5 Finding Vulnerabilities

Lab Scenario

Now that you have done such a great job of finding and enumerating all the machines in your target list, it is time to start associating vulnerabilities that you will be able to exploit. You are asked to use two vulnerability scanners to perform testing on one machine and then compare the results for future exploitation. STAY IN THE BOUNDS OF THE ASSESSMENT, WE ARE NOT EXPLOITING AT THIS TIME.

Lab Objectives

1. To learn the basics of Vulnerability Assessments.
2. Learn how to use Nessus and Saint.
3. Learn how to read the reports and compare different products.

Lab Resources

1. Nessus (Optional)
2. Saint – Saint VM

Lab Tasks Overview

1. Use Nessus to scan one of your servers.
    a. Connect the Nessus client to the server localhost.
    b. Enter the server you want to scan.
    c. Choose Scan Now and wait.
2. Analyze the results when you are finished.
3. Start Saint
4. Under the Scan Set-Up tab, enter the same server you scanned with Nessus.
5. Choose Scan Now and wait patiently.
6. Once the scan is finished use the Report Writer to produce a Full Technical Report.
7. Compare the results with the Nessus Scan.

Lab Details - Step-by-Step Instructions

5.1 Nessus Vulnerability Scanner

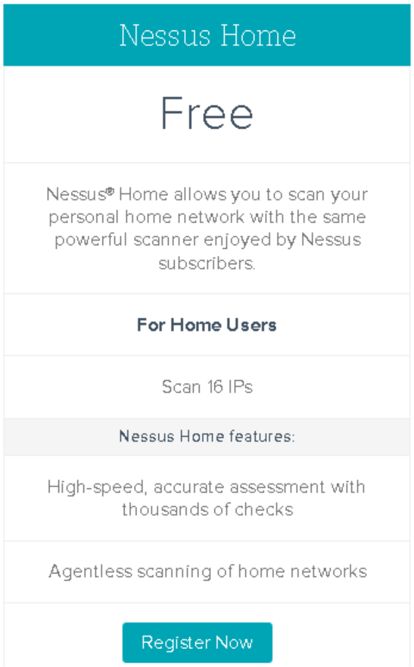
This is to be done on your Kali Linux VM.

Pre-steps:

Google “Obtain activation code Nessus home feed” or go here to register and obtain an activation code:

https://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code

Select “Register Now” for activation code which will be sent to email used while registering.



Nessus Home

Free

Nessus® Home allows you to scan your personal home network with the same powerful scanner enjoyed by Nessus subscribers.

For Home Users

Scan 16 IPs

Nessus Home features:

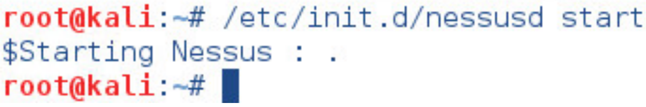
High-speed, accurate assessment with thousands of checks

Agentless scanning of home networks

Check your email for the activation code. Copy and paste activation code into Nessus, as requested.

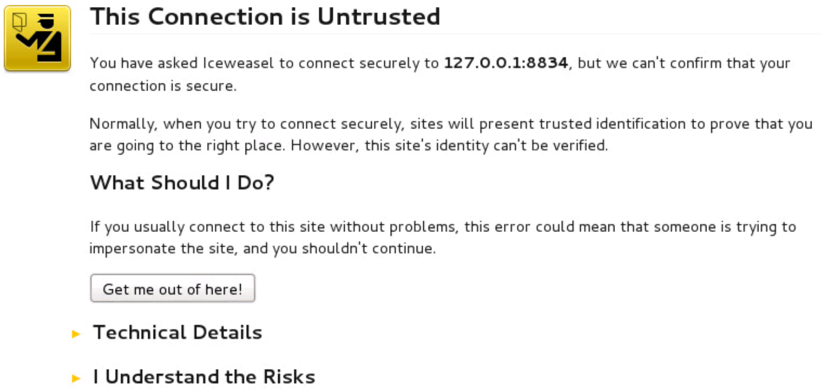
Note: The Reporting options are not available in Nessus home.

1. Run the following command to start Nessus: /etc/init.d/nessusd start



```
root@kali:~# /etc/init.d/nessusd start
$Starting Nessus : .
root@kali:~# 
```

2. Now open the web browser and goto https://127.0.0.1:8834/



This Connection is Untrusted

You have asked Iceweasel to connect securely to **127.0.0.1:8834**, but we can't confirm that your connection is secure.

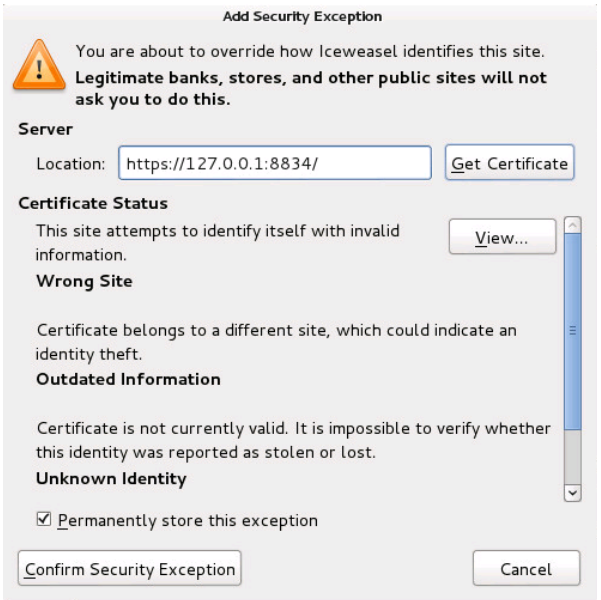
Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

3. If you receive this message, click “I Understand the Risks” and then Add Exception...

4. On the next screen click “Confirm Security Exception”



Add Security Exception

You are about to override how Iceweasel identifies this site. **Legitimate banks, stores, and other public sites will not ask you to do this.**

Server

Location: https://127.0.0.1:8834/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

Certificate belongs to a different site, which could indicate an identity theft.

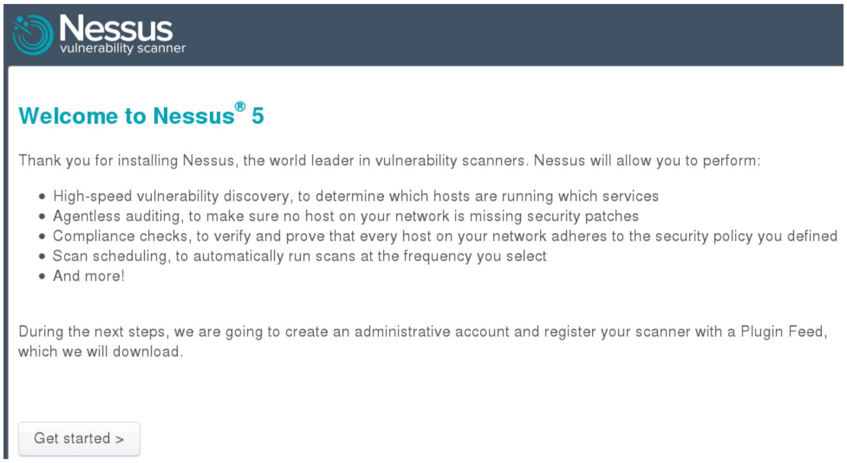
Outdated Information

Certificate is not currently valid. It is impossible to verify whether this identity was reported as stolen or lost.

Unknown Identity

☑ Permanently store this exception

5. Click “Get Started”



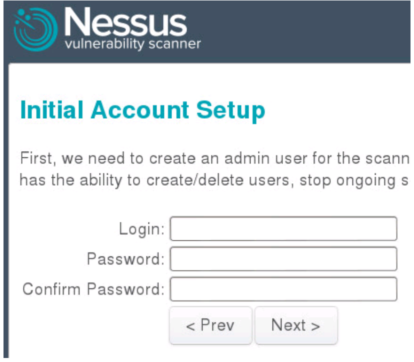
Welcome to Nessus® 5

Thank you for installing Nessus, the world leader in vulnerability scanners. Nessus will allow you to perform:

- High-speed vulnerability discovery, to determine which hosts are running which services
- Agentless auditing, to make sure no host on your network is missing security patches
- Compliance checks, to verify and prove that every host on your network adheres to the security policy you defined
- Scan scheduling, to automatically run scans at the frequency you select
- And more!

During the next steps, we are going to create an administrative account and register your scanner with a Plugin Feed, which we will download.

a. Choose a username and password and click Next.

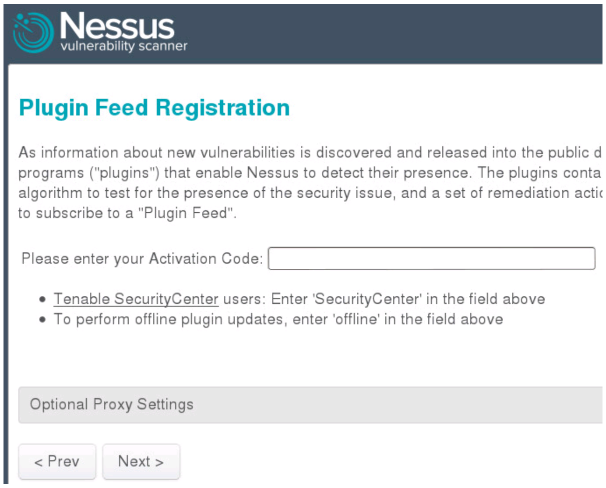


Initial Account Setup

First, we need to create an admin user for the scann
has the ability to create/delete users, stop ongoing s

Login:
Password:
Confirm Password:

b. Enter in the activation code that was emailed after registering and click Next.



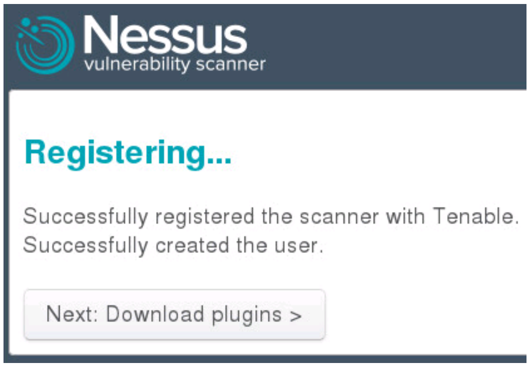
Plugin Feed Registration

As information about new vulnerabilities is discovered and released into the public d
programs ("plugins") that enable Nessus to detect their presence. The plugins conta
algorithm to test for the presence of the security issue, and a set of remediation actic
to subscribe to a "Plugin Feed".

Please enter your Activation Code:

- Tenable SecurityCenter users: Enter 'SecurityCenter' in the field above
- To perform offline plugin updates, enter 'offline' in the field above

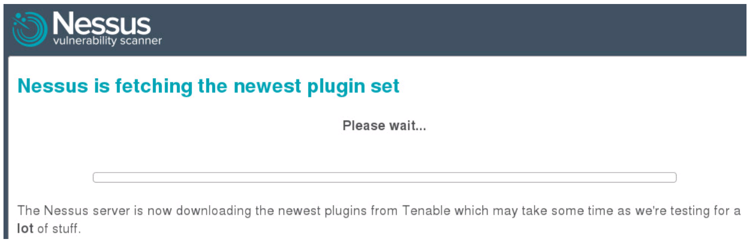
c. If you registered successfully, you will reviece this message. Click Next.



Registering...

Successfully registered the scanner with Tenable.
Successfully created the user.

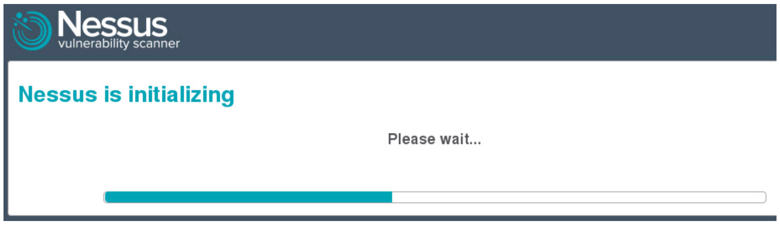
d. Nessus will take a while to download plugins and initialize.



Nessus is fetching the newest plugin set

Please wait...

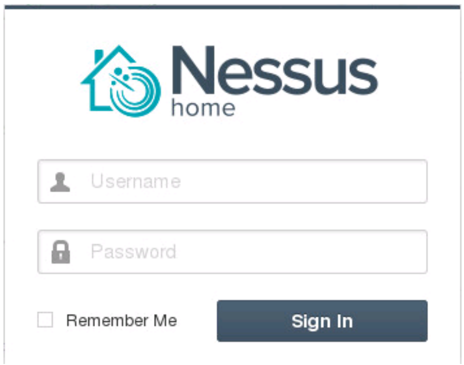
The Nessus server is now downloading the newest plugins from Tenable which may take some time as we're testing for a **lot** of stuff.



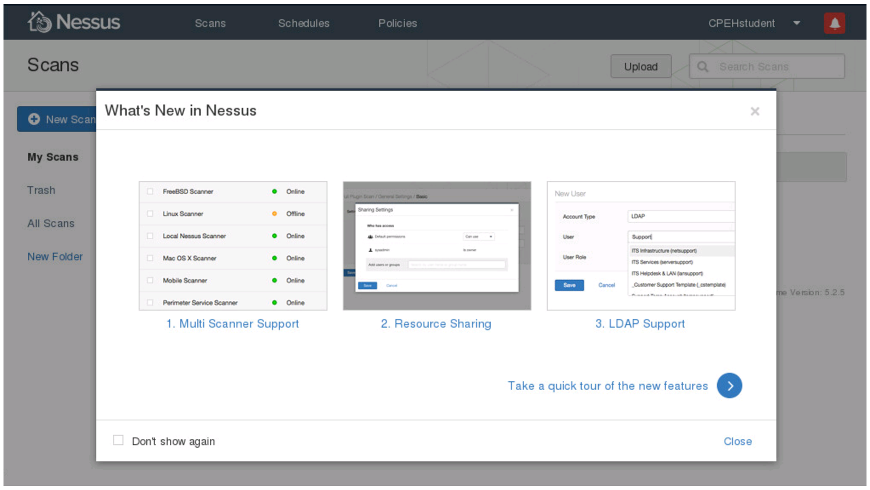
Nessus is initializing

Please wait...

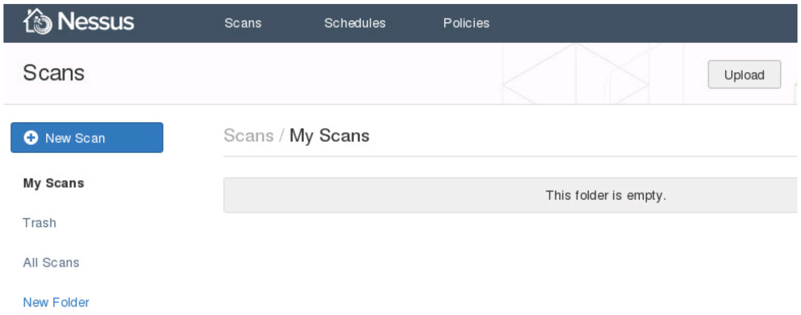
e. Log into Nessus after the initialization is complete.



6. Upon logging in, click Close.

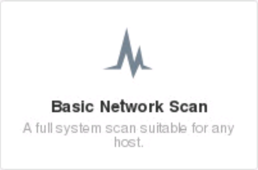


7. Create a new policy by clicking “Policies”



8. Click New Policy

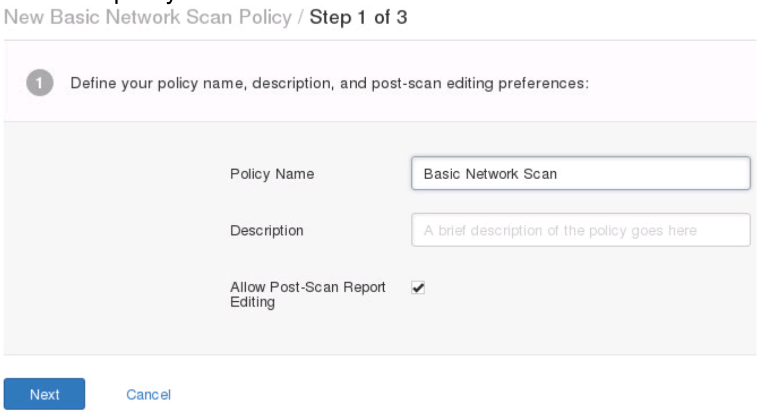
9. There are several scan poilies to choose from. For this example Click “Basic Network Scan”



Basic Network Scan

A full system scan suitable for any host.

a. Name the policy and click Next.



New Basic Network Scan Policy / Step 1 of 3

1 Define your policy name, description, and post-scan editing preferences:

Policy Name: Basic Network Scan

Description: A brief description of the policy goes here

Allow Post-Scan Report Editing ☑

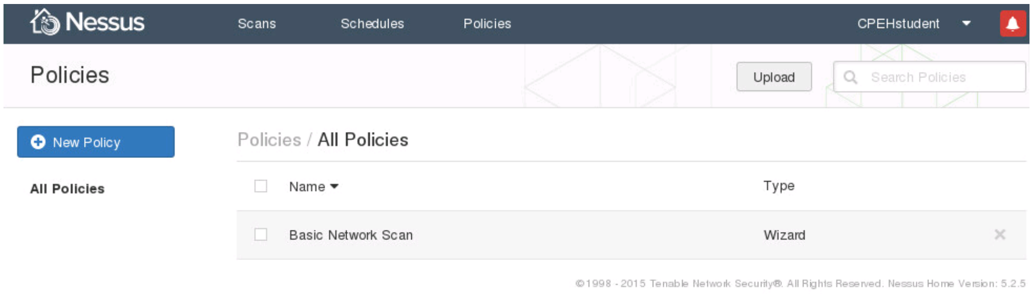
b. In Step 2 of 3, leave “Scan type” set to “Internal” and click Next.

NOTE:

External Network Scan - This policy is tuned to scan externally facing hosts, which typically present fewer services to the network. The plugins associated with known web application vulnerabilities (CGI Abuses and CGI Abuses: XSS plugin families) are enabled in this policy. Also, all 65,535 ports are scanned for on each target

Internal Network Scan - This policy is tuned for better performance, taking into account that it may be used to scan large internal networks with many hosts, several exposed services, and embedded systems such as printers. The "CGI Abuse" plugins are not enabled and a standard set of ports is scanned for, not all 65,535.

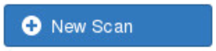
c. In Step 3 of 3, Windows enumeration can be setup if the username, password and/or domain is known. Otherwise, leave this blank and click Save to complete the scan policy



Policies / All Policies

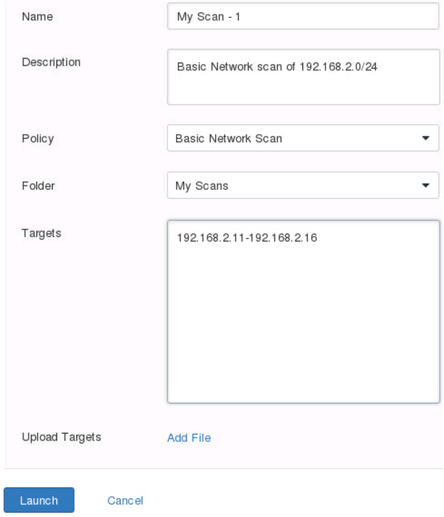
	Name	Type
□	Basic Network Scan	Wizard

©1998 - 2015 Tenable Network Security®. All Rights Reserved. Nessus Home Version: 5.2.5

10. Now create a new scan by clicking “Scans” at the top then 

11. Fill in each field and click “Launch”.

    Note: To save scan time, and IP range was used in the “targets” field that only included the range of computers available to scan. 192.168.2.0/24 could also be used.



Name: My Scan - 1

Description: Basic Network scan of 192.168.2.0/24

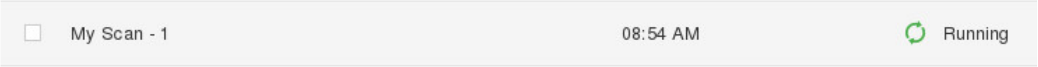
Policy: Basic Network Scan

Folder: My Scans

Targets: 192.168.2.11-192.168.2.16

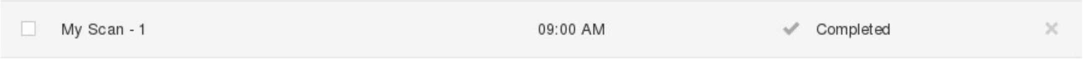
Upload Targets: Add File

12. This scan will take about 10 minutes.



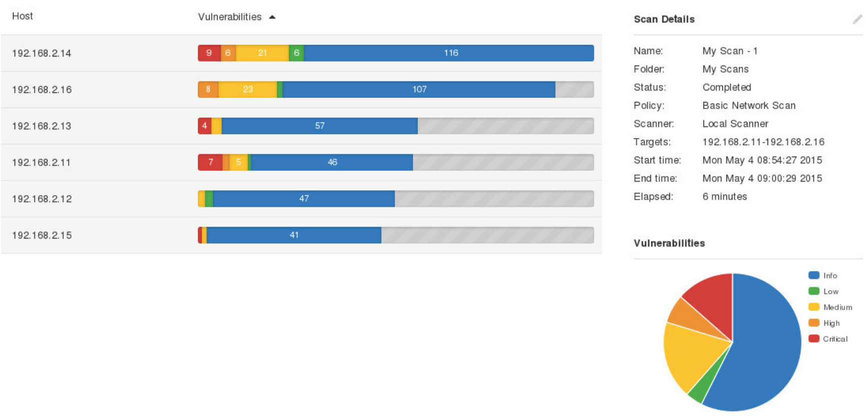
□ My Scan - 1 08:54 AM Running

13. Click “My Scan – 1” to view the scan results.



□ My Scan - 1 09:00 AM ✓ Completed ✕

14. Each host is listed with a graphical representations of its vulnerabilities.



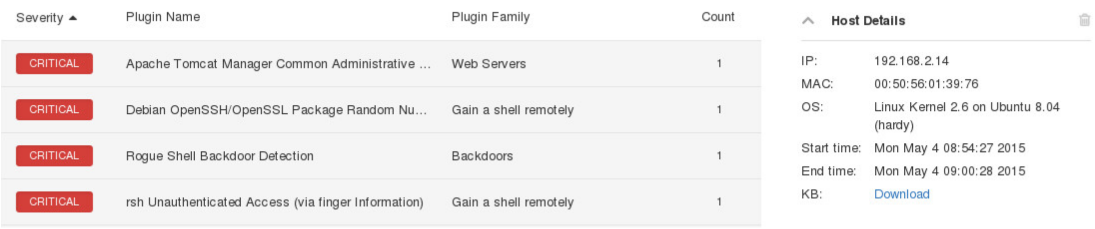
Host	Vulnerabilities ▲
192.168.2.14	9 6 21 6 116
192.168.2.16	8 23 107
192.168.2.13	4 57
192.168.2.11	7 5 46
192.168.2.12	47
192.168.2.15	41

Scan Details

Name: My Scan - 1
Folder: My Scans
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Targets: 192.168.2.11-192.168.2.16
Start time: Mon May 4 08:54:27 2015
End time: Mon May 4 09:00:29 2015
Elapsed: 6 minutes

Vulnerabilities

15. Click on any IP address for specific vulnerability assessment information of each host.

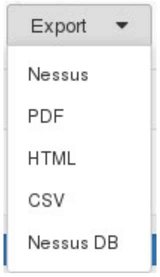


Severity ▲	Plugin Name	Plugin Family	Count
CRITICAL	Apache Tomcat Manager Common Administrative ...	Web Servers	1
CRITICAL	Debian OpenSSH/OpenSSL Package Random Nu...	Gain a shell remotely	1
CRITICAL	Rogue Shell Backdoor Detection	Backdoors	1
CRITICAL	rsh Unauthenticated Access (via finger Information)	Gain a shell remotely	1

Host Details

IP: 192.168.2.14
MAC: 00:50:56:01:39:76
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start time: Mon May 4 08:54:27 2015
End time: Mon May 4 09:00:28 2015
KB: Download

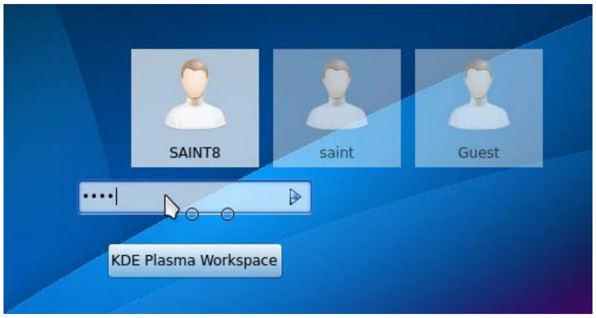
16. Click “Export” to save the report to multiple formats to view later.



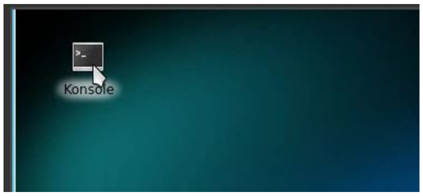
5.2 SAINT Vulnerability Scanner

This is to be done on your SAINT VM.

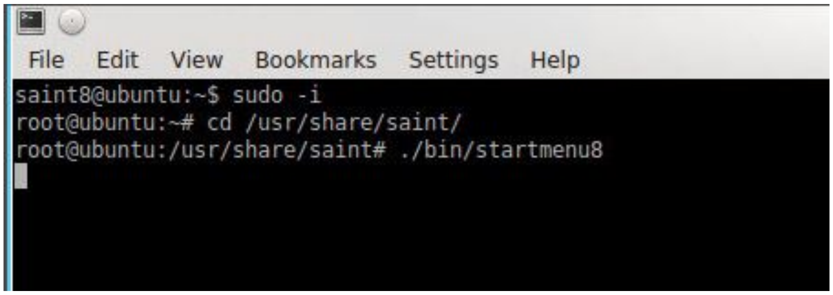
1. Log in to SAINT 8 using *toor* as password



2. Double-click Konsole icon

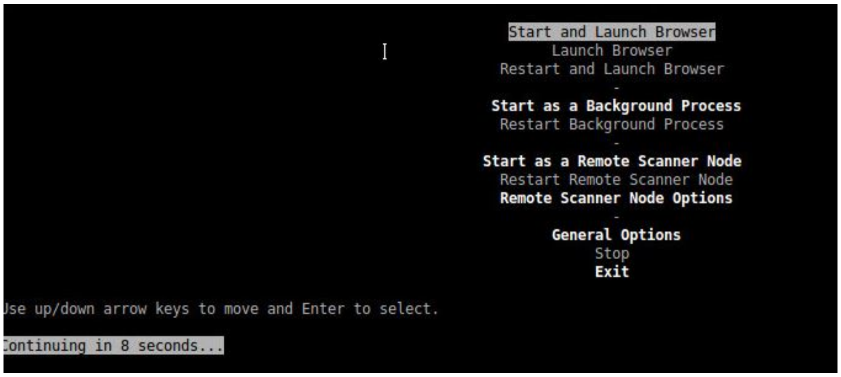


3. Once console opens, type sudo –i, press enter. Type cd /usr/share/saint/ and press enter. Type /usr/share/saint# ./bin/startmenu8



```
saint8@ubuntu:~$ sudo -i
root@ubuntu:~# cd /usr/share/saint/
root@ubuntu:/usr/share/saint# ./bin/startmenu8
```

4. In the following screen, use the up and down arrow keys to highlight *Start and Launch Browser*, then press Enter.

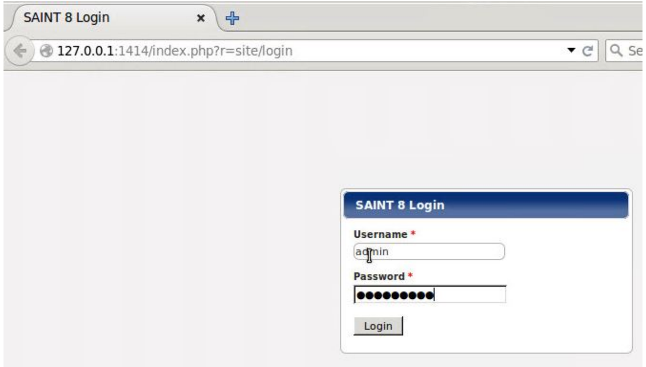


```
                                        Start and Launch Browser
                                             Launch Browser
                                       Restart and Launch Browser
                                                   -
                                       Start as a Background Process
                                        Restart Background Process
                                                   -
                                      Start as a Remote Scanner Node
                                       Restart Remote Scanner Node
                                       Remote Scanner Node Options
                                                   -
                                             General Options
                                                  Stop
                                                  Exit

Jse up/down arrow keys to move and Enter to select.

Continuing in 8 seconds...
```

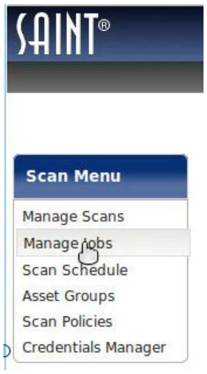
5. Once web browser opens, log in with admin /admintoor.



Username: admin

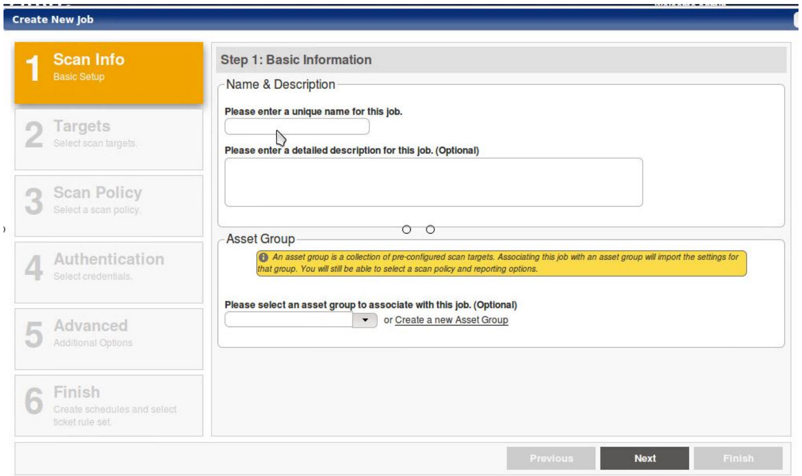
Password: ●●●●●●●●●

6. On menu options, choose Manage Jobs.



7. On the Create New Jobs wizard:

    - Enter unique job name, click Next
    - Enter Target IP address (Metasploitable), click Next
    - Select Policy Category -Vulnerability and Policy –Heavy/Vulnerability Scan, click Next
    - Leave default settings for authentication and credentials, click Next
    - Leave default settings for Advanced Settings, click Next
    - Select Schedule Immediately, click Finish



Create New Job

Step 1: Basic Information

Name & Description

Please enter a unique name for this job.

Please enter a detailed description for this job. (Optional)

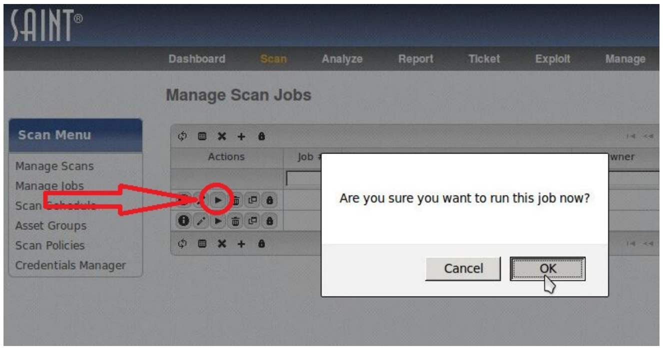
Asset Group

An asset group is a collection of pre-configured scan targets. Associating this job with an asset group will import the settings for that group. You will still be able to select a scan policy and reporting options.

Please select an asset group to associate with this job. (Optional)

or Create a new Asset Group

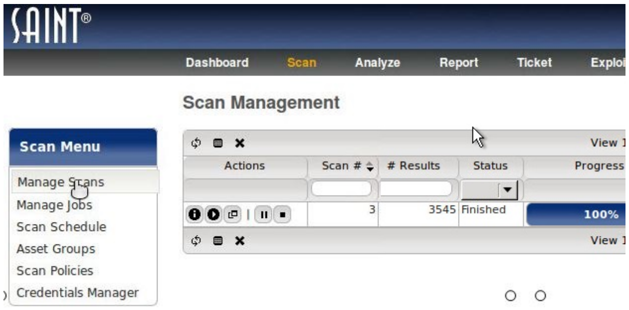
8. On Manage Scan Jobs page, select the Play button. When asked, "Are you sure you want to run this job now", select OK.



Manage Scan Jobs

Are you sure you want to run this job now?

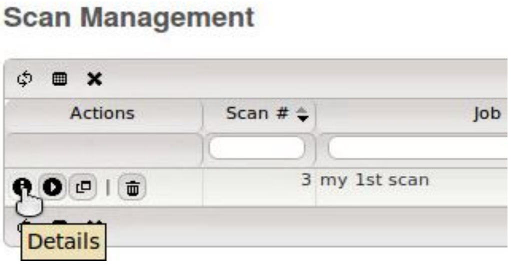
9. To watch progress of scan, select Manage Scans from the scan menu. Note: This scan will take a very long time. Start the scan but then come back to check the results the following day.



Scan Management

Actions	Scan #	# Results	Status	Progress
	3	3545	Finished	100%

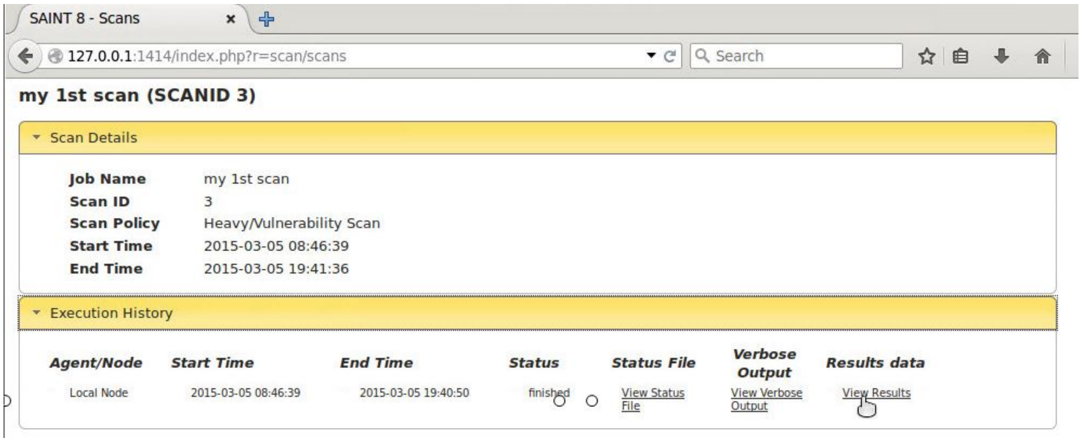
10. Once scan completes, select the Details button.



Scan Management

Actions	Scan #	Job
	3	my 1st scan

11. If needed, click on Execution History, then select View Results.



my 1st scan (SCANID 3)

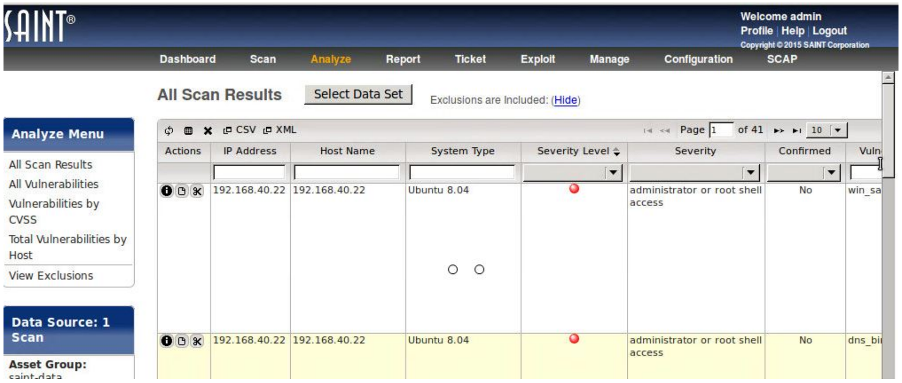
Scan Details

Job Name my 1st scan
Scan ID 3
Scan Policy Heavy/Vulnerability Scan
Start Time 2015-03-05 08:46:39
End Time 2015-03-05 19:41:36

Execution History

Agent/Node	Start Time	End Time	Status	Status File	Verbose Output	Results data
Local Node	2015-03-05 08:46:39	2015-03-05 19:40:50	finished	View Status File	View Verbose Output	View Results

12. Look over results and proceed to next step.

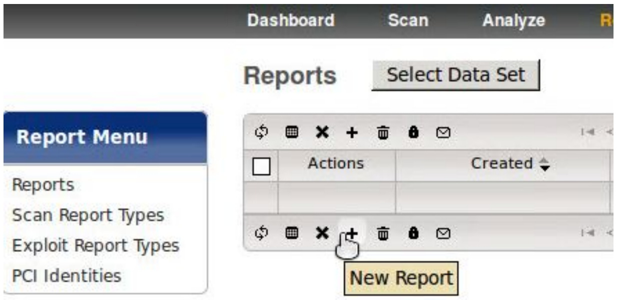


All Scan Results

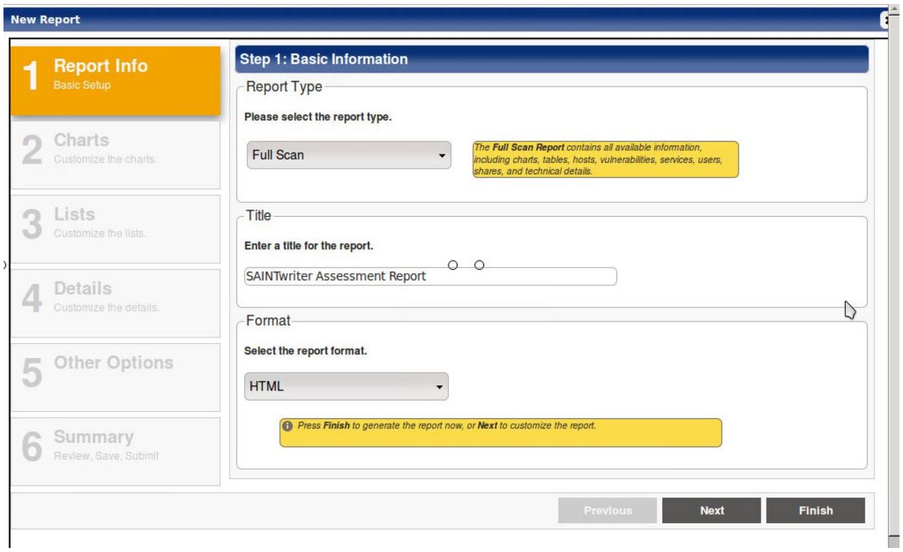
Exclusions are Included: (Hide)

Actions	IP Address	Host Name	System Type	Severity Level	Severity	Confirmed	Vuln
	192.168.40.22	192.168.40.22	Ubuntu 8.04	●	administrator or root shell access	No	win_sa
	192.168.40.22	192.168.40.22	Ubuntu 8.04	●	administrator or root shell access	No	dns_bi

13. Click on Report from top menu and then select + for the New Report wizard.



14. On the New Report wizard, select report type, title and format, then click Next.



Step 1: Basic Information

Report Type

Please select the report type.

Full Scan

*The **Full Scan Report** contains all available information, including charts, tables, hosts, vulnerabilities, services, users, shares, and technical details.*

Title

Enter a title for the report.

SAINTwriter Assessment Report

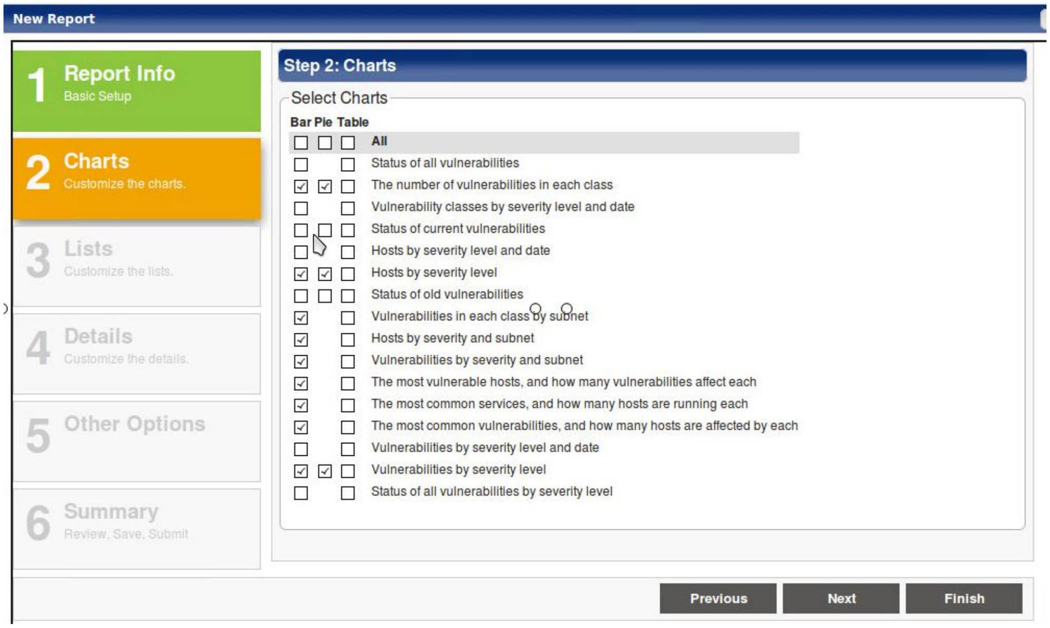
Format

Select the report format.

HTML

*Press **Finish** to generate the report now, or **Next** to customize the report.*

15. Select appropriate check boxes for charts, click Next.

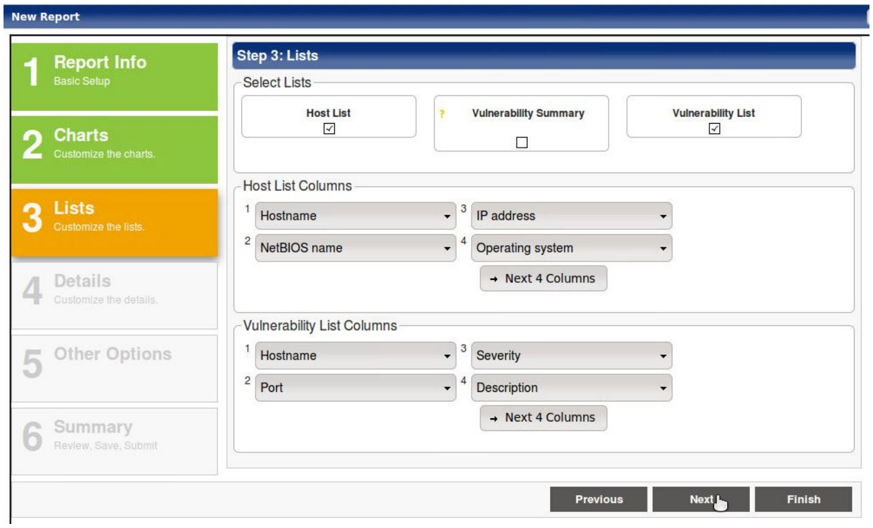


Step 2: Charts

Select Charts

Bar	Pie	Table	
□	□	□	**All**
□		□	Status of all vulnerabilities
☑	☑	□	The number of vulnerabilities in each class
□		□	Vulnerability classes by severity level and date
□	□	□	Status of current vulnerabilities
□		□	Hosts by severity level and date
☑	☑	□	Hosts by severity level
□	□	□	Status of old vulnerabilities
☑		□	Vulnerabilities in each class by subnet
☑		□	Hosts by severity and subnet
☑		□	Vulnerabilities by severity and subnet
☑		□	The most vulnerable hosts, and how many vulnerabilities affect each
☑		□	The most common services, and how many hosts are running each
☑		□	The most common vulnerabilities, and how many hosts are affected by each
□		□	Vulnerabilities by severity level and date
☑	☑	□	Vulnerabilities by severity level
□		□	Status of all vulnerabilities by severity level

16. On the Lists page, click Next.



Step 3: Lists

Select Lists

Host List ☑

Vulnerability Summary □

Vulnerability List ☑

Host List Columns

1 Hostname
2 NetBIOS name
3 IP address
4 Operating system

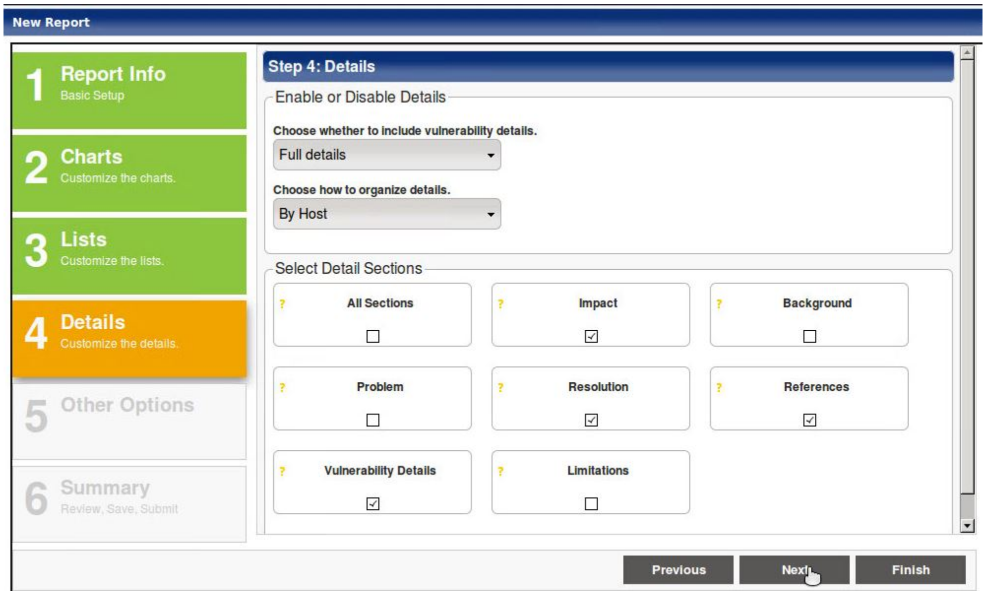
→ Next 4 Columns

Vulnerability List Columns

1 Hostname
2 Port
3 Severity
4 Description

→ Next 4 Columns

17. Click Next on the Details page.



Step 4: Details

Enable or Disable Details

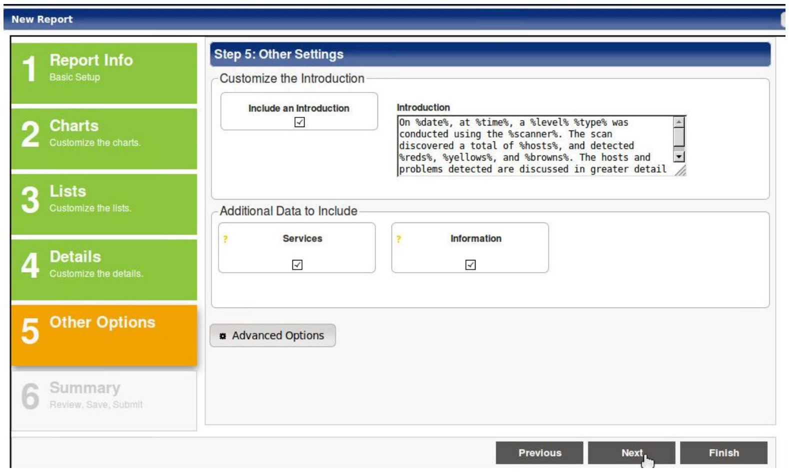
Choose whether to include vulnerability details.
Full details

Choose how to organize details.
By Host

Select Detail Sections

All Sections □	Impact ☑	Background □
Problem □	Resolution ☑	References ☑
Vulnerability Details ☑	Limitations □	

18. Click Next on the Other Options page.



Step 5: Other Settings

Customize the Introduction

Include an Introduction ☑

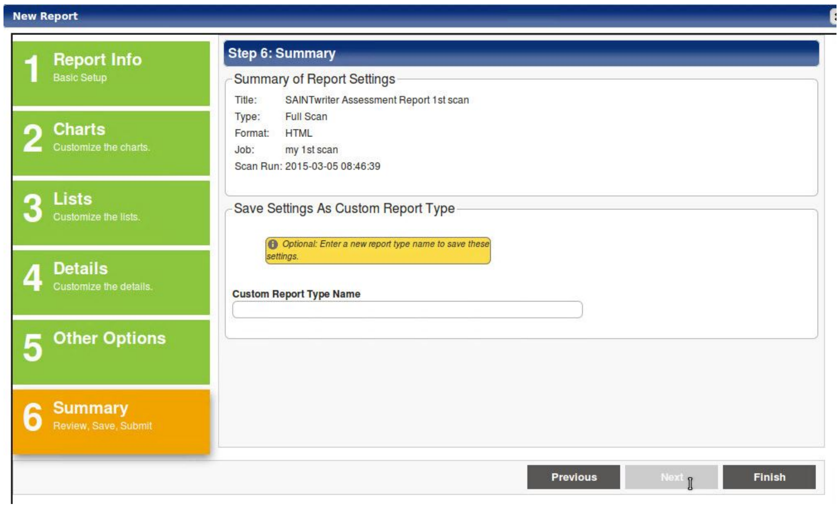
Introduction

```
On %date%, at %time%, a %level% %type% was
conducted using the %scanner%. The scan
discovered a total of %hosts%, and detected
%reds%, %yellows%, and %browns%. The hosts and
problems detected are discussed in greater detail
```

Additional Data to Include

Services ☑
Information ☑

19. Select Finish on the Summary page.



New Report

1	Report Info Basic Setup
2	Charts Customize the charts.
3	Lists Customize the lists.
4	Details Customize the details.
5	Other Options
6	Summary Review, Save, Submit

Step 6: Summary

Summary of Report Settings

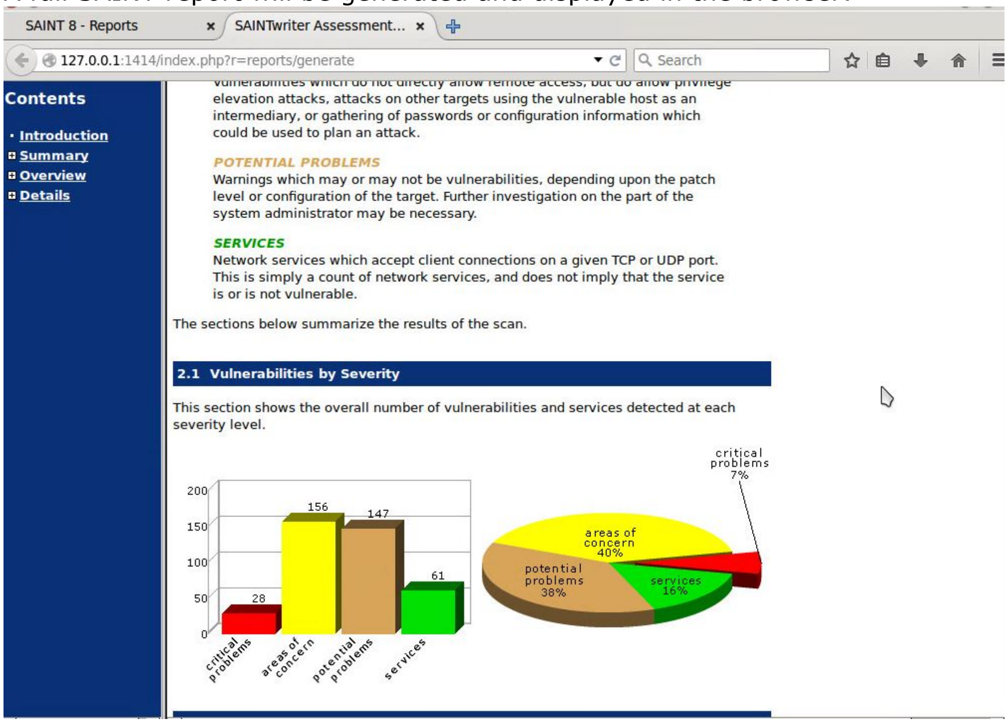
Title: SAINTwriter Assessment Report 1st scan
Type: Full Scan
Format: HTML
Job: my 1st scan
Scan Run: 2015-03-05 08:46:39

Save Settings As Custom Report Type

Optional: Enter a new report type name to save these settings.

Custom Report Type Name

20. A full SAINT report will be generated and displayed in the browser:



SAINT 8 - Reports
SAINTwriter Assessment...
127.0.0.1:1414/index.php?r=reports/generate
Search

Contents

- Introduction
- Summary
- Overview
- Details

vulnerabilities which do not directly allow remote access, but do allow privilege elevation attacks, attacks on other targets using the vulnerable host as an intermediary, or gathering of passwords or configuration information which could be used to plan an attack.

POTENTIAL PROBLEMS
Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Further investigation on the part of the system administrator may be necessary.

SERVICES
Network services which accept client connections on a given TCP or UDP port. This is simply a count of network services, and does not imply that the service is or is not vulnerable.

The sections below summarize the results of the scan.

2.1 Vulnerabilities by Severity

This section shows the overall number of vulnerabilities and services detected at each severity level.

Document all the results and reports gathered during the lab.

Tool/Utility	Information Collected/Objectives Achieved
SAINT	Scan Target Machine: Windows Server 2008 Performed Scan Policy: Network Scan Policy Target IP Address: Result: SAINT Report