

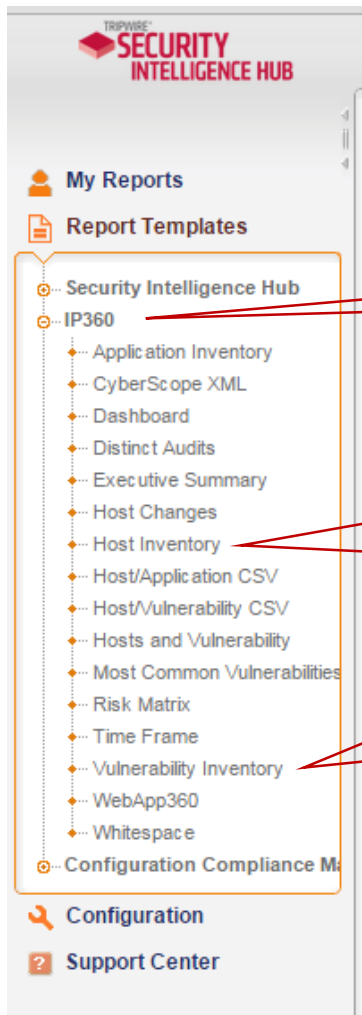
TripWire Instructions

Contents:

- I. [Login](#)
- II. [Report Template Selection](#)
- III. [Choose Asset Group](#)
- IV. [Vulnerability Inventory / Risk Matrix](#)
- V. [Host Listing](#)
- VI. [Host Detail](#)
 - a. [Save/Schedule reports](#)
- VII. [Vulnerability CVE / Remediation](#)
- VIII. [Edit Report Parameters / Filter Reports](#)

Log Into Tripwire

Log into the Tripwire vulnerability scanning report server at <https://ncircle.ouhsc.edu/sih/index.plx> using your OUHSC User-ID and password, choose "OUHSC-AD" as the "Auth" type.



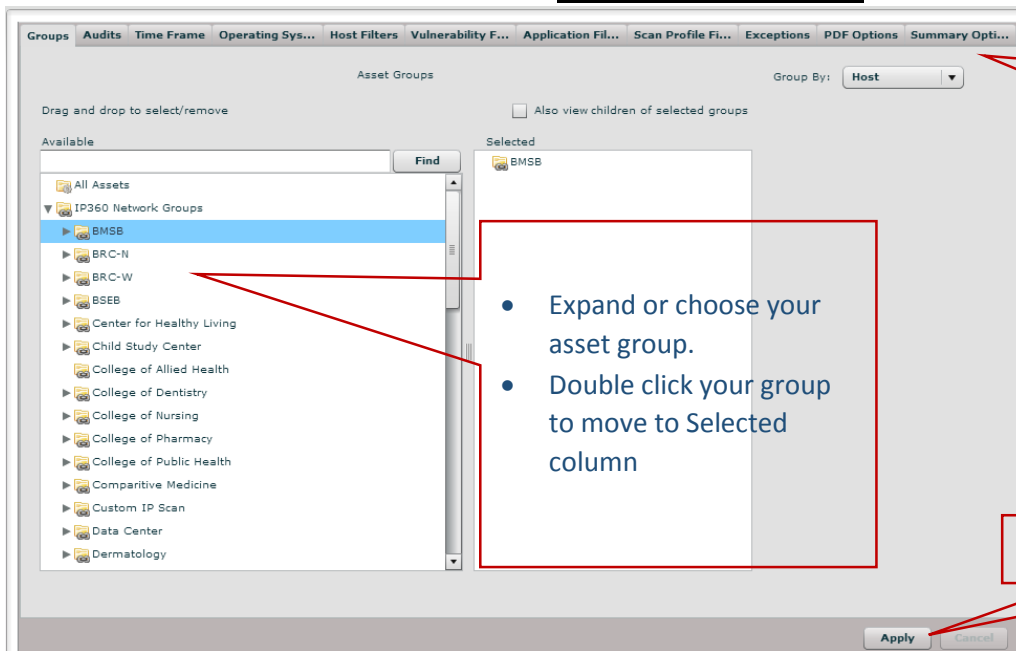
Report Template Selection

Select the **IP360** menu

- Host Inventory:** list of hosts (filters can be added) including:
 - IP Address
 - NetBIOS Name (Computer Name)
 - Host Score

- Vulnerability Inventory:** Risk Matrix > an enumeration of current Risk.
 - Goal is to maintain a Host Score below 1000 at all times.

Choose Asset Group



A variety of filters are available

- Expand or choose your asset group.
- Double click your group to move to Selected column

Click **Apply** to run the report

Vulnerability Inventory: Risk Matrix

Edit Report Parameters...
Save/Schedule Report...
Export...

Hosts (with vulns):	191	Unique Vulnerabilities:	3,168	Unique Applications (with vulns):	104
Average Hosts:	228	Average Vulnerabilities:	25,440	Average Applications:	9,222
Average Score:	7,721	Average Score:	69	Average Score:	190
Highest Observed Score:	684,753	Most Serious:	56,601	Highest Score:	56,601
Average Asset Value:	0	Display Mode:	Show Excepted Findings		

Risk Matrix

Automated Exploit	10	187	55	8	19	20	
Easy	9	104	12	2	10	9	
Moderate	1	14	2	2	2	1	
Difficult	3	23	5	4	2	1	
Extremely Difficult	14	63	6	3	2	6	
No Known Exploit	212	126	1787	325	25	48	
	Exposure	Local Availability	Local Access	Local Privileged	Remote Availability	Remote Access	Remote Privileged

This is the Highest Risk area. Focus on Highest Risk Hosts first.

These numbers are hyperlinks and will drill down into the affected Hosts

Vulnerability Count by Risk Logarithmic Scale

Risk Level	Count
Exposure	~200
Local Availability	~150
Local Access	~2100
Local Privileged	~400
Remote Availability	~100
Remote Privileged	~100
Remote Access	~100
Custom Rules	~100

IP	DNS Name	NetBIOS Domain	NetBIOS Name	Operating System	Host Score	IP360 Asset Value	Has Exceptions?
10.64.44.86	10.64.44.86	OUHSC	OPTIXE	Windows Vista x86	684753	0	
10.64.44.18	10.64.44.18	OUHSC	PHYS-BMSB-617	Windows XP SP3	78301	0	
10.64.44.151	10.64.44.151	OUHSC	CB-IMAGERPC	Windows XP SP3	71419	0	
10.64.45.254	10.64.45.254			APC Web/SNMP UPS	56601	0	
10.64.45.134	10.64.45.134	WORKGROUP	MACMINI-4A195	Mac OS X 10.6.x	45914	0	
10.64.44.113	10.64.44.113	OUHSC	PEDS-4Z4ZCP1	Windows 7 x86 SP1	36646	0	
10.64.45.151	10.64.45.151	OUHSC	PEDS-54M2WD1	Windows 7 x64 SP1	29172	0	
10.64.44.209	10.64.44.209	OUHSC	PEDS-BBM49P1	Windows 7 x86 SP1	28255	0	
10.64.44.85	10.64.44.85	OUHSC	COMD-BMSB-34	Windows 7 x86 SP1	23459	0	
10.64.44.33	10.64.44.33	OUHSC	OUP-BMSB-ECO	Windows 7 x86 SP1	23070	0	
10.64.44.141	10.64.44.141			HP JetDirect Printer	22628	0	
10.64.44.50	10.64.44.50			HP JetDirect Printer	22626	0	

Page 1 of 1 Total Records: 228 Per Page: 5000 Jump to Page: 1

DNS Name is a hyperlink to drill down into the vulnerabilities affecting this host

Report is sorted by Host Score (highest risk at the top)

05/15/2015 08:49, session logout in 56.29 minutes © 2003-2015 Tripwire. All Rights Reserved.

[\[Back To Top\]](#)

Host Listing

Columns are sortable by clicking on the column header

IP	DNS Name	NetBIOS Domain	NetBIOS Name	Operating System	Host Score	Last Scan
192.168.235.50	192.168.235.50			OS Undetermined	0	01/03/2011
192.168.234.51	192.168.234.51			Unix Variant	19	01/03/2011
192.168.234.50	192.168.234.50			Unix Variant	19	01/03/2011
192.168.235.30	192.168.235.30			OS Undetermined	1	02/24/2011
192.168.235.157	192.168.235.157			Linux 2.4-2.6	321	02/24/2011
192.168.235.47	192.168.235.47			Unix Variant	1	02/24/2011
192.168.235.195	192.168.235.195			Unix Variant	8	02/24/2011
192.168.235.165	192.168.235.165			Unix Variant	1	02/24/2011
192.168.235.177	192.168.235.177			Linux 2.4-2.6	8	02/24/2011

Click the hyperlink DNS Name to view the host details, including the Vulnerability

Save/Schedule Report...

This will store your favorite reports in My Reports on the main menu list

Host Detail

ID	Protocol/Port	Name	Score	CVE	Remediation
10680	tcp/80	phpMyAdmin Default Root Access Vulnerability	48153		
1650	tcp/80	Apache /server-info	1998		
25580	tcp/80	PHP sqlite.c Arbitrary Code Execution Vulnerability	513	CVE-2010-1868	
24492	tcp/80	OpenSSL 'zlib_stateful_finish()' Denial of Service Vulnerability	163	CVE-2009-4355	
25581	tcp/80	PHP HTTP Chunked Encoding Stream DoS Vulnerability	102	CVE-2010-1866	
24491	tcp/80	OpenSSL 'dtls1_retrieve_buffered_fragment()' Out of Sequence DTLS Hi	82	CVE-2009-1387	
1651	tcp/80	Apache /server-status	66		
25571	tcp/80	OpenSSL 'bn_wexpend()' Error Handling Unspecified Vulnerability	63	CVE-2009-3245	
3338	udp/137	MS03-034; Microsoft Windows NetBIOS Name Service Reply Information	52	CVE-2003-0661	
25575	tcp/80	PHP fnmatch Stack Consumption Denial of Service Vulnerability	45	CVE-2010-1917	

Vulnerability Details – Each detail has a magnify glass to view available Remedies for each Vulnerability

Vulnerability CVE/ Remediation

Vulnerability details, affected versions, and Remediation (including links to Remediation update or hotfix). Perform the listed actions for remediation.

ID	Name
12072	JRE, JDK, and SDK in Java Web Start Privilege Escalation Vulnerability

CVE Links:
[CVE-2008-1190](#) [CVE-2008-1190](#)

Description:
 Unspecified vulnerability for Java Web Start in Sun JDK and JRE which allows remote attackers to gain privileges via an untrusted application.
 See this link for more information:
[http://sunsolve.sun.com/search/document.do?assetkey=1-26-233323-1\[Defunct\]](http://sunsolve.sun.com/search/document.do?assetkey=1-26-233323-1[Defunct])

AFFECTED VERSIONS
 Unspecified vulnerability in Java Web Start in Sun JDK and JRE 6 Update 4 and earlier, 5.0 Update 14 and earlier, and SDK/JRE 1.4.2_16 and earlier allows remote attackers to gain privileges via an untrusted application, a different issue than CVE-2008-1191, aka the "fourth" issue.
 JDK and JRE 5.0 Update 14 and earlier

Remediation:

Close

Description of vulnerability

Affected Versions

Remediation list

Edit Report Parameters/Filtering Reports

Reports are filterable by many variables. This example will show how to filter by computer name within the specified asset group.

The screenshot shows the 'Edit Report Parameters' window with three tabs: 'Edit Report Parameters...', 'Save/Schedule Report...', and 'Export...'. The 'Host Listing' table is visible, showing columns for IP, DNS Name, NetBIOS Domain, NetBIOS Name, and Operating System. A red box highlights the 'Edit Report Parameters...' tab with the text 'Select Report Parameters...'. Below the table, the 'Host Filters' tab is selected, showing a dropdown menu for 'DNS Name' with a list of filter options. A red box highlights the 'Host Filters' tab with the text 'Host Filters tab'. Another red box highlights the 'NetBIOS Name' option in the dropdown menu with the text 'Select NetBIOS Name (to filter by computer name)'. Below the dropdown, the 'NetBIOS Name' filter is configured with a text input field containing 'computername2' and an 'Add' button. A red box highlights the text input field with the text 'Type the computer name and click Add for each computer name you wish to filter by..'. Below the configuration, a table shows the filter configuration:

Attribute	Value	Action
NetBIOS Name	computername1	<Include>

** After adding computer names, you select Apply to run the report.

** Save/Schedule Report: make sure to save your report with a unique descriptive name so you don't have to add filters again.