Incident Report

Date: 11-04-2022
Investigated by: Max, Geoff, Tyler
Report Typed by: Max
Fwd To: (Details removed for privacy reasons)

_____

What Happened:

The UDP protocol indicates that the DNS server is either down or unreachable. This is evidenced by the network analysis results, which show that the ICMP echo reply returned the error message "udp port 53 unreachable." Port 53 is typically designated for DNS protocol traffic. It is highly probable that the DNS server is not responsive.

Our Analysis:

The incident transpired today at 11:23pm. The organization was alerted by customers who reported encountering the message "destination port unreachable" when attempting to access the website. The IT team promptly initiated an investigation to resolve the issue and restore customer access.

As part of our investigation, we conducted packet sniffing tests utilizing tcpdump. The resulting log file revealed that DNS port 53 was unreachable. Our next course of action is to determine whether this unreachability is due to the DNS server being down or if traffic to port 53 is being obstructed by the firewall. Potential causes for the DNS server unavailability could range from a successful Denial of Service attack to a configuration error.