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, our network services suddenly stopped responding for about two hours. Normal internal network traffic could not access any network resources. According to the data logs captured we could clearly see an incoming flood of ICMP packets. We believe that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Identify	The company's cybersecurity team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. They found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall that overwhelmed the company's network through a distributed denial of service (DDoS) attack.

Protect	To address this security event, the cybersecurity 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	The team is implementing an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics and network monitoring software to detect abnormal traffic patterns.
Respond	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. Network security team implemented below solutions to avoid any future DDoS attacks, • 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
Recover	The Cyber Security team, Incident management team and Network security team worked together to restore services which compromised the internal network for two hours. Employees were informed of the incident and the reason for the issue via internal email communication. Further investigations will be conducted to identify the threat actor(s) and bring up legal actions against them.

Reflections/Notes: