The Exemplar Explained
Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log	Explanation
A. The UDP protocol reveals that the DNS server is down or unreachable. B. As evident by the results of the network scan, the ICMP echo reply returned the error message: "udp port 53 unreachable"." C. Port 53 is commonly used for DNS protocol traffic. It is highly likely the DNS server is not responding.	A. **Offers a brief summary of the DNS and ICMP log analysis.** Following the instructions, you should have identified "which network protocol and service were impacted by this incident." The scenario states: "[The log file] displays which protocol was used to handle communications and which port it was delivered to. In the error log, this shows as udp port 53 unreachable. This means that the UDP protocol was used to request a domain name resolution using the address for the DNS server over port 53." B. **Gives a few details on what was indicated in the logs:** The Scenario section states that you performed a network analysis using tcpdump, which recorded ICMP packets from your source computer to the IP address and port for the website (203.0.113.2.domain). It also recorded the ICMP responses from the website back to your computer. If you check the DNS and ICMP error log, the ICMP replies include an error message type, which tcpdump represents as "udp port 53 unreachable." C. **Interpret the issues found in the logs.** The Scenario section (or a quick internet search for "port 53") will show that this port number is commonly used for DNS protocol communications. Since port 53 is unreachable and that port is commonly used for DNS server

	communications, you can conclude that the DNS server is unreachable or “not responding.” This could be caused by a DoS attack against the DNS server, for example.

Part 2: Explain your analysis of the data and provide one solution to implement	Explanation
D. The incident occurred today at 1:23 p.m..	D. **States when the problem was first reported:** This info was obtained from the log file date and time stamps. In the log, this is the first sequence of numbers displayed: 13:24:32.192571. This displays the time 1:24 p.m., 32.192571 seconds, with the hour in 24-hour format. The Scenario indicates this event occurred today.
E. Customers called the organization to notify the IT team they received the message “destination port unreachable” when they attempted to visit the website.	E. **Provides the scenario, events, and symptoms identified when the event was first reported:** The Scenario states that, “A handful of customers contacted your company to report that they were not able to access the company website, and saw the error “destination port unreachable” after waiting for the page to load.”
F. The network security professionals within the organization are currently investigating the issue so customers	F. **Explains the current status of the issue:** The Scenario states that, "This incident, in the meantime, is being handled by security engineers after you and other analysts have reported the issue to

can access the website again.	your direct supervisor."
G. 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.	G. **Describes info discovered from investigating the issue up to this point in time:** Provides a concise recap of what you did to investigate the issue. The Scenario states,"You visit the website and you also receive the error "destination port unreachable." Next, you load your network analyzer tool, tcpdump, and load the webpage again. This time, you receive a lot of packets in your network analyzer. In the analyzer, you send UDP packets and receive an ICMP response to return to the host. The results contain an error message: "udp port 53 unreachable.""
H. The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall.	H. **Lists the next steps in troubleshooting and resolving the issue:** The next step in troubleshooting is to determine if the DNS server is not functioning properly. If the DNS server is fine, the team should check the firewall settings to see if someone changed the configuration to block network traffic on port 53. Firewalls offer the ability to block network traffic on specific ports. Port blocking can be used to stop or prevent an attack.
I. DNS server might be down due to a successful Denial of Service attack or a misconfiguration.	I. **Provides the suspected root cause of the problem:** Previously, you learned about several types of Denial of Service (DoS) attacks. The goal of a DoS attack is to send a flood of information to a network device, like a DNS server, to crash it or make it unable to respond to legitimate network traffic. It is possible that an attacker disabled the DNS server with a DoS attack. Alternatively, someone from your team could have made a configuration change on the firewall that blocked port 53.