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	Earlier today there was a flood of ICMP packets that caused the network services to be unresponsive. The incident management team then blocked all incoming ICMP packets, stopped all non-critical networ services, and restored the critical network services.
Identify	The incident management team identified the attack as a DDoS in the form of an ICMP packet flood that disabled the organizations network services. Within the audit the team found that an intern's login and password were obtained by a malicious attacaker and used to access the data from the customer database. Upon intial review it appears that some customer data was deleted from the database.
Protect	The team has implemented new firewall rules that limit the rate of incoming ICMP's and a source IP address verification to check for spoofed IP addresses on incoming ICMP packets. Network monitoring software was installed to detect abnormal traffic patterns. Lastly, an intrusion prevention system (IPS) system was added to filter out some ICMP traffic based on suspicious characteristics.
Detect	To detect new unauthorized accessattacks in the future the team will use an intrusion detection system (IDS) to monitor all incoming traffic alongside a

	firewall logging tool.
Respond	After disabling the intern’s network account we provided training to interns and employees on how to rotect login credentials in the future with better password policies and multifactor authentification (MFA). Upper management was informed of this even and they will contact customers by mail to inform them about the data breach. Management will also need to inform law enforcement and other organizations as required by law.
Recover	The deleted data will be restored using last nights full backup data. The staf has been informed that any customer information logged after last night was not recorded on the backup, so all information will need to be re-entered.

Reflections/Notes: