

# Lab 05 Report

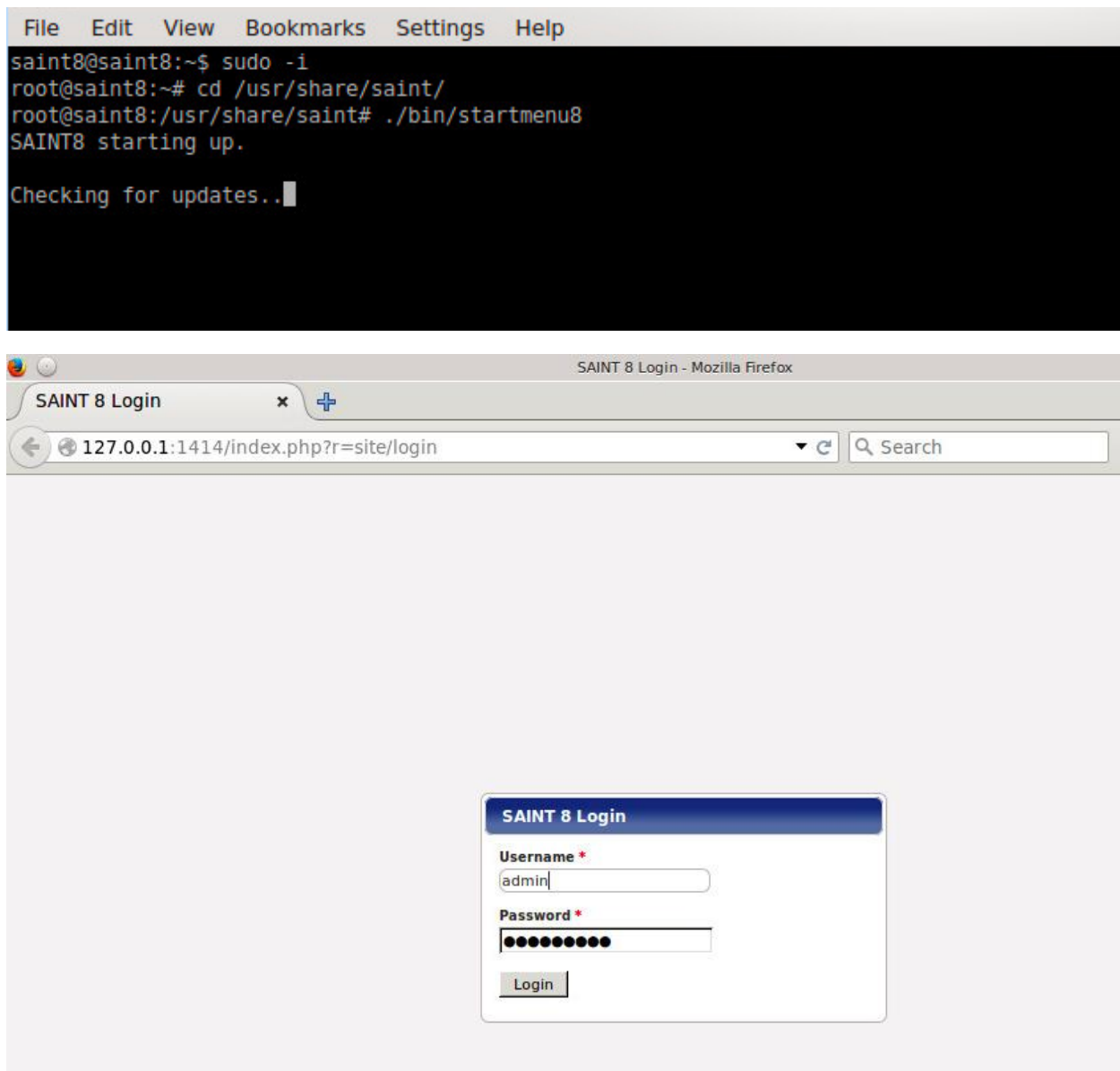
Report by Joynal Abedin

## Documentation

### 5.1 Nessus Vulnerability Scanner

I skipped this section with Prof. Schott's permission.

### 5.2 SAINT vulnerability Scanner



# Lab 05 Report

The screenshot shows the SAINT web application interface. At the top, there is a browser address bar with the URL `127.0.0.1:1414/index.php?r=scan/jobs` and a search bar. Below the browser bar is the SAINT logo and a navigation menu with the following items: Dashboard, Scan (highlighted), Analyze, Report, Ticket, Exploit, Manage, and Configuration. The main content area is titled "Manage Scan Jobs". On the left, there is a "Scan Menu" sidebar with the following options: Manage Scans, Manage Jobs, Scan Schedule, Asset Groups, Scan Policies, and Credentials Manager. The main content area contains a message: "No scan jobs have been created. [Would you like to create one?](#)"

The screenshot shows the "Create New Job" wizard in the SAINT web application. The wizard is divided into six steps: 1. Scan Info (Basic Setup), 2. Targets (Select scan targets), 3. Scan Policy (Select a scan policy), 4. Authentication (Select credentials), 5. Advanced (Additional Options), and 6. Finish (Create schedules and select ticket rule set). The current step is "Step 1: Basic Information". The "Name & Description" section contains two text input fields: "Please enter a unique name for this job." and "Please enter a detailed description for this job. (Optional)". The "Asset Group" section contains a yellow information box stating: "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." Below the information box, there is a text input field with a dropdown arrow, followed by the text "or [Create a new Asset Group](#)". At the bottom of the wizard, there are three buttons: "Previous", "Next", and "Finish".

# Lab 05 Report

Create New Job

1 Scan Info  
Basic Setup

2 Targets  
Select scan targets.

3 Scan Policy  
Select a scan policy.

4 Authentication  
Select credentials.

5 Advanced  
Additional Options

6 Finish  
Create schedules and select ticket rule set.

Step 2: Select Scan Targets

Enter Scan Targets

Local Node

Enter target(s)  
192.168.2.16  
More Options...

Node Information  
Description: SAINT Built-In Scanner  
Status: Active

Selected Target(s)

Remove All

Enter Target Restrictions

Enter target(s)

Target Restrictions(s)

Create New Job

1 Scan Info  
Basic Setup

2 Targets  
Select scan targets.

3 Scan Policy  
Select a scan policy.

4 Authentication  
Select credentials.

5 Advanced  
Additional Options

6 Finish  
Create schedules and select ticket rule set.

Step 3: Scan Options

Select a Scan Policy

Select Policy Category  
Vulnerability

Select Policy  
Heavy/Vulnerability Sca

The Heavy/Vulnerability Scan runs all available vulnerability check selected targets.

Scan Policy Options

Exhaustive Scan ?  
☒

Allow Dangerous Tests ?  
☐

Previous

Next

# Lab 05 Report

**Create New Job**

**1** Scan Info  
Basic Setup

**2** Targets  
Select scan targets.

**3** Scan Policy  
Select a scan policy.

**4** Authentication  
Select credentials.

**5** Advanced  
Additional Options

**6** Finish  
Create schedules and select ticket rule set.

**Step 6: Schedules and Ticket Rule Set**

**Job Schedule**

*You may opt not to create a schedule for this job at this time.*

**Create a new Schedule**

Schedule ImmediatelySchedule OnceSchedule Recurring

**Create Scan Window**

Scan Window

**Schedule(s)**

**Ticket Rule Set**

*You may choose a ticket rule set to apply when this job runs.*

**Select Ticket Rule Set**

**SAINT®**

Welcome admin  
Profile | Help | Logout  
Copyright © 2015 SAINT Corporation  
SCAP

DashboardScanAnalyzeReportTicketExploitManageConfigurationSCAP

**Manage Scan Jobs**

**Scan Menu**

Manage ScansManage JobsScan ScheduleAsset GroupsScan PoliciesCredentials Manager

Actions

Job

Are you sure you want to run this job now?

CancelOK

Page 1 of 1

20

Owner	Last Run	# Runs
	2018-02-02 10:13:46	1

Page 1 of 1

20

Ethical Computer Hacking

Wayne State University Computer Science CSC 5991 Special Topics in Computer Science

page 4 of 9

# Lab 05 Report

**SAINT®**

Welcome admin  
Profile | Help | Logout  
Copyright © 2018 SAINT Corporation

Dashboard **Scan** Analyze Report Ticket Exploit Manage Configuration SCAP

**Scan Menu**  
Manage Scans  
Manage Jobs  
Scan Schedule  
Asset Groups  
Scan Policies  
Credentials Manager

Page 1 of 1 20

View 1 - 2 of 2

Job Name	Start Time	End Time	# Targets	# Results	Status	Progress
			1		Queued	
	2018-02-02 10:13:46		1		Running	10

Page 1 of 1 20

View 1 - 2 of 2

**SAINT®**

Welcome admin  
Profile | Help | Logout  
Copyright © 2018 SAINT Corporation

Dashboard **Scan** Analyze Report Ticket Exploit Manage Configuration SCAP

**Scan Management**

**Scan Menu**  
Manage Scans  
Manage Jobs  
Scan Schedule  
Asset Groups  
Scan Policies  
Credentials Manager

Page 1 of 1 20

View 1 - 2 of 2

Actions	Scan #	Job Name	Start Time	End Time	# Targets	# Results	Status	Progress
	2	wizard1			1		Queued	
	1	wizard1	2018-02-02 10:13:46		1		Running	10

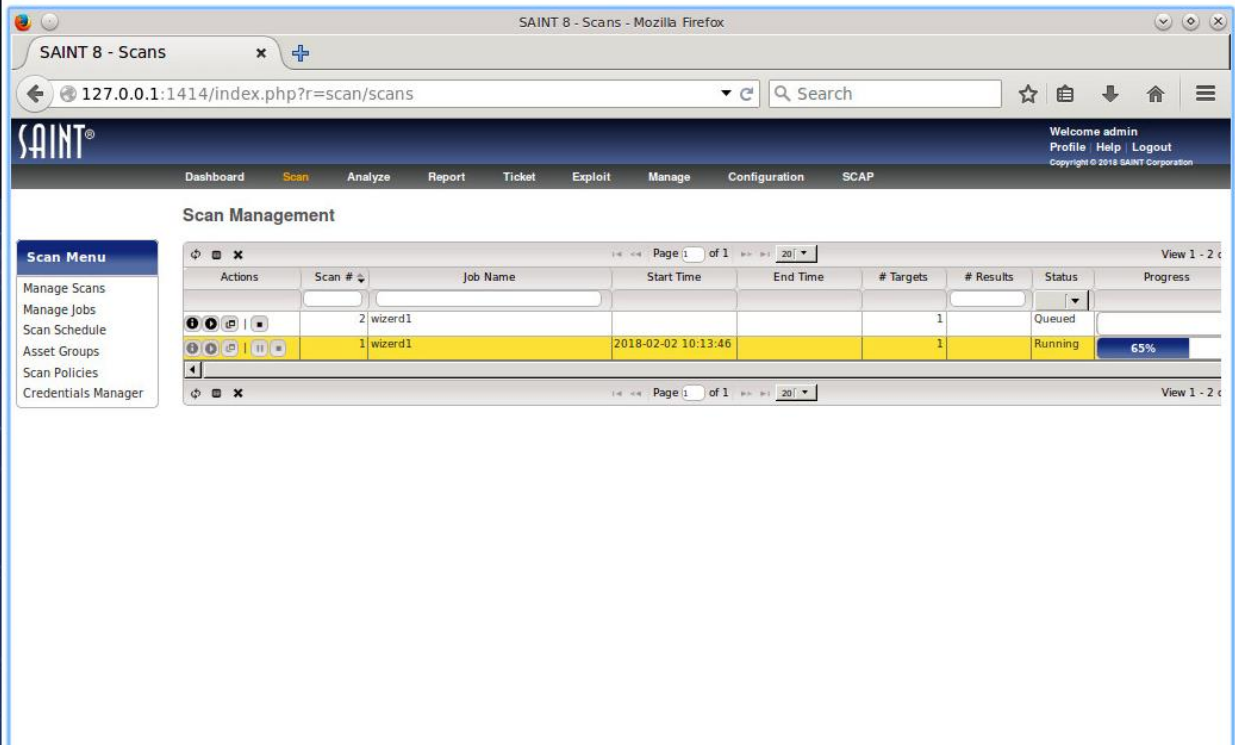
Page 1 of 1 20

View 1 - 2 of 2

# Lab 05 Report

CPEH-Saint

English (US)   



SAINT 8 - Scans - Mozilla Firefox

SAINT 8 - Scans

127.0.0.1:1414/index.php?r=scan/scans

SAINT®









Welcome admin  
Profile | Help | Logout  
Copyright © 2018 SAINT Corporation

Dashboard Scan Analyze Report Ticket Exploit Manage Configuration SCAP

Scan Management

Scan Menu

- Manage Scans
- Manage Jobs
- Scan Schedule
- Asset Groups
- Scan Policies
- Credentials Manager

Actions	Scan #	Job Name	Start Time	End Time	# Targets	# Results	Status	Progress
   	2	wizerd1			1		Queued	
   	1	wizerd1	2018-02-02 10:13:46		1		Running	65%

# Lab 05 Report

**CPEH-Saint** English (US)

SAINT 8 - Scans - Mozilla Firefox

127.0.0.1:1414/index.php?r=scan/scans

Welcome admin  
Profile Help  
Copyright © 2018 SAINT

**Scan Details**

**wizerd1 (SCANID 1)**

▼ Scan Details

<b>Job Name</b>	wizerd1
<b>Scan ID</b>	1
<b>Scan Policy</b>	Heavy/Vulnerability Scan
<b>Start Time</b>	2018-02-02 10:13:46
<b>End Time</b>	2018-02-02 20:07:28

▼ Execution History

Agent/Node	Start Time	End Time	Status	Status File	Verbose Output	Results data
Local Node	2018-02-02 10:13:46	2018-02-02 20:06:49	finished	<a href="#">View Status File</a>	<a href="#">View Verbose Output</a>	<a href="#">View Results</a>

SAINT 8 - Reports SAINTWriter Assessment Report - Mozilla Firefox

127.0.0.1:1414/index.php?r=reports/generate

**SAINT® Vulnerability Assessment Report**

**SAINTWriter Assessment Report**

Report Generated: February 2, 2018

**1.0 Introduction**

On February 2, 2018, at 8:04 PM, a heavy vulnerability assessment was conducted using the SAINT® 8.6.3 vulnerability scanner. The scan discovered a total of one live host, and detected 24 critical problems, 153 areas of concern, and 123 potential problems. The hosts and problems detected are discussed in greater detail in the following sections.

**2.0 Summary**

The following vulnerability severity levels are used to categorize the vulnerabilities:

**CRITICAL PROBLEMS**  
Vulnerabilities which pose an immediate threat to the network by allowing a remote attacker to directly gain read or write access, execute commands on the target, or create a denial of service.

**AREAS OF CONCERN**  
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.

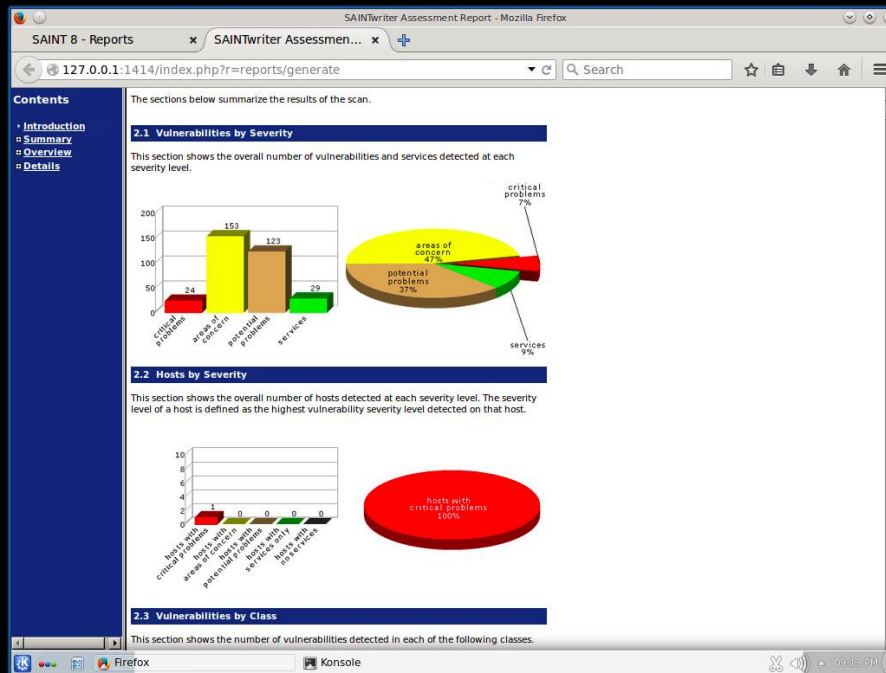
The sections below summarize the results of the scan.

**2.1 Vulnerabilities by Severity**

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



# Lab 05 Report





# ***Lab 05 Report***

## Vulnerabilities

### Vulnerability 01

#### Description

Someone from remote location can gain access and execute any commands or crash the file server.

#### Relative Risk (High, Medium, Low)

- High
  - Approximately 10 times more expensive than a “medium” risk
  - Although threat is high it will not require additional budget

#### Mitigation

Update the apache server to the latest version and problem will be solved.