Multimedia Company DDoS Attack: Incident Report Analysis

Summary	Earlier this week, several employees reported a sudden halt in the organization's network services. Investigation revealed that the network was inundated with ICMP packets, indicative of a Distributed Denial of Service Attack (DDoS). The flood overwhelmed the network due to an unconfigured firewall, rendering normal internal network traffic inaccessible.
Identify	The incident management team conducted audits on network devices, firewalls, and access policies to pinpoint security vulnerabilities. They discovered an unconfigured firewall lacking port blocking or IP rules. This outage led to a complete halt in business operations and revenue-generating services for a total of 2 hours. Data integrity checks against backups are underway to assess any potential damage or data theft.
Protect	In response, the team implemented new firewall rules to restrict incoming ICMP packet rates, enforced source IP address verification for firewalls, deployed network monitoring software to detect abnormal traffic patterns, and installed an Intrusion Detection/Prevention System (IDS/IPS) to filter suspicious network activity. Additionally, they are defining new baseline configurations for all firewalls to ensure adherence to secure standards.
Detect	To identify similar attacks and potential precursors, the team will utilize firewall logging tools and an IDS to monitor incoming network traffic from external IP addresses. Consideration is also given to transitioning to a Next Generation Firewall (NGFW) based on the organizational benefit from its advanced features like intrusion protection.

Respond	The team reconfigured firewall and security rules to effectively mitigate ICMP floods and similar request flood attacks. The targeted firewall now boasts robust security rules aligned with the baseline configuration. All security personnel have been briefed on the incident's cause, response, and outcomes. Upper management is informed, and steps are taken to notify customers about the outage. Legal obligations necessitate communication with law enforcement and relevant entities as per local regulations.
Recover	The affected server has been restored to its baseline configuration and is fully operational. Data and assets associated with the server have been reverted to the most recent backups, typically from the previous night. To fortify against future attacks, external ICMP requests are blocked at the firewall level upon confirmation of an ongoing flood. Non-critical network services are temporarily halted to mitigate internal network congestion. Critical network services are prioritized for restoration, followed by non-critical services and damaged systems. Communication with organizational leadership is essential throughout the recovery process.

Reflections/Notes:

This incident underscores the critical importance of proactive security measures and continual vigilance in safeguarding our network infrastructure. The discovery of an unconfigured firewall highlighted a significant gap in our defenses, emphasizing the need for regular audits and updates to security policies.

Moving forward, it's evident that robust firewall rules, along with stringent password policies and multi-factor authentication, are imperative to prevent similar incidents. Additionally, implementing advanced monitoring tools and intrusion detection systems will enable us to swiftly detect and respond to anomalous network activities.

Communication proved to be key during the incident response process, from promptly notifying security personnel to liaising with upper management and legal authorities. Going forward, ensuring clear lines of communication and establishing predefined protocols for incident response will be paramount.