

Cybersecurity Incident Report:

Network Traffic Analysis

Part 1: Provide a 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 food recipe website. Port 53 is normally used for DNS traffic. DNS is responsible for translating domain names (such as "yummyrecipesforme.com") into corresponding IP addresses that computers can understand. This problem may arise from misconfigured firewall rules, network connectivity issues, or the DNS server being down or unresponsive. It also may be the indication of a malicious DOS attack on the web server.

Part 2: Explain your analysis of the data and provide one solution to implement

The incident occurred earlier this afternoon when several users of the website as well as developer's team reported that they could not access the "yummyrecipesforme.com" 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 traffic, is not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore access to the website securely. Our next steps include investigating and addressing the firewall configuration. We check the firewall rules to ensure that inbound and outbound traffic on port 53 is allowed for DNS communication. If necessary, we adjust the firewall rules to permit DNS traffic between the client and the DNS server. This solution focuses on addressing any potential blockages or misconfigurations in the firewall that may be causing the port 53 unreachability, thereby enabling proper DNS resolution and resolving the issue with accessing the desired websites.