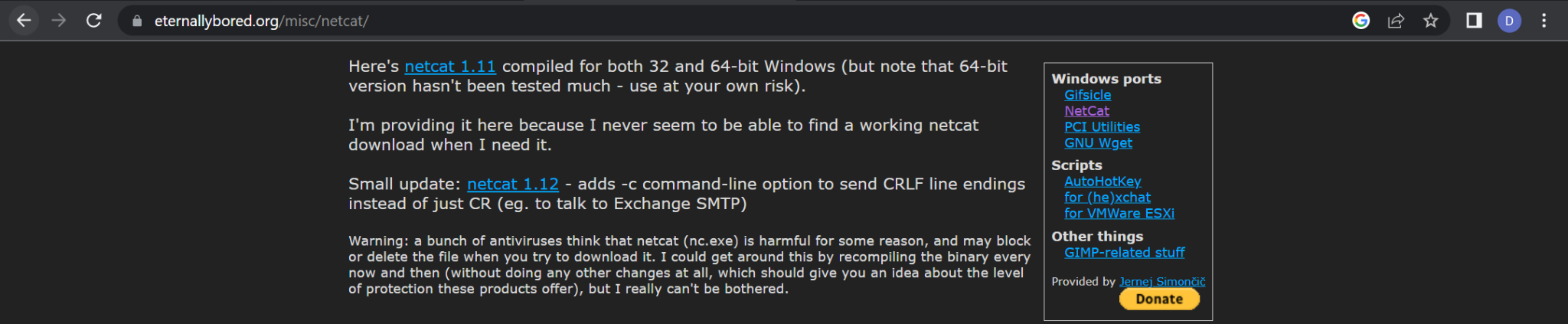
## c. Comprova que funciona llistant els ports oberts de les teves màquines de la xarxa RedNat

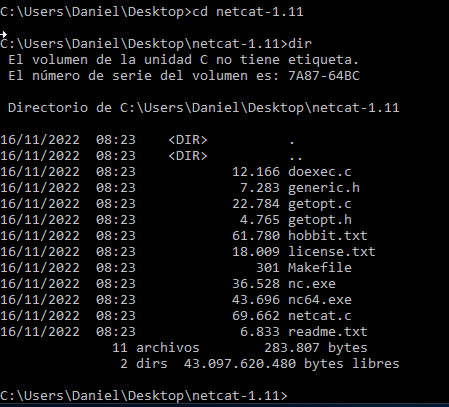
## 

# Exercici 7 – Netcat

## a. En una màquina Windows 10 instal·la Netcat (Recorda que segons el sistema, també pot rebre el nom de ncat o nc) (Netcat es considera una eina de hacking i segurament Windows posarà problemes per a instal·lar-la, caldrà deshabilitar Windows Defender i el Firewall).



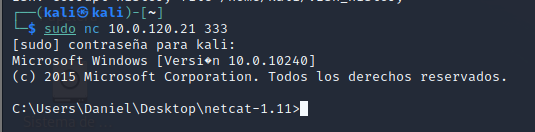




## b. Des de la màquina Windows 10, utilitzant Netcat, obre el port 333 i fes que estigui en espera un cmd de Windows. Per a aconseguir-ho, executa la següent comanda des d’un terminal de Windows 10 à nc -lvp 333 -e cmd



## c. Des de la màquina atacant Kali Linux, connecta’t a la víctima al port 333 (suposem que la víctima té la IP 10.0.2.200). Per a aconseguir-ho, executa la següent comanda à nc 10.0.2.200 333



## d. Automàticament podrem executar comandes a través de cmd des de Kali Linux sobre la màquina Windows 10. Per exemple, des de Kali, a través del cmd obert, ves a l’escriptori de Windows i posa-hi un fitxer anomenat à Hacked.txt Per fer-ho, pots teclejar: echo Aquest sistema ha estat hackejat! > Hacked.txt



## e. Comprova des de la màquina Windows 10 que en l’escriptori s’ha creat aquest fitxer i que per tant la màquina ha estat hackejada remotament.

