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 has recently suffered an ICMP flood attack, stopping all network services from functioning. This compromised the internal network for 2 hours until the incident management team could block incoming ICMP packets, stop all non-critical network services, and restore all the critical services. Upon investigation of the event, it was found that the malicious actor had taken advantage of an unconfigured firewall. This vulnerability is what allowed the threat actor to perform a DDoS attack on the organization. In response the network security team implemented a new firewall rule to limit ICMP packets, source IP address verification, network monitoring software, and an IDS/IPS filtering system.
Identify	Upon further investigation it was found that the threat actor took advantage of a vulnerability on the company network via an unconfigured firewall. This brought all network activity to a halt as a DDoS attack was performed, specifically an ICMP flood attack. This stopped normal business operations for all users.
Protect	In response to the incident the security team has implemented a new firewall rule to limit ICMP packets traffic into the network, a source IP address verification to check for spoofed IP addresses attached to the ICMP packets, a network monitoring software to help identify any suspicious traffic, and an

	IDS/IPS filtering system to stop any suspicious ICMP traffic.
Detect	More emphasis is needed on security analysis, specifically using SIEM tools. With these tools the organization can more efficiently monitor and respond to suspicious future activity on the network and address it before it gets out of hand.
Respond	More emphasis will be placed on properly configuring firewalls, network hardening, and maintaining up to date security standards along with more frequent security audits. Network segmentation will be implemented to further isolate these incidents in the future and stop any other potential attacks from totally stopping all operations. Upper management has been contacted about this event and in case of any serious data breaches will go on to contact customers and law enforcement.
Recover	To recover from this DDoS attack we first restore and critical network services back online to begin going back to normal business operations. Once this is done all non-critical network services will be restored. In the future an ICMP flood attack should be blocked by the newly configured firewall and IDS/IPS filter.

Reflections/Notes: