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	Recently, our organization’s network services stopped responding due to an incoming flood of ICMP packets. The internal network was then compromised, and normal internal network traffic was unable to access any network resources. The incident management team responded to the incident by blocking all incoming ICMP packets, stopping all non-critical services offline, and restoring critical network services. The total time that the internal network was compromised was 2 hours when services were restored. The company’s cybersecurity team then investigated the security event. They 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 DDoS attack. To address this incident, and any further attacks of this nature in the future, the network security team implemented: ● 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 ● An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

Identify	The attack was identified as an Internet Control Message Protocol (ICMP) flood due to the network being overloaded by ICMP packets. It was found to have occurred due to an unconfigured firewall that the malicious actor used to send the flood of ICMP packets. Due to the attack, internal network resources were unable to be utilized by internal network traffic.
Protect	To better protect the organization against ICMP floods, the unconfigured firewall will be configured to limit the rate of incoming ICMP packets. The firewall will also be able to verify source IP addresses to defend against IP spoofing on incoming ICMP packets. An IPS will be installed to filter out suspicious ICMP traffic.
Detect	An IDS system will be installed to detect abnormal traffic patterns and network monitoring software will be installed to detect suspicious network activity.
Respond	In the future should such an attack occur, the security team will block the incoming ICMP packets, shut down all non-critical services offline, then restore the critical services. The security team has reported the incident to upper management and will follow-up with appropriate legal authorities if necessary.
Recover	Access to internal network resources need to be restored. Non-critical services need to be stopped to free up network traffic for critical services to run. After the introduced firewall blocks the incoming ICMP packets, then non-critical services can be brought back online.

Reflections/Notes: