**Incident report analysis**

**You are a cybersecurity analyst working for a multimedia company that offers web design services, graphic design, and social media marketing solutions to small businesses. Your organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved.**

**During the attack, your 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.**

**The company’s cybersecurity team then investigated the security event. They found that 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.**

**To address this security event, the network security team implemented:**

* **A new firewall rule to limit the rate of incoming ICMP packets**
* **Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets**
* **Network monitoring software to detect abnormal traffic patterns**
* **An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

| **Summary** | A multimedia company has experienced a DDoS attack which compromised the internal network for 2hrs. Until it was resolved. During the attack, your 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 | The network service of the organization was attacked by the malicious actor due to an unconfigured firewall in network security system. | | |
| Protect | The has implemented new security event :  A new firewall rule to limit the rate of incoming ICMP packets,  Source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets,  Network monitoring software to detect abnormal traffic patterns,  An IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics | | |
| Detect | To detect new network attacks in the future, the team will use a firewall logging tool and an intrusion detection system (IDS) to monitor all incoming traffic from the internet. | | |
| Respond | The firewall and network monitoring system has improved in stronger way to prevent further attack. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. | | |
| Recover | Not all the data were lost so the recovery was good. | | |

| Reflections/Notes: |
| --- |