Nicolas Shinozaki, 1

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 company experienced a DDoS attack using a flood of ICMP packets, causing all network services to stop responding. The cybersecurity team mitigated the attack by blocking the malicious traffic and shutting down non-critical services to prioritize restoring critical network functions.
Identify	The attack targeted the company's internal network with an ICMP flood. All critical resources were affected and needed to be secured and restored.
Protect	To prevent future incidents: • The team implemented a firewall rule to limit incoming ICMP packet rates. • An IDS/IPS system was added to filter ICMP traffic with suspicious characteristics.
Detect	To improve detection: • Source IP verification was configured on the firewall to identify spoofed IP addresses. • Network monitoring software was deployed to detect abnormal traffic patterns.
Respond	For future events:

	• Affected systems will be isolated to minimize disruption. • Critical systems and services will be restored first. • Network logs will be analyzed for suspicious activity. • All incidents will be reported to upper management and legal authorities if required.
Recover	To recover from ICMP flood attacks: • Restore critical network services first while blocking external ICMP flood traffic at the firewall. • Halt non-critical services to reduce internal network strain. • Once the attack subsides, gradually bring non-critical systems back online.

Reflections/Notes: