Office Hours: June 2018

Facilitator: Corey Sinay

1. **Welcome**
   a. Introduce speaker, topic, and the purpose of Office Hours

2. **Overview of Nessus**
   a. Nessus is a security scanner utilized by Safeguards to conduct automated compliance scanning against information systems that receive, process, store, and/or transmit Federal Tax Information (FTI) during on-site reviews.

   b. It is a tool that delivers enhanced information regarding the security controls in place to protect FTI.

   c. Nessus scans are non-intrusive and have no impact on the agency's network. Safeguards compliance baselines are tailored for Publication 1075 requirements. It is a requirement that Nessus scans use the Safeguards compliance baselines.

   d. Running and / or obtaining Nessus compliance scan results is required for the onsite assessment of vendor supported Windows and UNIX operating systems, Oracle and SQL Server database management systems, Apache and IIS web servers, Cisco ASA and IOS software and VMware ESXi hypervisors.

   e. Scans are required for all locations receiving, storing, accessing and / or processing FTI. This includes, but is not limited to: agency data centers, consolidated data centers, third party vendors and county or field offices.

   f. IRS provides guidance for use of Tenable Nessus security scanner; however, agencies may use Tenable SecurityCenter or Tenable.IO to facilitate scans. Other compliance scanning tools or products cannot be used to satisfy Safeguards requirements.

      i. Discuss the difference between the 3 platforms

3. **Preparing for the Onsite Review**

   a. Preliminary Security Evaluation (PSE)

      i. Agencies will receive the Nessus preparation package through the initial PSE outreach communication.

      ii. Agencies are requested to complete the PSE form and indicate whether they have Nessus. If so, the agency should identify the Nessus POC. It is important for the Nessus POC to attend the PSE call because the Safeguards review team will provide a brief overview of Nessus scanning.

      iii. The Nessus prep package contains the most current Safeguards Nessus audit profiles and prep material.

      iv. An excel based "Listing of FTI Systems and IPs" document is included in the Nessus prep package. It is imperative for the agency to have a documented list of the FTI systems and corresponding hostnames/IP addresses prior to the review. Guidance on how to collect the required information will be discussed during the PSE call and through email coordination with assigned Safeguards team members in the weeks prior to an onsite review.

b. Nessus Preparation Call

   i. Upon finalization of the agency scope, the Nessus scope will be identified and the agency may request a Nessus Preparation Call where the review team will review each technology that will be assessed. Nessus prep calls can be held together with all applicable third parties or separately, based on the agency's preference.

c. Preparing for the Review

   i. Safeguards testing staff will work with agency staff in the months preceding the on-site review to ensure technical requirements are met prior to arriving on site.

   ii. Any third-parties or data center organizations should be fully involved at this stage of the review process and be aware of what technologies are in scope and how they will be assessed.

   iii. Proposed scope of systems and IT review schedule has been shared with all necessary security and systems personnel

   iv. Required technical settings / parameters have been configured to permit Nessus scanning per the Nessus Preparation Technical Memo

   v. For agencies using their own instance of Nessus, successful test compliance scans have been conducted against the FTI inventory of systems

d. Common Issues seen before the Review

   i. Changing settings on local machines (e.g. disable lockdown mode, enable SSH, open ports, etc.).

   ii. Registry keys and other configuration elements need to be explicitly set and configured to meet Safeguards requirements. Using defaults or unconfigured items will lead to Nessus determining a NULL result which cannot be accepted.

   iii. Ensuring credentials with the appropriate level of permissions are created and entered per the Nessus prep package guidance.

   iv. Define network location for scanning, whitelist scan engine.

   v. Taking down or whitelisting firewalls.

   vi. Ensure test scans prior to the on-site visit are successful by validating the existence of "Compliance Details" for each host. Compliance details must be gathered for Safeguards to complete the assessment.

   vii. Please do not combine technologies in the same family (e.g. - Windows 7, 8.1, 10). One scan (or more if needed) per operating system is needed to complete reporting requirements.

   viii. *Run through Nessus prep call checks e.g. For VMware, lockdown mode needs to be disabled.

4. <u>During the Onsite Review</u>

a. Agencies do not have to own Nessus. The computer security review team will use IRS Nessus laptops or leverage the agency's instance of Nessus to gain scan results.

b. IRS provides guidance for use of Tenable Nessus security scanner; however, agencies may use Tenable SecurityCenter or Tenable.IO to facilitate scans. Other compliance scanning tools or products cannot be used to satisfy Safeguards requirements.

c. All scans are expected to be completed by the first day of the onsite review, as the schedule permits.

d. Failure to assess will result in a critical finding during the on-site review.

e. Onsite Requirements

  i. Compliance scan results must be provided to the onsite review team in three formats: (i) .nessus, (ii) .csv, (iii) .html

  ii. Availability of key personnel to support troubleshooting during an onsite review (e.g., network personnel, system/database administrators, etc.).

  iii. When using an agency owned instance of Nessus:

    1. Scan accounts must be created and provided to the agency or data center POC facilitating the scans.

    2. Scans must be witnessed by an IRS Safeguards team member and be conducted during business hours.

  iv. When using an IRS owned instance of Nessus:

    1. Temporary scan accounts must be created and provided to the onsite Safeguards team.

f. Common issues seen during the on-site review

  i. Turn off host protection software.

  ii. Ensure availability of staff during scans.

  iii. Common Issues for Nessus scans:

    1. Windows

      a. Local accounts were used but the LocalAccountTokenFilterPolicy registry key was not set to ensure Local Administrator accounts can access the remote registry.

      b. Nessus results in "WARNING"

    2. Linux/Unix

      a. Proper root equivalency through elevation is not achieved.

    3. Database

      a. Oracle – Improper SID is entered.

      b. SQL Server – Instance name is incorrect. Removing instance name from scan may be required.

      c. All – Appropriate active node IP address or Virtual IP (VIP) is not provided.

    4. VMware

a. Errors in the form of NULL results are returned if Nessus is virtualized in the same instance that is being scanned.

5. Post Review Activities

a. Nessus Scan Results

i. Nessus scan results will be left with the agency or third-party during the onsite review to support immediate remediation (if/as applicable).

b. Corrective Action Plan (CAP)

i. Providing .Nessus, .csv, and .html files are sufficient to close out automated scan findings within a CAP. The agency must provide a written response in the CAP itself for the evidence to be accepted.

ii. Agencies must provide complete scan results in all three file formats (.Nessus, .csv, .html).

c. Differences between SecurityCenter and the Cloud

i. Tenable SecurityCenter and Cloud have different methods of setting up, conducting, and executing scanning. Currently, the IRS Office of Safeguards provides guidance on Tenable Nessus product scanning.

d. Tools to Prepare

i. The IRS Office of Safeguards Technical Memo, “Preparing for Nessus Compliance Scanning”, is a useful tool that may be used by agencies to prepare adequately.

ii. Safeguards scan template and audit files can be downloaded from the Safeguards website.

iii. Agencies may email the Safeguards Mailbox (safeguardreports@irs.gov) to ask a question and receive either a written response or a conference call/working session.

6. Q&A