Cybersecurity Incident Report: Network Traffic Analysis

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

As part of the DNS protocol, the UDP protocol was employed to contact the DNS server for retrieving the IP address associated with the domain name bountyhunting.com. The ICMP protocol responded with an error message, indicating difficulties in establishing communication with the DNS server.

The UDP message, originating from your browser and directed towards the DNS server, is depicted in the first two lines of every log event. Subsequently, the ICMP error response from the DNS server to your browser is displayed in the third and fourth lines of each log event, accompanied by the error message, "udp port 53 unreachable." Given that port 53 is specifically linked to DNS protocol traffic, it is apparent that the issue lies with the DNS server.

Issues with the DNS protocol are clear. Look for a plus sign after query ID 35084, showing flags with the UDP message, and an “A?” symbol, indicating problems with DNS operations. The ICMP error mentioning port 53 strongly hints that the DNS server isn't working. This idea is backed by flags linked to the outgoing UDP message and the process of getting the domain name.

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

The incident occurred today at 4:00 p.m. Customers reported receiving the message "destination port unreachable" when attempting to visit the website bountyhunting.com. The cybersecurity team, responsible for providing IT services to their client organization, is currently investigating the issue to restore customer access to the website.

In our investigation, we conducted packet sniffing tests using tcpdump. In the resulting log file, we discovered that DNS port 53 was unreachable. The next step is to determine whether the DNS server is down or if traffic to port 53 is being blocked by the firewall. The DNS server may be down due to a successful Denial of Service attack or a misconfiguration.

step is to determine whether the DNS server is down or if traffic to port 53 is being blocked by the firewall. The DNS server may be down due to a successful Denial of Service attack or a misconfiguration.