NETWATCHER™

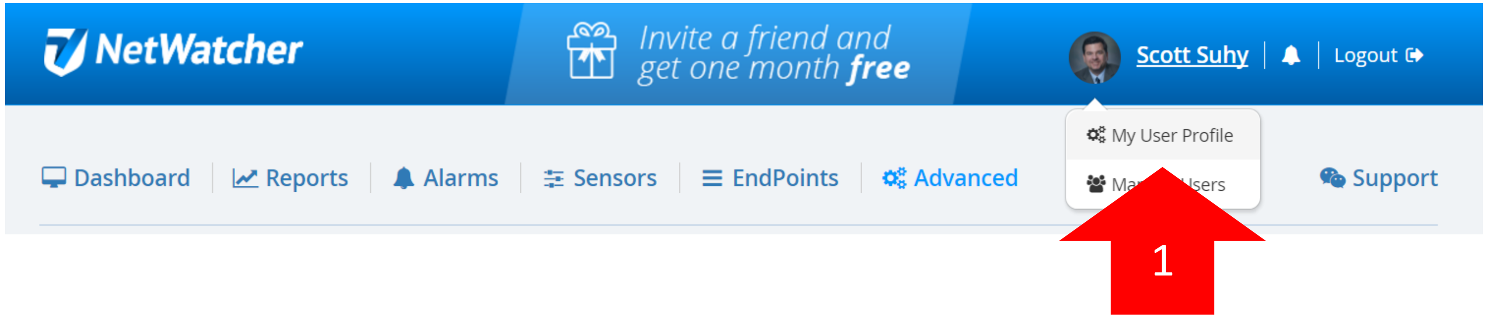
The NetWatcher Vulnerability Scanner

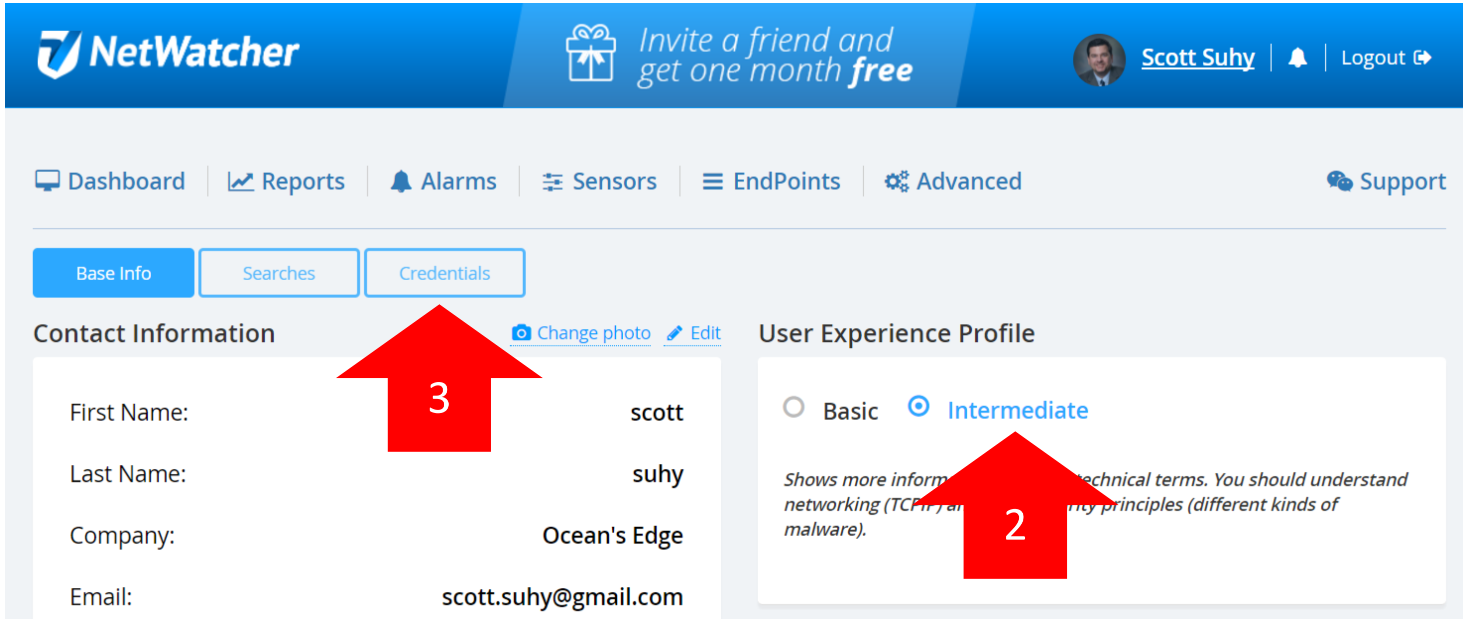
NETWATCHER™

info@netwatcher.com

Scanning & the Customer Portal

Update Your User Profile (1)





Contact Information

First Name: scott

Last Name: suhy

Company: Ocean's Edge

Email: scott.suhy@gmail.com

User Experience Profile

○ Basic ● Intermediate

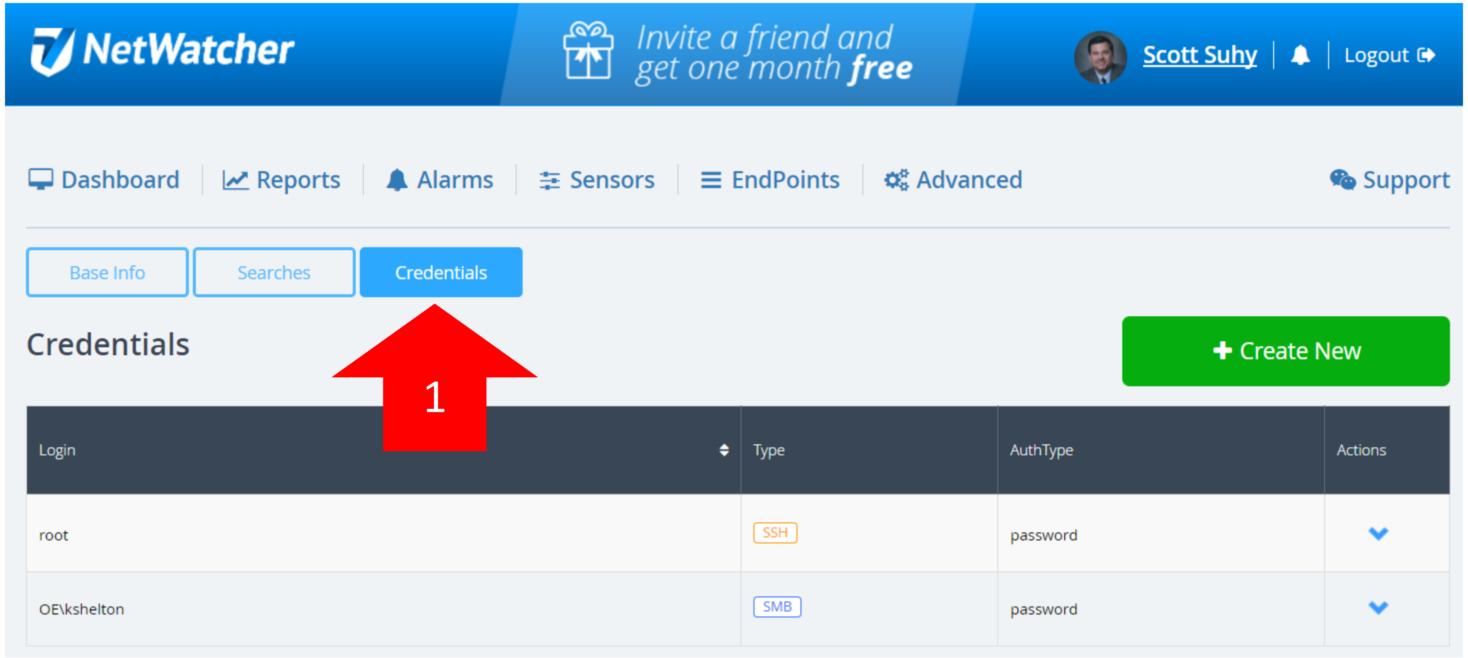
Shows more inform… echnical terms. You should understand networking (TCP/IP) a… rity principles (different kinds of malware).

1. Once you login to the NetWatcher Customer Portal, choose your Name in the upper right corner of the screen and choose “My User Profile”.

2. The NetWatcher Scanner is under the ‘Advanced’ tab in the Customer Portal. In order to enable the ‘Advanced’ tab the user needs to be setup with an ‘Intermediate’ Profile.

3. Add scanning credentials if your ‘Full and Fast’ scans are going to be credentialized.

Update Your User Profile (2) - Credentials



Credentials

Login	Type	AuthType	Actions
root	SSH	password	⌄
OE\kshelton	SMB	password	⌄

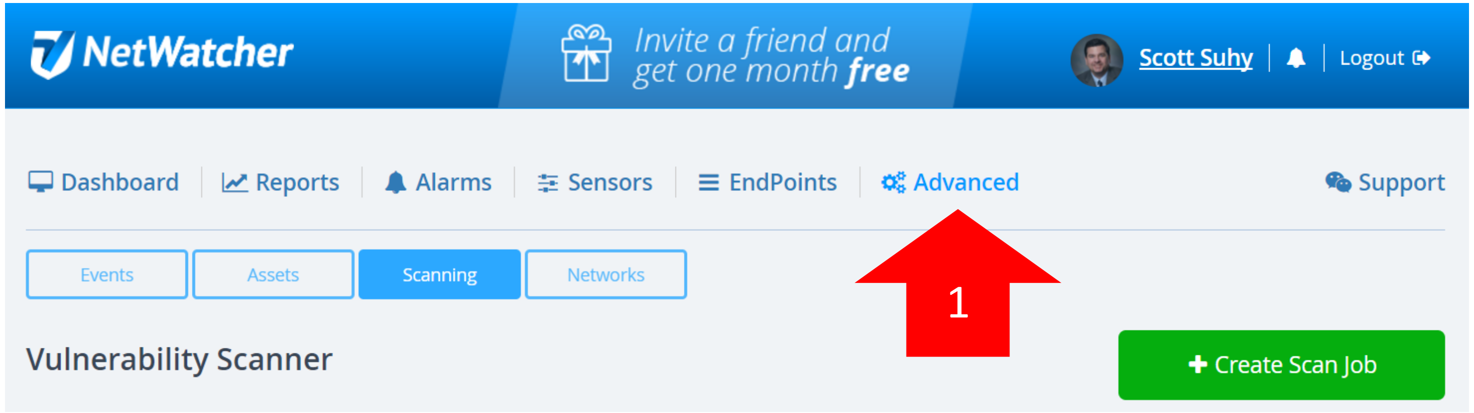
1. Its always best to run a ‘Full and Fast’ scan using login credentials.

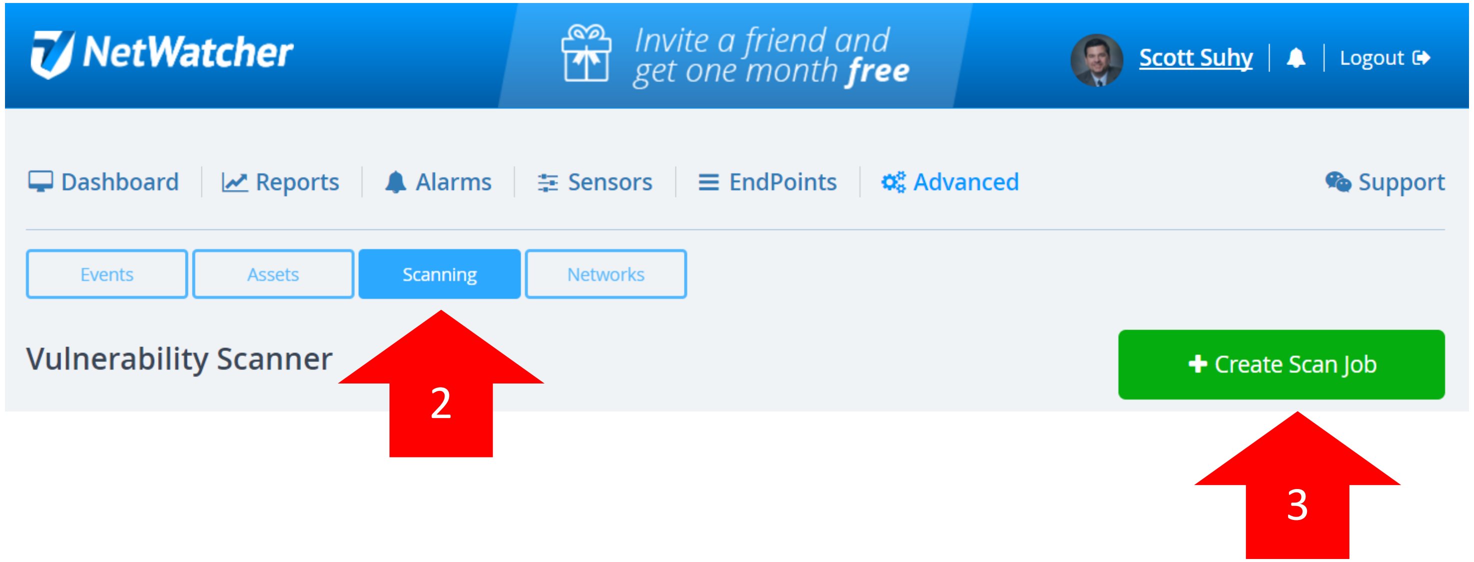
For Windows, choose SMB and use

DOMAIN\name

As the format.

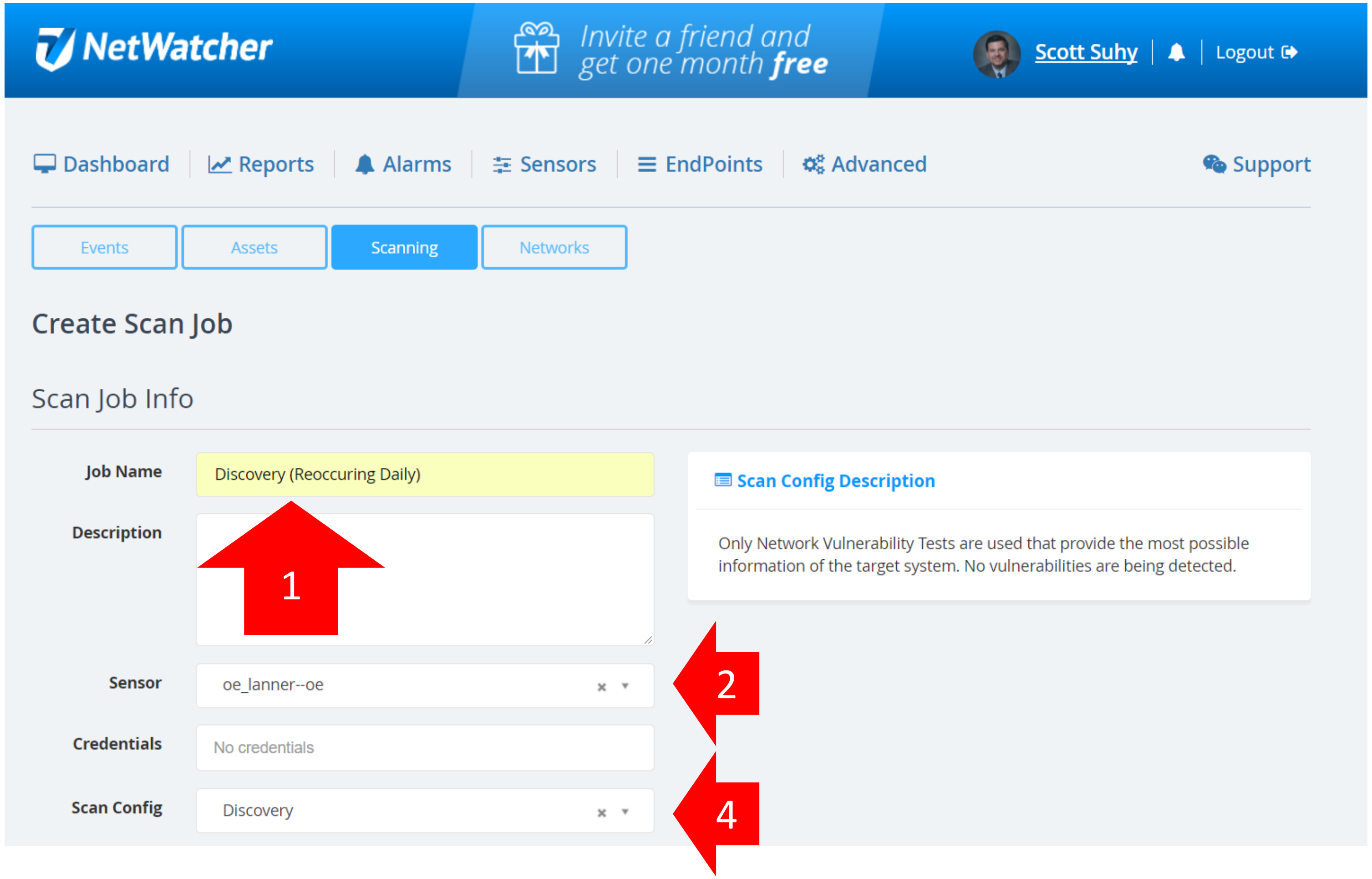
Update Your User Profile (3)





1. Under the 'Advanced' tab
2. You will find the 'Scanning' Button
3. The green 'Create Scan job' allows you to setup the scans

Setting Up The "Discovery" Scan (1)



Create Scan Job

Scan Job Info

Job Name: Discovery (Reoccuring Daily)

Description:

Sensor: oe_lanner--oe

Credentials: No credentials

Scan Config: Discovery

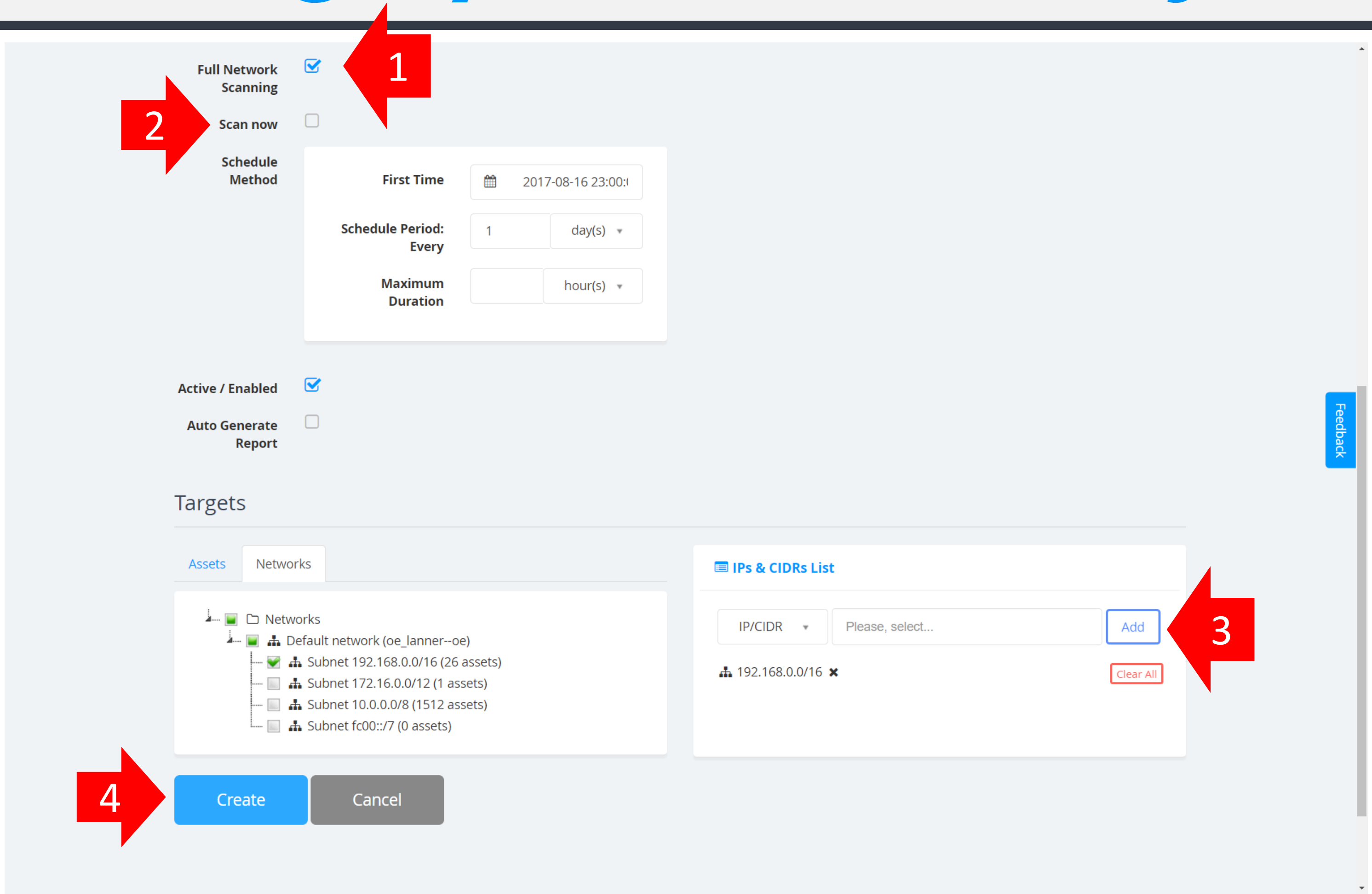
Scan Config Description

Only Network Vulnerability Tests are used that provide the most possible information of the target system. No vulnerabilities are being detected.

The 'Discovery' Scan will find all the assets on the network. This is necessary to know if new assets have appeared on the network since the last time the scan ran.

1. *Name the job 'Discovery (Reoccurring Daily)*
2. *Choose the sensor name*
3. *<u>Do not use</u> any credentials*
4. *Choose the 'Discovery' Scan Config*

Setting Up The "Discovery" Scan (2)



Full Network Scanning ☑

Scan now □

Schedule Method

First Time: 2017-08-16 23:00:(

Schedule Period: Every 1 day(s)

Maximum Duration: hour(s)

Active / Enabled ☑

Auto Generate Report □

Targets

Assets | Networks

- Networks
  - Default network (oe_lanner--oe)
    - ☑ Subnet 192.168.0.0/16 (26 assets)
    - □ Subnet 172.16.0.0/12 (1 assets)
    - □ Subnet 10.0.0.0/8 (1512 assets)
    - □ Subnet fc00::/7 (0 assets)

IPs & CIDRs List

IP/CIDR | Please, select... | Add

192.168.0.0/16 ✖

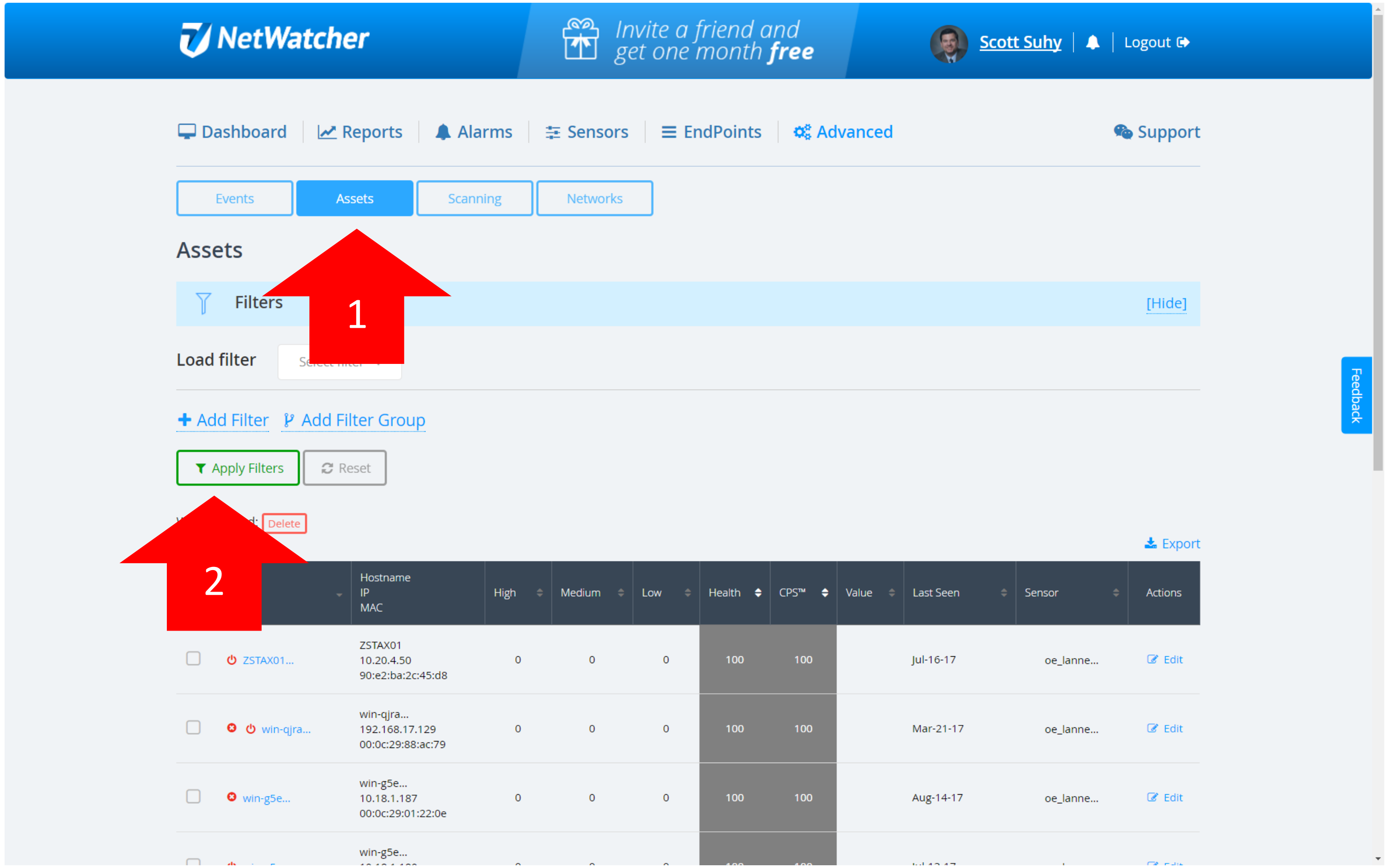
Clear All

Create | Cancel

Page down.

1. *Check Full Network Scanning – this allows us to review the entire IP range.*
2. *Uncheck 'Scan now' and schedule the scan for sometime late in the evening when there is the most downtime on the network. Schedule the scan to run every day.*
3. *Add the IP/CIDR range in to scan*
4. *Click the 'Create' button*

The Discovery Scan Will Populate The Assets



Assets

Filters [Hide]

Load filter Select filter

+ Add Filter   Add Filter Group

Apply Filters   Reset

Delete

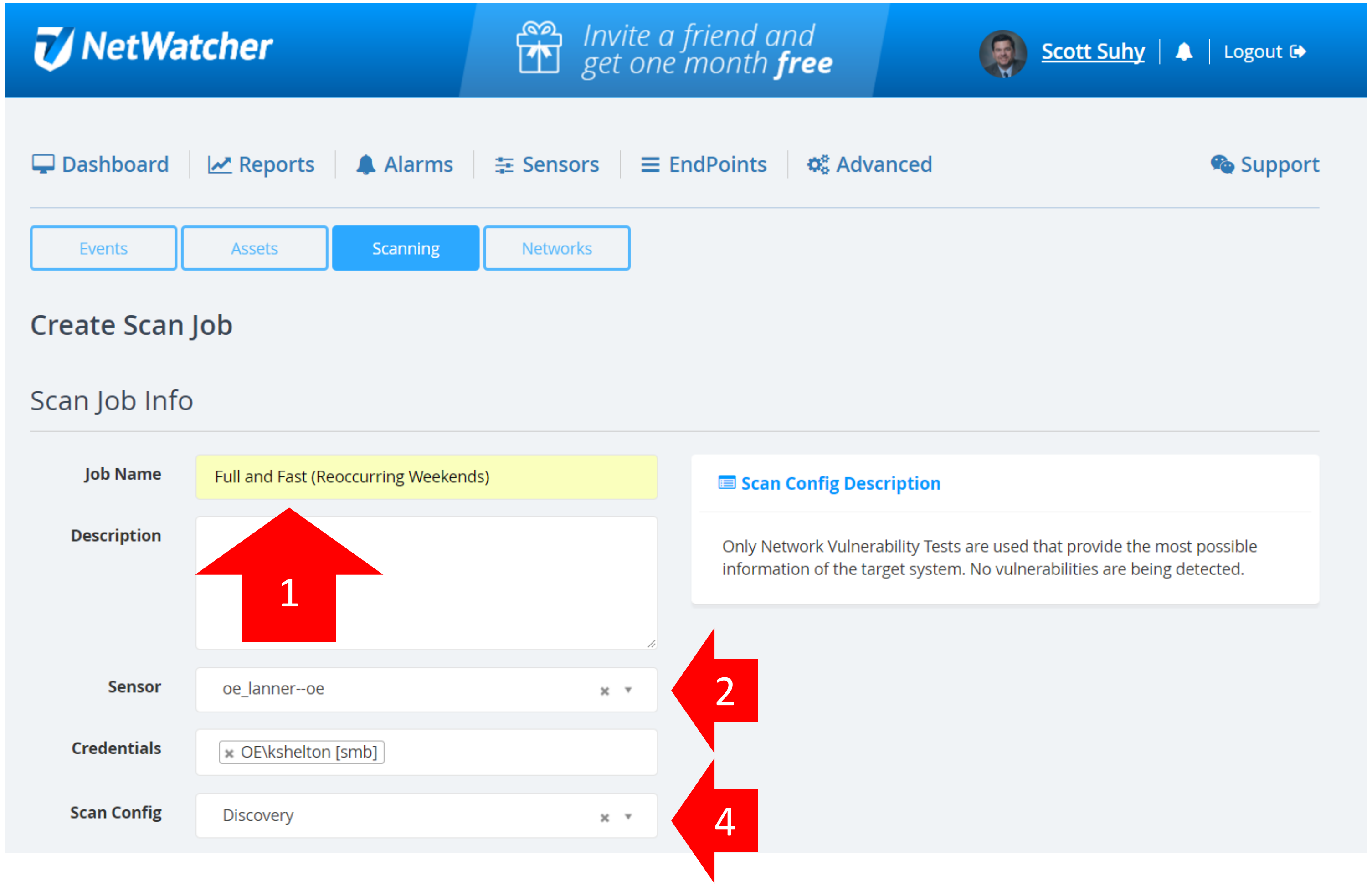
Export

		Hostname IP MAC	High	Medium	Low	Health	CPS™	Value	Last Seen	Sensor	Actions
□	ZSTAX01...	ZSTAX01 10.20.4.50 90:e2:ba:2c:45:d8	0	0	0	100	100		Jul-16-17	oe_lanne...	Edit
□	win-qjra...	win-qjra... 192.168.17.129 00:0c:29:88:ac:79	0	0	0	100	100		Mar-21-17	oe_lanne...	Edit
□	win-g5e...	win-g5e... 10.18.1.187 00:0c:29:01:22:0e	0	0	0	100	100		Aug-14-17	oe_lanne...	Edit
□		win-g5e...									

The ‘Discovery’ scan populates the asset database. If you want to review all the assets simply:

1. *Choose the ‘Assets’ button and then*
2. *Press the ‘Apply Filter’ button*

Setting Up The "Full and Fast" Scan (1)



Create Scan Job

Scan Job Info

Job Name: Full and Fast (Reoccurring Weekends)

Description:

Sensor: oe_lanner--oe

Credentials: OE\kshelton [smb]

Scan Config: Discovery

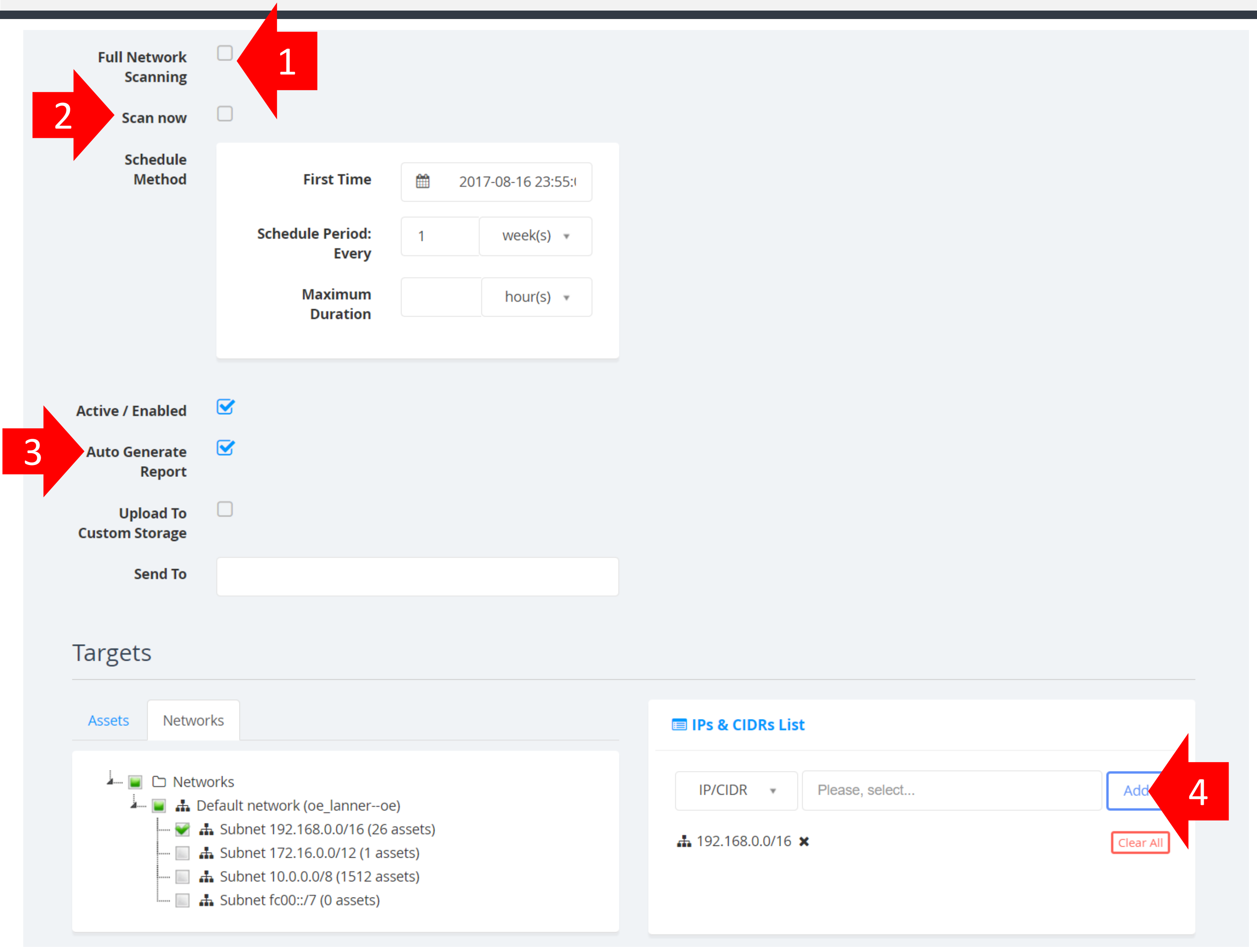
Scan Config Description

Only Network Vulnerability Tests are used that provide the most possible information of the target system. No vulnerabilities are being detected.

The 'Full and Fast' Scan will send Network Vulnerability Tests (NVTs) to the assets on the network. This is necessary to determine what vulnerabilities exist on the network.

1. *Name the job 'Full and Fast (Reoccurring Weekends)'*
2. *Choose the sensor name*
3. *Add credentials if necessary – This sends additional NVTs that require user credentials to test the asset*
4. *Choose the 'Full and Fast' Scan Config*

Setting Up The “Full and Fast” Scan (2)



Full Network Scanning □

Scan now □

Schedule Method

First Time 2017-08-16 23:55:(

Schedule Period: Every 1 week(s)

Maximum Duration hour(s)

Active / Enabled ☑

Auto Generate Report ☑

Upload To Custom Storage □

Send To

Targets

Assets | Networks

- Networks
  - Default network (oe_lanner--oe)
    - ☑ Subnet 192.168.0.0/16 (26 assets)
    - □ Subnet 172.16.0.0/12 (1 assets)
    - □ Subnet 10.0.0.0/8 (1512 assets)
    - □ Subnet fc00::/7 (0 assets)

IPs & CIDRs List

IP/CIDR | Please, select... | Add

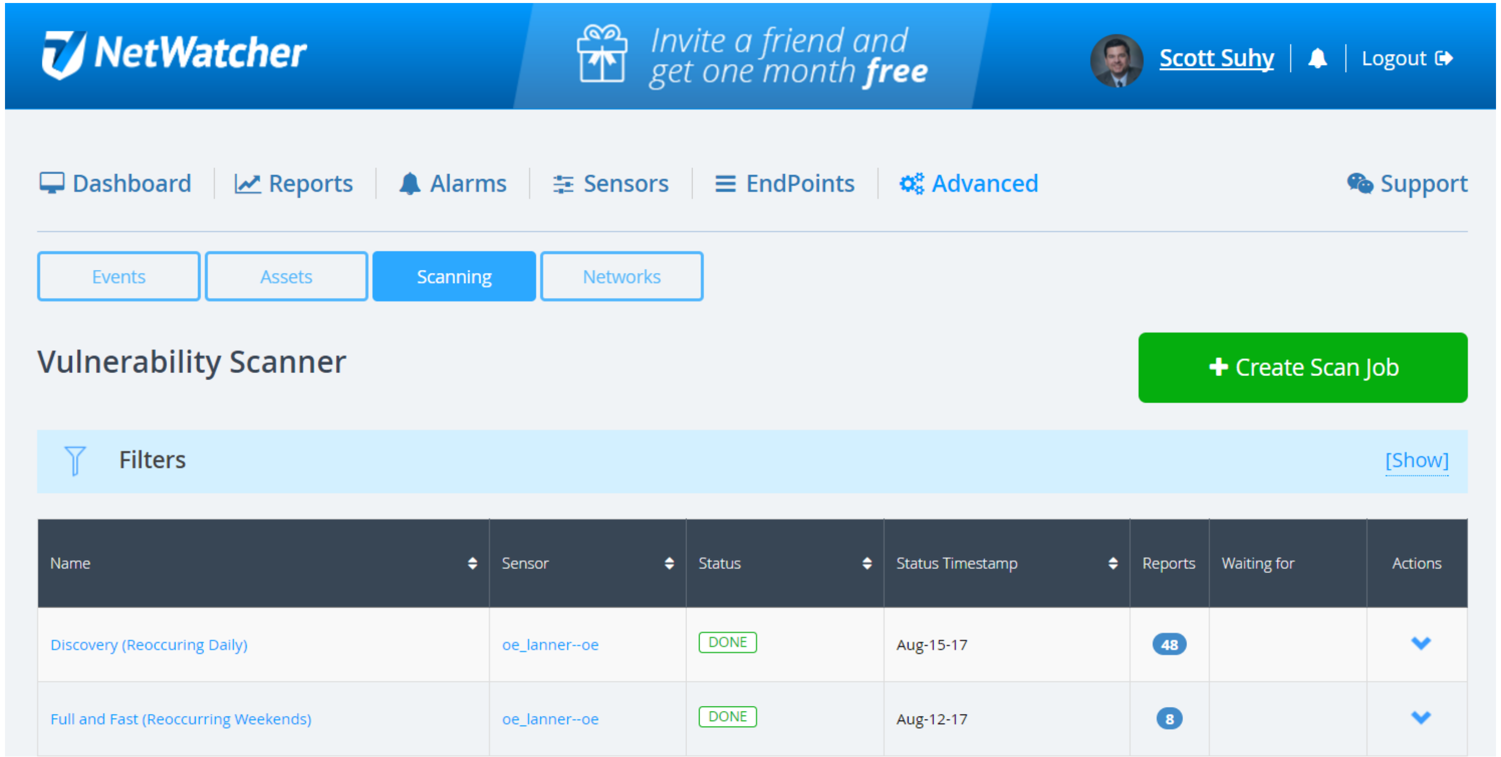
192.168.0.0/16 ✖

Clear All

Page down.

1. ***<u>Un-Check</u>*** *Full Network Scanning – this scan will use the assets in the database.*
2. *Uncheck ‘Scan now’ and schedule the scan for sometime late in the evening at least an hour after the ‘Discovery’ scan when there is the most downtime on the network. Schedule the scan to run every week.*
3. *Choose to Auto Generate Report if you want a PDF to be available for the customer. Note that you can also put in an email address in the ‘Send To’ field.*
4. *Add the IP/CIDR range in to scan*
5. *Click the ‘Create’ button*

Reviewing The Scan After It's Complete (1)



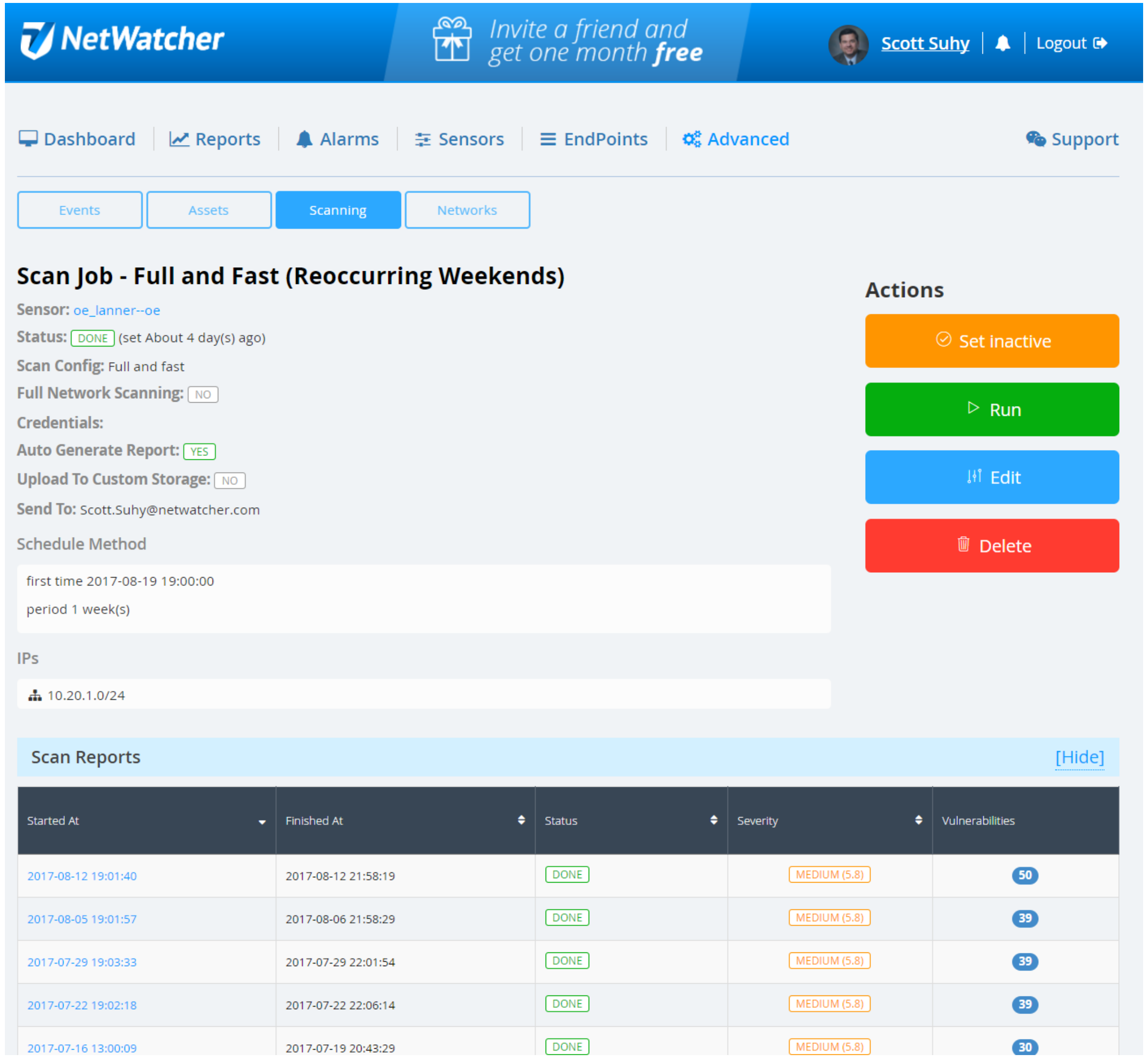
Vulnerability Scanner

Name	Sensor	Status	Status Timestamp	Reports	Waiting for	Actions
Discovery (Reoccuring Daily)	oe_lanner--oe	DONE	Aug-15-17	48		
Full and Fast (Reoccurring Weekends)	oe_lanner--oe	DONE	Aug-12-17	8		

Press the 'Scanning' button again and you will see both scheduled Scans as well as how many times they have been run (under the 'Reports' column). If you click on the # in the 'Reports' Column for the 'Full and Fast' scan you will be taken to the detail.

In this example, the 'Full and Fast' scan has run 8 times.

Reviewing The Scan After It's Complete (2)



Scan Job - Full and Fast (Reoccurring Weekends)

Sensor: oe_lanner--oe

Status: DONE (set About 4 day(s) ago)

Scan Config: Full and fast

Full Network Scanning: NO

Credentials:

Auto Generate Report: YES

Upload To Custom Storage: NO

Send To: Scott.Suhy@netwatcher.com

Schedule Method

first time 2017-08-19 19:00:00

period 1 week(s)

IPs

10.20.1.0/24

Scan Reports [Hide]

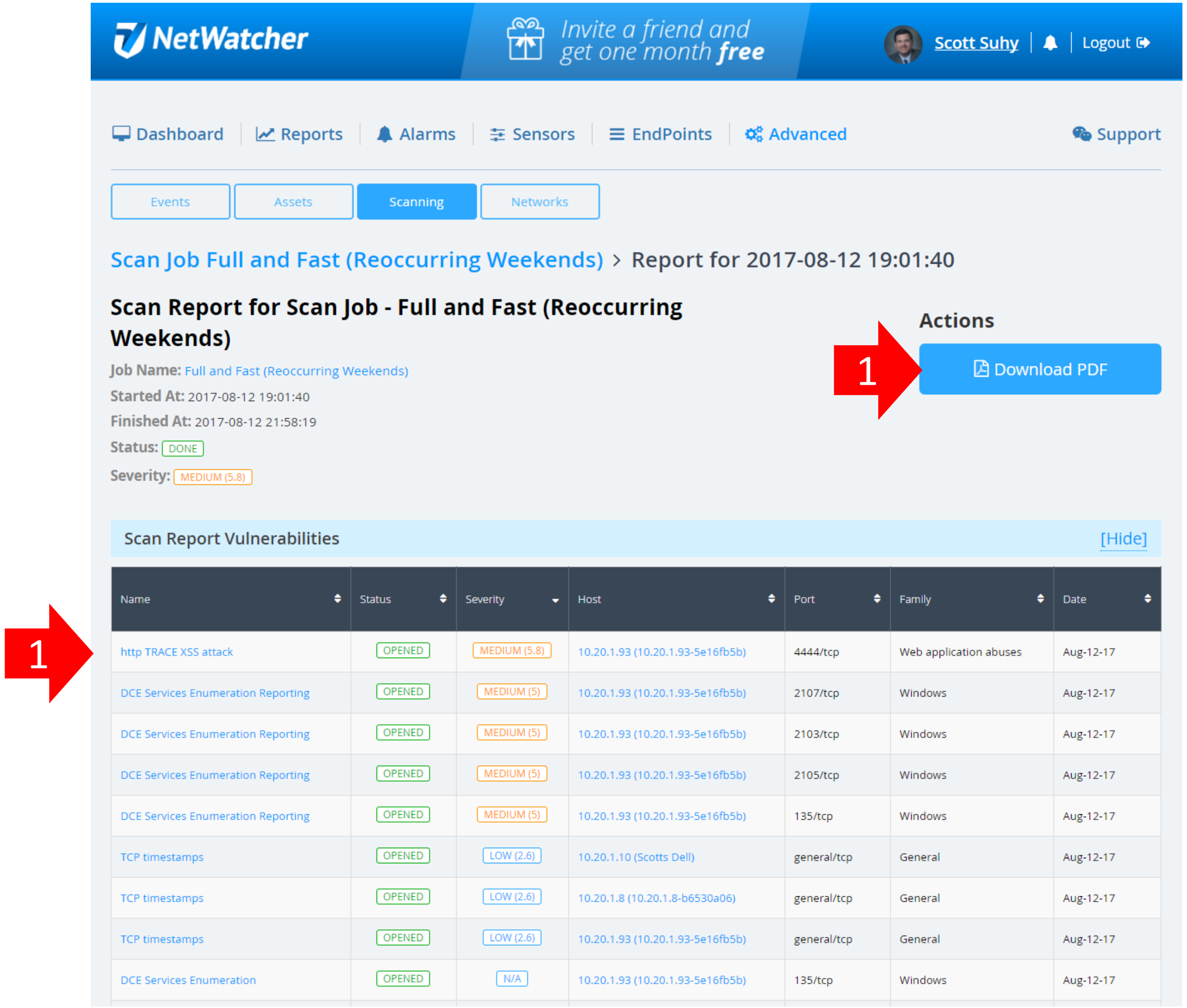
Started At	Finished At	Status	Severity	Vulnerabilities
2017-08-12 19:01:40	2017-08-12 21:58:19	DONE	MEDIUM (5.8)	50
2017-08-05 19:01:57	2017-08-06 21:58:29	DONE	MEDIUM (5.8)	39
2017-07-29 19:03:33	2017-07-29 22:01:54	DONE	MEDIUM (5.8)	39
2017-07-22 19:02:18	2017-07-22 22:06:14	DONE	MEDIUM (5.8)	39
2017-07-16 13:00:09	2017-07-19 20:43:29	DONE	MEDIUM (5.8)	30

The Scan detail page will show you each scheduled scan and what the maximum severity found in the scan as well as the date and time that the scan started and stopped as well as the number of vulnerabilities found.

The number of vulnerabilities from each scan can be found in the 'Vulnerabilities' column.

If you click on the # you will be taken to a list of those vulnerabilities.

Reviewing The Scan After It’s Complete (3)



Scan Job Full and Fast (Reoccurring Weekends) > Report for 2017-08-12 19:01:40

Scan Report for Scan Job - Full and Fast (Reoccurring Weekends)

Actions

Job Name: Full and Fast (Reoccurring Weekends)

Started At: 2017-08-12 19:01:40

Finished At: 2017-08-12 21:58:19

Status: DONE

Severity: MEDIUM (5.8)

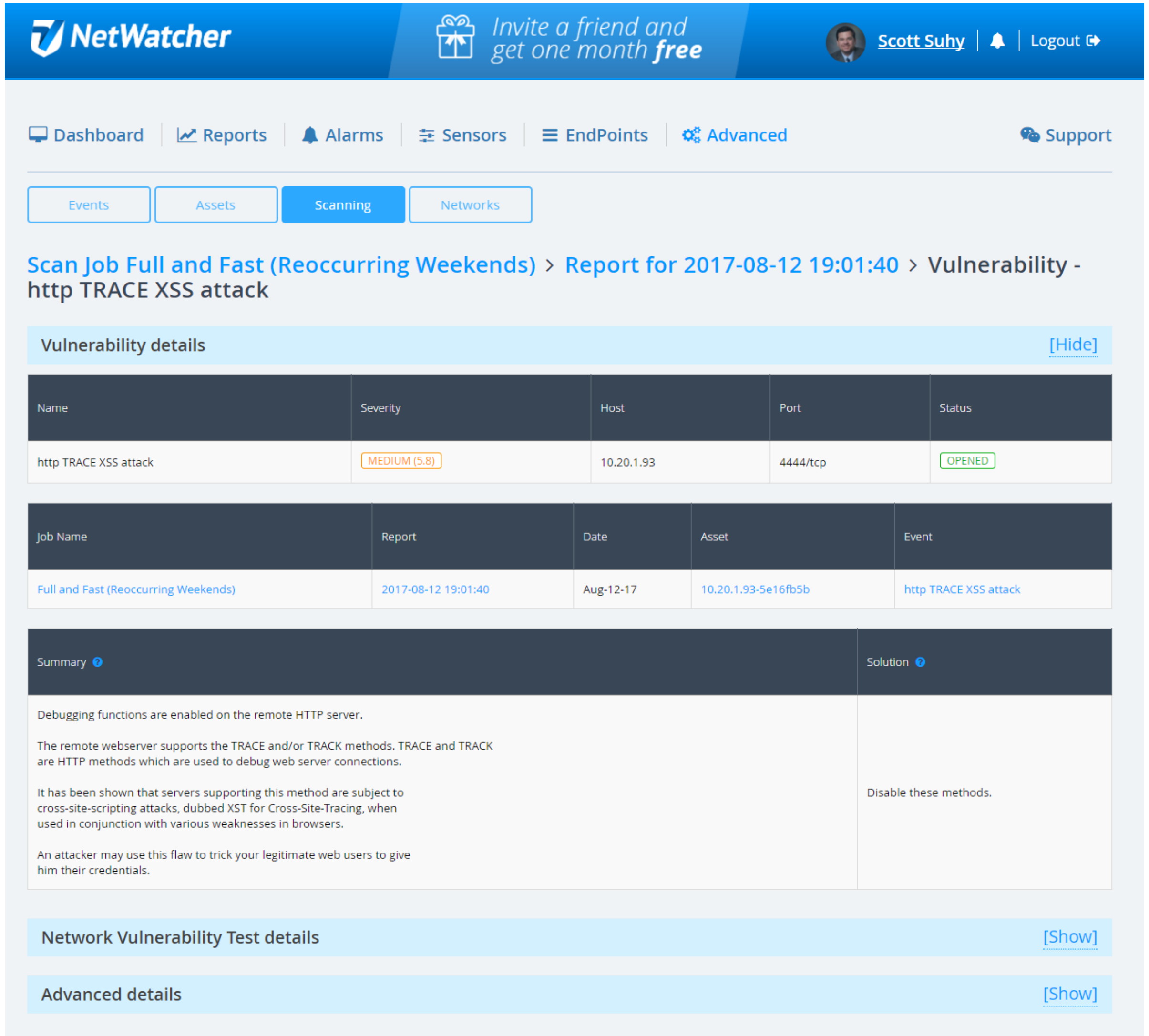
Scan Report Vulnerabilities [Hide]

Name	Status	Severity	Host	Port	Family	Date
http TRACE XSS attack	OPENED	MEDIUM (5.8)	10.20.1.93 (10.20.1.93-5e16fb5b)	4444/tcp	Web application abuses	Aug-12-17
DCE Services Enumeration Reporting	OPENED	MEDIUM (5)	10.20.1.93 (10.20.1.93-5e16fb5b)	2107/tcp	Windows	Aug-12-17
DCE Services Enumeration Reporting	OPENED	MEDIUM (5)	10.20.1.93 (10.20.1.93-5e16fb5b)	2103/tcp	Windows	Aug-12-17
DCE Services Enumeration Reporting	OPENED	MEDIUM (5)	10.20.1.93 (10.20.1.93-5e16fb5b)	2105/tcp	Windows	Aug-12-17
DCE Services Enumeration Reporting	OPENED	MEDIUM (5)	10.20.1.93 (10.20.1.93-5e16fb5b)	135/tcp	Windows	Aug-12-17
TCP timestamps	OPENED	LOW (2.6)	10.20.1.10 (Scotts Dell)	general/tcp	General	Aug-12-17
TCP timestamps	OPENED	LOW (2.6)	10.20.1.8 (10.20.1.8-b6530a06)	general/tcp	General	Aug-12-17
TCP timestamps	OPENED	LOW (2.6)	10.20.1.93 (10.20.1.93-5e16fb5b)	general/tcp	General	Aug-12-17
DCE Services Enumeration	OPENED	N/A	10.20.1.93 (10.20.1.93-5e16fb5b)	135/tcp	Windows	Aug-12-17

The list of vulnerabilities will be found on this scan details page.

1. *You can also download a PDF of all of these vulnerabilities from this page.*
2. *If you click on the name of the vulnerability you will be taken to the derailed explanation of that issue.*

Reviewing The Scan After It's Complete (4)
Reviewing A Vulnerability Event (page 1)



Scan Job Full and Fast (Reoccurring Weekends) > Report for 2017-08-12 19:01:40 > Vulnerability - http TRACE XSS attack

Vulnerability details [Hide]

Name	Severity	Host	Port	Status
http TRACE XSS attack	MEDIUM (5.8)	10.20.1.93	4444/tcp	OPENED

Job Name	Report	Date	Asset	Event
Full and Fast (Reoccurring Weekends)	2017-08-12 19:01:40	Aug-12-17	10.20.1.93-5e16fb5b	http TRACE XSS attack

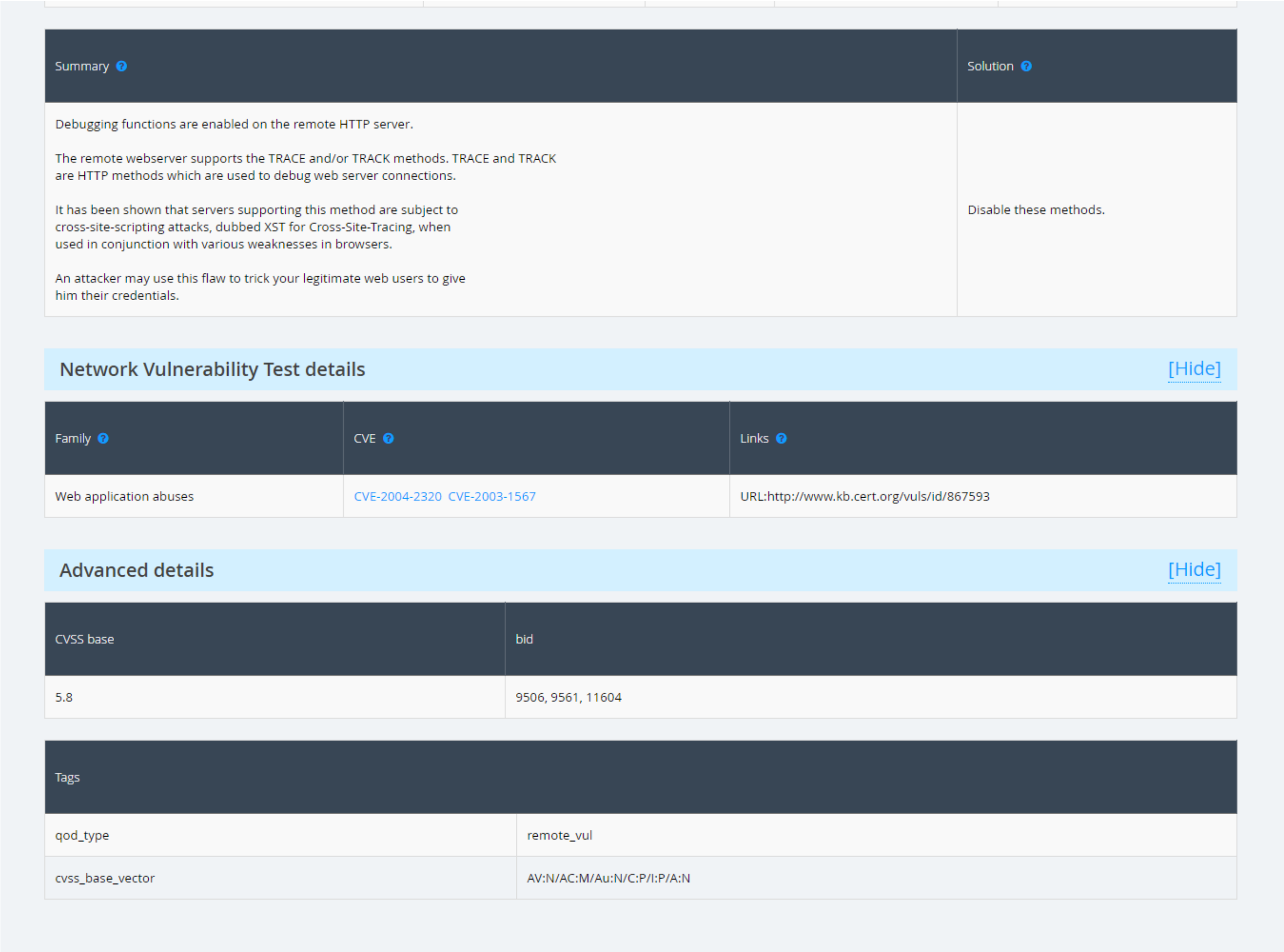
Summary	Solution
Debugging functions are enabled on the remote HTTP server. The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.	Disable these methods.

Network Vulnerability Test details [Show]

Advanced details [Show]

The Vulnerability detail for this issue and it's Summary and Solution can be found on this page.

Reviewing The Scan After It's Complete (5)
Reviewing A Vulnerability Event (page 2)



Summary	Solution
Debugging functions are enabled on the remote HTTP server. The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.	Disable these methods.

Network Vulnerability Test details

Family	CVE	Links
Web application abuses	CVE-2004-2320 CVE-2003-1567	URL:http://www.kb.cert.org/vuls/id/867593

Advanced details

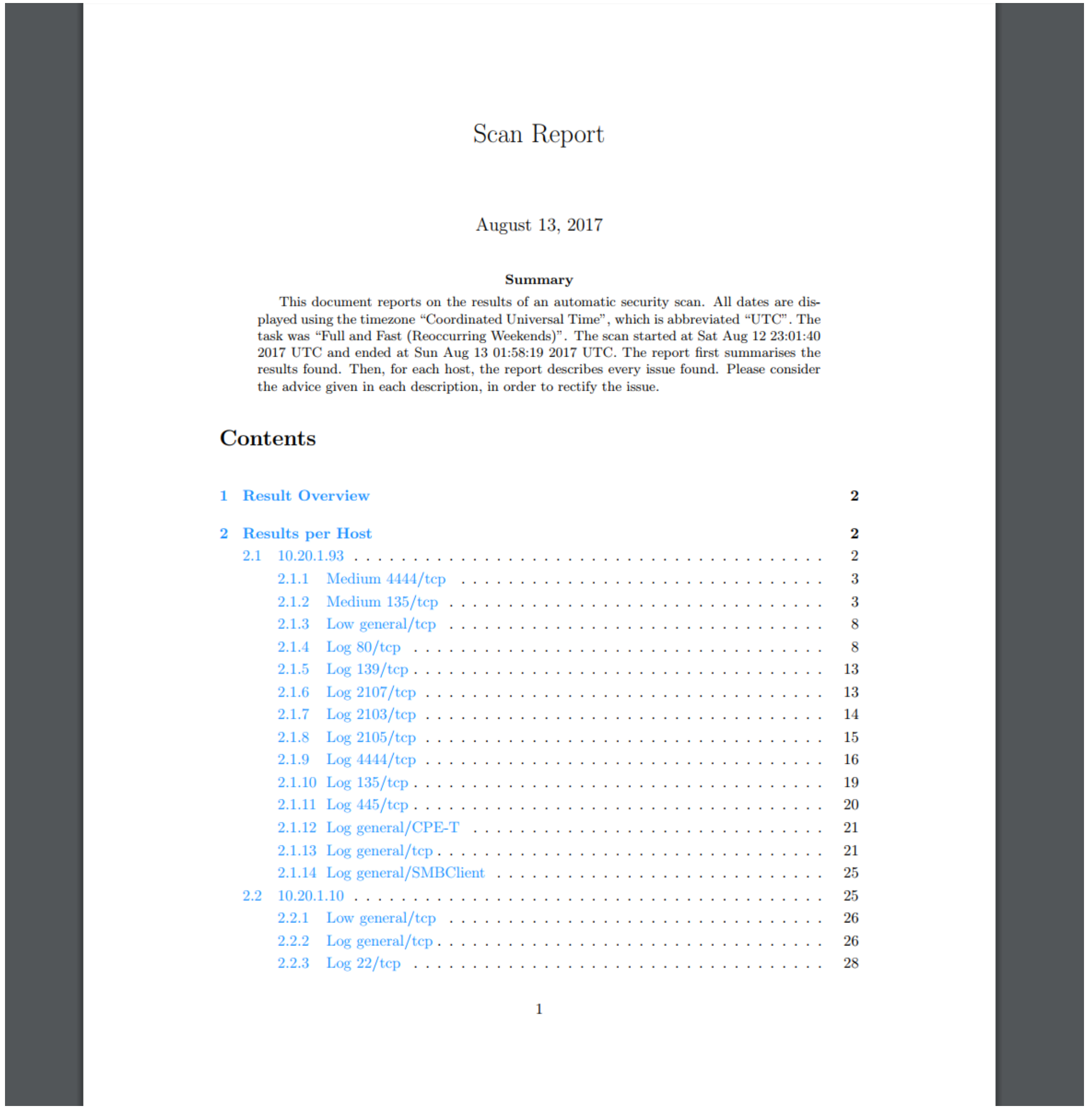
CVSS base	bid
5.8	9506, 9561, 11604

Tags	
qod_type	remote_vul
cvss_base_vector	AV:N/AC:M/Au:N/C:P/I:P/A:N

Page down if you want to see what CVE associated with this vulnerability and a link to it in the CVE database.

You can also click on the 'Advanced details' to see the CVSS base and Tags associated with the vulnerability.

Reviewing The Scan After It’s Complete (6)
Reviewing the Report



Scan Report

August 13, 2017

Summary

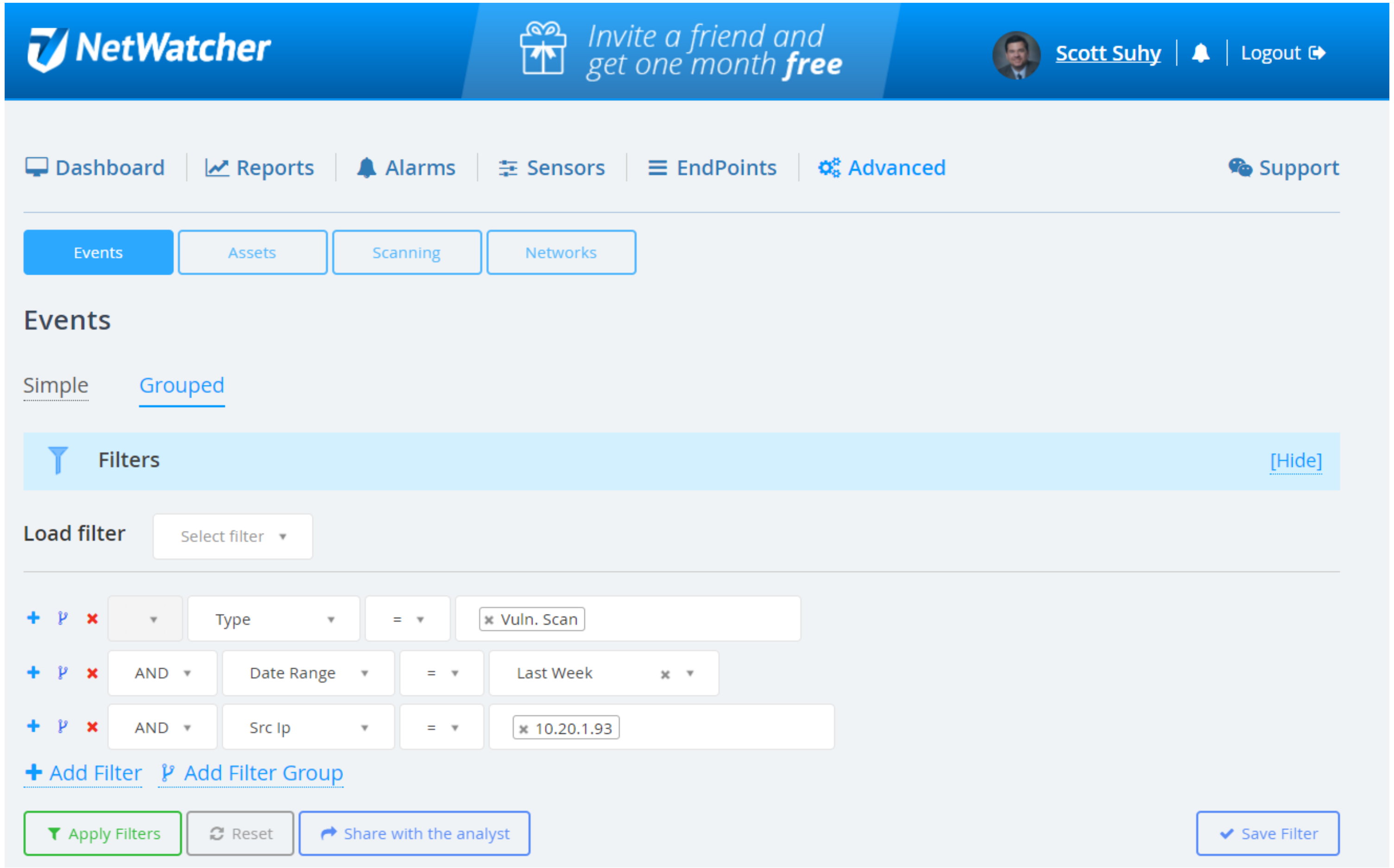
This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Full and Fast (Reoccurring Weekends)”. The scan started at Sat Aug 12 23:01:40 2017 UTC and ended at Sun Aug 13 01:58:19 2017 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1

If you did choose to create and download a PDF report for the customer you will find the format easy to read and sorted by vulnerability severity with an easy to navigate table of contents.

NetWatcher Advanced – Event Detail 1 of 2



Events

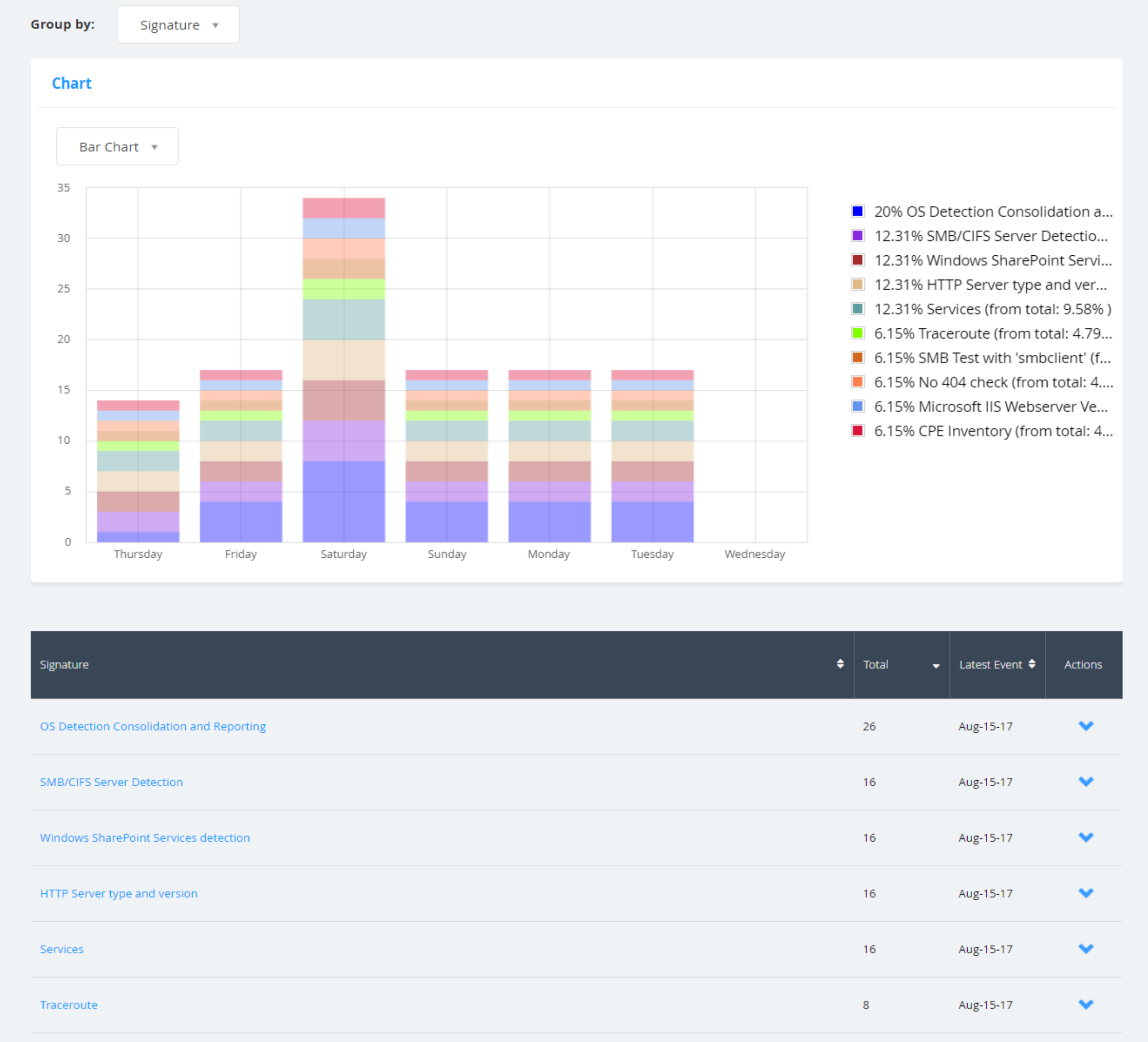
Load filter: Select filter

	Type	=	Vuln. Scan
AND	Date Range	=	Last Week
AND	Src Ip	=	10.20.1.93

If you wanted to look for a specific vulnerability you can always go to the ‘Events’ button under the ‘Advanced’ tab and do a query. Grouped queries consolidate all of the vulnerabilities of a certain type.

In this example we are looking for all the vulnerabilities from last weeks report on IP address 10.20.1.93

NetWatcher Advanced – Event Detail 1 of 2



Group by: Signature ▾

Chart

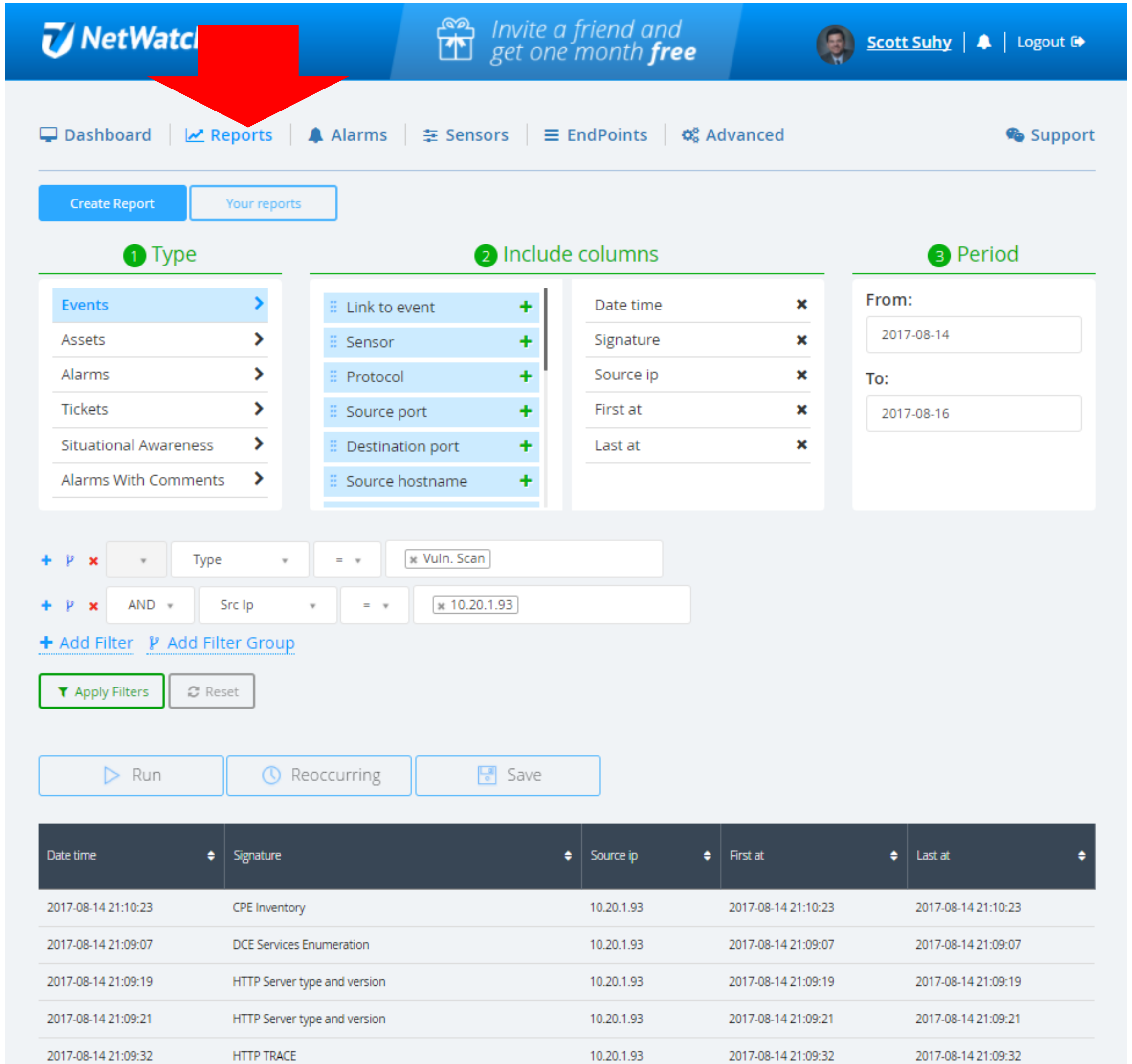
Bar Chart ▾

■ 20% OS Detection Consolidation a...
■ 12.31% SMB/CIFS Server Detectio...
■ 12.31% Windows SharePoint Servi...
■ 12.31% HTTP Server type and ver...
■ 12.31% Services (from total: 9.58%)
■ 6.15% Traceroute (from total: 4.79...
■ 6.15% SMB Test with 'smbclient' (f...
■ 6.15% No 404 check (from total: 4....
■ 6.15% Microsoft IIS Webserver Ve...
■ 6.15% CPE Inventory (from total: 4...

Signature	Total	Latest Event	Actions
OS Detection Consolidation and Reporting	26	Aug-15-17	⌄
SMB/CIFS Server Detection	16	Aug-15-17	⌄
Windows SharePoint Services detection	16	Aug-15-17	⌄
HTTP Server type and version	16	Aug-15-17	⌄
Services	16	Aug-15-17	⌄
Traceroute	8	Aug-15-17	⌄

If you page down you can also Chart the vulnerabilities and see a list of them (you can click through this detail as well).

Filtered Reporting



1 Type

- Events
- Assets
- Alarms
- Tickets
- Situational Awareness
- Alarms With Comments

2 Include columns

- Link to event +
- Sensor +
- Protocol +
- Source port +
- Destination port +
- Source hostname +

- Date time ×
- Signature ×
- Source ip ×
- First at ×
- Last at ×

3 Period

From: 2017-08-14

To: 2017-08-16

Type = × Vuln. Scan

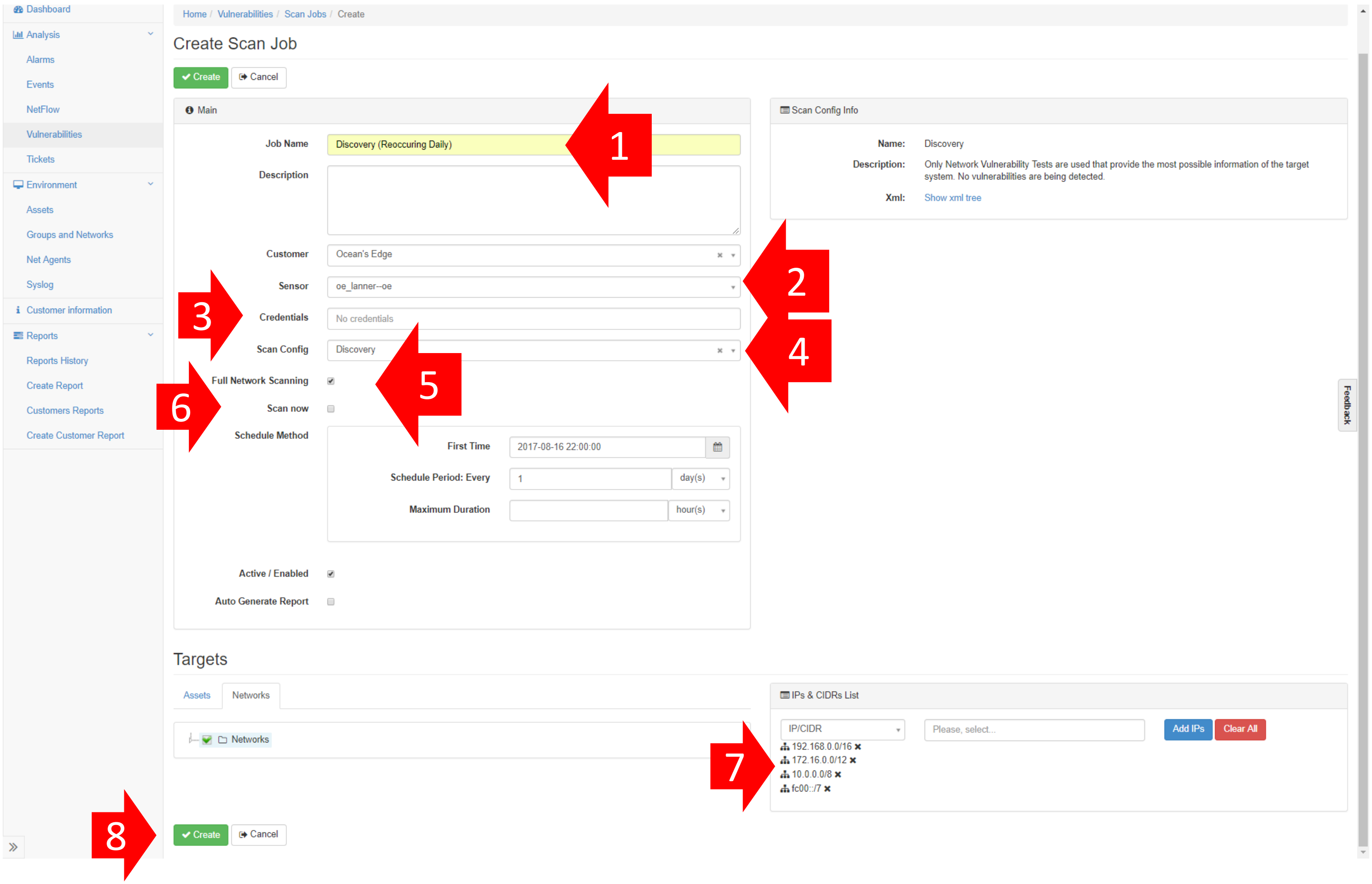
AND Src Ip = × 10.20.1.93

Date time	Signature	Source ip	First at	Last at
2017-08-14 21:10:23	CPE Inventory	10.20.1.93	2017-08-14 21:10:23	2017-08-14 21:10:23
2017-08-14 21:09:07	DCE Services Enumeration	10.20.1.93	2017-08-14 21:09:07	2017-08-14 21:09:07
2017-08-14 21:09:19	HTTP Server type and version	10.20.1.93	2017-08-14 21:09:19	2017-08-14 21:09:19
2017-08-14 21:09:21	HTTP Server type and version	10.20.1.93	2017-08-14 21:09:21	2017-08-14 21:09:21
2017-08-14 21:09:32	HTTP TRACE	10.20.1.93	2017-08-14 21:09:32	2017-08-14 21:09:32

If you want to Report on specific vulnerabilities in a way that the PDF doesn’t support, you can go to the ‘Reports’ tab and do a query and ‘Run’ the report and create either a CSV or a PDF.

Scanning & the Analyst/MSP Portal

Setting Up The "Discovery" Scan (1)



Create Scan Job

Main

Job Name: Discovery (Reoccuring Daily)

Description:

Customer: Ocean's Edge

Sensor: oe_lanner--oe

Credentials: No credentials

Scan Config: Discovery

Full Network Scanning ☑

Scan now ☐

Schedule Method

First Time: 2017-08-16 22:00:00

Schedule Period: Every 1 day(s)

Maximum Duration: hour(s)

Active / Enabled ☑

Auto Generate Report ☐

Scan Config Info

Name: Discovery

Description: Only Network Vulnerability Tests are used that provide the most possible information of the target system. No vulnerabilities are being detected.

Xml: Show xml tree

Targets

Assets | Networks

☑ Networks

IPs & CIDRs List

IP/CIDR | Please, select... | Add IPs | Clear All

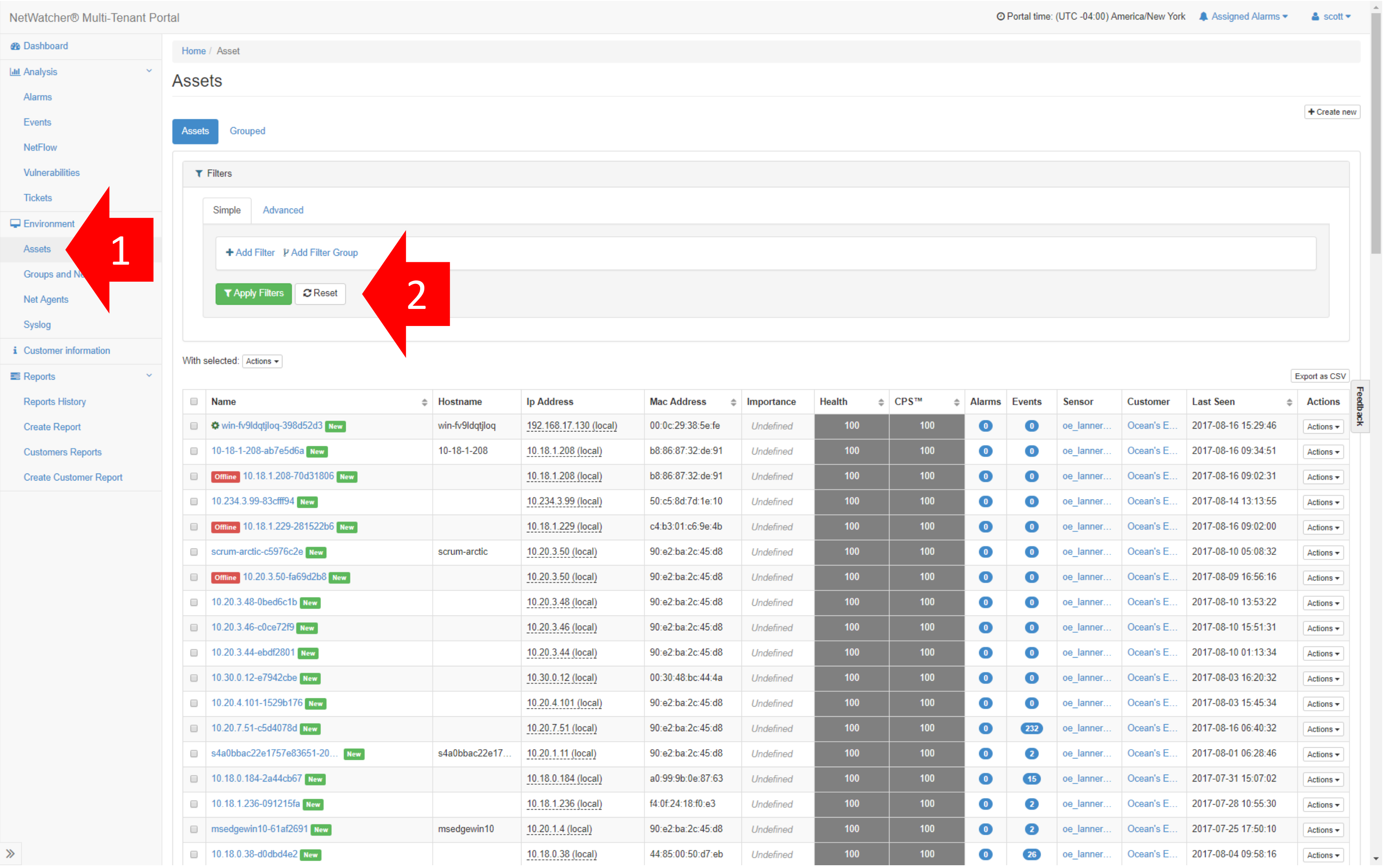
- 192.168.0.0/16 ✖
- 172.16.0.0/12 ✖
- 10.0.0.0/8 ✖
- fc00::/7 ✖

The 'Discovery' Scan will find all the assets on the network. This is necessary to know if new assets have appeared on the network since the last time the scan ran.

1. *Name the job 'Discovery (Reoccurring Daily)*
2. *Choose the sensor name*
3. *<u>Do not use</u> any credentials*
4. *Choose the 'Discovery' Scan Config*
5. *Check Full Network Scanning – this allows us to review the entire IP range.*
6. *Uncheck 'Scan now' and schedule the scan for sometime late in the evening when there is the most downtime on the network. Schedule the scan to run every day.*
7. *Add the IP/CIDR range in to scan*
8. *Click the 'Create' button*

NetWatcher

The Discovery Scan Will Populate The Assets



NetWatcher® Multi-Tenant Portal

Portal time: (UTC -04:00) America/New York · Assigned Alarms ▾ · scott ▾

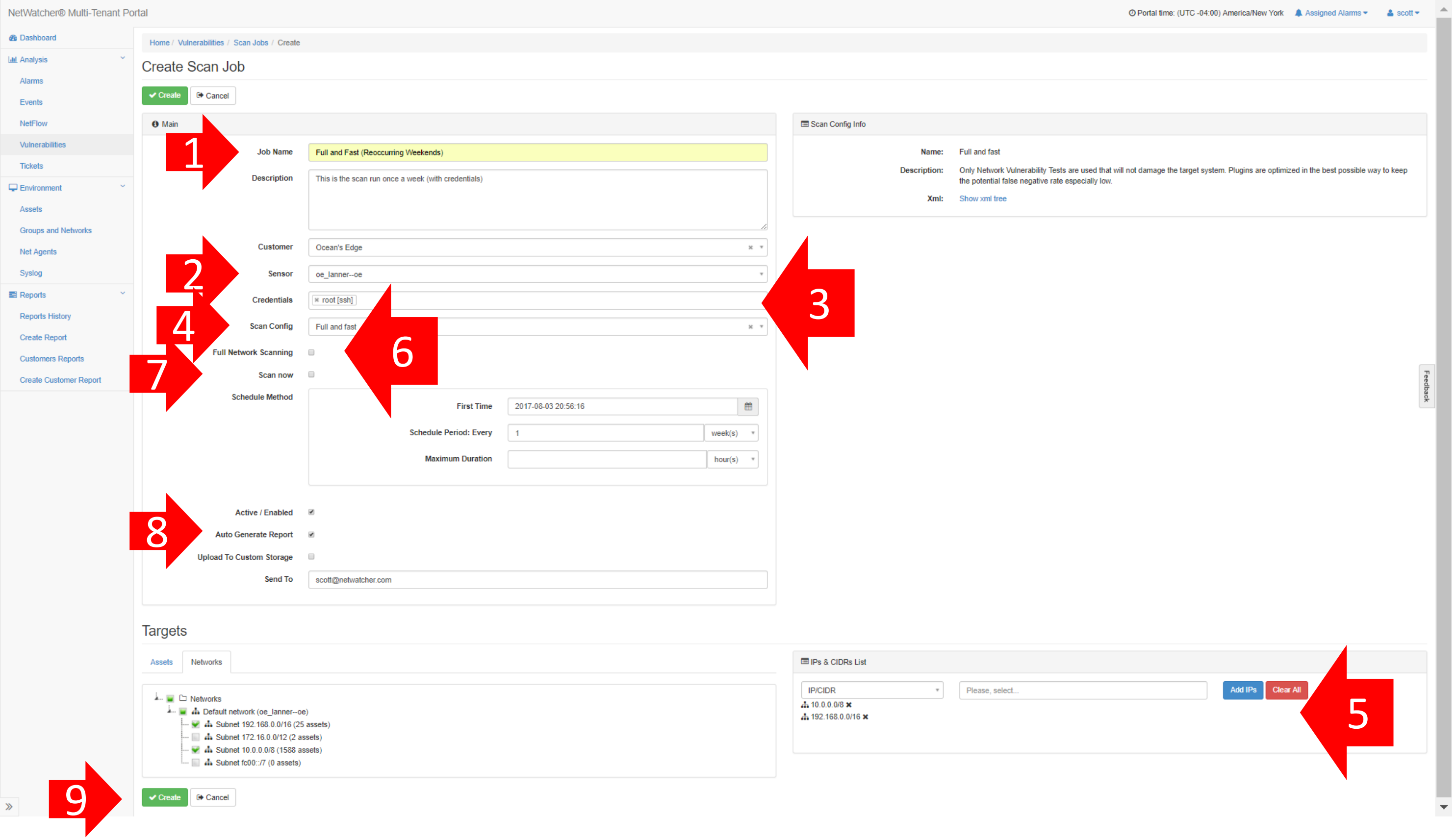
Assets

□	Name	Hostname	Ip Address	Mac Address	Importance	Health	CPS™	Alarms	Events	Sensor	Customer	Last Seen	Actions
□	win-fv9ldqtjloq-398d52d3 New	win-fv9ldqtjloq	192.168.17.130 (local)	00:0c:29:38:5e:fe	Undefined	100	100	0	0	oe_lanner...	Ocean's E...	2017-08-16 15:29:46	Actions ▾
□	10-18-1-208-ab7e5d6a New	10-18-1-208	10.18.1.208 (local)	b8:86:87:32:de:91	Undefined	100	100	0	0	oe_lanner...	Ocean's E...	2017-08-16 09:34:51	Actions ▾
□	Offline 10.18.1.208-70d31806 New		10.18.1.208 (local)	b8:86:87:32:de:91	Undefined	100	100	0	0	oe_lanner...	Ocean's E...	2017-08-16 09:02:31	Actions ▾
□	10.234.3.99-83cfff94 New		10.234.3.99 (local)	50:c5:8d:7d:1e:10	Undefined	100	100	0	0	oe_lanner...	Ocean's E...	2017-08-14 13:13:55	Actions ▾
□	Offline 10.18.1.229-281522b6 New		10.18.1.229 (local)	c4:b3:01:c6:9e:4b	Undefined	100	100	0	0	oe_lanner...	Ocean's E...	2017-08-16 09:02:00	Actions ▾
□	scrum-arctic-c5976c2e New	scrum-arctic	10.20.3.50 (local)	90:e2:ba:2c:45:d8	Undefined	100	100	0	0	oe_lanner...	Ocean's E...	2017-08-10 05:08:32	Actions ▾
□	Offline 10.20.3.50-fa69d2b8 New		10.20.3.50 (local)	90:e2:ba:2c:45:d8	Undefined	100	100	0	0	oe_lanner...	Ocean's E...	2017-08-09 16:56:16	Actions ▾
□	10.20.3.48-0bed6c1b New		10.20.3.48 (local)	90:e2:ba:2c:45:d8	Undefined	100	100	0	0	oe_lanner...	Ocean's E...	2017-08-10 13:53:22	Actions ▾
□	10.20.3.46-c0ce72f9 New		10.20.3.46 (local)	90:e2:ba:2c:45:d8	Undefined	100	100	0	0	oe_lanner...	Ocean's E...	2017-08-10 15:51:31	Actions ▾
□	10.20.3.44-ebdf2801 New		10.20.3.44 (local)	90:e2:ba:2c:45:d8	Undefined	100	100	0	0	oe_lanner...	Ocean's E...	2017-08-10 01:13:34	Actions ▾
□	10.30.0.12-e7942cbe New		10.30.0.12 (local)	00:30:48:bc:44:4a	Undefined	100	100	0	0	oe_lanner...	Ocean's E...	2017-08-03 16:20:32	Actions ▾
□	10.20.4.101-1529b176 New		10.20.4.101 (local)	90:e2:ba:2c:45:d8	Undefined	100	100	0	0	oe_lanner...	Ocean's E...	2017-08-03 15:45:34	Actions ▾
□	10.20.7.51-c5d4078d New		10.20.7.51 (local)	90:e2:ba:2c:45:d8	Undefined	100	100	0	232	oe_lanner...	Ocean's E...	2017-08-16 06:40:32	Actions ▾
□	s4a0bbac22e1757e83651-20... New	s4a0bbac22e17...	10.20.1.11 (local)	90:e2:ba:2c:45:d8	Undefined	100	100	0	2	oe_lanner...	Ocean's E...	2017-08-01 06:28:46	Actions ▾
□	10.18.0.184-2a44cb67 New		10.18.0.184 (local)	a0:99:9b:0e:87:63	Undefined	100	100	0	15	oe_lanner...	Ocean's E...	2017-07-31 15:07:02	Actions ▾
□	10.18.1.236-091215fa New		10.18.1.236 (local)	f4:0f:24:18:f0:e3	Undefined	100	100	0	2	oe_lanner...	Ocean's E...	2017-07-28 10:55:30	Actions ▾
□	msedgewin10-61af2691 New	msedgewin10	10.20.1.4 (local)	90:e2:ba:2c:45:d8	Undefined	100	100	0	2	oe_lanner...	Ocean's E...	2017-07-25 17:50:10	Actions ▾
□	10.18.0.38-d0dbd4e2 New		10.18.0.38 (local)	44:85:00:50:d7:eb	Undefined	100	100	0	26	oe_lanner...	Ocean's E...	2017-08-04 09:58:16	Actions ▾

The ‘Discovery’ scan populates the asset database. If you want to review all the assets simply:

1. *Choose the ‘Assets’ button and then*
2. *Press the ‘Apply Filter’ button*

Setting Up The “Full and Fast” Scan (1)



Create Scan Job

Job Name: Full and Fast (Reoccurring Weekends)

Description: This is the scan run once a week (with credentials)

Customer: Ocean's Edge

Sensor: oe_lanner--oe

Credentials: root [ssh]

Scan Config: Full and fast

Full Network Scanning □

Scan now □

Schedule Method

First Time: 2017-08-03 20:56:16

Schedule Period: Every 1 week(s)

Maximum Duration: hour(s)

Active / Enabled ☑

Auto Generate Report ☑

Upload To Custom Storage □

Send To: scott@netwatcher.com

Scan Config Info

Name: Full and fast

Description: Only Network Vulnerability Tests are used that will not damage the target system. Plugins are optimized in the best possible way to keep the potential false negative rate especially low.

Xml: Show xml tree

Targets

Assets | Networks

- Networks
  - Default network (oe_lanner--oe)
    - ☑ Subnet 192.168.0.0/16 (25 assets)
    - □ Subnet 172.16.0.0/12 (2 assets)
    - ☑ Subnet 10.0.0.0/8 (1588 assets)
    - □ Subnet fc00::/7 (0 assets)

IPs & CIDRs List

IP/CIDR | Please, select...

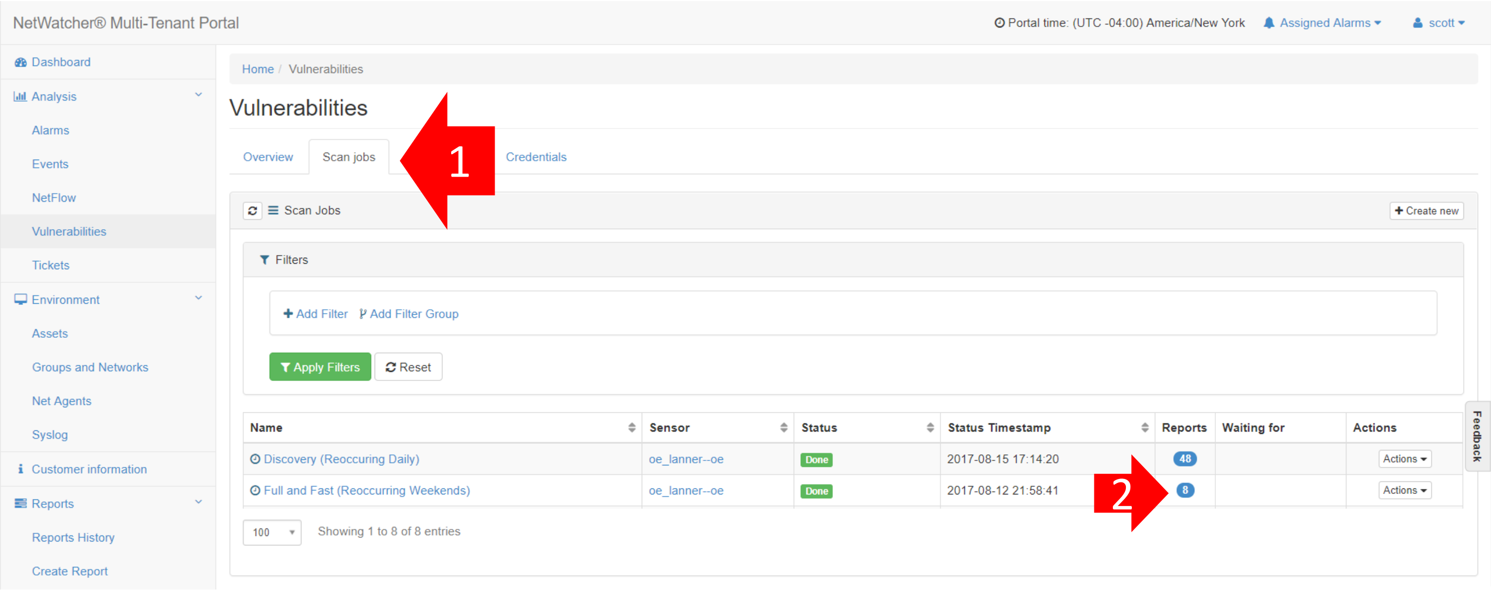
10.0.0.0/8 ✖

192.168.0.0/16 ✖

The ‘Full and Fast’ Scan will send Network Vulnerability Tests (NVTs) to the assets on the network. This is necessary to determine what vulnerabilities exist on the network.

1. *Name the job ‘Full and Fast (Reoccurring Weekends)’*
2. *Choose the sensor name*
3. *Add credentials if necessary – This sends additional NVTs that require user credentials to test the asset*
4. *Choose the ‘Full and Fast’ Scan Config*
5. *Add the IP Range and CIDR*
6. ***Un-Check** Full Network Scanning – this scan will use the assets in the database.*
7. *Uncheck ‘Scan now’ and schedule the scan for sometime late in the evening at least an hour after the ‘Discovery’ scan when there is the most downtime on the network. Schedule the scan to run every week.*
8. *Choose to Auto Generate Report if you want a PDF to be available for the customer. Note that you can also put in an email address in the ‘Send To’ field.*
9. *Click the ‘Create’ button*

Reviewing The Scan After It's Complete (1)



NetWatcher® Multi-Tenant Portal

Portal time: (UTC -04:00) America/New York | Assigned Alarms | scott

Vulnerabilities

Scan Jobs

Filters

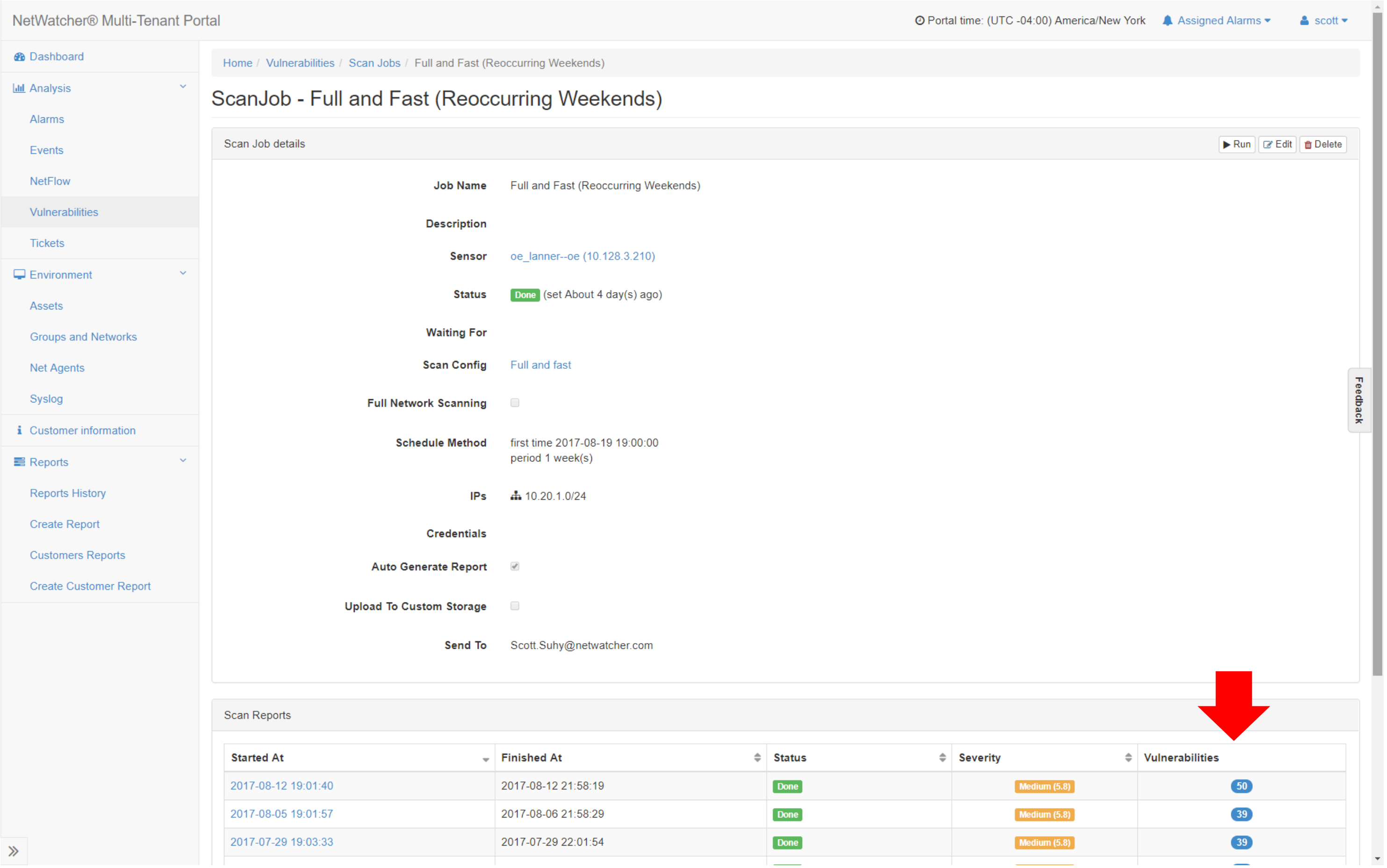
Name	Sensor	Status	Status Timestamp	Reports	Waiting for	Actions
Discovery (Reoccuring Daily)	oe_lanner--oe	Done	2017-08-15 17:14:20	48		Actions
Full and Fast (Reoccurring Weekends)	oe_lanner--oe	Done	2017-08-12 21:58:41	8		Actions

100 Showing 1 to 8 of 8 entries

1. Press the 'Scan Jobs' tab and you will see both scheduled Scans as well as how many times they have been run (under the 'Reports' column). If you click on the # in the 'Reports' Column for the 'Full and Fast' scan you will be taken to the detail.

2. In this example, the 'Full and Fast' scan has run 8 times.

Reviewing The Scan After It's Complete (2)



ScanJob - Full and Fast (Reoccurring Weekends)

Scan Job details

Job Name	Full and Fast (Reoccurring Weekends)
Description	
Sensor	oe_lanner--oe (10.128.3.210)
Status	Done (set About 4 day(s) ago)
Waiting For	
Scan Config	Full and fast
Full Network Scanning	□
Schedule Method	first time 2017-08-19 19:00:00 period 1 week(s)
IPs	10.20.1.0/24
Credentials	
Auto Generate Report	☑
Upload To Custom Storage	□
Send To	Scott.Suhy@netwatcher.com

Scan Reports

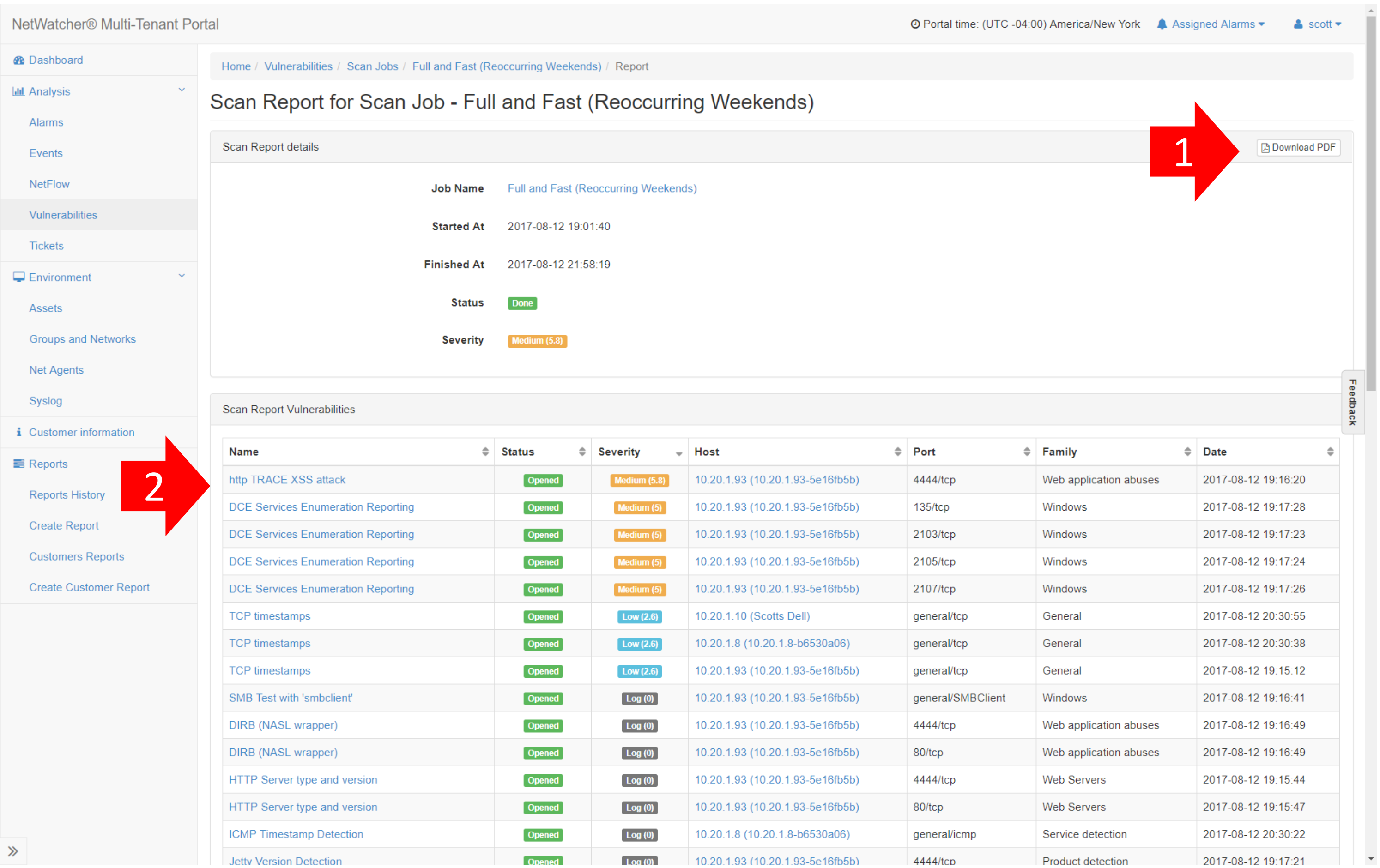
Started At	Finished At	Status	Severity	Vulnerabilities
2017-08-12 19:01:40	2017-08-12 21:58:19	Done	Medium (5.8)	50
2017-08-05 19:01:57	2017-08-06 21:58:29	Done	Medium (5.8)	39
2017-07-29 19:03:33	2017-07-29 22:01:54	Done	Medium (5.8)	39

The Scan detail page will show you each scheduled scan and what the maximum severity found in the scan as well as the date and time that the scan started and stopped as well as the number of vulnerabilities found.

The number of vulnerabilities from each scan can be found in the 'Vulnerabilities' column.

If you click on the # you will be taken to a list of those vulnerabilities.

Reviewing The Scan After It’s Complete (3)



Scan Report for Scan Job - Full and Fast (Reoccurring Weekends)

Scan Report details

Job Name	Full and Fast (Reoccurring Weekends)
Started At	2017-08-12 19:01:40
Finished At	2017-08-12 21:58:19
Status	Done
Severity	Medium (5.8)

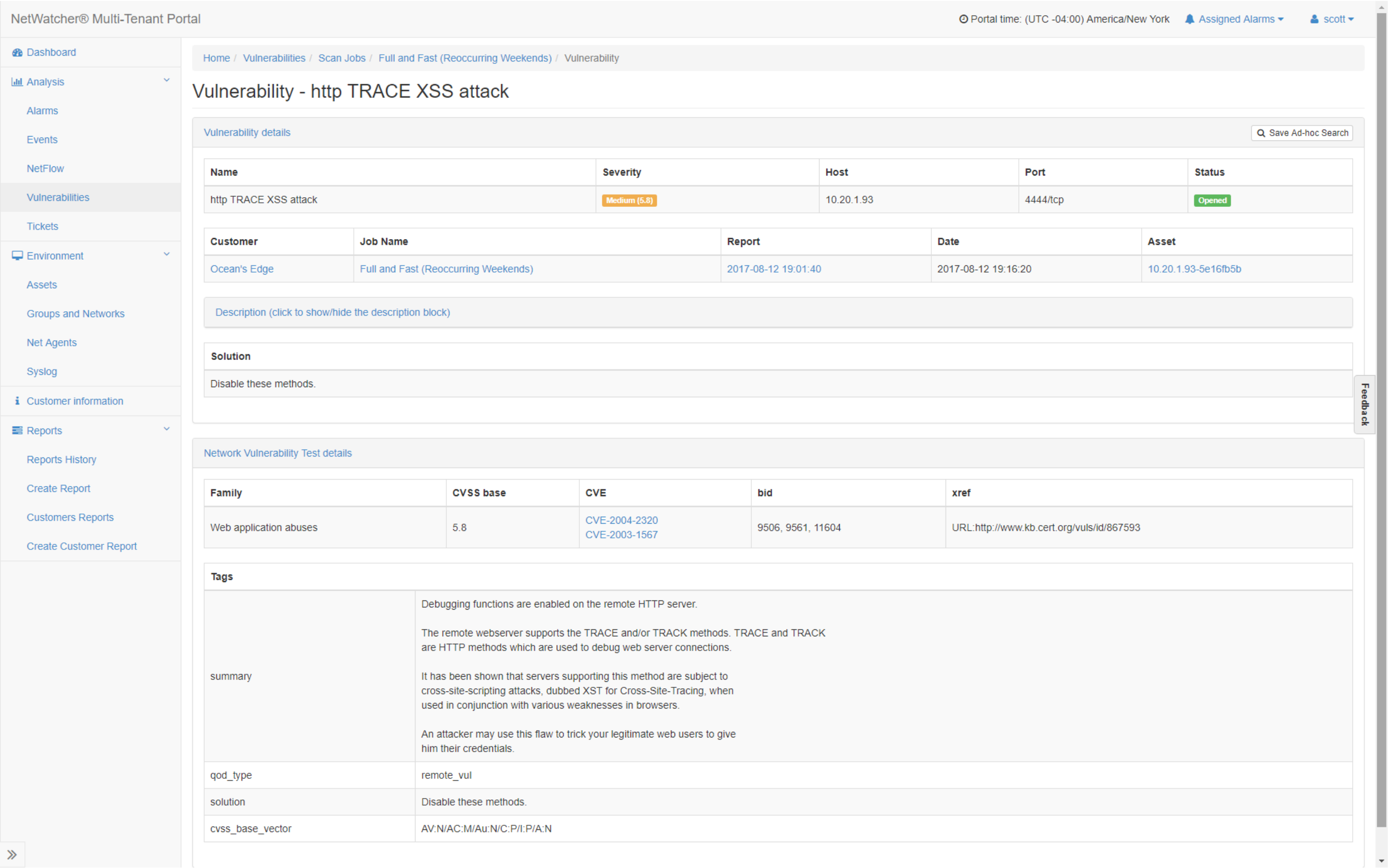
Scan Report Vulnerabilities

Name	Status	Severity	Host	Port	Family	Date
http TRACE XSS attack	Opened	Medium (5.8)	10.20.1.93 (10.20.1.93-5e16fb5b)	4444/tcp	Web application abuses	2017-08-12 19:16:20
DCE Services Enumeration Reporting	Opened	Medium (5)	10.20.1.93 (10.20.1.93-5e16fb5b)	135/tcp	Windows	2017-08-12 19:17:28
DCE Services Enumeration Reporting	Opened	Medium (5)	10.20.1.93 (10.20.1.93-5e16fb5b)	2103/tcp	Windows	2017-08-12 19:17:23
DCE Services Enumeration Reporting	Opened	Medium (5)	10.20.1.93 (10.20.1.93-5e16fb5b)	2105/tcp	Windows	2017-08-12 19:17:24
DCE Services Enumeration Reporting	Opened	Medium (5)	10.20.1.93 (10.20.1.93-5e16fb5b)	2107/tcp	Windows	2017-08-12 19:17:26
TCP timestamps	Opened	Low (2.6)	10.20.1.10 (Scotts Dell)	general/tcp	General	2017-08-12 20:30:55
TCP timestamps	Opened	Low (2.6)	10.20.1.8 (10.20.1.8-b6530a06)	general/tcp	General	2017-08-12 20:30:38
TCP timestamps	Opened	Low (2.6)	10.20.1.93 (10.20.1.93-5e16fb5b)	general/tcp	General	2017-08-12 19:15:12
SMB Test with 'smbclient'	Opened	Log (0)	10.20.1.93 (10.20.1.93-5e16fb5b)	general/SMBClient	Windows	2017-08-12 19:16:41
DIRB (NASL wrapper)	Opened	Log (0)	10.20.1.93 (10.20.1.93-5e16fb5b)	4444/tcp	Web application abuses	2017-08-12 19:16:49
DIRB (NASL wrapper)	Opened	Log (0)	10.20.1.93 (10.20.1.93-5e16fb5b)	80/tcp	Web application abuses	2017-08-12 19:16:49
HTTP Server type and version	Opened	Log (0)	10.20.1.93 (10.20.1.93-5e16fb5b)	4444/tcp	Web Servers	2017-08-12 19:15:44
HTTP Server type and version	Opened	Log (0)	10.20.1.93 (10.20.1.93-5e16fb5b)	80/tcp	Web Servers	2017-08-12 19:15:47
ICMP Timestamp Detection	Opened	Log (0)	10.20.1.8 (10.20.1.8-b6530a06)	general/icmp	Service detection	2017-08-12 20:30:22
Jetty Version Detection	Opened	Log (0)	10.20.1.93 (10.20.1.93-5e16fb5b)	4444/tcp	Product detection	2017-08-12 19:17:21

The list of vulnerabilities will be found on this scan details page.

1. *You can also download a PDF of all of these vulnerabilities from this page.*
2. *If you click on the name of the vulnerability you will be taken to the derailed explanation of that issue.*

Reviewing The Scan After It's Complete (4)
Reviewing A Vulnerability Event



Vulnerability - http TRACE XSS attack

Vulnerability details

Name	Severity	Host	Port	Status
http TRACE XSS attack	Medium (5.8)	10.20.1.93	4444/tcp	Opened

Customer	Job Name	Report	Date	Asset
Ocean's Edge	Full and Fast (Reoccurring Weekends)	2017-08-12 19:01:40	2017-08-12 19:16:20	10.20.1.93-5e16fb5b

Description (click to show/hide the description block)

Solution
Disable these methods.

Network Vulnerability Test details

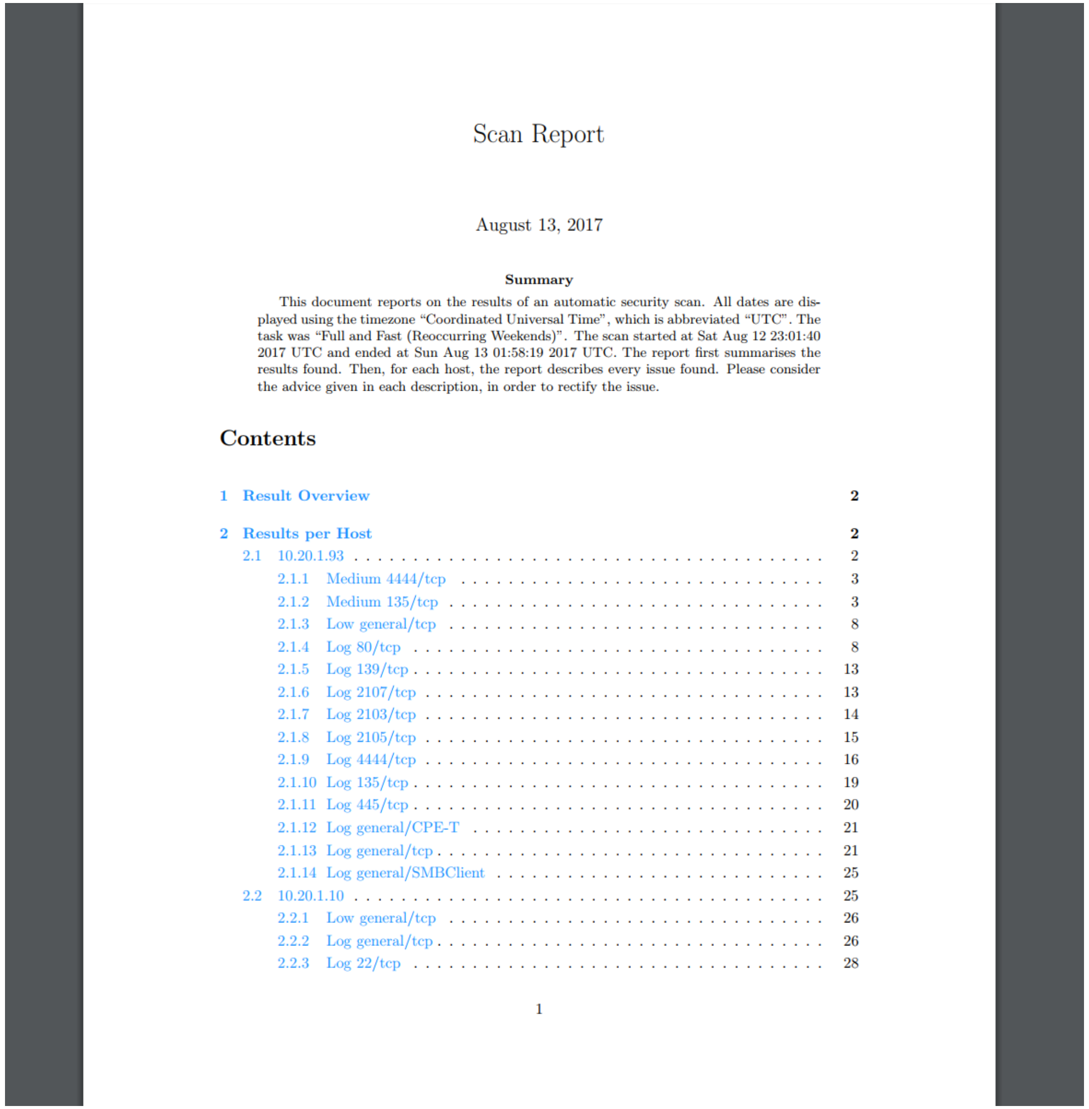
Family	CVSS base	CVE	bid	xref
Web application abuses	5.8	CVE-2004-2320 CVE-2003-1567	9506, 9561, 11604	URL:http://www.kb.cert.org/vuls/id/867593

Tags	
summary	Debugging functions are enabled on the remote HTTP server. The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials.
qod_type	remote_vul
solution	Disable these methods.
cvss_base_vector	AV:N/AC:M/Au:N/C:P/I:P/A:N

The Vulnerability detail for this issue and it's

- *Summary*
- *Solution*
- *What CVE associated with this vulnerability and a link to it in the CVE database*
- *CVSS base and Tags*

Reviewing The Scan After It's Complete (5)
Reviewing the Report



Scan Report

August 13, 2017

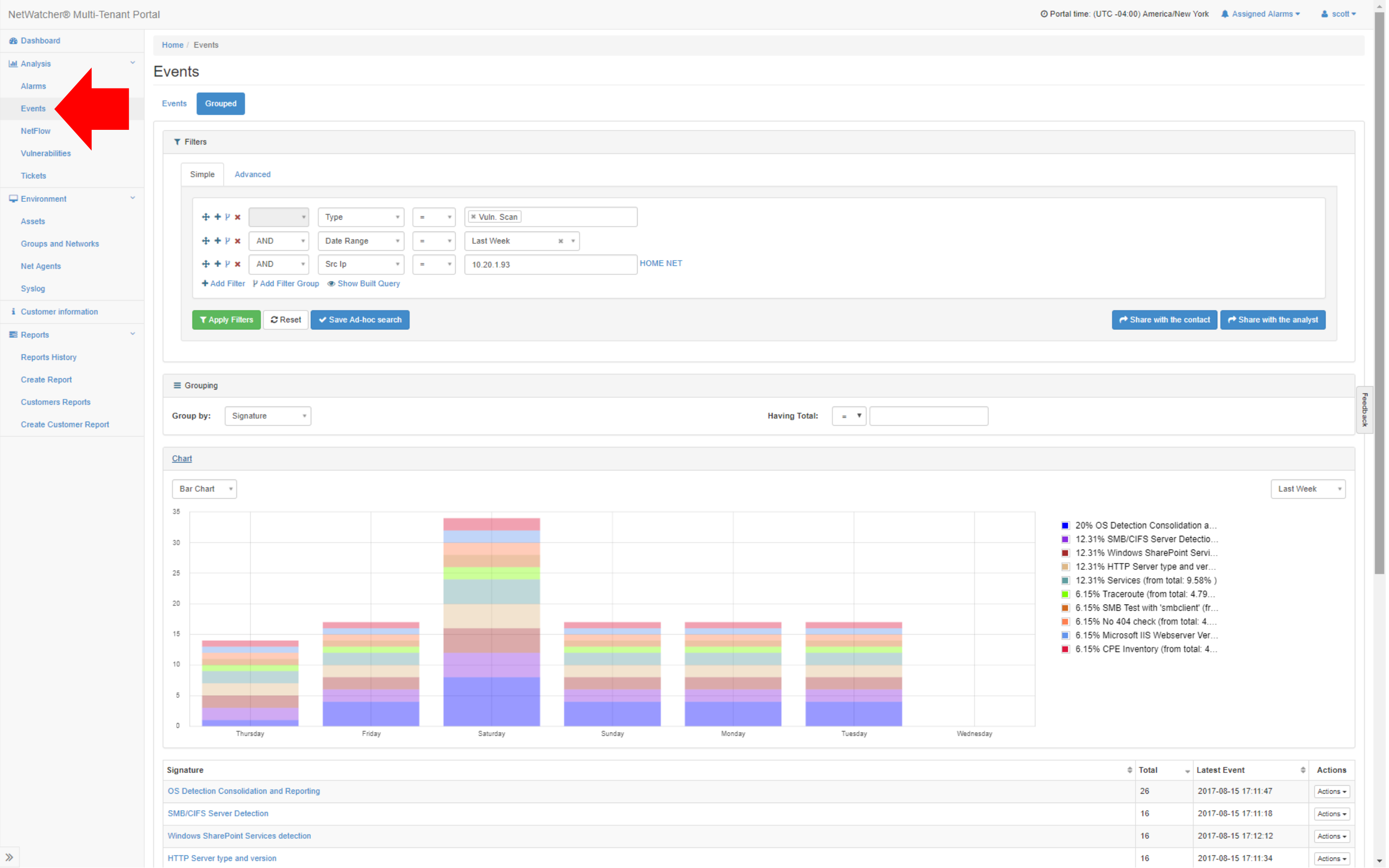
Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “Coordinated Universal Time”, which is abbreviated “UTC”. The task was “Full and Fast (Reoccurring Weekends)”. The scan started at Sat Aug 12 23:01:40 2017 UTC and ended at Sun Aug 13 01:58:19 2017 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

If you did choose to create and download a PDF report for the customer you will find the format easy to read and sorted by vulnerability severity with an easy to navigate table of contents.

NetWatcher Advanced – Event Detail 1 of 2



Type = Vuln. Scan
AND Date Range = Last Week
AND Src Ip = 10.20.1.93 HOME NET

Group by: Signature

Having Total: =

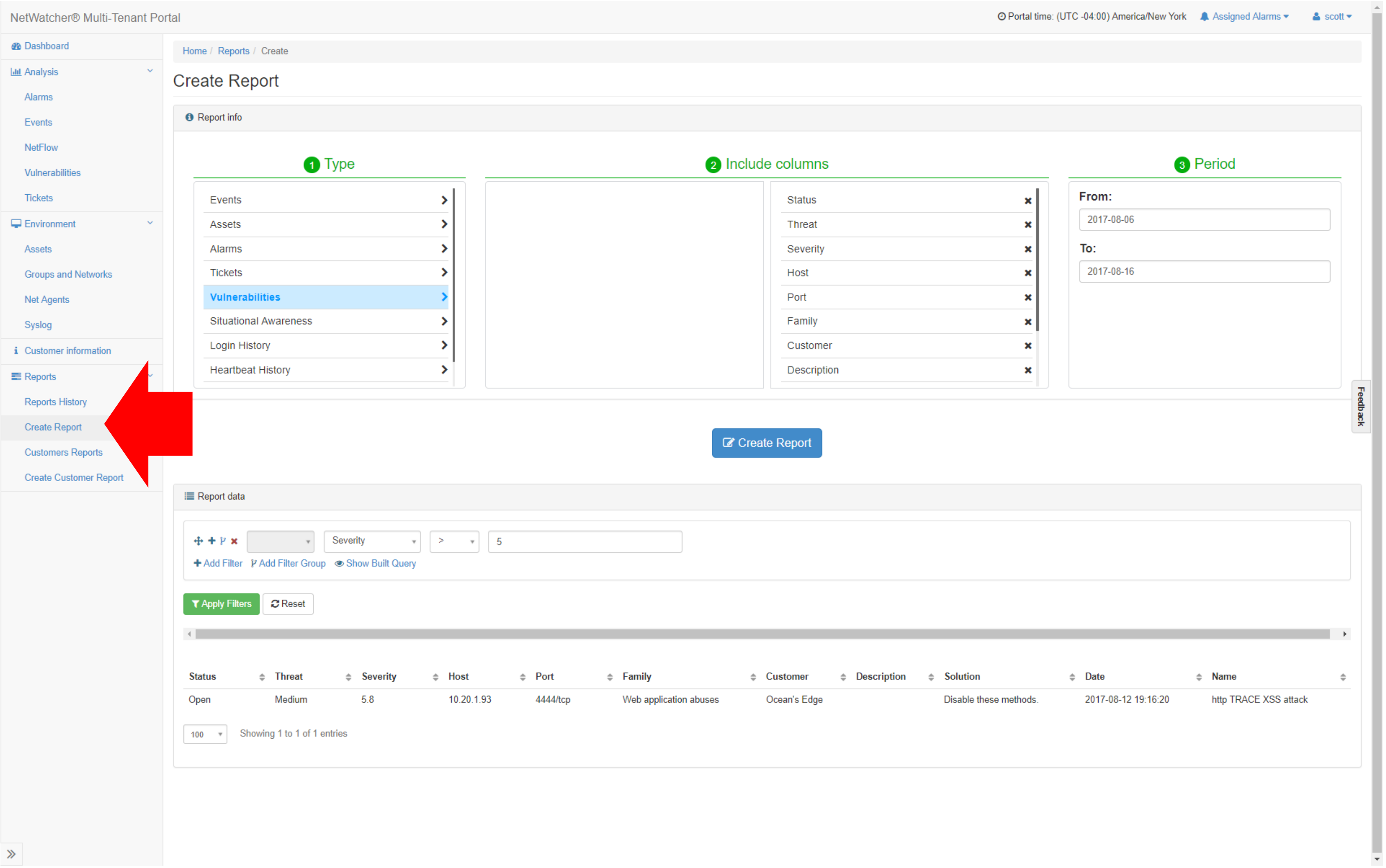
Signature	Total	Latest Event	Actions
OS Detection Consolidation and Reporting	26	2017-08-15 17:11:47	Actions
SMB/CIFS Server Detection	16	2017-08-15 17:11:18	Actions
Windows SharePoint Services detection	16	2017-08-15 17:12:12	Actions
HTTP Server type and version	16	2017-08-15 17:11:34	Actions

If you wanted to look for a specific vulnerability you can always go to the 'Events' menu and do a query. Grouped queries consolidate all of the vulnerabilities of a certain type.

In this example we are looking for all the vulnerabilities from last weeks report on IP address 10.20.1.93

Chart the vulnerabilities and see a list of them (you can click through this detail as well).

Filtered Reporting



Create Report

Report info

1 Type

- Events
- Assets
- Alarms
- Tickets
- Vulnerabilities
- Situational Awareness
- Login History
- Heartbeat History

2 Include columns

- Status
- Threat
- Severity
- Host
- Port
- Family
- Customer
- Description

3 Period

From: 2017-08-06

To: 2017-08-16

Create Report

Report data

Severity > 5

Status	Threat	Severity	Host	Port	Family	Customer	Description	Solution	Date	Name
Open	Medium	5.8	10.20.1.93	4444/tcp	Web application abuses	Ocean's Edge		Disable these methods.	2017-08-12 19:16:20	http TRACE XSS attack

100 Showing 1 to 1 of 1 entries

If you want to Report on specific vulnerabilities in a way that the PDF doesn’t support, you can go to the ‘Create Report’ menu and do a query and ‘Run’ the report and create either a CSV or a PDF. Note how you can query on Severity.

https://netwatcher.com