Disciplina *Securitatea Sistemelor Informatice*
Facultatea de Inginerie și Informatică, Universitatea Spiru Haret
Conf. Univ. Dr. Marius Iulian Mihailescu
m.mihailescu.mi@spiruharet.ro
09.03.2022

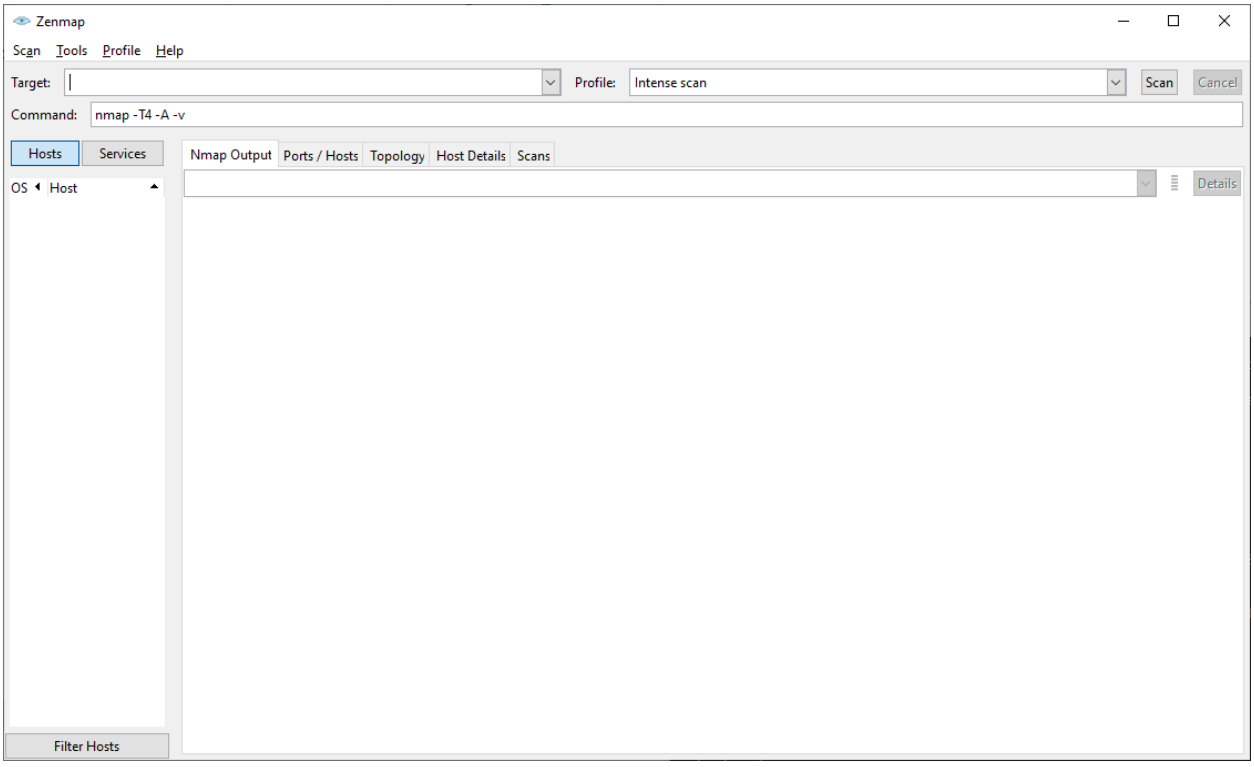
Laborator 3

Nmap

Note:

- https://nmap.org/
- Diferite definiții:
  - *"**Nmap can be used by hackers to gain access to uncontrolled ports on a system**. All a hacker would need to do to successfully get into a targeted system would be to run Nmap on that system, look for vulnerabilities, and figure out how to exploit them. Hackers aren't the only people who use the software platform, however."* - *https://www.holmsecurity.com/resources/what-is-nmap*

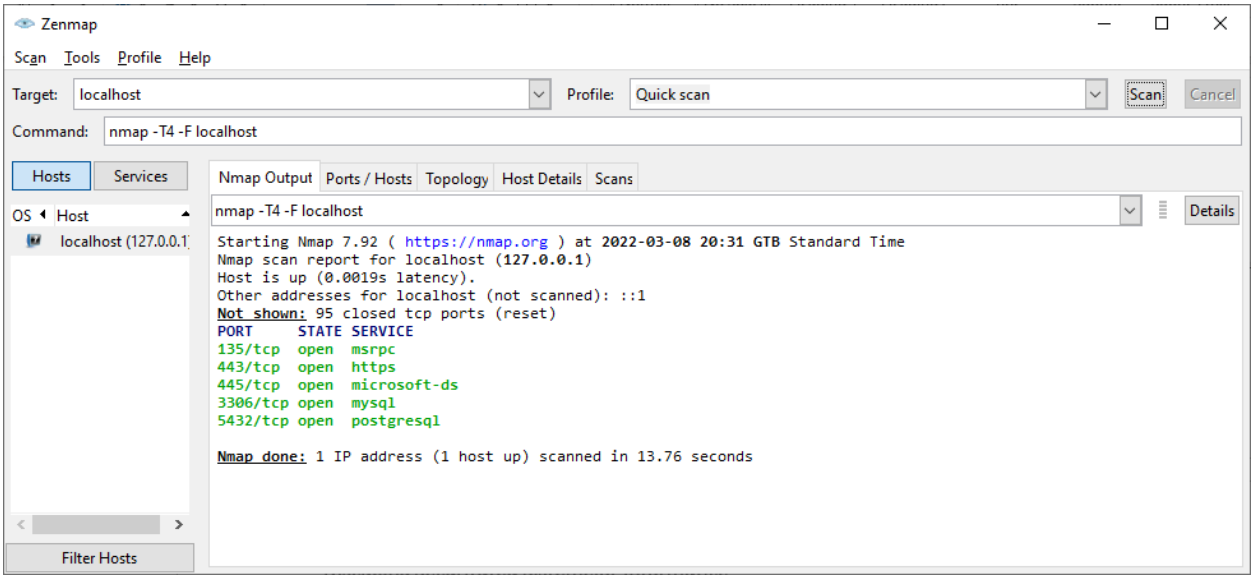
1. Instalați Nmap de la link-ul de mai sus.
2. Deschideți Nmap (fie în linie de comandă utilizând Command Prompt, fie GUI-ul aplicației Nmap, fie în Kali Linux, sau Ubuntu)



Disciplina *Securitatea Sistemelor Informatice*
Facultatea de Inginerie și Informatică, Universitatea Spiru Haret
Conf. Univ. Dr. Marius Iulian Mihailescu
m.mihailescu.mi@spiruharet.ro
09.03.2022

3. Rulați următoarele comenzi întruna dintre ferestrele preferate și studiați comportamentul.

3.1. nmap T4 -F localhost | Profile = Quick Scan



Studiați și comentați output-ul.

Ce este -F? Reprezintă modul rapid (fast mode).

Ce este T4? T-urile reprezintă timing templates. Sunt șase timing templates ce pot fi utilizate, după cum urmează:

- T0 = Paranoid
- T1= Sneaky
- T2 = Polite
- T3 = Normal
- T4 = Aggresive
- T5 = Insane

T0 și T1 – pentru evitarea IDS-urile

T2 – pentru încetinirea procesului de scanare pentru a utiliza mai puțină bandă și pentru a ținti resursele mașinii.

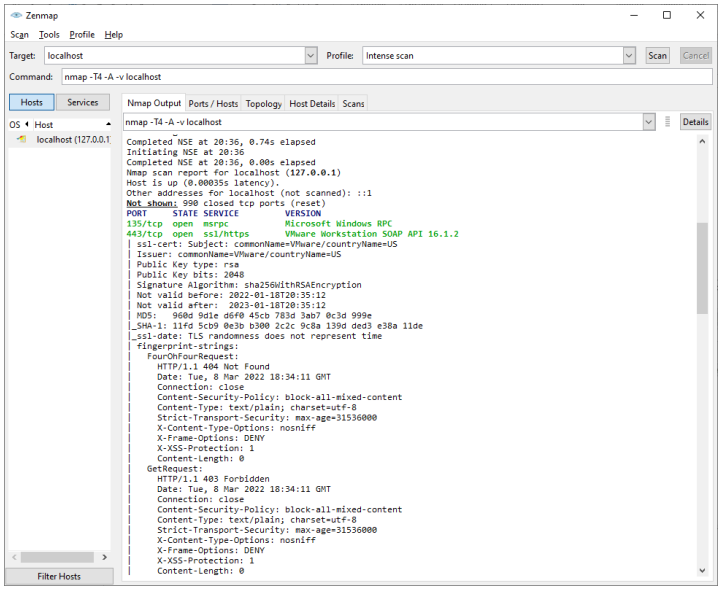
T3 – este modul default. Nu are niciun efect!

T4 – accelerează procesul de scanare, presupunând că ne aflăm într-o rețea rapidă și de încredere.

T5 – presupune că ne aflăm într-o rețea foarte rapidă sau suntem dispuși să sacrificăm ceva precizie pentru viteză.

Disciplina *Securitatea Sistemelor Informatice*
Facultatea de Inginerie și Informatică, Universitatea Spiru Haret
Conf. Univ. Dr. Marius Iulian Mihailescu
m.mihailescu.mi@spiruharet.ro
09.03.2022

nmap T4 -F localhost | Profile = Intense Scan



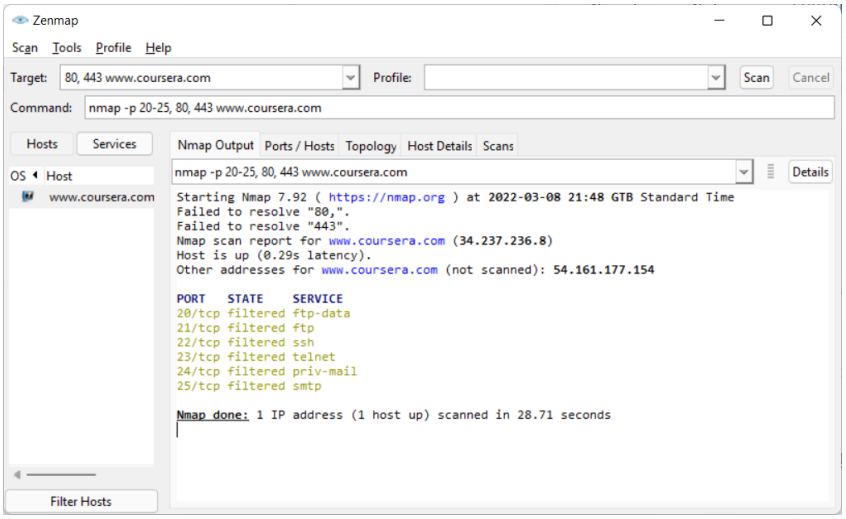
Studiați și comentați output-ul.

3.2. Pentru scanarea de hosturi multiple se utilizează următoarele comenzi:
nmap T4 -F 192.168.100.3 192.168.100.12 192.168.100.65
nmap T4 -F 192.168.100.2-45

3.3. Pentru a scana un fișier text cu mai multe adrese IP se poate utiliza comanda

nmap -iL fisier.txt

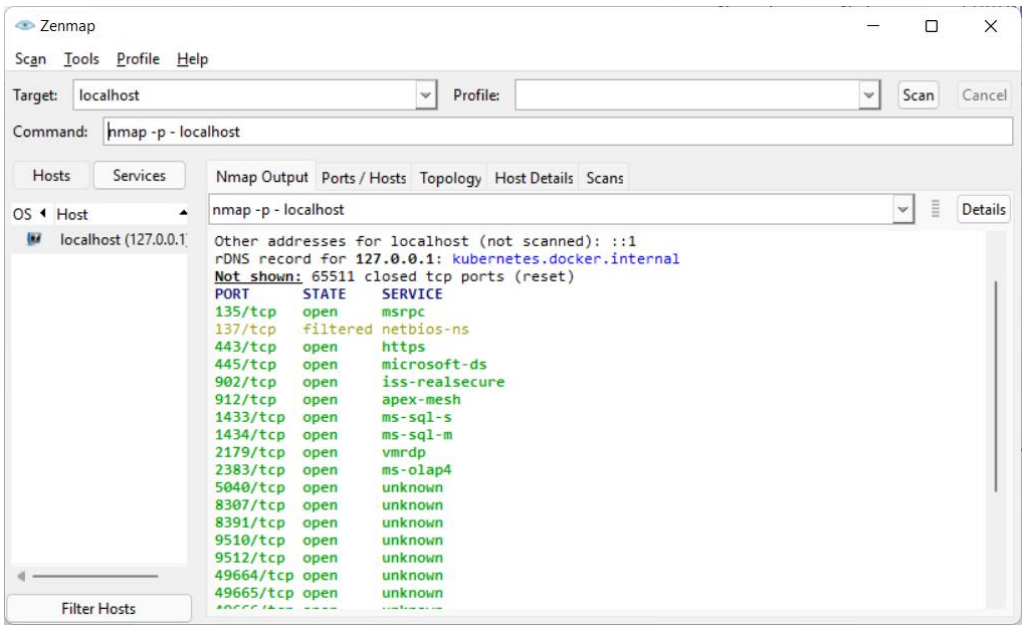
3.4. Să se scaneze porturile 20-25, 80 și 443 pentru o mașină virtuală sau un site (e.g., www.coursera.com)



