**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, our organization was the victim of a Distributed Denial of Service (DDoS) attack. During the attack, all network services were halted due to an incoming flood of ICMP packets through an unconfigured firewall. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, all non-critical network services offline, and restoring crucial network services. |
| Identify | The unconfigured firewall is a security risk. There was no established rate limit to incoming ICMP packets, and this vulnerability was exploited by the threat actor. There were also insufficient monitoring controls to check for spoofed IP addresses on incoming ICMP packets. The attack impacted the entire network, and all critical network resources needed to be secured and restored to a functioning state. |
| Protect | The security team has implemented a new firewall rule to limit the rate of incoming ICMP packets and prevent future ICMP flood attacks, as well as an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to filter out future ICMP traffic based on suspicious characteristics, including those found in this DDoS attack. |
| Detect | The team has also implemented source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets in an effort to prevent a malicious actor from gaining access to the network . In addition, the security team has installed network monitoring software to detect future abnormal traffic patterns, |
| Respond | For future security events, the cybersecurity team will isolate the affected systems to prevent further disruption to the network. They will attempt to restore any critical systems and services that were disrupted by the event. Upper management will be notified, as will the appropriate 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. The firewall can block future ICMP attacks (and other types of attacks). Then, all non-critical network services should be stopped to reduce internal network traffic.  Critical network services will be prioritized and restored first. Once the flood of ICMP packets have been resolved, all non-critical network systems and services can be brought back online. |

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