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	This morning a multimedia company experienced a DDoS attack, which compromised the network for 2 hours. The network came to a halt due to an incoming flood of ICMP packets that were sent into the network through an unconfigured firewall . Normal internal network traffic could not access any network resources. In response the cyber security department blocked incoming ICMP packets, all that were non-critical network services offline. Critical networks were restored. The team addresses the event by implementing a new firewall rule, to limit the rate of incoming ICMP packets. Source IP address verification was also implemented to check for spoofed IP addresses on incoming ICMP packets. Network monitoring software was installed as well as an IDS/IPS system to filter out ICMP traffic based on suspicious characteristics.
Identify	Type of attack: - (DDoS) Distributed Denial of Service Systems impacted: - Internal network services, particularly those handling ICMP packets
Protect	The team has implemented updates to the firewall configurations, will conduct regular security training for staff, implement strict access controls and

	encryption for sensitive data, and regularly update all systems and software to patch vulnerabilities.
Detect	To detect unauthorized access the team will implement continuous monitoring of network traffic for abnormalities, use advanced intrusion detection systems (IDS) to mark unusual patterns, regularly audit user activities and validate authentication logs, and deploy network analysis tools to inspect both incoming and outgoing traffic.
Respond	The response plan for future incidents will be establishing a protocol for immediate isolation of affected systems, developing a communication plan for internal teams and external stakeholders, keeping an updated incident response incident response playbook, and training the security response team on the latest threat detection and mitigation strategies.
Recover	To Recover we will implement backup plans for critical data and systems, create a disaster recovery plan detailing steps to restore services, regularly test and update the recovery procedures, and finally review and learn from each incident to improve recovery strategies.

Reflections/Notes: