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 experienced a DDoS attack. A DDoS attack is a type of Distributed Denial of Service attack where the server is loaded with a huge amount of requests from the attacker. In the attack we faced today, we received ICMP DDoS requests, as it is distributed attack, the requests were coming from all over the places/world. The incident management team responded by blocking incoming ICMP packets and restoring critical network services.The attacker was able to execute the DDoS attack because of the unconfigured firewall which was unable to block the attacker from flooding the ICMP requests. To address this security event, 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 incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found out that the attacker was able to flood the ICMP requests because of the unconfigured firewall. Because of this, the organization's network services stopped responding, particularly the internal network which includes servers
Protect	To protect the valuable information and assets of the organization, we need to implement policies that can be safeguarded from the attackers accessing them. The following security policies should be implemented: ● Update the firewall configuration ● 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
Detect	To detect this type of attack happening in future, we can use the IDS and SIEM tools to analyze the network log data and identify any ICMP DDoS attack in the future
Respond	To respond to the attack we can use the IPS that will on detection of the intrusion attack perform functions to contain the attack from spreading further more into the organization's network. The attack can be neutralized by configuring the firewall with a limited number of ICMP requests coming in, identifying source IP is legal or spoofed and using the IPS/IDS
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.