Logo

Description automatically generated

Denial of Service Attacks

Contents

[Tools Used 2](#_Toc133772173)

[SYN Flooding 2](#_Toc133772174)

[UDP Flooding 3](#_Toc133772175)

[ICMP Flooding 3](#_Toc133772176)

[TCP Flooding 4](#_Toc133772177)

[Results 4](#_Toc133772178)

[Moving Forward 5](#_Toc133772179)

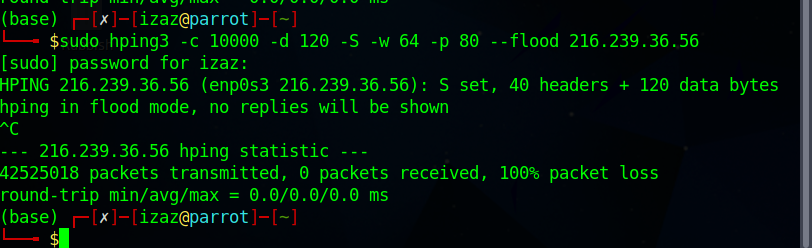
# Tools Used

Hping3

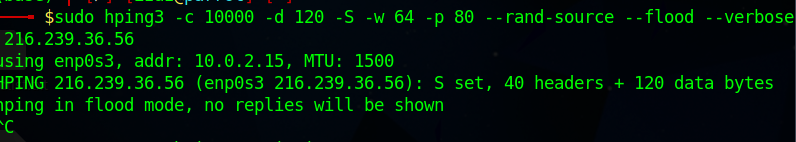
ParrotOS

# SYN Flooding

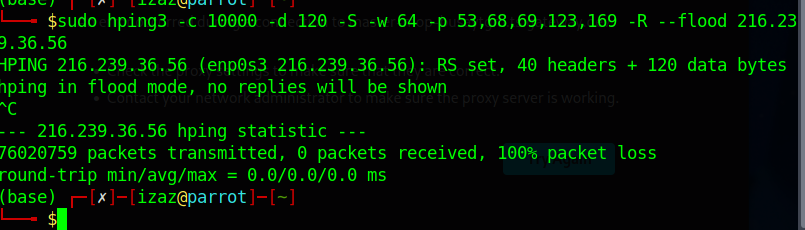
A SYN flood attack will try to overwhelm the server by sending a large amount of SYN requests to take advantage of the three way handshake, the reason why this attack can stop web traffic is because due to the large amount of SYN packets that get transmitted, if they get through the server is then unable to complete the three-way handshake with legitimate users. Learning Center (n.d.)



As we can see from the results of this attack, The website was able to know that this was a SYN flood attack and instead of letting it be vulnerable and attacked, however the idea occurred to me that after that I should be flooding the ports that were found by another team member. I also decided to modify the attack so that instead of the same IP address it will attack using random IP addresses, making it more difficult to detect whether this is legitimate traffic.

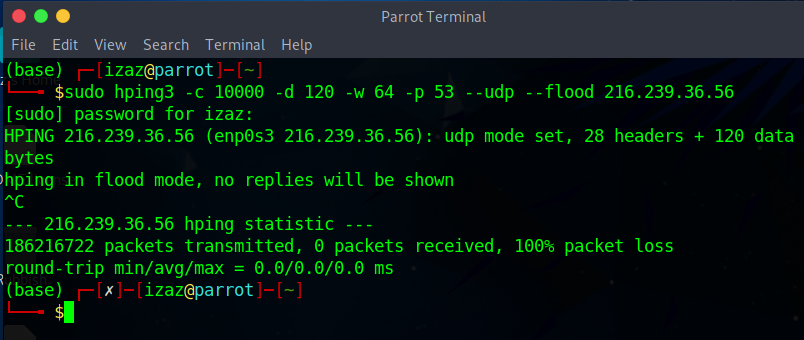


Even this did not help, as 100% of the packets still failed to be replied to

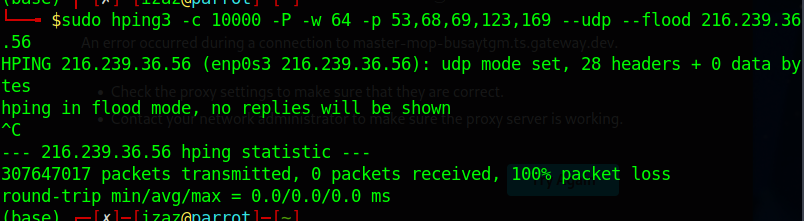


# UDP Flooding

UDP flooding is like SYN flooding however instead of flooding the server with SYN request it sends a large amount of UDP requests and because UDP is a connectionless protocol it can be sent without the three-way handshake. If the packets were to get through to the server then there would be no resources for legitimate users. Imperva (n.d.)



