**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** | Business experienced internal network downtime due to an malicious attacker overwhelming the company’s network through a distributed denial of service (DDoS) attack. This happened due to an internal firewall on the network which had been left unconfigured resulting in normal internal traffic not being able to access any network resources for two hours. | | |
| --- | --- | --- | --- |
| Identify | The Incident management team had audited the network the systems, devices, and access policies involved in the attack to identify the gaps in security. The team analyzed TCP/HTTP logs and were able to see a high amount of ICMP pings. Upon initial review, it appears due to an unconfigured firewall the malicious actor was able to flood the network with ICMP pings, resulting in downtime to the network. | | |
| Protect | The Team has now implemented a new firewall to limit the rate of incoming ICMP packets and source IP address verification on firewall to check for spoofed IP addresses on incoming ICMP packets. Additionally, have invested in an intrusion prevention system (IPS) to filter out some ICMP traffic based on suspicious characteristics. | | |
| Detect | To detect possible DDoS attacks in 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 incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. We informed upper management of this event and appropriate legal  authorities, if applicable. Measures to be put in place to prevent future attacks and analyze network logs to check for suspicious and abnormal activity. | | |
| Recover | The team have restored and secured any affected systems to normal operation that have been affected by an incident. Firstly 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: Importance of regular Firewall maintenance - entails checking and updating security configurations regularly to stay ahead of potential threats. |
| --- |