

Purdue University
Vulnerability Scanning Cluster

USER GUIDE

Developed by

Matthew Wirges
<wirges@purdue.edu> and
maintained by Information
Technology at Purdue (ITaP) Security
and Privacy

Documentation by

Charles R. Hunter <crh@purdue.edu>

Jonathan Davis
<davis155@purdue.edu>

©2005; 2006 Office of the Vice
President for Information Technology,
Purdue University

INTRODUCTION.....	4
VSC PURPOSE.....	4
DOCUMENT SCOPE.....	4
BEFORE YOU START	4
STARTING A SESSION	4
QUICK SCAN SESSION.....	5
USING THE INFORMATION BAR.....	5
NAVIGATING DOMAIN AND SUBDOMAIN LOCATIONS	5
CURRENT DOMAIN	6
PARENT AND CHILDREN DOMAINS.....	6
<i>Changing Focus to a Parent Domain.....</i>	<i>6</i>
<i>Changing Focus to a Child Domain.....</i>	<i>6</i>
OVERSEER MODE.....	6
THE MENU BAR.....	6
NEWS	6
MY SCANS	6
QUICK SCAN REQUEST.....	7
SCAN REQUEST WIZARD.....	7
SEARCH.....	7
SCHEDULER	7
SETTING UP CHILD DOMAINS	7
MANAGING PLUG-INS.....	8
HANDLING NEW PLUG-INS.....	9
<i>Viewing New Plug-ins</i>	<i>9</i>
MANAGING POLICIES.....	9
WHAT ARE POLICIES?.....	9
AUTOMATICALLY-GENERATED POLICIES	10
CUSTOM POLICIES.....	10
<i>When and Why to Create a Custom Policy</i>	<i>10</i>
<i>Creating a Custom Policy</i>	<i>10</i>
SCANNING	12
REVIEWING SCAN OUTPUT	13
EXPORTING OUTPUT	13
SCHEDULING REGULAR SCANS	14
MISCELLANEOUS FEATURES.....	14
MY INFO	14
LIST USERS	14
GRANT PRIVILEGES.....	15
SEARCH AND VIEW SESSIONS	15
MANAGE NEWS.....	15
SEARCHING	15
SYSTEM CONFIG	15
HOST ENTRIES AND HOST FAMILIES	15
SEARCHING AND ANALYZING REPORTS.....	16

ANALYSIS OF A SCAN..... 16
 Scan Information..... 17
DIFFERENTIAL REPORTS 17
TROUBLESHOOTING 17
 I CAN'T START A SESSION!..... 17
 I CAN'T ACCESS THE ADMINISTRATION FUNCTIONS! 18
 THE VSC WON'T ALLOW ME TO ADD AN IP TO A SUBDOMAIN! 18

Introduction

The *Vulnerability Scanning Cluster*, or VSC, is a system designed to conveniently scan large networks for potential vulnerabilities efficiently and on a regular schedule. The VSC, in its entirety, refers to a hardware and software scanning solution that includes the following elements:

- VSC management tool
- Properly configured network hardware
- Properly configured network software

Most users come into contact with only the VSC management tool, so you may hear it abbreviated to VSC.

VSC Purpose

The VSC system is designed to provide managers, administrators, and auditors with a scalable enterprise-level solution for scanning large networks. The VSC uses *Nessus* (<http://www.nessus.org>), one of the more popular vulnerability scanning tools, to perform the actual scans of each node.

You can find out more about the VSC project by visiting the VSC Source Forge page at <http://vscweb.sf.net>. To offer questions, ideas and concerns to Purdue's ITaP, send an e-mail to itap-vsc@purdue.edu.

Document Scope

This user guide discusses how to use the VSC, including the configuration of domains, networks, hosts, and host families, as well as scheduling and performing scans.

Before You Start

To use the information in this user guide, you must have an established and working vulnerability scanning cluster, and the VSC management tool must be running properly on a Web server you can access.

If you need help installing and configuring the VSC, refer to the *Vulnerability Scanning Cluster Installation Guide*.

Starting a Session

Do the following to start a VSC session:

1. Direct your Web browser to the management tool on the Web server. The VSC tool has been tested most thoroughly on the Mozilla, Firefox, and Safari browsers.
2. Click "login."

3. Log in with a registered user name and password to authenticate.

If you do not have a registered user name and password, contact the VSC system administrator.

If you are not able to start a session, ensure that you have access to the server, that the management tool is properly running on it, and that you have been granted management tool access by the system administrator.

Quick Scan Session

If you just want to get started with a default full scan, do the following:

1. Check the [Information Bar](#) to ensure that the system is not under a heavy load of scans.
2. Click the “[Quick Scan Request](#)” link.
3. Add a host IP address to the text box, click or select “>” from the list of hosts, and click the “Add” button.
4. (Optional) If you wish, you can choose a different [policy](#) from among the [automatically generated policies](#). By default, the full scan is selected.
5. Click the “Request” button to place the scan in the queue to be executed.

Using the Information Bar

The information bar resides near the top of the VSC and provides convenient access to basic statistics about the cluster, including:

- the number of scan requests queued,
- the number of individual hosts in these requests,
- the current status of the queuing system,
- the total number of scan plug-ins that have been installed on the system, and
- the number of newly installed scan plug-ins.

This information describes the current use of the cluster itself, and is useful for deciding whether you can quickly run a scan.

Navigating Domain and SubDomain Locations

The information bar lists “where you are” in the network management system in terms of “parent” and “children” domains.

Current Domain

The domains you have permission to manage are listed in the dropdown box under the **Current** heading. This listing allows you to quickly jump between disparate or navigationally distant domains.

You can also create multiple subdomains to keep networks organized and to allow you to delegate scanning privileges.

Parent and Children Domains

The **Parent** and **Children** sections allow you to focus your view of VSC activity on specific domains or subdomains.

Changing Focus to a Parent Domain

Do the following to change the viewing focus from the currently selected domain to its parent domain:

1. Select the appropriate parent domain using the dropdown box under the **Parent** heading.
2. Click the **Switch** button to execute the selected change.

Changing Focus to a Child Domain

Do the following to change the focus from the currently selected domain to its child domain:

1. Select the appropriate subdomain using the dropdown box under the **Children** heading.
2. Click the **Switch** button to execute the selected change.

Overseer Mode

Click the on/off button under “Overseer” to view all the scans, hosts, and policies in the current domain and all its child domains. Use the “Search” link to view the effects of enabling overseer mode.

The Menu Bar

Use the menu bar for links to the various submenus and to select actions to perform with the VSC.

News

The **News** page is the default view, and lists the latest updates, changes, outage notifications, and other news, starting with the most recent item.

My Scans

Select **My Scans** to view information about the scans that have run from the currently logged-in user account.

Quick Scan Request

Select **Quick Scan Request** to quickly select and run a scan. This feature uses automatically (or previously) generated profiles to run standardized sets of Nessus plug-ins on the hosts you choose.

Scan Request Wizard

Select **Scan Request Wizard** to launch a wizard that walks you through the creation and execution of a new scan. The wizard allows you to create a scan that is far more tailored to your system's needs than the [quick scan request](#).

For example, the Scan Request Wizard allows you to run a scan immediately or schedule it for a future time frame, perhaps when your system's load will be lighter. The scheduling ability features recurrence, so you can set up a series of perhaps monthly or weekly scans. You can also finely control the parameters the scanning engine uses when running the Nessus plug-ins, which allows you to control the nature and duration of the scan.

To use the wizard, click the "Scan Request Wizard" link, and then follow the onscreen instructions, clicking "Next" or "Finish" when necessary.

Search

Use the **Search** feature to find specific scans or groups of scans. You can search by host name, user, and start or end dates.

Tip: [Overseer Mode](#) allows you to see all of the scan activity for both the current domain and all child domains. By default, Overseer Mode is turned off, in which case a search displays only the scan information for the currently selected domain.

Scheduler

Use the **Scheduler** to view a calendar representation of all the scans that have been executed in the past, are in process now, or have been scheduled for the future.

Setting Up Child Domains

To run scans, you must establish a domain. Do the following to establish a domain:

- 1) Click the **Show Advanced Menu** button to access the administration-specific functions.

Note: If you do not see these options, you may not have the appropriate permissions. If there is an administrator above you (in the chain of command sense), you may need to request Privileges by clicking on the Request Privileges link.

- 2) Select **Domain Management**.
- 3) Name your new domain.



Tip: Make this a name that is descriptive of the networks you will put in it. Typically, it is good to name the domain based on your organization, “Accounts Receivable,” a building name, or some other common name for the group you are supporting.

Make sure you have devised a clear breakdown of your network before creating domains. You probably want to use the VSC because you have a large network.

4) Add IP ranges.

A little planning now will go a long way in the future. While it is useful to divide your networks into their smallest logical groupings, you must be careful not to break your networks down too small. As a rule of thumb, the minimum size you’ll want a subdomain to be is the set of machines you will *commonly* scan apart from the parent domain.

For example:

Pat is the network administrator in the Chemistry department of Acme University, and has two class “C” subnets to monitor. Pat creates his domain called “Chemistry” and sub-domains “Faculty Offices,” “Staff Offices,” “Research,” and “Student Labs” having 100, 62, 120, and 200 hosts, respectively. Each subdomain represents a different set of users with different requirements and usage habits. This represents a reasonable logical view of the network, and Pat may find it useful to classify the machines further with Host Families later. Within the “Research” subdomain, Pat could have chosen to split this even further by naming each research group. In this case, however, there would be little to gain from doing so. The resulting subdomains would be quite small, and the maintenance requirements of so many entries with hosts—that may go in and out of the group—could become significant. Realistically, Pat is not likely to scan “Research” group A more frequently than “Research” group B or scan them by any different

While you are naming your domain criteria, you can also specify a network address range to be associated with that domain name. This may be specified in traditional *x-y range* (inclusive) notation, or in CIDR notation. You may add or modify network ranges later by selecting the *Network Management* link

You may create as many subdomains as you deem necessary, but it is extremely important to note that IP ranges in a defined subdomain may not overlap with other subdomains. A set of IPs may not belong to more than one subdomain. The system will not allow an IP to be added to a subdomain if it already belongs to another domain.

Managing Plug-ins

“Plug-ins” are what Nessus calls the individual tests for specific security vulnerabilities. Nessus categorizes plug-ins into families representing either a vulnerability type or specific platform or group of platforms with common vulnerabilities.

Click “**View Plug-ins**” from the Advanced Menu for a list of the currently installed Nessus plug-ins, categorized by the type of vulnerability. Use the dropdown box to change the category.

Handling New Plug-ins

Plug-ins are marked “new” if they have not been viewed by anyone using the current user account. This feature exists to alert you to the existence of new plug-ins and to allow you to easily view them and decide whether to include them in your [custom policies](#). This feature exists for better organization only, and is analogous to marking an email message as “read”.

Viewing New Plug-ins

Do the following to view the new plug-ins:

1. Click the radio button labeled “View New Plug-ins.”
2. Click the “Update” button.

Listing only the new plug-ins can be valuable because the system self-updates on a frequent basis.

To acknowledge a plug-ins as having been read, select one or more and click the “Mark Seen” button. The selected plug-ins are no longer regarded as new.

To review the information about a given plug-in, highlight the plug-in and click the “*Plug-in Info*” button. This opens a new window containing a table that describes the plug-in. Once you view a plug-in description, it is automatically marked “seen” by the system.

Managing Policies

Policies are perhaps the most important and powerful component of the VSC, and among the least used.

What Are Policies?

Policies are configuration files that govern the behavior of a scanner node. Policies are used to define which plug-ins (of the more than 11,000 available) are run, how they are run, and what to do when they cannot run.

Policies are a powerful tool for streamlining the vast amount of data that can be returned from a general vulnerability scan. By using a policy, you can create a scan that returns a limited amount of data that is targeted to your specific computing tools. You may use policies created by the system, or you may create your own.

Automatically-Generated Policies

The automatically generated policies are taken from Nessus plug-in families and are designed to scan for general vulnerabilities.

Custom Policies

When you find a situation where you want finer control over the included plug-ins in a scan, or finer tuning of the actual scanning process, create your own policy.

When and Why to Create a Custom Policy

Well-tailored custom policies are important. Custom policies limit the scope of the vulnerability scan, and make the likelihood of detecting a vulnerability, and of noticing key vulnerability data in the resulting reports, much greater.

As a novice VSC user, you may find it is best to start with the “full scan” or other default policy. As you review reports generated by these policies, you will get a better feel for your systems, discovering which plug-ins are unnecessary for a particular set of systems and which generate false positives. You will realize the full benefit of a set of accurate custom policies when you begin to schedule regular scans of your network. These regular scans are far more valuable if the information they report is limited to the potential vulnerabilities peculiar to your systems.

Creating a Custom Policy

Do the following to create your own scanning policy:

1. Click the “Manage Policies” link from the **Advanced Options** menu.
2. Click the “Add” button.

You are presented with a list of parameters for your new custom policy.

3. Set the following parameters for your new custom policy; then, click “Add.” Changing a parameter from its default value is optional, unless the parameter is marked “required.”

Global: Check this box to make this new policy available to other administrators at or below your level.

Policy name (required): Type in an appropriate name for this policy.

Max simultaneous hosts represents the maximum number of hosts to be tested at any one moment. The highest reasonable number depends on the network I/O speed of your systems. If the number is too high, the VSC will fail.

Max simultaneous plug-ins represents the maximum number of plug-ins to be tested at any one moment. This number, coupled with the

“Max simultaneous hosts” value, allows you to configure the VSC to approach the maximum test speed capabilities of your system.

Log entire scan should typically be set to “no,” unless debugging due to the sheer amount of data returned when set to “yes.”

Report killed plug-ins provides a list of plug-ins that were not able to completely run.

CGI-bin path: Set this field to whatever path your systems use for a CGI bin or equivalent.

Port range limits the range of ports scanned by the VSC to whatever you specify. The default behavior is to scan every possible port.

Optimize Tests

Language selects the language in which you want the VSC tool to operate. Options are English, etc.

Delay_between_tests specifies a delay, in seconds, between the testing of each plug-in.

Plug-in imeout (in seconds) specifies a period of inactivity, in seconds, before a plug-in timesout and the VSC moves on to the next test.

Disable unsafe plug-ins disables plug-ins that would otherwise attempt to cause damage to a system by typical “hacker” methods.

Auto-enable dependencies configures the VSC to also run any plug-ins that are necessary precursors to plug-ins you have selected to run. For example, if you select Plug-in B to run, and Plug-in B requires results from the otherwise unselected Plug-in A, this feature will cause Plug-in A to run before Plug-in B. If you were to turn off this feature, neither Plug-in A nor Plug-in B would run, even though Plug-in B is selected.

Use MAC Address (if available): Copy needed here?

Host Expansion by: Copy needed here?

Ping hosts before scanning configures the VSC to ping each host’s IP address before attempting to scan. This verifies that the hosts are online and responsive beforehand. You might disable this feature when scanning hosts that are configured not to respond to pings.etc.

Reverse Lookups: ? Copy needed here?

Unscanned_Close: ? Copy needed here?

Ports not to scan simultaneously identifies ports that should be scanned only sequentially, for whatever reason.

Timeout for plug-in is distinct from plug-in timeout in that...etc.

Managing Performance Characteristics

The *maximum simultaneous plug-ins*, *delay between tests* and *plug-in timeout* parameters are the most important for managing cluster performance. A value that is too high or too low for your environment can significantly delay scanning. Special care has been taken to provide default values that will perform well. It is usually unnecessary to modify these.

The *Port Range* field is also very important when developing custom policies. Without specifying a range of ports in your policy, the scanner will default to the entire range of ports, tremendously increasing the potential time to complete the scan.

1. Click the link at the top of the page to manage the new policy's plug-ins.
2. Select the plug-ins you want the VSC to use when executing this policy. You can add plug-ins in any of the following ways:
3. Type in the plug-in number and click
4. Select one or more plug-ins from the list, and click.
5. Click the "Add" button to add all plug-ins.

For information about a specific plug-in, highlight the plug-in in the list and click the "Info" Button. You can also use the "»" and ">" buttons to remove all plug-ins or selected plug-ins from the policy.

The added plug-ins appear in the list of attached plug-ins. Changes are saved immediately and automatically upon clicking the arrowed buttons.

You have now created your custom policy.

Scanning

Once you have an established domain and are satisfied with the current plug-in set and policies, you're ready to test what will be the normal operation of the VSC: scanning, scheduling, and reporting.

First, we will walk through a simple Quick Scan Request as a basic test to make sure everything is working correctly. Log in to the VSC, and click on the Quick Scan Request link on the navigation bar. This will allow you to choose a host or hosts to scan from the networks defined in your domain. You may choose to add the hosts manually by entering them in the text input box and clicking the *add* button, or if you have entered hosts or ranges before, you will see a history of entries in the list below and to the left of the box.

The hosts you are entering will appear in the list to the right. As with other cases, the familiar arrow button interface will allow you to make further modifications to the list, with single arrows denoting adding or

removing currently highlighted entries, and double arrows allowing you to quickly add or remove *all* entries.

Once you have selected the hosts you want to scan, you must choose a policy that you want applied to these hosts. The policies will determine the kinds of vulnerabilities for which the cluster will search. (Refer to the [Managing Policies](#) section for more information.) For our first scan, it is most appropriate to run the catch-all “Full Scan” policy. As the name implies, this scan will run all tests available on the machines in question. This is likely to generate a lot of data, but will be very useful for understanding the capabilities and limitations of the VSC reporting mechanism.

Please note: You should attempt to launch your scan only from the most appropriate subdomain. That is, if you have already established a subdomain that includes the range you are scanning, do not attempt to add those machines to a parent domain. This will cause an unintended side effect of permanently associating those machines with the parent domain.

Once you are satisfied with your choice of hosts you want to scan and the policy you want to apply, click the button marked *Request* at the bottom of the screen to submit your scan. The resulting page that loads gives you a summary of the submitted scan. For now, just remember your scan ID number. It is not terribly important to write any of this down because the system will notify you, via email, when the scan is complete and will contain the scan ID.

If you are impatient, or just curious, you may check on the status of your scan or by going back up to the *Navigation bar* and selecting *My Scans*. This page will list your current scans and the results of previous scans and their status. You may click on the scan number of each entry to see a more detailed status.

Reviewing Scan Output

After the scan has been completed, you should receive notice of it by email. Now you can review the results. By visiting the VSC website *My scans* section again and clicking on the appropriate scan number, you will see a scan status summary. This summary will list many of the details you saw in the *my scans* list. Most interesting to us at this point is the View Report section underneath the *Scan Host Information* header. From this menu, we can select how we want to view our scan output report. First, we choose the desired output format: *text*, *html*, *fancy html*, or *csv*. Next, we must specify the scope of the report we want to view. If you want to see the complete report as it was received by Nessus, select *All Results*. If you are only concerned with the hosts in your scan that have registered as vulnerable, select *Critical Only*. Finally, if you simply want the general host information discovered by the scan, select *All but Critical*.

Exporting Output

At the time of this writing, it is not possible to explicitly download a scan report. CSV or text reports may be easily copied from the browser

window if a report is sufficiently small, but the output from large reports is cumbersome.

Scheduling Regular Scans

Use of the VSC is greatly enhanced by the ability to schedule future scans and reoccurring scans. Performing “one off” scans or scanning the network only when a compromise is suspected is lazy and imprudent. An upstanding and conscientious administrator will perform regular scans of his/her network and pay special attention to systems considered “high risk.” It may be sufficient to scan the entire network semi-annually, or perhaps quarterly, while high-risk systems may need to be scanned on a weekly basis. You must decide this in conjunction with your management.

In some cases where federal regulations may apply to your systems, such as HIPAA, GLBA, or FERPA, you may need to scan and provide reports on a much more frequent basis. Some users may, at this point, consider scanning on a daily schedule. Bear in mind, however, you will be inundated with reports that need a human to review them who will likely have to sift through a significant amount of “noise.”

The VSC is not very useful as an intrusion detection system and should not be treated as such. Other products are better positioned to fill this role. If you must have this granularity for scanning your systems, a suggested alternative to a daily schedule would be to split the network into subdomains (if you have not already done this) and schedule each subdomain as a weekly reoccurring scan on a fixed day of the week. Then, scan the second segment on the next day, and so on.

As you adopt a regular scanning schedule, keep in mind that over time custom policies tailored specifically to your system types should now begin to play their role. Knowing each scan group’s operating systems, installed applications, and services is vitally important for efficient operation.

Miscellaneous Features

You might not use initially several other features found in the “Advanced Options” menu.. As the size of your actively-scanned network or the number of auditors or subdomain administrators grows, you may find the following features useful.

My Info

Use **My Info** to record the personal information that you want visible in the **List Users** report. Any users, privileged or unprivileged, can modify personal information. Personal information is viewable by only the user, the user’s peers in the same domain, and the administrators of the domains above.

List Users

The **List Users** feature lists users who are in a peer relationship with you in a particular domain. If you are an administrator for a higher-level domain, you can see privileged users who belong to the domain

and any unprivileged users in the domain or subdomain below you. Note that if you activate **Overseer Mode**, you may see a great deal more entries than you intended.

Grant Privileges

Use **Grant Privileges** to grant requests for privileges made by other users in your domain.

Administrators can modify the permissions of members of their own domain. Administrators cannot modify the permissions of members of the domains above them.

Search and View Sessions

One other feature that may be useful to the administrator for auditing purposes is the ability to search and review previous sessions for his/her users. By clicking on the Search Sessions link, you may type in a username and an optional date range.

Manage News

You may also use the *Manage News* facility to post messages to be displayed in the main window when an authorized user connects to the VSC and enters your domain. The user may also see these messages by explicitly clicking on the *News* link on the navigation bar. New messages may be added to the page by filling in the text boxes and clicking on the *add* button. You can edit or delete each message by clicking on the corresponding links at the bottom of the screen. If you want to send a message to all subdomains as well, check the *broadcast* checkbox.

Searching

By clicking on the *Search* link on the navigation bar, you may access the scan search facility. From this interface, you can search the current domain (and all subdomains if you enable the *overseer* mode) by *date*, *hostname*, *user*, or *status*. Scan results are listed below the scan, and you can take further actions on the results in the *Action* dropdown box.

System Config

If you are the administrator of the root domain on the system, you will also see the *System Config* button. This allows you to change the behavior of the core system and modify various configuration options.

Host Entries and Host Families

Each individual IP address on your domain may also have a corresponding host entry added to the system. Host entries provide further information about the machine in question. This includes the *hostname*, the corresponding *IP address(es)*, *NETBIOS name*, and *MAC address*. It also includes several freeform fields for your own use such as *location*, *serial number*, and *other ID*. Finally, you may modify the selected *Host Family*.

Host Families are sets of hosts that have a common trait. These sets exist entirely for your custom use and are definable by you and any administrators above you. You can create sets based on physical criteria, such as the location or manufacturer, or for more systemic purposes, such as for tracking common operating systems or confidentiality requirements. For example:

Suppose the security office requires all hosts storing medical information that fall under HIPAA regulations be scanned nightly. Rather than scan all your systems and sift through the resulting mountain of data for what you want, you can define a host family that includes only those hosts that require nightly scanning.

Furthermore, the security office manager might create this host family ahead of time and set it to be globally viewable so all administrators below could use this specification without having to define their own. In this way, the manager can run a scan on *all* the HIPAA hosts from the top domain.

To create host families, select the “Add Host Families” link in the **Advanced Options** menu.

If you find a value for a particular field too general or unsuitable for your needs, contact the maintainer of the VSC management tool web interface for your organization.

Searching and Analyzing Reports

Analysis of a Scan

To successfully interpret the output of a scan, it is necessary to understand what the results really mean.

Do not assume that a scan is completely reliable. Just because a scan shows a particular system as vulnerable to a particular attack, does not mean that it truly is. The VSC features built-in safeguards that, by default, prevent the VSC testing from proving the vulnerability of a machine by actually compromising it. While this safety feature protects the hosts being scanned, it introduces the possibility that a scan report will return false positive results.

Verify the results of the scan with the appropriate system administrator. Check the patch levels of the OS on the system, installed applications that may be vulnerable, and applications that could create an unknown profile for the scanner. To facilitate speedy evaluations of reported vulnerabilities, create a regular and thorough audit process for systems on your network.

Regardless of the output type, individual scan reports will have essentially the same fields. In many cases, the particular vulnerability listed will have an obvious remedy, such as a system upgrade, filtered or otherwise restricted access to a service, or removal of an unnecessary service.

Scan Information

To learn more about a particular scan, display the report in “Fancy HTML” format, then either—

- click the *plug-in ID* link to display the Nessus plug-in information, including the official description and the source code to the plug-in, or
- click the *CVE* link to view information about the actual vulnerability for which the plug-in scans.

Both links are helpful in analyzing a machine with an ambiguous vulnerability status.

Differential Reports

It is also possible to view the differences between separate scans. If you select two or more scans in the scans list and then select *Scan Diff* as the action, you will be able to generate a differential report for the hosts common in the scans selected. Similar to the normal scan report generation, you may select several formats to view your scan in, as well modify the report scoping. This mechanism allows you to check the status of the remediation of prior vulnerabilities for a large number of hosts. A differential report will contain only those hosts common to all reports selected. The report will contain a table of specific vulnerabilities and the ID numbers of the scans in the set that are vulnerable. To check the status of remediation, simply compare the column of the most recent scan (usually the one furthest to the right) to the previous scan. If a table cell is empty, its associated vulnerability was not detected in the most recent scan and can be considered repaired.

If there are sufficient scans with the appropriate common hosts, differential reports can be generated for more than two scans. Differential reports of multiple scans may be generated without limit, though there may not be much to gain from a differential of more than three or four, other than historical information.

Troubleshooting

Use the following circumstances and fixes to troubleshoot your VSC session:

I can't start a session!

- Do you have access to the server?
- Is the management tool properly running on the Web server?
- Have you been granted management tool access by the system administrator?

I can't access the administration functions!

Make sure you have the appropriate level of privileges from the controlling administrator.

The VSC won't allow me to add an IP to a subdomain!

A set of IPs may not belong to more than one subdomain. The system will not allow an IP to be added to a subdomain if it already belongs to another domain.