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 security event was caused by a flood of ICMP packets from a malicious actor attempting to cause a distributed denial of service (DDoS) attack. Normal internal network traffic could not access any network resources. The aforementioned DDoS attack compromised the internal network for two hours until it was resolved. The incident management team responded by blocking all incoming ICMP packets, stopping all non-critical network services offline, so that critical network services could be restored.
Identify	Malicious actor(s) targeted the company with an ICMP flood attack. The entire internal network was affected. All critical network resources needed to be secured and restored to a functioning state.
Protect	The network security team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic that tries to access the network based on suspicious characteristics.
Detect	The network security team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented a network monitoring software to detect abnormal traffic patterns.

Respond	For future security events the cybersecurity team will isolate the affected systems to prevent whole disruption to the network. They will attempt to restore any critical systems and services that were affected and disrupted by the event. Following which the team will analyze network logs to check for suspicious and abnormal activity across the internal network. The team will also report all incidents to upper management and appropriate legal authorities, if applicable to the attack.
Recover	To recover from a DDoS attack by ICMP flooding access to network services needs to be restored to a normal functioning state. In the future external ICMP flood attacks can be blocked at the firewall(s) previously implemented and continuously monitored.. Following which all non-critical network services should be stopped to reduce the strain on internal network traffic. Next critical network services should be fully restored first. Finally once the flood of ICMP packets have timed out all non-critical network systems and services can be brought back online to begin normal everyday procedures.

Reflections/Notes: