**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** | Today we experienced a DDOS attack, which compromised the internal network for two hours until it was resolved. During the attack our network services completely stopped. While going through the logs and performing analysis we found out that the malicious actor flooded our network service system with ICMP packets which led to the sudden stoppage or access to the systems. The team responded by blocking the attack and stopping all non-critical network services, so that the critical network services could be restored. | | |
| --- | --- | --- | --- |
| Identify | The incident management team audited the systems, devices, and access  policies involved in the attack to identify the gaps in security. The team found out that the threat actor flooded the network systems with lots of ICMP packets that led to distributed denial of service attack (DDOS). Visitors of the website that are mainly the clients were affected with this attack. | | |
| Protect | The team has implemented new firewall rules to limit the rate of incoming ICMP packets and IPS to filter out some ICMP traffic based on suspicion charachterstics. | | |
| Detect | The team has implemented source IP address verification on the firewall to check for spoofed IP addresses in incoming ICMP packets, network monitoring software to detect abnormal traffic patterns and IDS to filter out some ICMP traffic based on suspicion characteristics. | | |
| Respond | For future security events like DDoS attacks the incident management team will isolate the affected systems to prevent any further disruption to the network, later it will respond by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical network services. The team will also report all incidents to upper management and appropriate legal authorities, if applicable. | | |
| Recover | To recover from ICMP flooding which led to DDOS attack, the team should restore network services to a normal functioning state. In future, external ICMP flood attacks can be blocked at firewall. Then, all non critical network services will be shut down to reduce the internal network traffic. Next, critical network services should be restored first. Finally once the ICMP flood attack is timed out, all non critical network services should be restored and brought back online. | | |

| Reflections/Notes: |
| --- |