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	On _____ at ___ hours, the company experienced a distributed denial of service attack (DDoS) through a flood of ICMP packets that compromised the internal network for approximately 2 hours.
Identify	The security team investigated the event and found that a malicious actor had sent a flood of ICMP packets to the company network through an unconfigured firewall.
Protect	The security team has configured the firewall to limit the number of ICMP pings and created a rule for source IP address verification on the firewall to check for spoofed IP addresses.
Detect	The team implemented network monitoring software to detect abnormal network patterns, as well as an IDS/IPS system to filter ICMP traffic based on suspicious characteristics.
Respond	During future events, the security team will isolate affected systems and attempt to restore critical systems. They will examine logs to identify any suspicious activity and report the incident to upper management.
Recover	For recovery after future attacks by DDoS ICMP flood attacks, the security team will restore systems to a functioning state. ICMP flood attacks can be

	stopped by a firewall. Restoring critical systems will be prioritized followed by non-critical systems once the ICMP packets have been blocked.

Reflections/Notes: