Incident report analysis

Summary	Recently our company experienced a Distributed Denial of Service (DDoS) attack that disrupted the company's internal network for two hours. The attack targeted the network with a flood of ICMP packets, causing widespread service unavailability. The incident management team responded by blocking incoming ICMP packets, temporarily shutting down non-critical network services, and restoring critical services. Subsequent investigation by the cybersecurity team revealed that the attack exploited an unconfigured firewall, allowing a malicious actor to execute the DDoS attack. In response, the organization implemented several security measures, including rate-limiting incoming ICMP packets, introducing source IP address verification on the firewall, and implementing an IDS/IPS system to filter suspicious ICMP traffic.
Identify	After an in-depth investigation, the cybersecurity team ascertained that the malevolent actor executed the attack by inundating the company's network with a substantial volume of ICMP pings. This exploit was facilitated by compromising an inadequately configured firewall, thereby providing the malicious actor with the means to effectively orchestrate a Distributed Denial of Service (DDoS) attack against the company's infrastructure.
Protect	In response to this security incident, the network security team proactively enacted a series of protective measures. These included the implementation of a novel firewall rule designed to curtail the influx of incoming ICMP packets by regulating their rate. To counter the threat of IP address spoofing, they introduced source IP address verification within the firewall's framework. Additionally, the team enhanced the organization's defense mechanisms through the deployment of sophisticated network monitoring software, enabling the swift identification of aberrant traffic patterns.

Detect	To detect this type of incident before it occurs an Intrusion Detection and Prevention System (IDS/IPS) was employed, empowering the system to selectively filter out potentially malicious ICMP traffic based on discerned suspicious characteristics. Collectively, these measures serve to enhance the resilience of the organization's network against similar threats in the future.
Respond	To proactively address similar threats and attacks in the future, the organization should establish comprehensive response plans encompassing prompt threat detection, firewall optimization, and resource isolation. Effective communication protocols need to be outlined for internal teams, end users, and IT staff, ensuring transparent updates throughout the incident. In response to similar attacks, a meticulous analysis of attack vectors, techniques, and vulnerabilities should guide adaptive security measures. Mitigation efforts should prioritize rapid resource isolation and consider traffic redirection strategies to minimize disruptions. To refine response procedures, routine penetration testing, firewall reviews, and post-incident reviews are essential, ensuring continuous improvement and heightened readiness.
Recover	In response to the incident, the company enacted a meticulous recovery plan, by prioritizing the restoration of vital resources and services impacted by the attack. The recovery process involved systematic validation and utilization of regularly updated backups to ensure data integrity and facilitate the staged restoration of systems. To enhance the current recovery systems and processes, the organization focused on implementing more frequent and comprehensive backup procedures, introducing automated recovery scripts, and integrating redundant failover mechanisms to minimize downtime.

Reflections/Notes: