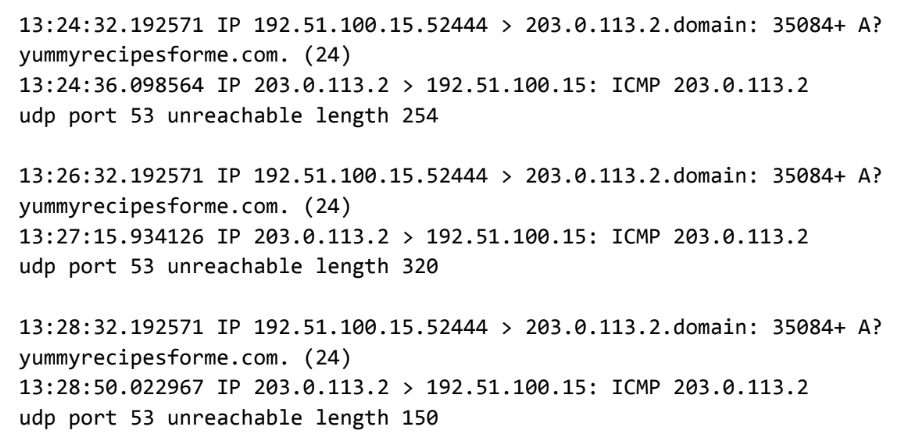
***Cyber Security Scenario and Incident Report for Yummyrecipesforme.com***

You are a cybersecurity analyst working at a company that specializes in providing IT consultant services. Several customers contacted your company to report that they were not able to access the 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 visit the website and you also receive the error “destination port unreachable.” Next, you load your network analyzer tool, tcpdump, and load the webpage again. This time, you receive a lot of packets in your network analyzer.

The analyzer shows that when you send UDP packets and receive an ICMP response returned to your host, the results contain an error message: “udp port 53 unreachable.”



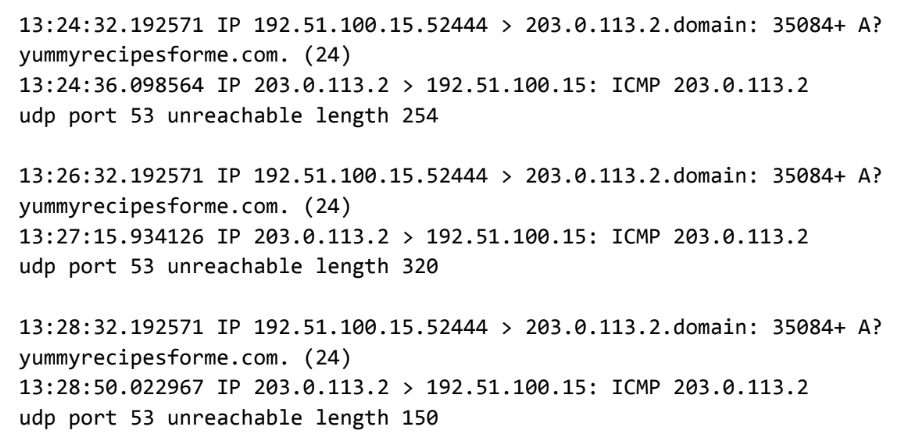
In the DNS and ICMP log, you find the following information:

1. In the first two lines of the log file, you see 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.

1. Next you find timestamps that indicate when the event happened. In the log, this is the first sequence of numbers displayed. For example: 13:24:32.192571. This displays the time 1:24 p.m., 32.192571 seconds.
2. The source and destination IP address is next. In the error log, this information is displayed as: 192.51.100.15.52444 > 203.0.113.2.domain. The IP address to the left of the greater than (>) symbol is the source address. In this example, the source 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
3. The second and third lines of the log show the response to your initial ICMP request packet. In this case, the ICMP 203.0.113.2 line is the start of the error message indicating that the ICMP packet was undeliverable to the port of the DNS server.
4. Next are the protocol and port number, which displays which protocol was used to handle communications and which port it was delivered to. In the error log, this appears as: udp port 53 unreachable. This means that the UDP protocol was used to request a domain name resolution using the address of the DNS server over port 53. Port 53, which aligns to the .domain extension in 203.0.113.2.domain, is a well-known port for DNS service. The word “unreachable” in the message indicates the message did not go through to the DNS server. Your browser was not able to obtain the IP address for yummyrecipesforme.com, which it needs to access the website because no service was listening on the receiving DNS port as indicated by the ICMP error message “udp port 53 unreachable.”
5. The remaining lines in the log indicate that ICMP packets were sent two more times, but the same delivery error was received both times.

Cybersecurity Incident Report:

Network Traffic Analysis



|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log. |
| The UDP protocol reveals that: Upon opening a web browser and visiting the site “Yummyrecipesforme.com”, the website is unsearchble  This incident is based on the results of the network analysis, which show that the ICMP echo reply returned the error message: udp port 53 unsearchable length 320  The port noted in the error message that this particular message is used for: Domain Name services  The most likely issue is: This is a (DoS) attach at work |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| Time incident occurred: 1:24 pm  Explain how the IT team became aware of the incident: When different members of the SOC team visited the website the page did not load.  Explain the actions taken by the IT department to investigate the incident: When the page was visited a second time with the network analyzer tool (Packet sniffer) we received an error message  Note key findings of the IT department's investigation (i.e., details related to the port affected, DNS server, etc.): udp port 53 unserachable  Note a likely cause of the incident: DoS acctack or DDoS attack |

Cybersecurity Incident Report: Network Traffic Analysis

|  |
| --- |
| Part 1: Provide a summary of the problem found in the DNS and ICMP  traffic log |
| The UDP protocol reveals that the DNS server is unreachable. This can be the result of a number of causes. The results of the network analysis revealed that the ICMP echo reply returned the following  error message “udp port 53 unreachable,”  Port 53 is known for DNS protocol traffic. Taking into consideration all of the above it is likely that the DNS server is not responding. |
|

|  |
| --- |
| Part 2: Explain your analysis of the data and provide at least one cause of the incident. |
| The incident occurred today at 1:23 p.m.. Several clients contacted the organization to notify the IT team that they received the message “destination port unreachable” when they attempted to visit the website. The COS team within the organization is currently investigating the issue so customers can access the website. During the investigation of the incident, we conducted packet analyzation tests using tcpdump. In the resulting log file, we discovered that that DNS port 53 was unreachable. At this juncture, the COS team must determine wheter or not the DNS server is down or traffic to port 53 is blocked by the firewall. It is likely the case that the DNS server might be down due to a successful Denial of Service attack or a misconfiguration. |