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 multimedia was going through a regular day when they experienced a DDOS attack that compromised the internal network for over two hours until the situation was resolved. Their network services stop responding entirely because of an influx of ICMP Packets. The team then responded with blocking the DDOS attack and stopping all unnecessary network services till all network services have been fixed and restored.
Identify	Network services were down for over two hours due to the influx of ICMP packets, which is an ICMP flood attack. Had to shutdown all non-critical network services because the entire internal network was affected. Therefore, all of these critical network resources need to be safely secured, and be restored to a functioning state
Protect	The cybersecurity team needs to start implementing protection to these network services. They do this by implementing: - A new firewall rule to help against ICMP flood attacks - A IDS/IPS system to detect and prevent any possible suspicious traffic
Detect	The cybersecurity team configured a firewall that looks at source IP address to check for spoofed IP addresses on incoming ICMP packets and a network monitoring software to detect abnormal traffic patterns

Respond	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: N/A