**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** | While working for my organization, we experienced a DDOS attack, which compromised the internal network for two hours until it was resolved. Our network services suddenly stopped working due to an ICMP flood attack. Our incident management team responded by blocking incoming ICMP packets, stopping offline services and restoring online services for normal use. Our cybersecurity team investigated the event and found that a malicious actor sent a flood of ICMP pings to the network through an unconfigured firewall. Misconfigured firewalls are a huge red flag for vulnerabilities which can jeopardize the security of the network. |
| Identify | ICMP flood attack occurred where the network was flooded with ICMP packets |
| Protect | * **To further secure the organizations network operations, a nightly TCPDUMP should be implemented so that each night the network is refreshed and updated securely for the next days operations. The TCPDUMP will capture and view network communications and collect statistics about the network. It will also establish a baseline for the network traffic patterns and network utilization metrics, it will detect and identify malicious traffic and create customized alerts to send the right notifications when network issues or security threats arise. Lastly, the TCPDUMP will locate unauthorized IM, traffic, or wireless access points.** * **When systems refresh themselves at midnight while the organization is closed, morning patch updates should take place which will ensure security hardening tactics to secure daily operations have taken place and systems should then be ready for normal use. These patch updates will address security vulnerabilities within our programs.** * **MFA needs to be implemented moving forward to secure the user and the network from potential vulnerabilities and security threats. MFA will require the user to verify their identity in more ways than one ensuring the correct user is using the more secure network.** |
| Detect | Implementing password policies and MFA & 2FA policies for network usage can help add additional security to the organization's network. The password updates can occur routinely once a month or when a user files a complaint about the security of their account. The MFA & 2FA policy can occur once a week to refresh the users account about verification of the user or when and if the user files a complaint about the security of their account. |
| Respond | After discussing with my cybersecurity team about how we should move forward with threats, vulnerabilities and attacks, we have concluded that the following security hardening measures will be implemented in our organization’s IT policies:   * Implementing the organization’s baseline configuration of the network will secure a documented set of specifications within a system that is used as a basis for future builds, releases and updates. * Assisting the morning patch updates, a morning penetration test should take place in the system to strengthen security operations. This penetration test will identify vulnerabilities in systems, networks, websites, applications and processes. * With the MFA & 2FA policy moving forward, the three category questions will change around to prevent consistency of the user’s answer making it a risk for a malicious actor to attempt to login to the users account. |
| Recover | After investigating the incident, we at the cybersecurity team find it vital that we implement these security hardening tools for the safety of our organization’s network and our customers' accounts immediately. With the rise of cyber attacks and threats, it is important to implement these changes immediately to also ensure our returning customers and new customers information is safe. It is our duty to ensure our customers the best experience when in the hands of our care both physically and virtually. |

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