1 ASIX

**MÒDUL 16: CIBERSEGURETAT I HACKING ÈTIC**

ACTIVITAT 1.6: Eines avançades de scanning

línea horizontal

# 



**Alumne**: Daniel Mascarilla del Olmo

**Professor**: Sergi Andrés

**Curs**: 1 ASIX

**Centre**: Jaume Viladoms

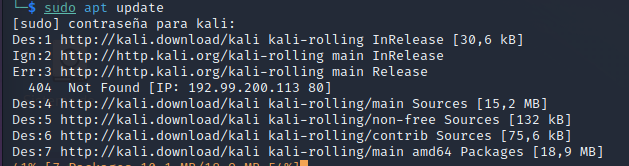
**ÍNDEX**

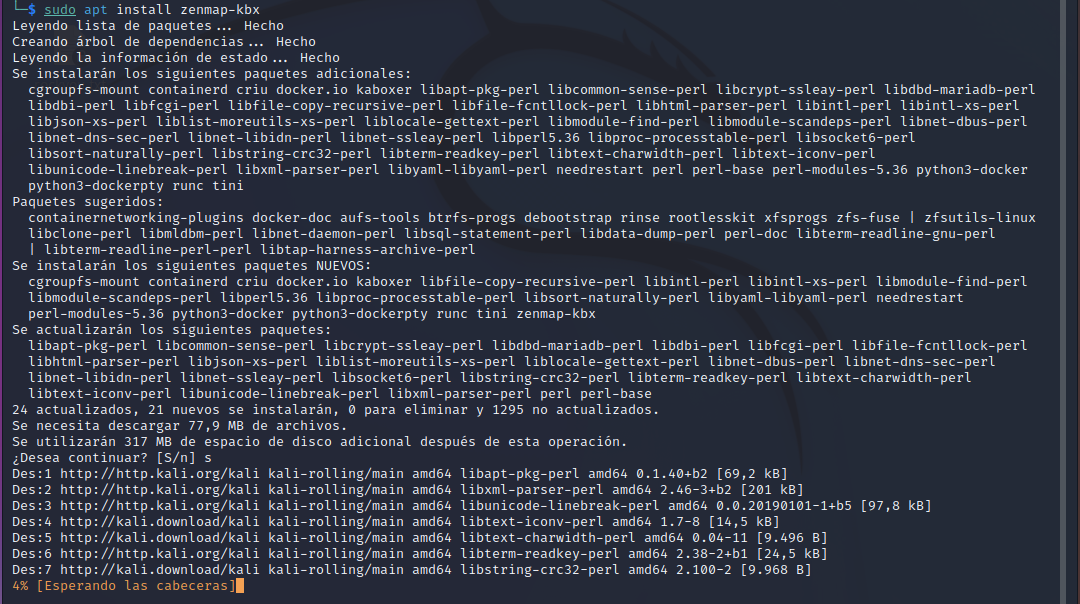
[**Exercici 1 – Eines avançades: Zenmap**](#_ywllt1woizva) **3**

[**Exercici 2 – Nmap amb scripts NSE**](#_gnq8nl53xhjg) **12**

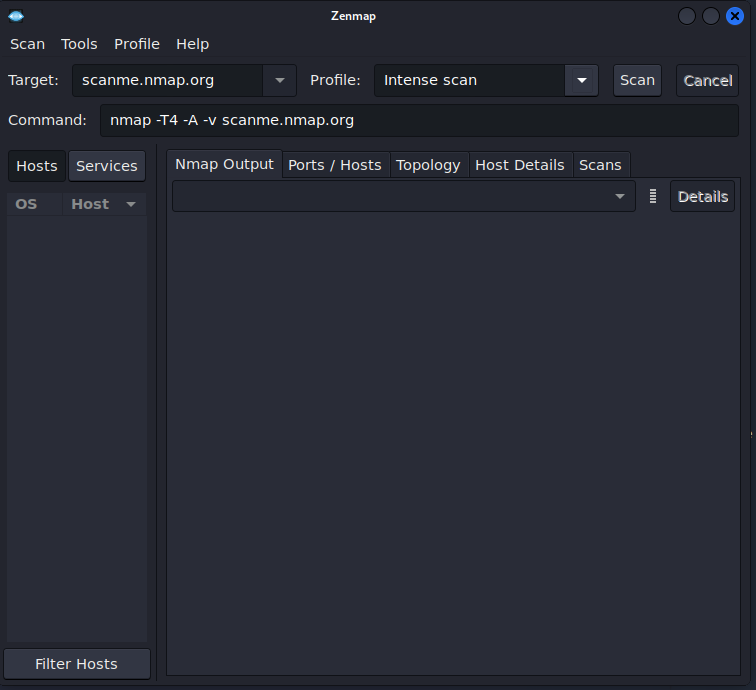
[**Exercici 3 – Nmap amb scripts no estàndards**](#_jk3np1b1z2kn) **15**

# Exercici 1 – Eines avançades: Zenmap

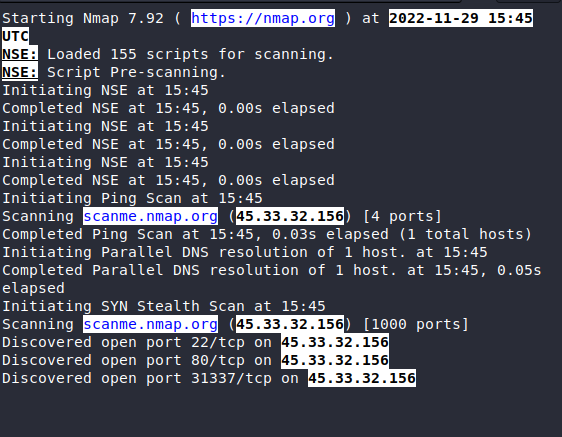




1. Utilitza Zenmap per veure tots els ports oberts de scanme.nmap.org



Utilitzant aquesta configuració, ens ha trobat això:



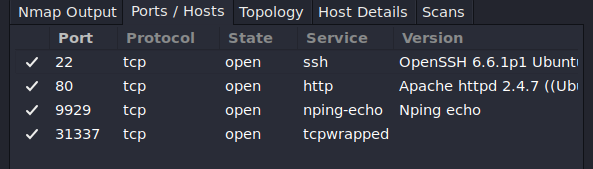
Podem veure que ha trobat diversos ports tcp.

1. Comprova dins les diferents pestanyes la informació que et mostra

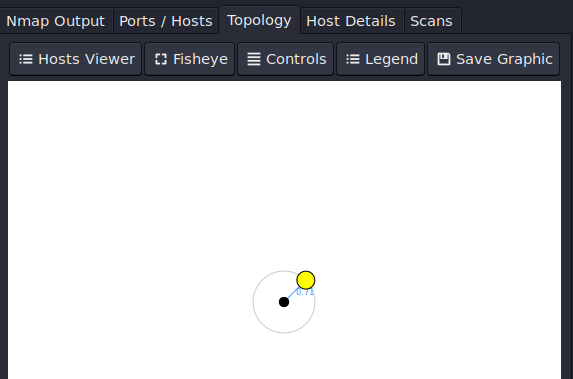
Si mirem les diferents pestanyes:



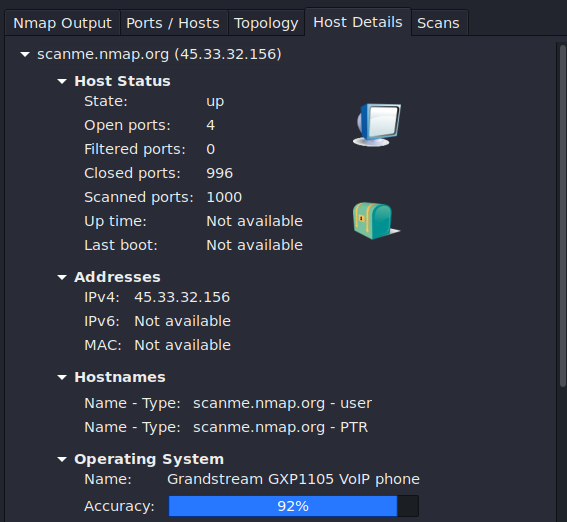
A la pestanya de ports/hosts podem veure els ports que ha escanejat:



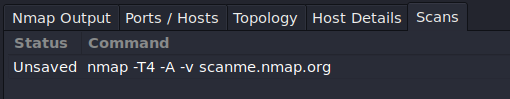
A la pestanya de Topology podem veure això:



A la pestanya de host details podem veure el host, l’estat del host, direccions ip, hostnames, el percentatge de precisió… :

