Cybersecurity Incident Report: Network Traffic Analysis

Scenario

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
```

A summary of the problem found in the DNS and ICMP traffic log.
The DNS query from the browser could not be delivered to the DNS server because the destination port was unreachable, this is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: “udp port 53 unreachable”. The port noted in the error message is used for: DNS services that resolve domain into IP address, and the DNS service on the server was unavailable or not listening on port 53, preventing domain name resolution.

Analysis of the data and provide at least one cause of the incident.
Time incident occurred: 13.24.32.192571 The IT team became aware of the incident after users reported being unable to access a specific website, and the network monitoring tools captured error logs indicating DNS resolution failures and immediately after receiving the alert, they used tcpdump to inspect

traffic between the client and the DNS server. They reviewed the UDP queries sent to the DNS server and the ICMP responses received.

The investigation revealed that UDP packets sent from the client (192.51.100.15) to the DNS server (203.0.113.2) on port 53 were returned with ICMP error messages stating “udp port 53 unreachable.” This indicated that DNS requests could not be processed. The likely cause of the incident was that the DNS service on the server was unavailable or not listening on port 53, which prevented domain name resolution and caused website access failures.