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	
Identify	Our organization recently experienced a DDoS attack, compromising the internal network for two hours until it was resolved. During the attack, we identified through server logs that there was a flood of ICMP packets which rendered any legitimate users blocked out and pour website offline. We identified it was through an unconfigured firewall that caused the vulnerability.
Protect	To address this security event, the network security team implemented: • A new firewall rule to limit the rate of incoming ICMP packets • Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets • Network monitoring software to detect abnormal traffic patterns • An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics
Detect	To further detect any threats, risks, or vulnerabilities we should always implement a SIEM tool. This in collaboration with a packet analyzer tool can detect any unauthorized users or unusual activity.
Respond	An IDS/IPS system can be implemented to further restrict and filter the ICMP

	packets that are threats to our network. These new rules in the firewall, and filters and checks in place work in a way of filtering any illegitimate traffic from legitimate traffic, keeping our servers safe and online.
Recover	With all these systems in place, we can get our servers running back online and be proactive in our approach to cybersecurity when monitoring any intrusions and have a stronger sense of security.

Reflections/Notes: