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 resulting in a compromise of the internal network for two hours. The incident management team responded by blocking incoming ICMP packets, stopping non-critical network services, and restoring critical ones. An investigation revealed a malicious actor used an unconfigured firewall to launch the DDoS attack. To enhance network security, the team implemented new firewall rules, source IP address verification, network monitoring software, and an IDS/IPS system.
Identify	Regular audits of internal networks, systems, devices, and access privileges were conducted to identify gaps in security. The incident management team discovered a malicious actor obtained an intern's login and password, leading to unauthorized access to the customer database. Some customer data was found to be deleted during the attack.
Protect	To prevent future attacks, the team implemented new authentication policies, including multi-factor authentication (MFA), limiting login attempts, and providing training on protecting login credentials. Additionally, a new protective firewall configuration and an intrusion prevention system (IPS) were implemented.
Detect	For enhanced detection capabilities, the team will use a firewall logging tool

	and an intrusion detection system (IDS) to monitor incoming traffic from the internet for unauthorized access.
Respond	In response to the incident, the team disabled the compromised account, provided training to employees, informed upper management, and initiated customer notification procedures. Legal requirements for informing law enforcement and relevant organizations will be adhered to.
Recover	To recover from the incident, the team plans to restore the deleted data by using the database's last night's full backup. Staff has been informed about the need to re-enter any customer information entered or changed during the morning, as it won't be recorded in the backup.

Reflections/Notes: