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	The organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. After investigation it was found out that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall resulting in DDoS attack. The internal network was compromised for two hours until it was resolved. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline and restoring critical network services. The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets, also set a source IP address verification on the firewall to check spoofed IP addresses, added an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Identify	The company's cybersecurity team investigated the security event and found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack. The internal network was compromised for two hours until it was resolved. Normal internal network traffic could not access any network resources.

Protect	The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To detect new unauthorized access attacks in the future, the team will use a network monitoring software to detect abnormal traffic patterns and has configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets.
Respond	For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyse network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.
Recover	To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.

Reflections/Notes: