# Vulnerability Scanning With Metasploit Using Nessus

Vulnerability scanning is part of penetration testing. A vulnerability scanner is an automated program designed to look for weaknesses in computer systems, networks, and applications. There are many vulnerability scanners available for penetration Testing. But here we use Metasploit framework for scanning vulnerability.

Various operating systems respond differently because of the different networking implementations in use. These unique responses that vulnerability scanner uses to determine the operating system version and even its patch level. A vulnerability scanner can also use a given set of user credentials to log into the remote system and enumerate the software and services to determine whether they are patched.

The scanner presents a report outlining any vulnerability detected on the system. That report can be useful for both network administrators and penetration testers.

## Installing Nessus:

For Installing Nessus follow my previous post of installing nessus.

Nessus is the vulnerability management solution to analyze vulnerabilities, controls, and configurations to find who, what, and where of IT security risk. Tenable Network Security offers multiple versions of

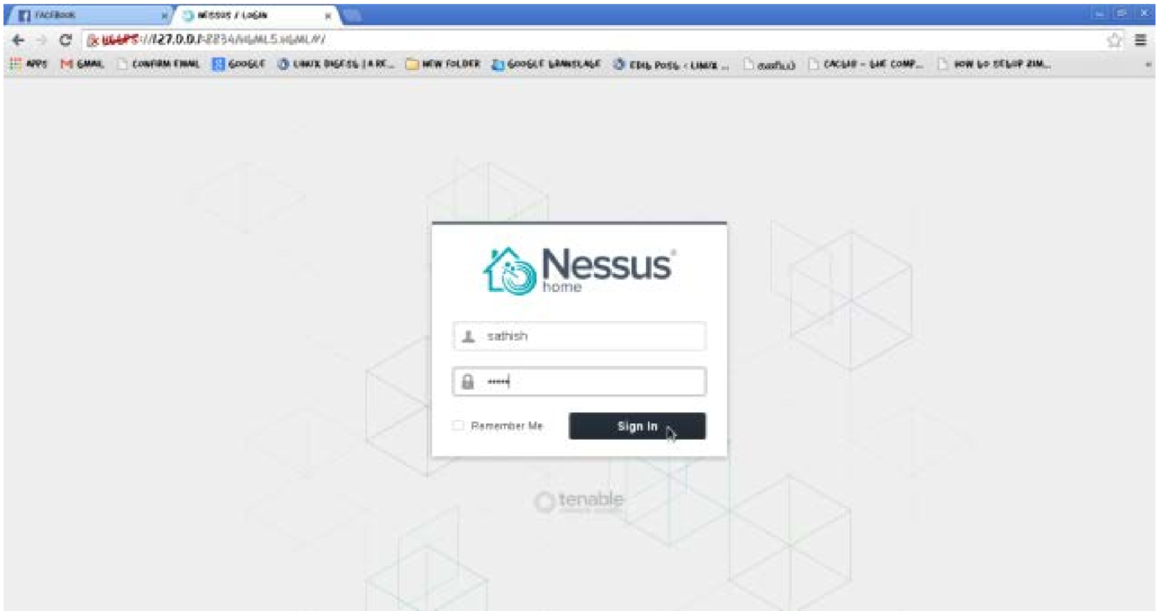
Metasploit's Nessus plug-in lets you launch scans and pull information from Nessus scans via console.

## Nessus Configuration:

After you have downloaded and installed Nessus, open your web browser and navigate to https://localhost:8834

Accept the certificate warning, and log into Nessus using the credentials you created during installation.

You should see the Nessus login window, as shown below.

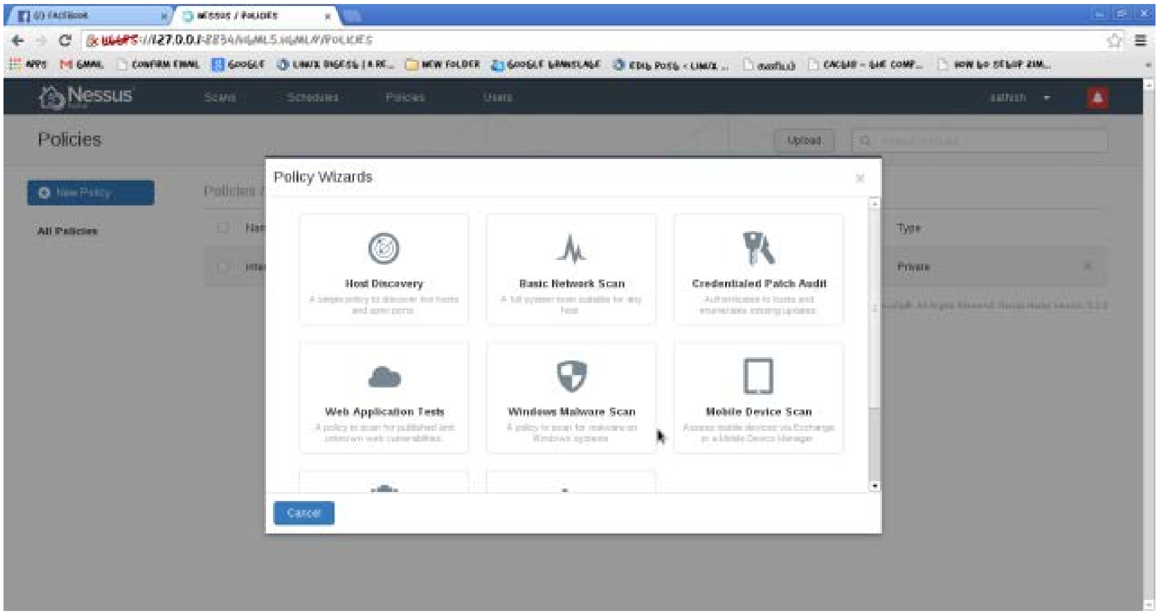


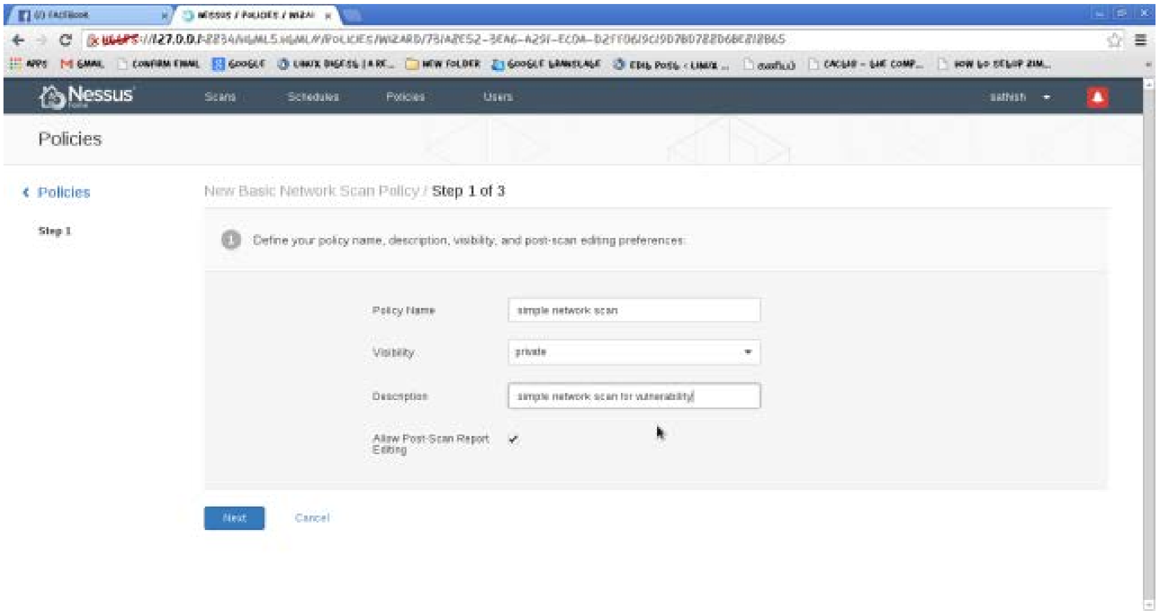
You should see the Nessus window after login, as shown below.

## Creating a Nessus Scan Policy:

Before beginning a scan, you first need to create a Nessus scan policy. On the *Policies tab*, click the green Add button to open the policy configuration window and select Basic Network Scan shown below:

Basic Scan contains three steps to configure Basic Network Scan Policy. So we select Basic Network Scan from the list and fill details shown as below:



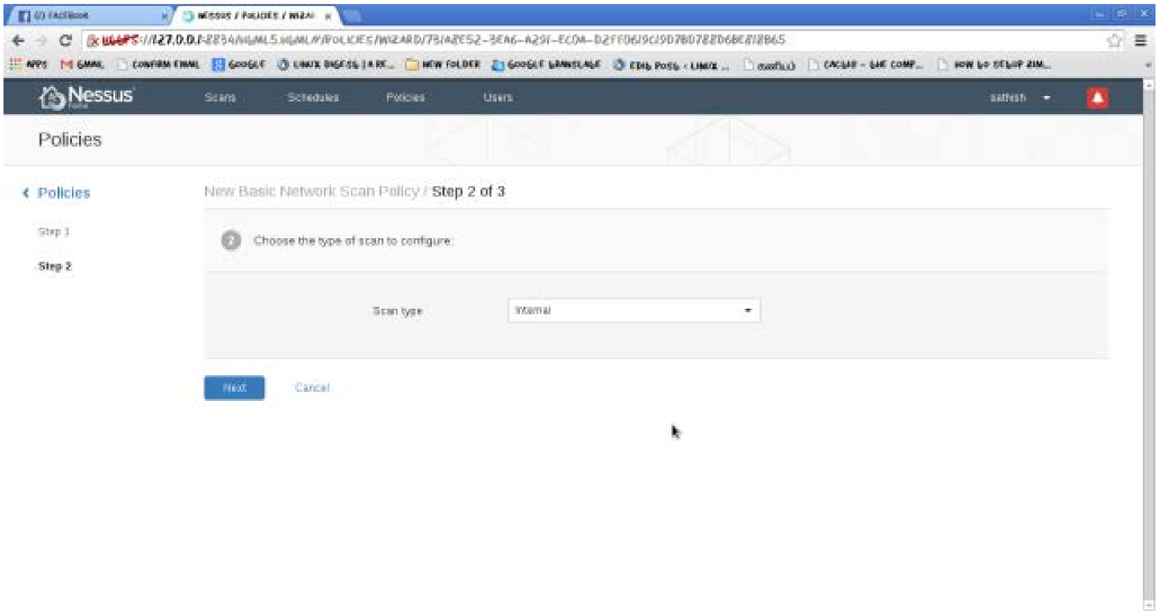


New Basic Network Scan Policy / Step 1 of 3

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

Policy Name: simple network scan
Visibility: private
Description: simple network scan for vulnerability
Allow Post-Scan Report Editing: ✓

Now next step is select scan type. In this case we scan internal Network Scan, So we choose Internal from dropdown list as shown below:

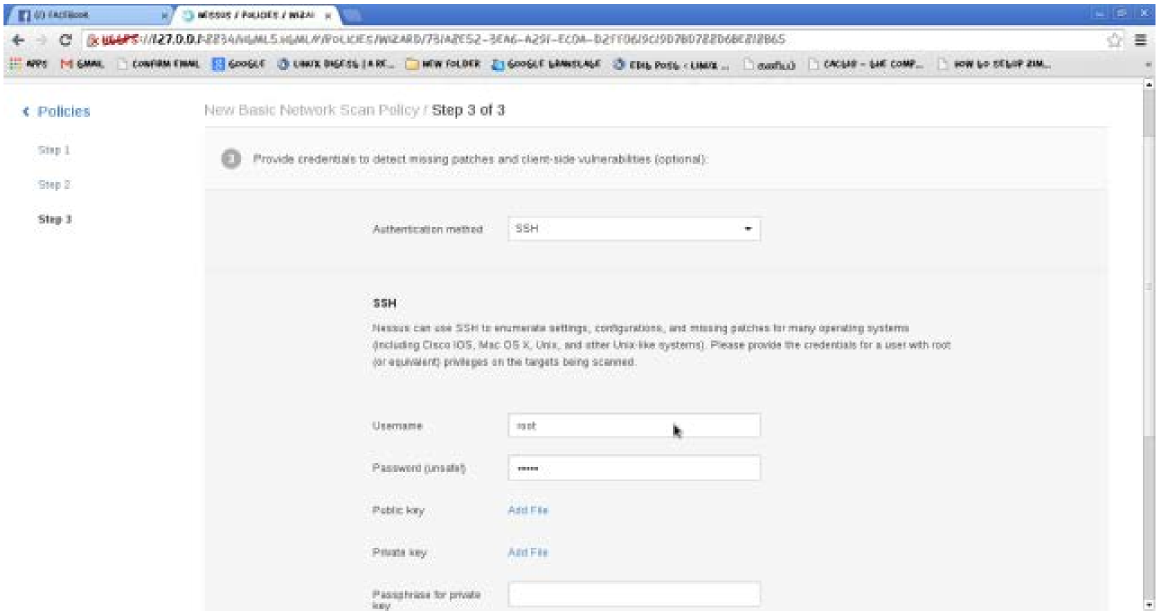


New Basic Network Scan Policy / Step 2 of 3

Choose the type of scan to configure:

Scan type: Internal

Now final step is fill credentials to detect missing patches and client-side Vulnerabilities As show below:



New Basic Network Scan Policy / Step 3 of 3

Provide credentials to detect missing patches and client-side vulnerabilities (optional):

Authentication method: SSH

SSH

Nessus can use SSH to enumerate settings, configurations, and missing patches for many operating systems (including Cisco IOS, Mac OS X, Unix, and other Unix-like systems). Please provide the credentials for a user with root (or equivalent) privileges on the targets being scanned.

Username: root

Password (unsafe): ••••••

Public key

Private key

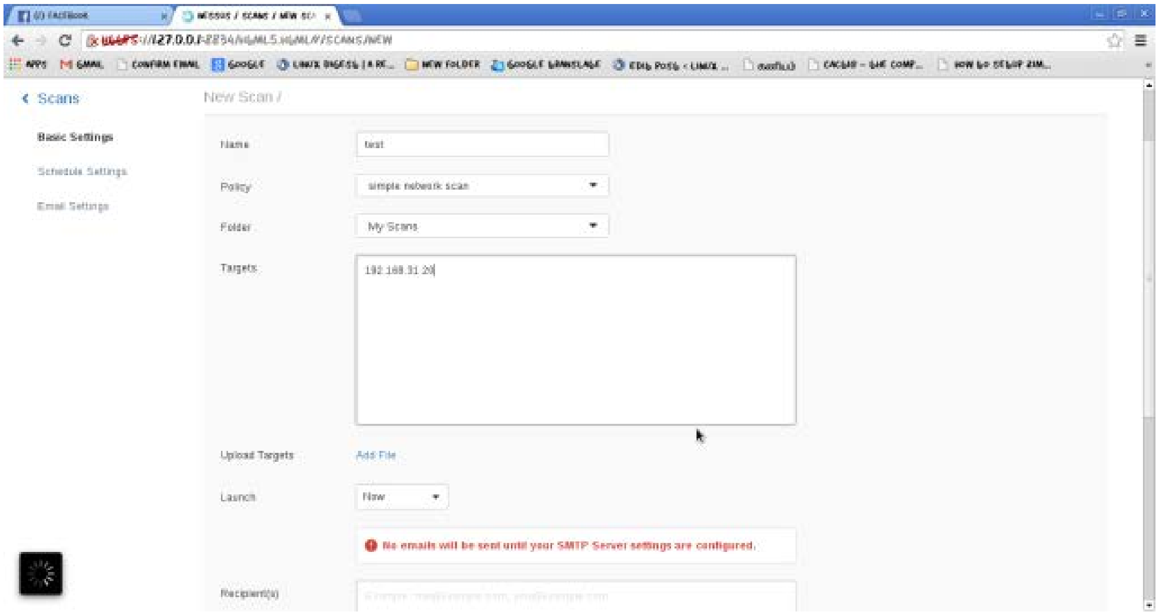
Passphrase for private key

When you are done with your selections, click Submit to save the new policy. Your newly added policy should be displayed under Policies.

## Running a Nessus Scan:

After you have created a scan policy, you are ready to configure a scan.

Select the Scans tab, and then click the New Scan button to open the scan configuration window. Fill credentials as shown below button:



New Scan /

Name: test

Policy: simple network scan

Folder: My Scans

Targets: 192.168.31.20

Upload Targets

Launch: Now

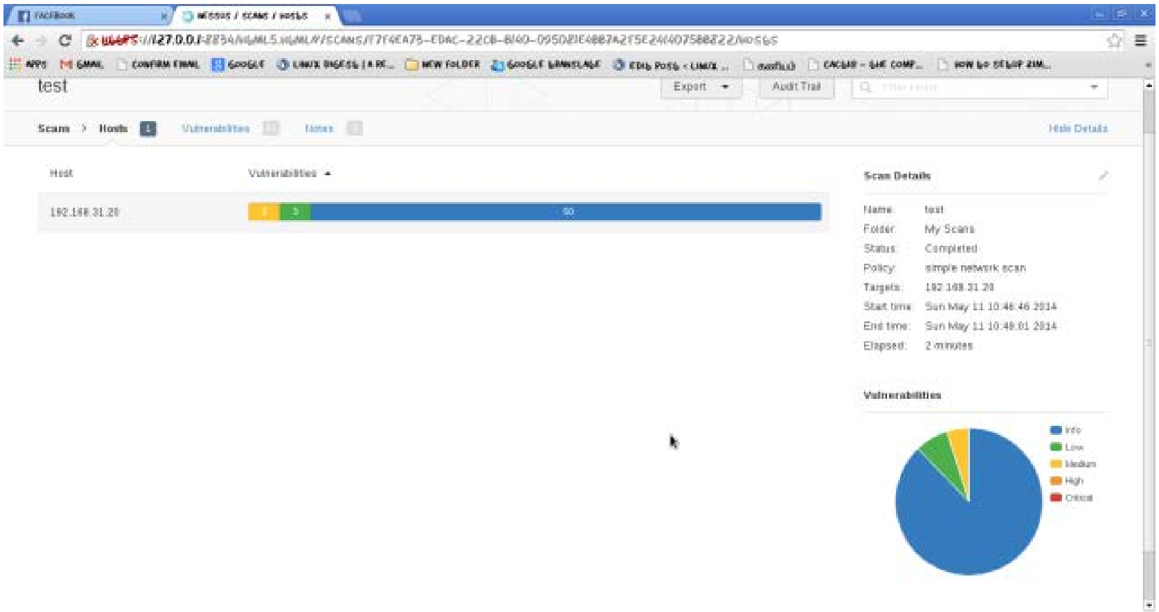
No emails will be sent until your SMTP Server settings are configured.

Recipient(s)

In our example, we are scanning only one host, but you can also enter IP address ranges in CIDR notation or even upload a file containing the addresses of the targets you want to scan. When you are satisfied with the scan configuration, click Launch.

## Nessus Reports:

After the scan is complete, click on scan and then you can see its status. Now import report as shown below:



192.168.31.20

**Scan Details**

Name: test
Folder: My Scans
Status: Completed
Policy: simple network scan
Targets: 192.168.31.20
Start time: Sun May 11 10:46:46 2014
End time: Sun May 11 10:49:01 2014
Elapsed: 2 minutes

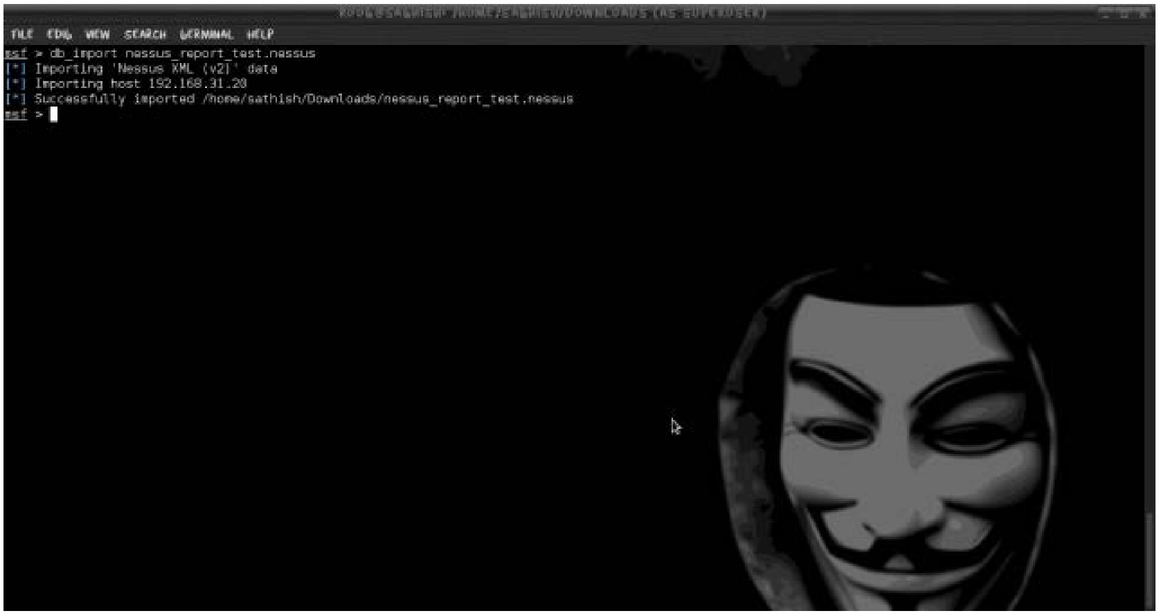
**Vulnerabilities**

## Importing Results into the Metasploit Framework:

Click the Export button to save the results to your hard drive. The default file format for Nessus reports is ".nessus" that can be supported by Metasploit. So export report as Nessus as shown below:

Load msfconsole, and import the Nessus results file by entering db_import followed by the report filename.

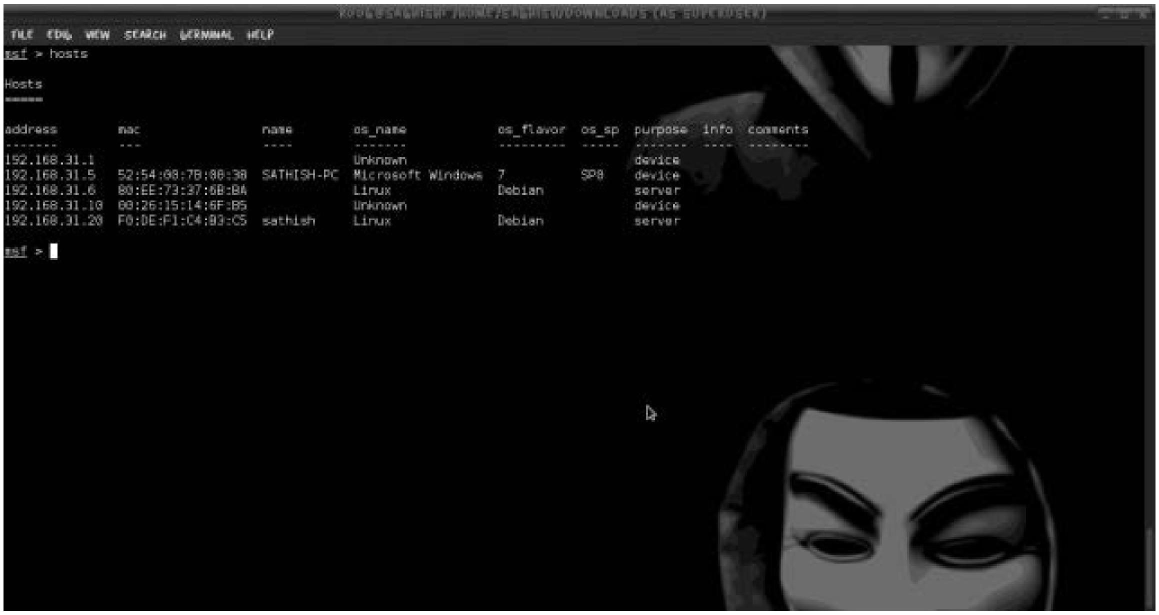
```
#msf> db_import nessus_report_test.nessus
```



```
msf > db_import nessus_report_test.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.31.20
[*] Successfully imported /home/sathish/Downloads/nessus_report_test.nessus
msf >
```

To verify that the scanned host and vulnerability data was imported properly, enter hosts as shown next. This should output a brief listing with the target IP address, the number of services detected, and the number of vulnerabilities found by Nessus.

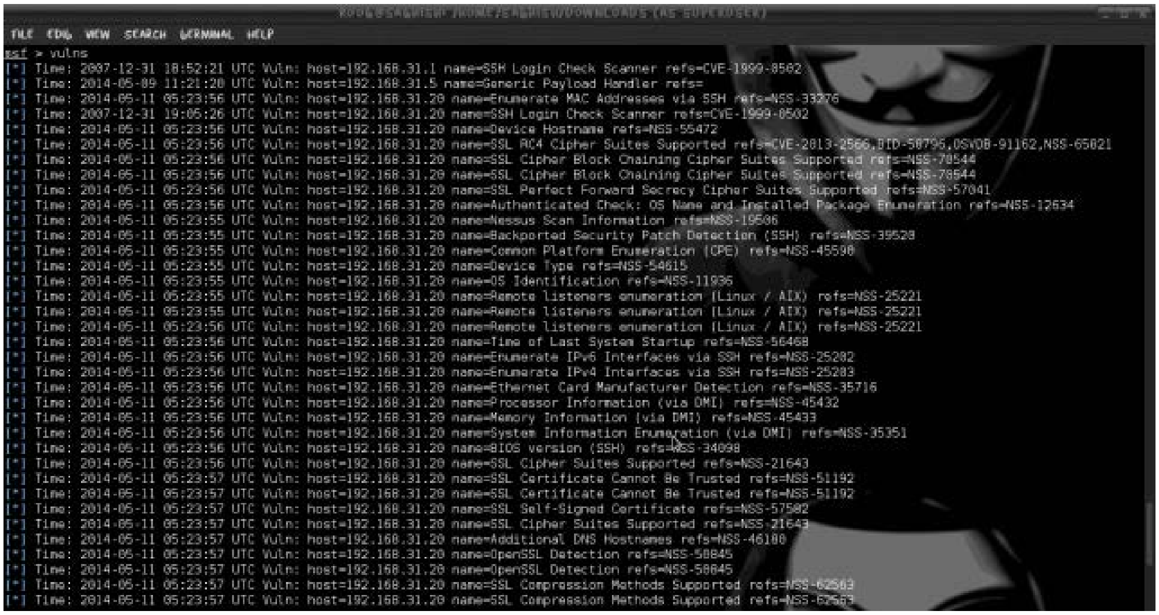
```
#msf>hosts
```



```
msf > hosts

Hosts
=====

address        mac                name        os_name            os_flavor  os_sp  purpose  info  comments
-------        ---                ----        -------            ---------  -----  -------  ----  --------
192.168.31.1                                  Unknown                              device
192.168.31.5   52:54:00:7B:80:38  SATHISH-PC  Microsoft Windows  7          SP0    device
192.168.31.6   80:EE:73:37:6B:BA              Linux              Debian            server
192.168.31.10  00:26:15:14:6F:B5              Unknown                              device
192.168.31.20  F0:DE:F1:C4:B3:C5  sathish     Linux              Debian            server

msf >
```

For a complete listing of the vulnerability data that was imported into Metasploit. Enter vulns command as shown below:

```
#msf>vulns
```



```
msf > vulns
[*] Time: 2007-12-31 18:52:21 UTC Vuln: host=192.168.31.1 name=SSH Login Check Scanner refs=CVE-1999-0502
[*] Time: 2014-05-09 11:21:20 UTC Vuln: host=192.168.31.5 name=Generic Payload Handler refs=
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=Enumerate MAC Addresses via SSH refs=NSS-33276
[*] Time: 2007-12-31 19:05:26 UTC Vuln: host=192.168.31.20 name=SSH Login Check Scanner refs=CVE-1999-0502
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=Device Hostname refs=NSS-55472
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=SSL RC4 Cipher Suites Supported refs=CVE-2013-2566,BID-58796,OSVDB-91162,NSS-65821
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=SSL Cipher Block Chaining Cipher Suites Supported refs=NSS-70544
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=SSL Cipher Block Chaining Cipher Suites Supported refs=NSS-70544
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=SSL Perfect Forward Secrecy Cipher Suites Supported refs=NSS-57041
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=Authenticated Check: OS Name and Installed Package Enumeration refs=NSS-12634
[*] Time: 2014-05-11 05:23:55 UTC Vuln: host=192.168.31.20 name=Nessus Scan Information refs=NSS-19506
[*] Time: 2014-05-11 05:23:55 UTC Vuln: host=192.168.31.20 name=Backported Security Patch Detection (SSH) refs=NSS-39520
[*] Time: 2014-05-11 05:23:55 UTC Vuln: host=192.168.31.20 name=Common Platform Enumeration (CPE) refs=NSS-45590
[*] Time: 2014-05-11 05:23:55 UTC Vuln: host=192.168.31.20 name=Device Type refs=NSS-54615
[*] Time: 2014-05-11 05:23:55 UTC Vuln: host=192.168.31.20 name=OS Identification refs=NSS-11936
[*] Time: 2014-05-11 05:23:55 UTC Vuln: host=192.168.31.20 name=Remote listeners enumeration (Linux / AIX) refs=NSS-25221
[*] Time: 2014-05-11 05:23:55 UTC Vuln: host=192.168.31.20 name=Remote listeners enumeration (Linux / AIX) refs=NSS-25221
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=Remote listeners enumeration (Linux / AIX) refs=NSS-25221
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=Time of Last System Startup refs=NSS-56468
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=Enumerate IPv6 Interfaces via SSH refs=NSS-25202
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=Enumerate IPv4 Interfaces via SSH refs=NSS-25203
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=Ethernet Card Manufacturer Detection refs=NSS-35716
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=Processor Information (via DMI) refs=NSS-45432
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=Memory Information (via DMI) refs=NSS-45433
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=System Information Enumeration (via DMI) refs=NSS-35351
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=BIOS version (SSH) refs=NSS-34098
[*] Time: 2014-05-11 05:23:56 UTC Vuln: host=192.168.31.20 name=SSL Cipher Suites Supported refs=NSS-21643
[*] Time: 2014-05-11 05:23:57 UTC Vuln: host=192.168.31.20 name=SSL Certificate Cannot Be Trusted refs=NSS-51192
[*] Time: 2014-05-11 05:23:57 UTC Vuln: host=192.168.31.20 name=SSL Certificate Cannot Be Trusted refs=NSS-51192
[*] Time: 2014-05-11 05:23:57 UTC Vuln: host=192.168.31.20 name=SSL Self-Signed Certificate refs=NSS-57582
[*] Time: 2014-05-11 05:23:57 UTC Vuln: host=192.168.31.20 name=SSL Cipher Suites Supported refs=NSS-21643
[*] Time: 2014-05-11 05:23:57 UTC Vuln: host=192.168.31.20 name=Additional DNS Hostnames refs=NSS-46180
[*] Time: 2014-05-11 05:23:57 UTC Vuln: host=192.168.31.20 name=OpenSSL Detection refs=NSS-50845
[*] Time: 2014-05-11 05:23:57 UTC Vuln: host=192.168.31.20 name=OpenSSL Detection refs=NSS-50845
[*] Time: 2014-05-11 05:23:57 UTC Vuln: host=192.168.31.20 name=SSL Compression Methods Supported refs=NSS-62563
[*] Time: 2014-05-11 05:23:57 UTC Vuln: host=192.168.31.20 name=SSL Compression Methods Supported refs=NSS-62563
```

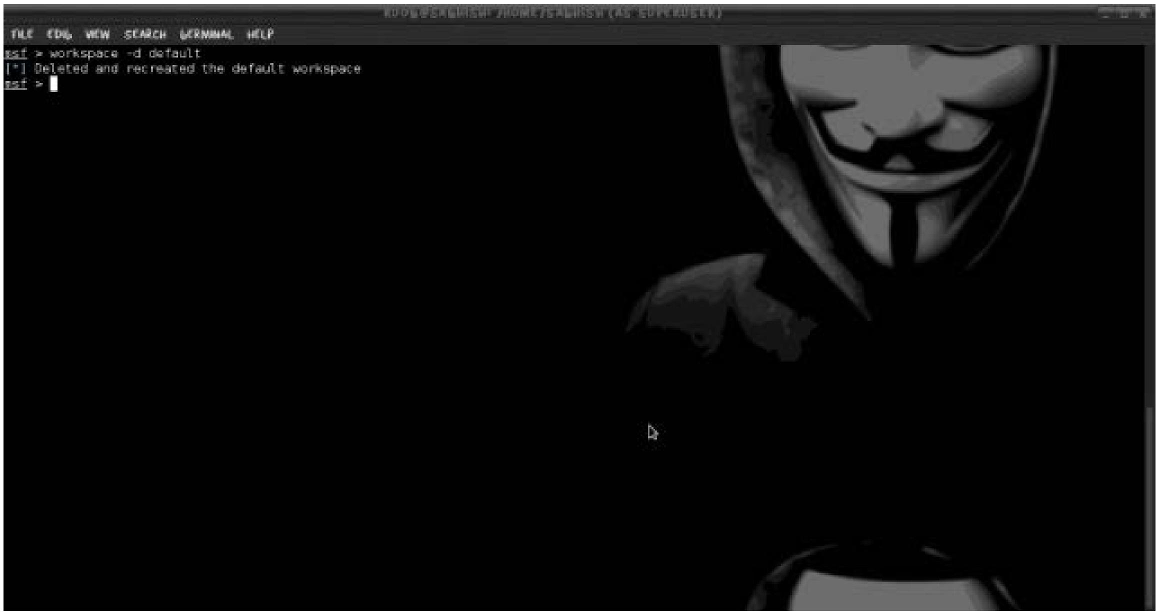
If you are lazy to work with GUI in Nessus, don't worry you can work with metasploit  by loading nessus plugin.

## Scanning Vulnerability using Nessus Metasploit's Plug-in:

The Nessus allows you to control Nessus completely through the Metasploit Framework. Run scans, interpret results, and launch attacks based on the vulnerabilities identified through Nessus.

First destroy the existing database. We can destroy database using  Workspace command to do same. So delete previous pentesting results as shown below:

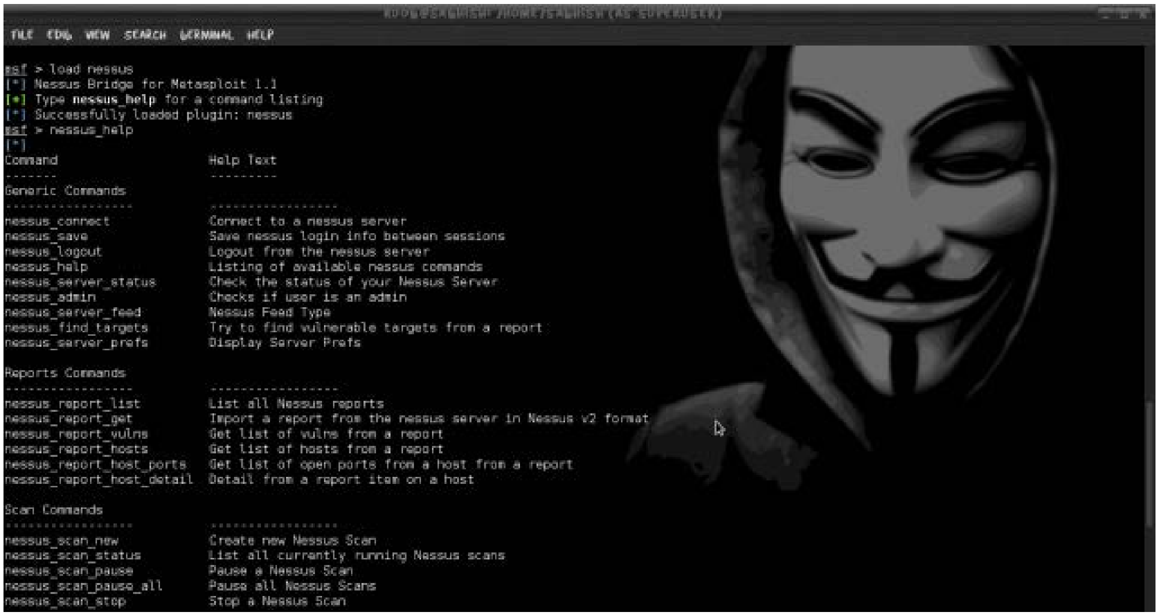
```
#msf > workspace -d default
```



```
msf > workspace -d default
[*] Deleted and recreated the default workspace
msf >
```

Load the Nessus plug-in by running load nessus and Running the command nessus_help will display all of the commands that e plug-in supports. As shown below:

```
#msf > load nessus

#msf > nessus_help
```



```
msf > load nessus
[*] Nessus Bridge for Metasploit 1.1
[+] Type nessus_help for a command listing
[*] Successfully loaded plugin: nessus
msf > nessus_help
[*]
Command                     Help Text
-------                     ---------
Generic Commands
-----------------           -----------------
nessus_connect              Connect to a nessus server
nessus_save                 Save nessus login info between sessions
nessus_logout               Logout from the nessus server
nessus_help                 Listing of available nessus commands
nessus_server_status        Check the status of your Nessus Server
nessus_admin                Checks if user is an admin
nessus_server_feed          Nessus Feed Type
nessus_find_targets         Try to find vulnerable targets from a report
nessus_server_prefs         Display Server Prefs

Reports Commands
-----------------           -----------------
nessus_report_list          List all Nessus reports
nessus_report_get           Import a report from the nessus server in Nessus v2 format
nessus_report_vulns         Get list of vulns from a report
nessus_report_hosts         Get list of hosts from a report
nessus_report_host_ports    Get list of open ports from a host from a report
nessus_report_host_detail   Detail from a report item on a host

Scan Commands
-----------------           -----------------
nessus_scan_new             Create new Nessus Scan
nessus_scan_status          List all currently running Nessus scans
nessus_scan_pause           Pause a Nessus Scan
nessus_scan_pause_all       Pause all Nessus Scans
nessus_scan_stop            Stop a Nessus Scan
```

Before starting a scan with nessus plug-in, you first need to authenticate to your Nessus server using nessus_connect command.

```
#msf > nessus_connect  sathish:bhuvi@localhost:8834
```

As with the GUI version of Nessus, you need to initiate a scan using a defined policy by its policy ID number. To list the available scan policies on the server, use nessus_policy_list

```
#msf > nessus_policy_list
```

Take policy ID to use for your scan, and then launch a new scan with nessus_scan_new followed by the policy number, a name for your scan, and your target IP address as shown below.

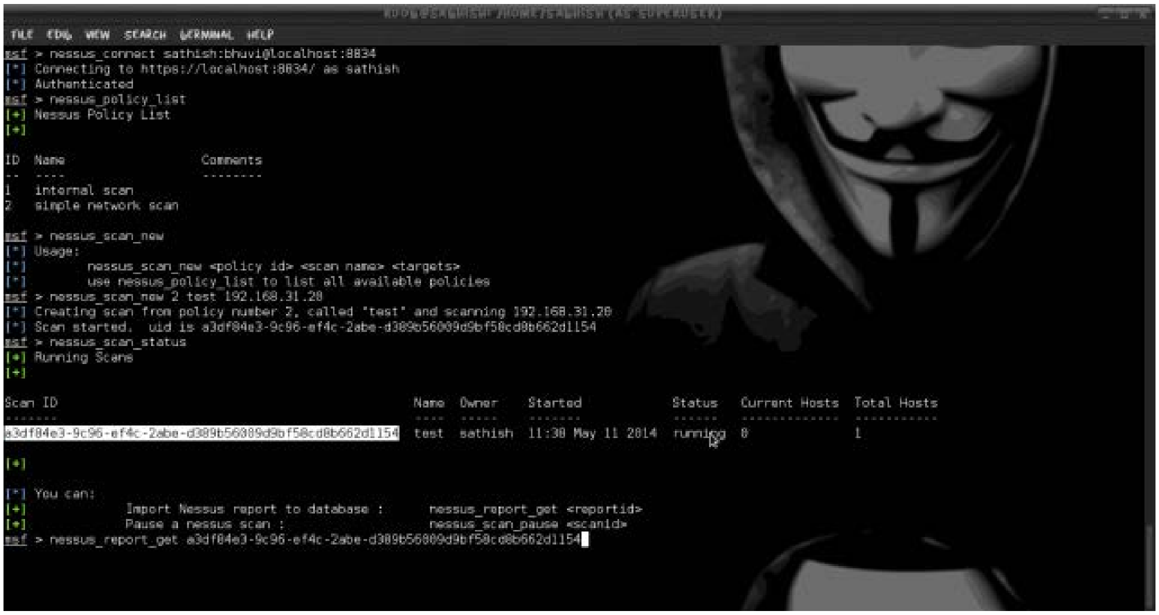
```
#msf > nessus_scan_new
```

While your scan is in progress, you can see its status by running the nessus_scan_status command. When this command's output responds with "No Scans Running," as shown next, you will know that your scan has completed.

```
#msf > nessus_scan_new  2  test  192.168.31.20
```

After the scan has completed, you can list the available scan reports with the nessus_report_list command. Identify the ID of the report you want to import and enter nessus_report_get to download the report and import it into the Metasploit database automatically.

```
#msf >  nessus_report_get  ID
```



```
msf > nessus_connect sathish:bhuvi@localhost:8834
[*] Connecting to https://localhost:8834/ as sathish
[*] Authenticated
msf > nessus_policy_list
[+] Nessus Policy List
[+]

ID  Name                 Comments
--  ----                 --------
1   internal scan
2   simple network scan

msf > nessus_scan_new
[*] Usage:
[*]        nessus_scan_new <policy id> <scan name> <targets>
[*]        use nessus_policy_list to list all available policies
msf > nessus_scan_new 2 test 192.168.31.20
[*] Creating scan from policy number 2, called "test" and scanning 192.168.31.20
[*] Scan started.  uid is a3df84e3-9c96-ef4c-2abe-d389b56089d9bf58cd8b662d1154
msf > nessus_scan_status
[+] Running Scans
[+]

Scan ID                                                Name  Owner    Started            Status   Current Hosts  Total Hosts
-------                                                ----  -----    -------            ------   -------------  -----------
a3df84e3-9c96-ef4c-2abe-d389b56089d9bf58cd8b662d1154   test  sathish  11:30 May 11 2014  running  0              1

[+]

[*] You can:
[+]           Import Nessus report to database :      nessus_report_get <reportid>
[+]           Pause a nessus scan :                   nessus_scan_pause <scanid>
msf > nessus_report_get a3df84e3-9c96-ef4c-2abe-d389b56089d9bf58cd8b662d1154
```

You can use hosts to verify that the scan data was imported successfully.

We can check all vulnerabilities by typing vulns command. As you can see above tutorials Metasploit is power full framework for penetration tester.

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses. And it’s a part of penetration testing. If you do not know target vulnerability then you cannot success most of the time during your penetration testing process.