Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	The IT department was advised by employees they were unable to access the internal network. The cybersecurity analyst noticed the organization's network services suddenly stopped responding due to incoming flood of ICMP packets. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The company's Cybersecurity team investigated the security event and determined that a malicious actor had sent a flood of ICMP pings through an unconfigured firewall. This vulnerability allowed the threat actor to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Identify	Cybersecurity analysts have determined that a DDoS attack had occurred which overwhelmed the network causing the system to be down for 2 hours. The DDoS attack happened because a malicious actor was able to gain access to the network through an unconfigured firewall by sending a flood of ICMP pings. This then spread across the network affecting servers, users, and services.
Protect	● Firewall maintenance by implementing a stateful firewall: This entails checking and updating security configurations regularly to stay ahead

	of potential threats. ○ This can happen regularly. The rules can be updated in response to an event that allows abnormal network traffic into the network. In this instance this will protect from future DDoS attacks. ● Port filtering: A firewall function that blocks or allows certain port numbers to limit unwanted communication. ○ Port filtering is used to control network traffic and can prevent potential attackers from entering a private network. ● Implement IDS/IPS systems: An IDS system will detect and alert the network administrator about possible intrusions, attacks, and other malicious traffic. The IPS system will monitor activity for intrusions and anomalies and take action to stop them. ○ With both systems in place they will monitor the network traffic coming in to check for intrusions and if they detect intrusion they will alert the network administrator of any malicious attacks while also trying to prevent access. ● Implement SIEM tool: Is an application that collects and analyzes log data to monitor critical activities in the organization. It works in real time to report suspicious activity in a centralized dashboard. ○ It will analyze network log data sourced from IDSs, IPSs, firewalls, VPNs, proxies, and DNS logs.
Detect	The cybersecurity team will utilize the SIEM to monitor network traffic that is being received. It will utilize the log data that is being received by the intrusion detection system, the intrusion prevention system and firewall. This will allow security analysts to detect unauthorized attacks in the future.
Respond	The incident management team will isolate affected systems to prevent further disruption to the network. They will attempt to restore critical systems and services that were disrupted by the event. Advise upper management and

	appropriate legal authorities of the attack. They can notify clients of the network down time.
Recover	Once the cybersecurity team has established firewall maintenance this will block ICMP flood attacks. The next step would be for all non-critical network services to be put offline to reduce the spread of the infection. Next will be restoring critical network services that should be done first. Once the flood of ICMP packets have timed out, all non-critical network systems and services should be brought back online after making sure devices and servers have been cleared of any infection.

Reflections/Notes: