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	Our multimedia company suffered a DDoS attack through ICMP packet flooding, disrupting services for two hours due to an unconfigured firewall. Response actions included blocking ICMP traffic, isolating services, and restoring critical operations. We implemented firewall enhancements, IP verification, and monitoring systems. Communication was managed with stakeholders, and post-incident, we improved security training and recovery processes. This event highlighted the need for continuous security audits, proactive threat management, and robust recovery strategies to safeguard our network-reliant business operations.
Identify	The attack was a Distributed Denial of Service (DDoS) using ICMP ping floods, overwhelming the network through an unconfigured firewall. It impacted web design, graphic design, and social media marketing services by rendering network services unreachable for two hours. Hardware like routers, switches, and possibly servers were affected, disrupting all network-dependent operations. Employees needing access to network tools, including IT for management and designers for cloud-based work, were directly impacted, highlighting vulnerabilities in network management and business continuity.

Protect	The team protected the network by implementing new firewall rules to limit ICMP packet rates, adding source IP verification to combat spoofing, and deploying network monitoring software along with an IDS/IPS system to detect and filter suspicious traffic. Access control was tightened, ensuring only trusted sources could interact with critical systems. Awareness training was extended to all employees to recognize and prevent similar attacks. Data security was reviewed, though no specific data was compromised, procedures were updated to enhance data asset protection. Maintenance included updates to affected hardware and software to patch vulnerabilities, and protective technologies were reassessed and bolstered to safeguard against future DDoS threats.
Detect	To detect the DDoS attack, the team implemented network monitoring software to spot anomalies in traffic patterns. A Security Information and Event Management (SIEM) system was used to alert IT security staff of unusual activities. For continuous security monitoring, they enhanced their IT processes with real-time network traffic analysis tools. An Intrusion Detection System (IDS) was crucial in the detection process, identifying the flood of ICMP packets characteristic of this attack, thereby allowing for timely response and mitigation.
Respond	In response to the DDoS attack, the team blocked incoming ICMP packets, took non-critical network services offline, and restored critical services to mitigate the impact. They formulated action plans for future responses, including procedures for traffic filtering and resource isolation. Communication was managed by notifying IT staff and stakeholders about the incident and preventive measures. Analysis involved a post-incident review to understand the attack vector and effectiveness of the response. Improvements included updating response protocols, enhancing communication strategies, and training staff on new procedures to ensure a more efficient response to future incidents.

Recover	Recovery from the DDoS attack involved gradually bringing network services back online once the threat was neutralized, starting with critical systems. They restored resources by ensuring all systems were functioning correctly after the attack, possibly using backup data if necessary. Improvements to recovery processes included updating recovery plans to include more robust testing of backups and quicker rollback procedures. Communication about restoration was managed through updates to IT staff and stakeholders, informing them of system status and expected return to normal operations, ensuring transparency and maintaining trust.

Reflections/Notes: The DDoS attack on our multimedia company was a stark reminder of the importance of network security. It exposed vulnerabilities, particularly with the unconfigured firewall, which allowed an overwhelming flood of ICMP packets to disrupt our services for two hours. The response was swift, involving blocking these packets, isolating non-critical services, and restoring essential operations, but it underscored the need for quicker, more automated responses to minimize downtime. Communication with stakeholders was critical, and while we managed to keep everyone informed, there's a clear need for more structured and rapid communication protocols. The incident analysis led to immediate enhancements like new firewall rules, IP verification, and the deployment of network monitoring software and an IDS/IPS system to prevent future occurrences. However, it also highlighted areas for improvement in our security training programs, ensuring all employees are aware of cybersecurity threats and response procedures. The recovery phase taught us the value of having robust backup and recovery systems, as we restored services methodically, though this process could benefit from more rigorous testing and quicker rollback mechanisms. This event has been a critical learning point, emphasizing the need for continuous security audits, updates to our incident response and recovery plans, and the development of better business continuity strategies. It's clear that our network services are vital to our operations, pushing us towards greater resilience through redundancy or perhaps third-party DDoS protection services. Moving forward, we must foster a culture of security consciousness, regularly update