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	Today we were alerted that our organization’s internal network was down for two hours. During those two hours the organization’s network services were not responding due to a flood of incoming ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking the flow of incoming ICMP packets and shutting down all non-critical network services and restoring critical services. After investigation by the cybersecurity team, this was the result of a DDos attack which the malicious attacker was able to launch a flood of ICMP pings into the company’s network through an unconfigured firewall.
Identify	The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that a malicious actor or actors launched a flood of ICMP pings into the company’s network through an unconfigured firewall. This caused the organization’s network services to suddenly not respond due to the flood of ICMP packets.
Protect	The team has implemented the following: - A new firewall rule that limits the rate of incoming ICMP packets - An IDS/IPS system to filter out some ICMP traffic based on suspicious

	characteristics
Detect	To detect these type of attacks, the team configured a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, installed a network monitoring software to detect abnormal traffic patterns to prevent an DDoS attack from bringing the organization’s network services.
Respond	For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore all critical network services and services that were disrupted during the event. The team has already instituted firewall rules and configurations to mitigate risk of another attack like this occurring. The team will also use SIEM tools to analyze network logs to check for suspicious and abnormal activity. The team will also inform upper management about this event and they will inform their small business partners about their network services being down. The team will also report all incidents appropriate legal authorities, if applicable.
Recover	To recover from a DDoS attack, access to access to network services needs to be restored to a functional state to allow for normal network operations. Fortunately, in a DDoS attack data is not tampered with, only the systems and servers fail. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: This was a great activity which showed me the usefulness of the CSF when dealing with a security incident. It allows me to first gain an understanding of the important summary of event that took place in the security incident. Then it helps me with organizing my thought process on how to respond to proactively prevent an incident from occurring but then how to respond to one in the moment as well as mitigate the risk of future attacks.