Incident Report Analysis

Summary	At approximately 10am this morning, our IT department reported network service outages. The team promptly responded by mitigating the issue through the implementation of an effective solution: blocking all incoming ICMP traffic on the network. As a result, there was a total of 2 hours of downtime before complete restoration of network services.
Identify	In this scenario, the attackers exploited an unconfigured firewall, leading to a typical DDoS attack where the internal network was flooded with ICMP spoofed packets.
Protect	By deploying a firewall, incoming ICMP packets can be restricted, while incorporating source IP address authentication to identify and prevent spoofed connections. Augmenting the network monitoring software enables the detection of anomalous traffic patterns, while an IDS/IPS system can effectively filter ICMP traffic based on suspicious attributes.
Detect	To enhance detection capabilities, it is imperative to thoroughly analyze all potential entry points into the network. Maintaining up-to-date logs and conducting regular audits of authorized users' computer IDs and IPs play a crucial role in mitigating the risk of unauthorized access from unfamiliar sources.
Respond	Automated and human alerts should be treated with utmost seriousness and subjected to thorough review. The implementation of IDS/IPS tools enables automation of certain tasks, significantly reducing the risk of widespread company outages. However, active review of logs remains crucial as it allows for the prompt identification and isolation of unauthorized users or systems from the network, while safeguarding network resources. It is essential to

	maintain disciplined procedures consistently and in a timely manner, starting from the initial alert through remediation, reporting, and recovery, to uphold the desired security posture. Utilizing logs, the IDS interface, and a SIEM solution provides a comprehensive overview and empowers control over network activities.
Recover	The primary objective is to minimize downtime while upholding the CIA triad (confidentiality, integrity, and availability). Strict procedures should be implemented for recovery processes, including backups stored on local servers and appropriate handling of physical hardware. Maintaining the chain of custody for all evidence, both physical and digital, is essential to aid investigations. It is vital to preserve critical services to ensure business continuity, and resorting to service shutdown should be a last resort. Instead, emphasis should be placed on the prevention and remediation techniques discussed earlier.

Reflections/Notes: