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	Two hours before the incident resolved, organization experienced Denial of Service (DoS) Attack with flood of ICMP packets method, which is compromised internal network for two hours, because malicious actor had sent flood of ICMP packet through an unconfigured firewall. During the attack organization network services suddenly stopped responding due to an incoming flood of ICMP packet and normal internal network services couldn't access any resources. The Incident management responded by blocked incoming ICMP packet, Stopping non-critical network service offline and restoring critical network services. To address security event, the network security team will implented : 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 an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Identify	The network security team investigated the incident. They found that threat actor had sent incoming flood of ICMP packet through an unconfigured firewall. This vulnerability allowed malicious attacker to overwhelmed the company network through Denial of Service (DoS) attack.
Protect	To prevent future attacks the network security attacks implemented : new

	firewall rule to limit rate of incoming ICMP packet, 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. Additionally the team implemented an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	To detect future attacks, we will use Network monitoring software to detect traffic patterns, Source IP address verification on the firewall to check for spoofed IP addresses on incoming flood packets. Additionally, we will use an IDS/IPS system to monitoring and filter out based on suspicious characteristics.
Respond	After making some improvement on network security, we will use a new firewall to limiting suspicious traffic, verifying source IP address to check for spoofed IP addresses on incoming malicious packets, use an IDS/IPS to filter out malicious packets and stopping non-critical network services offline.
Recover	During incident recover method is stopped non crucial network services offline, after network turned into offline, the team will restored crucial network service data. If the attack already solved, crucial network service data will be brought online. But for improvements before malicious actor attack the company will save crucial network services data.

Reflections/Notes: