ICMP Flood Attack

Marian Codrin Cretu

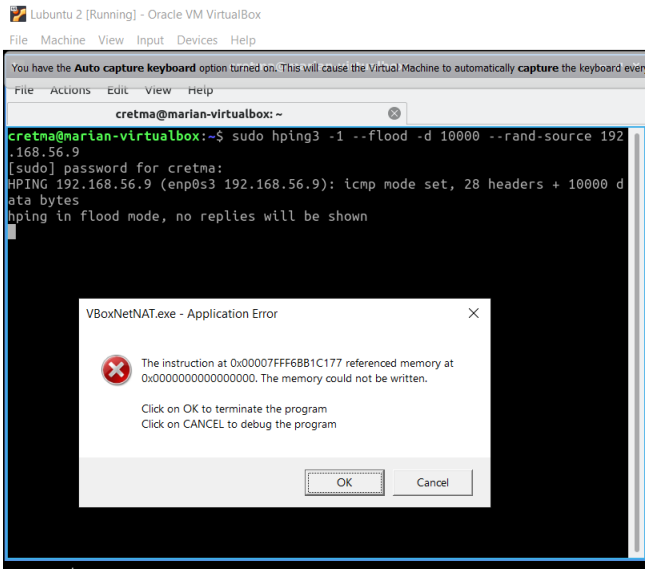
May 2021

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.

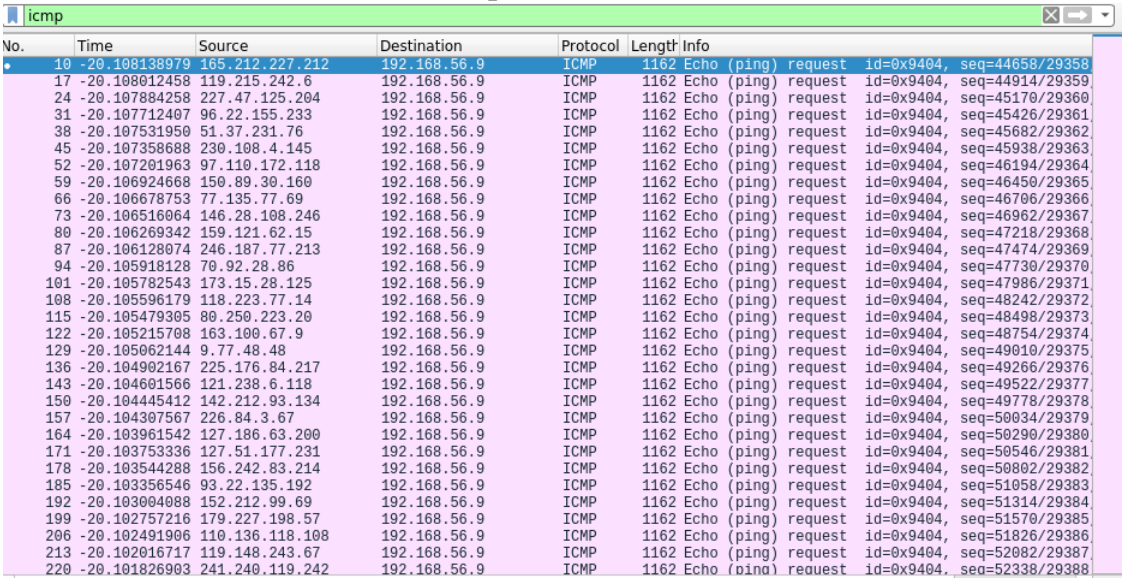
Comanda rulată de pe mașina atacatorului:
sudo hping3 -1 –flood -d 10000 –rand-source 192.168.56.9
Explicații parametrii:
-1 – modul ICMP (ping)
–flood – opțiunea de a trimite pachete în mod continuu (fără a aștepta neapărat un răspuns)
-d 10000 – dimensiunea pachetului să fie de 10000 bytes
–rand-source – 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).



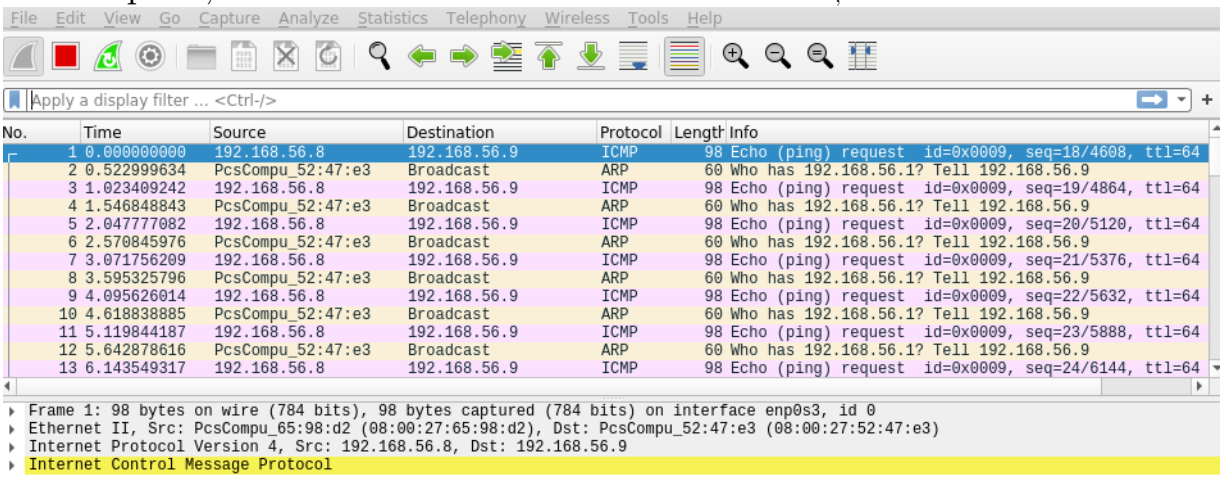
Observăm următorul mesaj de la Windows (*buffer overflow*) imediat după ce începe

atacul.

Capturi de ecran Wireshark:
Atacatorul are următoarea captură:



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.



2 Contramăsuri

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/