**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** | This morning, the organization was unable to access the internal network. The IT team was tasked with analyzing and inspecting this issue. The team took action and used the necessary tools to investigate what was compromised. After careful inspection, the team found out that the network was compromised by DDos attack which was interfering with the internal service. This attack is referred to as flooding the server or the network from many computers and its main goal is to stop or shut down the service.The attack was used by sending a flood of ICMP pings requests into the company’s network causing it to overwhelm the system. This action was taken to try to stop the service since a correct firewall was not configured properly. Our team, established the service by stopping the attack and bringing back the internal service back to normal operations. | | |
| --- | --- | --- | --- |
| Identify | The incident response team used the appropriate tools to inspect and analyze the situation and the issue involved in this attack. The team identified misconfiguration in the network as unconfigured firewalls were not set up correctly. This inconvenience made a vulnerability for the attacker to get it since the firewall did not properly restrict unauthorized access or validate trusted traffic for the allowed users. Also, they found a huge amount of ICMP requests to the server which was causing the internal network to be overwhelmed and slow. This was the reason why the internal network shut down for two hours. The team identified this attack as DDos attack which was used from many devices flooding with many ICMP requests to the server. The root cause was traced to the lack of proper firewall rules and monitor mechanisms for detecting abnormal traffic patterns. | | |
| Protect | The response team has implemented a firewall rule to limit the rate of incoming ICMP packets, preventing traffic overload. This ensures that only valid packets are granted access. In addition to that, IP verification was added to the firewall rule to check for spoofed IP addresses on incoming ICMP packets. This action ensures that only authorized valid IP addresses are allowed to enter or exit the network. | | |
| Detect | To detect new unauthorized access attacks in the future, the team will use a network monitoring system to detect abnormal traffic patterns such as an IDS. This will alert the team to any inconsistencies in the network. This tool will analyze, filter out ICMP traffic while setting up alarms to notify the team for anomalies. | | |
| Respond | The response team will use an IPS to monitor, analyze and take action such as blocking ICMP traffic, based on suspicious activity. It is important to train the company and employees on how to secure their organization. Awareness training is essential for the company to understand that proper firewall configuration can help to prevent any type of DDoS attack. While it may not stop it completely, it could prevent future ones. | | |
| Recover | The team restored the system back after two hours of being compromised by the attack. The information about this attack will be shared with superiors and recommendations will be provided to the organization. This issue could have been prevented if the firewalls had been configured correctly. Customers can now visit their favorite website again. | | |

| Reflections/Notes: |
| --- |