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. 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. B. 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	A. **Include a brief summary of the tcpdump log analysis and identify which protocols were used for the network traffic.** The scenario summarizes the issue and identifies the protocols used. The scenario states: “To load the webpage, your browser first sends a query to a DNS server via the UDP protocol to retrieve the IP address for the website's domain name; this is part of the DNS protocol...The analyzer shows that when you send UDP packets to the DNS server, you receive ICMP packets containing the error message: “udp port 53 unreachable.” ” B. **Provide a few details on what was indicated in the log.** The first and second step of the scenario section states that you performed a network analysis using tcpdump, which recorded UDP packets from your source computer to the IP address and port for the DNS server (203.0.113.2.domain). It also recorded the ICMP error responses from the DNS server back to your computer with the error message “udp port 53 unreachable.” We mention in the 6th step that “Port 53, is a port for DNS service,” which means this is an issue with the DNS server. We include further signs of issues with DNS performance in the fifth step of the scenario, “The plus sign after the query identification number indicates there are flags associated with the UDP message. The "A?" indicates a flag associated with

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. C. 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.	the DNS request for an A record, where an A record maps a domain name to an IP address." C. **Interpret the issues found in the log.** 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 at least one cause of the incident	Explanation
D. The incident occurred today at 1:24 p.m.	D. **State 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 notified the organization that they received the message “destination port unreachable” when they attempted to visit the website yummyrecipesforme.com.	E. **Provide 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 cybersecurity team providing IT services to their client organization are currently investigating the issue so customers can access the website again. 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.	F. **Explain 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 your direct supervisor." G. **Describe 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. **List 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. **Provide 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.