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	Most recently our company experienced a distributed denial of service attack(DDoS) due to an unconfigured firewall on the network. The attackers exploited this by flooding our network with ICMP requests. The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored. After recovering from the attack our team implemented some new security measures to prevent this type of attack in the future. • 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 incident management team audited the systems involved in the attack. The team found that there had been an unconfigured firewall on the network in which the attacker or attackers were able to exploit by sending an unimaginable number of ICMP requests. The incident affected our entire network. All critical network resources needed to be secured and restored to a functioning state.

Protect	The team has implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The team has also added networking monitoring software to detect abnormal traffic patterns. The team has also configured source IP address verification 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 analyze 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: