Cybersecurity Incident Report: Network Traffic Analysis (My Responses)

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
The UDP protocol reveals that: Based on this scenario, I predict that the DNS server was contacted using the UDP protocol to retrieve the IP address for the domain name yummyrecipesforme.com which is part of the DNS protocol. This is crucial evidence because it uses UDP to send requests and receive responses. Then the browser initiates the request to the DNS server via a UDP packet. **This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message:** From the network analysis in the scenario and the supporting files given, it was found that after sending a UDP packet to the DNS server, the system received an ICMP error response. The ICMP message contained the error "udp port 53 unreachable", indicating that the DNS server on the specified port could not be reached. **The port noted in the error message is used for:** In the supporting files, the error message specifically points to port 53, which is the default port used for DNS protocol traffic. Port 53 is essential for DNS operations, as it handles both UDP and TCP traffic related to DNS queries. The error also suggests that the DNS service on this port is unavailable or blocked. **The most likely issue is:** Overall, based on the scenario, since the ICMP error message was indicating that UDP port 53 is unreachable, it is likely or very predictable that the DNS server is either down, misconfigured, or under attack (security risk). Since there was an absence of responses from the server on port 53, this evidence suggests that it is not functioning correctly or not operational. Upon investigating, I hypothesize that this could be due to a Denial of Service (DoS) attack aimed at overwhelming the DNS server, or it could be a misconfiguration in the firewall blocking the traffic to port 53.

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

Time incident occurred:
With the given supporting files and the scenario give, it is noticeable that the incident occurred at 1:24 p.m. You can see the exact time through the timestamp 13:24:32.192571 in the tcpdump log (supporting attachments that were given), which shows the specific time of the first incident-related packet capture.

Explain how the IT team became aware of the incident:
Based on the scenario and the evidences, I predict that the IT team became aware of the issue when a handful of customers reported that they could not access the website yummyrecipesforme.com. This is where then the customers saw the error message "destination port unreachable" when trying to load the page. Because of this, it alerted the team to investigate the problem with DNS resolution.

Explain the actions taken by the IT department to investigate the incident:
I noticed that based on the reports, the cybersecurity team began their investigation by performing packet sniffing tests using tcpdump, a network analysis tool. As given on the support documents attached and the scenario sequence of events that happened, the test involved capturing network traffic and examining the packets exchanged between the browser and the DNS server. Then, the team analyzed the logs and observed that the UDP packets sent to the DNS server were followed by ICMP error messages indicating that port 53 was unreachable.

Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.):
Based on the evidences, the key findings of the IT department's investigation included: **1)** the Port 53 was unreachable on the DNS server as the error message "udp port 53 unreachable" appeared in the ICMP response; **2)** the UDP packets were being sent by the browser, but no response was received from the server; **3)** The flags associated with the UDP message and the query identification number (35084) indicated that a DNS query for an A record was being made, but the request was not being resolved, likely due to the server being down or unreachable; **4)** The DNS server IP address under investigation was 203.0.113.2.

Note a likely cause of the incident:
Overall, with this in mind, I hypothesize and conclude that the likely cause of this security risk issue is a Denial of Service (DoS) attack and could have been aimed at the DNS server, overwhelming it with traffic and causing it to become unresponsive. However, I also believe that the problem could also be related to a misconfiguration in the firewall, which could have hypothetically blocked traffic to port 53 as a defensive measure or an unauthorized change in the configuration system by someone or something...

Additional Information:

Review the scenario below. Then complete the step-by-step instructions.
You are a cybersecurity analyst working at a company that specializes in providing IT services for clients. Several customers of clients reported that they were not able to access the client company website www.yummyrecipesforme.com, and saw the error “destination port unreachable” after waiting for the page to load.
You are tasked with analyzing the situation and determining which network protocol was affected during this incident. To start, you attempt to visit the website and you also receive the error “destination port unreachable.” To troubleshoot the issue, you load your network analyzer tool, tcpdump, and attempt to load the webpage again. To load the webpage, your browser 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. Your browser then uses this IP address as the destination IP for sending an HTTPS request to the web server to display the webpage 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.”

```
13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 254

13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 320

13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A?
yummyrecipesforme.com. (24)
13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2
udp port 53 unreachable length 150
```

In the tcpdump log, you find the following information:

1. The first two lines of the log file show the initial outgoing request from your computer to the DNS server requesting the IP address of yummyrecipesforme.com. This request is sent in a UDP packet.
2. The third and fourth lines of the log show the response to your UDP packet. In this case, the ICMP 203.0.113.2 line is the start of the error message indicating that the UDP packet was undeliverable to port 53 of the DNS server.
3. In front of each request and response, you find timestamps that indicate when the incident happened. In the log, this is the first sequence of numbers displayed: 13:24:32.192571. This means the time is 1:24 p.m., 32.192571 seconds.
4. After the timestamps, you will find the source and destination IP addresses. In the first line, where the UDP packet travels from your browser to the DNS server, this

information is displayed as: 192.51.100.15 > 203.0.113.2.domain. The IP address to the left of the greater than (>) symbol is the source address, which in this example is your computer's IP address. The IP address to the right of the greater than (>) symbol is the destination IP address. In this case, it is the IP address for the DNS server: 203.0.113.2.domain. For the ICMP error response, the source address is 203.0.113.2 and the destination is your computers IP address 192.51.100.15.

5. After the source and destination IP addresses, there can be a number of additional details like the protocol, port number of the source, and flags. In the first line of the error log, the query identification number appears as: 35084. The plus sign after the query identification number indicates there are flags associated with the UDP message. The "A?" indicates a flag associated with the DNS request for an A record, where an A record maps a domain name to an IP address. The third line displays the protocol of the response message to the browser: "ICMP," which is followed by an ICMP error message.
6. The error message, "udp port 53 unreachable" is mentioned in the last line. Port 53 is a port for DNS service. The word "unreachable" in the message indicates the UDP message requesting an IP address for the domain "www.yummyrecipesforme.com" did not go through to the DNS server because no service was listening on the receiving DNS port.
7. The remaining lines in the log indicate that ICMP packets were sent two more times, but the same delivery error was received both times.

Now that you have captured data packets using a network analyzer tool, it is your job to identify which network protocol and service were impacted by this incident. Then, you will need to write a follow-up report.

As an analyst, you can inspect network traffic and network data to determine what is causing network-related issues during cybersecurity incidents. Later in this course, you will demonstrate how to manage and resolve incidents. For now, you only need to analyze the situation.

This event, in the meantime, is being handled by security engineers after you and other analysts have reported the issue to your direct supervisor.

Step 3: Provide a summary of the problem found in the tcpdump log

After analyzing the data presented to you from the tcpdump log, identify trends in the data. Assess which protocol is producing the error message from the DNS server for the yummyrecipesforme.com website. Recall that one of the ports that is displayed repeatedly is port 53, commonly used for DNS. In your analysis:

- Include a brief summary of the tcpdump log analysis and identify which protocols were used for the network traffic.
- Provide a few details about what was indicated in the log.
- Interpret the issues found in the log.

Record your responses in part one of the cybersecurity incident report.

Step 4: Explain your analysis of the data and provide one solution to implement

Now that you've inspected the traffic log and identified trends in the traffic, describe why the error messages appeared on the log. Use your answer in the previous step and the scenario to identify the reason behind the ICMP error messages. The error messages indicate that there is an issue with a specific port. What do the different protocols involved in the log reveal about the incident? In your response:

- State when the problem was first reported.
- Provide the scenario, events, and symptoms identified when the event was first reported.
- Explain the current status of the issue.
- Describe the information discovered while investigating the issue up to this point.
- List the next steps in troubleshooting and resolving the issue.
- Provide the suspected root cause of the problem.

Record your responses in part two of the cybersecurity incident report.

What to Include in Your Response

Be sure to address the following items in your completed activity:

- Provide a summary of the problem found in the tcpdump log
- Explain your analysis of the data and provide one possible cause of the incident