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	The company experienced a Distributed Denial of Service (DDoS) attack that used a large volume of ICMP packets to flood the internal network. These packets came from multiple sources, which suggests it was a coordinated DDoS attack by malicious actors. Because of this, the network couldn’t respond to normal traffic, and internal services were inaccessible for about two hours. The incident response team acted quickly by blocking incoming ICMP traffic, taking non-critical services offline, and restoring the essential ones. While the situation was eventually contained, the attack exposed a gap in the firewall configuration that left the network vulnerable.
Identify	After investigating the incident, the cybersecurity team found that the firewall had not been properly configured. This made it possible for the attackers to send a flood of ICMP pings into the network, overwhelming it and making it unavailable to normal users. The team confirmed it was a DDoS attack exploiting that open vulnerability.
Protect	To improve protection and reduce the chances of a similar attack, the team implemented several changes: • A firewall rule was added to limit the rate of incoming ICMP packets. • Source IP address verification was enabled to filter out spoofed IPs.

	• Network monitoring tools were set up to catch unusual traffic patterns. • An IDS/IPS system was installed to detect and block suspicious ICMP traffic. These measures aim to strengthen the network's defenses and reduce the attack surface moving forward.
Detect	To detect future threats more effectively, the company now uses a combination of tools: • The firewall helps filter and rate-limit ICMP traffic. • The IDS/IPS system alerts the security team when it notices strange or known malicious behavior. • Ongoing network monitoring provides visibility into traffic patterns and flags anything that looks unusual. These tools help the team react faster and with more confidence if something seems off.
Respond	If another similar attack happens in the future, the plan is to act immediately. The team will: • Use the firewall to block the source of the attack quickly. • Rely on IDS/IPS alerts to respond as soon as suspicious activity is detected. • Train staff regularly, so they know how to respond calmly and effectively during a cybersecurity incident. Having a plan in place helps everyone stay focused and respond efficiently without panic.
Recover	After an attack is contained, the team will restart network services in a controlled way, making sure everything is stable and safe before going fully back online. It's also important to check for any leftover issues or vulnerabilities that could be used again later. Lessons learned from the incident will be reviewed and shared so that the team and company continue to improve.

Reflections/Notes: This incident highlights the importance of having strong security configurations in place, especially on firewalls. Even a small oversight can lead to serious network disruptions. It also shows how effective tools like firewalls, IDS/IPS, and monitoring software are in detecting and stopping attacks. The NIST CSF framework helps guide the response in a clear and organized way, from identifying the issue to recovering from it. Regular training and updated procedures are key to improving how a team handles future security events.