Incident report analysis

Scenario

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.

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	Due to a recent distributed denial of services (DDoS) attack, the organization's internal network services were compromised for two hours until it was resolved. This attack was caused by a flood of incoming ICMP packets, preventing access to any network resources. The incident management team responded by blocking incoming ICMP packets and stopping all non-critical

	network services offline in order to restore critical network services.
Identify	- Technology/Asset Management: Which hardware devices, operating systems, and software were affected? Trace the flow of the attack through the internal network. - Process/Business environment: Which business processes were affected in the attack? - People: Who needs access to the affected systems? Malicious actor/s targeted the company's network through an ICMP flood attack. All the entire internal network was compromised. Critical services needed to be secured and restored. The actors exploited an unconfigured firewall.
Protect	- Access control: Who needs access to the affected items? How are non-trusted sources blocked from having access? - Data security: Is there any affected data that needs to be made more secure? - Maintenance: Do any of the affected hardware, operating systems, or software need to be updated? - Protective technology: Are there any protective technologies, like a firewall or an intrusion prevention system (IPS), that should be implemented to protect against future attacks? The internal network was protected by implementing a new firewall rule to limit the rate of incoming ICMP packets. The network security team also implemented an IDS/IPS system.
Detect	- Anomalies and events: What tools could be used to detect and alert IT security staff of anomalies and security events, such as a security information and event management system (SIEM) tool? - Security continuous monitoring: What tools or IT processes are needed to monitor the network for security events? - Detection process: What tools are needed to detect security events,

	such as an IDS? The network security team installed a new network monitoring software to detect abnormal traffic patterns and configured a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Respond	- Response planning: What action plans need to be implemented to respond to similar attacks in the future? - Analysis: What analysis steps should be followed in response to a similar attack? - Mitigation: What responding steps could be used to mitigate the impact of an attack, such as offlining or isolating affected resources? - Improvements: What improvements are needed to improve response procedures in the future? After recovering from the incident, the cybersecurity team designed a new action plan for responding to this type of attack. In the first place, the non affected systems would be isolated and contained to prevent the attack from spreading. If possible, critical network systems affected by the attack will be recovered. Once the attack is contained, by blocking news ICMP packets too, the team analyzed network logs to check abnormal or malicious activities. Finally, the incident will be reported to the appropriate superior or legal figure.
Recover	- Recovery planning: How will resources be restored following an attack? - Improvements: Do any improvements need to be made to the current recovery systems or processes? - Communications: How will restoration procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff? To recover from a DDoS attack by ICMP flooding, the access to the network needs to be restored to regular behavior. Then, the non-critical services will be stopped, to prevent unnecessary traffic. At this moment, the critical network

	services will be restored. Finally, once the attack is fully stopped and controlled, all the network systems can begin working correctly. The implementation of a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system should help block incoming ICMP flooding attacks.