Incident report analysis

Summary	A DDos attack (Distributed denial of service attack) occurred which compromised the internal network for two hours until it was resolved. There was an incoming flood of ICMP packets so the network services suddenly stopped working and the normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets which restored critical network services. In order to resolve the issue, we had to implement a few more things like creating a new firewall rule to limit the rate of incoming ICMP packets and network monitoring software to detect abnormal traffic patterns.
Identify	A DDos attack (Distributed denial of service attack) occurred due to a flood of ICMP packets. Our network services suddenly stopped responding so the normal internal network traffic could not access any network resources.
Protect	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services.
Detect	After an in depth analysis was done, we found out that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This allows the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Respond	In order to be better prepared, we implemented a few things that we realized were loopholes for future attacks. Those things were a new firewall rule to limit the rate of incoming ICMP packets, source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, network monitoring software to detect abnormal traffic patterns, and

	implementing an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Recover	We verified and restored all network services to ensure normal operations as well as tested and validated the effectiveness of the new firewall rules and network monitoring tools. The incident response has been updated based on lessons learned from this attack. Lastly, training was conducted for the IT team on identifying and mitigating similar threats in the future.

Reflections/Notes:

- A misconfigured firewall was a critical vulnerability that facilitated the attack. Regular audits of firewall settings and configurations are essential.
- Quick incident response measures (blocking ICMP packets) significantly reduced the downtime.
- Implementing proactive tools like IDS/IPS and monitoring software strengthens detection and prevention capabilities.
- Schedule regular network security audits.
- Expand training for staff on incident response procedures.
- Periodically test the IDS/IPS systems and firewall rules to ensure they remain effective against evolving threats.
- Collaboration within the incident management team was crucial to resolving the attack quickly.
- Continuous monitoring and periodic updates to security protocols help mitigate future risks.