Incident report analysis

Name: Brian Trujillo

Summary	A DDoS attack was launched against the company's network using a flood of ICMP packets which compromised network services for two hours. The attack exploited a firewall configuration vulnerability.
Identify	The security team identified the root cause of the incident as a flood of ICMP packets coming through an unconfigured firewall, indicating a lack of proper security measures for network traffic control.
Protect	To protect against similar incidents in the future, the following measures were implemented: A new firewall rule to limit the rate of incoming ICMP packets. Source IP address verification to prevent spoofed IP packets. Installation of network monitoring software to observe traffic patterns.
Detect	Network monitoring software and an IDS/IPS system were deployed to detect abnormal traffic patterns and filter out suspicious ICMP traffic, enhancing the organization's capability to recognize potential threats.
Respond	The incident management team's response involved: Blocking incoming ICMP packets. Taking non-critical network services offline. Restoring critical network services to operational status.
Recover	Implementing security measures to mitigate the effects of the DDoS attack. Conducting a post-incident review to improve incident response strategies and recovery plans.

Reflections/Notes: This incident highlighted the importance of having a configured and updated firewall to prevent unauthorized access and potential attacks. The response and recovery process showed effective teamwork and quick decision-making. Moving forward, regular security audits and training on incident response will be vital to maintaining network integrity and resilience. Implementing the NIST framework can help structure the approach to cybersecurity in the organization.