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	Network service in the company stopped responding to activity. We surmised that this was done by a DDoS attack or a distributed denial of service attack. They flooded our network with ICMP packets. The team rapidly blocked the attack and restored critical network services.
Identify	The company was the target of an ICMP Flood attack and as a result the entire company's network was affected.
Protect	The team configured new firewall settings and rules to limit ICMP packets and implemented an IDS/IPS system to filter out suspicious traffic.
Detect	The firewall was configured to check for spoofed IP Addresses and implemented a network monitoring software to detect any suspicious activity.
Respond	The team will analyze any suspicious activity using the newly implemented monitoring software and IDS/IPS system. If another attack occurs, the team will respond quickly to block traffic and isolate the attack as well as restore critical systems as soon as possible.
Recover	Non critical services are to be stopped so critical services can be up and running as soon as possible to continue business. Firewalls will need to be continuously configured to block similar attacks.

Reflections/Notes: