tags:

- Networks
- Hacking

Zer da firewall bat

Segurtasun sistema bat da. Sarean zehar irten eta sartzen de trafikoa gainbegiratzen du, arau batzuei jarraituz.

Barnean zabalik daduen portuak aurkitu

- Fragmented (-f): Firewall-ak trafikoa eskaneatze gisa ezagutu ez dezan bidalitako paketeak zatikatzean oinarritzen da teknika hau. - f aukerak Nmapen paketeak zatikatzea eta bereizita bidaltzea ahalbidetzen du, Firewall detektatzea saihesteko

```
nmap -p22 -198.162.11.1 -f
```

- **Praktika**: Egin eskaneo bat eta wiresharkeking, hurrengo filtroa erabiliz aurkitu nmapek erabili dituen pakete fragmentatu hauek.

ip.flags.mf == 1 (0 pakete normalentzat)

Nmapen eskaneatze jarduera izkutatu

- Decoy (-D): -D komandoari esker, erabiltzaileak pakete faltsuak bidal ditzake benetako eskaneatze-paketeekin batera, bere jarduera ezkutatzeko. Nmapen eskaneoa izkutatzeko teknika honi esker, erabiltzaileak pakete faltsuak bidal ditzake sarera, sarkinak detektatzeko sistemak nahasteko eta firewalla gu ez detekta gaitzan.

Imagina firewalla konfiguratua dagoela zeren bakarrik ip zehatz bat

- Praktika:

1. Eskaneoa egin

```
nmap -p22 192.168.111.1 -D 192.168.111.215
```

- 192.168.111.1 eskaneatu nahi dugun helbidea
- 192.168.111.215 eskaneorako ip alternativo bat, beste iturri baten itxura emoteko.

2. Gorde sare trafikoa

```
tcpdump -i ens33 -w Captura.cap -v
```

- ens33 : Sare interfazearen izena (aurkitu ifconfig erabiliz)

- Captura.cap : Sare trafikoaren traza gordetzeko fitxategia

3. Ikusi trafiko hau wireshark erabiliz

```
wireshark Captura.cap >& /dev/null & disown
```

erabili filtroa *tcp.port == 22*