Tyler Ebra
CSEC 2003
October 29, 2024
Incident Report

The UDP protocol reveals that the device on IP address 192.51.100.15 has sent multiple DNS requests to the IP of 203.0.113.2 on port 53.
This is based on the result of the network analysis, which shows that the ICMP echo reply returned the error message UDP port 53 unreachable.
The port noted in the error message is used for DNS as it is port 53.
The most likely issue is that the DNS server is down or that the IP address 192.51.100.15 is being blocked.

The incident began happening at 1:24 all the way until 1:28..
The issue became apparent when customers put in complaints as they could not reach the company website.
The network traffic was analyzed and documented using wireshark.
The network traffic analysis showed that port 53 is the port that is causing the customers to repeatedly fail when trying to connect to the DNS server. The logs indicate that real users are not able to connect to the server due to a high number of SYN requests being sent.

A potential explanation can be a DoS attack that is sending SYN requests to overwhelm the server.
The logs indicate a massive amount of SYN requests being sent to the server from the same IP address.
The most likely explanation is that it is a SYN flood attack.

A SYN flood attack is when a malicious actor sends a large amount of SYN packets they are trying to overload the server and cause it to crash. This works by sending one request that gets acknowledged and then it sends many more SYN until no one else is able to use the server as it is moved all resources to dealing with the overwhelming number of SYN requests.

Packet Capture Using WireShark

The IP address 184.97.44.177 is from Best Buy's website. My VM was listening on port 80. I captured multiple packets using wireshark and was able to observe the connection attempts and successful connection of the device using the IP address of 10.0.2.5.

The first screenshot is the log of the first successful connection attempt and the second screenshot is the log of the successful disconnection of the website. In both screenshots the completed SYN ACK and FIN ACK requests are highlighted.