Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption
One potential explanation for the website's connection timeout error message is: The logs show that: a large number of TCP SYN requests coming from an unfamiliar IP address causing the web server to stop responding This event could be: SYN attack, a type of DoS attack

Section 2: Explain how the attack is causing the website to malfunction
When website visitors try to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. Explain the three steps of the handshake: 1.A SYN packet is sent from the source to the destination, requesting to connect. 2. The destination replies to the source with a SYN-ACK packet to accept the connection request. The destination will reserve resources for the source to connect. 3. A final ACK packet is sent from the source to the destination acknowledging the permission to connect. Explain what happens when a malicious actor sends a large number of SYN packets all at once:overwhelms the server’s available resources to reserve for the connection. When this happens, there are no server resources left for legitimate TCP connection requests. Explain what the logs indicate and how that affects the server:server is unable to open a new connection to new visitors who receive a connection timeout message.

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that: The DNS request from the client computer to the DNS server did not reach its destination because the server was not responding to port 53 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,” indicating that the DNS server is not responding or is misconfigured The port noted in the error message is used for: DNS resolution, which translates domain names into IP addresses The most likely issue is: the DNS server is either down, misconfigured, or blocking requests on port 53, preventing clients from resolving domain names

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
Time incident occurred:1:24pm, 32.192571 seconds Explain how the IT team became aware of the incident: customers reporting not being able to access the website Explain the actions taken by the IT department to investigate the incident: Verify DNS Server Status using network monitoring tools Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): ICMP error message confirmed that no service was listening on port 53, may have been caused by a server outage, misconfiguratrion, or a firewall blocking DNS traffic Note a likely cause of the incident:DNS server failure, firewall or security policy change, network connectivity issue

Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the tcpdump log

As part of the DNS protocol, the UDP protocol was used to contact the DNS server to retrieve the IP address for the domain name of yummyrecipesforme.com. The ICMP protocol was used to respond with an error message, indicating issues contacting the DNS server. The UDP message going from your browser to the DNS server is shown in the first two lines of every log event. The ICMP error response from the DNS server to your browser is displayed in the third and fourth lines of every log event with the error message, “udp port 53 unreachable.” Since port 53 is associated with DNS protocol traffic, we know this is an issue with the DNS server. Issues with performing the DNS protocol are further evident because the plus sign after the query identification number 35084 indicates flags with the UDP message and the “A?” symbol indicates flags with performing DNS protocol operations. Due to the ICMP error response message about port 53, it is highly likely that the DNS server is not responding. This assumption is further supported by the flags associated with the outgoing UDP message and domain name retrieval.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred today at 1:24 p.m. Customers notified the organization that they received the message “destination port unreachable” when they attempted to visit the website yummyrecipesforme.com. The cybersecurity team providing IT services to their client organization are currently investigating the issue so customers can access the website again. In our investigation into the issue, we conducted packet sniffing tests using tcpdump. In the resulting log file, we found that DNS port 53 was unreachable. The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server might be down due to a successful Denial of Service attack or a misconfiguration.