Interview homework

SUMMARY:
Test if rule ‘sshd_set_idle_timeout’ from scap-security-guide is correctly evaluated by the openscap scanner.

OBJECTIVE:

- Read basics about how openscap [1] (scanner) and scap-security-guide [2] (security content, consumed by the openscap scanner) work. You can also look at [3] and [4].
- Figure out and design test scenarios for the ‘sshd_set_idle_timeout’ rule from the PCI-DSS security profile (see 3b. for more details about this rule).
- Implement a test script using Bash.

SCOPE:
Implementation of the test code should not take more than 4 hours (don’t over-engineer it). It is fine to submit a partial solution if it seems it would take you more time to finish the assignment completely.

ASSIGNMENT:

1. Script needs to work on Fedora 33.
    a. Prepare a machine in advance, e.g., using VirtualBox/virt-manager - download and installation takes time.
2. Script contains functions 'setup' and 'cleanup'. The first one should prepare the system for the test execution (prepare necessary files, install required packages, etc.) while the latter should undo all the changes done by the setup function and the test itself, therefore bringing the test system to the original state (i.e., the state in which the system was before running the test script).
3. Your task is to test the following functionality:
    a. `oscap xccdf eval --profile pci-dss --rule xccdf_org.ssgproject.content_rule_sshd_set_idle_timeout /usr/share/xml/scap/ssg/content/ssg-fedora-ds.xml`
    b. Note: The command from 3a. evaluates the ‘sshd_set_idle_timeout’ rule. The rule description can be found in the static guide of the PCI-DSS profile [5].
    c. Note: Due to rule dependency, the ‘ClientAliveCountMax’ option in the ‘/etc/ssh/sshd_config’ configuration file needs to be set to ‘0’ for the ‘sshd_set_idle_timeout’ rule to work properly.
4. Design test scenarios to cover positive and negative use cases when scanning the ‘sshd_set_idle_timeout’ rule from the PCI-DSS security profile. In other words, the test needs to exercise use cases where the rule is reported as fail and also use cases where it is reported as pass by the openscap scanner.
5. Each test scenario is represented by a function (choose appropriate name for the function) which will perform required configuration on the system before running the openscap scanner (command from 3a.).

a. After the test scenario is executed, a short summary with test result is printed. The summary lists a short description about test scenario and respective test result (PASS/FAIL).

HINTS:

- Consider that we will run your test script on a clean Fedora 33 installation, so make sure that ‘setup’ function installs all packages required for testing.
- The target of testing is openscap and scap-security-guide, so even though you will modify ‘/etc/ssh/sshd_config’ file your test script should not stop/restart sshd service.

REFERENCE:

- [1] https://www.open-scap.org/tools/openscap-base/
- man openscap
- [2] https://www.open-scap.org/security-policies/scap-security-guide/
- man scap-security-guide
- [3] https://www.fit.vut.cz/study/thesis-file/23098/23098.pdf (Section 2.2 presents a nice overview of all SCAP projects)
- [4] http://static.open-scap.org/openscap-1.3/oscap_user_manual.html
- [5] https://static.open-scap.org/ssg-guides/ssg-fedora-guide-index.html