Cybersecurity Incident Report: Network Traffic Analysis

Benjamin Taylor – Google Cybersecurity

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

The UDP protocol reveals that: Port 53 is unreachable when trying to connect to the website containing cooking recipes (yummyrecipesforme.com).

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 length 254".

The port noted in the error message is used for: Port 53 is used for DNS service.

The most likely issue is: No service is listening on the receiving DNS port.

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

Time incident occurred: 1:24 PM, 32.192571 seconds.

Explain how the IT team became aware of the incident: Several customers of clients reported they were not able to access their client company website. They saw the error "destination port unreachable" when waiting for the page to load.

Explain the actions taken by the IT department to investigate the incident: To investigate the incident, the IT department first attempted to visit the website and received the same error message. After loading a network analyzer tool and tcpdump for troubleshooting, an attempt was made to reload the page. Checking the tcpdump log gave the results we needed to assess the situation.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): UDP packets were sent to the DNS server 203.0.113.2 on port 53, and the DNS server responded with an ICMP error: "udp port 53 unreachable". No DNS devices were found listening on that port which presented resolution of the website's domain name.

Note a likely cause of the incident: The most likely cause is that the DNS service on the server at 203.0.113.2 is down, misconfigured, or not running, so it is not listening on UDP port 53. This is potentially preventing domain resolution.