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	Organization's network services stopped responding. ICMP logs shows a flood of ICMP Packets, indicating a DDos attack. Network resources could not be accessed. We responded by blocking the ICMP packets and restore critical network services. Investigation revealed a malicious actor sent a flood of ICMP pings through an unconfigured firewall
Identify	The team cybersecurity audited the internal networks, systems, devices, and access privileges to identify potential gaps in security. The team founded an unconfigured firewall where the malicious actor used to send a flood of ICMP pings into the company's network. All critical network services need to be restored.
Protect	The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Detect	Source IP address is verified on firewall to prevent IP spoofing. Network monitoring software is installed to detect abnormal traffic patterns.
Respond	Future affected systems will be isolated to prevent further disruption to the network and attempted to restore critical system affected. Network logs will

	be regularly monitored and analyzed for potential attacks. Upper management will be reported of all incidents.
Recover	Future DDos attacks can be blocked at firewall. Non-critical network should be stopped to reduce internal network traffic while the critical services is prioritized for restoration. Once the attack is over, all non-critical services can be brought back online.

Reflections/Notes: