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	It was noticed that the company recently encountered a DDOS attack which compromised the organization's internal network for at least 2 hours. During the attack, the organisation's network system stopped working due to a flood of ICMP packets leaving all normal network traffic unattended to. The security team then responded by blocking all ICMP packets, stopping all non-critical network services and restoring critical network services. After thorough investigation by the security team, it was noticed that a malicious actor sent a tonne of ICMP packets through an unconfigured firewall. This vulnerability allowed the malicious actor to overwhelm the organisation's network with a DDOS attack that compromised the organisation's network. To address the security challenge, the following were implemented: 1. A new firewall rule to limit the rate of incoming ICMP packets 2. Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets 3. Network monitoring software to detect abnormal traffic patterns 4. An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics

Identify	The attack that occurred was a distributed denial of service (DDOS) attack which has to do with a malicious actor using devices or servers in remote locations to target a particular network and flood it with unwanted traffic. This attack was based on the ICMP flood attack which had to do with the repeated sending of ICMP packets to a network. The attack had a negative impact on the organisation's web servers and all other day to day operations. It made the website unavailable to genuine users, thereby, truncating the business flow of the day for about two hours
Protect	A new firewall rule to limit the rate of incoming ICMP packets. This will help reduce the likelihood of DDOS and ICMP flood attacks. Another way of protection involves source IP verification on the firewall to check for spoofed IP addresses sending ICMP packets.
Detect	The use of IPS/IDS should be used to help prevent and detect malicious traffic from an unknown IP address. And also to detect an attempt of IP spoofing from a malicious actor.
Respond	For situations like this, it was advised that all incoming ICMP packets should be blocked, non critical network services should be stopped and only critical network services should be allowed. then the affected systems should be isolated so as to reduce the spread of the damage to other parts of the network.
Recover	To recover from the incident, a DDOS protection e.g cloudflare rules, AWS setup etc needs to be set up that makes it almost impossible to occur in the nearest future. Then, gradually restoring network services.

Reflections/Notes: