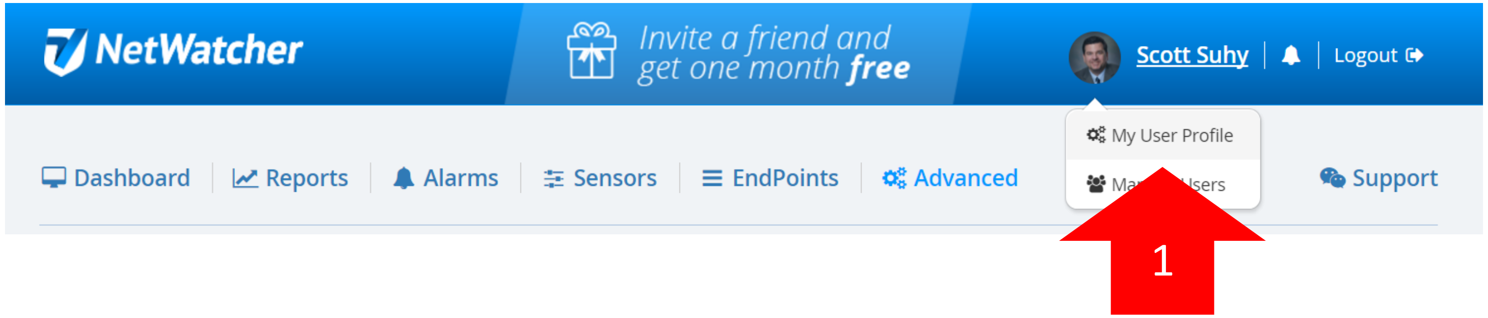
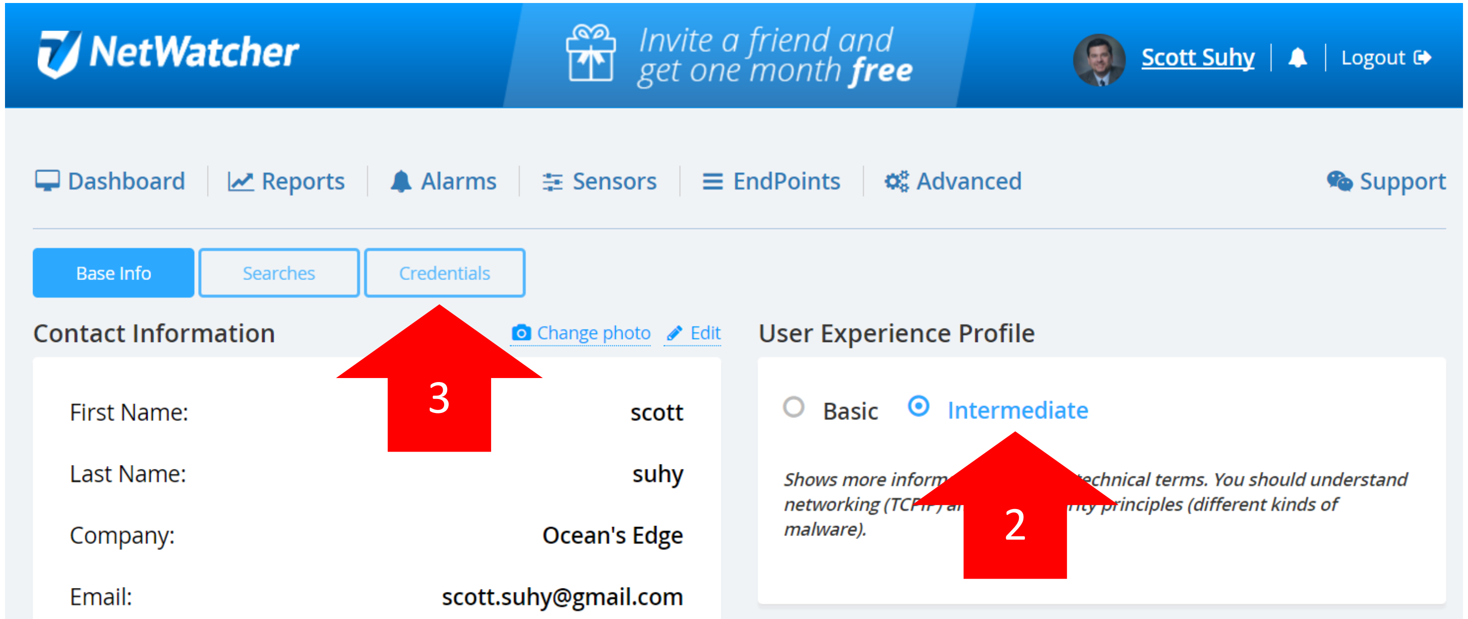
NetWatcher Vulnerability Scanner

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

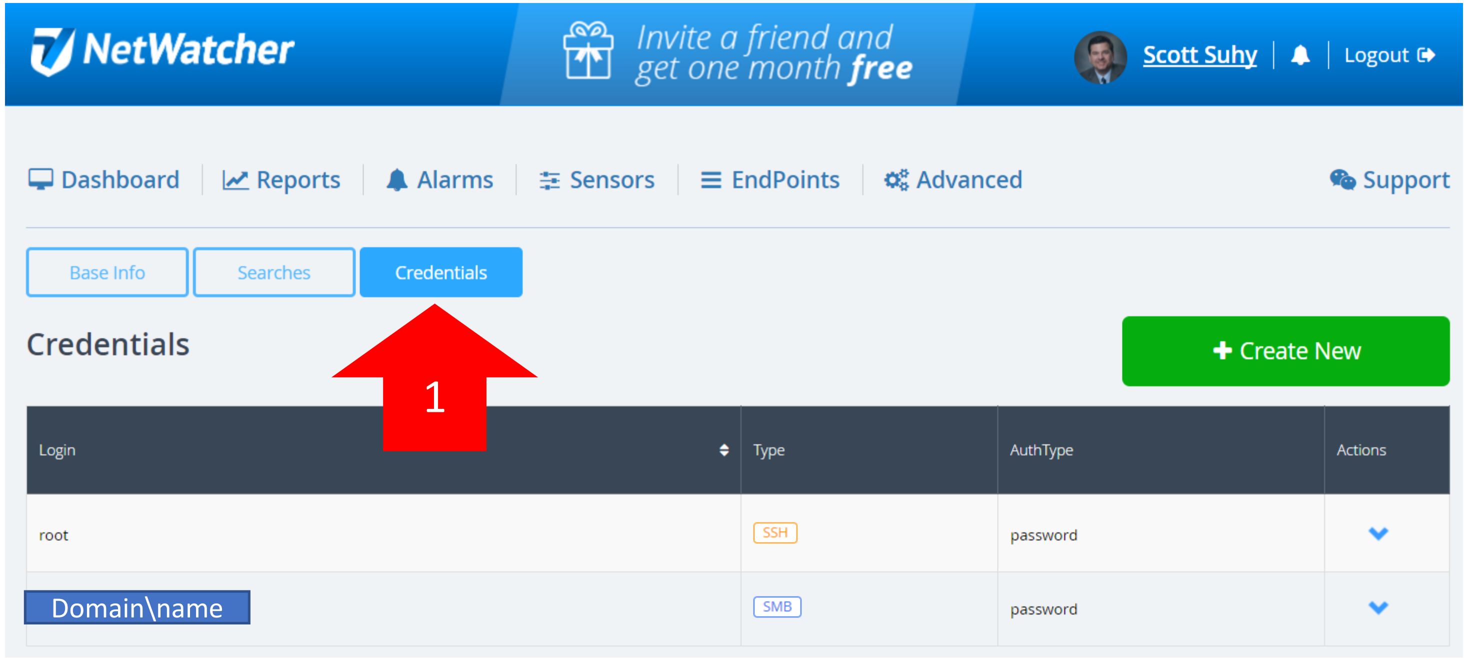
Shows more inform… technical terms. You should understand networking (TCP… a… …rity principles (different kinds of malware).

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	⌄
Domain\name	SMB	password	⌄

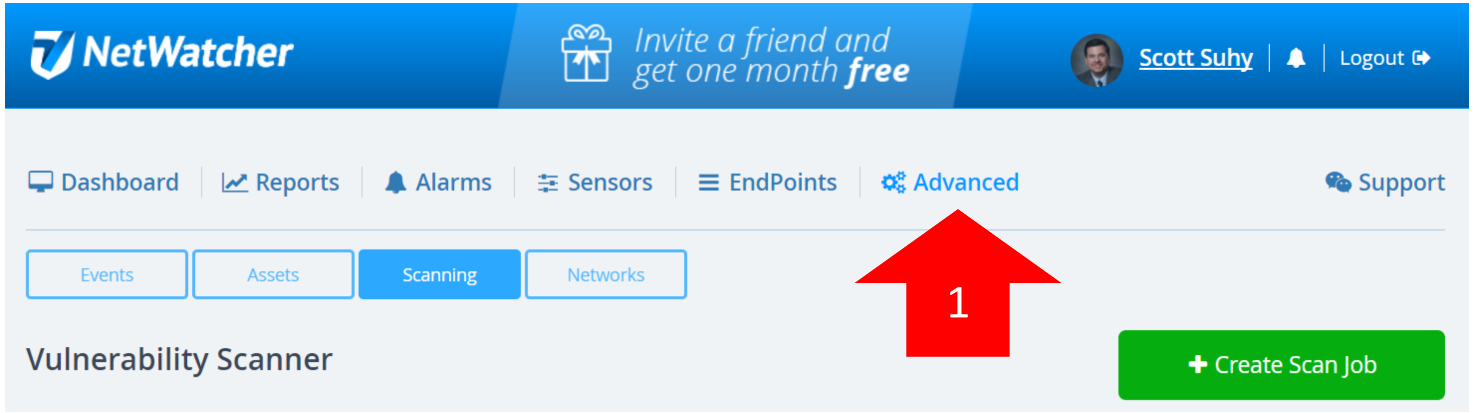
1. Its always best to run a 'Full and Fast' scan using login credentials.

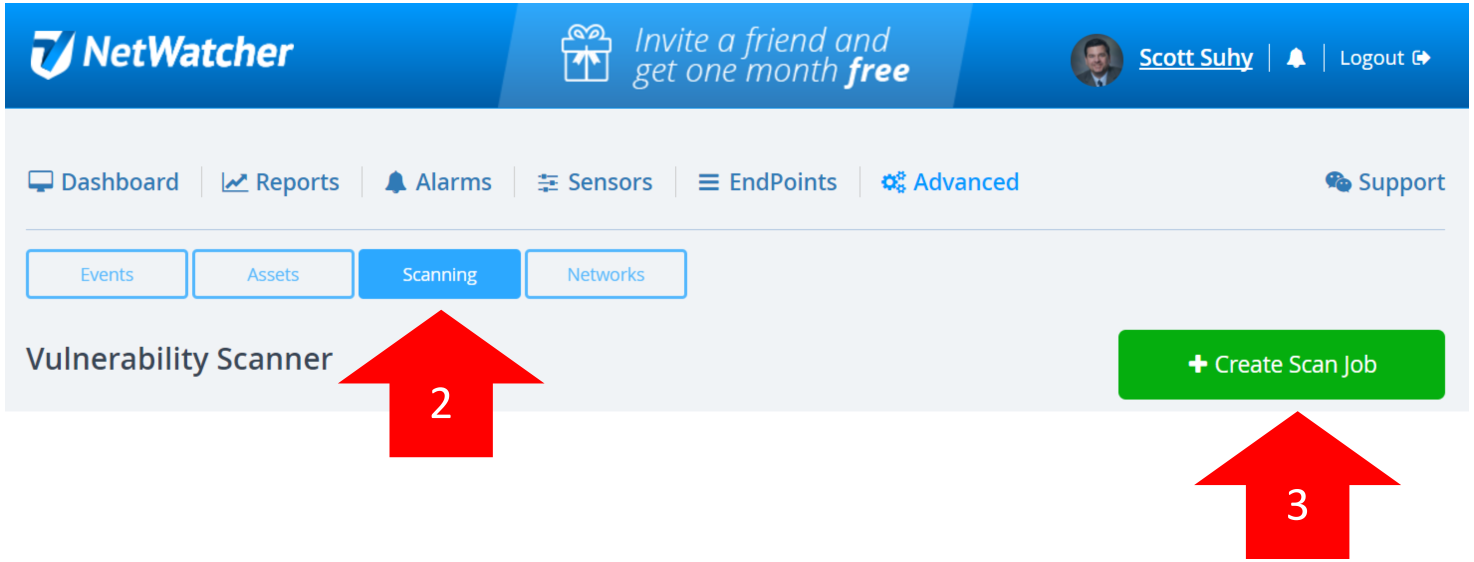
For Windows, choose SMB and use

DOMAIN\name

As the format.

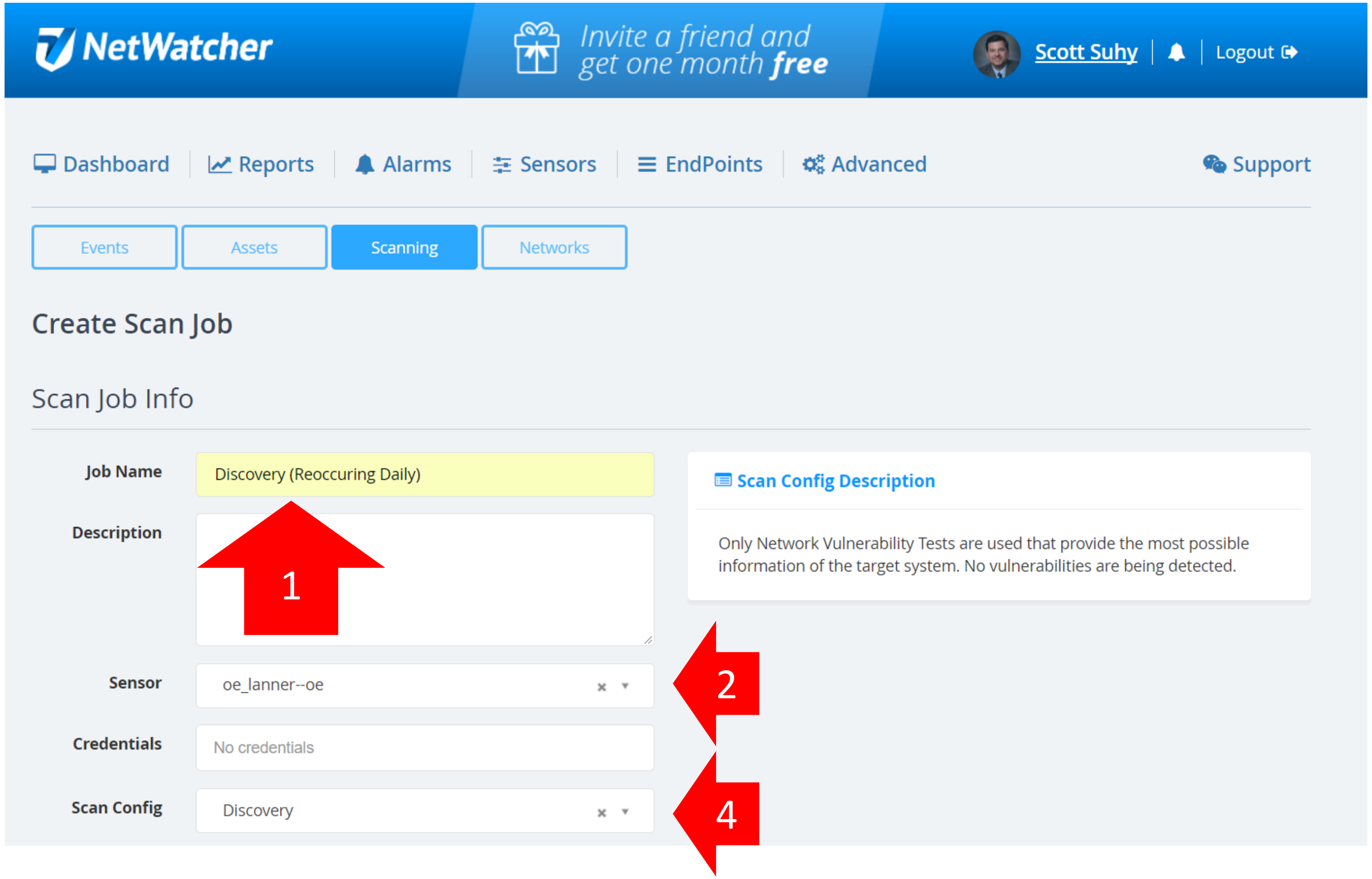
Update Your User Profile (3)





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

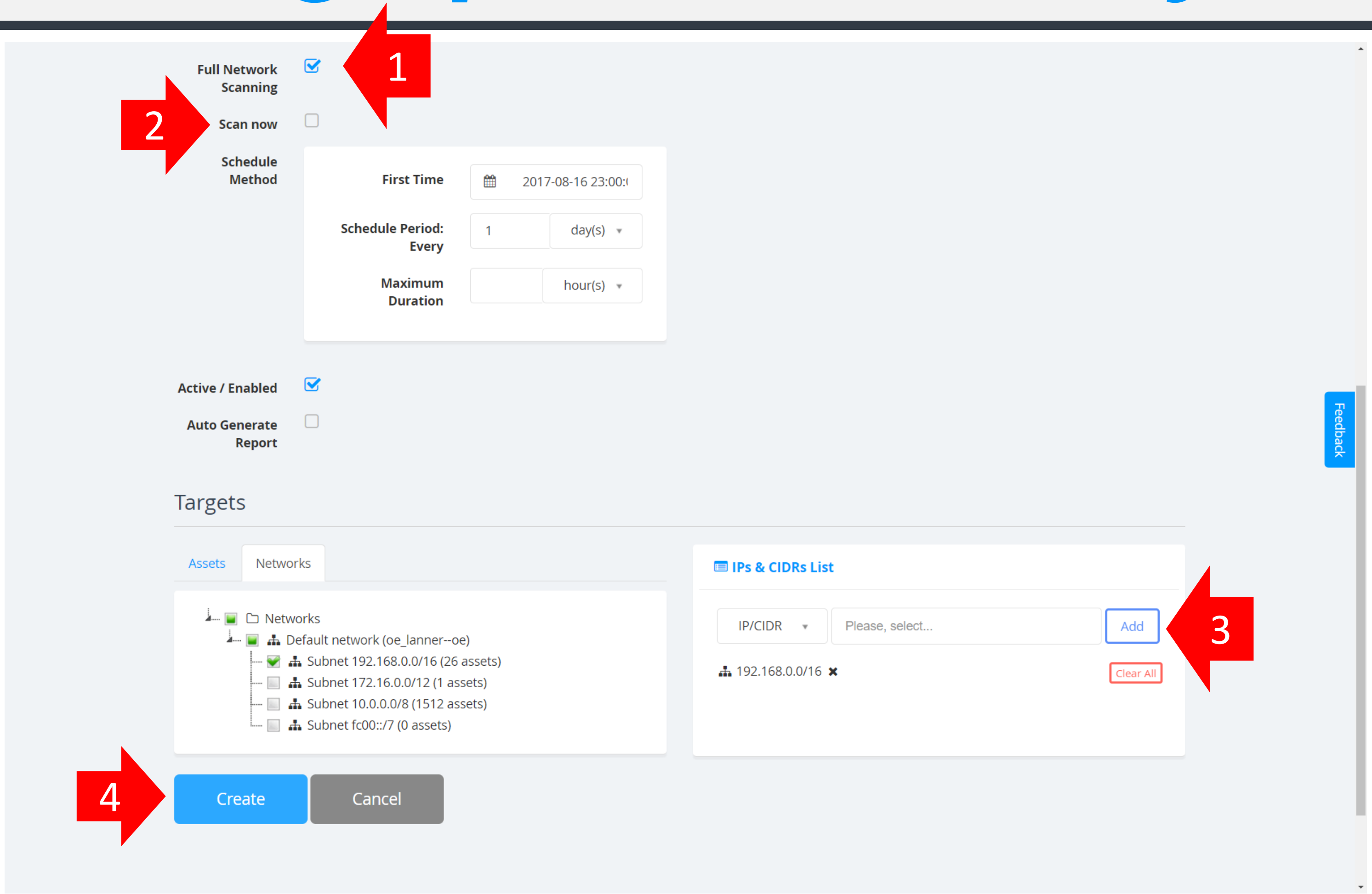
Only Network Vulnerability Tests are used that provide the most possible information of the target system. No vulnerabilities are being detected.

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. *Do not use any credentials*
4. *Choose the 'Discovery' Scan Config*

NetWatcher

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

- 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

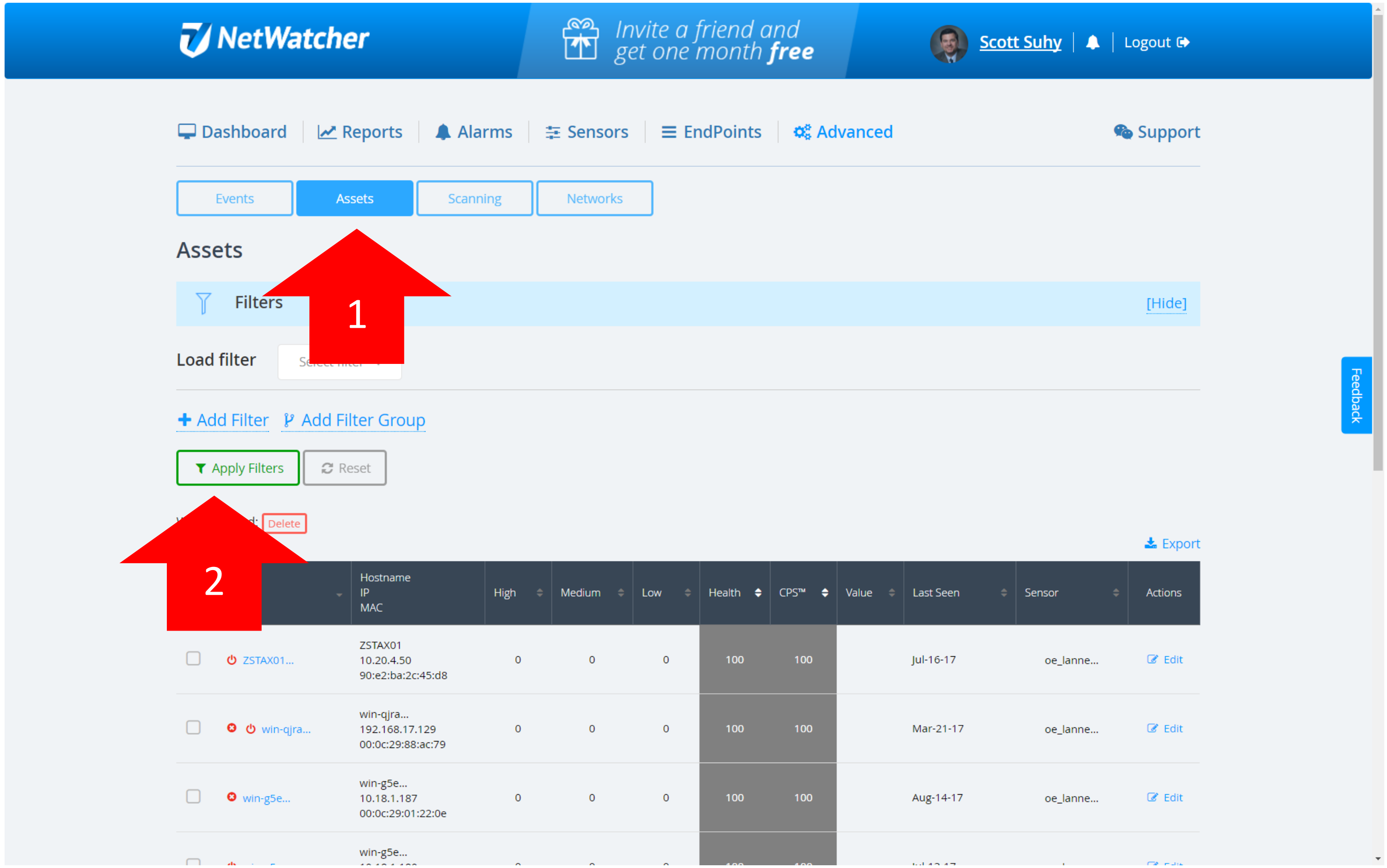
IP/CIDR Please, select...

192.168.0.0/16 ✖

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

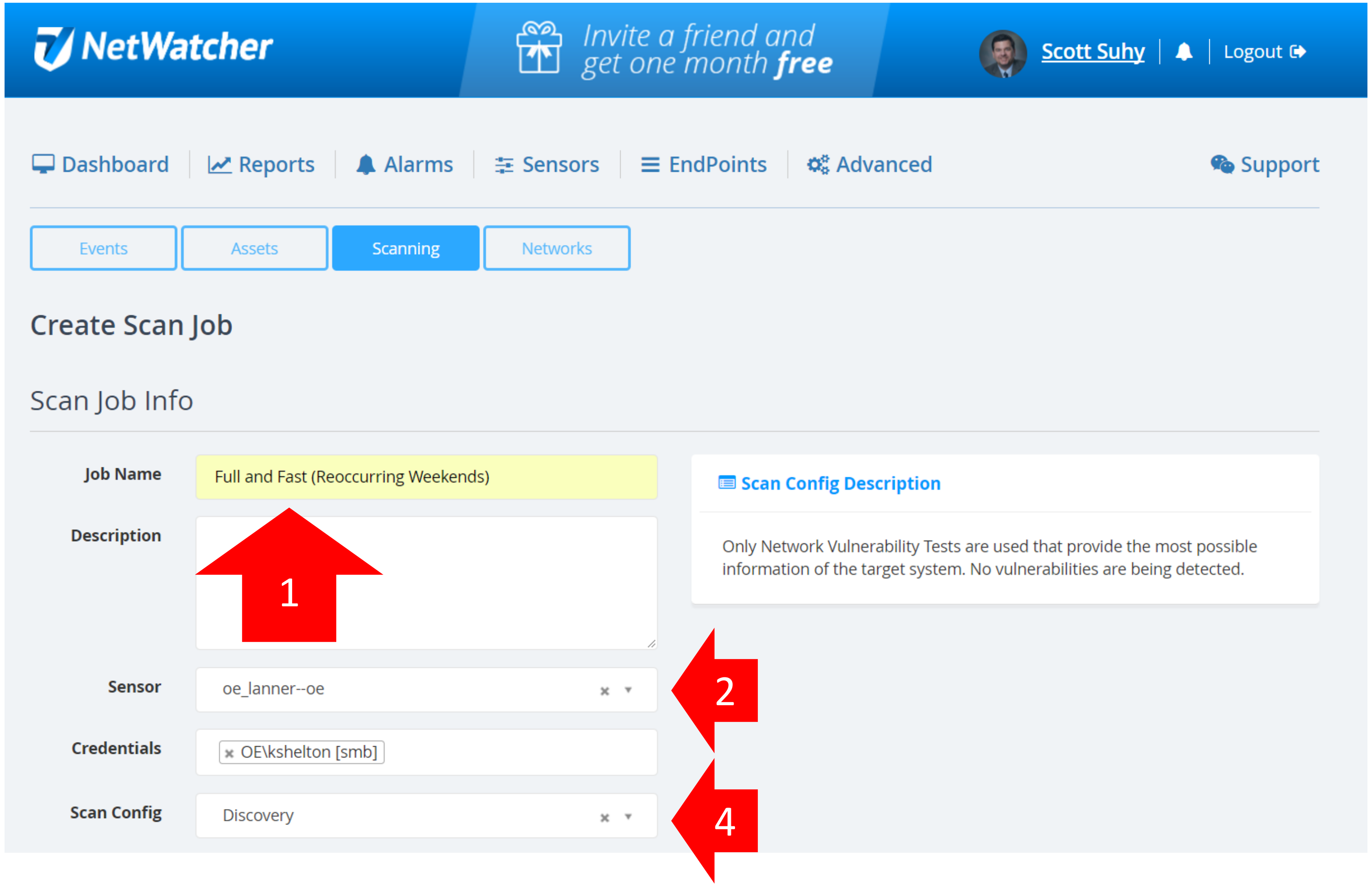


		Hostname IP MAC	High	Medium	Low	Health	CPS™	Value	Last Seen	Sensor	Actions
□	ZSTAX01...	ZSTAX01 10.20.4.50 90:e2:ba:2c:45:d8	0	0	0	100	100		Jul-16-17	oe_lanne...	Edit
□	win-qjra...	win-qjra... 192.168.17.129 00:0c:29:88:ac:79	0	0	0	100	100		Mar-21-17	oe_lanne...	Edit
□	win-g5e...	win-g5e... 10.18.1.187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

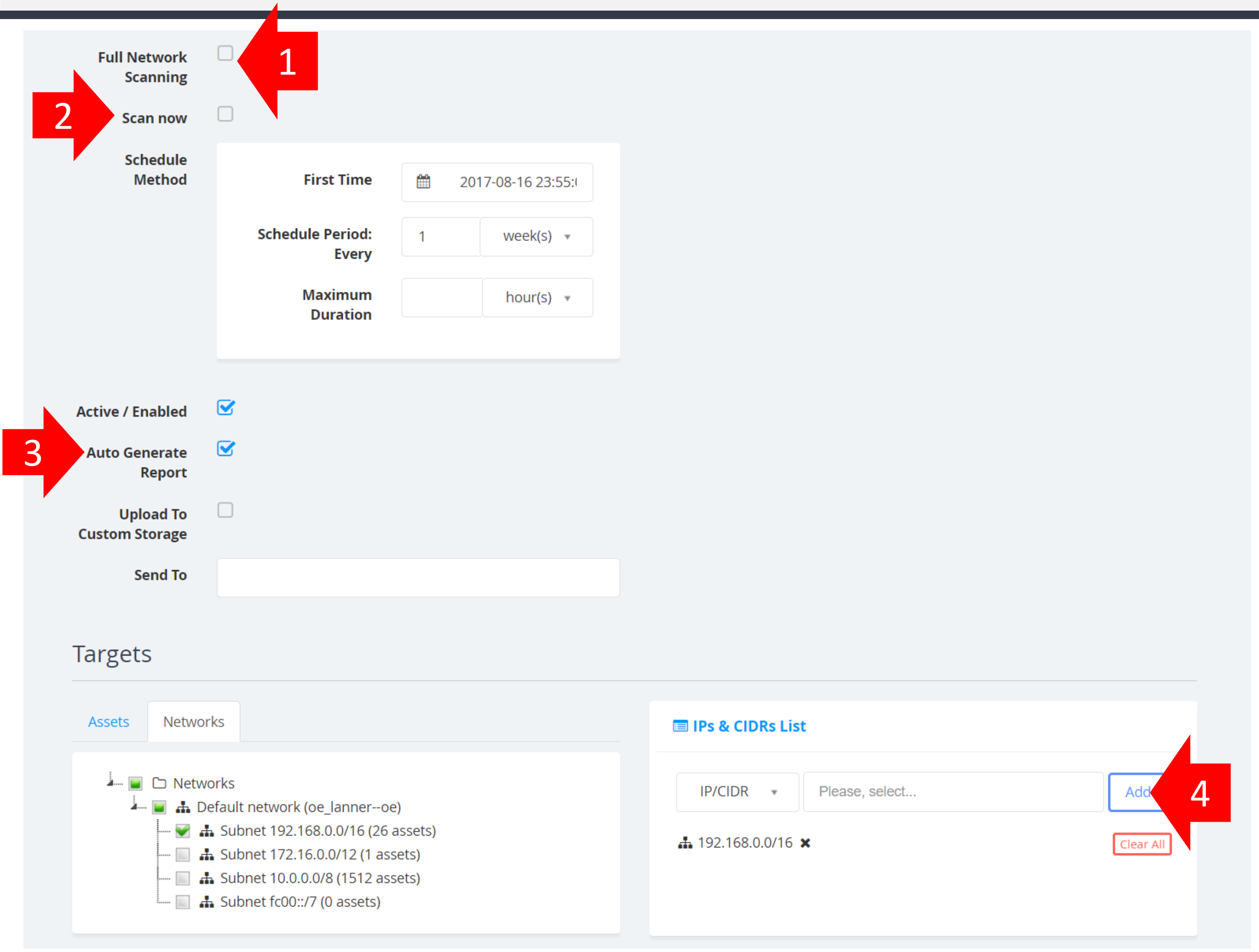
Scan Config Description

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

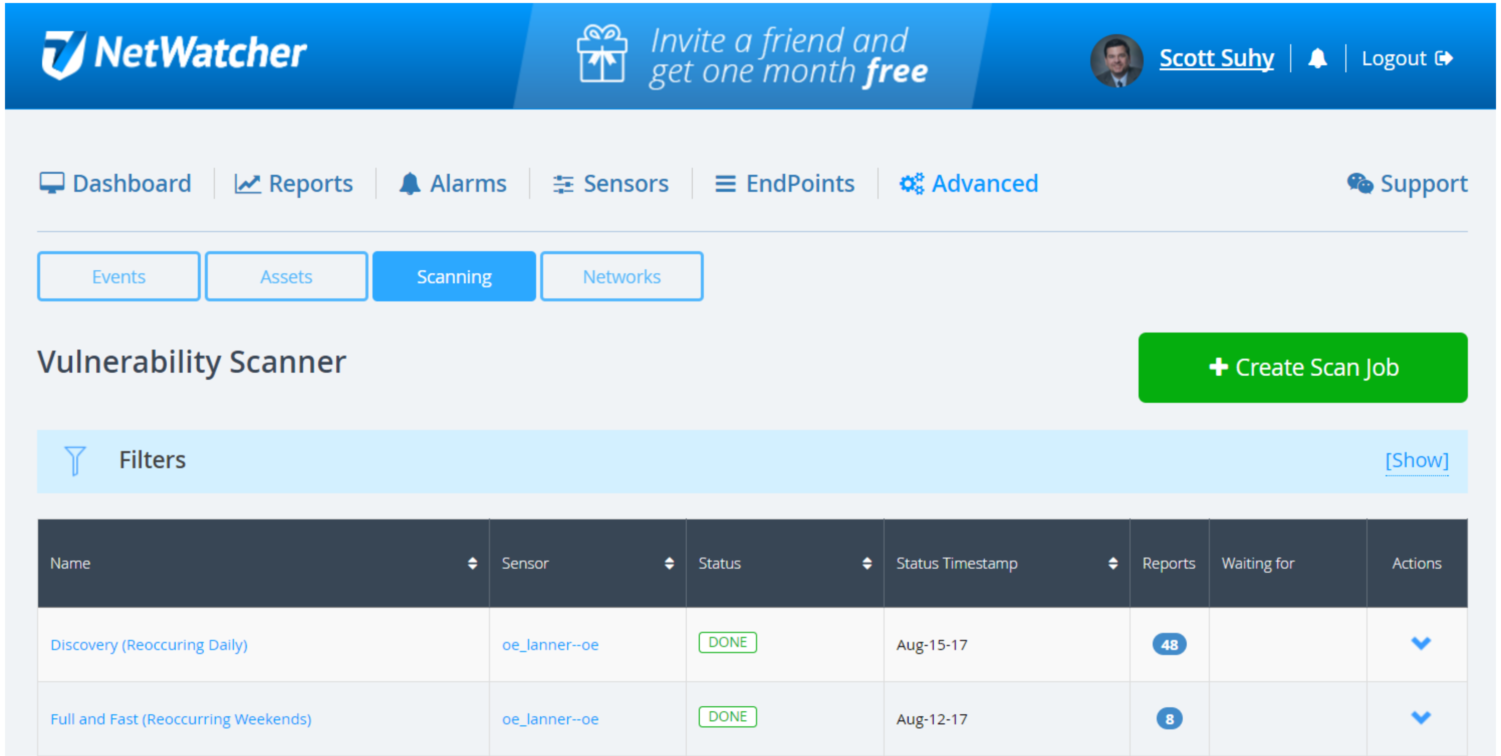
192.168.0.0/16 ✖

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)



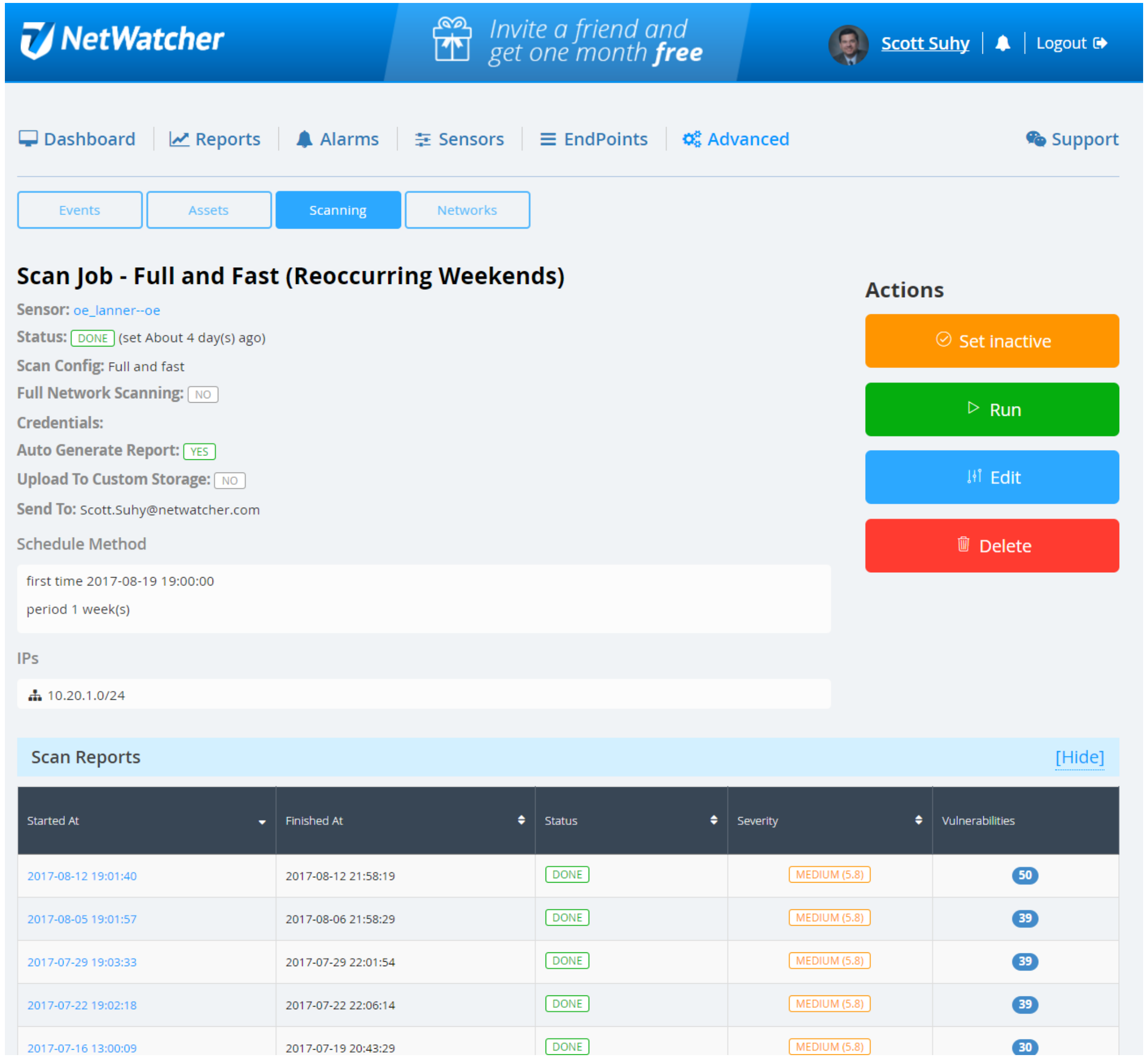
Vulnerability Scanner

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

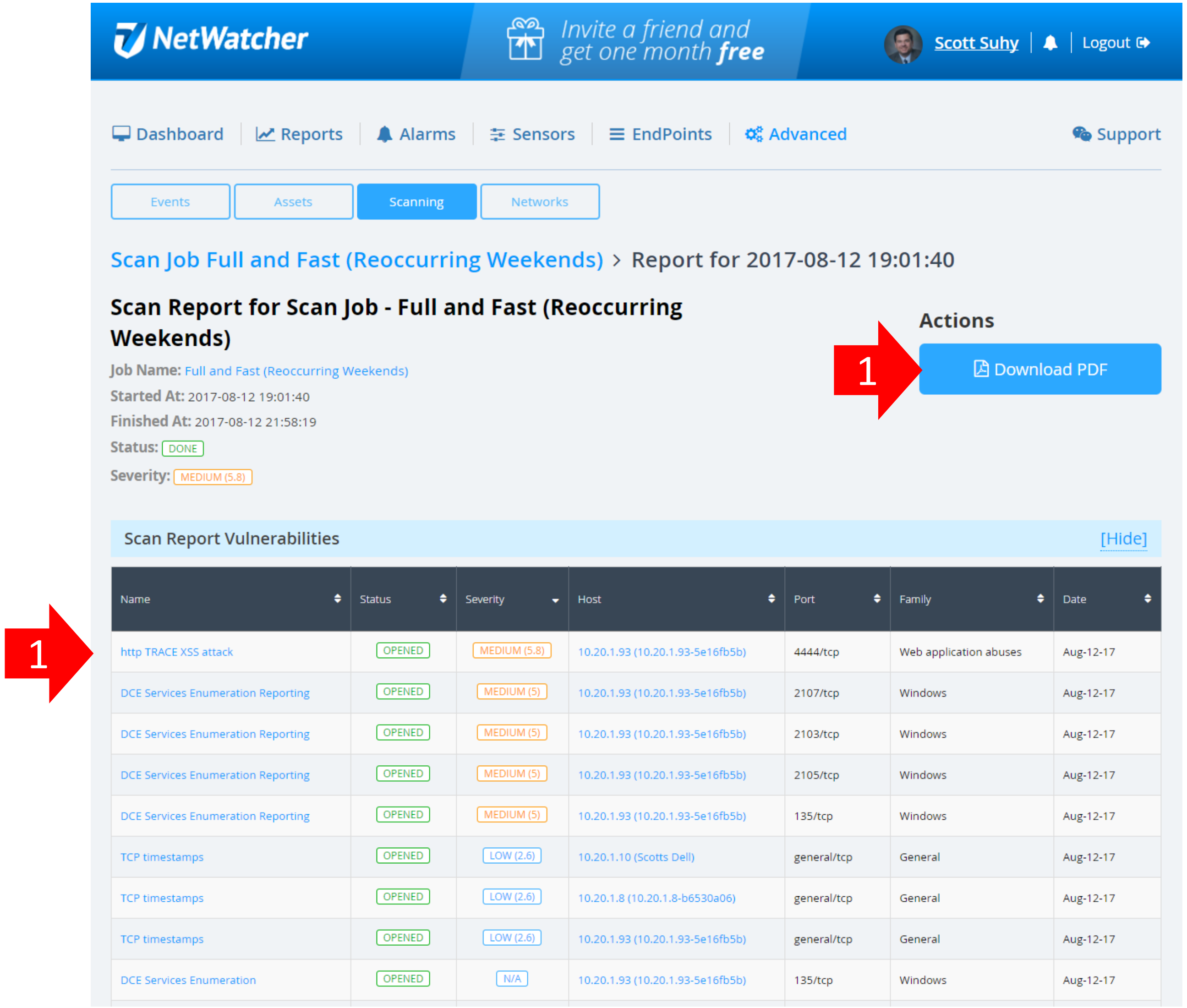
Started At	Finished At	Status	Severity	Vulnerabilities
2017-08-12 19:01:40	2017-08-12 21:58:19	DONE	MEDIUM (5.8)	50
2017-08-05 19:01:57	2017-08-06 21:58:29	DONE	MEDIUM (5.8)	39
2017-07-29 19:03:33	2017-07-29 22:01:54	DONE	MEDIUM (5.8)	39
2017-07-22 19:02:18	2017-07-22 22:06:14	DONE	MEDIUM (5.8)	39
2017-07-16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

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)

Actions

Download PDF

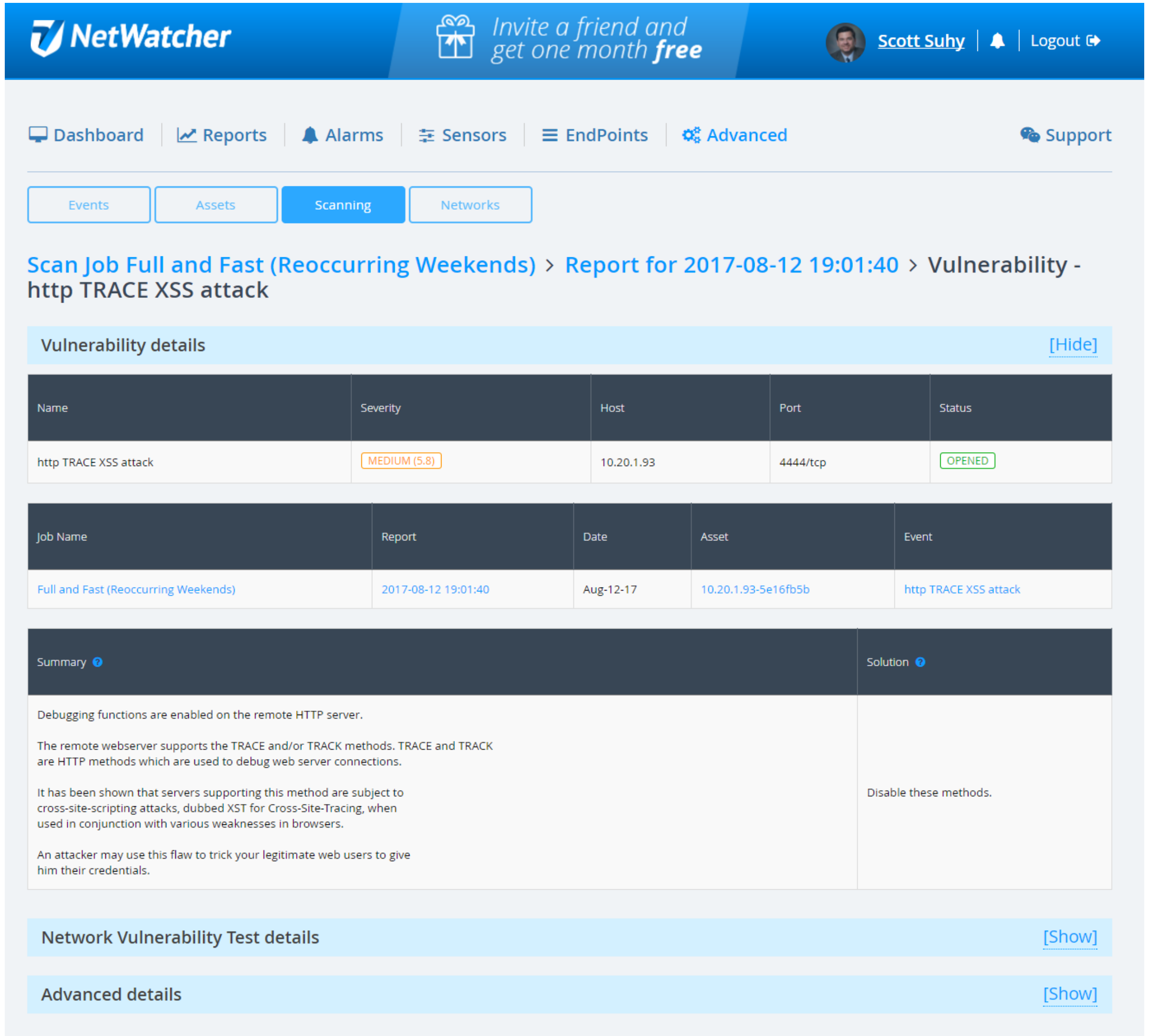
Scan Report Vulnerabilities [Hide]

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

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

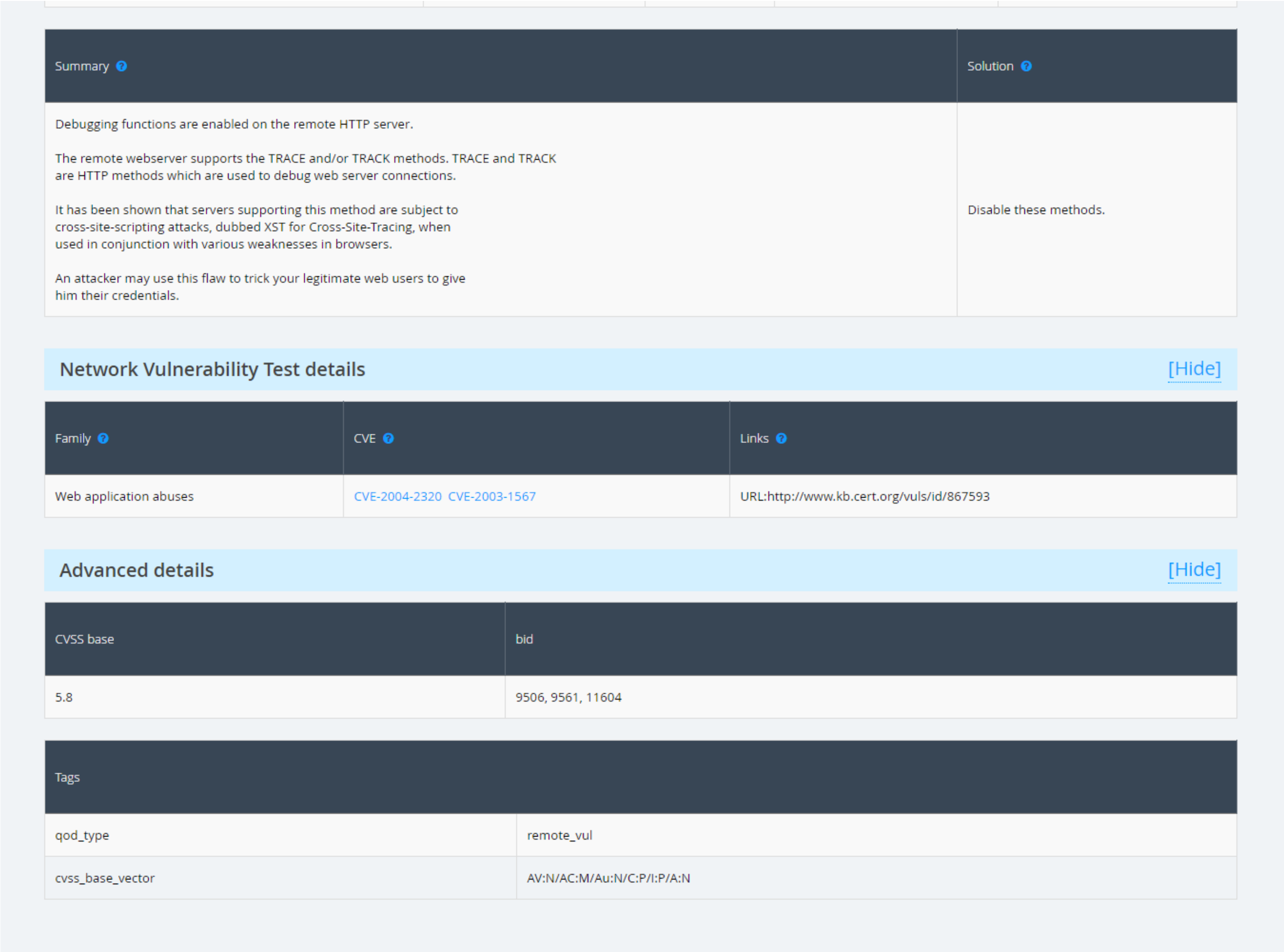
Summary	Solution
Debugging functions are enabled on the remote HTTP server. The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. It has been shown that servers supporting this method are subject to cross-site-scripting 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

Advanced details

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 [Hide]

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

Advanced details [Hide]

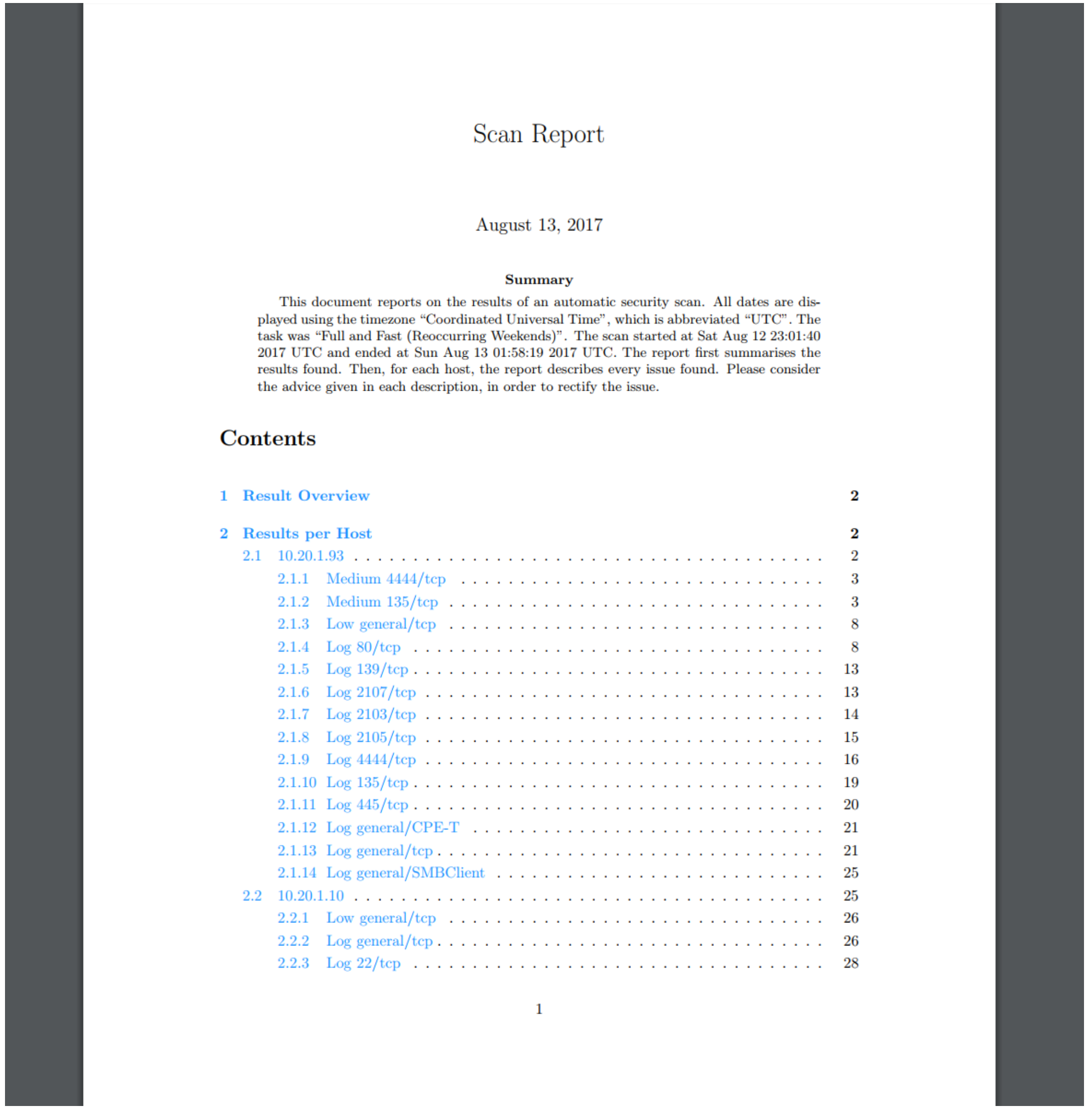
CVSS base	bid
5.8	9506, 9561, 11604

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

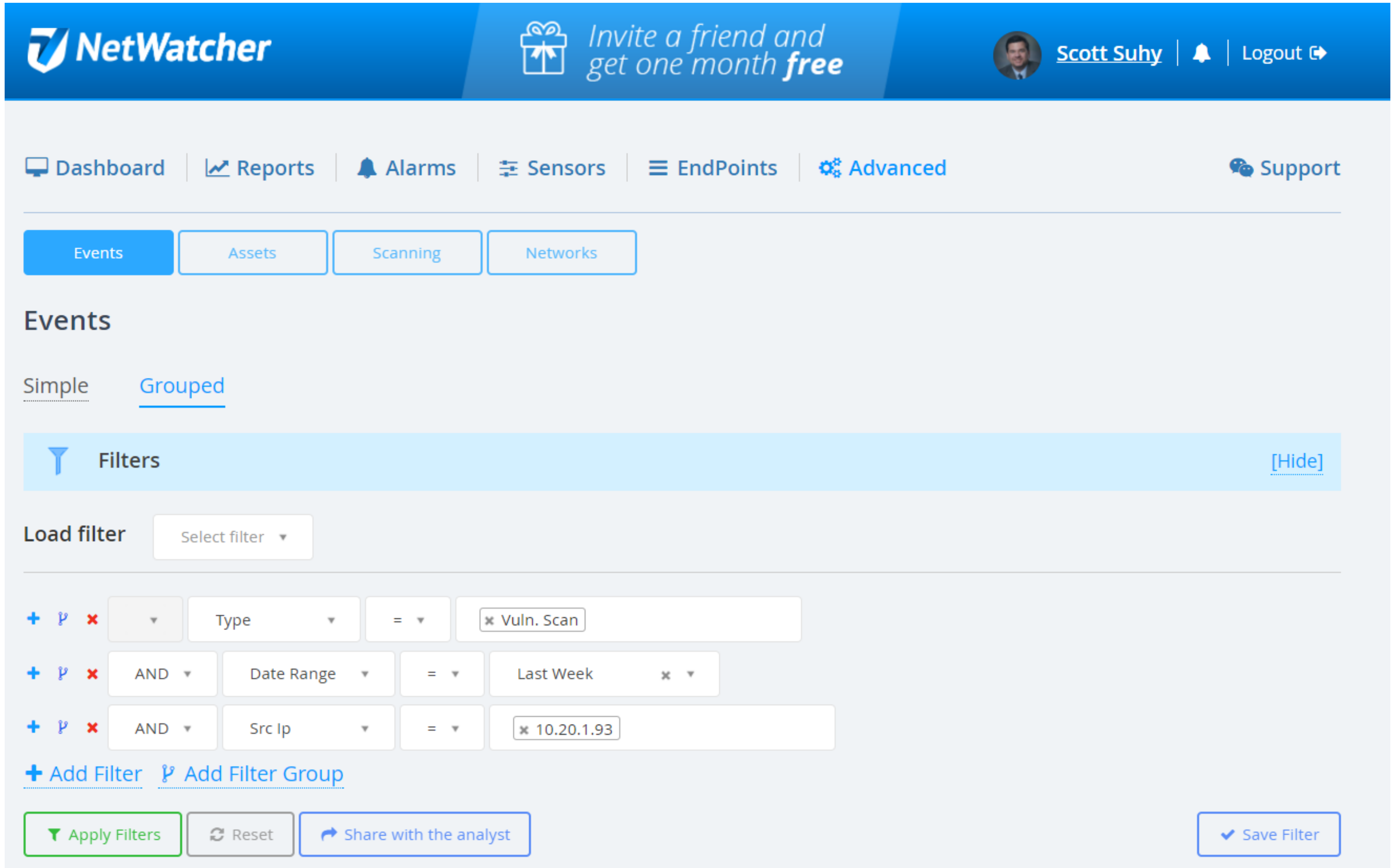
This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Full and Fast (Reoccurring Weekends)". The scan started at Sat Aug 12 23:01:40 2017 UTC and ended at Sun Aug 13 01:58:19 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

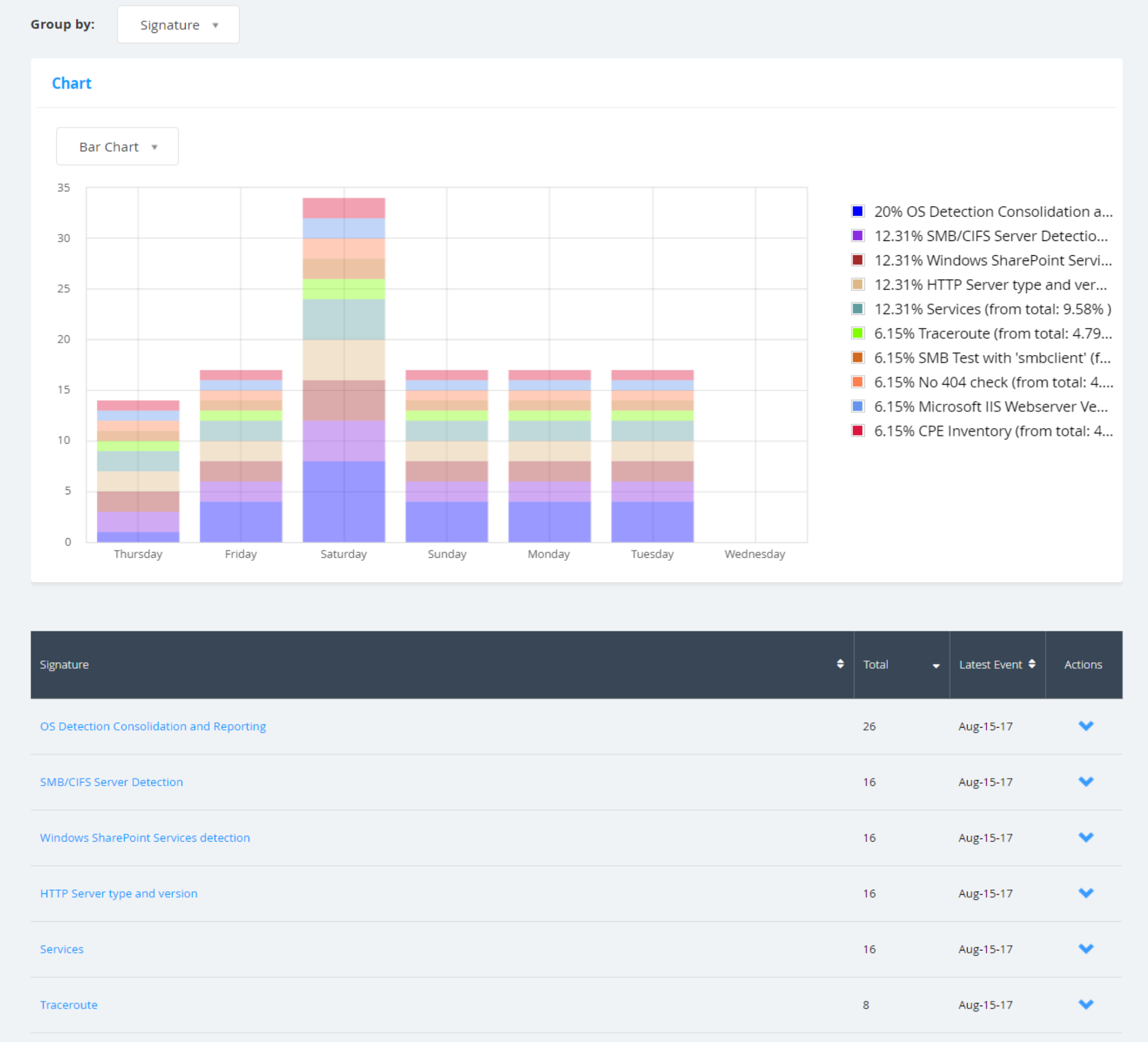
AND Date Range = Last Week

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

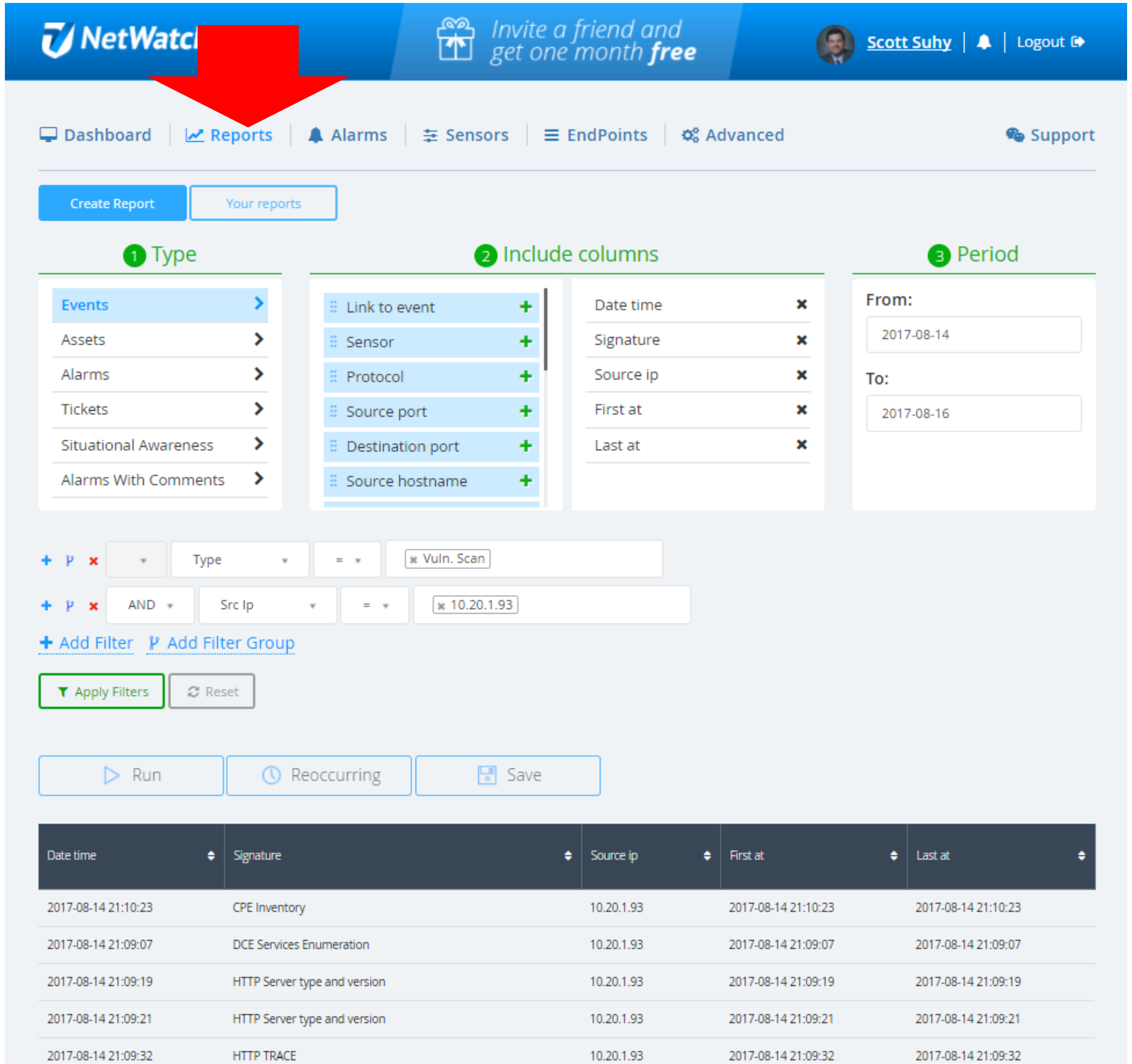
Bar Chart

35
30
25
20
15
10
5
0
Thursday
Friday
Saturday
Sunday
Monday
Tuesday
Wednesday
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



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.

https://netwatcher.com