Multimedia Company DDoS Attack: Incident Report Analysis

Summary	Earlier this week, various staff members reported a sudden halt in the responsiveness of the organization's network services. Subsequent investigation revealed a disruption caused by an influx of ICMP packets, indicative of a Distributed Denial of Service Attack (DDoS). The origin of these requests was traced to multiple sources, orchestrating an ICMP flood that penetrated an inadequately configured firewall. Consequently, the normal flow of internal network traffic was obstructed, impeding access to essential network resources.
Identify	The incident management team conducted a comprehensive audit of the network devices, firewalls, and access policies implicated in the attack to pinpoint security vulnerabilities. During the examination, the team uncovered that one of the organization's firewalls was inadequately configured, lacking both port blocking and IP rules. This configuration lapse led to a downtime of 2 hours, during which there was a complete cessation of business operations and revenue-generating services. Additionally, as part of the identification process, all data stored within the network must undergo a comparison with backups to detect any potential instances of damaged or pilfered data.
Protect	In response to the incident, the team has executed a series of proactive measures to enhance network security. A new firewall rule has been introduced to restrict the rate of incoming ICMP packets, bolstered by source IP address verification for firewalls. Furthermore, the implementation includes the deployment of network monitoring software to detect and address abnormal traffic patterns. To fortify the defense against potential threats, an Intrusion Detection/Prevention System (IDS/IPS) has been installed to filter out any suspicious network activity. As part of ongoing efforts, the team is set to establish new baseline configurations for all firewalls, ensuring that each

	adheres to a secure standard.
Detect	To identify potential threats and anomalies with the potential to evolve into attacks, the team will employ firewall logging tools and an Intrusion Detection System (IDS). This comprehensive monitoring approach involves scrutinizing all incoming network traffic originating from IP addresses outside the internal network. Additionally, the team is contemplating a potential transition to a Next Generation Firewall (NGFW) based on the perceived benefits, especially in terms of enhanced features such as intrusion protection.
Respond	The team has reconfigured firewall and security rules to recognize ICMP floods and similar request flood attacks. The targeted firewall has been reconfigured with strong security rules to match that of the baseline configuration. All security employees have been notified of the cause, response, and results of the attack. We have informed upper management of this event and they will work with content teams to notify customers about the outage. Management will also need to inform law enforcement and other organizations as required by local laws.
Recover	The affected server has been reset back to the baseline configuration and is fully functioning. All data or assets related to the server have been confirmed to be reverted to their most recent backups, which should be from the previous night. For future attacks like this, external ICMP requests need to be blocked at the firewall level after confirmation of an ongoing flood. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, critical network services should be restored first. Finally, when the attack has been resolved, security team members can begin restoring non-critical services, restoring damaged systems, and communicating to organization leadership.