# **Incident Report:**

# **Network Traffic Analys**is

As 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.

I was tasked with analyzing the situation and determining which network protocol was affected during this incident. To start, i attempted to visit the website and i also received the error “destination port unreachable.” To troubleshoot the issue, i loaded my network analyzer tool, tcpdump, and attempt to load the webpage again. To load the webpage, my 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. My 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.”

| **Summary of the problem found in the DNS and ICMP**  **traffic log**. |
| --- |
| The network protocol analyzer logs indicate that port 53 is unreachable when attempting to access the company website. Port 53 is normally used for DNS service. This may indicate a problem with the network connectivity, DNS server availability, incorrect DNS settings, ISP issues, DNS query size or the firewall configuration etc. It is possible that this is an indication of a malicious attack on the web server, a DDoS or DoS specifically |
|

| **Analysis of the data** |
| --- |
| The incident occurred towards mid-day when customers reported that they could not reach the company website. The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used for DNS service, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the secure web portal. As a member of the network security team I was told to check the firewall configuration to see if port 53 is blocked and contact the system administrator for the web server to have them check the system for signs of an attack and also check if the DNS server is down. The network security team suspects this person might have launched a DoS attack to crash the DNS server. |