Shafee Ahmed

Wednesday, Feb 14 2024

Axiom Apparel 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 a client is attempting to use the DNS server to resolve a domain name. In this case, axiomapparel.com. However, there is a communication error since the expected DNS responses are not being received. This is based on the results of the network analysis, which show that the ICMP echo reply returned the error message "port unreachable". This suggests that the destination device is not able to receive packets on port 53. The port noted, port 53, is typically used for DNS services. DNS uses this port number to listen to queries from clients. The issues may indicate a problem with either an absent DNS service on port 53, firewall blockage(s), or an misconfigured DNS configuration.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident was detected at 13:24 today. Automated alerts and user reports of inability to access the website axiomapparel.com. The IT department used a variety of investigations to analyze the incident. tcpdump was used to monitor network traffic and quickly identify the high volume of "port unreachable" error messages from our DNS server. The most likely issue is there is either no DNS service on that server. Or, a firewall could be blocking UDP traffic on port 53. Another possible issue could be an incorrect DNS configuration, which might have led to the inability to establish a connection on that required port.