Incident report analysis

Instructions

Summary	Earlier today, our company encountered a DDoS (Distributed Denial of Service) attack that disrupted our internal network for a duration of two hours until its resolution. The attack caused a sudden halt in the organization's network services, attributed to an overwhelming influx of ICMP packets, rendering normal internal network traffic unable to access resources. In response, the incident management team swiftly acted by implementing measures such as blocking incoming ICMP packets, taking non-critical network services offline, and restoring critical network functionalities. Subsequently, the cybersecurity team conducted a thorough investigation into the security incident.
Identify	The incident management team's investigation revealed that a malicious actor exploited an unconfigured firewall to inundate the company's network with a barrage of ICMP pings. This vulnerability enabled the attacker to execute a distributed denial of service (DDoS) attack, causing a substantial disruption. As a result, critical network resources required immediate securing and restoration to ensure a return to normal operational status.
Protect	The network security team enacted proactive measures, including the implementation of a new firewall rule designed to restrict the influx of incoming ICMP packets by imposing rate limitations. Additionally, an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) were deployed to intelligently filter suspicious ICMP traffic based on identified anomalous characteristics. These actions fortify our network's defenses against potential threats, aligning with the proactive protection measures advocated by the NIST CSF.

Detect	The incident response team implemented network monitoring software to identify irregular traffic patterns and instituted source IP address verification within the firewall. This approach enables the detection of potential DDoS attacks or other threats by scrutinizing incoming ICMP packets for potential IP address spoofing, aligning with the NIST CSF's guidelines for robust detection strategies.
Respond	The incident management team will proactively monitor high-risk events by leveraging network analyzer's logs. This will facilitate the thorough analysis of network logs to detect any signs of suspicious or abnormal activities. Additionally, the team will ensure the diligent reporting of all incidents to upper management and relevant legal authorities, aligning with the NIST CSF's emphasis on proactive response and comprehensive reporting protocols.
Recover	In future incidents, external ICMP flood attacks will be prevented by implementing firewall blocks. To minimize internal network congestion, non-critical network services will be temporarily halted. Priority will be given to restoring critical network services promptly. Once the ICMP packet flood times out, non-critical network systems and services will be gradually reinstated.

Reflections/Notes: