

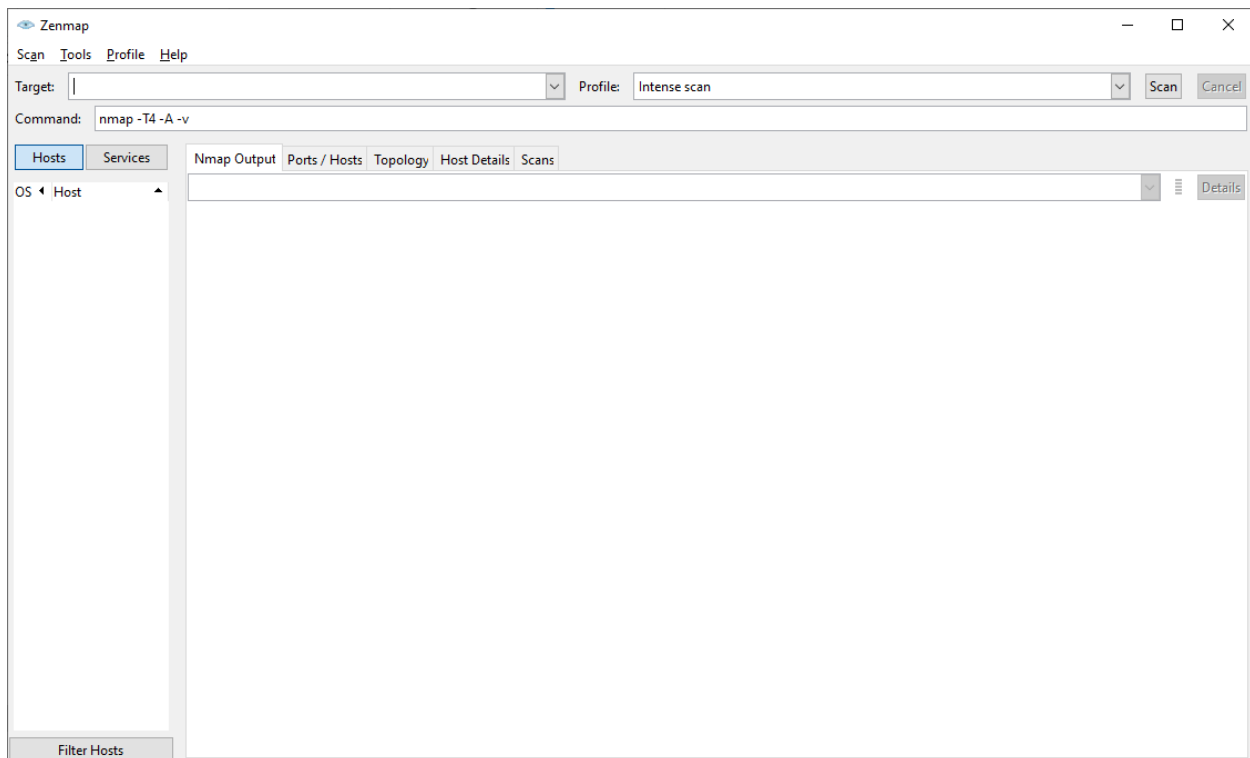
Laborator 3

Nmap

Note:

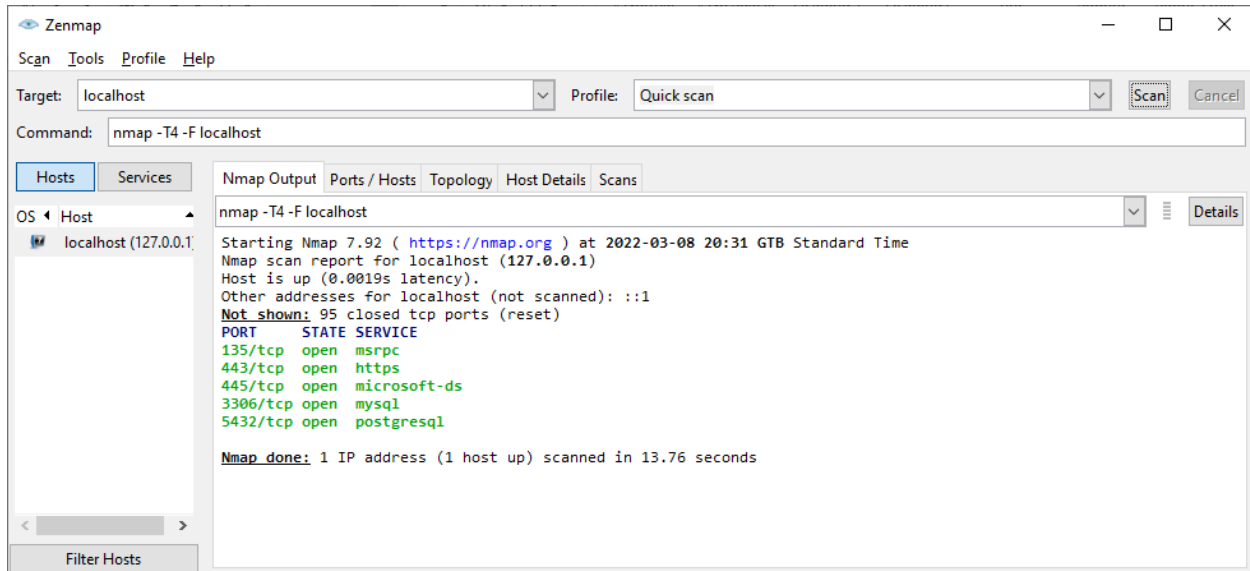
- <https://nmap.org/>
- Diferite definiții:
 - o *“Nmap can be used by hackers to gain access to uncontrolled ports on a system. All a hacker would need to do to successfully get into a targeted system would be to run Nmap on that system, look for vulnerabilities, and figure out how to exploit them. 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)



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 = Aggressive
- T5 = Insane

T0 și T1 – pentru evitarea IDS-urilor

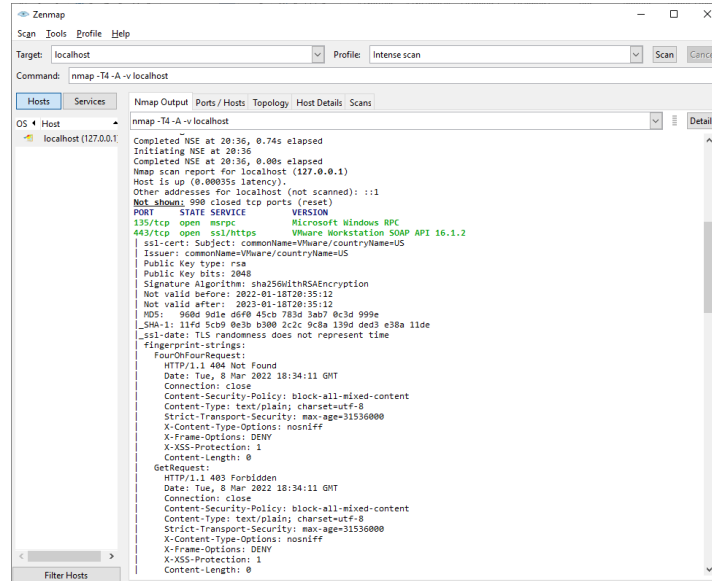
T2 – pentru încetinirea procesului de scanare pentru a utiliza mai puțină bandă și pentru a ținti resursele mașinii.

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.

