Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that: This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: “udp port 53 unreachable” The port noted in the error message is used for: DNS The most likely issue is: Port is overloaded with data packets Summary: The UDP protocol reveals that when trying to access DNS lookup for yummyrecipesforme.com, the destination port is unreachable. Using the network analysis tool shows several UDP packets receiving an ICMP response “udp port 53 unreachable”. Port 53 is commonly used as a DNS port. This may be a problem stemming from the host’s firewall configurations, or the web browser itself . This may also be a threat-actor conducting an attack.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

Time incident occurred: 13:24:23 - 13:28:50

Explain how the IT team became aware of the incident: Several customers contacted the company saying they were unable to access the website.

Explain the actions taken by the IT department to investigate the incident:

1. Visit the website to see what happens
2. Next, run the network analyzer tool. Tcdump, and load the webpage again

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):

- Udp port 53 is used for DNS
- The message did not go through to the DNS server, so the IP address for the domain name yummyrecipesforme.com was undetectable

Note a likely cause of the incident:

- There was likely an overloading of port 53 due to the malicious flooding of handshake packets sent to the DNS server.

Summary:

The incident occurred in the early afternoon when several customers reached out regarding inability to access the company website. They were unable to reach the website, receiving the error “udp port 53 unreachable”. The IT department used tcpdump network analysis tool to begin the investigation. The ICMP responses in the logs indicated that port 53, which is typically used for DNS services, had been rendered unreachable. Further investigation is needed to find the exact cause of this error. We need to check the configuration of the firewall to see if it is filtering users from accessing port 53. We will contact the web server to ask them to check if there has been any suspicious activity on their end. There was likely a DoS attack designed by a threat actor injecting UDP packets to overload the DNS server. There may exist a competing company in the same demographic as our client’s whose aim is to halt or slow our client’s business operations.