Information Security Architecture
North Richland Hills, TX 76180
www.itdiscovery.info

Nexpose Vulnerability Scanning Platform Procedure

Original Date: August 15, 2016

Purpose:

Vulnerability scanning is the process of verifying the current operating system configurations are secure. The Vulnerability scanning system is set to run monthly to determine the effectiveness of the patching program, if the server operating systems have been configured to the corporate standards, and that applications are kept current with the latest security patches and software. Additionally, all services must be inspected for configurations that compromise security (such as default usernames and poor passwords). Also, every quarter, a discovery scan of all known networks is performed to deliver a gap analysis of asset management, find Clients where installed software is running enterprise services or new Servers have been put on the corporate network outside of the appropriate process.

Scope:

Any device connected to the corporate network or subsidiary network housed on behalf of the company are within scope of the vulnerability scanning process.

Devices are broken into two categories Clients and Systems. A “System” is any device connected to the corporate network that is running a service that has been determined as being an “Enterprise” level service. These services include (but are not limited to) web, mail, database, telnet, file/print, and time synchronization services.

All systems that provide enterprise services are scanned monthly with the metrics and vulnerabilities reported to the Data Owner, Custodian and Information Security Manager. Clients are scanned quarterly to ensure that enterprise services are not running on them and are included in the asset and patch management programs. Client devices are not scanned for vulnerabilities unless there is significant deviation from the standard image (such as running an enterprise service); the networks they reside on are grouped by the matching Corporate and Site Patch groups. Server devices are grouped by individual IP and by matching their Patching groups (by owner and priority).

Every quarter, a discovery scan of all known networks is performed to deliver a gap analysis of stated client inventory, systems by owner and priority to the Information Security Manager.

Scanning has four levels of intensity:

1. A **Discovery Scan** provides basic information about the system such as Operating Systems and services the system provides. This information is then used to determine priority, impact and asset management information.

2. A **Compromise Scan** checks for vulnerabilities "that can be used by an unskilled attacker, or a system that is already compromised".

3. A **DOS (Denial of Service) Scan** checks for vulnerabilities "that can be taken advantage of by automated attack tools, or by a moderately skilled attacker"). Denial of Service checks will be performed during this stage of the vulnerability scan. These scans, by their nature, must attack the resource in order to see if it is susceptible. Because this test has the potential to interrupt production business processes, the scan should be submitted to the appropriate Change Control Council.

4. A **Brute Force Scan** checks for vulnerabilities "that can be taken advantage of by highly skilled attacker, or for signs that a system is not configured correctly". Verifying the integrity of application passwords and service accounts is performed by repeatedly trying common words. Because this test has the potential to interrupt production business processes, the scan should be submitted to the appropriate Change Control Council.

Architecture:

The Nexpose system consists of the management front end and a database back end. There are two scanning engines, the primary one installed on XXXXXXXXX and one in the Azure cloud (XX.XX.XX.XX) which is used only for external scanning.

Authentication is via the CCCCCCCC Active Directory system with two local back up accounts held by the Information Security Manager and the IT Systems/Support director. Authorization is internal to Nexpose; using three of the provided roles: Administrator, Asset Owner and User.

Procedures:

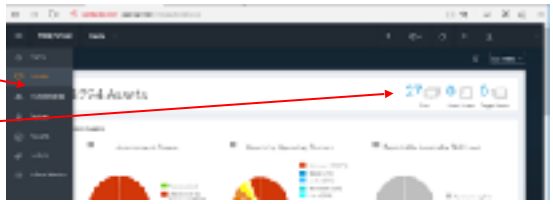
1. Procedure to Acquire

The Nexpose system is accessed via web bowser: https://XXXXXXX:3780. Active Directory credentials are used. Approval for entry to the system is via the Information Security Manager.

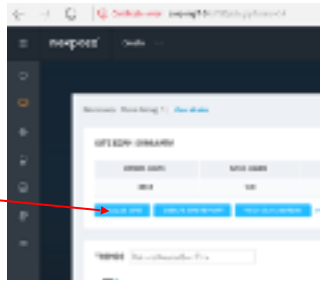
2. Adding a New Site/IP Range to an Asset Group

New store networks are added to a “Discovery –Store Group X” site group.

1. This is done from the Assets menu.
2. Choose “Sites”



3. Choose the applicable “Discovery” site from the list (the sites should have a relatively equal number of active assets) and then click on “Manage Site”.



4. Click on the Assets tab.

5. Click on the pencil to add the network range of the site. Complete the process by clicking on “Save”. There is no need to scan every time a new range is added.

3. Adding a New Server to an Asset Group

New servers are added to the “Vulnerability” site group that represents the owner and priority (“Vulnerability – AppDev P1” or “Vulnerability – Systems/Support P2-4” as examples).

1. This is done from the Assets menu, choosing “Sites”.

2. Choose the applicable “Vulnerability” site from the list based on owner and priority; then click on “Manage Site”.

3. Click on the Assets tab and then the pencil to add the server’s IP address. Complete the process by clicking on “Save”. There is no need to scan every time a new range is added. There is no need to scan every time a new server is added.

4. Quarterly Discovery Scan

Every quarter, a discovery scan of all known networks is performed to deliver a gap analysis of asset management, find Clients where installed software is running enterprise services or new Servers have been put on the corporate network outside of the appropriate process. This mini project follows a timeline:

- Day 1: CAB Discussion Item: Process Start and Schedule all Scans;
- Night 1: Discovery in Server-Core and External Networks;
- Day 2: Gap Analysis of Server inventory and Discovery Results;
- Night 2: Discovery of Corporate Group 1, DC and Site Group 1;
- Day 3: Port analysis of Clients for Enterprise Services;
- Night 3: Discovery of Corporate Group 2, Site Group 2;
- Day 4: Port analysis of Clients for Enterprise Services;
- Night 4: Discovery of Site Group 3;
- Day 5: Port analysis of Clients for Enterprise Services;
- Night 5: Discovery of Site Group 4;
- Day 6: Port analysis of Clients for Enterprise Services;
- Night 6: Discovery of Site Group 5;
- Day 7:
    - Port analysis of Clients for Enterprise Services;
    - Compile metrics by OS, System Owner, Priority and Type
    - Compile punch list of low priority issues found and status of high priority items discovered during the process.

5. Monthly Vulnerability Scan

Every month, a vulnerability scan of all Servers is performed to provide configuration and compliance analysis of operating systems and applications. This mini project (that should be scheduled after the last of the servers have been patched) follows a timeline:

- Day 1: CAB Discussion Item: Process Start and Schedule all Scans;
- Night 1: Vulnerability scan Test Baseline;
- Day 2: Survival and Assurance Analysis of Test Baseline;
- Night 2: Discovery of Corporate Group 1, DC and Site Group 1;
- Day 3: Port analysis of Clients for Enterprise Services;
- Night 3: Discovery of Corporate Group 2, Site Group 2;
- Day 4: Port analysis of Clients for Enterprise Services;

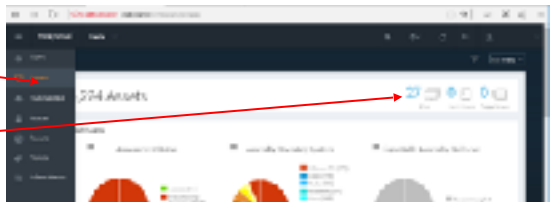
- Night 4: Discovery of Site Group 3;
- Day 5: Port analysis of Clients for Enterprise Services;
- Night 5: Discovery of Site Group 4;
- Day 6: Port analysis of Clients for Enterprise Services;
- Night 6: Discovery of Site Group 5;
- Day 7:
    - Port analysis of Clients for Enterprise Services;
    - Compile metrics by OS, System Owner, Priority and Type
    - Compile punch list of low priority issues found and status of high priority items discovered during the process.

6. Schedule Scans

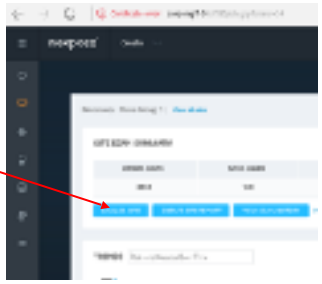
Scheduling the scans is performed via the “Assets” menu, then Sites. Select the site to schedule and then “Manage Site”.

1. This is done from the Assets menu.

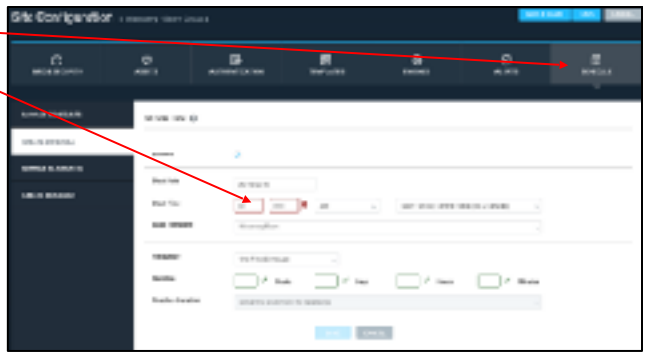
2. Choose “Sites”.



3. Choose the applicable “Discovery” site from the list (the sites should have a relatively equal number of active assets) and then click on “Manage Site”.



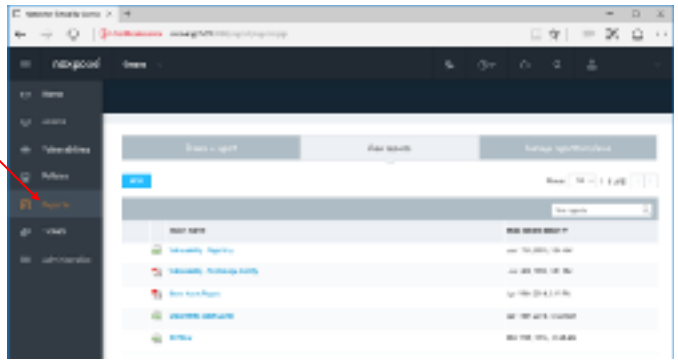
4. Click on the Schedule tab and then “Create Schedule”. Enter the start time (usually 5:00PM CST) and the day and then “Save”.



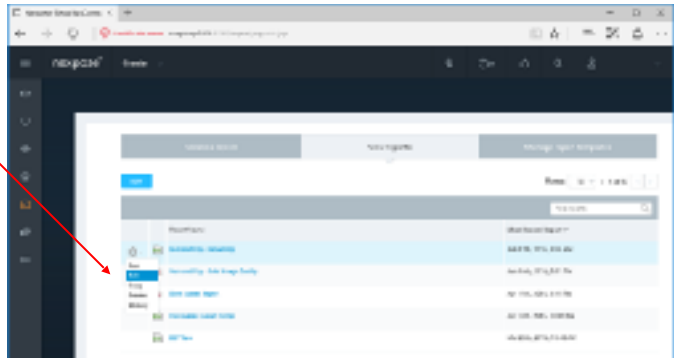
7. Reporting on Vulnerability Scans

Reporting on vulnerability scans entails exporting the data to Excel, ensuring all systems have been scanned (inventory check), findings are appropriately grouped and vetted.

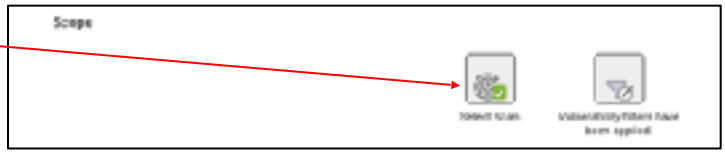
1. Each site's Vulnerability Scan will be exported via the Reports menu.



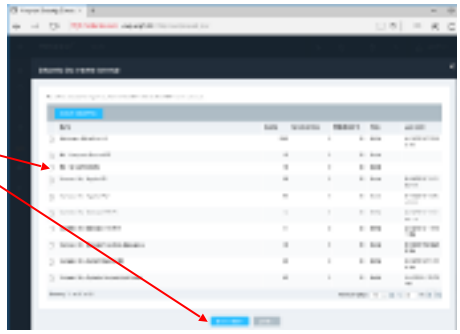
2. Select "Edit" under the appropriate site. Sites are labeled "Vulnerability" or "Discovery" a dash, then the site name.



3. Scroll to the bottom of the page and click on the "Select Scan" icon.



4. The site to report on ("Vulnerability – AppDev P1" for example) will already be selected. Click on "Select Scan". Then elect the date of the scan to report on and click on "OK".



5. Click on “Save & Run the Report". Nexpose will bring you back to the Reports menu. When it has completed generating the report, click on the link to download the file. Multiple reports can be generated at the same time (which is why each site has its own report).

6. Create and Excel sheet called, “Christus Vulnerabilities – (ddmmmyyyy).xlsx” (date of analysis completion). Add all the downloaded vulnerability CSV files into a tab called “Master”.

7. Create 4 tabs for the spreadsheet:

The spreadsheet should have six tabs total:
- Summary (report page)
- Inventory data – from inventory folder
- Application scan report data – from Nexpose
- Vulnerability report data – from Nexpose

The last 2 tabs should still be empty:
- Vulnerability Remediations – derived from Vulnerability data
- Inventory Check – derived from inventory comparison with Nexpose scans

7.1. Inventory Check

The first processing step is to validate that all of the listed inventory has been scanned (no missing children), and that all of the scanned systems are in the listed inventory (no orphans). IP is used as unique identifiers (even though this actually may not be the case).

Orphans and Missing Children are listed on the Summary page.

The checks can be done in two ways:

For Small Systems:
1. On the Inventory Check tab, paste in the IP column from each of the three reports.
2. Remove periods (.), format as numbers, and remove duplicates (Data ribbon, Data Tools group, Remove Duplicates);
3. Sort each column and compare results – they should be identical;
4. Listed inventory IPs missing from the scanned inventory(ies) are “missing children,” any IPs scanned which are not part of the inventory list are “orphans.”

For Larger Systems, use the vLookup() function to compare IPs:
1. On the Inventory Check tab, paste in the IP column from the inventory listing, name the column “Listed Inventory.” Remove all duplicates from this column and ensure that contents are values, not formulas;
2. Next, paste in the IP column from the either of the two scanned reports (just pick one). Name the column “Scanned Inventory.” Remove all duplicates from this column and ensure that contents are values, not formulas;
3. Create a 3rd column named “Was Scanned”. Populate this column with a vLookup() function which references each IP in the Listed Inventory column against the entire “Scanned Inventory” column: For example: =VLOOKUP(A2, B$2:$B$25,1,FALSE)

   Any Listed Inventory which finds a matching IP was scanned, otherwise (#N/A) you have a “missing child” – an IP in your listed inventory which did not get scanned;

4. Create a 4th column named “Not Orphan,” and this time lookup each IP in the Scanned Inventory” column against the entire “Listed Inventory” column.

   For example: =VLOOKUP(B2, A$2:$A$25,1,FALSE)

   Any Scanned Inventory which finds a matching IP is in your inventory, otherwise (#N/A) you have an “orphan” – an IP scanned in your reports is not part of your listed inventory.

7.2. Application Check – Highlighted Ports

1. Sort Application tab by "Port";
2. Highlight any Port numbers listed below - they generally should not exist, and if they do exist, they are a priority for justification or remediation and should be listed on the Summary page.

21	FTP	143	Mail
23	Telnet	194	IRC
25	Mail	389	LDAP
53	DNS	513	rlogin
69	TFTP	514	rshell
79	Finger	636	LDAP
109	Mail	2049	NFS
110	Mail	5631	PCAnywhere
119	NNTP	5900	VNC Remote Control
123	NTP		

7.3. Vulnerability Check – By Remediation

Copy Remediation column from Vulnerability tab, copy to the Vulnerability Remediations tab.

Add a second column which uses the countif() funtion to count duplicates, for example: "=COUNTIF($A$2:$A$1038,A2)"

1. Format countif values as non-formula values (copy, paste special >> values);
2. Sort by Count (largest at top), delete any invalid "#Value!" rows;
3. Select both columns and remove duplicates with "Count" deselected;
4. Select Count column and apply conditional formatting using color scales, using green for low and red for high;
5. Add a Categories column after the Count column and categorize the top several vulnerabilities as "Patch", "Config", or "Other";
6. The top 5 (or so) should be copied to the Summary page

7.4. Summary Page:

The summary page of the spreadsheet will be different for each system, as dictated by the particularities of each: Below are suggested minimums. Anything communicated on the Summary page should be clear and concise – K.I.S.S.

- Total number of systems in inventory
- Total number of High or Critical findings
- Top 5 (or so) vulnerability remediation
- Listing of port violations

- Listing of any Missing Children
- Listing of any Orphans
- Aging and/ or POA&M notes
- Analyst comments and specific recommendations

Discussions with system administrators should address essentially the same information as presented on the Summary page, as prioritized by importance and deliverability, with ongoing consideration targeting identification and elimination of causal factors.