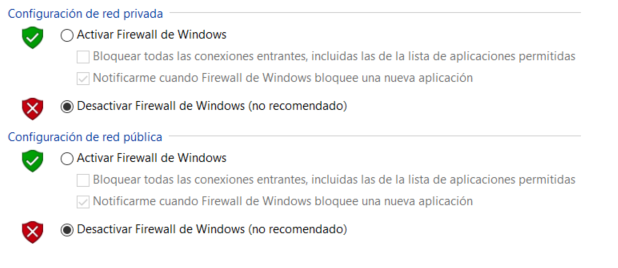


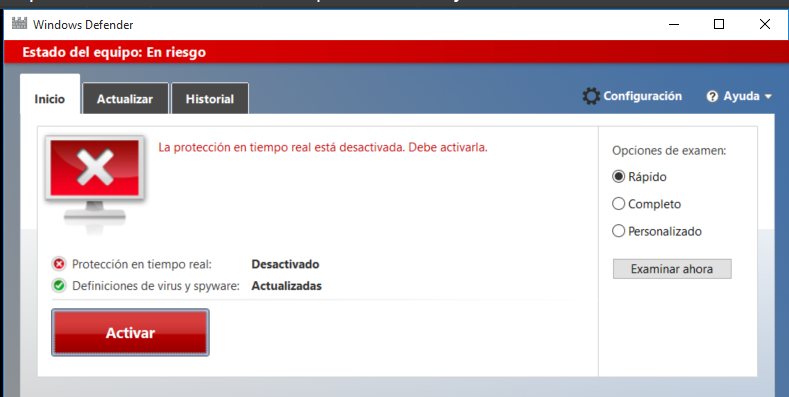
A la pestanya de scans podem observar el estat de la comanda i la pròpia comanda executada:



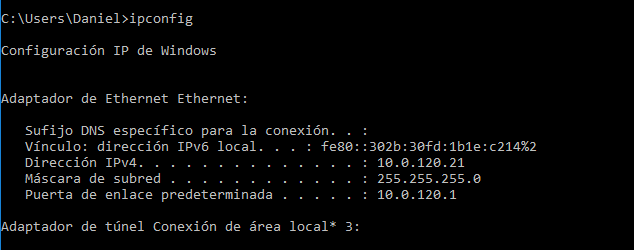
1. Utilitza Zenmap per a veure tots els ports oberts d’una màquina Windows 10 (recorda fer-ho amb el Firewall desactivat) i comprova la informació de les diferents pestanyes de zenmap

En una màquina Windows 10 tancarem el firewall i el windows defender:





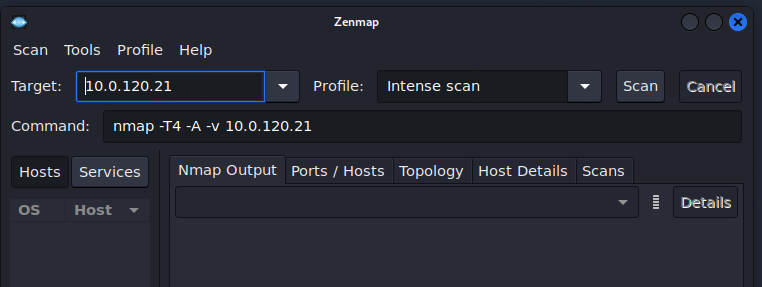
Un cop desactivat tot, mirarem la ip de la màquina windows en un cmd:

Podem veure que es la 10.0.120.21.

A la màquina kali linux executarem la següent comanda:

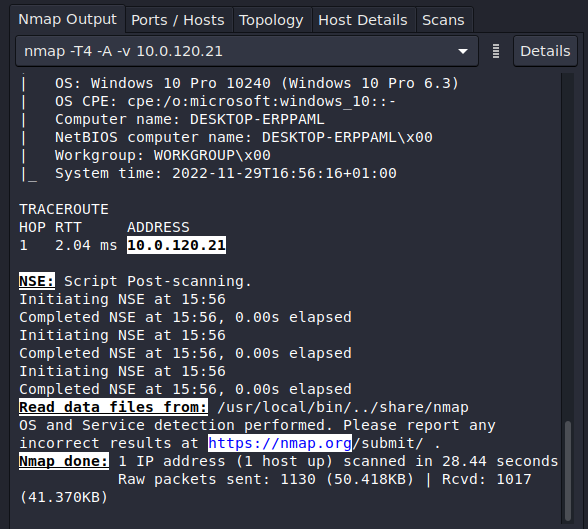


Un cop executada, se’ns obrirà el zenmap i podrem començar el scaneig:

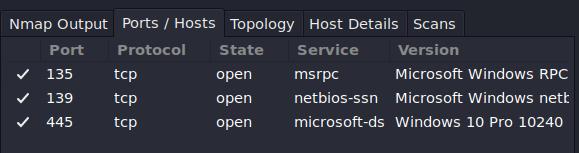


Esperarem fins que acabi el escaneig i mirarem les diverses pestanyes:

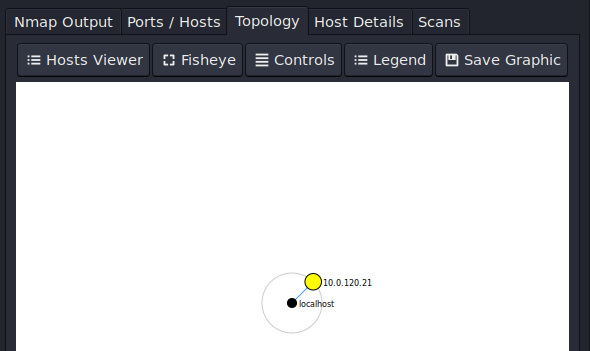
* A la de nmap output trobem:



