Incident report analysis

Instructions

Summary	This morning, a DDoS (Distributed Denial of Service) attack compromised our internal network for approximately two hours before it was resolved. The attack resulted in a flood of ICMP (Internet Control Message Protocol) packets, causing our network services to become unresponsive. Our incident management team promptly responded by blocking incoming ICMP packets, taking non-critical network services offline, and restoring critical network services.
Identify	Type of Attack: DDoS (Distributed Denial of Service) attack Systems Affected: Internal network services, network resources
Protect	To enhance the security of our organization's assets and mitigate future cybersecurity incidents, we have implemented the following measures: New firewall rule: A firewall rule has been established to limit the rate of incoming ICMP packets, preventing overwhelming traffic. Source IP address verification: The firewall now checks for spoofed IP addresses on incoming ICMP packets, mitigating potential IP address-based attacks. Network monitoring software: We have deployed network monitoring software to detect abnormal traffic patterns and identify potential threats promptly. IDS/IPS system: An Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) have been implemented to filter out suspicious ICMP traffic based on predefined characteristics.
Detect	To proactively detect potential cybersecurity incidents and maintain a secure network environment, we will employ the following measures: Continuous network traffic monitoring: Regularly monitoring network traffic on devices to identify any suspicious activity, such as incoming external ICMP packets from non-trusted IP addresses attempting to bypass our network firewall.

	Application monitoring: Implementing software applications to monitor and analyze network traffic, track authorized versus unauthorized users, and detect any unusual activity on user accounts.
Respond	In the event of future cybersecurity incidents, we will follow this response plan: Incident containment: Swiftly containing cybersecurity incidents and isolating affected devices to minimize the impact on our network and systems. Incident neutralization: Implementing appropriate procedures and countermeasures to neutralize cybersecurity incidents effectively and prevent further unauthorized access or damage. Incident analysis: Collecting relevant data and information to analyze the incident thoroughly, identifying the root causes and any vulnerabilities that need to be addressed. Recovery process improvement: Identifying areas where our organization's recovery process can be enhanced to better handle future cybersecurity incidents, such as streamlining data restoration procedures and establishing clear recovery priorities.
Recover	To recover from this cybersecurity incident and ensure a return to normal operation, we will undertake the following steps: Immediate recovery information: We will prioritize the recovery of critical systems, such as network services and essential data repositories, to minimize disruption to our operations. Established recovery processes: Leveraging established recovery processes and procedures to restore affected systems and assets, ensuring that backups are up to date and readily accessible.

Reflections/Notes: During the incident response process, it became evident that our organization would benefit from ongoing monitoring and analysis of network traffic. Implementing network traffic monitoring tools and user behavior analytics will enable us to proactively detect and mitigate potential cybersecurity threats. Additionally, regular reviews of our incident response plan and continuous employee training are essential to maintain a strong security posture and adapt to evolving attack vectors. By incorporating these reflections into our cybersecurity practices, we aim to further enhance our network security and protect our organization's assets.