Safeguards Technical Assistance Memorandum
Preparing for Nessus Compliance Scanning
(9/29/17)

Introduction

The IRS Safeguards Review Team will be using Tenable Nessus as the tool to conduct automated compliance scanning against our data sharing partners information systems that receive, process, store, and/or transmit FTI. Nessus will be executed on a dedicated IRS scanning laptop, and in order for the automated scan to operate properly, certain configuration requirements need to be addressed before the Review Team arrives on-site. All changes may be reverted once the safeguards review is completed.

Using the Safeguards Templates

The IRS Safeguards Review Team provides a copy of the templates we use as a skeleton for the scans we run. If you decide to import these policy templates, you will need to enter credentials and upload the appropriate audit file for the Operating System you wish to scan. Due to the templates being XML and for security reasons, when a template is exported, credentials and audit files are not included.

Virtualization and Network Preparation

Please ensure each step below is completed prior to the Review Team's arrival.

1. (If using IRS issued scanners) Set aside an IP address for the IRS Nessus scanning laptop on a subnet that can reach all applicable servers and workstations.
2. The following types of systems (if used) will need to whitelist the scanning IP address:
    a. HIPS/NIPS
    b. HIDS/NIDS
3. Ensure the IP address and physical port assigned by the Agency can communicate with the Virtual Switch (vSwitch) containing the applicable Windows server or workstation.

Note: If a virtual firewall is used, ensure communications over SMB/WMI (Ports 135, 139, 445) for Windows Systems and SSH (Port 22) for *NIX are allowed.

Note: Do not use \ in the username field of Nessus (e.g – DOMAIN\JohnDoe) in any scan. Nessus will treat this as an escape character and will not authenticate.

System Preparation

Windows 7, 8.x, 10, Windows 2008(R2), Windows 2012(R2), Windows 2016

For Windows systems, please ensure each step below is completed prior to the Review Team's arrival. For each step, see the referenced Appendix.

1. Scanning Account must be a Domain or Local Administrator. **(Appendix 1)**
2. Opening ports for Nessus to Scan. **(Appendix 2)**
3. Enabling Services required for Nessus - Services. **(Appendix 3)**
4. Enabling Services required for Nessus – Network Card. **(Appendix 4)**
5. Local Accounts - Concessions for User Account Control (UAC) **(Appendix 5)**

(*NIX) systems (Linux, Unix flavors)

NOTE: DB2 requires both an OS and Database level scan for full results.

1. Ensure the proper switch user (su) and sudo capabilities are in place (Appendix 6)

Database systems (SQL Server, DB2, Oracle)

1. Ensure the account used has SA equivalent permissions **(Appendix 7)**

Networking Devices (Cisco ASA, Cisco IOS)

1. Ensure the Cisco account used has proper permissions **(Appendix 8)**

Hypervisors (VMware ESXi)

1. Ensure the Vmware accounts to access the SOAP API are configured properly **(Appendix 9)**

Web Server

1. Web Server Requirements **(Appendix 10)**

Appendix 1: Scanning Account must be a Domain or Local Administrator

Configuring a Local Account

Nessus compliance scanning operation requires the use of an Administrator account to be able to evaluate a system configuration. It is recommended that a new test account be created with administrator privileges. If all servers and workstations are connected to the domain controller, we recommend that a domain administrator account be created for testing in order to more easily identify Nessus traffic and activities. To configure a stand-alone Windows systems with credentials to be used that is not part of a domain, simply create a unique account as an administrator. Refer to respective operating system manual for instructions on creating a local account.

Once the local account has been created, please ensure that the authentication mode for the Windows target is set to Classic:

Configuring via GPO:

1. Open “Group Policy” by clicking on “start”, click “Run”, type “gpedit.msc” and then click “OK”.
2. Select Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options.
3. From the list of policies open “Network access: Sharing and security model for local accounts”.
4. In this dialog, select “Classic – local users authenticate as themselves” and click “OK” to save this.

Configuring on Local System:

1. On the Windows Start menu, click Start -> Control Panel -> Administrative Tools -> Local Security Settings.
2. On the left side pane, expand Local Policies -> Security Options.
3. In the right pane, double-click “Network access: Sharing and security model for local accounts.”
4. Choose "Classic - local users authenticate as themselves," and click OK.

Configuring a Domain Account:

Step 1: Creating a Security Group

1. Log onto a Domain Controller, open Active Directory Users and Computers.
2. Create a security Group from Menu select Action -> New -> Group.

3. Name the group Nessus Local Access. Make sure it has a “Scope” of Global and a “Type” of Security.

4. Add the account you will use to perform Nessus Windows Authenticated Scans to the Nessus Local Access group.

Step 2: Create Group Policy

1. Open the Group Policy Management Console.
2. Right click on Group Policy Objects and select New.
3. Type the name of the policy “Nessus Scan GPO”.

Step 3: Configure the policy to add the “Nessus Local Access” group as Administrators

1. Right click “Nessus Scan GPO” Policy then select Edit.

2. Expand *Computer configuration\Policies\Windows Settings\Security Settings\Restricted Groups*.
3. In the Left pane on Restricted Groups, right click and select “Add Group”.

4. In the Add Group dialog box, select browse and type Nessus Local Access and then click “Check Names”.

5. Click OK twice to close the dialog box.

6. Click Add under “*This group is a member of:*”

7. Add the “Administrators” Group.

8. Click OK twice.

Appendix 2: Opening ports for Nessus to Scan – Windows Firewall

NOTE: Microsoft settings for Windows Firewall may vary by operating system or service pack.

NOTE: To ensure full results, a rule can be created to allow a 1:1 rule (from the Nessus scanner to the Windows Systems) on all ports for all services.

Configuring via GPO:

1. Right click “Nessus Scan GPO” Policy then select Edit.
2. Expand *Computer configuration\Policies\Windows Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Inbound Rules*
3. Right-click in the working area and choose New Rule.
4. Choose the Predefined option, and select Windows Management Instrumentation (WMI) from the drop-down list.
5. Click on Next.
6. Select the Checkboxes for:
    a. Windows Management Instrumentation (ASync-In)
    b. Windows Management Instrumentation (WMI-In)
    c. Windows Management Instrumentation (DCOM-In)
    d. File and Printer Sharing (Spooler Service - RPC-EPMAP)
7. Click on Next, Click on Finish

Configuring on Local System:

1. Navigate to the Control Panel, click Security and then click Windows Firewall.
2. Click Change Settings and then click the Exceptions tab.
3. In the Exceptions window, select the check box for Windows Management Instrumentation (WMI) to enable WMI traffic through the firewall.
    a. If there are sub-options such as (ASync-In, WMI-In, DCOM-In) – please check each item.
4. Allow File and Print Sharing (Spooler Service).

Appendix 3: Enabling Services required for Nessus - Services

Remote Registry and Windows Management Instrumentation (WMI) services must be set to automatic:

1. Navigate to the Windows Services menu by going to Start -> Run and type “services.msc”. In newer versions of Windows, type “services.msc” in the search bar inside the Start Menu.
2. Inside the Services program, navigate to Remote Registry. Right click Remote Registry and click Properties.
3. Ensure the Startup Type is set to Automatic and the service is currently “Started”.
4. Inside the Services program, navigate to Windows Management Instrumentation. Right click Windows Management Instrumentation and click Properties.
5. Ensure the Startup Type is set to Automatic and the service is currently “Started”.

Appendix 4: Enabling Services required for Nessus – Network Card

File and Print Sharing service must be active:

1. Navigate to the Windows Control Panel menu by going to Start -> Control Panel.

2. Inside the Control Panel, navigate to Network (may be called Network and Sharing Center).

3. Find the Network Interface Card (NIC) adapter that is used by the server by clicking on *Change Adapter Settings.*

4. Right Click the NIC that is used by the server and click on Properties.
   Note: If there are multiple NICs, do this step onward for each NIC.

5. Under “This connection uses the following items” window, ensure File and Print Sharing is enabled.

SOURCE: Tenable.com - Nessus Credential Checks for *NIX and Windows, November 24, 2014, Revision 38

Appendix 5: Local Accounts - Concessions for User Account Control (UAC)

Nessus uses privileged shares to login and communicate with the remote server. Depending on environmental configurations, UAC may prevent privileged functions performed over the network. If a domain administrator account is not used, the following items need to be considered:

1) If the use of a domain administrator account is possible, utilize that account for the assessment.

2) Attempt to allow local account authorization using the LocalAccountTokenFilterPolicy by editing the Registry
    a. Click Start, type regedit in the Start Search box, and then click regedit.exe in the Programs list.
    b. Locate and then click the following registry subkey: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system
    c. On the Edit menu, point to New, and then click DWORD Value.
    d. Type LocalAccountTokenFilterPolicy for the name of the DWORD, and then press ENTER.
    e. Right-click LocalAccountTokenFilterPolicy, and then click Modify.
    f. In the Value data box, type 1, and then click OK.
    g. Exit Registry Editor.

3) Enable the built-in Local Administrator account (RID 500) and change its password for use for the scan. The built-in “Administrator” account should be able to bunker bust through UAC. Note, this account may have been renamed.

4) Disable Windows UAC.
    i. Open User Account Control Settings by clicking the Start button Picture of the Start button, and then clicking Control Panel. In the search box, type uac, and then click Change User Account Control settings.
    ii. To turn off UAC, move the slider to the Never notify position, and then click OK. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
    iii. The computer will require a restart for UAC to be turned off. Notify the scanning administrator if a system reboot is not possible.

Appendix 6: Ensure Root equivalency is achieved (Nessus can read all configuration files)

Nessus uses SSH to connect to the target system to complete its credentialed scans. The user must have the ability to run any command on the system or escalate to root. On *NIX systems, this is known as “root” privileges.

By default, Nessus will use port 22 for Secure Shell connectivity. However, if you are using a non-standard port for Secure Shell, please advise the Scanning Administrator. Some environments prohibit administrative (root) logins from any network location and only allow administrative logins from the console. Nessus supports privilege elevation for environments where systems are configured with this restriction.

For AIX, scans may need to be ran as root to assess over the network. Nessus runs many checks that require access to the LSSEC command – access to this command is needed.

Nessus supports many privilege elevation methods. The options for Safeguards reviews are:

1) Sudo privilege elevation: Nessus logs into an account that has administrative sudo privileges. Using the sudo privileges, each command is prepended with the sudo command.
    a. Sudo account should be root to achieve root equivalency.

2) Su+sudo privilege elevation: combines the su and sudo functions. Nessus logs into one account, then switches to another account using su, and from that account the sudo command is issued for testing.

    a. If using su+sudo, you will need to make the following changes to the /etc/sudoers file
        i. Defaults: {NessusUserID} !requiretty
        ii. {NessusUserID} ALL=(ALL) ALL

For more information on achieving proper sudo, please visit https://www.tenable.com/blog/nessus-spotlight-susudo-feature

NOTE: The usual suspect for incomplete scans is Nessus not having access to certain configuration files within /etc/, specifically the **"The file /etc/ssh/sshd_config" could not be found”** error within the compliance output of the plugins. This file exists on most *NIX operating systems, but Nessus cannot read it. Proper root equivalency will ensure this file is read. If this file has been moved, be sure to mention it the scanning Administrator.

Appendix 7: Ensure the Database account used has SA equivalent permissions

Tenable recommends running a database compliance scan with a user having the following privileges:

- SYSDBA privileges for Oracle (**sys equivalency is needed to read the password table**)
- "sa" or an account with **sysadmin server role** for MS-SQL
- **DB2 instance user account** for DB2

These privilege levels ensure completeness of the report as some system or hidden tables and parameters can only be accessed by an account with such privileges. Note that for Oracle, in most cases a user assigned the DBA role will perform most of the checks in Tenable audits, but some checks may report errors because of insufficient access privileges. This same argument is applicable to other databases as well; a lesser privilege account could be used for database auditing but the downside is a complete report cannot be ensured. We ask for a sys equivalent account in order to read the password fields, to test for default passwords.

NOTE: DB2v10 for Windows requires PowerShell for the read-only commands to execute properly

NOTE: For Oracle databases that utilize Oracle in-flight encryption, one of the following four ciphers must be enabled while on-site in order to scan with Nessus. Not listed are variants of DES and 3DES which Nessus does not support.

SQLNET.ENCRYPTION_TYPES_SERVER = (AES256,RC4_256,AES192,AES128)

SQLNET.ENCRYPTION_TYPES_CLIENT = (AES256,RC4_256,AES192,AES128)

If the Office of Safeguards cannot perform a successful scan of a target system within the scope of the review, it will be left up to the discretion of the onsite Safeguards Review Chief to consider the system as a critical finding in the Safeguards Review Report.

Appendix 8: Ensure the Cisco ASA or IOS account has proper permissions

Tenable recommends running a Cisco Network device compliance scan with a user having the following privileges:

- SSH access with administrator equivalent access (level 15 or enable secret)

Cisco IOS compliance checks typically require the “enable” password to perform a full compliance audit of the system configuration. This is because Nessus is auditing the output of the “show config” command, available only to a privileged user. If the Nessus user being used for the audit already has “enable” privileges, the “enable” password is not required.

Nessus can run two types of scans against Cisco ASA or IOS devices:

1) **Online** – Nessus will login via SSH and query the configuration of the ASA or IOS device across the network.

2) **Offline** – Nessus can take a provided configuration file **(show running-config all)** and run the scan against the configuration uploaded to the Nessus scanner. No network traffic will be generated and the scan will be removed prior to leaving the State. To protect sensitive data, please XXXXX items such as passwords or SNMP strings when providing the configuration.

Appendix 9: Ensure the VMware account has Administrative access to the SOAP API

Tenable recommends running an ESX scan (ESXi and vCenter) compliance scan with a user having the following privileges:

- Administrative access to the ESXi Server.
- Administrative access to vCenter (if used).

Note that by default, local ESXi users are limited to “Read-only” roles. Using such an account will result in a 21745 error. Either an administrative account or one with “Global” -> “Settings” permission must be used to facilitate this audit.

Credentials for the VMware ESX SOAP API and VMware Vcenter SOAP API must be supplied when creating a new policy for a complete audit. If Vcenter is not utilized, please tell the scanning administrator, certain checks will need to be conducted by interview (manually).

NOTE: Lockdown mode must be disabled and access to the SOAP API HTTP Calls (Ports 80 and/or 443) must be allowed from/to the scanner.

NOTE: Checks for VMware have been made manual that require PowerCLI. These questions will be assessed with the Administrator and not with Nessus. PowerCLI is required for the manual assessment. Logging into the ESXi instance is required.

Appendix 10: Web Server Requirements

Web Server audit files require the same effective permissions as their host operating systems (Appendices 1-5 for Windows and Appendix 6 for *NIX). The Nessus scanner will need permissions to read the configuration files – which may be owned by the web service.