Atakante bezala, funtzeskoa da ezagutzea zen portu dauden zabalik.

Oinarrizko parametroak

Portu guztiak eskaneatzeko

```
nmap -p- 192.168.0.1
```

65535 portu daude, guztiak eskaneatzeko

```
nmap -p1-65535 192.168.0.1
```

- Portua egon daiteke Zabalik, Itxita edo Filtratua

500 portu erabilienak eskaneatzeko:

```
nmap --top-ports 500 192.168.0.1
```

Bakarrik zabalik dauden portuak eskaneatzeko:

```
nmap --top-ports 500 --open 192.168.0.1
```

Verbose, eskaneoa astiro badoa eta aldi berean zein portu dauden zabalik jakin nahi badugu:

```
nmap --top-ports 500 --open 192.168.0.1 -v
```

DNS ez aplikatzeko erabili, eskaneoa azkarragoa izango da:

```
nmap --top-ports 500 --open 192.168.0.1 -v -n
```

Plantilla de temporizado:

-Tn (n : 0 - 5) 0. Oso geldoa baina ixila (modo paranoico) 5. Oso azkarra baina saratatzua (modo loco)

```
nmap -p- -T5 192.168.0.1
```

TCP connect scan

Eskaneatze modu honetan, nmap-ek tcp protokoloaren 3-way-handshake-a egiten saiatuko da. Gogoratu nola harrapau genituen pakete hauek Wiresharken:

- Portua zabalik badago (SYN ACK -> SYN -> ACK)
- Portua itxita badao (SYN ACK -> RST)

```
nmap -p- -T5 -sT --open 192.168.0.1 -v -n
```

Eskaneatu edozein host (activos y no activos)

- -Pn parametroa erabili beharko dugu

```
nmap -p- -T5 --open 192.168.0.1 -v -n -Pn
```

UDP protokoloa erabiliz eskaneatu

- -Su parametroa erabiliko dugu honetarako

```
nmap --top-ports 100 --open -Su 192.168.0.1 -v -n
```

Piztutako Hostak aurkitzeko subsare baten (Ping sweep)

```
nmap -sn 192.168.0.1/24
```

Sistema eragilearen ezaugarriak aurkitzeko

⚠ Ez dago oso gomendatuta, astuna baita.

```
nmap -O 192.168.0.1
```

Paketeen TTL-a erabiliz

Bizi-denbora (TTL), bideratzaile batek baztertu aurretik, sare baten barruan pakete bat egon behar dela ezarri den denbora-kopuruari edo "jauziei" dagokie. TTLa beste testuinguru batzuetan ere erabiltzen da, hala nola CDN cachean biltegiratzean eta DNS cachean biltegiratzean.

Informazio-pakete bat sortzen denean eta Internet bidez bidaltzen denean, bideratzaile izatetik bideratzaile izatera igarotzeko arriskua dago, mugarik gabe. Aukera hori arintzeko, paketeak bizi-denbora edo jauzien muga izeneko iraungipenarekin diseinatzen dira. Paketeen TTLa ere baliagarria izan daiteke pakete jakin bat zenbat denboraz zirkulazioan egon den zehazteko, eta bidaltzaileak Internet bidez pakete baten ibilbideari buruzko informazioa jaso ahal izatea ahalbidetzen du.

Pakete bakoitzak zenbakizko balio bat gordetzen duen leku bat du, eta balio horrek zehazten du zenbat denbora jarraitu behar duen sarean mugitzen. Bideratzaile batek pakete bat jasotzen duen bakoitzean, bat kentzen zaio TTLren zenbaketari, eta sareko hurrengo tokira pasatzen du. Uneren batean TTLren zenbaketa zerora iristen bada kenketaren ondoren, bideratzaileak paketea baztertu eta ICMP mezu bat bidaliko du jatorrizko hostora.

Zer zerikusi du horrek sistema eragilearen identifikazioarekin? Beno, hainbat sistema eragilek TTLren balio lehenetsiak dituzte. Adibidez, Windows sistema eragileetan, TTLren balio lehenetsia 128 da, eta Linux sistema eragileetan, berriz, 64.

Beraz, makina batera pakete bat bidaltzen badugu eta 128ko TTL balioa duen erantzun bat jasotzen badugu, litekeena da makina Windows exekutatzen aritzea. 64ko TTL balioa duen erantzun bat jasotzen badugu, litekeena da makina Linux exekutatzen aritzea.

Metodo hau ez da hutsezina eta sare-administratzaileek engaina dezakete, baina zenbait egoeratan baliagarria izan daiteke makina baten sistema eragilea identifikatzeko.

Jarraian, gela honetan erakusten dugun orria partekatzen dizuegu, dauden TTL balioei dagokien sistema eragilea identifikatzeko.

Linux/Unix: 64 Windows: 128 MacOS: 64 Solaris/AIX: 254 FreeBSD: 64

Subin 's Blog: https://subinsb.com/default-device-ttl-values

Era berean, lortutako TTLaren arabera sistema eragilea identifikatzeko ardura duen Python-en scripta partekatzen dizuegu:

WhichSystem: https://pastebin.com/HmBcu7j2

Portuen serbitzuak detektatu

```
nmap -p80 192.168.0.1 -sV
```

NMAP scriptak erabiltzen

Scriptal eta kategoriak aurkitzen

```
# Scriptak
locate .nse

# Script kopurua
locate .nse | wc -l

# Categoriak modu paraleloan aurkitu
locate .nse | xargs grep 'categories'

# Filtratu mserbitzuak
locate .nse | xargs grep 'categories' | greo -oP '".*?"' |sort -u
```

Exekutatu script sorta bat

Exekutatu script sorta bat, sC parametroarekin script guztietatik, erabilenen artean daduden sorta bat exekutatuko dira portu horretan.

```
nmap -p22 192.168.0.1 -sC -SV
```

Exekutatu script sorta bat kategoriakoak

```
nmap -p80 192.168.0.1 --script="vuln or/and safe" -sV


# Zerbitzuak portuan ikusi
lsof -i:80

# Prozesu bat nondik exekutzen den aurkitzeko
pwdx idprocesso
```