**ASSIGNMENT**

**Name: OKU, Ediomo Samuel**

**NIST-CSF-Security-Incident-Report**

1. [Introduction](https://github.com/ChrisJabb21/NIST-CSF-Security-Incident-Report?tab=readme-ov-file#introduction)
2. [Scenario](https://github.com/ChrisJabb21/NIST-CSF-Security-Incident-Report?tab=readme-ov-file#scenario)
3. [Objective](https://github.com/ChrisJabb21/NIST-CSF-Security-Incident-Report?tab=readme-ov-file#objective)
4. [Incident Report Analysis](https://github.com/ChrisJabb21/NIST-CSF-Security-Incident-Report?tab=readme-ov-file#incident_report_analysis)
5. [Notes](https://github.com/ChrisJabb21/NIST-CSF-Security-Incident-Report?tab=readme-ov-file#notes)
6. [Reflections](https://github.com/ChrisJabb21/NIST-CSF-Security-Incident-Report?tab=readme-ov-file#reflections)

**Introduction**

A security incident report done as part of requirement for a 3MTT cybersecurity training to gain an understanding of network-level vulnerabilities and how to secure networks using Wireshark and NIST/CSF incident respond framework.

The first part of this report will be to identify and investigate incident before the respond plan as contain in this report.

**DDOS Attacks:**

A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once. The distribution of hosts that defines a DDoS provide the attacker multiple advantages:

He can leverage the greater volume of machine to execute a seriously disruptive attack.

The location of the attack is difficult to detect due to the random distribution of attacking systems (often worldwide)

It is more difficult to shut down multiple machines than one.

The true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems.

Modern security technologies have developed mechanisms to defend against most forms of DoS attacks, but due to the unique characteristics of DDoS, it is still regarded as an elevated threat and is of higher concern to organizations that fear being targeted by such an attack.

**Case Scenario**

As a cybersecurity analyst working for an ERP software development company that offers customized software design, development, and hosting solutions to small businesses. My organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was responded to.

During the attack, my 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.

A screenshot of a computer

Description automatically generated

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.

**Objective**

I was 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*).

The different steps of analyzing this cybersecurity incident and integrate your analysis into a general security strategy align with NIST's CSF's five core functions:

* **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**

**Summary**

A security incident occurred where the organization’s internal network experienced a distributed denial of service (DDoS) attack. During the attack, the organization’s network services suddenly stopped responding. Devices on the internet network were affected and network resources within the affected network could not be accessed.

|  |  |
| --- | --- |
| **Phase** | **Description of what happened at each NIST CSF phase** |
| Identify | The cybersecurity team investigated the security event and discovered a malicious actor had sent a flood of ICMP Pings into the company’s network through an unconfigured firewall. This vulnerability of the misconfigured firewall allowed the attacker to overwhelm the company’s network through a DDoS attack. |
| Protect | To protect and safeguard against future DDoS attacks, the network security team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to be able filter out some ICMP traffic to the internal network based on suspicious characteristics. |
| Detect | To detect new and similar unauthorized network intrusions and improve the ability to detect these threats, the security team will install network monitoring software to detect abnormal traffic patterns and Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. |
| Response | The incident management team responded by blocking incoming ICMP packets, stopping all and bring non-critical network functionality offline, and restoring critical network services to contain the issue and begin identifying the root cause.Training for security personnels on this tool and updates to incident response playbooks for the Detect and Protect phases should be implemented to any existing documentation to improve response procedures. Management will have to promptly inform law enforcement of the DDoS incident depending on the affected organization’s industry based on the impact for the outage. (example: reporting the DDoS issue to a local FBI Field Office) |
| Recover | This attack took the network down for two hours and the IT and Security operation teams worked jointly to bring the network back online for normal business operations while the internal network was down for 2 hours. The cybersecurity team informed staff of what is going on and held a lesson learned session to present the root cause behind this attack as well as safeguards that will need to implement to protect against future attacks. Being able to respond and recover faster then the 2 hours will be looked into and assessed after the safeguards in the protect and detect phases are implemented. Consideration of Cyber Insurance provider to help with recovery and consultation advice will need to be taken as well to try counter revenue loss. Next, an investigation will be conducted for legal actions pertaining to this cyberattack and determining the person(s) responsible for the attack and take it from there to assess the extent of the damage caused by the cyberattack. |

**Lesson Learned**

The recent Distributed Denial of Service (DDoS) attack on our network provided invaluable insights into our organization's resilience against cyber threats. In the aftermath of the attack, several critical lessons emerged:

**Importance of Proactive Monitoring:** The incident underscored the necessity of continuous monitoring of network traffic and systems for anomalous behavior. Early detection can significantly mitigate the impact of DDoS attacks by enabling swift response measures.

**Need for Scalable Infrastructure:** Our response highlighted the importance of having scalable infrastructure capable of handling sudden spikes in traffic during DDoS attacks. Implementing cloud-based mitigation services or deploying additional bandwidth resources can enhance our network's capacity to withstand such assaults.

**Effective Communication and Coordination:** Clear communication and coordination among IT security teams, network administrators, and stakeholders are essential during DDoS attacks. Establishing predefined communication channels and escalation procedures ensures swift decision-making and coordinated response efforts.

**Continuous Improvement of Mitigation Strategies:** DDoS attack techniques are constantly evolving, necessitating continuous improvement of mitigation strategies. Regular testing and refinement of DDoS defense mechanisms, such as rate limiting, IP blacklisting, and traffic filtering, are critical to staying ahead of emerging threats.

**Collaboration with ISPs and Security Vendors:** Building strong partnerships with Internet Service Providers (ISPs) and security vendors can enhance our ability to mitigate DDoS attacks effectively. Leveraging their expertise and resources, such as traffic scrubbing services and threat intelligence feeds, strengthens our defense mechanisms against sophisticated DDoS threats.

**Employee Training and Awareness:** Enhancing employee awareness and training programs on cybersecurity best practices, including recognizing signs of DDoS attacks and responding appropriately, is essential. Educating employees on the potential impact of DDoS attacks and their role in incident response can help minimize downtime and mitigate associated risks.