Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The network protocol analyzer revealed that port 53 is unreachable when attempting to access a DNS Server request. Port 53 uses the UDP protocol in order to match the domain name with the corresponding IP address to permit website access. The logs noted the error as port 53 being “unreachable”. This most likely issue for this error is that the DNS server is not responding to the ICMP packet requests.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
This Incident occurred at 1:23 PM. This incident was recognized due to several customer complaints that they were not able to access the company website. This issue is currently being investigated by the IT team in order to get website access back up for the customers. For exploring this error we used the tcpdump packet sniffer so that we could get better detail of what was going on at the server. This is when we found that “udp port 53 unreachable“, meaning that the DNS server was not responding to the ICMP packet requests. This most likely means that the DNS server is down, which could be a result of a misconfiguration or a successful Denial of Service attack on the DNS server. More investigating by the IT team needs to be done to be sure

DNS & ICMP Traffic Log

13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?

yummyrecipesforme.com. (24)

13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2

udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?

yummyrecipesforme.com. (24)

13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2

udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?

yummyrecipesforme.com. (24)

13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2

udp port 53 unreachable length 150