**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 encountered a Distributed Denial of Service (DDoS) attack that disrupted network services for a duration of two hours. The attack involved a flood of ICMP (Internet Control Message Protocol) packets, overwhelming the internal network and rendering normal operations inaccessible. This attack exploited an unconfigured firewall vulnerability, allowing the malicious actor to flood the network.The incident management team swiftly responded by blocking incoming ICMP packets, taking non-critical network services offline temporarily, and restoring critical network services. Subsequently, the cybersecurity team investigated and implemented several measures. | | |
| --- | --- | --- | --- |
| Identify | During the investigation following the DDoS attack, the incident management team audited various systems, devices, and access policies involved in the incident. It was uncovered that a malicious actor gained access to the network through an unconfigured firewall.The uncovered vulnerabilities were the lack of proper firewall configuration and insufficient monitoring of abnormal traffic patterns. | | |
| Protect | To protect the organisation from future breaches the team has implemented new policies in compliance with the NIST framework that include:  A new firewall rule limiting incoming ICMP packets' rate and source IP address verification to prevent spoofed addresses.  Implementation of policies and employee training on safeguarding network configurations and recognizing suspicious traffic. | | |
| Detect | To be able to detect potential future breaches, the security team suggests introduction of network monitoring software to detect abnormal traffic patterns and an IDS/IPS system to filter suspicious ICMP traffic. | | |
| Respond | The immediate actions of the team were to promptly respond by blocking incoming ICMP packets, temporarily stopping non-critical network services, and restoring critical services The team also conducted a comprehensive investigation to identify the attack's source and nature, leading to the implementation of new security measures. | | |
| Recover | In efforts to recover affected systems involved the restoration of the network through backups and informed staff about potential data loss after the last backup. | | |

| Reflections/Notes  Based on the NIST Framework recommendations are as follows:  Conduct regular audits to identify vulnerabilities and gaps in network security, ensuring consistent monitoring for abnormal traffic patterns.  Strengthen firewall configurations continuously and implement additional security protocols to prevent similar attacks.  Enhance incident response procedures, including predefined actions for different types of attacks, ensuring a swift and effective response.  Regularly back up critical systems and data, ensuring backup reliability, and developing efficient recovery plans to minimize downtime. |
| --- |