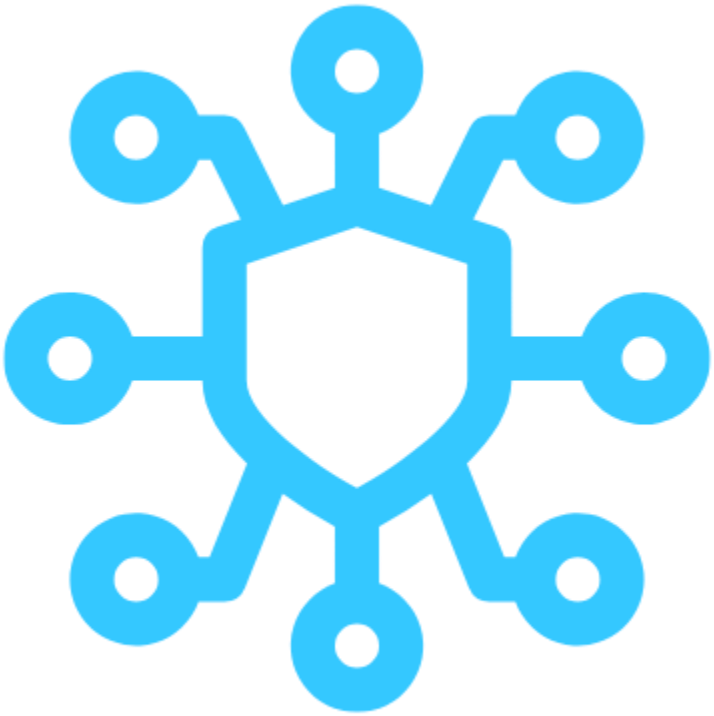
Section 2: Threat Mitigation



What Will We Do About It?

Task 1: Implement HIDS

The first security alarm about the ongoing cyberattack came from the Host-Based Intrusion Detection System is about multiple failed login attempts from a foreign IP address. Launch the host IDS and analyze the logs and events captured in the system. To verify that the IDS is up and working, try connecting to the virtual machine via SSH and notice the new login entry created in the IDS web UI. Take a snapshot of the newly created log lines and name it `succesful_ssh_logon.png`. This will ensure that the IDS system is working as expected and capturing logs in real-time. Once you have taken the snapshot, upload it to the `/starter/section_2/` directory in Github.

Task 2: Locate Suspicious IP

Once you have verified that the IDS is working fine, you are now required to collect the next indicator of compromise(IoC), which is the IP address that attempted to break into the system. This IoC will prove significant in attributing the threat actors behind the cyber attack. You were told that the initial security alarm consisted of multiple failed login attempts on the jump host server. To verify that, filter the IDS alerts to specifically look for failed logins followed by a successful one. To further disrupt the network after a successful login, the attackers execute a command to elevate their privilege to system root. Your goal is to identify that IP address which made the logon attempts and then performed privilege escalation to the 'root' user. Report the IP address in the `attacker_IP.txt` file.

Since the attack happened in the year 2020, and that's when we captured the OVA image. Make sure that you are looking for the logs during that time frame.

Task 3: IPtables Rule

Once you have identified the attacking IP address, you are now required to create an IPtables rule to make sure that any SSH connection requests from this host are blocked in the future. Hopefully, this will stop this agent from the so-called National Peace Agency from connecting again. Report your IP table rule in the `Iptable_rule.txt` that will deny SSH access to the attacking IP.

Task 4: Detect Backdoor Username, Process & Port

Once the attackers managed to break into the system, they created a backdoor username and launched a process that allows them to log in through a non-standard port number. This is a common tactic implemented by nation-state actors to ensure continuous access to the compromised system. Your goal is:

1. **Identify the rogue username:** Analyze the logs to find the rogue user added to the system. Once you have the username, you'd want to view the */var/log/auth.log* to check for the authorization events. Next, fetch all processes that are currently running for that user.

2. **Locate the malicious process:** Consider that the newly created rogue user has sufficient permissions to use the root credentials to run the backdoor process. Therefore, **you will not find a process running in the name of the rogue user.** Instead, the backdoor process will be

running as root. Analyze the currently running processes to find that suspicious process.

***Tip**: Investigate the http://localhost/ossec/ IDS logs for the bruteforce attacks.*

3. **IP address/port**: Once you have the process name with you, find the "non-standard" port it is listening on.

Both IDS logs, as well as system commands, can be used to perform this task. Report these three details, along with a justification, in the `backdoor_details.txt` file.
Delete the rogue username and kill the backdoor process to remove the persistence created by the attackers.

Task 5: Disable SSH Root Access

So far, we have figured out that the attack was carried out through brute-forcing ssh login credentials. Can you update the SSH configuration file to ensure that root login through SSH is never allowed, even if the correct set of credentials have been used? Report your changes by modifying the respective configuration entry and providing a snapshot of the change you have made. Name the file as `remote_config_change.jpg`.
***As an optional stand out task**, you can also provide a set of best practice recommendations to the senior leadership about further securing the remote login process and password management in the organization. While you appreciate the job security, you also don't appreciate the National Peace Agency making you come in on your day off. Provide your recommendation in the `additional_remote_security_recommendations.txt` file.*