nmap T4 -F localhost | Profile = Intense Scan



```
OS 4 Host
+ localhost (127.0.0.1)
  Completed NSE at 20:36, 0.74s elapsed
  Initiating NSE at 20:36
  Completed NSE at 20:36, 0.88s elapsed
  Nmap scan report for localhost (127.0.0.1)
  Host is up (0.00035s latency).
  Other addresses for localhost (not scanned): ::1
  Not shown: 990 closed tcp ports (reset)
  PORT      STATE SERVICE          VERSION
  135/tcp   open  msrpc            Microsoft Windows RPC
  443/tcp   open  ssl/https        VMware Workstation SOAP API 16.1.2
  | ssl-cert: Subject: commonName=VMware/countryName=US
  | Issuer: commonName=VMware/countryName=US
  | Public Key type: rsa
  | Public Key bits: 2048
  | Signature Algorithm: sha256WithRSAEncryption
  | Not valid before: 2022-01-18T20:35:12
  | Not valid after: 2023-01-18T20:35:12
  | MD5: 968d 9d1e d6f8 45cb 783d 3ab7 8c3d 999e
  |_SHA-1: 11f8 5c09 0e3b b090 2c1c 9c8a 139d 0ed3 e8ba 110e
  |_ssl-data: TLS randomness does not represent time
  | Fingerprint-strings:
  | FourFourRequest:
  |   HTTP/1.1 404 Not Found
  |   Date: Tue, 8 Mar 2022 18:34:11 GMT
  |   Connection: close
  |   Content-Security-Policy: block-all-mixed-content
  |   Content-Type: text/plain; charset=utf-8
  |   Strict-Transport-Security: max-age=31536000
  |   X-Content-Type-Options: nosniff
  |   X-Frame-Options: DENY
  |   X-KSS-Protection: 1
  |   Content-Length: 0
  | GetRequest:
  |   HTTP/1.1 403 Forbidden
  |   Date: Tue, 8 Mar 2022 18:34:11 GMT
  |   Connection: close
  |   Content-Security-Policy: block-all-mixed-content
  |   Content-Type: text/plain; charset=utf-8
  |   Strict-Transport-Security: max-age=31536000
  |   X-Content-Type-Options: nosniff
  |   X-Frame-Options: DENY
  |   X-KSS-Protection: 1
  |   Content-Length: 0
```

Studiați și comentați output-ul.

3.2. Pentru scanarea de hosturi multiple se utilizează următoarele comenzi:

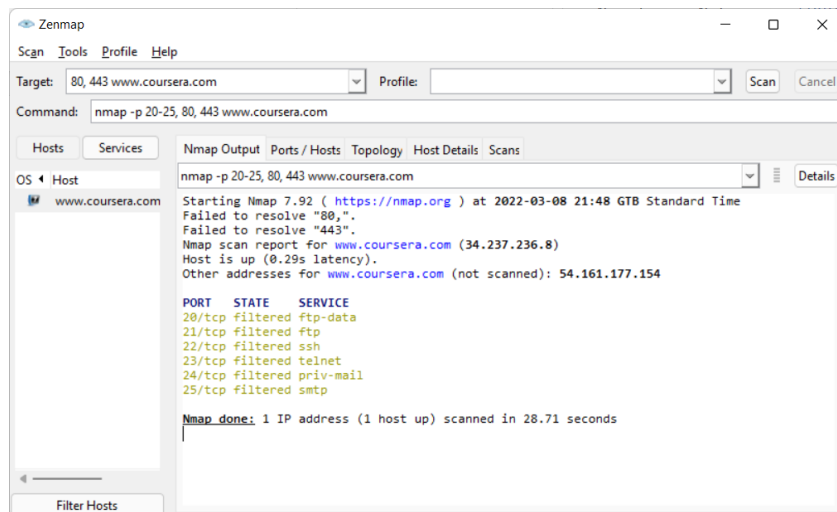
```
nmap T4 -F 192.168.100.3 192.168.100.12 192.168.100.65
```

```
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)



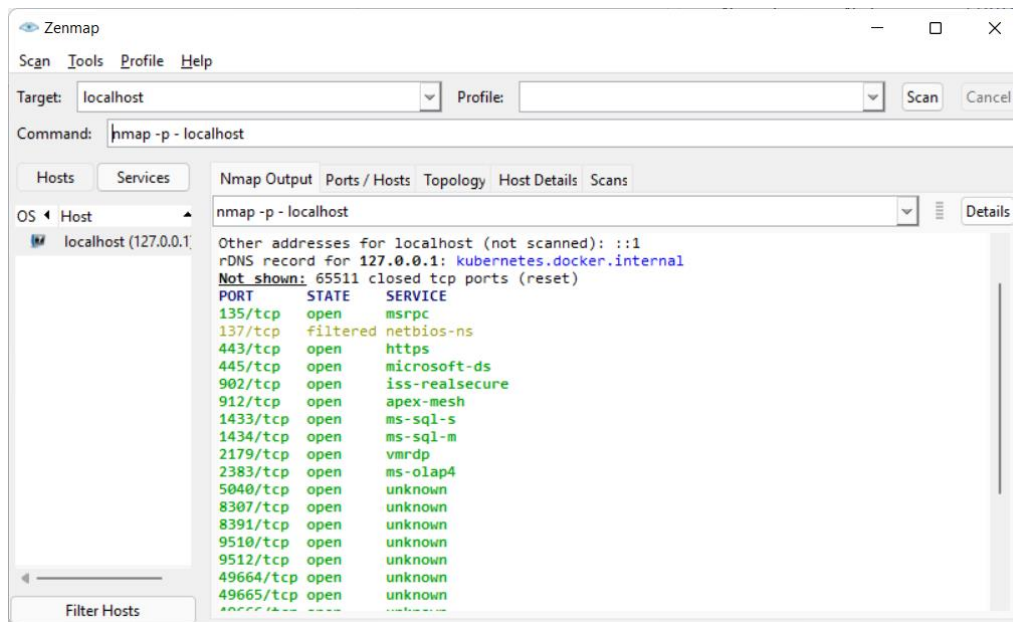
```
OS 4 Host
+ www.coursera.com
  Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-08 21:48 GTB Standard Time
  Failed to resolve "80".
  Failed to resolve "443".
  Nmap scan report for www.coursera.com (34.237.236.8)
  Host is up (0.29s latency).
  Other addresses for www.coursera.com (not scanned): 54.161.177.154
  PORT      STATE SERVICE
  20/tcp   filtered ftp-data
  21/tcp   filtered ftp
  22/tcp   filtered ssh
  23/tcp   filtered telnet
  24/tcp   filtered priv-mail
  25/tcp   filtered smtp
  Nmap done: 1 IP address (1 host up) scanned in 28.71 seconds
```

3.5. Utilizați comanda de mai jos pentru a verifica protocolul http sau alte protocoale/servicii

`nmap -p http adresaIP`

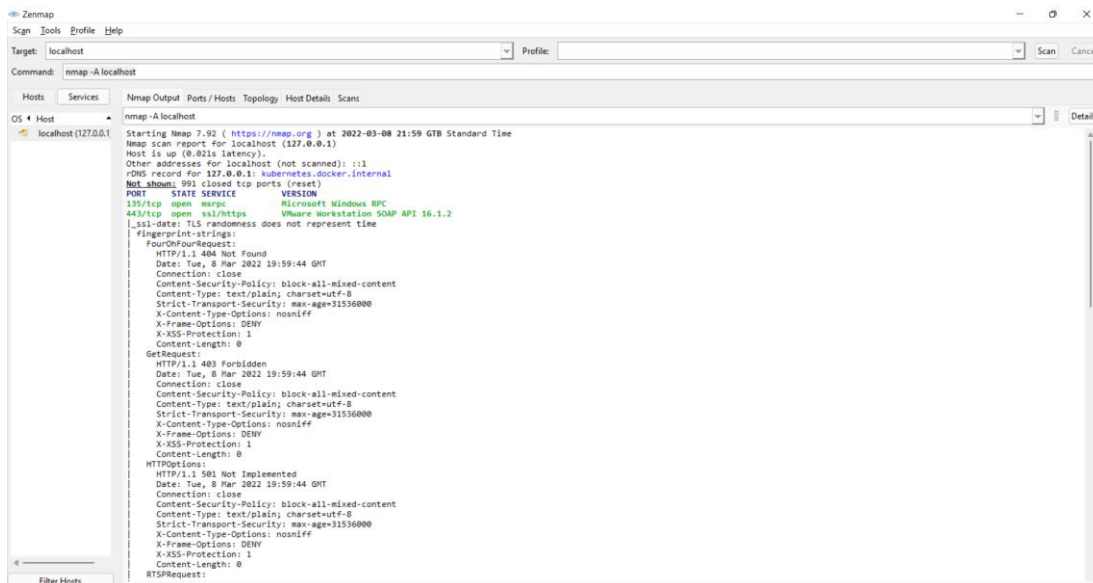
`nmap -p http, mysql, ftp adresaIP`

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



3.7. Utilizați scanarea agresivă utilizând următoarea comandă (durează foarte mult ca și timp):

`nmap -A localhost`. Avantajul constă în detaliile despre detaliile afișate despre rute etc.



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 și 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
```