Lab 05 Report

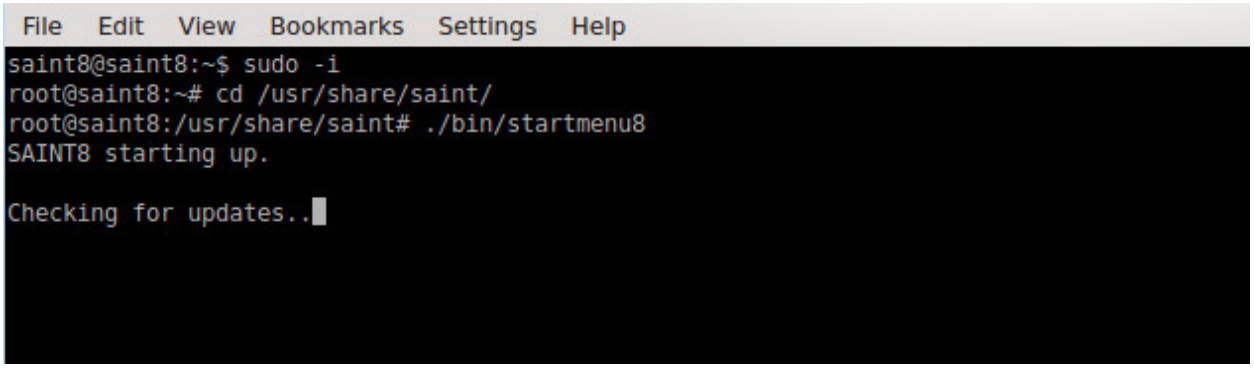
Report by Joynal Abedin

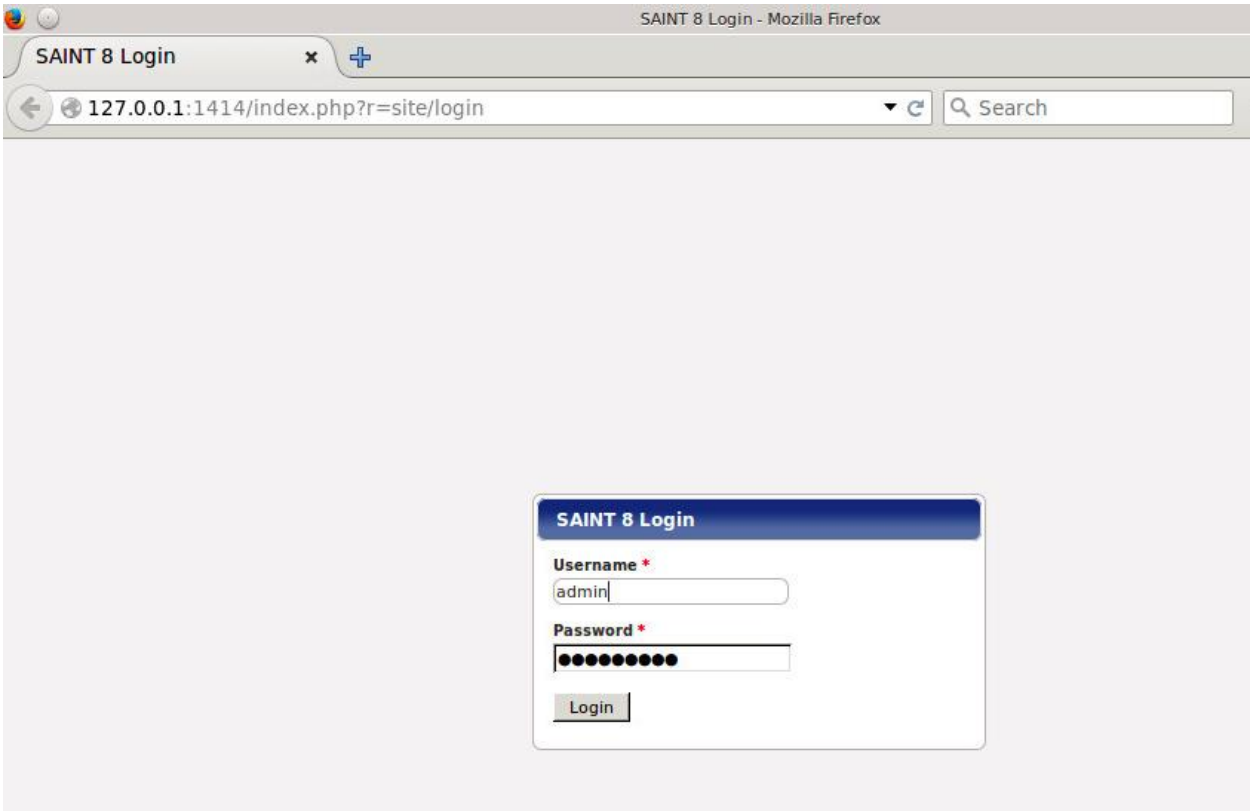
Documentation

5.1 Nessus Vulnerability Scanner

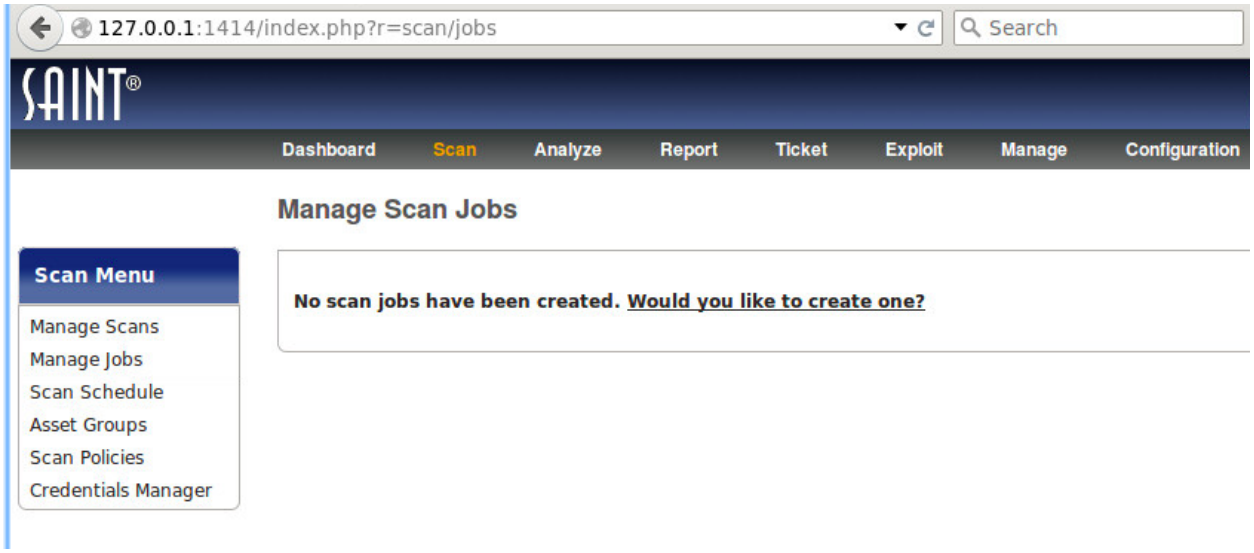
I skipped this section with Prof. Schott's permission.

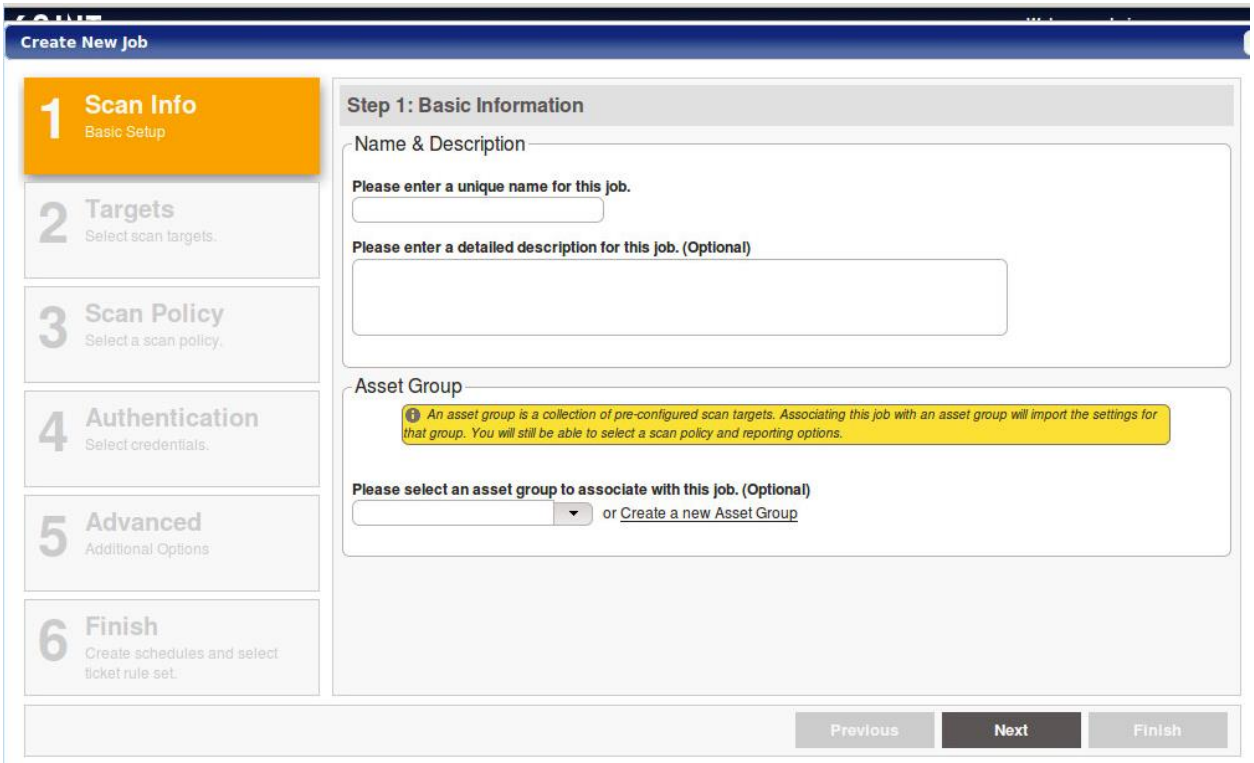
5.2 SAINT vulnerability Scanner

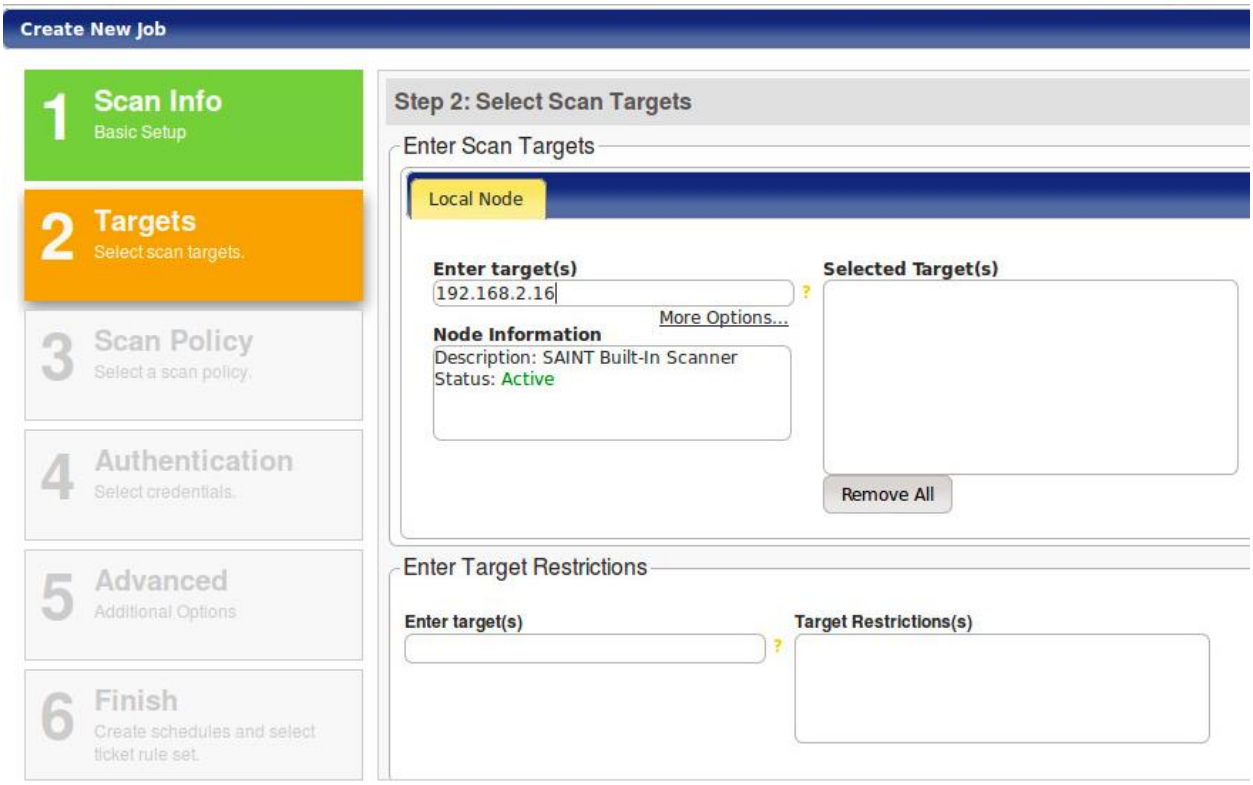


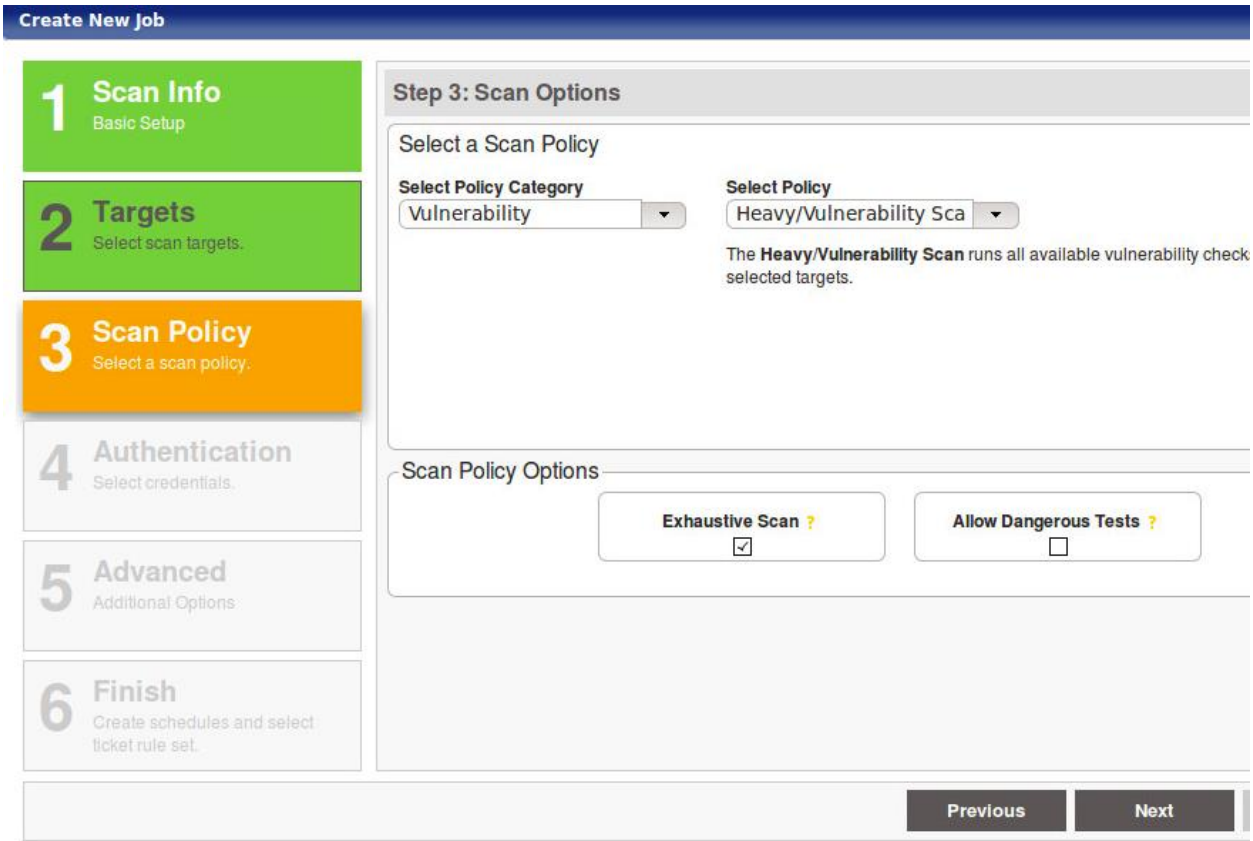


