1 ASIX

**MÒDUL 16: CIBERSEGURETAT I HACKING ÈTIC**

ACTIVITAT 1.7: Vulnerabilitats amb NESSUS

línea horizontal

# 



**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Sergi Andrés

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

**ÍNDEX**

[**Exercici 1: Instal·lació i configuració de NESSUS**](#_dsr1qy2754jn) **3**

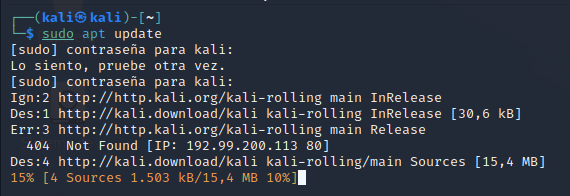
[**Exercici 2: Anàlisi de vulnerabilitats amb NESSUS**](#_j8bufoa41kot) **9**

[**Exercici 3: Metasploitable 3 Windows**](#_zotbqlr7fgz) **15**

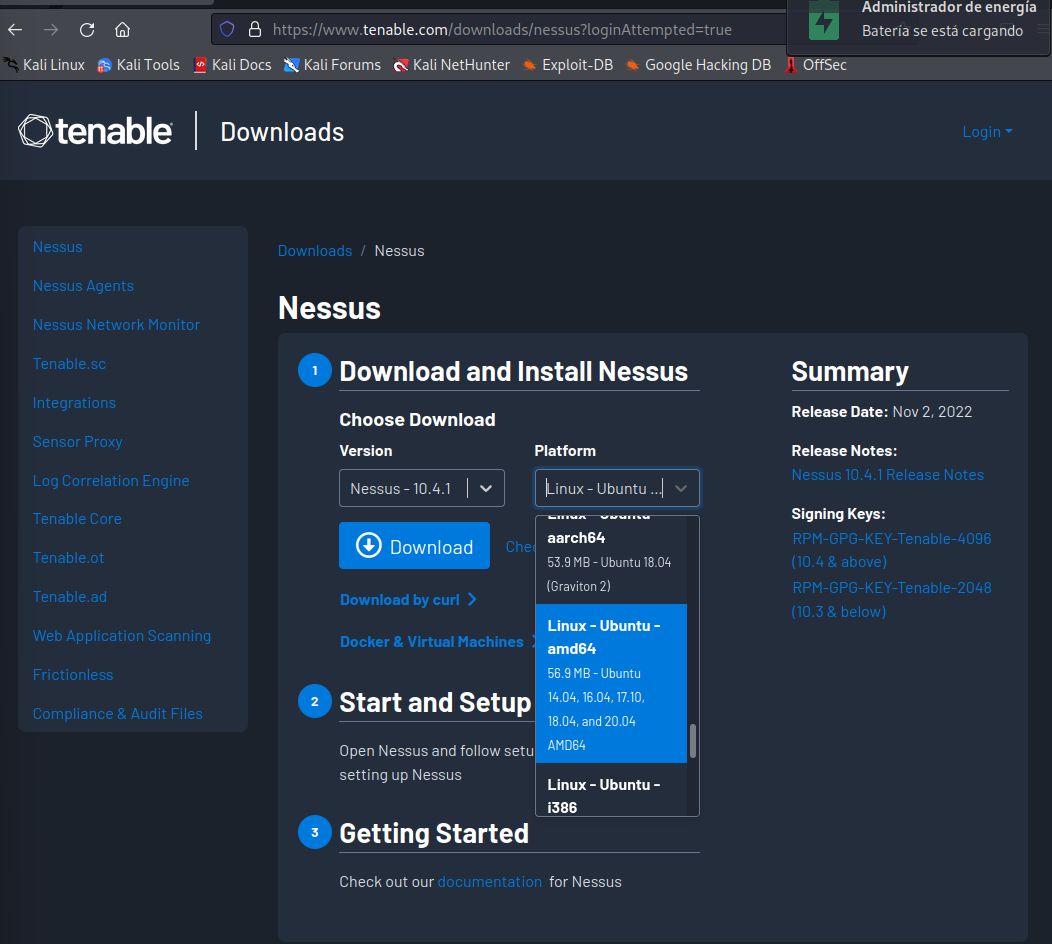
[**Exercici 4: Recordant altres eines**](#_vq6h3m9px87k) **19**

# Exercici 1: Instal·lació i configuració de NESSUS

En una màquina Kali Linux, executarem primer de tot un “sudo apt update”:



Després agafarem el arxiu de NESSUS de la pàgina mostrada a l’enunciat:

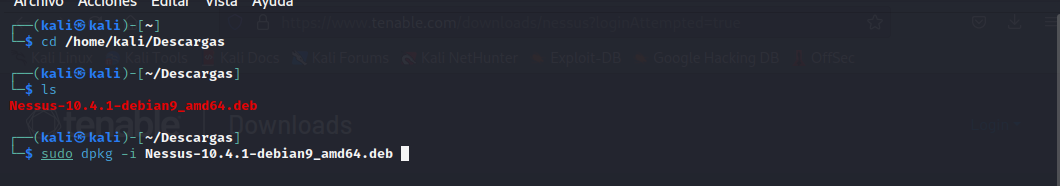


Escollirem l’opció de Linux - Debian - amd64:



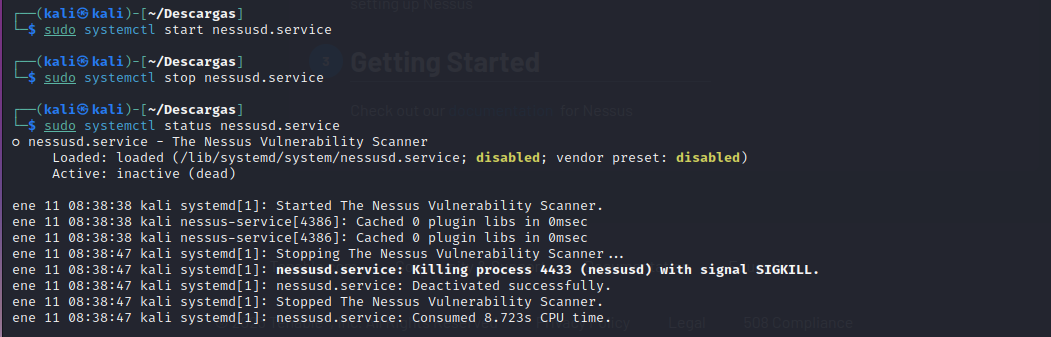


Ara anirem al directori de descarregues de kali linux i executarem la següent comanda:

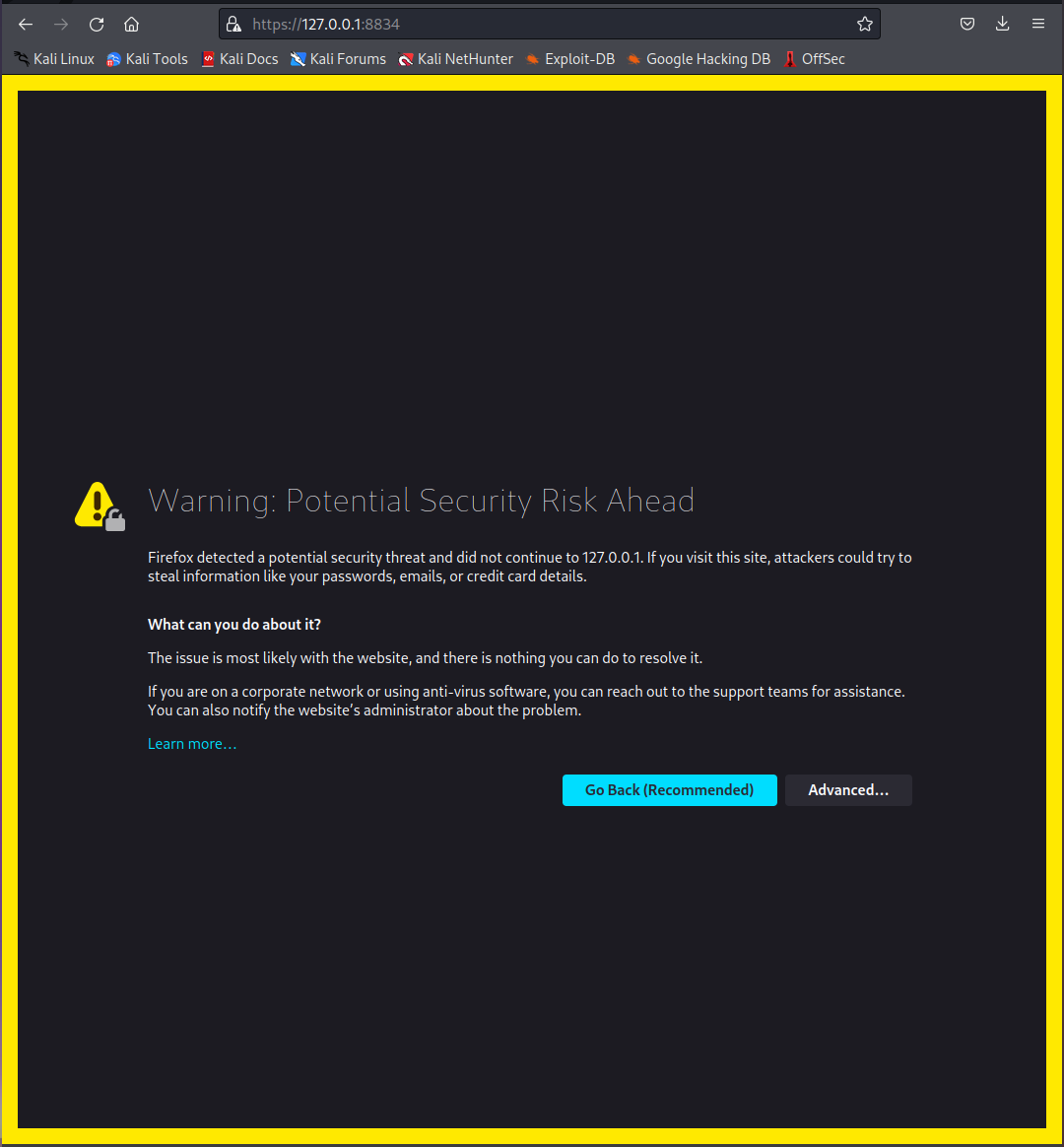




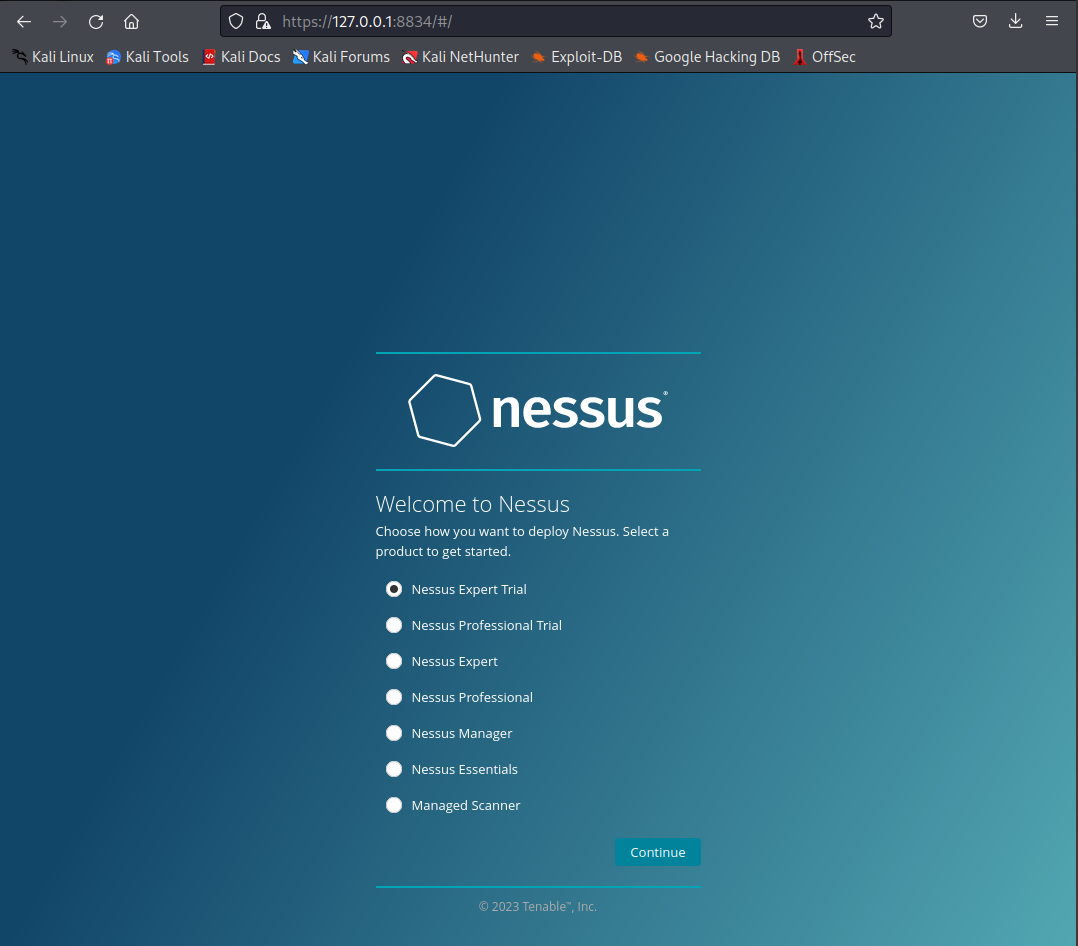
Ara executarem les comandes per iniciar, parar i mirar l’estat del nessus:



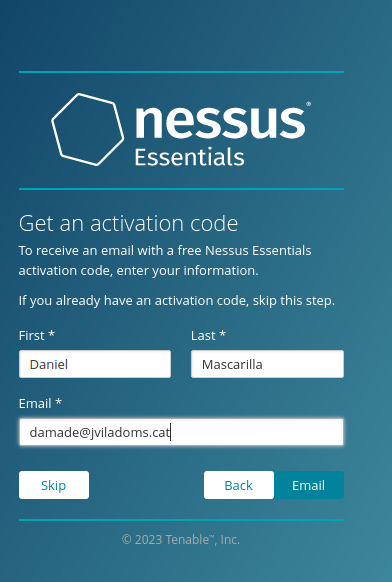
Ara obrirem el navegador web i intentarem entrar al nessus, que s’allotja en el port 8834:



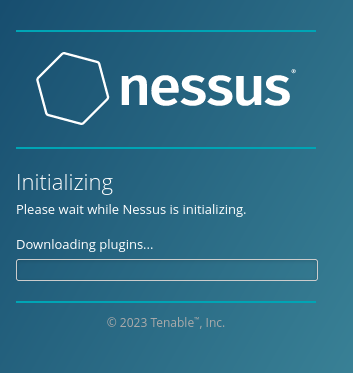
Aquesta pantalla es normal, haurem de fer clic a “Advanced” i “Accept the risk and continue”:



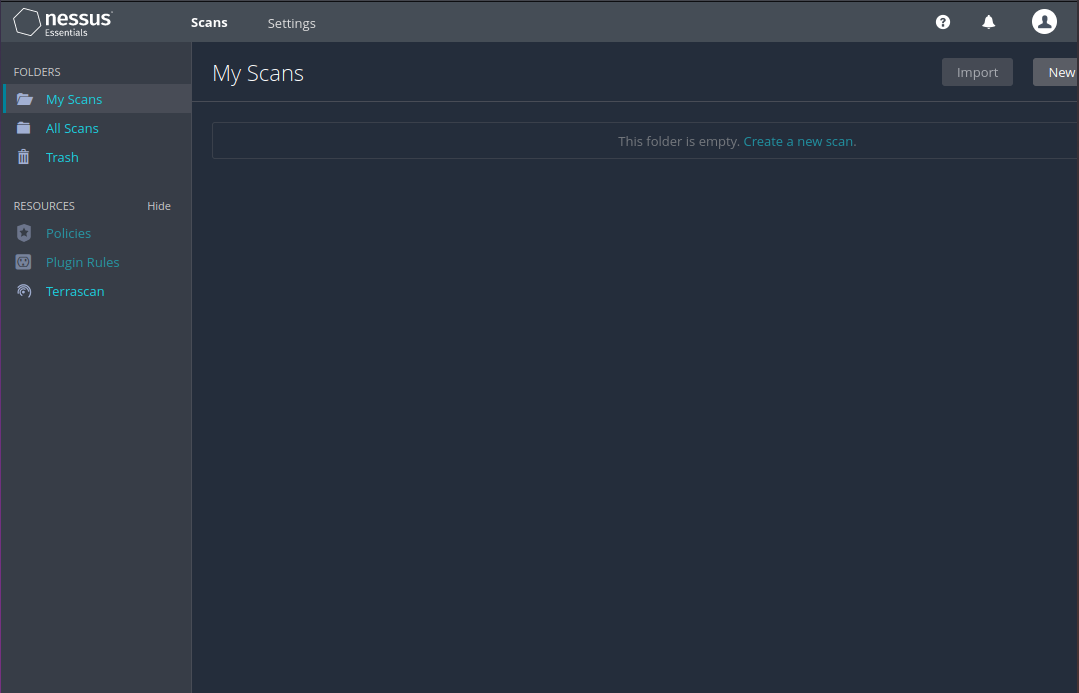
Ja serem dins de NESSUS, escollirem la versió Nessus Essentials:



Ens demana dades per el registre. Un cop ficades les dades i la confirmació, començarà la instal·lació:



Un cop acabada la instal·lació, ja serem dins de Nessus:



# Exercici 2: Anàlisi de vulnerabilitats amb NESSUS

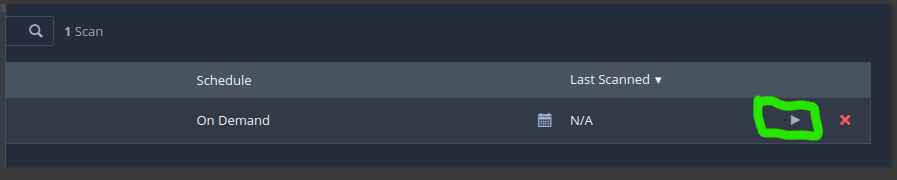
Obrirem una màquina Windows 10 i des de Kali Linux buscarem vulnerabilitats, treurem la ip de la màquina windows 10:



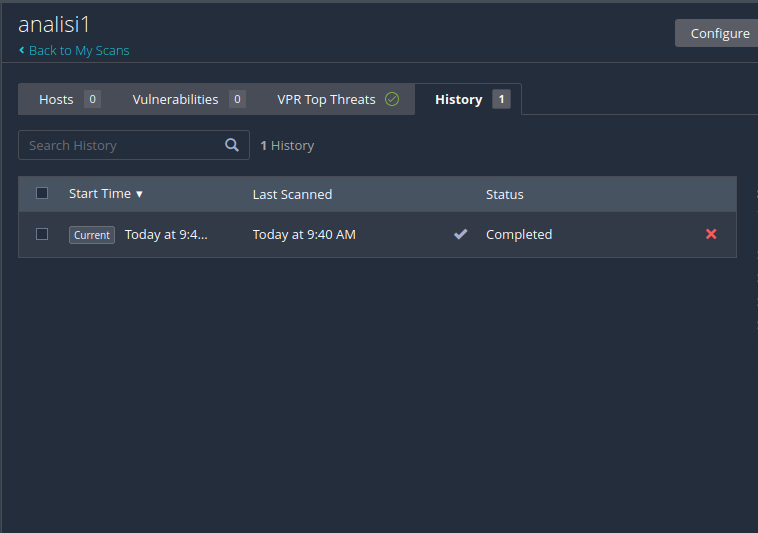
Configurarem el scan:



Guardar el scan i a la carpeta de My Scans l’executarem:

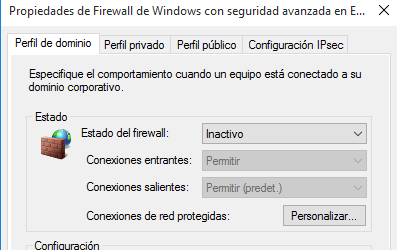


Un cop realitzat el scaneig, veurem si ha trobat alguna vulnerabilitat:

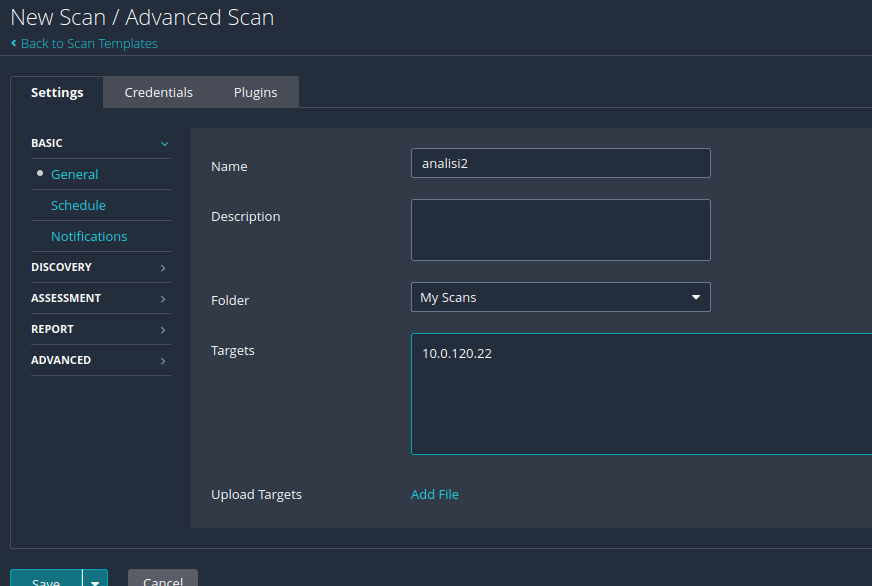


Podem veure que no ha trobat cap.

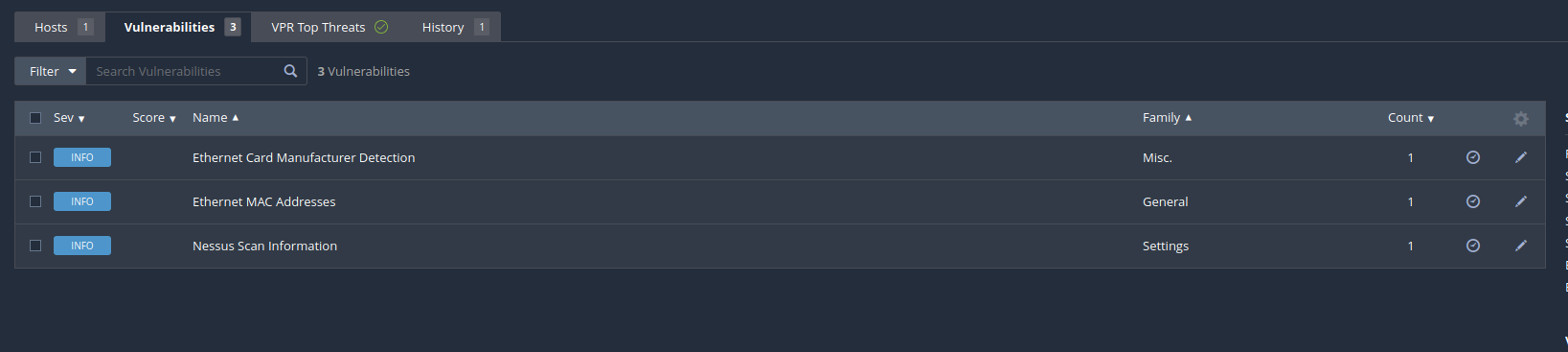
Ara probarem però desactivant el Firewall de Windows:



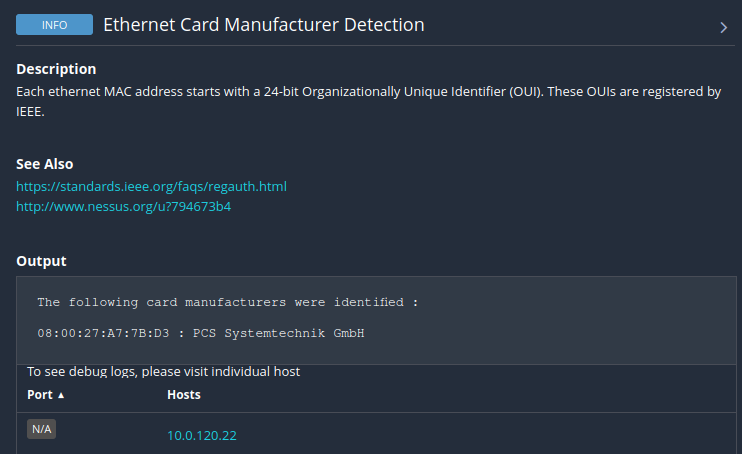
Un cop desactivat el firewall, tornarem a probar:

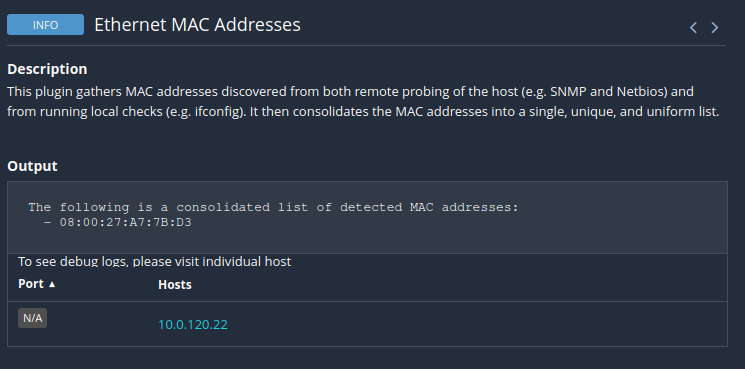


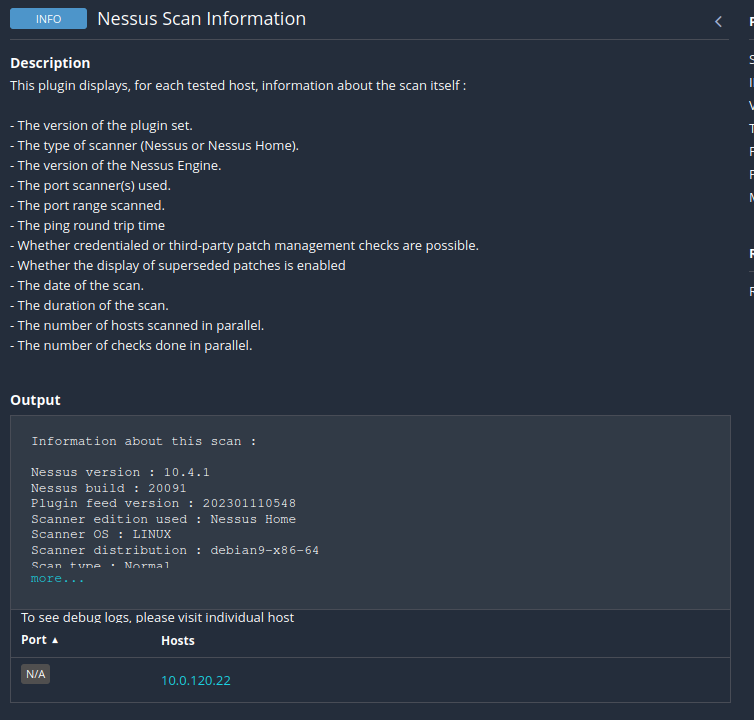
Veurem els resultats:



Ha trobat 3 vulnerabilitats, dos the Ethernet i informació sobre l’escanegi de nessus.



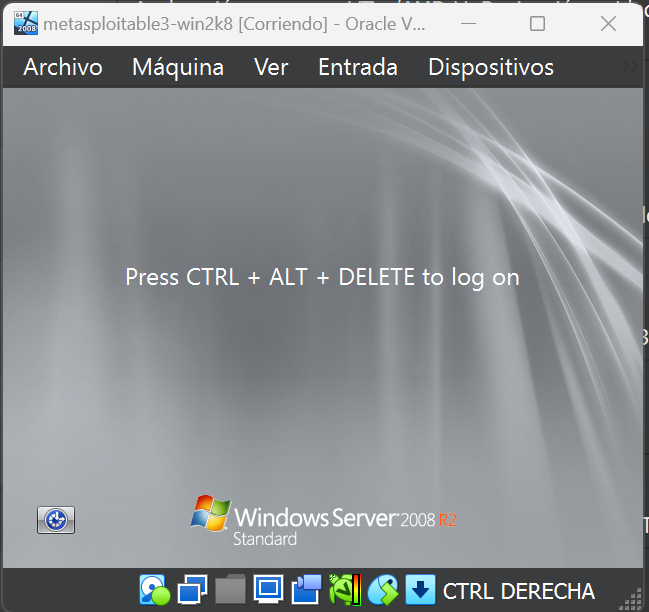




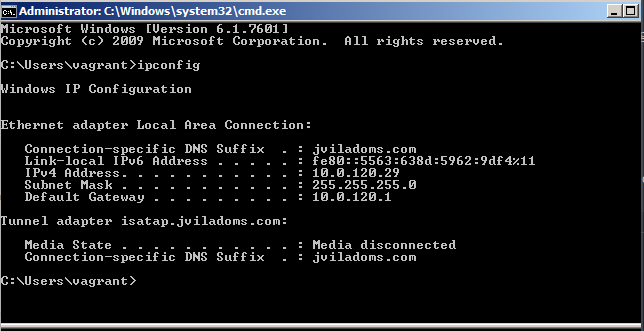
Podem observar que amb el firewall desactivat si que troba alguna vulnerabilitat més, però no ha trobat cap que sigui d’un risc mitjanament elevat.

# Exercici 3: Metasploitable 3 Windows

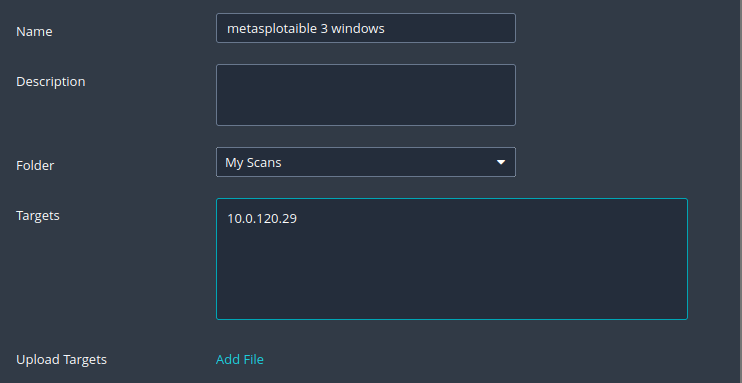
Per aquesta activitat necessitarem una màquina anomenada Metasploitable 3 versió Windows.



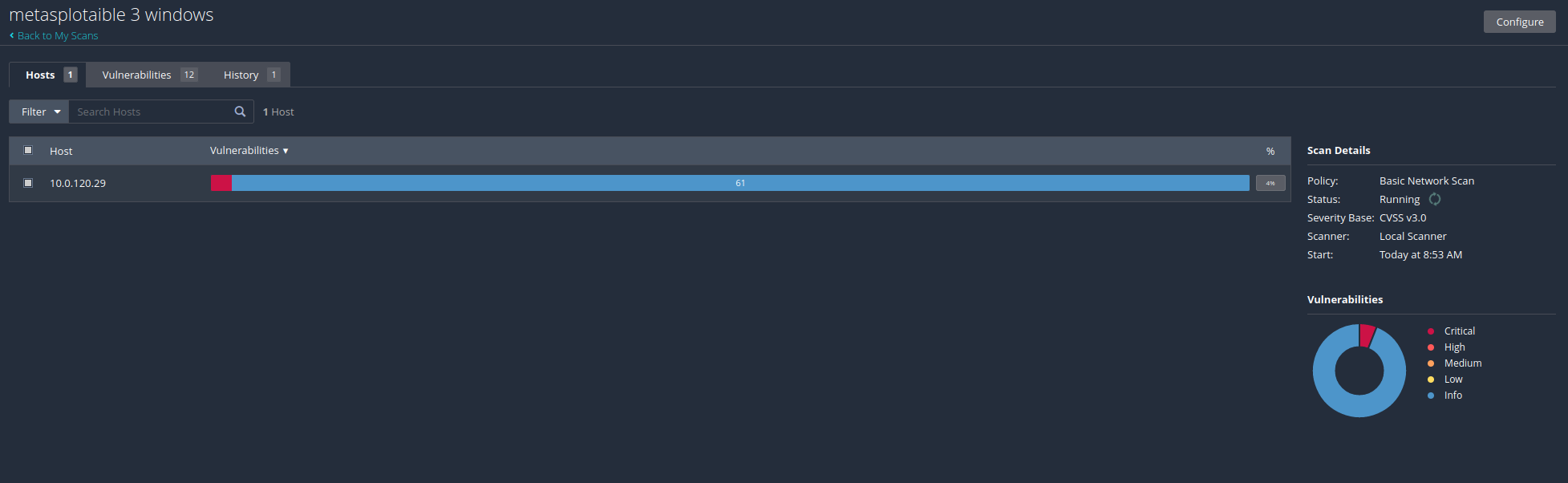
Ara amb un netdiscover descobrirem la ip de aquesta màquina per fer-li un anàlisi de vulnerabilitats.



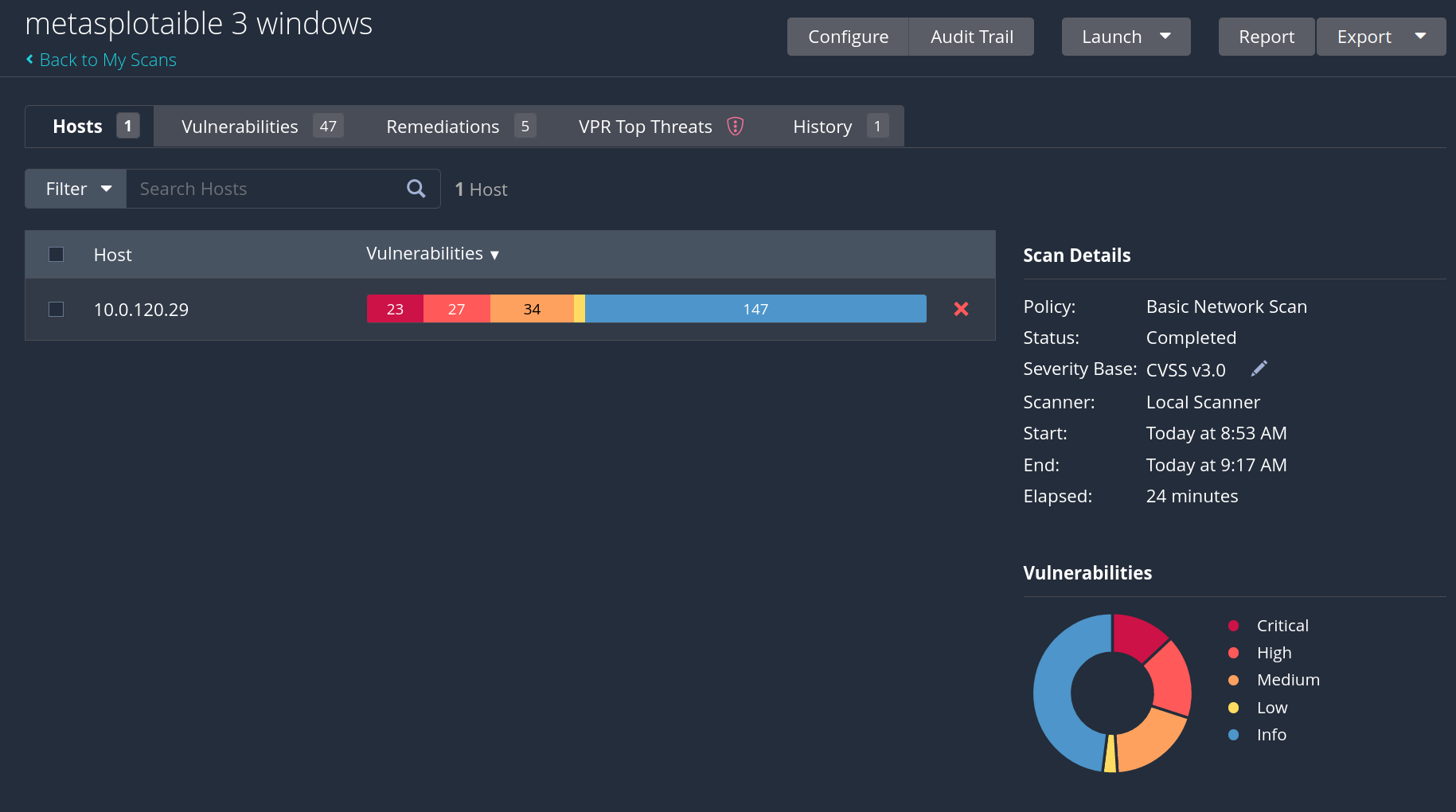
Un cop trobada la ip, farem l’anàlisi de vulnerabilitats de la màquina:



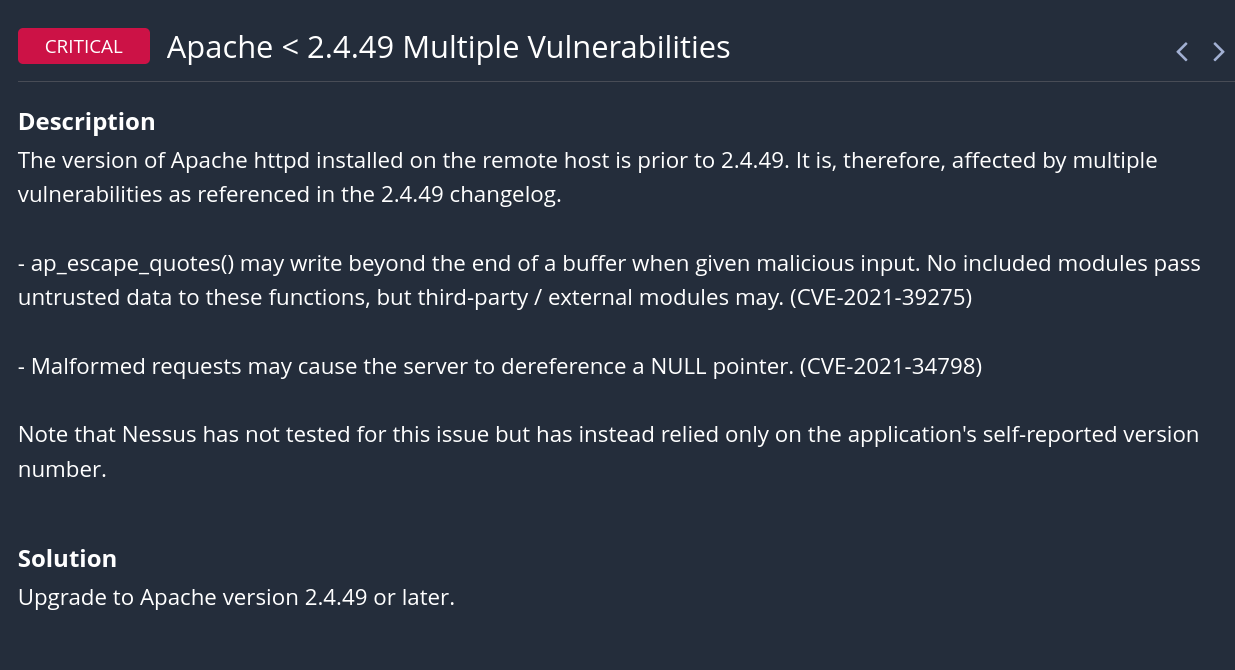
Troba bastants vulnerabilitats:



Un cop acabat, hem trobat totes aquestes vulnerabilitats:



Podrem observar, per exemple, una vulnerabilitat crítica que hem trobat,



Ens diu de que tracta la vulnerabilitat i una solució d’aquesta.

En resum, la versió d'Apache httpd instal·lada a l'amfitrió remot és anterior a la 2.4.49. Per tant, està afectat per una vulnerabilitat tal com es fa referència al registre de canvis 2.4.49.

- Una sol·licitud uri-path dissenyada pot fer que mod\_proxy reenviï la sol·licitud a un servidor d'origen escollit per l'usuari remot.

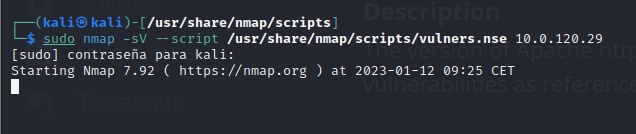
Nessus no ha provat aquest problema, sinó que només s'ha basat en el número de versió autoinformat de l'aplicació.

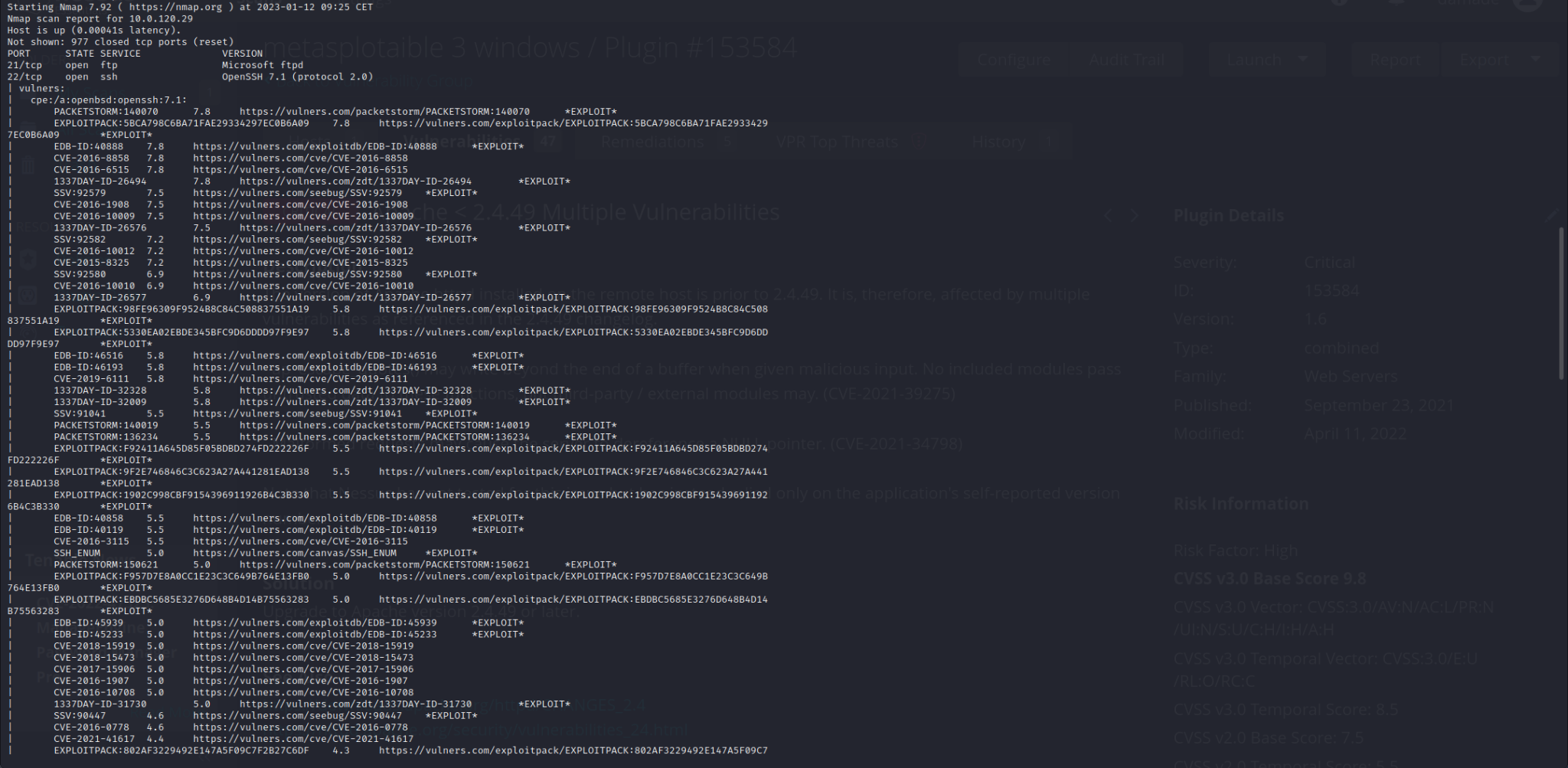
I la solució tracta de:

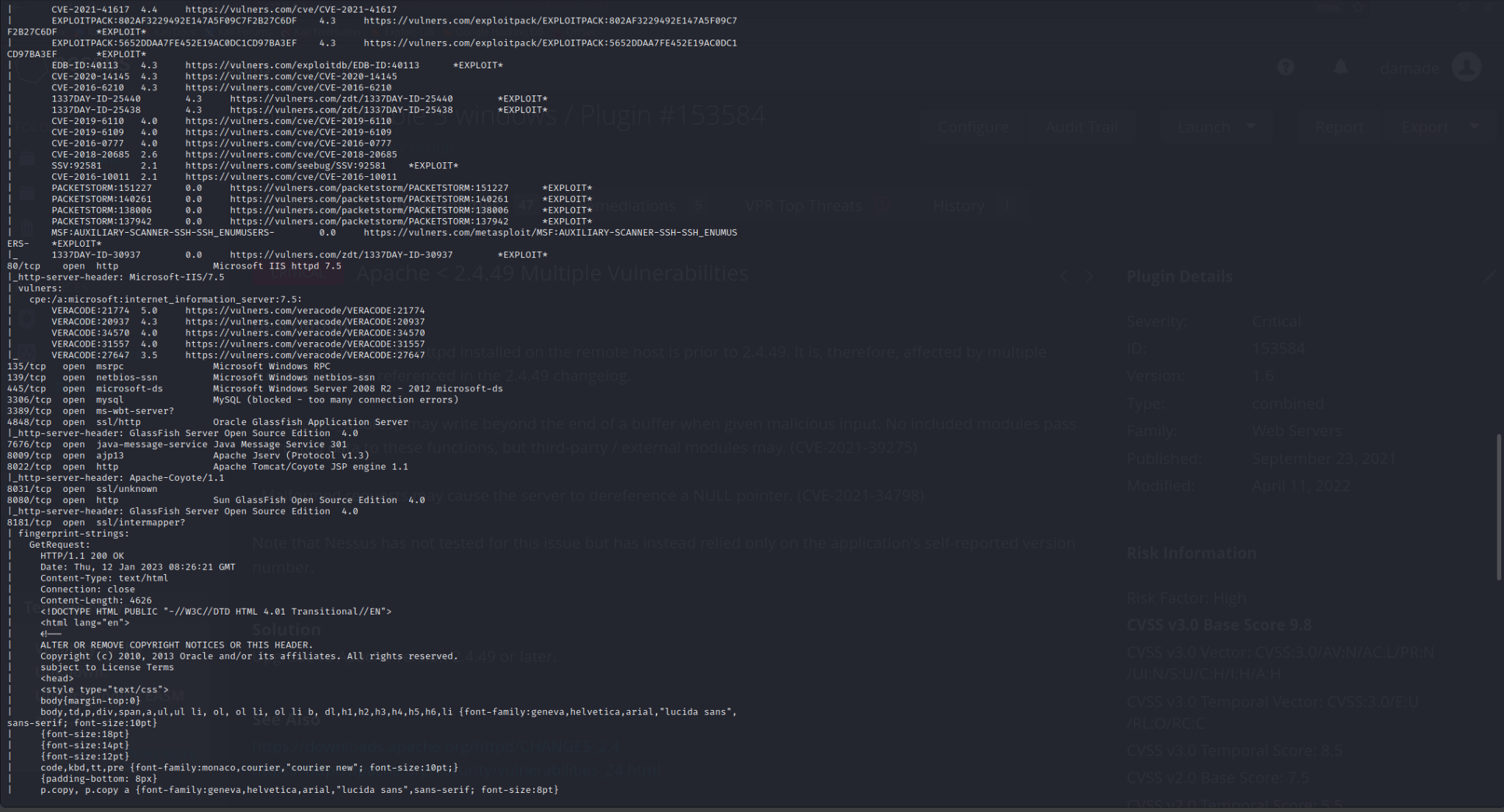
Actualitzar a la versió d'Apache 2.4.49 o posterior.

