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, the company has experienced a DDos attack which compromised the internal network for 2 hours. This incident led to an investigation that unfolded security gaps within our configuration. During the attack, the incident the organization's network services experienced an flood of ICMP packets. To mitigate this, the security team blocked all incoming iCMP packets and shit down all non-critical network services offline.
Identify	Through our security audit, we have discovered a potential gap in our security resulting from the attack. We found that the malicious actor has sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability led to the company's DDoS attack.
Protect	The company has decided to implement a new firewall rule that will limit the rate of incoming ICMP packets. This will deter future ICMP flood attacks and solve one security flaw. We have also opted to implement a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. In addition, we have installed a network monitoring software to detect abnormal traffic patterns preventing future attacks similar to this security incident
Detect	To further our security hardening, we have installed an IDS/IPS (intrusion

	Detection System/Intrusion Prevention System) system which would help us log firewall traffic and prevent unwanted infiltrations. We have also implemented an IP address verification on the firewall to check for spoofed IP addresses from ICMP packets.
Respond	We have disabled/blocked incoming ICMP packet traffic to recover network resources. This will stop all non-critical network services and restore critical services. The security team will begin network log analyzation to check for suspicious/abnormal activity
Recover	Recovering from DDoS attack (ICMP Flood), all network services must be reinstated to their original normal state. To do so, all non-critical network services will be stopped to recover network resources and reduce network traffic. Critical network services will be reestablished first to mitigate down-time. Once network resources have been recovered and all operations are normal, non-critical network services will be reinstated. Additionally, for future events, we have set a rule to block external ICMP flood attacks on our firewall.

Reflections/Notes: