**Incident report analysis**

**Link to the NIST Frameworks:** [**NIST CSF**](https://d.docs.live.net/5db82be82310d3c0/Documents/CREATING%20PORTFOLIO/blaise-portfolio/Blaise-portfolio/Google%20Cybersecurity%20Certificate/project2-nist-csf/Applying%20the%20NIST%20CSF%20.docx)

**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** | A cyber attack recently targeted our organization through a Distributed Denial of Service (DDoS) attack that utilized ICMP ping flooding. The attacker exploited an unconfigured firewall to send an overwhelming number of ICMP requests into the company’s internal network. This flood of requests disrupted network functionality for approximately two hours, significantly impacting system performance and response times. The network security team responded effectively by implementing several critical measures. These included configuring a new firewall rule to limit the rate of incoming ICMP packets, verifying the source IP addresses to prevent spoofed packets, deploying network monitoring software to identify abnormal traffic patterns, and installing an Intrusion Detection/Prevention System (IDS/IPS) to help filter out malicious ICMP traffic. |
| Identify | The primary threat identified was a DDoS attack, which directly affected the internal network. A DDoS attack is a method where a malicious actor sends a flood of traffic. In this case, ICMP pings to a target system, with the intent to overload it and render services unavailable. The internal network, a critical component of the organization's infrastructure, was significantly impaired during the attack, resulting in slow response times and temporary unavailability of network-dependent services. |
| Protect | To improve the organization's defenses against future attacks, several protective measures were implemented. A firewall rule was set to limit the number of ICMP ping requests the network can receive, striking a balance between security and system functionality. Additionally, the firewall was configured to verify source IP addresses, reducing the risk of spoofed traffic entering the system. Network monitoring tools were also introduced and automated to regularly assess traffic patterns, while an IDS/IPS system was deployed to identify and filter out ICMP traffic that exhibited suspicious behavior. |
| Detect | Detection capabilities were strengthened through the installation of the IDS/IPS system, which now helps to analyze and flag ICMP traffic that deviates from normal behavior. The firewall’s source IP verification plays a key role in identifying spoofed packets. Furthermore, real-time network monitoring software was deployed to detect unusual traffic surges, providing early warnings of potential DDoS attacks or other anomalies that could compromise the network. |
| Respond | In response to the incident, the organization acted swiftly and calmly. The network security team followed incident response protocols, investigated the source and scope of the attack, and applied the necessary technical controls to mitigate the threat. Lessons were documented from the event to inform future preparedness, acknowledging that cyber threats are constantly evolving and that organizations must remain vigilant and adaptable. |
| Recover | Following the incident, recovery focused on restoring operations and data integrity. It is assumed that data versioning had been previously set up, enabling the team to restore from the most recent stable version prior to the attack. Communication was made with relevant departments to ensure that any new data created during the downtime while systems were being investigated was not lost, and instructions were given to resynchronize that data where applicable. A final verification was performed to confirm that systems were fully restored and secured before resuming normal business functions. |

|  |
| --- |
| Reflections/Notes: This incident demonstrates the critical need for basic security configurations, such as properly setting up firewalls, to prevent easily avoidable attacks. The organization responded effectively by implementing ICMP rate limiting, source IP verification, and deploying monitoring and IDS/IPS systems. It also underlines the importance of proactive monitoring, regular audits, and having a clear response and recovery plan. Moving forward, maintaining a security-first mindset and continuous improvement will be essential to staying ahead of evolving threats. |