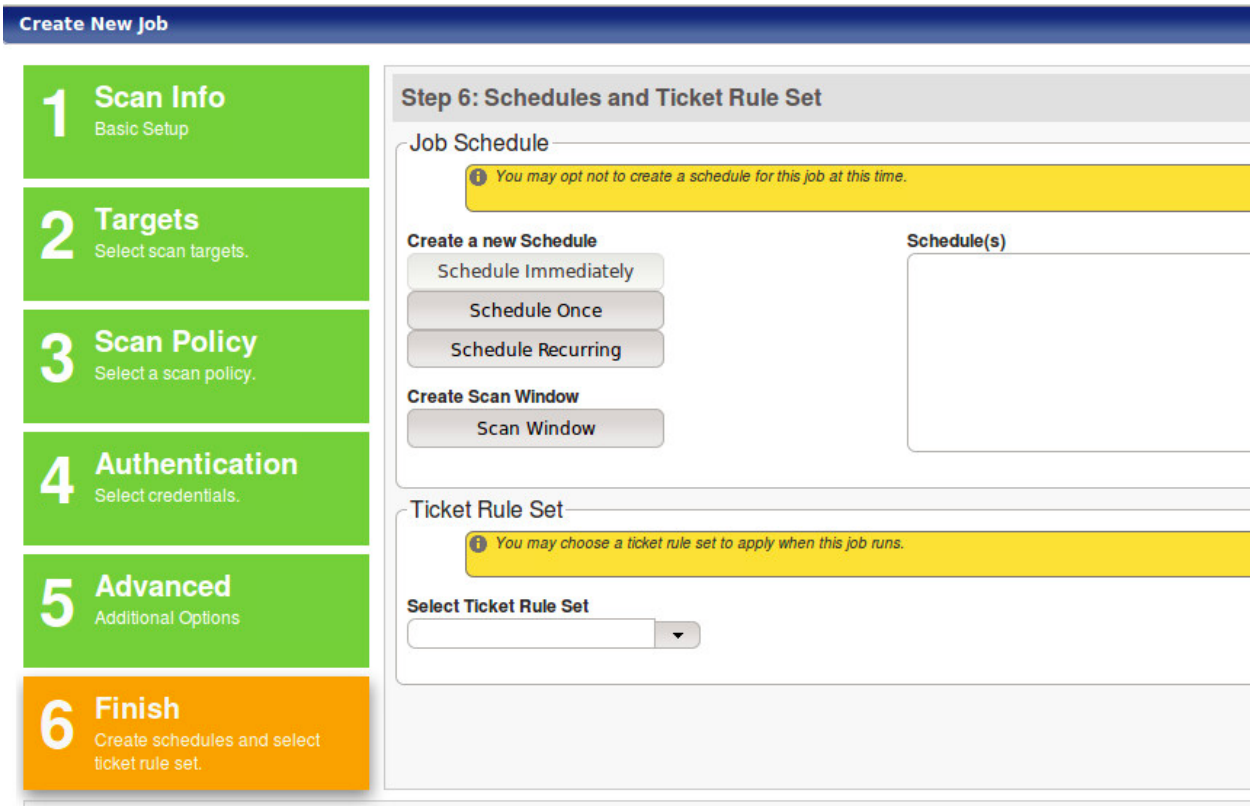
Lab 05 Report

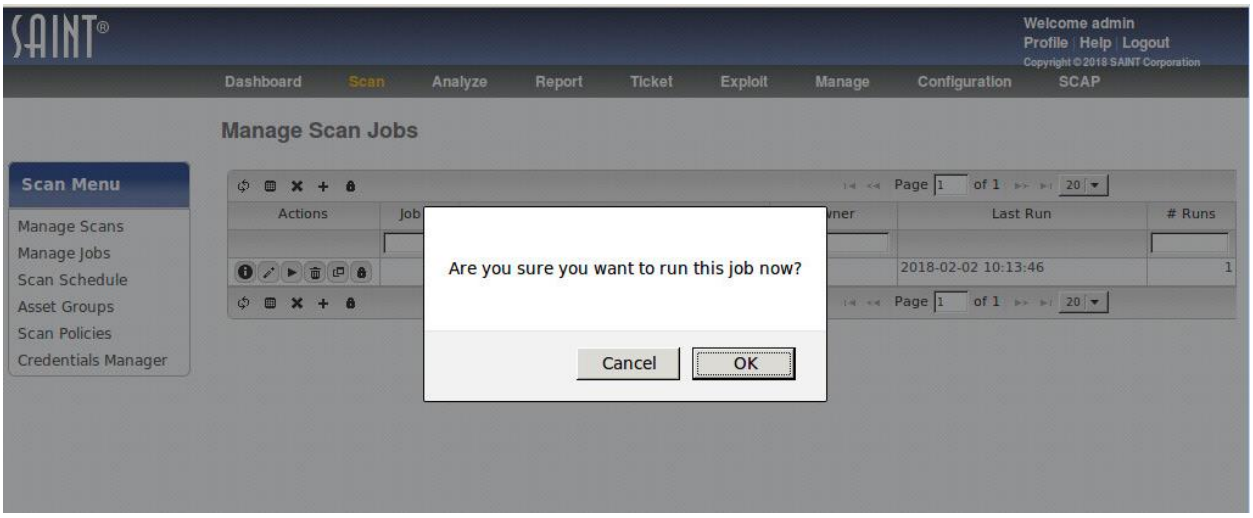




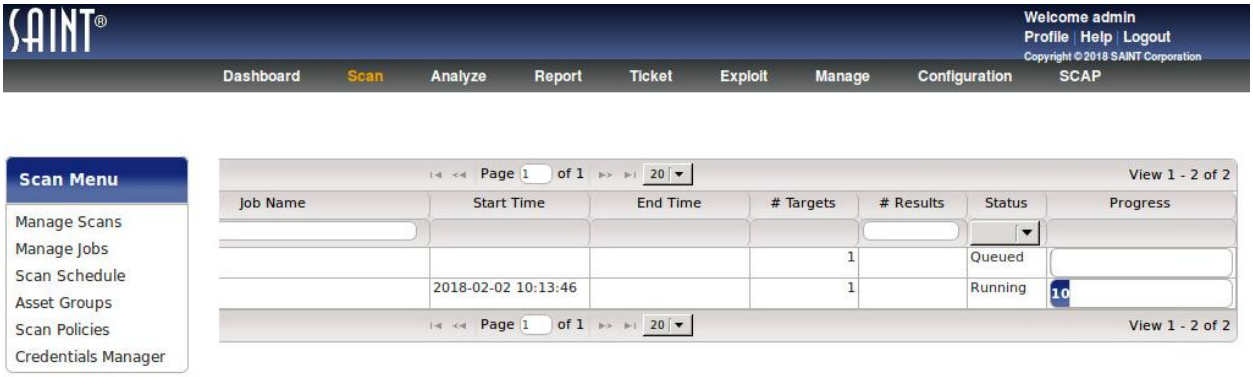

Create New Job
1 Scan Info
Basic Setup
2 Targets
Select scan targets.
3 Scan Policy
Select a scan policy.
4 Authentication
Select credentials.
5 Advanced
Additional Options
6 Finish
Create schedules and select ticket rule set.
Step 2: Select Scan Targets
Enter Scan Targets
Local Node
Enter target(s)
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)

