Cybersecurity Framework NIST

Scenario

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 incident and integrate your analysis into a general security strategy:

1. Identify security risks through regular audits of internal networks, systems, devices, and access privileges to identify potential gaps in security.
2. Protect internal assets through the implementation of policies, procedures, training and tools that help mitigate cybersecurity threats.
3. Detect potential security incidents and improve monitoring capabilities to increase the speed and efficiency of detections.
4. Respond to contain, neutralize, and analyze security incidents; implement improvements to the security process.
5. Recover affected systems to normal operation and restore systems data and/or assets that have been affected by an incident.

Respond

Summary

ICMP/ping flood attack is possible due to multiple compromised systems sending a huge volume of ICMP echo requests to the target. In this case, ICMP/ping flood causes network services to become unresponsive or stop working. Then, the organization decided to block the flood attack and stop all non-critical network services to overcome the disruptions caused by denial of services (DDos) through incoming ICMP/Ping flood packets.

NIST CSF

No	Description
1	Identify the following: - Technology/Asset: Which system and devices were affected? - Process/Business environment: Which business processes were affected in the attack? - People: Who needs access to the affected systems? Here is my respond: The attacker targeted the company with an ICMP flood attack. As a result, the internal network was affected and disrupted all staff from doing the operation tasks. Therefore, to function again, the internal network has to be restored.
2	Protect and implement safeguards: - Access controls: Who needs to the affected items? How are non-trusted sources blocked from having access? - Awareness/Training: Who needs to be made aware of this attack and how to prevent it from happening again? - Data security: Is there any affected data that needs to be made more secure? - Information protection and procedures: Do any procedures need to be updated or added to protect data assets? - Maintenance: Do any of the affected hardware, OS or software need to be updated? Protective Technology: Are there any protective technologies, like a firewall or an intrusion prevention system (IPS), that should be implemented to protect against future attacks? Here is my respond: The cybersecurity team should be alerted immediately when the attacks occur. Since all staff need to gain access via the internal network, it is best to implement a new firewall rule to limit the rate of incoming ICMP packets and update it regularly to keep up with the attack trends. In addition, the cybersecurity team should update and monitor the current status of devices, OS or software to ensure the latest updates have taken place. Moreover, the cybersecurity team should implement an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
3	Detect threats and attacks: - Anomalies and events: What tools could be used to detect and alert IT security staff of anomalies and security events, such as a security information and event management system (SIEM) tool? - Security continuous monitoring: What tools or IT processes are needed to monitor the network for security events? - Detection process: What tools are needed to detect security events, such as an IDS? Here is my respond: The cybersecurity team could configure source IP address

No	Description
	verification on the firewall, analyze the spoofed IP address on wireshark or TCPdump on incoming ICMP packets, and implemented network monitoring software (SIEM, such as Splunk, LogRhythm) to detect abnormal traffic patterns.
4	Respond to threats and attacks: - Planning: What action plans need to be implemented to respond to similar attacks in the future? - Communications: How will security event response procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff? - Analysis: What analysis steps should be followed in response to a similar attack? Mitigation: What responding steps could be used to mitigate the impact of an attack, such as offlining or isolating affected resources? Improvements: What improvements are needed to improve response procedures in the future? Here is my respond: The cybersecurity team should establish risk management for future security events. This report should act as a guide or standard operation when threats arise. Should it occur, the cybersecurity would inform the end users what is the next step immediately and take action to reduce the spread of malicious files in the network by isolating affected systems. The team will attempt to restore any disruptive critical systems and services. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will have to report all incidents to upper management and legal authorities as per law and regulation.
5	Recover affected systems or data: - Recovery planning: How will resources be restored following an attack? - Improvements: Do any improvements need to be made to the current recovery systems or processes? - Communications: How will restoration procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff? Here is my respond: To begin with, we need to address the issue of ICMP flooding to ensure uninterrupted access to network services. The team may use a firewall to block ICMP flood attacks. In practice, the critical network services should be the top priority, while the non-critical networks could go offline. Finally, once the flood of ICMP packets has timed out, all non-critical network systems and services can go back online.