Office Hours – Nessus Scanning Call Notes

The following are questions from the audiences and responses from the moderators compiled from every Nessus Compliance Scanning Office Hours Call held.

Comment: The agency asked if Safeguards will be sending out the common issues that were not part of the agenda for agencies to prep for onsite visits.

Moderator's response: Noted that they may be sent out.

Comment: The agency recently transitioned over to SecurityCenter. They have an old instance of Nessus and it is not licensed. They asked if a licensed version of Nessus is required for the audit scans.

Moderator's response: Noted that the compliance scanning can be conducted by either SC or Nessus. Advised the agency that standalone instance of Nessus can be used as well. Added that recently there have been instances of unlicensed or trial versions of Nessus being unable to conduct compliance scanning. Advised agencies to work within Tenable's User License Agreement and follow the rules of use of their software.

Comment: Agency stated that many audit files are fairly old on the website. The agency runs Windows 2016 and SQL server 2016 and Hyper-V and there are no files for these products.

Moderator's response: Noted that Safeguards has introduced new technologies into its portfolio as part of Nessus scanning. Updating the audit files is an item Safeguards is working on for the future. Noted that the team will circle back and look at updating these versions. For Hyper V, there is no CIS benchmark. Also noted that the team is being flexible when determining common security controls.

Comment: Agency noted that there are only Windows Server 2012 and old SQL files online.

Moderator's response: Noted that we may be able to send the agency the latest offline.

Comment: The agency does Nessus scans monthly. Asked whether the onsite visit will be done similarly to the Nessus compliance test. Also asked if they need to add the virtual IP as a static IP. Asked about the data center as well.

Moderator's response: Responded that the team will scan systems in scope and may need to scan at the agency and data center. Noted that if the agency has Nessus, the review team may use it (it can be fully credentialed and ready for scanning). If the data center has Nessus, the team can use theirs otherwise will use IRS-issued laptops to conduct testing. The team will require an IP address to be set aside that is whitelisted across systems determined to be in scope.

Comment: The agency inquired about using STIGs as opposed to CIS benchmarks. Asked if the review team can make a modification for STIGs.

Moderator's response: Noted that CIS is the standard and minute changes will be made as needed to match IRS requirements. Changes have not been made to accommodate STIGs in the past, and is not being considered at this point.

Comment: Agency asked what the timeline is to receive the prep materials/post review activities.

Moderator's response: Preparation document is available on the website, provided timeline/dates.

Comment: Agency asked if database scans are supported for DB2.

Moderator's response: Noted that there are audit files for DB2 for Linux, Unix and Windows. There are no audit files for Mainframe.

Comment: Agency asked if Nessus professional works for the onsite review.

Moderator's response: Agencies usually use Security Center or Tenable IO. All guidance is written around the Tenable scanner and one cannot be recommended over another.

Comment: The agency asked if everything covered for Nessus in terms of guidance will be effective starting with their next review.

Moderator's response: Noted that this is all current guidance and things are subject to change. Added that any enhancements to documentation will be uploaded to the website. Additionally, the team will continue to build out Nessus Technical Memo.

Comment: Agency asked if they should request a Conference Call through the mailbox regarding CIS vs STIGs.

Moderator's response: Advance discussions should be made through TI mailbox

Comment: The agency asked if the Nessus scans must be witnessed in person. Stated that his team members usually work remote.

Moderator's response: Having a WebEx or another form of witnessing the scans needs to be run by the review chief but it has been done.

Comment: Agency asked if Nessus scans are satisfactory in terms of replying to a CAP finding or if they should submit screenshots as evidence.

Moderator's response: As long as screenshots or reports define the settings and how it is being pushed out into the environment, they should be satisfactory as evidence.

Comment: Agency wants to know how they will know if Nessus scans are accepted as evidence to close out a finding.

Moderator's response: Noted that the CAP team looks at evidence and notes to determine if it is sufficient. Added that it is up to agency to provide Nessus scans or not, but Nessus scans are very detailed, and the CAP team can look at then in lieu of other gpresults and/or evidence.

Comment: The agency inquired about the IRS template and the possibility of an updated version of the CIS templates. Stated that they've been using Nessus Pro for many years and are facing the issue of false-positives for scans. They want to know about updated templates. They stated that NIST has updated templates and have been using those. Stated that the agency is unable to point out to the onsite reviewer that there are inconsistencies and have issues explaining this in CAPs.

Moderator's response: Mentioned we utilize the CIS benchmarks and the audit files are written by Tenable against CIS. Stated that the team is working on the audit file profile and is working to update certain audit files in the near future. The current one can be found in the SCSEMs or audit file. Onsite, the team will use whatever is available.

Comment: The agency is concerned that they work to harden their systems according to the SCSEM's, yet they are measured against something else. The scans are creating a lot of work for agencies and DES's and not adding value in terms of compliance. Asked why audit files are not written to follow the SCSEMs.

Moderator's response: Stated that Nessus will never cover a full technology and Nessus requires effective permissions to be able to read files owned by root which can be tough. The scanner uses the permissions it has.

Comment: Stated that it seemed like their scans are run correctly (permissions were elevated) yet the findings were incorrect. The experience created a lot of unnecessary work.

Moderator's response: The files were probably unreadable but normally Nessus scans provide a robust response of what is found on the system.

Comment: Stated that they do not get to mitigate false positives with technicians onsite and are left answering CAPs for months. Stated False Positives should be mitigated onsite when the scan is run.

Recommends tightening the process to be able to mitigate these false positives before they are reported because they reflect negatively on him and his staff.

Moderator's response: Stated that as soon as the scan is completed, they are available for review. After the review, a conference call can be held after the submission of a Technical Inquiry. Advised the agency to show screenshots in the CAP submissions.

Comment: Mentioned that the Windows SCSEM is not updated, and the agency fails about 30-40 items because EMET is no longer supported. This is another problem with the audit files being outdated with errors.

Moderator's response: Mentioned that the latest Nessus Preparation Package fixes this error and they may request the latest through the Safeguards mailbox.