**Incident report analysis**

**Instructions**

As you continue through this course, you may use this template to record your findings after completing an activity or just to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to continue practicing applying the NIST CSF framework to different situations you may encounter.

|  |  |
| --- | --- |
| **Summary** | The organization recently experienced a DDoS attack, which compromised the internal network for two hours until it was resolved. The normal internal network could not access any network resources. The cybersecurity team found the disruption was caused by a DDoS attack through a flood of 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 | A malicious actor or actors targeted the company with an ICMP flood attack. The entire internal network was affected. All critical network resources needed to be secured and restored |
| Protect | Based on the scenario, the following systems or procedures can be updated or changed to further secure the organization's assets:   * Configuration of Firewalls: The firewall configuration can be reviewed and updated to block all incoming ICMP packets and prevent the possibility of DDoS attacks in the future. Also, the firewall can be configured to check for spoofed IP addresses on incoming ICMP packets, which will help mitigate the possibility of malicious traffic. * Regular Audits: Regular audits of internal networks, systems, devices, and access privileges can be conducted to identify potential gaps in security and address them before they are exploited. |
| Detect | The cybersecurity team has enabled source IP address verification on the firewall in order to examine incoming ICMP packets for any signs of spoofed IP addresses. Additionally, they have deployed network monitoring software to effectively identify and flag any irregular traffic patterns.. |
| Respond | To ensure enhanced security measures in future events, the cybersecurity team will take proactive steps by isolating affected systems to mitigate further disruptions to the network. They will diligently work on restoring any critical systems and services that were impacted during the event. Subsequently, the team will conduct a comprehensive analysis of network logs to identify any suspicious or abnormal activities. Additionally, all incidents will be promptly reported to upper management and, if necessary, the relevant legal authorities will be informed accordingly. |
| Recover | It is crucial to restore access to network services and bring them back to a normal functioning state. In order to prevent future occurrences of external ICMP flood attacks, the firewall can be configured to block such malicious traffic. A recommended course of action involves temporarily halting non-critical network services to minimize internal network congestion. Priority should also be given to restoring critical network services promptly. Finally, once the influx of ICMP packets has timed out, it is safe to bring all non-critical network systems and services back online. |