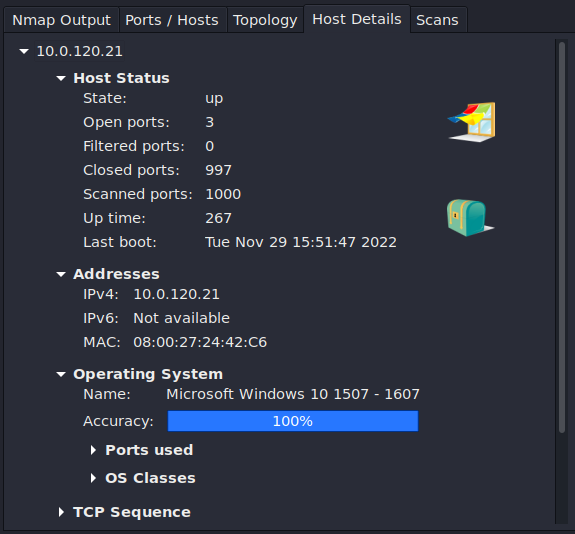
* A la de ports/hosts trobem



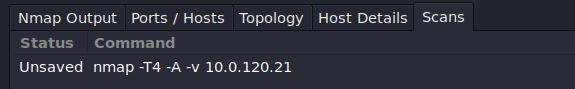
* A la de topology trobem:



* A la de host details trobem:

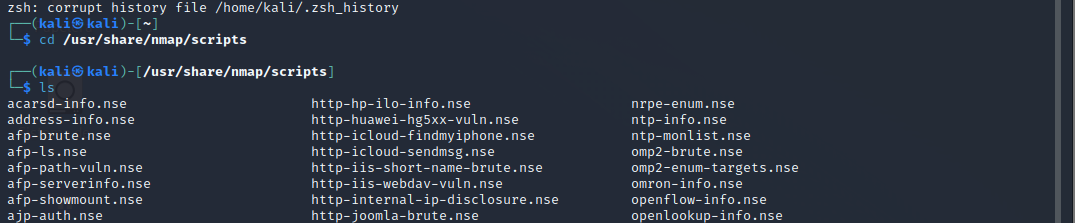


* I a la de scans trobem:



