A Cybersecurity Incident Response Report

Summary of the problem found in the traffic log
The network protocol analyzer(tcpdump) logs indicate that UDP port 53 is unreachable when attempting to access the website. Port 53 is a port used for DNS service. This means that the UDP message that requests an IP address for the company website's domain did not go through to the DNS server because no service was listening on the receiving DNS port. This indicates a problem with the web server or the firewall configuration. This may be an indication of a malicious attack probably a DoS SYN attack on the server.

Analysis of the data and cause of the incident
The incident occurred in the mid-morning hours when several customers of our client company reported that they were not able to access the company's website and saw an error "destination port unreachable" on the webpage. I responded and began running tests with the network protocol analyzer tool tcpdump at 1.24 pm. The resulting logs revealed that port 53, which is used for DNS service, is not reachable. I continued to send requests but still received ICMP packets with the same delivery error. I forwarded the issue to my direct supervisor who sent it to security engineers who will investigate the root cause of the issue to determine how we can restore access to the client website. Our next steps include checking the firewall configuration to see if port 53 is blocked and contacting the system administrator for the web server to have them check the system for signs of an attack. The network security team suspects this person might have launched a DoS attack to crash the client company website.