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	An apparent ICMP flood from an external bad actor using a spoofed IP addressed caused network access to be heavily impacted. The security team responded by restricting inbound ICMP traffic from the spoofed IPs, confirming affected servers were back into operation and taking further steps to harden network gear for DoS attacks like this.
Identify	A DDoS attack took place and impacted the availability of network bandwidth to legitimate users. Network routers, switches, load balancers, and internal servers were impacted.
Protect	Firewalls often have DoS attack protection. Enabling this protection on internet-facing firewalls could help minimize this type of attack in the future.
Detect	Intrusion detection systems and intrusion prevention systems can help detect and prevent this type of attack.
Respond	Conducting penetration testing and network firewall auditing can help prevent these types of attacks by finding problems and fixing them before they occur.
Recover	Communicate the attack information to the organization's users so they are better aware of the realities of constant cybersecurity awareness and dangers.

	Conducting network system audits can help prevent these in the future.

Reflections/Notes: