Lab 2

Aim: Use the Nessus tool to scan the network for vulnerabilities.

Objectives: Objective of the module is scan system and network analysis.

Outcomes: The learner will be able to:

- Identify network vulnerability with tool
- Use current techniques, skills, and tools to find out different vulnerabilities and the countermeasures for identified vulnerabilities.

Hardware / Software Required: Nessus Vulnerability Scanner | Tenable Network Security tool

Theory:

Nessus is a proprietary comprehensive vulnerability scanner which is developed by Tenable

Network Security. It is free of charge for personal use in a non-enterprise environment.

Operation

- Nessus allows scans for the following types of vulnerabilities.

- Vulnerabilities that allow a remote hacker to control or access sensitive data on a system.

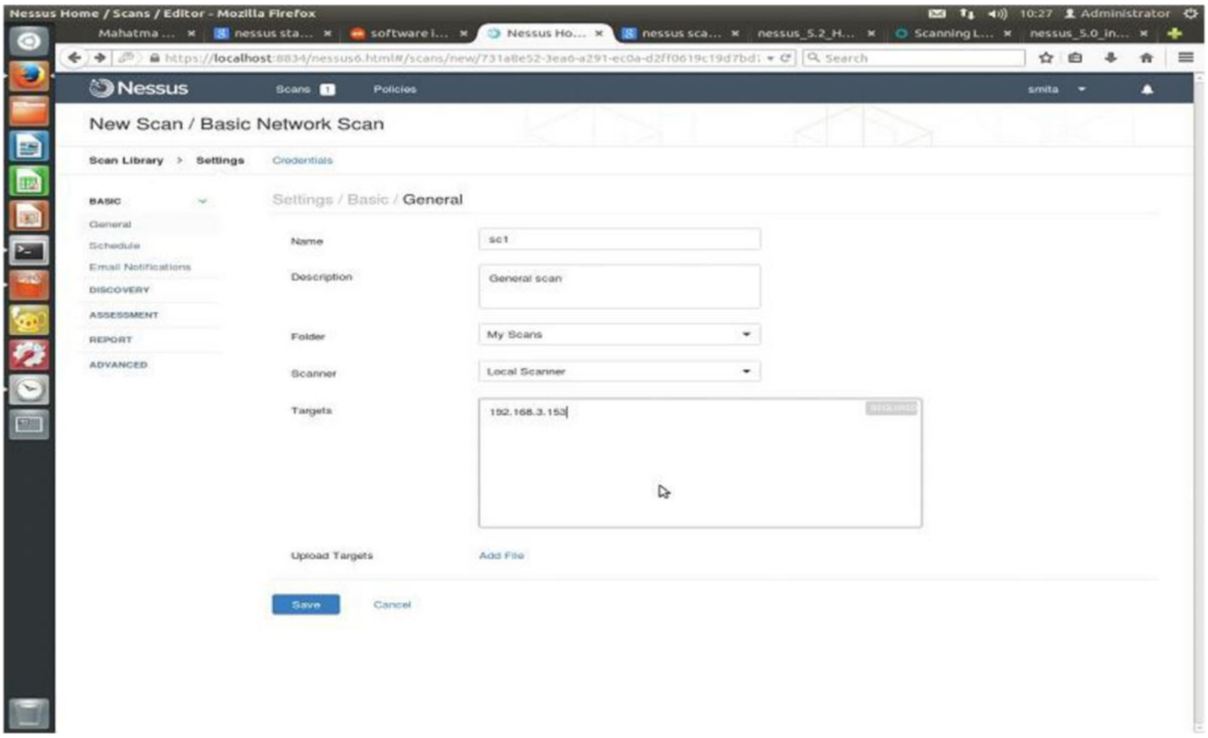
- Misconfiguration (e.g. open mail relay, missing patches, etc.).

Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack. Denials of service against the TCP/IP stack by using malformed packets.

Preparation for PCI DSS audits

On UNIX (including Mac OS X), it consists of nessusd, the Nessus daemon, which does the scanning, and nessus, the client, which controls scans and presents the vulnerability results to the user. In typical operation, Nessus begins by doing a port scan with one of its four internal port scanners (or it can optionally use AmapM or Nmap) to determine which ports are open on the target and then tries various exploits on the open ports. The vulnerability tests, available as subscriptions, are written in NASL (Nessus Attack Scripting Language), a scripting language optimized for custom network interaction. Tenable Network Security produces several dozen new vulnerability checks (called plugins) each week, usually on a daily basis. These checks are available for free to the general public; commercial customers are not allowed to use this Home Feed any more. The Professional Feed (which is not free) also give access to support and additional scripts (e.g. audit files, compliance tests, additional vulnerability detection plugins). Optionally, the results of the scan can be reported in various formats, such as plain text, XML, HTML and LaTeX. The results can also be saved in a knowledge base for debugging. On UNIX, scanning can be automated through the use of a command-line client. There exist many different commercial, free and open source tools for both UNIX and Windows to manage individual or distributed Nessus scanners. If the user chooses to do so (by disabling the option 'safe checks'), some of Nessus' vulnerability test may try to cause vulnerable services or operating systems to crash. This lets a user test the resistance of a device before putting it in production. Nessus provides additional functionality beyond testing for known network vulnerabilities. For instance, it can use Windows credentials to examine patch levels on computers running the Windows operating system, and can perform password auditing using dictionary and brute force methods. Nessus 3 and later can also audit systems to make sure they have been configured per a specific policy, such as the NSA's guide for hardening Windows servers.

Basic Network scanning:



New Scan / Basic Network Scan

Settings / Basic / General

Name: sc1

Description: General scan

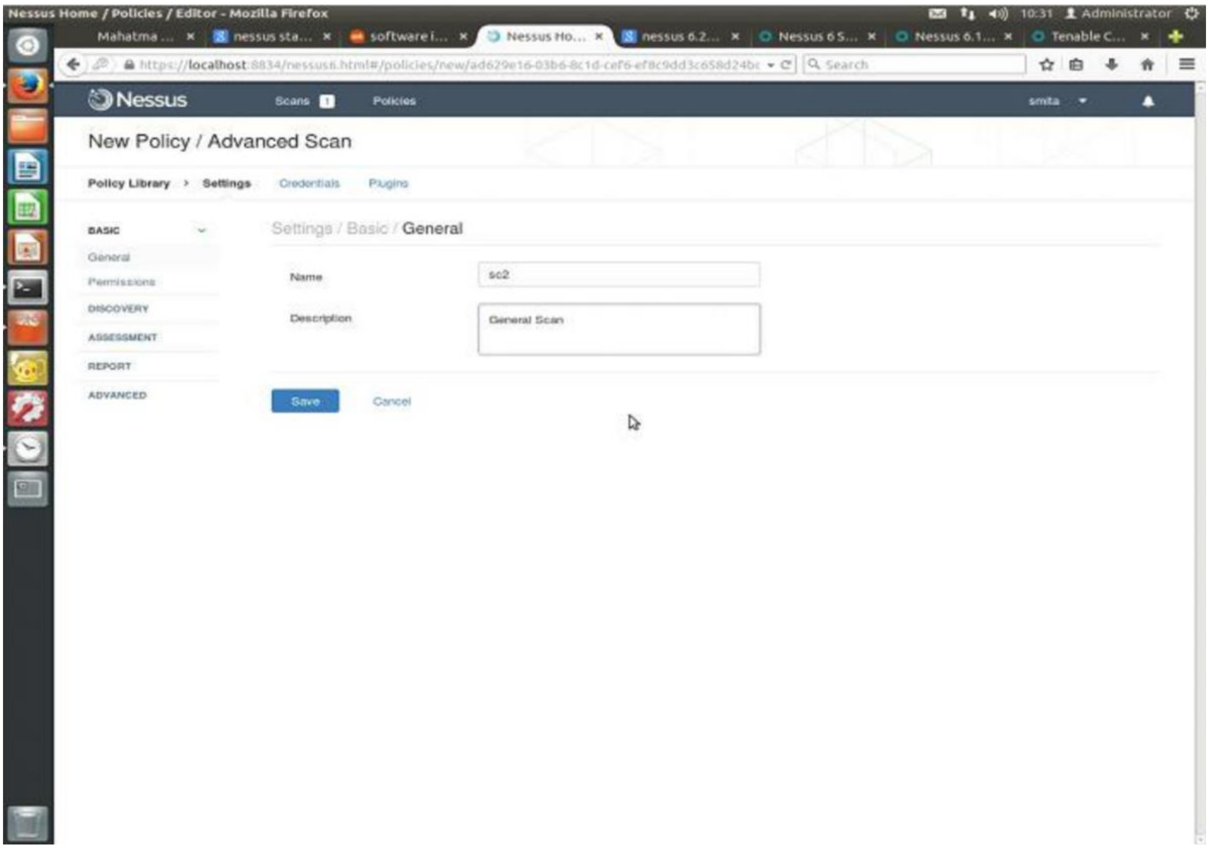
Folder: My Scans

Scanner: Local Scanner

Targets: 192.168.3.153

Upload Targets: Add File

Advanced scanning in general search:



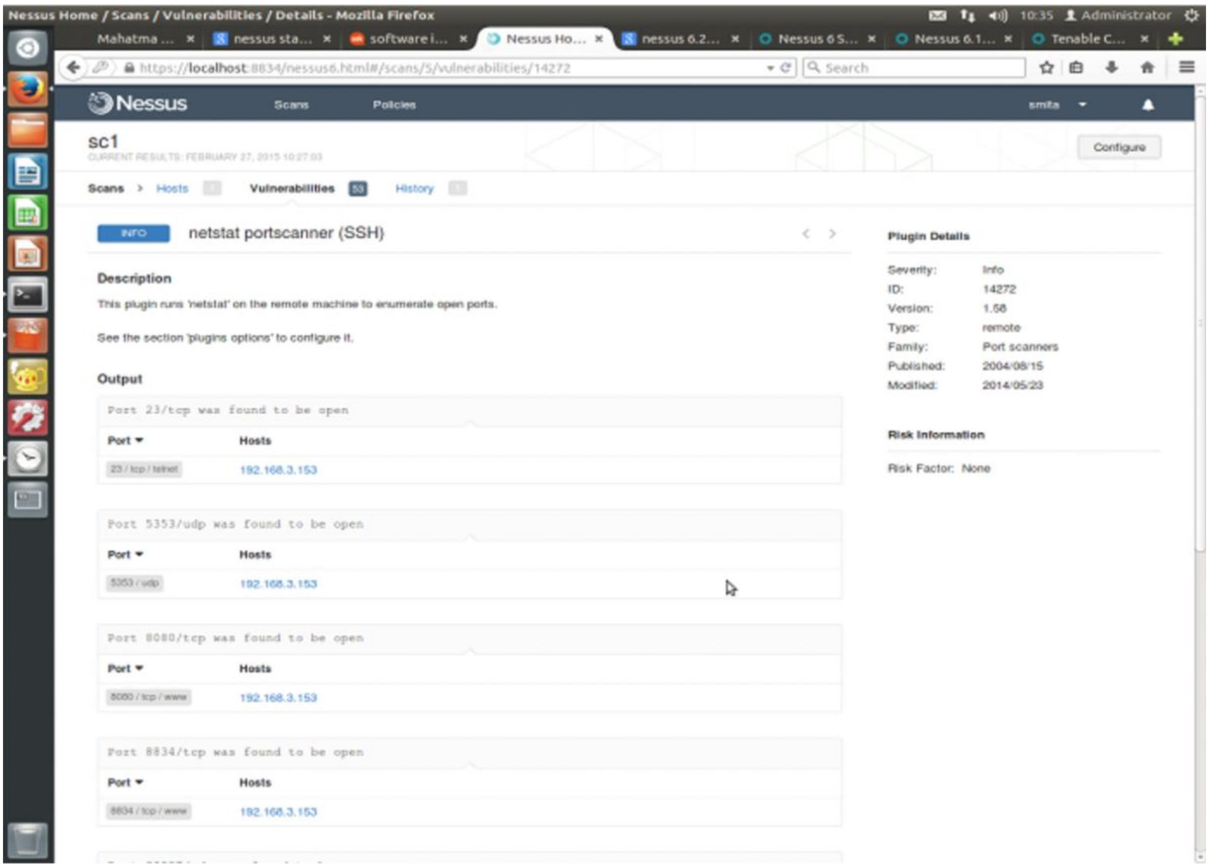
New Policy / Advanced Scan

Settings / Basic / General

Name: sc2

Description: General Scan

Ntstat port scanning:



https://localhost:8834/nessus6.html#/scans/5/vulnerabilities/14272

sc1

CURRENT RESULTS: FEBRUARY 27, 2015 10:27:03

Scans > Hosts Vulnerabilities 53 History

INFO netstat portscanner (SSH)

Description

This plugin runs 'netstat' on the remote machine to enumerate open ports.

See the section 'plugins options' to configure it.

Output

```
Port 23/tcp was found to be open
```

Port	Hosts
23 / tcp / telnet	192.168.3.153

```
Port 5353/udp was found to be open
```

Port	Hosts
5353 / udp	192.168.3.153

```
Port 8080/tcp was found to be open
```

Port	Hosts
8080 / tcp / www	192.168.3.153

```
Port 8834/tcp was found to be open
```

Port	Hosts
8834 / tcp / www	192.168.3.153

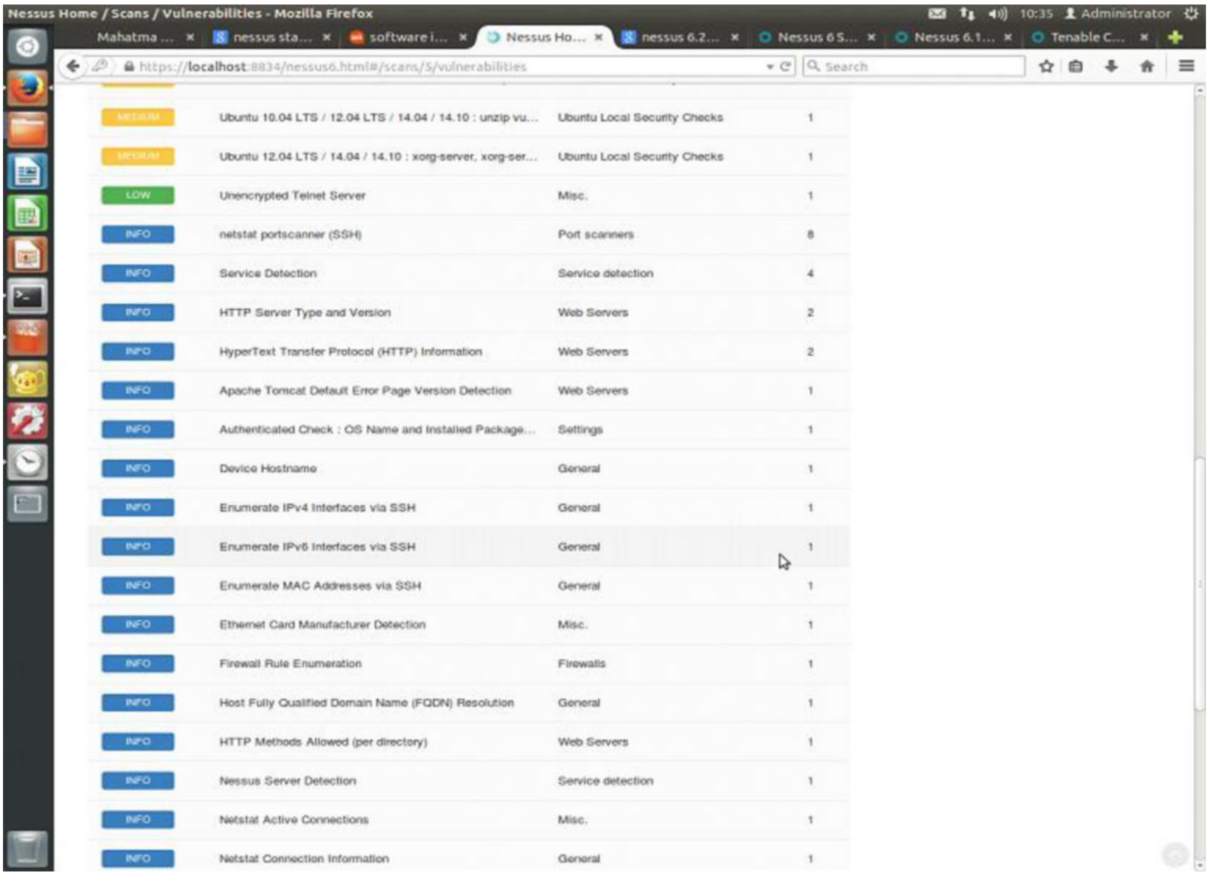
Plugin Details

Severity:	Info
ID:	14272
Version:	1.58
Type:	remote
Family:	Port scanners
Published:	2004/08/15
Modified:	2014/05/23

Risk Information

Risk Factor: None

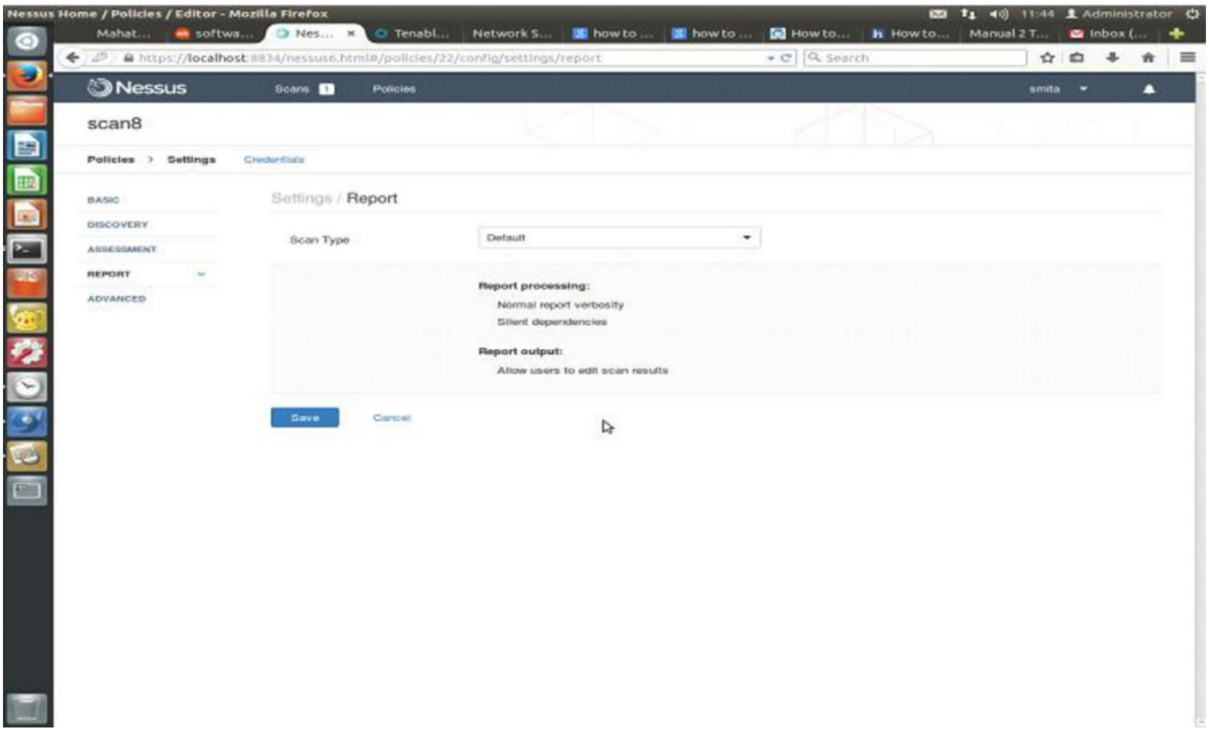
Vulnerability Mapping:



https://localhost:8834/nessus6.html#/scans/5/vulnerabilities

MEDIUM	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : unzip vu...	Ubuntu Local Security Checks	1
MEDIUM	Ubuntu 12.04 LTS / 14.04 / 14.10 : xorg-server, xorg-ser...	Ubuntu Local Security Checks	1
LOW	Unencrypted Telnet Server	Misc.	1
INFO	netstat portscanner (SSH)	Port scanners	8
INFO	Service Detection	Service detection	4
INFO	HTTP Server Type and Version	Web Servers	2
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	2
INFO	Apache Tomcat Default Error Page Version Detection	Web Servers	1
INFO	Authenticated Check : OS Name and Installed Package...	Settings	1
INFO	Device Hostname	General	1
INFO	Enumerate IPv4 Interfaces via SSH	General	1
INFO	Enumerate IPv6 Interfaces via SSH	General	1
INFO	Enumerate MAC Addresses via SSH	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Firewall Rule Enumeration	Firewalls	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	HTTP Methods Allowed (per directory)	Web Servers	1
INFO	Nessus Server Detection	Service detection	1
INFO	Netstat Active Connections	Misc.	1
INFO	Netstat Connection Information	General	1

Policies:


Nessus Home / Policies / Editor - Mozilla Firefox
11:44 Administrator
Mahat… softwa… Nes… Tenabl… Network S… how to … how to … How to… How to… Manual 2 T… Inbox (…
https://localhost:8834/nessus6.html#/policies/22/config/settings/report
Search
Nessus
Scans 1
Policies
smita

scan8

Policies > Settings Credentials

BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED

Settings / Report

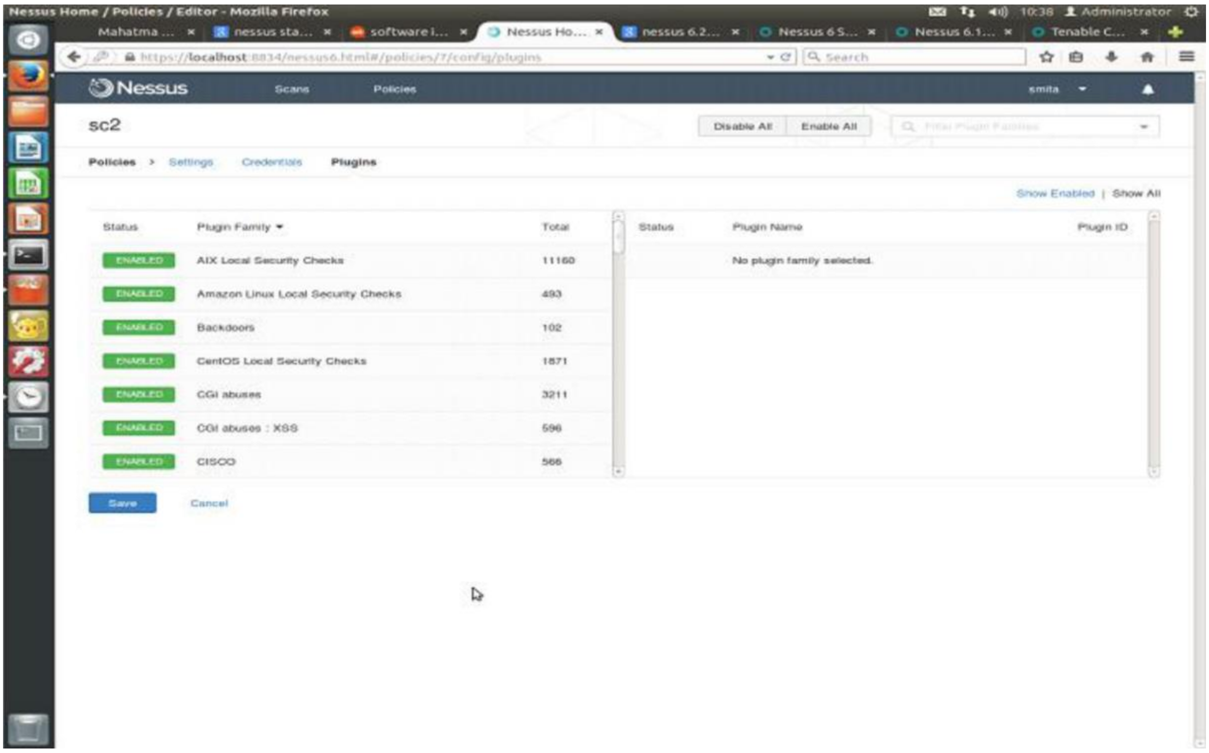
Scan Type: Default

Report processing:
Normal report verbosity
Silent dependencies

Report output:
Allow users to edit scan results

Save Cancel

Plugins:


Nessus Home / Policies / Editor - Mozilla Firefox
10:38 Administrator
Mahatma … nessus sta… software i… Nessus Ho… nessus 6.2… Nessus 6 S… Nessus 6.1… Tenable C…
https://localhost:8834/nessus6.html#/policies/7/config/plugins
Search
Nessus
Scans
Policies
smita
Disable All
Enable All
Filter Plugin Families

sc2

Policies > Settings Credentials Plugins

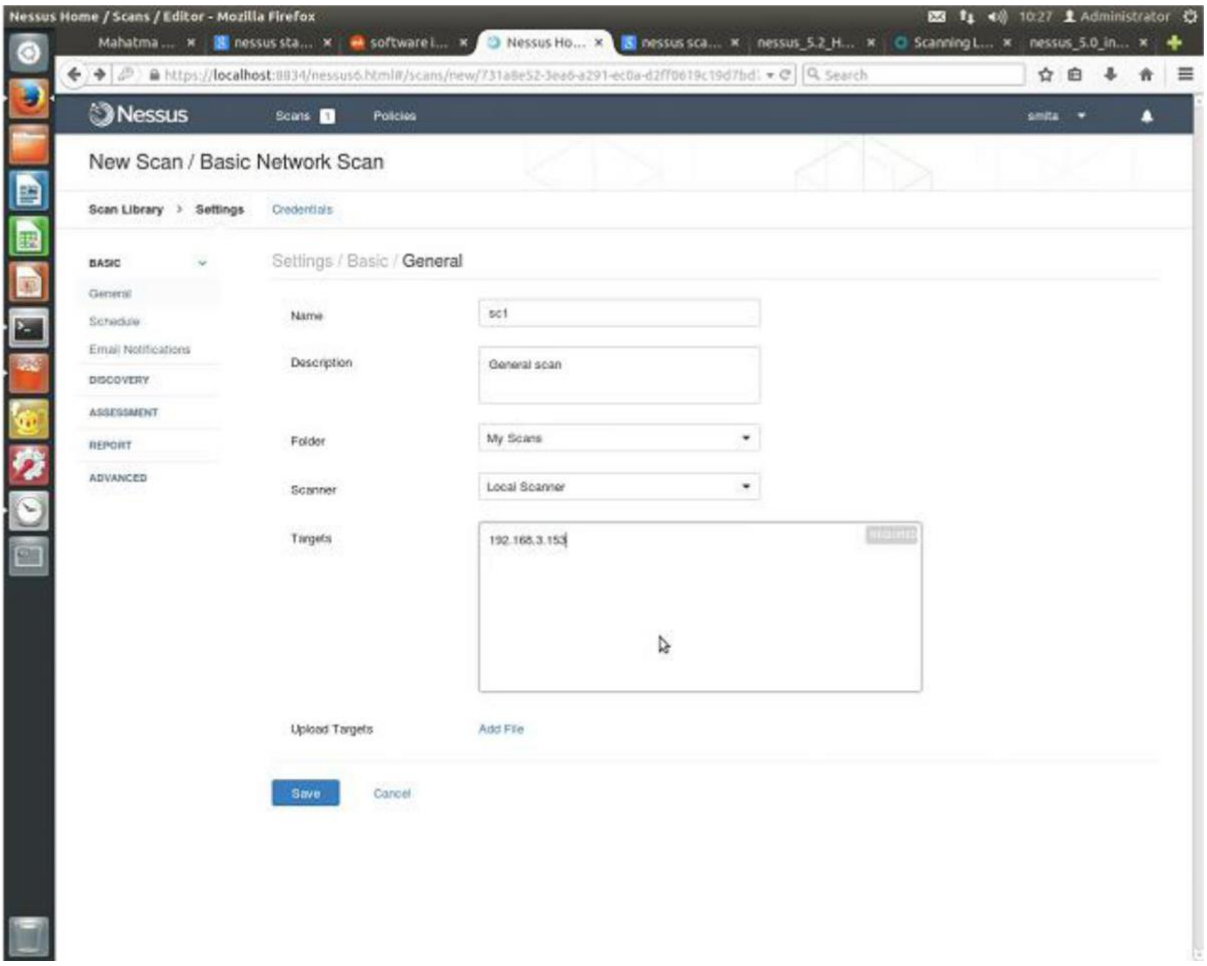
Show Enabled | Show All

Status	Plugin Family	Total
ENABLED	AIX Local Security Checks	11160
ENABLED	Amazon Linux Local Security Checks	493
ENABLED	Backdoors	102
ENABLED	CentOS Local Security Checks	1871
ENABLED	CGI abuses	3211
ENABLED	CGI abuses : XSS	596
ENABLED	CISCO	566

Status	Plugin Name	Plugin ID
	No plugin family selected.	

Save Cancel

General Scanning:



New Scan / Basic Network Scan

Settings / Basic / General

Name: sc1

Description: General scan

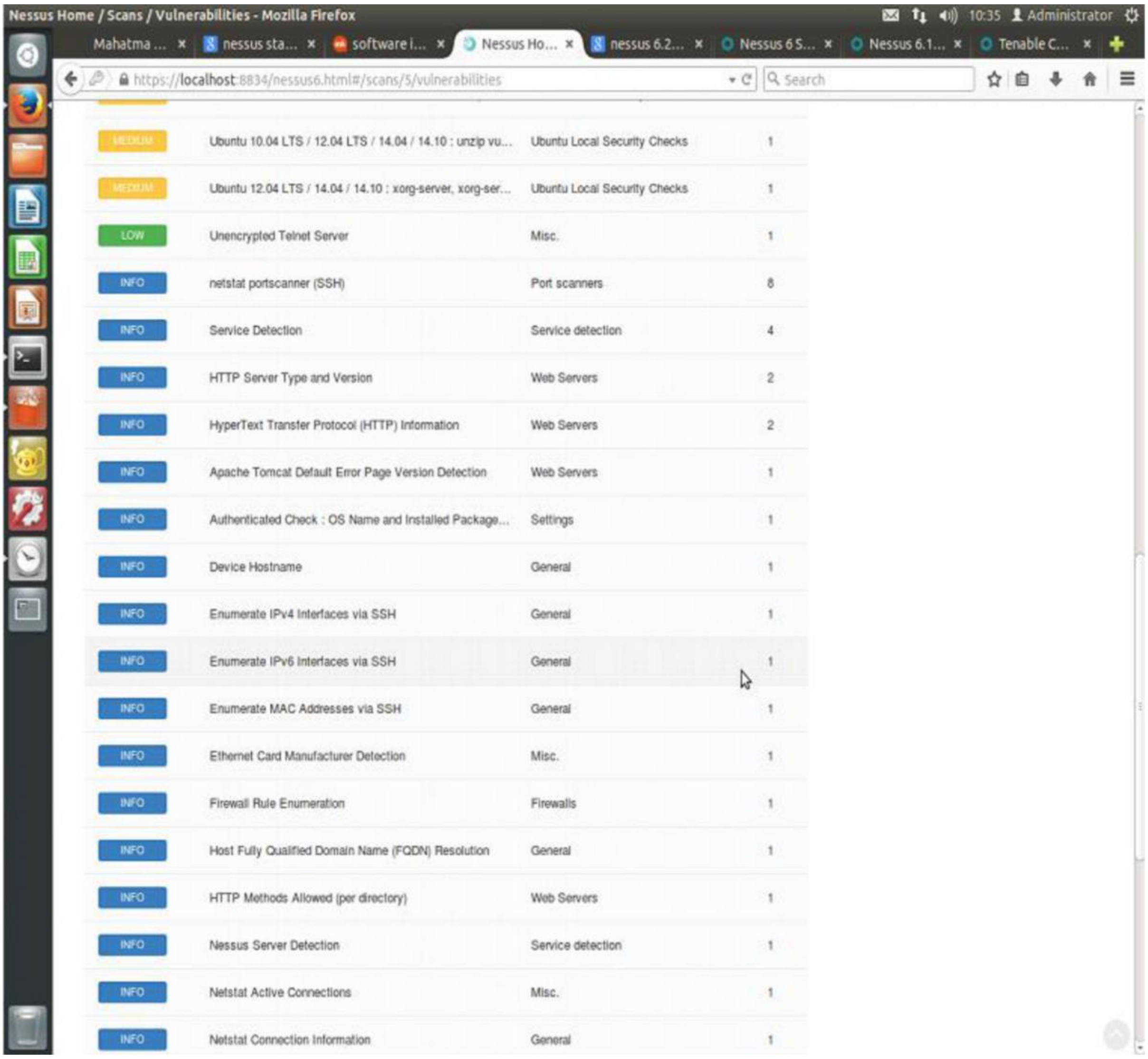
Folder: My Scans

Scanner: Local Scanner

Targets: 192.168.3.153

Upload Targets: Add File

Port Scanning:



MEDIUM	Ubuntu 10.04 LTS / 12.04 LTS / 14.04 / 14.10 : unzip vu...	Ubuntu Local Security Checks	1
MEDIUM	Ubuntu 12.04 LTS / 14.04 / 14.10 : xorg-server, xorg-ser...	Ubuntu Local Security Checks	1
LOW	Unencrypted Telnet Server	Misc.	1
INFO	netstat portscanner (SSH)	Port scanners	8
INFO	Service Detection	Service detection	4
INFO	HTTP Server Type and Version	Web Servers	2
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	2
INFO	Apache Tomcat Default Error Page Version Detection	Web Servers	1
INFO	Authenticated Check : OS Name and Installed Package...	Settings	1
INFO	Device Hostname	General	1
INFO	Enumerate IPv4 Interfaces via SSH	General	1
INFO	Enumerate IPv6 Interfaces via SSH	General	1
INFO	Enumerate MAC Addresses via SSH	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Firewall Rule Enumeration	Firewalls	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	HTTP Methods Allowed (per directory)	Web Servers	1
INFO	Nessus Server Detection	Service detection	1
INFO	Netstat Active Connections	Misc.	1
INFO	Netstat Connection Information	General	1

Conclusion:

Running a security scanner against your systems is a very important part of the job. It is a system administrator or security officer’s job to keep their systems secure and the data contained in them safe. Hackers have access to all the same information and tools that the rest of us do. Hackers run the very same tools and it is advantageous to know what the results are that they see if they scan your system. They find time to do the research, so we must also. Nessus provides a lot of functionality in one tool. It utilizes Nmap, easy to update plug-ins, and nice reporting tools for upper management. It is has repeatedly scored high on comparisons between scanners including commercial scanners that come with a hefty price tag. And of course as budgets tighten, remember Nessus is a free tool. The only cost is the users time in learning it and using it, but that is a cost associated with all tools. And luckily Nessus is an easy to learn tool. Using this tool and seeing the vulnerabilities will help you gain knowledge of your systems and help teach you how to protect them.

Questions:

Submit the screenshots of your lab and the answers to the below questions in a document file (.doc/.pdf)

1. What's the current version of Nessus?

2. What OS platforms does Nessus have builds for?

3. What are the system/hardware requirements for using Nessus?

4. What is the heart of the nessus?

5. When using the Nessus user interface, which of browsers are supported?