**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** | It has been reported that the network services have suddenly stopped responding at this time. Due to this, an ICMP Ping of death DDoS attack has been identified. After recovery of systems crashing, new implementations of Firewall rules as well as network traffic sniffers for multiple layers has been added along with checking for IP Spoofing. |
| Identify | The Incident management team has been alerted through a downed network, investigated and determined that incoming ICMP Packets have caused a possible DDoS attack due to high amounts of flooding ICMP Pings into the Server. |
| Protect | Incident management has determined that a new firewall rule be enabled to limit the incoming ICMP packets. Also Source IP address Verification is being enabled to check for Spoofed IP Addresses, and Network Monitoring Software to detect Abnormal Patterns in traffic. Finally, an IDS/IPS system is being brought online to filter out some ICMP traffic based on suspicious characteristics. |
| Detect | From the scan of the system after determining the issue cause of the problem, the Incident management team determined that a malicious actor sent a flood of ICMP pings through the unconfigured firewall of the system. Detection of the issue can be seen through the IDS/IPS implementation along with new IP Address verification and even Network Monitoring Software to detect abnormal patterns in the Server. |
| Respond | Immediate response has been to restore services and to filter all responses of the server. On top of that, the security process has been increased and locked down for the situation at this time. New measures for detection has been implemented for use within the system and will assist in response for future attempts. |
| Recover | Recovery of the system was completed by the Incident management team blocking incoming ICMP packets, and completing a process of stopping all non-critical network services offline, and restoring all critical network services that have been harmed through this incident. |

|  |
| --- |
| Reflections/Notes: |