**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.

| **Summary** | Xyz Multimedia Company that provides web Design, Graphic Design and Social Media Marketing Services to small Businesses had an DDoS Attack , the threat actor used Distributed Networks to flood the organisation’s system with overwhelming ICMP packets , affecting all the internal and critical Network activity of the organisation. Thus Stopping all of the network activity for 2+ hours and unable to access any network resources through internal Network | | |
| --- | --- | --- | --- |
| Identify | The CS team has identified via internal network that a Malicious actor was flooding the Network with ICMP packets through an unconfigured Firewall .This vulnerability allowed the malicious attacker to overwhelm the company’s network through a distributed denial of service (DDoS) attack.  This attack Affected all of the Internal Network Devices from accessing any Network resource | | |
| Protect | The CS team has implemented   * New Rule Configuration for the Firewall to limit the [no.of](http://no.of) ICMP Packets coming into the network * Source IP Address Verification is configured into the Firewall to avoid/ check IP spoofing * Network Monitoring Software to Detect abnormal Network patterns * IDS/IPS system installed to filter out some ICMP traffic based on suspicious patterns | | |
| Detect | To Detect Future Threats , IDS/IPS System and Network Monitoring Software will detect for known and unknown DDoS attacks | | |
| Respond | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. | | |
| Recover | Respond activity has restored the system , in future these steps needs to be followed if Detection fails for unknown reason | | |

| Reflections/Notes: |
| --- |