Cybersecurity Incident Report: Network Traffic Analysis

In this example, I will analyze DNS and ICMP traffic in transit using data from a network protocol analyzer tool.

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
```

Incident Report

Summary of Incident

www.yummyrecipesforme.com was inaccessible for users. Cybersecurity analysts accessed the ICMP logs to find port 53 was non operational. Most likely the DNS server, associated with port 53, was unresponsive, thus no translation of IP addresses could be made from the user or web domain, thus no access to the website for users.

Analysis

At 13:24, use of the website www.yummyrecipesforme.com halted and users contacted the IT department, a department which cybersecurity aids in, and told them they kept getting an error "destination port unreachable". The task was escalated to a cybersecurity analyst who accessed the internet control message protocol (ICMP) logs with tcdump, a network protocol analyzer tool (packet sniffer), to find while outside network IP addresses were requesting data, "udp port 53 unreachable" was continuously appearing; port 53 is associated with DNS servers. Most likely the DNS server was down and the issue was escalated to network engineers to investigate the DNS server, which was most likely hosted by a 3rd party company. Some reasons the DNS server could have been down include: Dos/DDos attack, power outage, misconfiguration, and blocked firewall access.