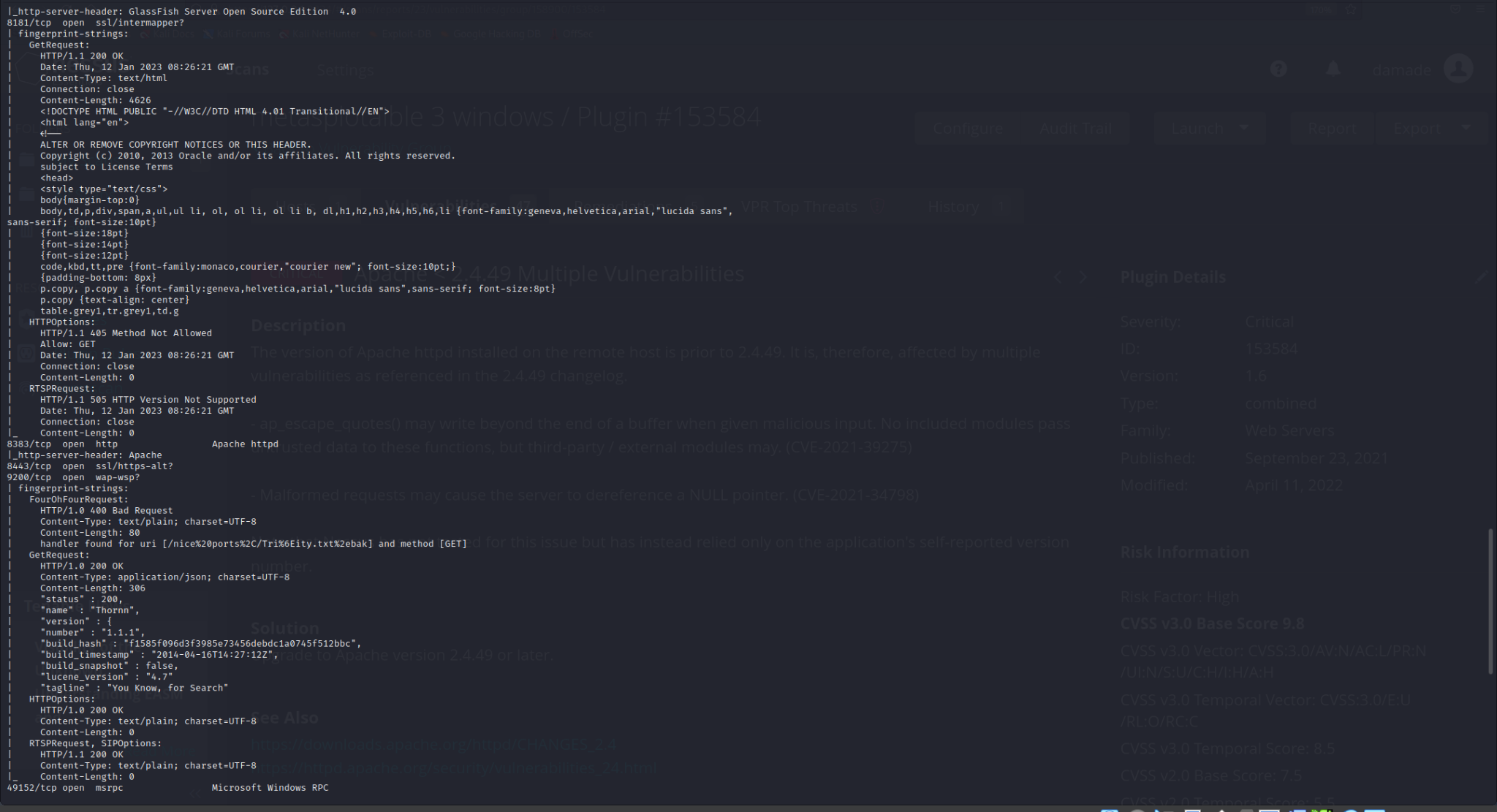
# Exercici 4: Recordant altres eines

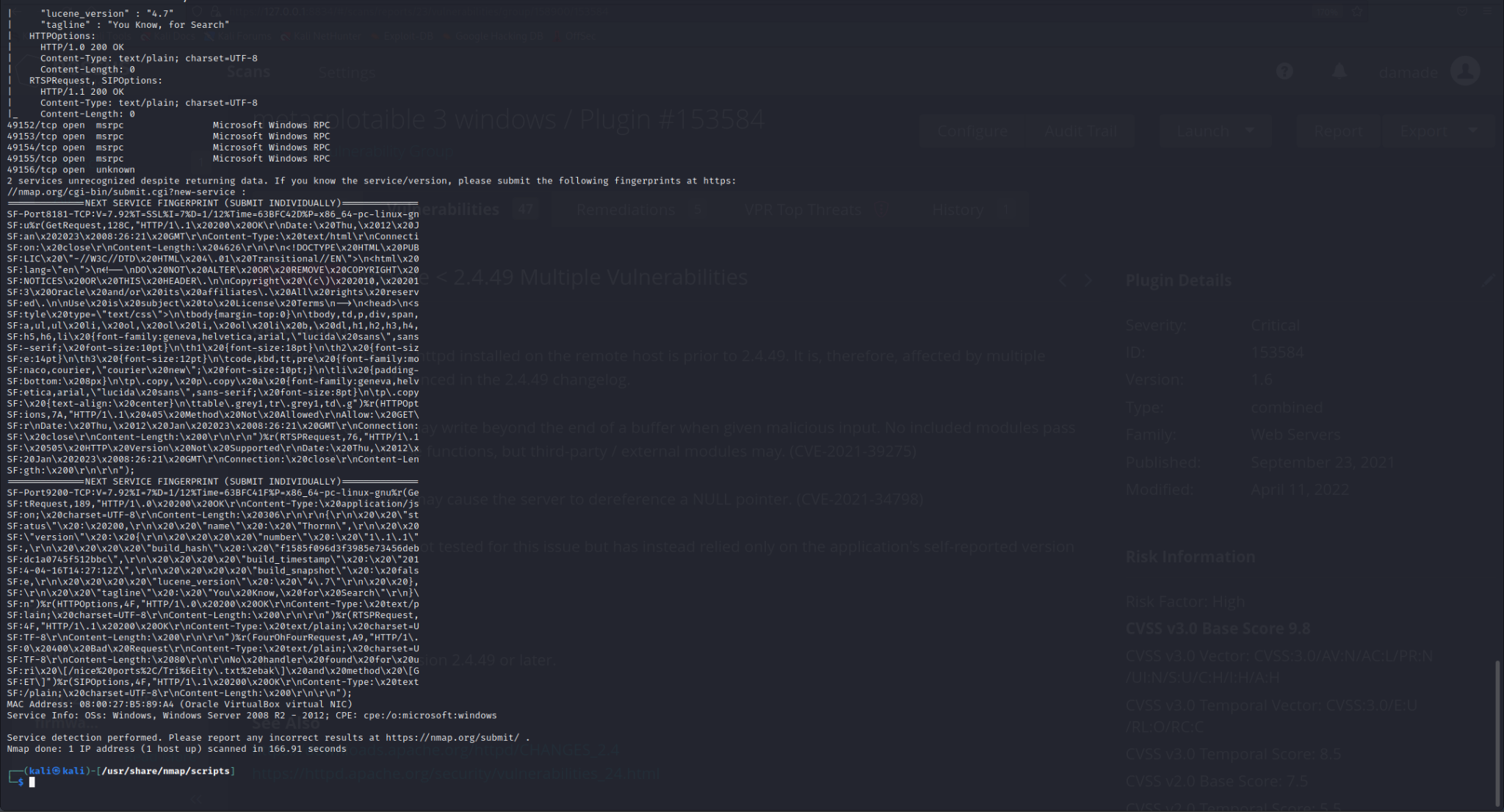
Ara farem el mateix amb algun script de nmap. (Utilitzaré el script vulners.nse)











Podem observar que tant el nmap com el nessus han trobat moltes vulnerabilitats en aquesta màquina.

Vulnerabilitats d’EXPLOIT, CVE, SSH, EDB , …

En comparació amb els resultats obtinguts en l’escaneig amb nessus, podem dir que no surt amb el nmap tanta informació sobre de que es la vulnerabilitat i et diu si es exploit, cve, ssh, etc; en canvi en el nessus t’explica millor sobre aquesta vulnerabilitat i et posa una solució per erradicar-la.

Foto d’exemple de nessus