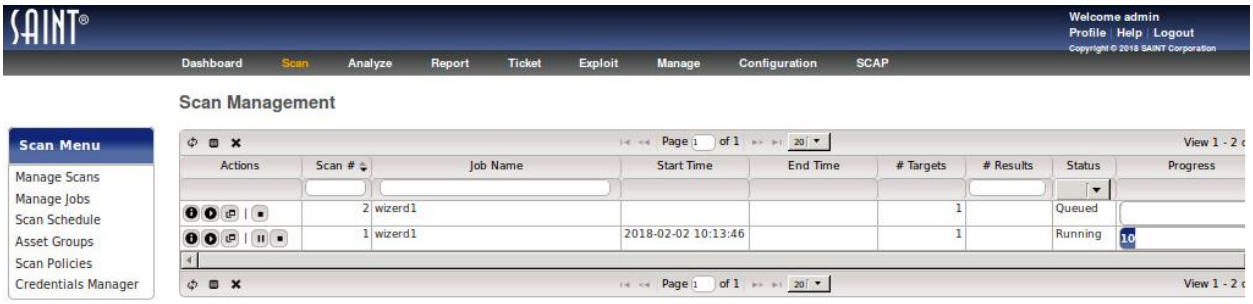

Create New Job
1 Scan Info
Basic Setup
2 Targets
Select scan targets.
3 Scan Policy
Select a scan policy.
4 Authentication
Select credentials.
5 Advanced
Additional Options
6 Finish
Create schedules and select ticket rule set.
Step 3: Scan Options
Select a Scan Policy
Select Policy Category
Vulnerability
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


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 Immediately
Schedule Once
Schedule 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

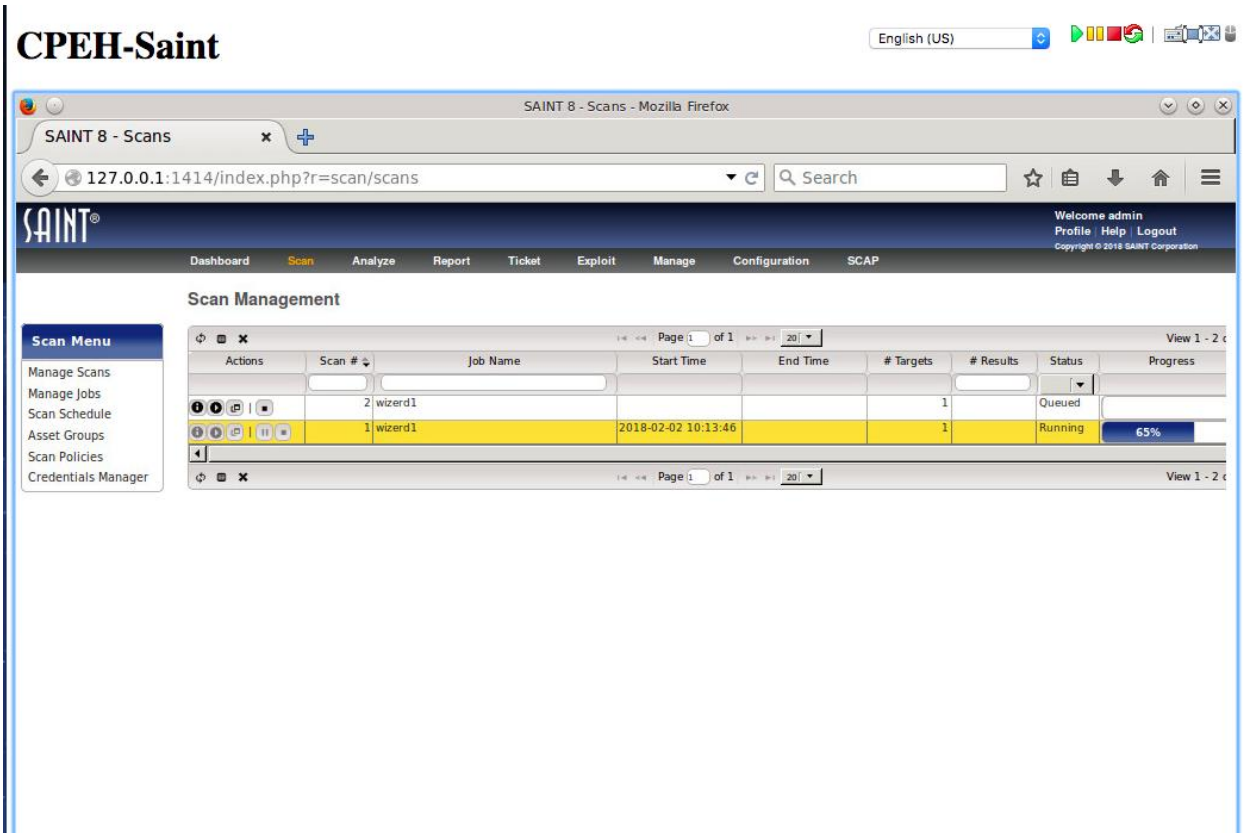

SAINT
Welcome admin
Profile | Help | Logout
Dashboard
Scan
Analyze
Report
Ticket
Exploit
Manage
Configuration
SCAP
Manage Scan Jobs
Scan Menu
Manage Scans
Manage Jobs
Scan Schedule
Asset Groups
Scan Policies
Credentials Manager
Actions
Last Run
Runs
2018-02-02 10:13:46
Are you sure you want to run this job now?
Cancel
OK

Lab 05 Report

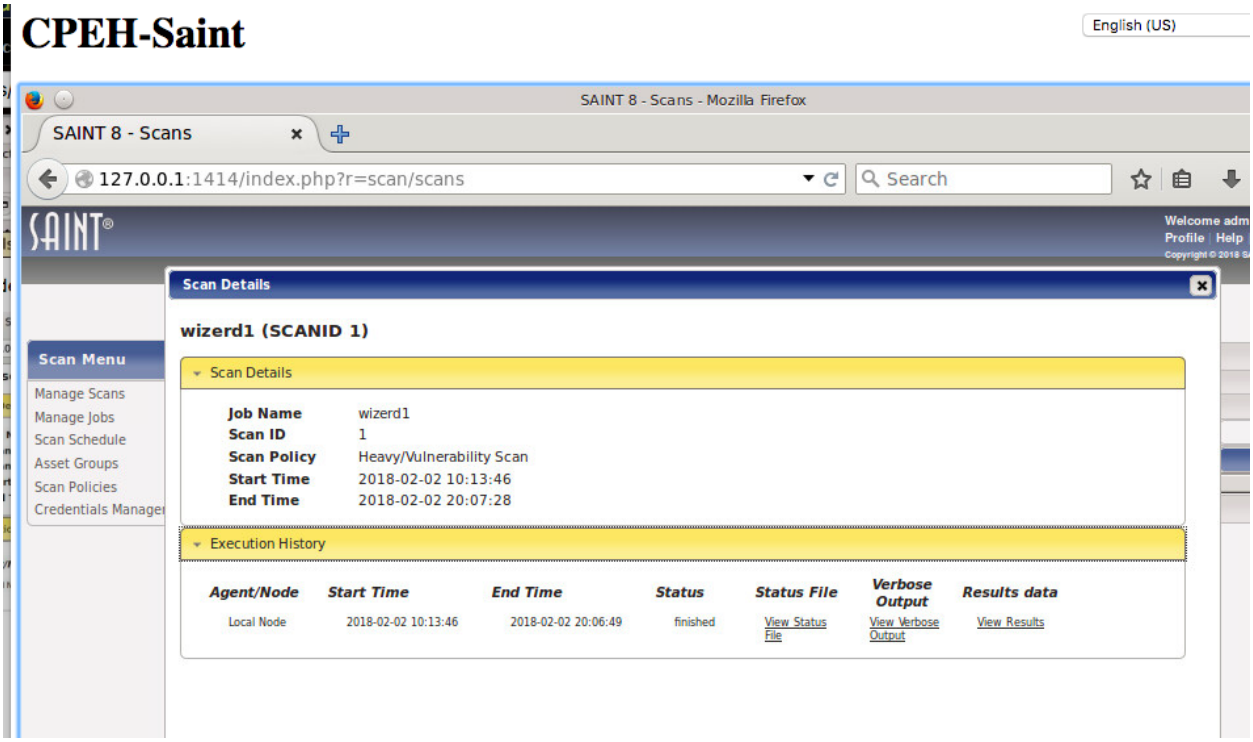


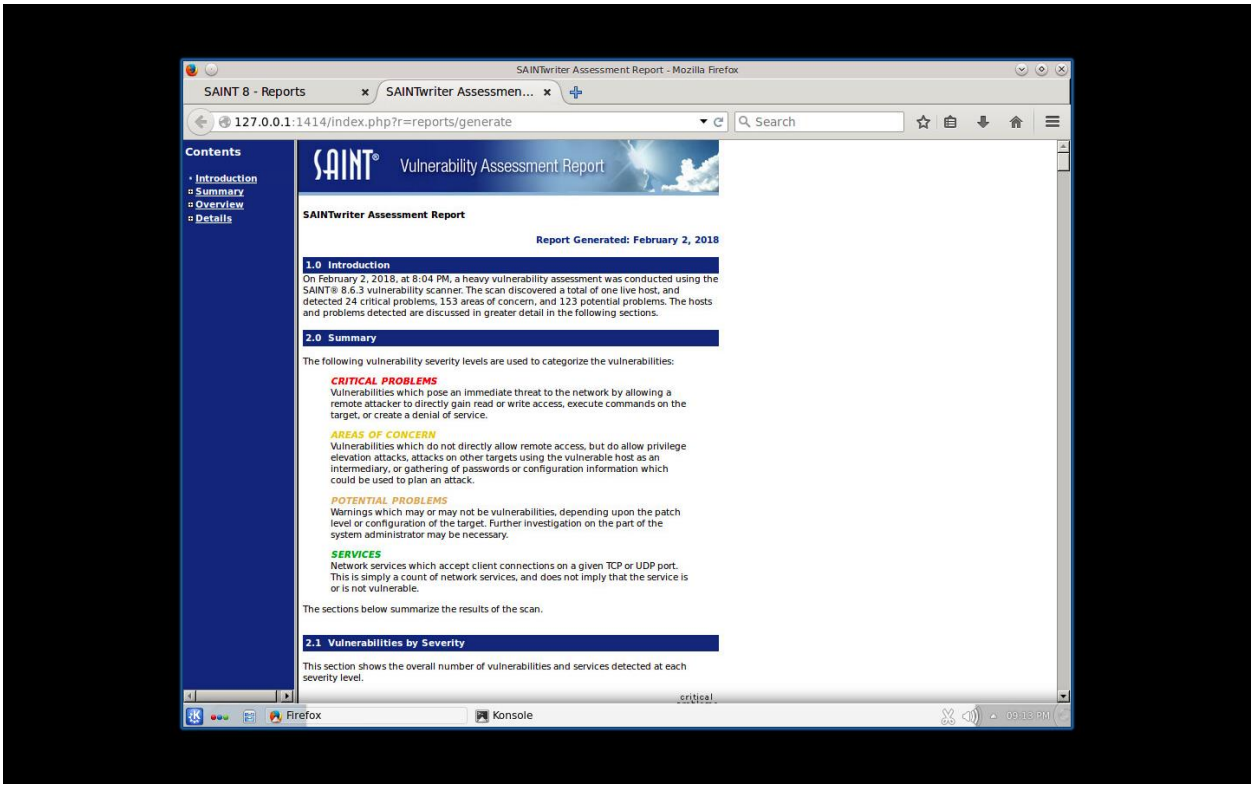


Lab 05 Report

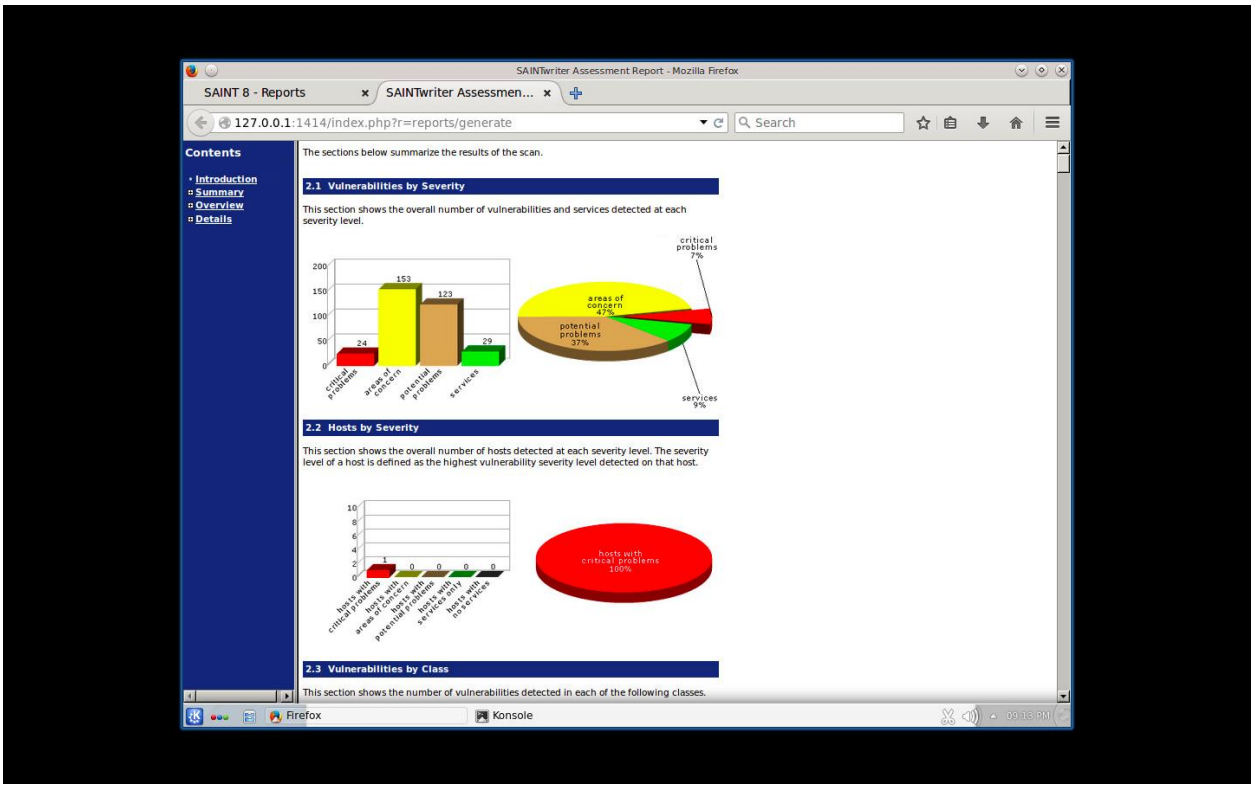


Lab 05 Report





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.