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	A DDoS attack occurred recently which compromised the internal network for two hours until it was resolved. The attack caused network services to suddenly stop responding due to ICMP packets. The cause was a malicious actor which sent a flood of ICMP pings into the companies network through an unconfigured firewall. The team responded by blocking the incoming ICMP packets, stopping all non-critical network services offline, and restoring network services.
Identify	A DDoS attack occurred. The firewall was flooded by the ICMP packets causing internal network services to stop responding. The status of the internal network needed to be restored back to normal.
Protect	As the firewall has been flooded by the packets, the team has changed the firewall settings to limit the rate of incoming ICMP packets and IDS/IPS system to filter out some ICMP traffic which was suspicious.
Detect	Firewall was configured to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect suspicious traffic.
Respond	For future security events, the cybersecurity team will isolate affected systems

	to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	To recover, all of the network services need to be restored to its original normal state.

Reflections/Notes: