**Multimedia Company Incident report analysis**

| **Summary** | For two hours a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses recently experienced a DDoS attack, which compromised the internal network until it was resolved.  During the attack, the organization’s network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. |
| --- | --- |
| Identify | A malicious actor had sent a flood of ICMP pings into the company’s network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack. |
| Protect | The network security team implemented the following to protect the network system of the organization:  1. A new firewall rule to limit the rate of incoming ICMP packets.  2. An IDS/IPS system to prevent out some ICMP traffic based on suspicious characteristics. |
| Detect | To detect new unauthorized access attacks in the future, the team will use a source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and network monitoring software to detect abnormal traffic patterns. |
| Respond | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. 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 | The organization will recover as the organization’s network services will start responding correctly due to an incoming filtered of ICMP packets. Normal internal network traffic will be able to access any network resources. 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: Firewall rules should be maintained at all time. |
| --- |