**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** | The organization experienced a security attack event in which all network services suddenly stopped responding. The cybersecurity team found it was caused by a distributed denial of services (DDoS) attack through a flood of incoming ICMP packets. The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored. | | |
| --- | --- | --- | --- |
| Identify | The entire internal network was affected by the attack. All critical network resources needed to be secured and restored to a functioning state. The Normal internal network traffic could not access any network resources. The team found that the cause of this attack was due to an unconfigured firewall rule, which the malicious actor took advantage of to launch a DDoS attack. | | |
| Protect | The team has implemented a Firewall Maintenance, updating the rules set on the firewall to prevent potential threats similar to this one. Having Network Log Analysis, which will help detect any abnormalities in the network, and notify the analysts before it is too late, as the consequences of this attack resulted in the denial of service for two hours. The Network Log can be configured to alert the security team when there is abnormal traffic on the network. | | |
| Detect | To detect irregularities on the network traffic in the future, the team will use a  firewall logging tool and the mentioned Network Log Analysis to monitor all  incoming traffic from the internet. In addition to this, IP address verification to detect spoofing IP on incoming packages was implemented by the team. | | |
| Respond | The team will isolate network sections and systems to prevent disruption of the network and not resort to shutting down the entire network. They will also attempt to restore data lost during the attack. The team will report this incident to upper management, and legal authorities if applicable. | | |
| Recover | To recover from a DDoS attack by ICMP flooding, access to network services  need to be restored to a normal functioning state. In the future, external ICMP  flood attacks can be blocked at the firewall. The team added new Firewall rules and configurations to deal with attacks similar to this incident and, with the help of the new logs from the Network Analysers, identify and respond by blocking any incoming ICMP packets, once an irregularity on incoming packets has been detected in the network. Then, all non-critical network services should be stopped to reduce internal network traffic. Next, 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: |
| --- |