## **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.**

**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 network of the company suddenly went down as there was a DDoS (Distributed Denial of Service) attack root cause of which was a flood of ICMP packets.Later the security team was successful to stop incoming flood of the ICMP packets. | | |
| --- | --- | --- | --- |
| Identify | The threat actor targeted the servers of the company by ICMP flood. Due to which entire network of the company turned down. | | |
| Protect | To prevent this in future the firewall rules were updated to filter out the extra amount of the ICMP packet by limiting the ICMP packets entering the server or network. | | |
| Detect | Configured the firewall to detect the spoofed IP addresses. | | |
| Respond | To avoid the attack in future the cybersecurity team will need to analyze the logs. | | |
| Recover | To recover from this ICMP flood attack the access to the entire internal network of the organization needs to be gained. After configuration of the firewall extra ICMP packets will be blocked at the firewall. | | |

| Reflections/Notes: The proper configuration of rules of firewall is must. |
| --- |