**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 companies security team investigated and found a malicious actor flooded the companies network of ICMP pings which caused the organization's network to stop responding and go offline for 2 hours and was found to be a DDoS . | | |
| --- | --- | --- | --- |
| Identify | The security team found that the ICMP packets were being flooded through and unconfigured firewall causing the companies network to go offline. | | |
| Protect | The network security team has implemented:   * A new firewall rule to rate limit incoming ICMP packets, which will only allow a certain amount of ICMP packets to be let through at a time so a server cannot be flooded with packets. * Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, which allows for the detection of if the packets are being altered or sent by a threat | | |
| Detect | The team had also implemented several detection features:   * Network monitoring software which is used to analyze and detect abnormal traffic patterns so the team can be notified if there is an abnormal pattern. * An intrusion detection system is now in place that filters out ICMP traffic based on suspicious characteristics like if there are loads coming from the same location at once at a rate a human cannot do. | | |
| Respond | The incident management team had responded by blocking incoming ICMP packets and stopping all non-critical network services offline and restoring critical network services. | | |
| Recover | The team will recover systems by blocking remaining ICMP packets and take down non critical operations so that the critical operations become operational quickly and the rest of the services will follow when the servers traffic is reduced. | | |

| Reflections/Notes: |
| --- |

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.