Cybersecurity Incident Report

Task:

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.” Identify the type of attack causing this network interruption and explain how the attack is causing the website to malfunction.

```
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
```

Section 1: Identify the type of attack that may have caused this network interruption
The DNS protocol relies on UDP to communicate with the DNS server and retrieve the IP address for a domain, in this case, *yummyrecipesforme.com*. However, an ICMP error message was returned, indicating that port 53, the standard port for DNS traffic, was unreachable. This suggests an issue with the DNS server itself. The logs show that the outgoing UDP message from the browser to the DNS server includes a query identification number (35084) and flags, as indicated by a plus sign (+) and the "A?" symbol. These flags highlight potential issues with the DNS protocol operations. The ICMP error response further confirms that the DNS server is likely unresponsive, preventing successful domain name resolution.

Section 2: Explain how the attack is causing the website to malfunction
At 1:24 p.m. today, customers reported receiving a "destination port unreachable" error when trying to access *yummyrecipesforme.com*. The cybersecurity team began investigating the issue to restore website access. Using packet sniffing tests with `tcpdump`, they identified that DNS port 53 was unreachable. The next step is to determine whether the issue is caused by the DNS server being down or by a firewall blocking traffic to port 53. Potential causes include a Denial of Service (DoS) attack or a misconfiguration affecting the DNS server.