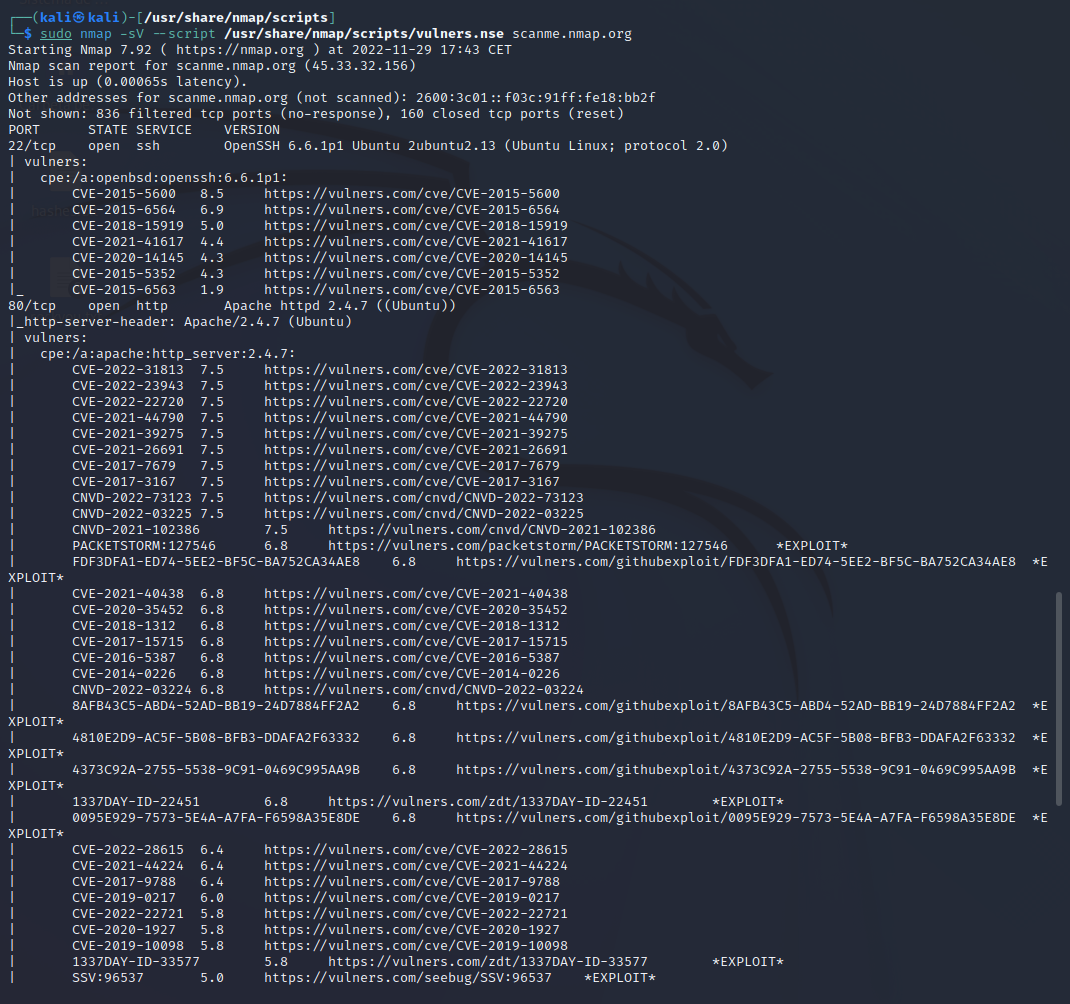
# Exercici 2 – Nmap amb scripts NSE

Anirem a scripts de nmap, a share, usr:

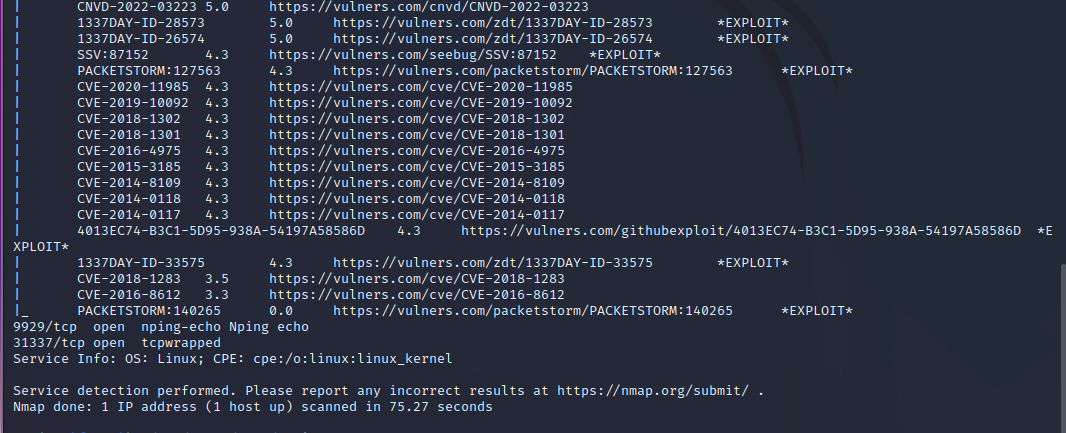


Ara executarem la comanda del primer enunciat:

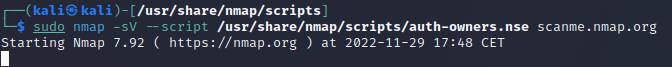
1. Executa l’script vuln contra la màquina scanme.nmap.org i comenta els resultats obtinguts

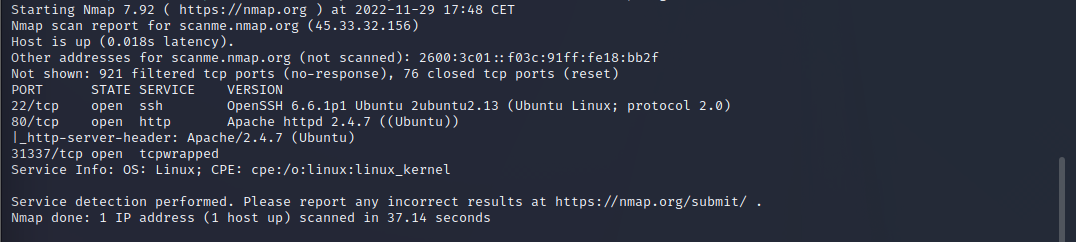


A la imatge podem veure la comanda i el que busca aquesta comanda. Aquesta comanda el que fa es descobrir les vulnerabilitats més conegudes. Com podem veure, les vulnerabilitats de la web de scanme.nmap.org són diverses, on podem trobar ports tcp oberts, l’estat dels ports, el servei i la versió d’aquests.



1. Executa l’script auth contra la màquina scanme.nmap.org i comenta els resultats obtinguts

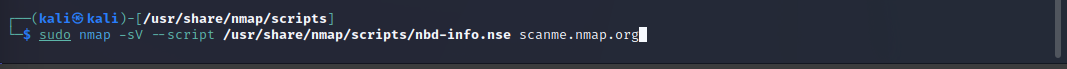


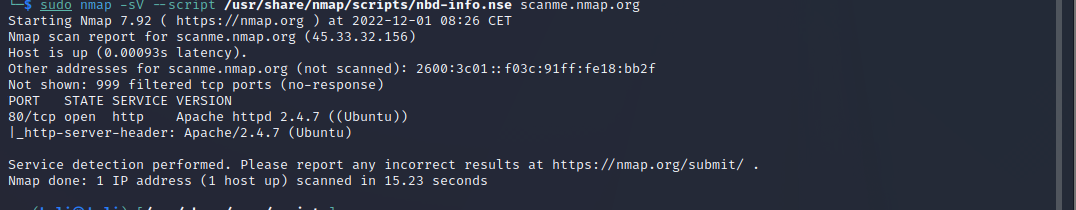


Utilitzant el script auth, el que ens proporciona es informació sobre si n’hi ha usuaris amb contrasenyes buides o si existeixen usuaris i contrasenyes per defecte.

Segons la imatge, podem observar que ens diu informació del servei, on trobem el sistema operatiu, el cpe, etc.

1. Busca algun altre script, dels que incorpora nmap per defecte que creguis interessant, executa’l i comenta els resultats obtinguts

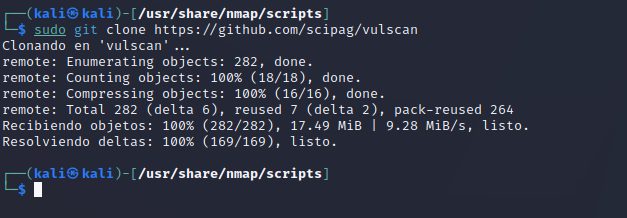


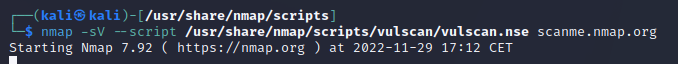


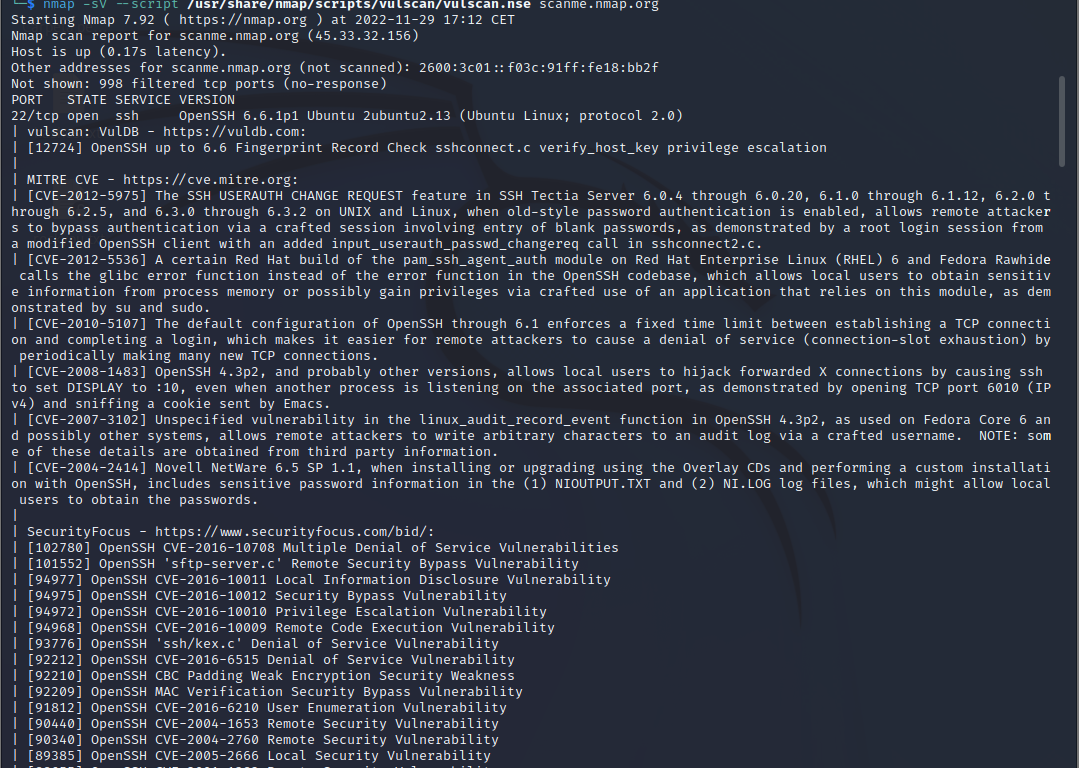
Aquest script serveix per mostrar informació sobre les metadades sobre el NDB server i exports.

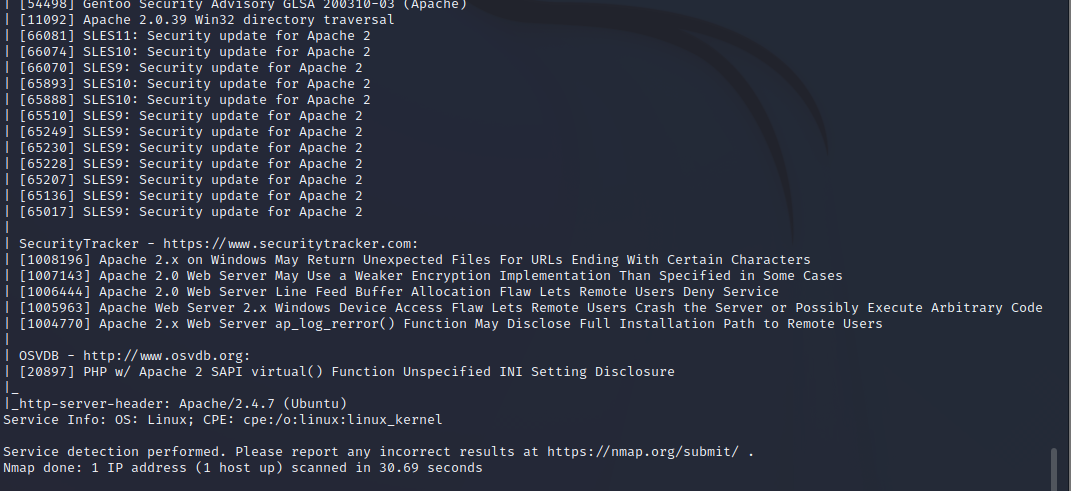
# Exercici 3 – Nmap amb scripts no estàndards

1. Descarrega’t amb git l’script vulscan i executa’l





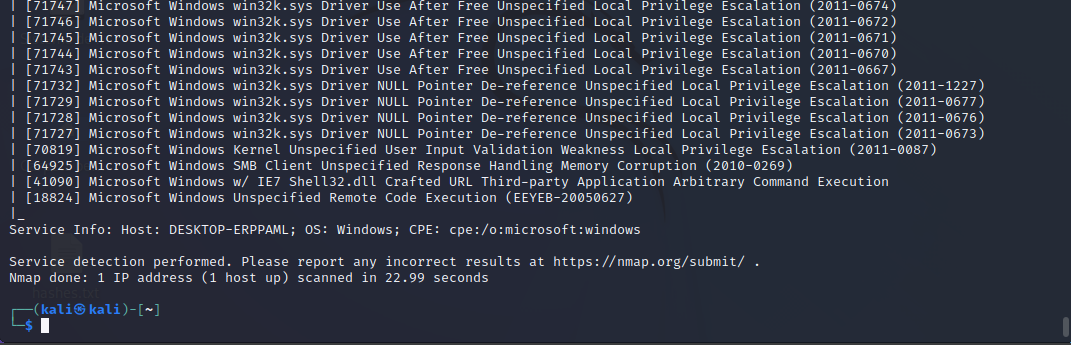




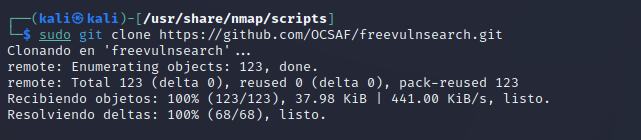
Ara probarem amb la màquina windows:

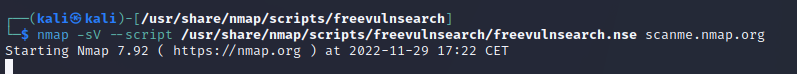


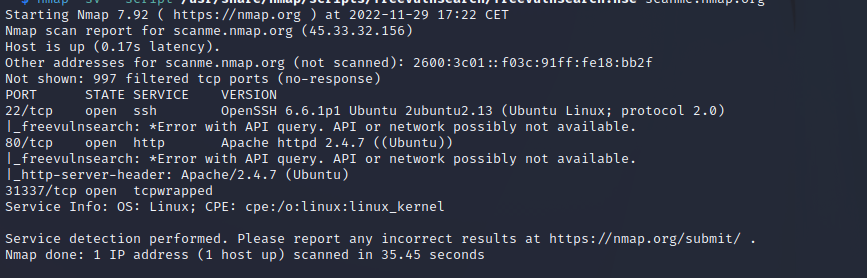




1. Descarrega’t amb git l’script freevulnsearch i executa’l.

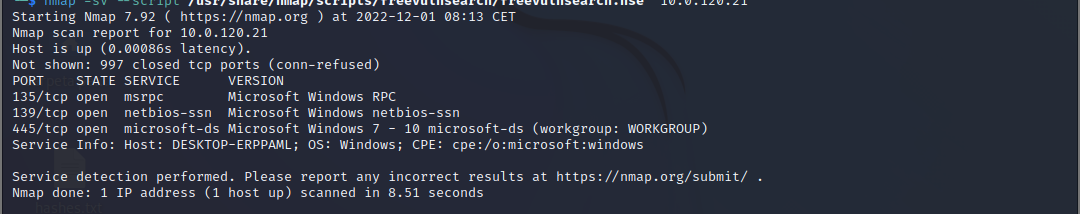




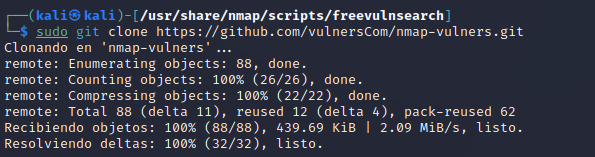


Ara probarem amb la mateixa comanda però amb una màquina windows 10:

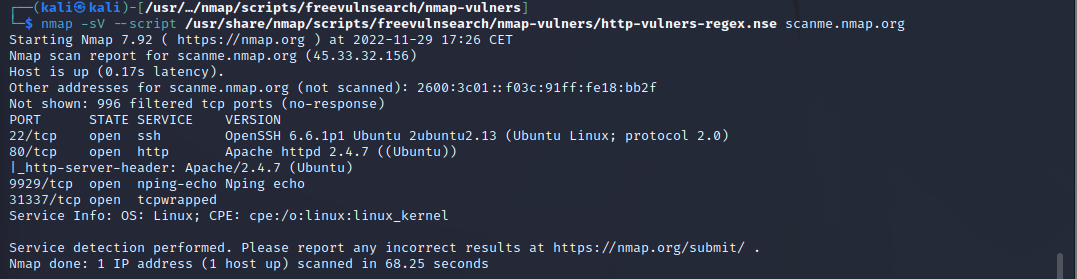




1. Descarrega’t amb git l’script vulners i executa’l.

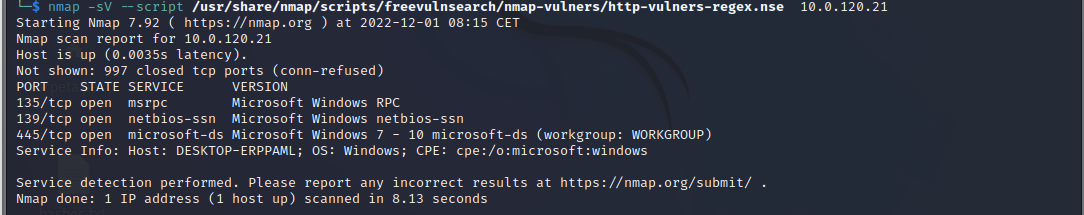






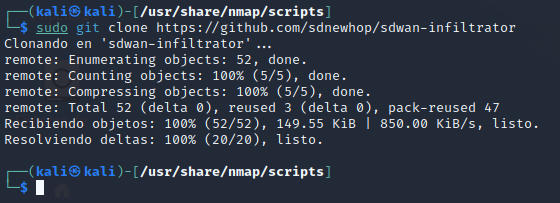
Ara probarem la mateixa comanda però amb windows 10:

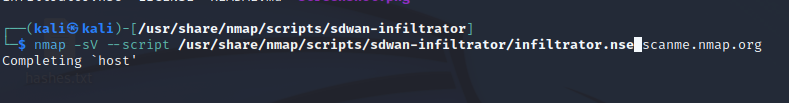


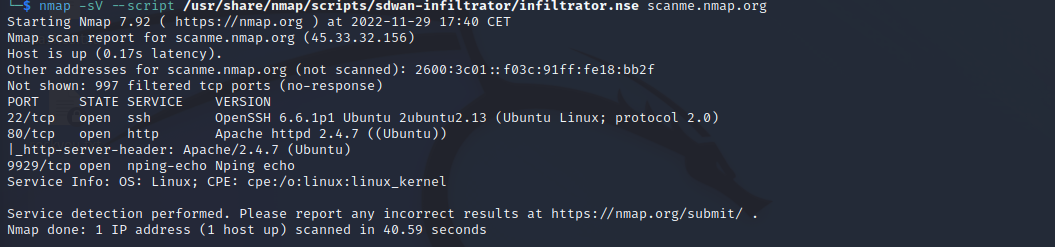


1. Busca algun script per a Nmap interessant de Github I prova el seu funcionament

Crec que el que he trobat es bastant interessant, es el script de infiltrator, és un script NSE per descobrir automàticament nodes SD-WAN en una xarxa local.







Per finalitzar, igual que els altres exercicis, probarem amb una màquina windows 10:



