Incident report analysis (My Responses)

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	Based on the given documents/scenario, the company experienced a cybersecurity incident when its network services suddenly stopped responding which was caused by a Distributed Denial of Service (DDoS) attack from an ICMP flood attack, in which the malicious actor sent a high volume of ICMP packets to overwhelm the company's network. The network disruption lasted for approximately two hours, rendering all internal network traffic unable to access essential network resources. Then, in the scenario it explains how the cybersecurity team went to resolve and secure this issue by blocking the incoming attack and shutting down all non-critical network services, allowing critical network services to be restored. Once blocking the attack, the cybersecurity team went to investigate the root cause of the attack and found that it was due to an unconfigured firewall vulnerability that allowed the flood of ICMP traffic to reach the network.
Identify	Based on the scenario and given documents provided, upon after investigating it, I identify that the attack was a Distributed Denial of Service (DDoS) attack, where the bad actors/hackers flooded the network with ICMP packets, rendering the network resources unavailable. This led to the entire internal network was affected by the attack, impacting the availability of all systems and services and targeted the network infrastructure like the routers,

	switches, and firewalls. Since the company's internal network and critical network services needed to be restored as part of the response to the attack, the vulnerability exploited during the attack was linked to an unconfigured firewall, which failed to block excessive incoming ICMP traffic, allowing the attack to overwhelm the network.
Protect	With the scenario and documents given, I recommend that the cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics. These are the recommendations: **1)** A new firewall rule was established to limit the rate of incoming ICMP packets, preventing a similar flood from occurring again; **2)** Implement a source IP address verification because since the firewall was configured to verify the source IP addresses of incoming ICMP packets to detect and block spoofed IP addresses in DDoS attacks; **3)** Implement network monitoring software to detect abnormal traffic patterns, finding and reviewing the identification of potential future attacks before they overwhelm the system; **4)** Implement or install the intrusion Detection/Prevention System (IDS/IPS) to filter out malicious ICMP traffic based on suspicious characteristics, adding an extra layer of defense against future attacks.
Detect	Based on this scenario and the documents given, to improve the organization's ability to detect future security incidents, I recommend that the cybersecurity team focused on enhancing the monitoring/detection by: **1)** Since implementing IP spoofing addresses detection using a firewall, seeing the breaches, can reveal the DDoS attack by filtering out malicious traffic that may be disguised as legitimate; **2)** Seeing Abnormal Traffic Pattern Detection after installing network monitoring software (think like SIEMs,. etc.) to analyzes network traffic for unusual patterns like sudden spikes in ICMP packets and send an alert to the security teams in real-time when detected; **3)** If the company has an Intrusion Detection System (IDS) and Intrusion Prevention

	System (IPS), it can help monitor for known attack signatures and prevent future DDoS traffic from reaching the network infrastructure.
Respond	Upon after investigating the DDoS attack with the scenario and the given documents, I recommend that the cybersecurity team should: **1)** isolate affected systems to prevent the attack from spreading across the network like blocking the malicious traffic at the firewall and shutting down non-critical systems to allow critical systems to be prioritized and restored; **2)** restoring critical network services first to minimize business disruption like email, file storage, and internet connectivity; **3)** Then, after the immediate threat has been mitigated, the team will analyze network logs and other data sources to investigate how the attack occurred, how it was executed, and whether there are any ongoing risks to identify any flaws; **4)** Lastly, the cybersecurity team should ensure that all incidents are reported and sent all details to upper management and relevant legal authorities for further action and compliance reporting.
Recover	Based on the scenario and the documents given, in order for this company to recover from a DDoS attack by ICMP flooding, the access to network services need to be restored to a normal functioning state. The external ICMP flood attacks can be blocked at the firewall and then, all non-critical network services should be stopped to reduce internal network traffic. And then after that, the critical network services should be restored first. Then to conclude, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online. In other words, with steps included to avoid the confusion of what I mean: **1)** restore access to critical network services so that essential business operations can continue; **2)** work with the Internet Service Provider (ISP) to block ICMP flood traffic at the external network edge; **3)** The team will shut down non-critical network services temporarily to reduce internal traffic load while mitigating the DDoS attack; **4)** Once the flood of ICMP packets has naturally timed out or been

	blocked, the team will gradually bring non-critical systems and services back online to restore full functionality; **5)** include a post-incident review to evaluate the response and recovery process for future repeated incidents.

Reflections/Notes:
This incident highlighted several weaknesses in the company's initial security posture, particularly regarding the firewall configuration and DDoS attack mitigation. With the given documents, by following the NIST Cybersecurity Framework, the company has taken the first step in improving its cybersecurity strategy. Each of the NIST CSF phases of Identify, Protect, Detect, Respond, and Recover is essential in building a resilient security posture and minimizing the impact of future incidents.

Additional Information:

Scenario Given:
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.

Link to template:

- Incident report analysis

Link to supporting materials:

- Applying the NIST CSF
- Example of an incident report analysis

Step 2: Summarize the security event

Using the template provided, provide a summary of the security event that occurred. Include information about the security event, its cause, the impact, and the response. You can also include information about targeted systems, the attack source, and the estimated impact.

Step 3: Identify the type of attack and the systems affected

Think about all of the concepts covered in the course so far and reflect on the scenario and define what type of attack occurred and which systems were affected. List this information in the incident report analysis worksheet in the section titled "Identify."

Step 4: Protect the assets in your organization from being compromised

Next, you will assess where the organization can improve to further protect its assets. In this step, you will focus on creating an immediate action plan to respond to the cybersecurity incident. When creating this plan, reflect on the following question:

- What systems or procedures need to be updated or changed to further secure the organization's assets?

Write your response in the incident report analysis template in the "Protect" section.

Step 5: Detect similar incidents in the future

It is important to continuously monitor network traffic on network devices to check for suspicious activity, such as incoming external ICMP packets from non-trusted IP addresses attempting to pass through the organization's network firewall.

For this step, consider ways you and your team can monitor and analyze network traffic, software applications, track authorized versus unauthorized users, and detect any unusual activity on user accounts. Write your response in the incident response analysis worksheet in the "Detect" section.

Step 6: Respond to future cybersecurity incidents

After identifying the tools and methods you and your organization have in place for detecting potential vulnerabilities and threats, create a response plan in the event of a future incident. This typically happens after the incident occurred and has been resolved by you and your team. In this case, you will create a response plan for future cybersecurity incidents. Some items to consider when creating a response plan to any cybersecurity incident:

- How can you and your team contain cybersecurity incidents and affected devices?
- What procedures are in place to help you and your team neutralize cybersecurity incidents?
- What data or information can be used to analyze this incident?
- How can your organization's recovery process be improved to better handle future cybersecurity incidents?

Write your response in the incident report analysis template under the "respond" section.

Step 7: Recover from the incident

Consider what steps need to be taken to help the organization recover from the cybersecurity incident. Reflect on all the information you gathered about the incident in the previous steps to consider which devices, systems, and processes need to be restored and recovered.
Consider the following questions:

- What information do you need to be able to recover immediately?
- What processes are in place to help the organization recover from the incident?

Write your response in the “recover” portion of the worksheet.

Be sure to address the following in your completed activity. Course 3 incident report analysis:

- Summarize the security event
- Identifies the type of attack and the systems impacted by the incident
- Offers a protection plan against future cybersecurity incidents
- Describes detection methods that can be used to identify potential cybersecurity incidents
- Includes a response plan for the cybersecurity incident and outline for future cybersecurity incidents
- Outlines recovery plans you and the organization can implement in future cybersecurity incidents.