Incident report analysis

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Summary	The orginaztion suffered a a DDoS attack via an out of date fire wall from a malicious actor. The Actor sent a flood of ICMP pings to the companies network thought an unconfigured fire wall. The incident managment team responded by blocking incoming packets, stopping non critical network services and restoring critical ones.
Identify	• Conduct regular audits of internal networks, systems, devices, and access privileges to identify potential vulnerabilities and security gaps. • Specifically, vulnerabilities related to firewall configurations, such as unconfigured settings that allow for excessive ICMP traffic, should be identified. • Ensure network infrastructure components like firewalls are regularly updated and configured correctly to mitigate security risks.
Protect	• Implement policies, procedures, and training programs to educate employees on cybersecurity best practices, including the importance of firewall configurations and the risks associated with DDoS attacks. • Deploy security tools and technologies, such as intrusion detection/prevention systems (IDS/IPS), to monitor and filter incoming traffic, particularly ICMP packets, for suspicious activity.

	• Enforce access controls and authentication mechanisms to prevent unauthorized access to network resources and infrastructure.
Detect	• Enhance monitoring capabilities by deploying network monitoring software to detect abnormal traffic patterns, such as sudden spikes in ICMP traffic indicative of a potential DDoS attack. • Implement alerting mechanisms to notify security teams of potential security incidents in real-time. This will allow for a rapid response to mitigate further damage.
Respond	• Develop incident response procedures and protocols to promptly contain, neutralize, and analyze security incidents. • In response to a DDoS attack, consider implementing firewall rules to limit the rate of incoming ICMP packets and performing source IP address verification to prevent IP address spoofing. • Collaborate with incident management teams to coordinate efforts to block malicious traffic, restore critical network services, and implement necessary improvements to prevent similar incidents.
Recover	• After containing the DDoS attack, focus on restoring affected systems to regular operation and ensuring the integrity of system data and assets. • Conduct post-incident analysis to identify lessons learned and areas for improvement in the incident response process. • Update security policies, procedures, and controls based on the incident analysis's findings to strengthen the organization's resilience against future cybersecurity threats.

Reflections/Notes:

- Review and update firewall configurations regularly to ensure they align with current security best practices and effectively mitigate emerging threats.
- Provide ongoing training and awareness programs to educate employees about cybersecurity risks and their role in maintaining a secure network environment.
- Continuously monitor and assess the effectiveness of security controls and incident response procedures to adapt to evolving cybersecurity threats.