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 multimedia company experienced a Distributed Denial of Service (DDoS) attack that disrupted its internal network for two hours. The attacker exploited an unconfigured firewall to flood the network with ICMP packets, overwhelming network devices and preventing legitimate traffic from accessing network resources. This resulted in the unavailability of critical services, including the company website, impacting employees and clients. **N NIST Cybersecurity Framework (CSF) Plan for Improvement** To enhance the company's network security and mitigate future DDoS attacks, the following plan utilizes the NIST CSF framework.
Identify	**(Security Risks)** Conduct regular vulnerability scans and penetration testing to identify and address security gaps in network devices and configurations. Maintain a comprehensive asset inventory and perform routine security audits to ensure all devices are properly secured and configured.

Protect	**(Internal Assets)** Implement firewall hardening with standardized configurations and regular rule reviews. Utilize network segmentation to isolate critical systems and limit the impact of attacks. Fine-tune Intrusion Prevention Systems (IPS) to detect and block DDoS attacks. Enforce strict access control policies and conduct security awareness training for employees.
Detect	**(Potential Security Incidents)** Deploy a Security Information and Event Management (SIEM) system for centralized log collection and analysis. Establish baseline traffic analysis and configure real-time alerts for suspicious network activity. Perform regular log analysis to identify patterns of malicious behavior.
Respond	**(Contain, Neutralize, Analyze)** Develop a comprehensive incident response plan outlining procedures for containing, eradicating, and recovering from DDoS attacks. Establish a clear communication plan to keep stakeholders informed during incidents.

	Conduct thorough post-incident analysis to identify root causes and improve security controls.
Recover	**(Affected Systems)** Implement regular data backups and test restoration procedures. Design redundant systems to minimize downtime during attacks. Develop a disaster recovery plan to ensure business continuity. Establish Service Level Agreements (SLAs) with service providers for timely recovery. Conduct regular testing of recovery plans.

Reflections/Notes: To keep it short and simple, utilizing this comprehensive approach; guided by the NIST CSF framework. Will help strengthen the company's security posture and reduce the risk of future DDoS attacks.

Reflections:
Importance of Proactive Security: This incident highlights the critical need for proactive security measures rather than relying solely on reactive responses. Regularly auditing network configurations, implementing robust firewalls, and employing intrusion detection/prevention systems are crucial for preventing such attacks.

Human Error: The unconfigured firewall emphasizes the role of human error in security breaches. It's essential to have processes in place to minimize misconfigurations and ensure consistent security practices.

Defense in Depth: The incident underscores the importance of a "defense in depth" strategy. Multiple layers of security, including firewalls, intrusion detection systems, and network monitoring, can help mitigate the impact of an attack, even if one layer fails.

Incident Response Planning: Having a well-defined incident response plan is crucial for minimizing downtime and ensuring a swift and effective response to security events. This includes clear communication protocols and recovery procedures.

Notes:
ICMP Rate Limiting: Consider implementing ICMP rate limiting on the firewall to prevent future ICMP floods.

Spoofed IP Address Detection: Investigate techniques for detecting and mitigating spoofed IP addresses to enhance the effectiveness of IP blocking.

Network Traffic Baselining: Establish baseline network traffic patterns to facilitate the identification of anomalies and potential attacks.

Security Awareness Training: Conduct regular security awareness training for employees to educate them about DDoS attacks, phishing scams, and other social engineering tactics.

Regular Updates and Patching: Ensure all network devices and software are regularly updated and patched to address known vulnerabilities.

Vendor Diversity: Avoid single points of failure by using multiple vendors for critical network infrastructure and services.

Cloud-Based DDoS Protection: Explore cloud-based DDoS protection services to provide additional resilience against large-scale attacks.