Justin Goncalves

7/23/24

Cyber Security Incident Response Project (NIST)

Activity Overview:

In this activity, you will create an incident report using the knowledge you've gained about networks throughout this course to analyze a network incident. You will analyze the situation using the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF). The CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. Creating a quality cybersecurity incident report and applying the CSF can demonstrate a proactive approach to security, improving communication and transparency with stakeholders, and improve security practices within your organization. You can also add the incident report you create to your cybersecurity portfolio when you complete it.

The CSF is scalable and can be applied in a wide variety of contexts. As you continue to learn more and refine your understanding of key cybersecurity skills, you can use the templates provided in this activity in other situations. Knowing how to identify which security measures to apply in response to business needs will help you determine which are the best available options when it comes to network security.

Be sure to complete this activity before moving on. In the next course item, you will be able to self-assess your response. After that, there will be a completed exemplar to compare to your own work. It will also provide an opportunity for you to answer rubric questions that allow you to reflect on key elements of your professional statement.

Use the NIST Cybersecurity Framework to Respond to a Security Incident

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.

Follow the instructions and fill in the sections to complete the activity.

Summary	The multimedia company recently experienced a Distributed Denial of Service (DDoS) attack that compromised its internal network for two hours. This attack involved a flood of ICMP packets, which overwhelmed the network and caused all network services to become unresponsive. The root cause of the attack was identified as an unconfigured firewall, which allowed the malicious actor to send a massive volume of ICMP packets into the company's network. During the two-hour attack, normal internal network traffic could not access any network resources, leading to a complete halt of the company's operations that relied on these services. This significant disruption affected business activities, potentially impacting client services and resulting in financial and reputational damage. The immediate response by the incident management team included blocking incoming ICMP packets, taking non-critical network services offline, and restoring critical network services to resume essential operations. Following the initial response, the cybersecurity team conducted a thorough investigation and identified the firewall configuration issue that facilitated the attack. To prevent future incidents, several measures were implemented: a new firewall rule to limit the rate of incoming ICMP packets, source IP address verification to detect and block spoofed IP addresses, network monitoring software to identify abnormal traffic patterns, and an IDS/IPS system to filter out suspicious ICMP traffic based on predefined characteristics.

	The attack targeted the company's internal network infrastructure, including critical network services essential for daily operations and client interactions. The source of the attack was traced back to multiple IP addresses, indicating a coordinated effort likely involving a botnet. The estimated impact of the attack includes two hours of network downtime, potential lost revenue, and costs associated with mitigation and implementing new security measures. Additionally, the company may face reputational damage and loss of client trust. By addressing these identified vulnerabilities and enhancing the network's security posture, the company aims to prevent future DDoS attacks and ensure robust protection of its network resources.
Identify	**Type of Attack:** The type of attack that occurred was a Distributed Denial of Service (DDoS) attack. Specifically, it was an ICMP flood attack, where the attacker overwhelmed the network with a massive volume of ICMP packets, causing network services to become unresponsive. **Systems Affected:** ● **Internal Network Infrastructure:** The primary target was the company's internal network, which became unresponsive due to the flood of ICMP packets. ● **Network Services:** All network services were affected, causing a complete halt in normal internal network traffic and preventing access to network resources. ● **Firewall:** The unconfigured firewall was a critical vulnerability that allowed the attack to succeed. ● **Business Operations:** The disruption impacted daily business operations and client services, highlighting the importance of network security for maintaining operational continuity. The DDoS attack exploited vulnerabilities in the company's network defenses, demonstrating the need for robust security measures to prevent similar incidents in the future.
Protect	To protect the organization's assets from future cybersecurity incidents, several systems and procedures need to be updated or changed. The following immediate action plan outlines the necessary steps: 1. **Update Firewall Configuration:** ○ Implement a new firewall rule to limit the rate of incoming ICMP packets, preventing the network from being overwhelmed by a flood of requests. ○ Configure the firewall to perform source IP address verification to detect and block spoofed IP addresses, ensuring only legitimate traffic can access the network. 2. **Enhance Network Monitoring:** ○ Deploy advanced network monitoring software to detect abnormal traffic patterns in real-time. This will allow for quicker identification of potential attacks and enable proactive measures to mitigate threats. 3. **Implement Intrusion Detection and Prevention Systems (IDS/IPS):** ○ Install and configure IDS/IPS to filter out suspicious ICMP traffic based on predefined characteristics. This system will help in identifying and blocking malicious traffic before it can impact the network. 4. **Strengthen Access Control Policies:** ○ Review and update access control policies to ensure that only authorized personnel have access to critical network resources. Implement role-based access control (RBAC) to minimize the risk of unauthorized access.

	5. **Regular Security Audits:** ○ Conduct regular security audits of internal networks, systems, devices, and access privileges to identify potential gaps in security and ensure compliance with best practices. 6. **Employee Training and Awareness:** ○ Provide ongoing training to employees on cybersecurity best practices, including recognizing and responding to phishing attempts, maintaining strong passwords, and understanding the importance of network security. By implementing these measures, the organization can significantly enhance its security posture, protect its assets from future attacks, and ensure the resilience of its network infrastructure.
Detect	To effectively detect similar incidents in the future, it is crucial to implement continuous monitoring and analysis of network traffic and user activities. The following measures can help achieve this: 1. **Advanced Network Monitoring:** ○ Deploy advanced network monitoring tools to continuously analyze network traffic for suspicious activity, such as incoming ICMP packets from non-trusted IP addresses. These tools can alert the security team to any anomalies in real-time. 2. **Intrusion Detection Systems (IDS):** ○ Implement IDS to monitor and analyze network traffic for signs of malicious activity. IDS can detect unusual patterns, such as a high volume of ICMP packets, and trigger alerts for further investigation. 3. **Security Information and Event Management (SIEM):** ○ Utilize SIEM solutions to aggregate and analyze logs from various network devices and software applications. SIEM can correlate events from different sources to identify potential security incidents and provide comprehensive visibility into network activity. 4. **User Activity Monitoring:** ○ Implement tools to track and analyze user activity on the network. This includes monitoring login attempts, access to sensitive data, and any unusual behavior that might indicate a compromised account. 5. **Anomaly Detection:** ○ Use anomaly detection algorithms to establish a baseline of normal network behavior and identify deviations from this baseline. This can help detect potential threats that do not match known attack signatures. 6. **Regular Audits and Penetration Testing:** ○ Conduct regular security audits and penetration tests to identify vulnerabilities and test the effectiveness of detection mechanisms. These activities can help ensure that monitoring tools are properly configured and capable of identifying potential threats. 7. **Automated Alerts and Incident Response:** ○ Configure automated alerts to notify the security team of any detected anomalies or suspicious activities. Establish clear incident response procedures to ensure timely investigation and mitigation of potential threats. By implementing these detection measures, the organization can proactively monitor its network for signs of potential attacks, quickly identify and respond to suspicious activities, and maintain a robust security posture.

Respond	Creating an effective response plan for future cybersecurity incidents is crucial to minimizing damage and ensuring a quick recovery. The following steps outline how the organization can respond to future incidents: 1. **Incident Containment:** ○ **Immediate Action:** Upon detecting a cybersecurity incident, the first step is to contain the threat to prevent it from spreading. Isolate affected devices from the network to stop the attacker's access and limit further damage. ○ **Network Segmentation:** Implement network segmentation to isolate critical systems from the rest of the network, making it easier to contain threats without disrupting all services. 2. **Neutralization Procedures:** ○ **Threat Identification:** Quickly identify the nature and scope of the attack using data from monitoring tools, IDS/IPS, and SIEM systems. This includes determining the attack vector, affected systems, and potential impact. ○ **Mitigation Actions:** Deploy specific countermeasures to neutralize the threat. This may involve removing malware, closing vulnerabilities, or applying patches. Ensure that the firewall rules and access controls are updated to block further malicious activity. 3. **Incident Analysis:** ○ **Data Collection:** Collect and preserve logs, network traffic data, and system snapshots to analyze the incident. This information helps in understanding the attack and identifying any weaknesses in the security posture. ○ **Root Cause Analysis:** Conduct a thorough analysis to determine the root cause of the incident. Identify how the attacker gained access, what vulnerabilities were exploited, and the extent of the damage. 4. **Improving the Recovery Process:** ○ **Develop a Recovery Plan:** Create a comprehensive recovery plan that includes steps to restore affected systems, recover lost or corrupted data, and resume normal operations. Ensure that backups are regularly updated and tested for reliability. ○ **Communication Plan:** Establish a communication plan to keep stakeholders informed about the incident and recovery efforts. This includes notifying customers, employees, and regulatory authorities as required. ○ **Post-Incident Review:** After resolving the incident, conduct a post-incident review to assess the effectiveness of the response. Identify lessons learned and areas for improvement. Update incident response plans and procedures based on the findings. 5. **Training and Drills:** ○ **Regular Training:** Provide regular training to the incident response team and all employees on the latest cybersecurity threats and response techniques. Ensure that everyone is familiar with their roles and responsibilities during an incident. ○ **Simulation Drills:** Conduct regular simulation drills to test the incident response plan and improve readiness. These drills help identify gaps in the response strategy and ensure that the team can respond effectively to real incidents. By implementing these response measures, the organization can effectively contain and neutralize cybersecurity incidents, analyze the root cause, and improve the recovery

	process. This proactive approach ensures that the organization is better prepared to handle future incidents and minimize their impact on business operations.
Recover	Recovering from a cybersecurity incident involves a systematic approach to restoring affected devices, systems, and processes to normal operation. The first step is to ensure immediate access to recent and reliable backups of all critical systems and data, which are essential for restoring systems to their pre-incident state. Collecting detailed logs and documentation from monitoring tools, IDS/IPS, and SIEM systems is crucial to understand the full scope of the incident and ensure no malicious activity remains. Having a predefined recovery plan that outlines the steps for restoring systems, data, and services, along with contact information for key personnel and external partners, is necessary for a smooth recovery process. The restoration begins with cleaning up affected devices by removing any malicious software or code, reimaging systems, or performing clean installations. Once systems are clean, data can be restored from backups, ensuring integrity and security. Reconfiguring systems, reapplying security patches, updating firewall rules, and configuring security controls are critical steps in the recovery process. The organizational recovery process includes conducting a thorough review of the incident response to identify any gaps or weaknesses in current procedures, updating the incident response plan to address these gaps, and improving future responses. Providing training to employees on updated security policies and procedures ensures they are aware of their roles in maintaining security. Regularly conducting simulation drills and updating recovery procedures based on lessons learned from the incident can significantly enhance the organization's resilience against future cybersecurity incidents. By implementing these recovery measures, the organization can restore normal operations, protect its assets, and strengthen its overall security posture.

Reflections/Notes:
Throughout this project, I gained valuable insights into the practical application of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) in analyzing and responding to cybersecurity incidents. This experience highlighted the importance of a structured approach to incident management, encompassing identification, protection, detection, response, and recovery. By breaking down the incident into these core functions, I was able to systematically address each aspect of the attack and implement effective measures to prevent future occurrences.

One of the key learnings was the critical role of continuous monitoring and real-time analysis in detecting potential threats early. Implementing advanced network monitoring tools and intrusion detection systems (IDS) can significantly enhance an organization's ability to identify and respond to suspicious activities promptly. Additionally, the importance of having a robust incident response plan and regularly updating and testing it through simulation drills became evident. These practices ensure that the team is well-prepared to handle real incidents efficiently and effectively.

I also learned the significance of maintaining strong access controls and regularly updating security configurations, such as firewall rules and authentication policies, to mitigate vulnerabilities. The experience underscored the need for comprehensive employee training on cybersecurity best practices, which is crucial in preventing social engineering attacks and ensuring adherence to security protocols. Overall, this project reinforced the necessity of a proactive and layered security approach to protect organizational assets and

maintain operational continuity in the face of evolving cyber threats.