

Incident Report

Incident Description

Several customers reported being unable to access the company website "www.yummyrecipesforme.com" and encountered the "destination port unreachable" error message upon page load. As a cybersecurity analyst, I was tasked with investigating and determining which network protocol and service were affected during this incident.

Analysis Performed

Personally visited the mentioned website and confirmed encountering the "destination port unreachable" error.

Utilized the network analysis tool, tcpdump, to capture packets while reloading the webpage.

During the analysis of the captured packets, it was found that when sending UDP packets and receiving an ICMP response, the results indicated an error message: "udp port 53 unreachable."

Reviewed the DNS and ICMP logs, and found the following relevant information:

The initial outgoing request from my computer to the DNS server for the IP address of yummyrecipesforme.com was recorded in the first two lines of the log. This request was sent in a UDP packet.

Timestamps indicated when the event occurred.

Source and destination IP addresses were identified. In the case of the error, the source IP address corresponds to my computer, and the destination IP address corresponds to the DNS server.

The subsequent lines in the log showed the response to my initial ICMP request. In this case, the ICMP 203.0.113.2 line indicated that the ICMP packet was undeliverable to the DNS server's port.

Affected Protocol and Service:

Based on the performed analysis, it was determined that the UDP protocol and the DNS service were affected during this incident. The error message "udp port 53 unreachable" indicates a failure to establish communication with the DNS server through port 53.

Oksana Syvun

Recommendations

Verify the availability and proper functioning of the DNS server used for domain name resolution.

Perform additional testing to identify any other potential issues that may impact the website's connectivity and accessibility.

Conclusions

The conducted analysis revealed that the incident of inaccessibility to the website www.yummyrecipesforme.com was related to a problem with the UDP protocol and the DNS service. It is important to take measures to address and resolve this issue, ensuring the proper functioning of the utilized DNS service.