OFFICE HOURS

TOPIC: NESSUS COMPLIANCE SCANNING

Office Hours are hosted by the Office of Safeguards as an opportunity for agencies to gain insight or additional support regarding specific topics relevant to the Safeguarding process. Office Hours serve as a forum for agencies to ask questions and interact with Subject Matter Experts.

Topic: Nessus Compliance Scanning

Date: June 2018

OVERVIEW OF NESSUS

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

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.[1]

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.

PREPARING FOR AN ONSITE REVIEW

Safeguards computer security reviewers will work with agency staff in the months preceding an onsite review to ensure technical requirements are met prior to arriving on site.

- **Pre-Review Activities:**
    - After an agency is notified of an upcoming onsite assessment, Preliminary Security Evaluation (PSE) outreach will occur which will include forms the agency must complete in preparation for the review and a Nessus prep package containing the most current Safeguards Nessus audit profiles and prep material.
    - Agencies should identify personnel to support the review. This includes, but is not limited to: security scanning technicians, network administrators, system administrators, database administrators, and desktop

[1] Additional technologies and platforms will be added as part of quarterly methodology updates based on available CIS benchmarks.

services personnel. Please note, early coordination between consolidated data center and/or contractor personnel is critical.

- 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.
- Upon finalization of an agency's IT 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.

Nessus Preparation Checklist:

- ✓ Nessus preparation package has been forwarded to security and systems personnel (this includes necessary representatives from the agency, data center, third party, etc.)
- ✓ PSE has been forwarded to system administrators, system architects, system developers, database administrators, network administrators and security scanning personnel
- ✓ Proposed scope of systems and IT review schedule has been shared with all necessary security and systems personnel
- ✓ Listing of *FTI Systems and IPs document* has been completed
- ✓ Required technical settings / parameters have been configured to permit Nessus scanning per the Nessus Preparation Technical Memo
- ✓ For agencies using their own instance of Nessus, successful test compliance scans have been conducted against the FTI inventory of systems

PARTICIPATING IN AN ONSITE REVIEW

As determined during the prep phase, the agency may elect to use their own implementation of Nessus or may choose to allow an IRS Nessus scanner (laptop machine) to scan the identified targets.

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.

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

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

- **Onsite Requirements**
  - Compliance scan results must be provided to the onsite review team in three formats: (i) .nessus, (ii) .csv, (iii) .html
  - Availability of key personnel to support troubleshooting during an onsite review (e.g., network personnel, system/database administrators, etc.).
  - When using an agency owned instance of Nessus:
    (a) Scan accounts must be created and provided to the agency or data center POC facilitating the scans.
    (b) Scans must be witnessed by an IRS Safeguards team member and be conducted during business hours.

- When using an IRS owned instance of Nessus:
    (a) Temporary scan accounts must be created and provided to the onsite Safeguards team.

POST-REVIEW ACTIVITIES

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

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.

Reference the IRS Office of Safeguards website (https://www.irs.gov/privacy-disclosure/safeguards-program) for the updates to Nessus audit profiles and testing methodology.

- **Corrective Action Plan (CAP) Reporting:**
    - 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.
    - Agencies must provide complete scan results in all three file formats (.nessus, .csv, .html).