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.

> 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.

Summary	Several hours ago, my organization was informed that we were experiencing a DDoS (Distributed Denial of Service) attack. Our network stopped responding due to a huge flood of ICMP packets. We couldn't access any network resources due to the traffic, so we responded by blocking incoming ICMP packets, stopping most of our network services offline. This cleared up the traffic a bit, restoring the critical network services. The company's cybersecurity team investigated the security incident and found

	that a malicious threat actor had flooded ICMP pings into the company's network through an unconfigured firewall. The vulnerability allowed the attacker to overwhelm the company's network through a DDoS attack.
Identify	This attack occurred due to our misconfiguration of the organization's firewalls. We didn't set many guidelines in place, allowing for a large attack surface from threat actors.
Protect	Knowing this, we configured our organization's firewalls and updated the rules. It will only allow a set limit of incoming ICMP packets in order to keep traffic at a minimum. In addition, we have added a form of multifactor authentication when accessing our firewalls. We have also implemented an IPS system that will filter ICMP traffic from suspicious behavior.
Detect	In addition, we have added a form of multifactor authentication when accessing our firewalls. Users are to verify that their IP address is legitimate and not spoofed. We have also implemented network monitoring software that will detect and alert us about abnormal traffic patterns.
Respond	When the threat occurred, my team responded by disabling all of the non-critical network services. This reduced the amount of traffic circulating in our network. The critical network services will be functional again. For the time being, the issue will be tamed while the experts are on the case of the ICMP traffic.
Recover	After the tech experts handle the ICMP packet traffic, all operations can return to normal. We have implemented the changes mentioned above in order to prevent similar incidents like this from happening again.

Reflections/Notes: Overall, this simulation was a great experience. It taught me to thoroughly think about and face possible circumstances I might face in this industry. It has also taught me to implement the five steps of the NIST CSF.