Section 3: System Hardening for Enhanced Security

Time for Implementation!

Task 1: OpenVAS Scan

Now that the cyber-attack has been successfully contained, you are also tasked with further hardening the jump host server. As a first step, perform an OpenVAS vulnerability scan on the system and provide a snapshot of the vulnerabilities identified by the scan. Name the snapshot as `openvas_vulnerability_report.png`.

Task 2: Patching Apache

Once you have provided your report on the existing vulnerabilities on the system, you notice that the jump host is also running an Apache HTTP server

which can be accessed from the internet and can serve as an attack point in future incidents. To harden the Apache server, you must remove the version banner from being publicly visible. This would make it difficult for an attacker to perform reconnaissance on the server and launch attacks. Your goal is to identify and report the current Apache httpd server version and then the configuration change required to prevent the version number from being publicly accessible. Report both these details in the filename `apache_version_patching.txt`.

Task 3: De-Privilege Apache Account

As a final task of hardening the system, you want to ensure that Apache always runs as a low privileged user with restricted system access. To do that, create a new user group called “apache-group” and a new user account called `apache-user`. Can you list the configuration changes you’ll have to make sure that Apache launches with this new user account and group name? Provide your response in `apache_user_account.txt`.

Optional Stand Out Task:

The head of security for South Udan is grateful to you for your services. They want to award you with a commendation, and you are asked to prepare an “Executive Summary” of the entire investigation and changes you have made to contain the threat. This executive summary will be used to brief the head of South Udan about the incident. You can provide your summary in the form of a PDF, Word or text file, depending on whether you want to use only text or add images. Name the file as “Executive_summary” and upload it to the `section 3` directory itself.