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 company's internal network was compromised for 2 hours. The network services had stopped responding because it was flooded with ICMP packets. This caused normal internal network traffic to be unable to connect to network resources. We believe this was caused by a malicious actor trying to disrupt the company's normal business operations. The team responded by blocking the attack and halting the non-critical network services in order to restore the critical network services.
Identify	The cybersecurity team found that the attacker sent a flood of ICMP pings to the company's network. This was done through an unconfigured firewall which allowed the attacker to perform a DDOS attack on the company's network.
Protect	The network security team has implemented firewall rules to verify source IP addresses in order to prevent spoofed IP addresses on incoming ICMP packets, they also added a rule to limit rate of incoming ICMP packets. They implemented a network monitoring software to detect abnormal traffic patterns and finally they implemented an IDS/IPS system in order to filter out ICMP traffic based on suspicious characteristic.
Detect	To detect an ICMP flood DDOS attack in the future, the network security team implemented a network monitoring system and IDS system in order to monitor

	network traffic. The firewall has also been configured to verify source IP addresses to detect spoofed IP addresses.
Respond	The incident management team shut down all non-critical services and restored the critical network services, they also blocked all incoming ICMP packets. For future events the team should isolate affected systems to prevent more disruption to the network, they also must report to upper management and legal authorities if possible.
Recover	In order to recover the network services the critical networks should be restored first while halting non-critical services in order to reduce internal network traffic. Once the flood of ICMP packets time out, non-critical network services should be restored next. This attack can be stopped by a properly configured firewall

---

Reflections/Notes: