Incident Report Analysis

Wrote a summary regarding a mock DDoS attack on an internal network using the NIST framework.

Summary	A multimedia company experienced a DDoS attack which compromised the internal network for two hours until it was resolved. The network services stopped responding due to the incoming flood of ICMP packets. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. After investigating, the Security Analyst team found that this attack happened through an unconfigured firewall.
Identify	The incident management team conducted audits of the internal network, devices, and access privileges to identify potential gaps in security. The malicious actor overwhelmed the organization's network by flooding the system by sending ICMP pings through an unconfigured firewall. This action resulted in a Distributed Denial of Service attack throughout the internal network.
Protect	The organization aims to protect itself from future attacks by implementing a new firewall rule to limit the rate of incoming ICMP packets. We will have source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets. We will also train employees to configure firewalls more frequently. Lastly, we will create an IPS (Intrusion Prevention System) system to filter out some ICMP traffic based on suspicious characteristics.
Detect	The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal traffic patterns.
Respond	The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical

	network services. We will also provide protected passwords to our firewall system and limit the number of employees who will have access to it. We also will implement a SIEM tool to report any suspicious activity in real time so we can prevent attacks occurring anywhere in our system. This way we can further monitor the IP addresses and firewalls. *For future security events, the cybersecurity team will isolate affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.*
Recover	*To recover from a DDoS attack by ICMP flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online.*

Reflections/Notes: