**Incident report analysis**

**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.

**Review the scenario below. Then complete the step-by-step instructions.**

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

|  |  |
| --- | --- |
| **Summary** | The company was the victim of a distributed denial of services (DDoS) caused by an overload of ICMP packets which resulted in all network services going down. In response, the security team strengthened their firewall and network monitoring, especially in regards to ICMP packets. |
| Identify | The company was the target of a DDoS attack that used ICMP packets to overwhelm the network. All network services went down. |
| Protect | The firewall was changed to add a rule that limits the rate of incoming ICMP packets. Also, and IDS/IPS system was installed to filter out suspicious packets. |
| Detect | The firewall was changed to verify the source IP address of every incoming ICMP packet, along with other network monitoring software. |
| Respond | The security team responded by blocking all incoming ICMP packets and shutting down every non-critical network service. |
| Recover | After taking the steps under “Respond,” the team was able to restore all systems. |