**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** | Reports from multiple employees stated that the organization’s network services had suddenly stopped responding. It was then discovered that the network had been disrupted by a flood of ICMP packets. The requests were originating from multiple sources, resulting in a Distributed Denial of Service Attack (DDoS) that created an ICMP flood through an unconfigured firewall. All normal internal network traffic was unable to access any network resources due to the network being overwhelmed with ICMP requests | | |
| --- | --- | --- | --- |
| Identify | The incident management team audited the network firewalls, access points, and devices to identify potential vulnerabilities in the security. They found that a firewall was left unconfigured and did not posses any port blocking or IP rules. The outage caused approximately a 2 hour downtime on the network. Any sensitive data needs to be compared to backups that the organization has to confirm if data has been stolen or damaged. | | |
| Protect | The firewall has been properly configured to limit the rate of ICMP packets. Other preventative security measures have been implemented such as network monitoring software for abnormal traffic patterns, and an Intrusion Detection/Prevention System (IDS/IPS) system to filter suspicious network activity. Lastly, the standard baseline for firewall configurations will be ensured in the future as to prevent ICMP packet flooding. | | |
| Detect | The use of firewall logging tools will be put into place so that network anomalies can be viewed and dealt with if they seem suspicious. Furthermore, an IDS will monitor all incoming traffic from IP addresses not within the network. Consideration for a Next Generation Firewall will be made depending on how much the organization can benefit from its features. | | |
| Respond | The firewall has be reconfigured to recongnize ICMP packet floods and similar request flood attacks. The targeted firewall was reconfigured with stronger security rules as well. All security personnel have been notified of the cause, response, and results of the incident. Upper management has also been informed of the attack. Management will also need to inform any law enforcement organizations in compliance with federal and local laws. | | |
| Recover | The targeted server has been reset back to its original configuration and is made sure to be functioning like normal. All data related to the server has been rolled back to the most up to date backups to ensure nothing was stolen or damaged. | | |

| Reflections/Notes: |
| --- |