DDOS: Ping Flood Attack

By: Zachary

What is a Ping Request?

- A ping request is where a user can test/verify if a network can take an IP address back to a specific device.
- This request also verifies if a host computer is operating and active. This request also ensures the availability of the host machine the attacker is trying to access.
- Simply, an ICMP request is sent to the network/device and a response is anticipated if active.

Ping Flood Attack

- The ping flood attack is a denial of service attack. It purposely floods the target device with requests packets.

- The attacker sends multiple ICMP requests to the network/device and blocks it from receiving normal network traffic.

- I selected this attack because DDOS are pretty common attacks, and having the knowledge to understand and mitigate these scenarios will certainly help when needed.

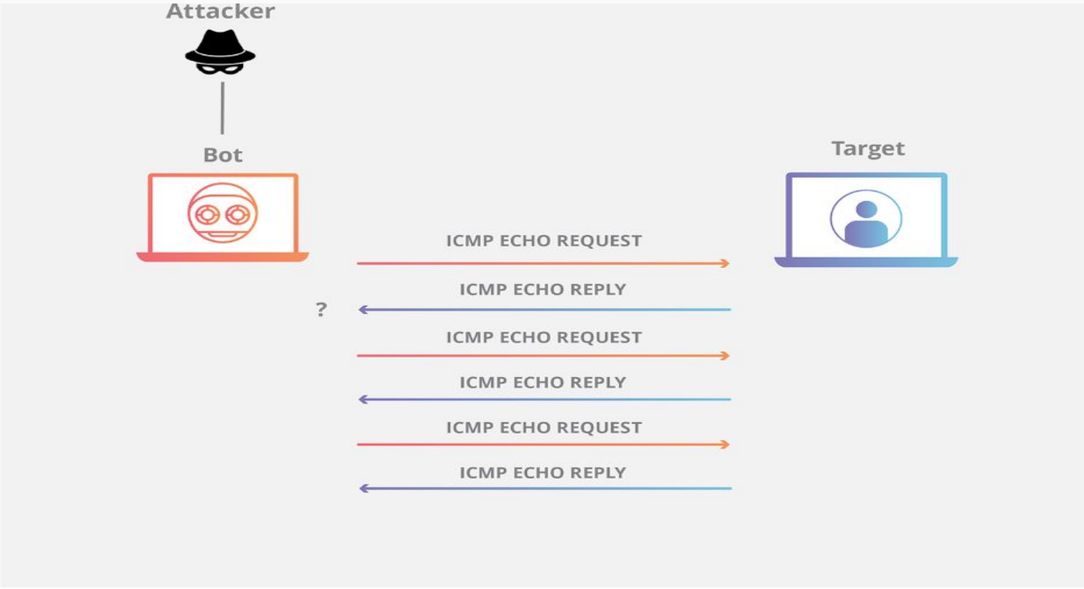
Research Steps

- My first step was to figure out how a ping flood attack functioned.
- Secondly, I researched via youtube and google what would be the command to run a ping flood attack.
- Lastly, I did my attack in a simulated environment, so nothing i did would be illegal/unethical.

Demonstration Preview Steps

- My first step was to nmap my IP address to find out which ports are open.
- Secondly, I used the ping flood attack on said IP address, which is: ‘hping3 -1 --fast “IP address”’
- Lastly, i ran the attack, which causes disruption in the server/router.

Brief Example of a Ping Flood Attack



Ping Flood Attack Demo

Demonstration Summary

- First I did an nmap scan on a specific IP address, which is used for security auditing and network exploration. This allows us to see what ports are open for that IP, as well as detect installed apps.

- Secondly, I ran the ping flood attack using the command hping3 -1 --fast “IP address”’ to that same IP address.

- When executing that command, it sends multiple ping requests to the server, causing a massive slow down in network traffic. This creates a denial of service, where the user of said IP address would not be able to perform his/her own tasks due to the overflow request of pings.

How to Mitigate Ping Flood Attacks

- We can use a firewall to prevent ICMP pings happening inside the network at the perimeter.
- We can also apply ‘egress filtering’, which looks for spoofed packets that do not originate from your network.
- You can also add a filter to your monitors to drop suspicious packets that are coming from an unknown source.

Thanks so much for listening!

Questions?