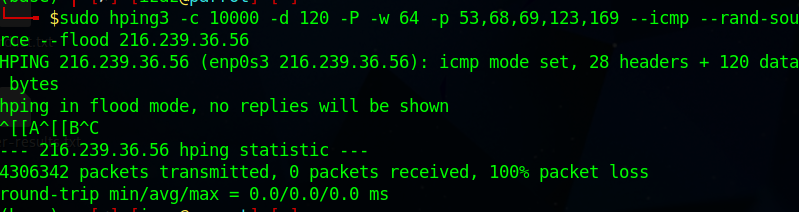
I tried testing further with the modified command for the extra ports.



I further modified the command so that it includes the extra ports and includes the random IP addresses, this shows once again the website is immune to this attack.

# ICMP Flooding

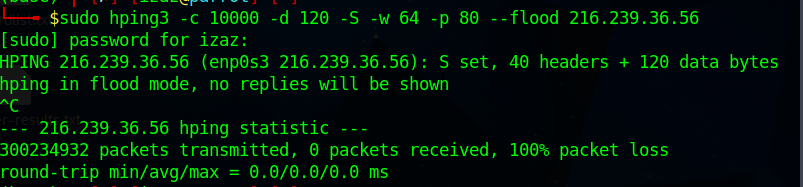
The next type of Denial-of-Service attack was ICMP flooding, as expected since the other flooding attacks failed this one did as well, with 0 packets being accepted by the server. It must seem as if there is protection in built to prevent a DoS attack. ICMP is like SYN however because ICMP is used for network management and because of that it is more draining on server hardware such as the CPU and RAM. If the ICMP packets were to pass through it could mean that the server itself could shut down due to the overprocessing that would occur in this situation. Netscout (n.d.)

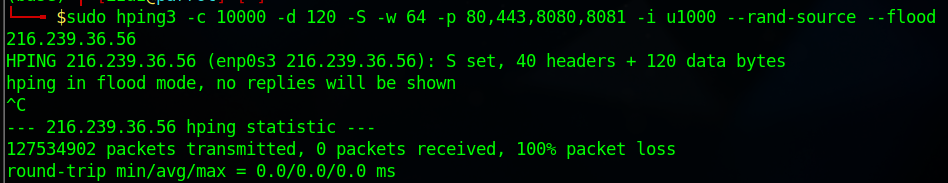


# TCP Flooding

TCP Flooding sends a massive amount of TCP traffic to a website, mainly using fake and multiple IP addresses to slow the server down. Unlike SYN requests, this kind of attack isn’t trying to establish a handshake and have multiple “users” instead this will send packets like a SYN request however it won’t complete the handshake by sending the client Ack back to the server, this means the packets that would get through the slower the server would get. Radware (n.d.)

In this case it didn’t matter if it came from multiple different IP’s or a singular as you can see within the screenshots no packets were accepted by the server despite the large amount being sent and because of that web traffic remained the same.





# Results

Unfortunately, none of these attacks were successful however there are further tools that can be used and will be used in a future attack, it could be because the website is being hosted on the google cloud platform and because of Cloud Armour many web-based attacks will fail. For further attempts I will try targeting specific ports (ideally open ports) with different attacks and use a variety of tools for a singular attack. Google Cloud (n.d.)

# Moving Forward

For different attacks I will use different tools such as LOIC or HOIC, Sucuri or PRTG. With further research into the google cloud platform I will try to find any vulnerabilities that exist within the platform that could leave it vulnerable to different attacks. If I do decide to revisit Denial of Service attacks then I will also research further into packet sizes (for all the attacks conducted above) and see if that could be a factor which lets me get past the initial security, as long as the initial security can be breached it means further vulnerabilities can be found and exploited.

Reference list

Google Cloud. (n.d.). *Cloud Armor Network Security | Google Cloud Armor*. [online] Available at: https://cloud.google.com/armor#:~:text=Cloud%20Armor%20security%20policy%20overview [Accessed 30 Apr. 2023].

Imperva (n.d.). *What is a UDP Flood | DDoS Attack Glossary | Imperva*. [online] Learning Center. Available at: https://www.imperva.com/learn/ddos/udp-flood/.

Learning Center. (n.d.). *What is a TCP SYN Flood | DDoS Attack Glossary | Imperva*. [online] Available at: https://www.imperva.com/learn/ddos/syn-flood/.

Netscout (n.d.). *What is an ICMP Flood Attack?* [online] NETSCOUT. Available at: https://www.netscout.com/what-is-ddos/icmp-flood.

Radware (n.d.). *What Is A TCP SYN Flood DDOS Attack? | Radware*. [online] www.radware.com. Available at: https://www.radware.com/security/ddos-knowledge-center/ddospedia/tcp-flood/ [Accessed 30 Apr. 2023].