





Module 06

Vulnerability Assessments

Vulnerability Assessments

Once the plausible threats are identified, a vulnerability assessment must be performed. The vulnerability assessment considers the potential impact of loss from a successful attack as well as the vulnerability of the facility/location to an attack. Impact of loss is the degree to which the mission of the agency is impaired by a successful attack from the given threat. A key component of the vulnerability assessment is properly defining the ratings for impact of loss and vulnerability. These definitions may vary greatly from facility to facility. For example, the amount of time that mission capability is impaired is an important part of impact of loss. If the facility being assessed is an Air Route Traffic Control Tower, a downtime of a few minutes may be a serious impact of loss, while for a Social Security office, a downtime of a few minutes would be minor. A sample set of definitions for impact of loss is provided below. These definitions are for an organization that generates revenue by serving the public.

ICON KEY	
	Important Information
	Quiz
	CPTe Labs
	Course Review

Lab Objectives

This lab will give you experience in scanning the network for vulnerabilities, and show you how to use Nessus. It will teach you how to:

- Use the SAINT tools
- Scan the network for vulnerabilities

Lab Scenario

Once attackers have the information related to network devices, they can use it as an entry point to a network for a comprehensive attack and perform many types of attacks ranging from DoS attacks to unauthorized administrative access. If attackers are able to get traceroute information, they might use a methodology such as firewalking to determine the services that are allowed through a firewall.

Lab Environment

This lab requires:

- A Firefox web browser with Internet connection
- Administrative privileges to run tools

Lab Duration

Time: 40 Minutes

Overview of Vulnerability Assessment in Penetration Testing

Vulnerability Assessment and Penetration Testing are two types of vulnerability testing. The tests have different strengths and are often combined to achieve a more complete vulnerability analysis. In short, Penetration Testing and Vulnerability Assessments perform two different tasks, usually with different results, within the same area of focus.

Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to cause damage and those that cannot. Vulnerability scanners alert companies to the preexisting flaws in their code and where they are located. Penetration tests attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application. Penetration tests find exploitable flaws and measure the severity of each. A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system. Together, penetration testing and vulnerability assessment tools provide a detailed picture of the flaws that exist in an application and the risks associated with those flaws.

Lab Tasks

Recommended labs to assist you in Enumeration:

- **Lab 1: Vulnerability Assessment Using SAINT Tool**

Lab Analysis

Analyze and document the results related to the lab. Give your opinion on your target's security posture and exposure through public and free information.

Lab

1

ICON KEY



Important
Information



Quiz



CPTe Labs



Course
Review

Vulnerability Assessment Using SAINT

SAINT Overview

SAINT is the Security Administrator's Integrated Network Tool. It is used to non-intrusively detect security vulnerabilities on any remote target, including servers, workstations, networking devices, and other types of nodes. It will also gather information such as operating system types and open ports. The SAINT graphical user interface provides access to SAINT's data management, scan configuration, scan scheduling, and data analysis capabilities through a web browser. Different aspects of the scan results are presented in linked HTML pages, and reports on complete scan results can be generated and saved.

Lab Scenario

SAINT begins a scan by detecting all live targets within the given target list or range. Next, SAINT will launch a set of core probes to run against each target. The selected scanning level determines which core probes SAINT runs. The data from the probes is used by SAINT's inference engine to schedule further probes and to infer vulnerabilities and other information based on rule sets. Data is logged to a file in a plain text format that can be interpreted by SAINT's data analysis and reporting modules to present the results in an easily readable fashion.

This lab will give you experience on vulnerability scanning, and show you how to use SAINT. It will teach you how to:

- Use the SAINT tool
- Scan the network for vulnerabilities

Lab Resources

To run this lab, you need the following:

- SAINT Virtual Machine
- Web browser with Internet access

Lab Duration

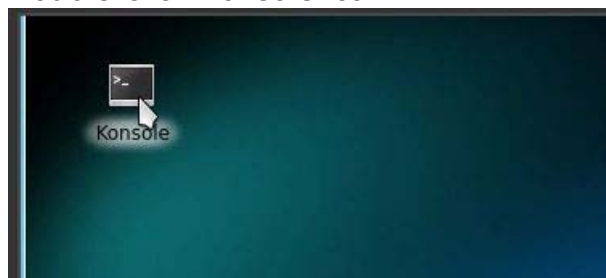
Time: 20 Minutes

Lab Tasks

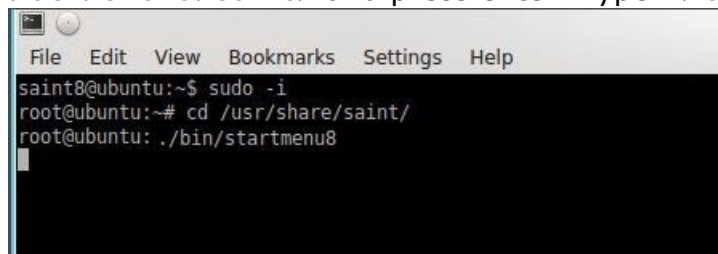
1. Log into SAINT 8(on SAINT 10 VM) using *toor* as password



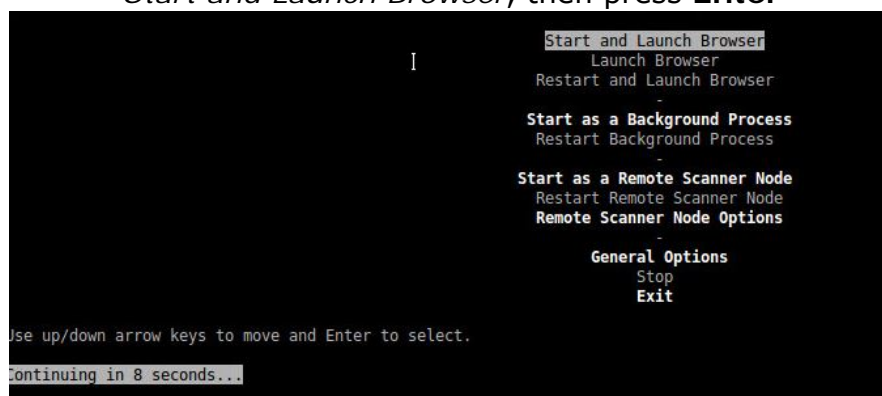
2. Double-click Konsole icon



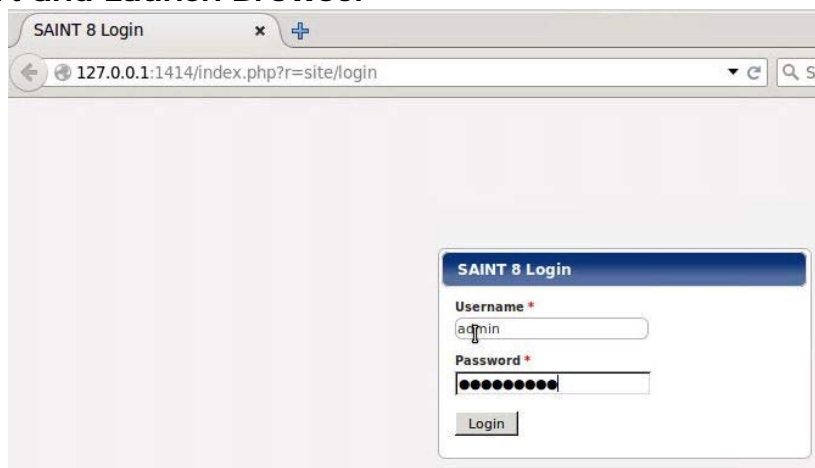
3. Once console opens, type **sudo -i**, press enter. Type **cd /usr/share/saint/** and press enter. Type **./bin/startmenuu8**



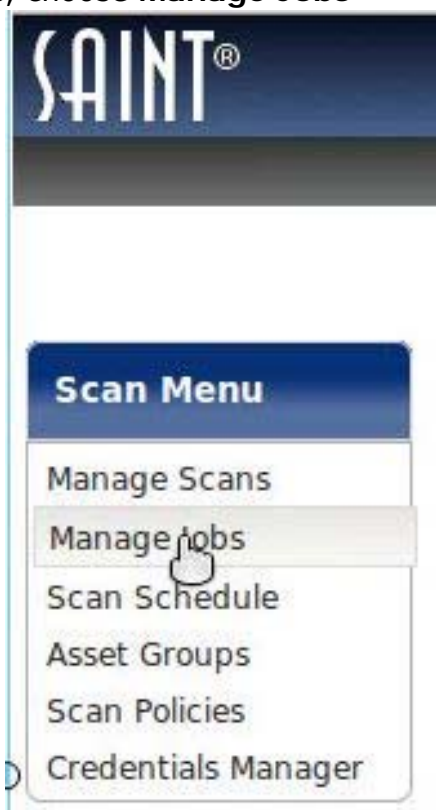
4. In the following screen, use the up and down arrow keys to highlight *Start and Launch Browser*, then press **Enter**



5. Once web browser opens, log in with **admin / admintoor**
FYI: If browser does not display, first select **STOP** from previous menu then select **Start and Launch Browser**

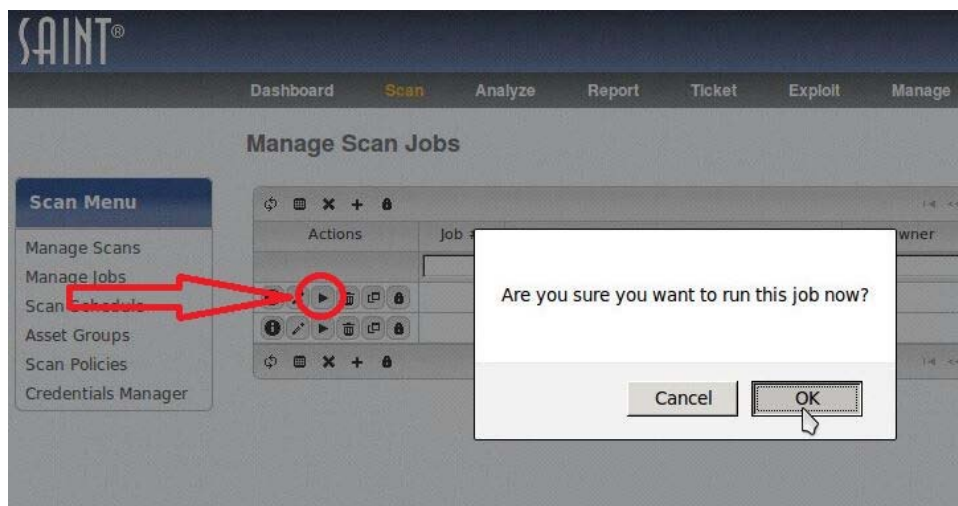


6. On menu options, choose **Manage Jobs**



7. On the Manage Scan Jobs wizard:
 - Select + to start the wizard
 - Enter unique job name, click Next
 - Enter Target IP address (Metasploitable), click Next
 - Select a Policy Category and a Policy, (Ex. **Information Gathering, Discovery**, then click Next
 - Leave default settings for authentication and credentials, click Next
 - Leave default settings for Advanced Settings, click Next
 - Select Schedule Immediately, click Finish

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



9. To watch progress of scan, select Manage Scans from the scan menu



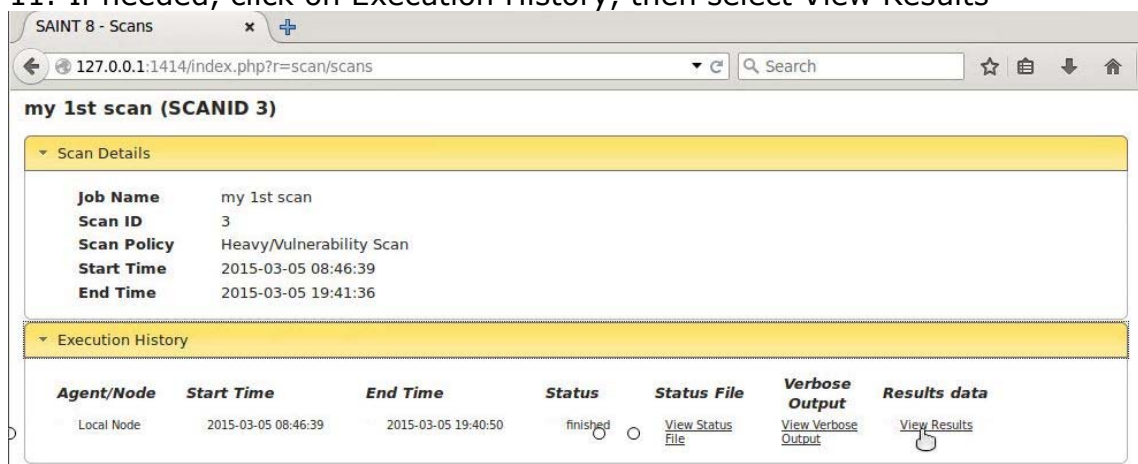
Note : Vulnerability Scans take a long time, plan on starting it and checking the results the following day

10. Once scan completes, select the Details button

Scan Management

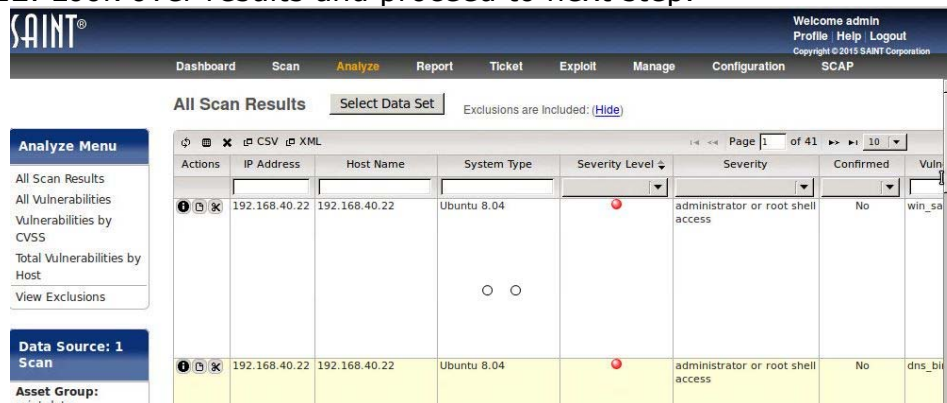


11. If needed, click on Execution History, then select View Results

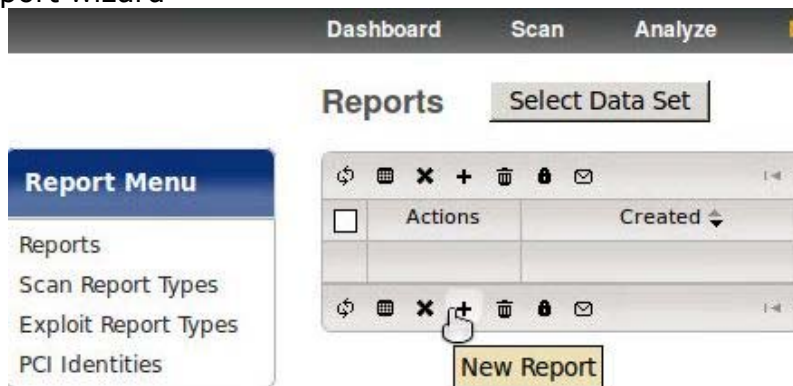


Note: View results will not have any interesting details if the scan was not a vulnerability scan of some type. If you ran an Information Gathering/Discovery scan the first time, try going back and running a vulnerability scan to complete these last steps of the lab.

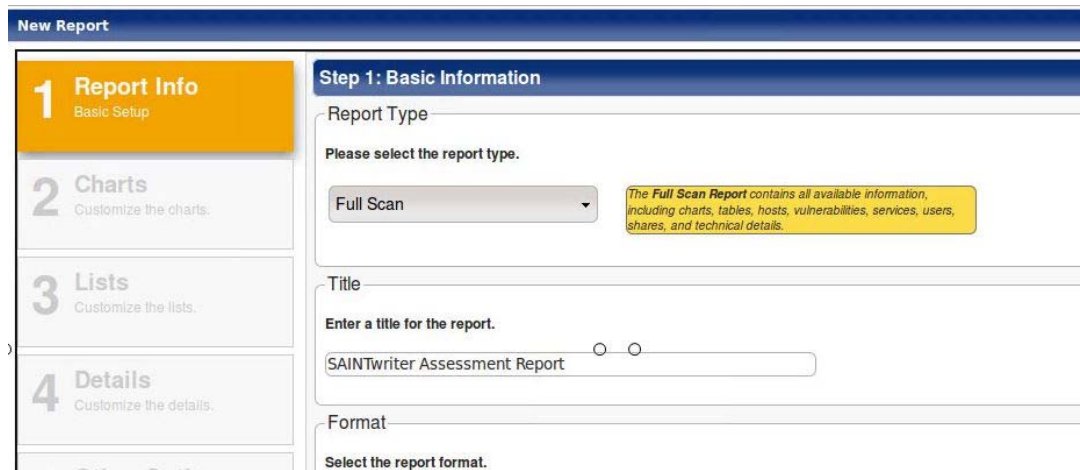
12. Look over results and proceed to next step.



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



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

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 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

Previous Next Finish

16. On the Lists page, click **Next**

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 3: Lists

Select Lists

Host List ☒ Vulnerability Summary ☐ Vulnerability List ☒

Host List Columns

1 Hostname 3 IP address

2 NetBIOS name 4 Operating system

Next 4 Columns

Vulnerability List Columns

1 Hostname 3 Severity

2 Port 4 Description

Next 4 Columns

Previous Next Finish

17. Click **Next** on the Details 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 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 ☒

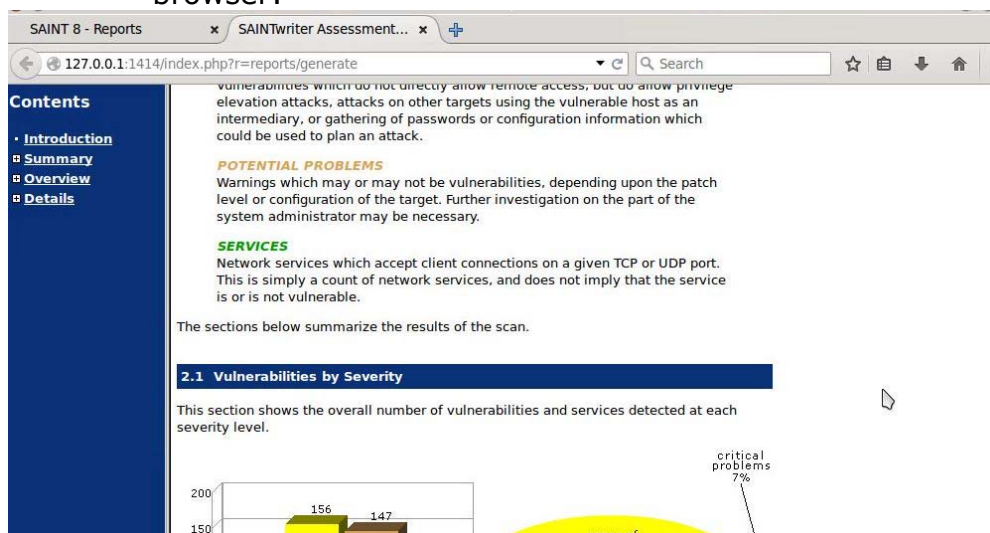
Vulnerability Details ☒ Limitations ☐

Previous Next Finish

18. Click Next on the Other Options page

19. Select Finish on the Summary page

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



Lab Analysis

Document all the results and reports gathered during the lab.

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

Quiz

1. Scan other Windows OS in the lab.
2. Use different scan options in SAINT.