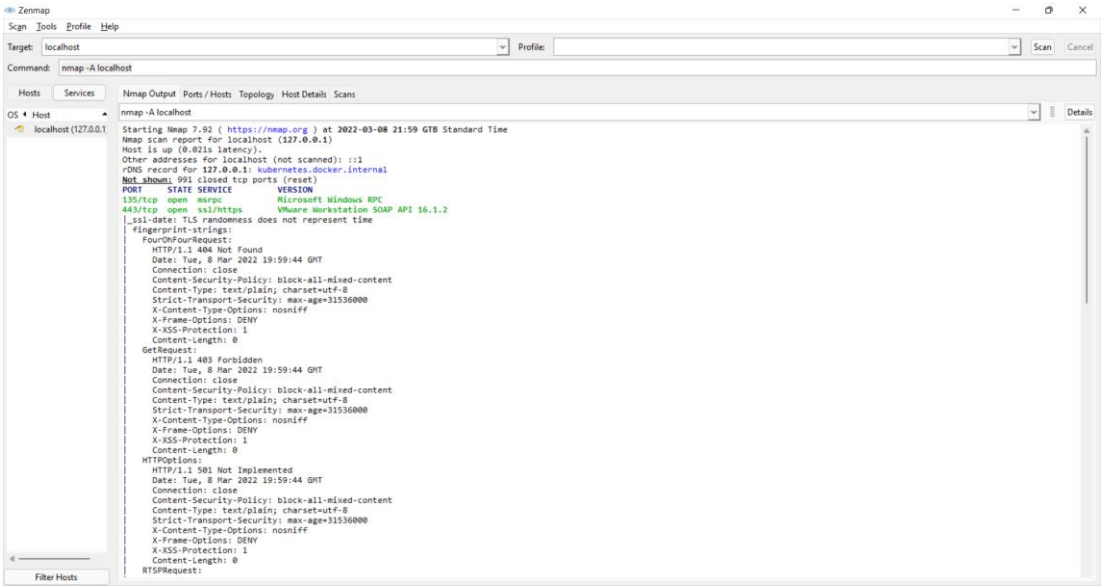
Disciplina *Securitatea Sistemelor Informatice*
Facultatea de Inginerie și Informatică, Universitatea Spiru Haret
Conf. Univ. Dr. Marius Iulian Mihailescu
m.mihailescu.mi@spiruharet.ro
09.03.2022

3.5. Utilizați comanda de mai jos pentru a verifica protocolul http sau alte protocoale/servicii
nmap -p http adresaIP
nmap -p http, mysql, ftp adresaIP

3.6. Scanați toate porturile utilizând comanda nmap -p- localhost



3.7. Uitlizați scanarea agresivă utilizând următoarea comandă (durează foarte mult ca și timp): nmap -A localhost. Avantajul constă în detaliile despre detaliile afișate despre rute etc.



Conf. Univ. Dr. Marius Iulian Mihailescu
m.mihailescu.mi@spiruharet.ro
09.03.2022

3.8. Utilizați comanda nmap –traceroute website și studiați comportamentul output-ului.

3.9. Salvarea output-ului rezultatelor întrun fișier se poate realiza cu ajutorul următoarei comenzi: nmap -F -oN results.txt website

3.10. Pentru a scana porturile 80 si 443 pentru hosturile 10.7.1.0/24 utilizați comanda

nmap -sS -p 80, 443 10.7.1.0/24

nmap -sT 10.7.1.226
nmap -sS 10.7.1.226

3.11. Detectați versiunea sistemului de operare utilizat pe o gazdă prin utilizarea comenzii:

nmap -O 10.7.1.226

3.12. Versiunea sistemului de operare, traceroute, sc

nmap -A 10.7.1.226