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 organization experienced a DDoS attack that disrupted their internal network for two hours, preventing access to critical services. Through the identity function, it was discovered that an unconfigured firewall allowed a flood of ICMP packets into the network, creating vulnerability that attackers exploited. To strengthen security, the company applied the protect and detect functions by implementing firewall rules to limit ICMP traffic, enabling source IP verification, introducing IDS/IPS systems, and using network monitoring tools. These measures help safeguard against future attacks and allow for quicker detection of malicious activity. The company responded quickly to block incoming ICMP traffic while restoring critical functions. The recover function was applied through timely restoration of services, improving detection tools, and incident response planning.
Identify	Technology/Asset Management The organization experienced a DDoS attack that compromised the internal network for two hours. The attack consisted of a flood of ICMP packets that overwhelmed the network, causing network services to stop responding. The issue was traced to an unconfigured firewall that allowed malicious traffic to enter the internal environment. Process / Business Environment The company offers web design services, graphic design, and social medial marketing to small businesses. During the incident, it prevented the organization from delivering their services. People

	Internal users were unable to access network resources to perform their work.
Protect	Internal users need uninterrupted access to the services (web design, graphic designs, and social media marketing) to deliver those services to customers. Based on the investigation it revealed that an unconfigured firewall allowed non-trusted sources to send ICMP traffic into internal network which resulted in service disruption. Management and senior leaders as well as the teams directly impacted in the delivery of company's services need to be made aware of the issue. To address this gap, the security team has implemented several measures: 1. A new firewall rule to limit the rate of incoming ICMP packets and reduce the risk of future flooding. 2. Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. 3. Networking monitoring software to detect abnormal traffic patterns. 4. IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To strengthen the organizations' ability to detect future incidents, the security team has implemented multiple detection focused measures. An Intrusion and Prevention system (IDS/IPS) to inspect and filter ICMP traffic and identify patterns with known attack characteristics. Additionally, networking monitoring software has been employed to detect abnormal traffic patterns and support early warning for potential DDoS attacks. The team also configured firewall rules to limit the rate of incoming ICMP packets, helping identify potential packet floods and triggering alerts when traffic exceeds expected baselines.
Respond	The effectively respond to similar attacks in the future, the organization has implemented security controls that support early detection and rapid containment. These include updated firewall rules, source IP address verification, networking monitoring software, and intrusion detection and prevention to inspect and block suspicious traffic. In the event of another DDoS attack, defined incident response procedures must be followed and communicated throughout the organization. This includes notifying IT staff, management, and impacted service teams in real time. During the recent attack, the security team responded by blocking incoming ICMP packets,

	taking all non-critical services offline, and restoring critical operations. This structured response helped reduce downtime and service disruption. Going forward, the company should continue to refine its incident response plan through log analysis and training to ensure teams are prepared to respond quickly.
Recover	During the incident, all non-critical services were taken offline while critical operations were restored quickly to minimize business disruption. This approach ensured essential services remained available while containment measures were deployed. The steps implemented such as firewall rules, traffic monitoring, and IDS/IPS will support early detection and containment for future attacks. To ensure long term effectiveness, these systems must be maintained regularly. Additionally, the recovery process should include routine reviews of backup procedures, post incident analysis, and clear restoration steps to all impacted teams. These efforts will help organizations recovery time in future incidents.

Reflections/Notes:

Scenario

Review the scenario below. Then complete the step-by-step instructions.

You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.

During the attack, your organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP

packets, stopping all non-critical network services offline, and restoring critical network services.

The company's cybersecurity team then investigated the security event. They found 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.

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

As a cybersecurity analyst, you are tasked with using this security event to create a plan to improve your company's network security, following the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). You will use the CSF to help you navigate through the different steps of analyzing this cybersecurity event and integrate your analysis into a general security strategy. We have broken the analysis into different parts in the template below. You can explore them here:

- **Identify** security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
- **Protect** internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
- **Detect** potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.
- **Respond** to contain, neutralize, and analyze security incidents; implement improvements to the security process.
- **Recover** affected systems to normal operation and restore systems data and/or assets that have been affected by an incident.