Cybersecurity Incident Report: Network Traffic Analysis

Frankie Bruno

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

The UDP protocol reveals that:

- The UDP used for the DNS queries, was unable to reach the designated port on the DNS server

This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:

- “udp port 53 is unreachable.” This message was consistently returned in response to the DNS queries, indicating a failure in reaching the DNS server at the specified port.

The port noted in the error message is used for:

- DNS services. Port 53 is the standard port for handling DNS queries, translating domain names into IP addresses.

The most likely issue is:

- A disruption in the DNS server, possible due to a (DoS) attack.

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

Time incident occurred: T

- he timestamp of the incident from the log states (13:24:32.192571) which is [1:24pm] and 32.192571 seconds

Explain how the IT team became aware of the incident:

- Several customers reported not being able to access ‘yummyrecipesforme.com’, receiving the error “destination port unreachable”. Subsequent checks by the IT team gave back the same error, prompting further investigation.

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

- The IT team used a network analyzer tool, tcpdump, to take and analyze the network traffic while attempting to access the website. Using the network analyzer allowed for a detailed examination of the packets sent and received, including error messages.

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

- The error message indicated that UDP port 53 was unreachable
- The source and destination IP addresses identified the user's computer and DNS server
- Repeated ICMP error responses confirmed consistent failure in reaching the DNS server

Note a likely cause of the incident:

- As mentioned above this could be due to a disruption in the DNS server likely caused by a Denial of Service (DoS) attack.