Cybersecurity Incident Report

Section 1: Identify the type of attack that may have caused this network interruption

Our monitoring system reported an issue with the web server. After attempting to visit the company's website, I received a timeout connection error. Network attacks can come in the form of DoS or DDoS attacks. Knowing this, I read Wireshark's TCP/HTTP logs. Reading the logs, I see one particular IP address continuously sending SYN packets. After a certain point, the logs only contain SYN packets from this one IP address. I can conclude this is the DoS attack type, SYN flooding.

Section 2: Explain how the attack is causing the website to malfunction

With the TCP protocol, a normal process would be three steps to establish a connection between devices:

1. SYN packet
2. SYN/ACK packet
3. ACK packet

Currently, our web server is only receiving SYN packets, which is abnormal. With a DoS (Denial-of-Service) attack, the attack comes from a single source, rather than multiple sources. Attacks from multiple sources and locations are a DDoS (Distributed Denial-of-Service) attack. In this case our SYN flood attack is coming from the one IP address, making it a DoS attack. Because of this IP address sending continuous SYN packets to the web server, it takes longer and longer for the web server to respond. This causes the server to eventually shutdown, and become unresponsive with the amount of packets it is receiving. That is why the company's website is only loading the timeout connection error. Due to this, employees will be unable to access the company's website indefinitely. This damages performance and revenue.

To avoid this in the future, the company should invest in a VPN. We can also bolster our firewall to make sure it is not accepting IP addresses that are the same/copy within the internal network from outside. A review of policies would also help to make sure employees are not accessing the company website through an unprotected WiFi network.