Kevin Torres Carias 03/28/24

Using the NIST Cybersecurity Framework to respond to a security incident

Instructions

Review the scenario below. Then complete then apply the NIST CSF to resolve the incident..
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.

Summary	A DDoS attack targeted the internal network of a multimedia company, disrupting services for two hours. The attack exploited an unconfigured firewall, flooding the network with ICMP packets. To counter this, the incident management team implemented measures including a new firewall rule to limit ICMP packet rates and source IP address verification. They also deployed network monitoring software and an IDS/IPS system to detect and filter out suspicious traffic.

Identify	The type of attack in this scenario is a Distributed Denial of Service (DDoS) attack. The systems affected by the attack are the internal network services.
Protect	• Firewall Configuration Review: Conduct a comprehensive review of firewall configurations to ensure they are properly configured to prevent similar DDoS attacks. This includes implementing stricter rules for ICMP packets and regular updates to firewall policies. • Enhanced Network Monitoring: Invest in more advanced network monitoring tools capable of detecting and mitigating DDoS attacks in real-time. These tools should provide granular visibility into network traffic and enable prompt response to abnormal patterns. • Employee Training and Awareness: Implement regular cybersecurity training sessions for all employees to raise awareness about DDoS attacks, phishing attempts, and other common threats. Ensure employees understand how to identify suspicious activities and report them promptly. • Incident Response Plan Refinement: Review and update the organization's incident response plan to include specific procedures for mitigating DDoS attacks. Define roles and responsibilities clearly, establish communication channels, and conduct regular drills to ensure preparedness. • Implement Redundancy and Failover Mechanisms: Introduce redundancy and failover mechanisms for critical network services to ensure continuity of operations during DDoS attacks. This may involve deploying backup servers or using cloud based services.

	• Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify potential weaknesses in the network infrastructure. Address any identified vulnerabilities promptly and prioritize patch management to prevent exploitation by attackers.
Detect	To detect similar incidents in the future, the team implemented IDS and IPS tools to detect and prevent network based security threats such as the DDoS attack that happened. Also, the team implemented source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. Lastly, network monitoring software was installed to detect abnormal traffic patterns.
Respond	Plan for Future Cybersecurity Incidents: Containment of Incidents and Affected Devices: • Immediately isolate affected devices from the network to prevent further spread of the incident. • Utilize network segmentation and access controls to contain the impact and limit unauthorized access. Neutralization Procedures: • Engage incident response team members to analyze the incident and determine appropriate actions. • Deploy intrusion detection and prevention systems to block malicious traffic and prevent further exploitation. • Apply security patches, updates, or configuration changes to address vulnerabilities exploited during the incident. • Restore affected systems from clean backups to ensure

	their integrity and eliminate any lingering threats. Data Analysis: ● Collect and analyze relevant data and logs from affected devices, network appliances, and security tools. ● Utilize SIEM tools to correlate and contextualize event data for comprehensive analysis. ● Identify indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) used by attackers to inform future prevention efforts. Improving Recovery Process: ● Conduct a post-incident review to assess response effectiveness and identify areas for improvement. ● Document lessons learned and update incident response procedures, including response roles and responsibilities. ● Enhance backup and recovery capabilities to ensure timely restoration of critical systems and data. ● Provide additional training and awareness programs for employees to recognize and respond to security threats effectively.
Recover	To recover immediately from the cybersecurity incident described in the scenario, the organization would require the following key information: Backup Data: Access to recent and clean backup data is crucial for restoring affected systems and services to their pre-incident state. Incident Response Documentation: Detailed documentation of the incident response efforts taken during the incident would

	provide valuable insights into the actions taken, the extent of the damage, and any remediation steps already initiated. Analysis Results: Insights gained from the analysis of security event data, network logs, and system snapshots collected during the incident response phase are essential for understanding the nature and scope of the incident. This information helps prioritize recovery efforts and address any underlying vulnerabilities. Prioritized Recovery Plan: A well-defined recovery plan outlining the sequence of steps required to restore and recover affected systems, applications, and services is necessary for efficient and organized recovery operations. This plan should prioritize critical assets and establish clear timelines for restoration. Based on the fact that the incident only affected the organization for 2 hours, were able to quickly detect the attack, put a plan in motion by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. It seems the organization already has a good incident response plan, critical service restoration procedures, and network monitoring measures.

Reflections/Notes: