



Information Assurance & Auditing

4th Year - 1st Semester

Assignment

Registration No: IT17065122

Name: Ranasinghe D.N.

Batch: CSNE-WE

Table of Contents

Introduction.	3
Create virtual machines in VMware workstation.	4
Source virtual machine creation.	4
Target virtual machine creation.	4
Install Applications in source and target virtual machines.	5
Source server application installation.	5
Target server application installation.	7
Scan remote server using Nessus.	9

Introduction.

Information security is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or at least reducing the probability of unauthorized or inappropriate access to data. Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data.

Information security is the most important and main point in working environment. Because if we do not manage security layer proper way data and services are in risk from attackers. Therefor we need to identify problems and fix those problems as possible. We can use security tool for identify issues which are available in virtual servers, web application such as services. We need to do security scan using one of those tool and it will provide list of issues about our target hosts or applications.

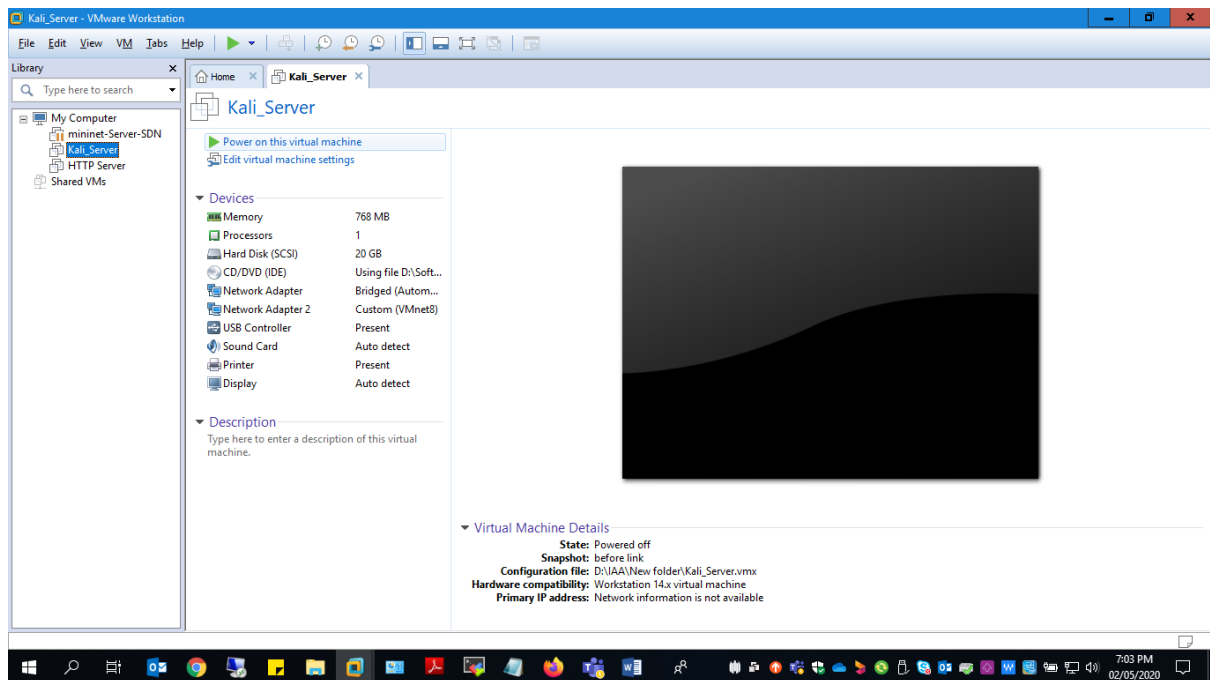
In this Assignment I'm going to use Nessus Manager tool to scan and identify problems are in my remote virtual host. Nessus is a one of best security tool to identify network level and application level bugs. In this report I will explain how to do a vulnerability scan and discuss what are the steps we want to follow to fix those issues.

Vulnerabilities are the weak points of application or operating system. After identifying those issues outside attackers can enter to our system or servers using those vulnerabilities. It can be a big problem for entire system. Because these type of attackers can be damage user sensitive data. It can be a disaster in IT base company. Therefor we need to fix those issues and mitigate risk from our working environment.

Create virtual machines in VMware workstation.

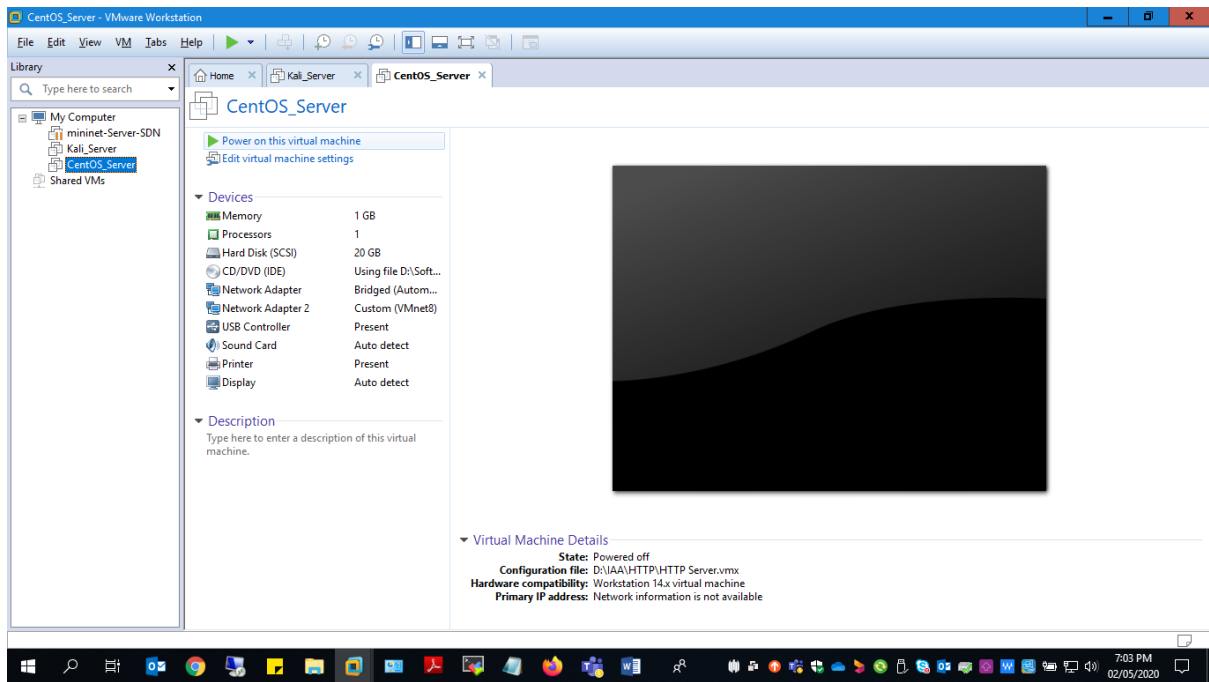
Source virtual machine creation.

I have created virtual machine with Kali Linux operating system for install Nessus Manager service.



Target virtual machine creation.

I have created virtual machine with CentOS 7.4 operating system. I'm going to install multiple applications in this server to expose several ports using TCP/UDP protocol.



Install Applications in source and target virtual machines.

Source server application installation.

In our source server based on kali Linux operating system. In this task we need to install Nessus Manager tool. Using this tool, we going to scan my target CentOS virtual machine located within same network range.

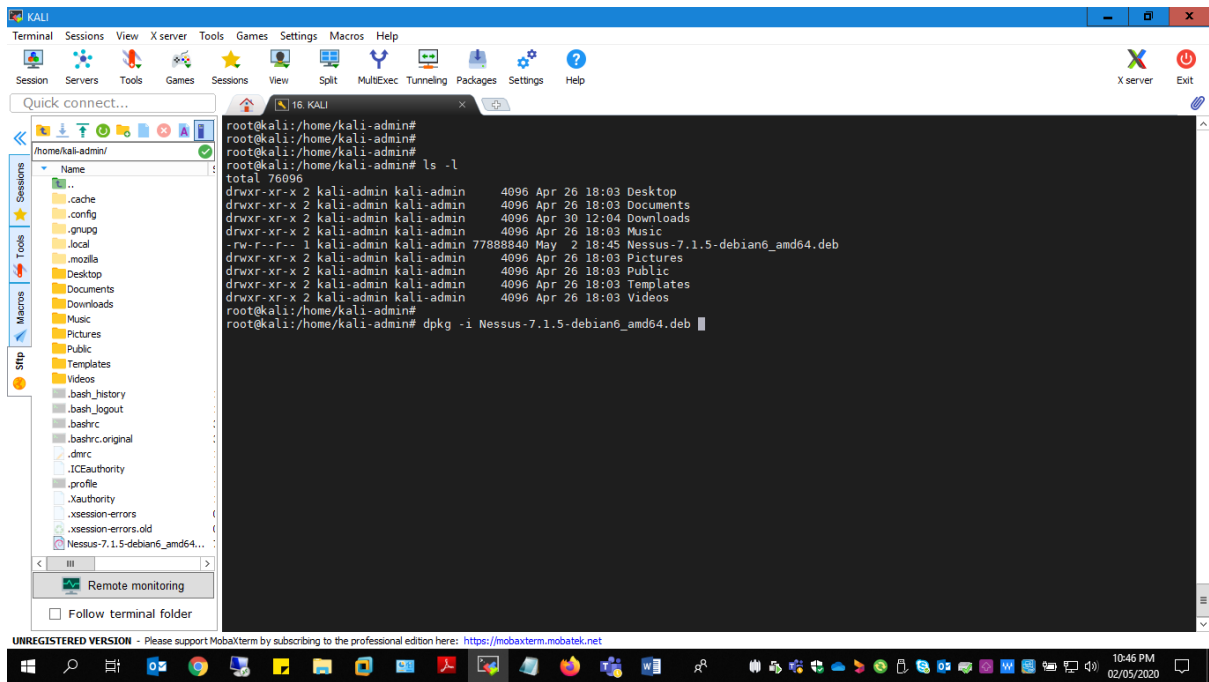
As initial step need to download Nessus application sources using below mention tenable official site.

URL :- <http://www.tenable.com/downloads>

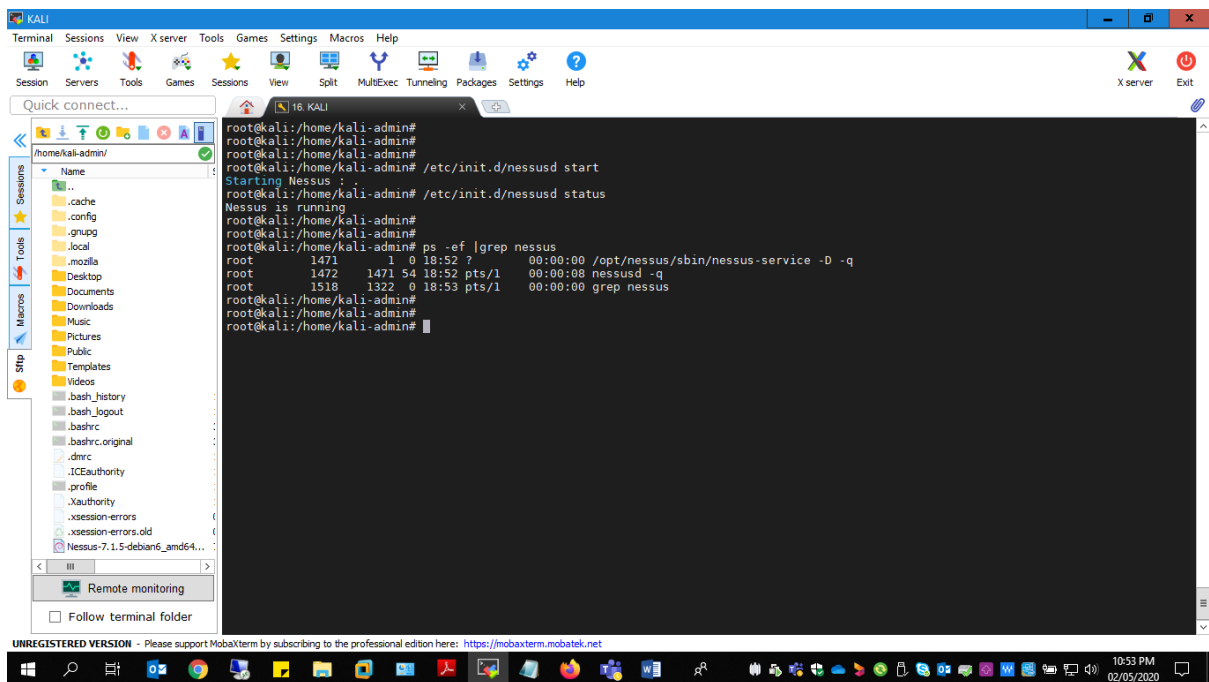
Need to download source relevant and support to operating system also,

After executing command as below service will be install.

```
dpkg -i < $package.deb >
```



After installed need to start Nessus service as below,



Target server application installation.

In target server operating system based on CentOS 7.4 image. I'm going to install multiple application services to expose several ports from target machine. Because while server scanning we can get more information about those ports.

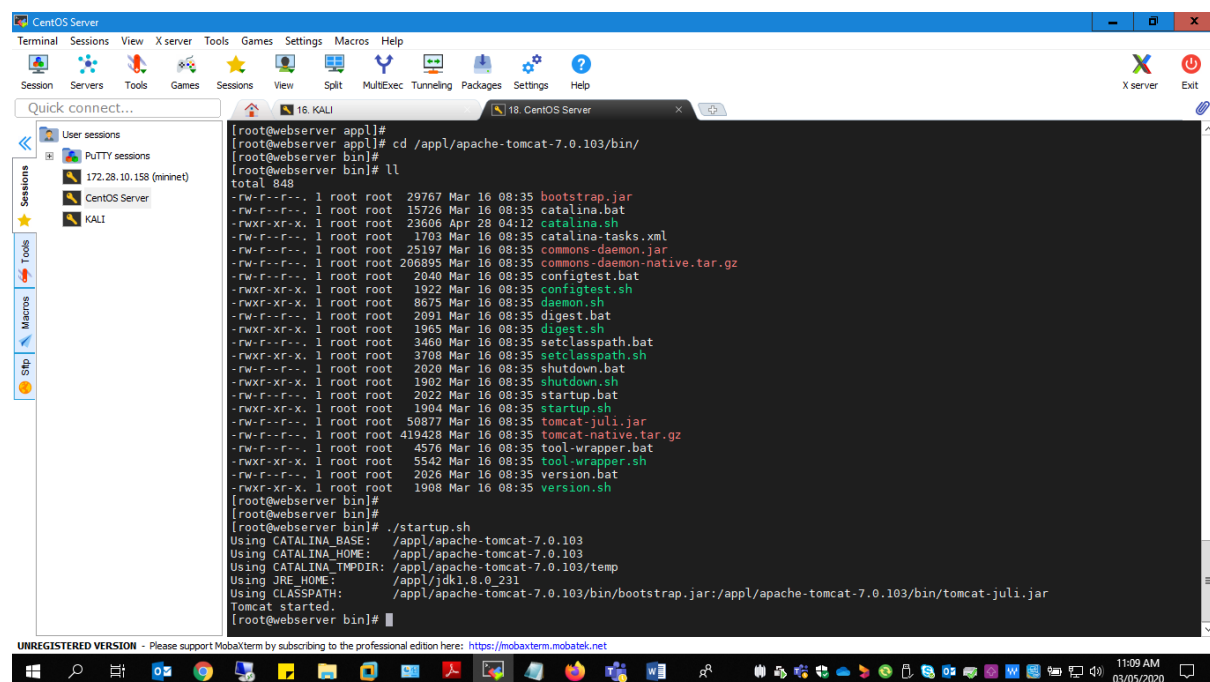
- Apache service installation.

We can download apache sources using <https://downloads.apache.org> web site.

After download I'm going to extract sources to "/appl" target directory. Below command will do the extract process.

"Unzip apache-tomcat-7.0.103.zip -d /appl/"

Then need to start apache service executing **startup.sh** file as below.



```
[root@webserver appl]#
[root@webserver appl]# cd /appl/apache-tomcat-7.0.103/bin/
[root@webserver bin]#
[root@webserver bin]# ll
total 848
-rw-r--r-- 1 root root 29767 Mar 16 08:35 bootstrap.jar
-rw-r--r-- 1 root root 15726 Mar 16 08:35 catalina.bat
-rwxr-xr-x 1 root root 23606 Apr 28 04:12 catalina.sh
-rw-r--r-- 1 root root 1703 Mar 16 08:35 catalina-tasks.xml
-rw-r--r-- 1 root root 25197 Mar 16 08:35 commons-daemon.jar
-rw-r--r-- 1 root root 206895 Mar 16 08:35 commons-daemon-native.tar.gz
-rw-r--r-- 1 root root 2040 Mar 16 08:35 configtest.bat
-rwxr-xr-x 1 root root 1922 Mar 16 08:35 configtest.sh
-rwxr-xr-x 1 root root 8675 Mar 16 08:35 daemon.sh
-rw-r--r-- 1 root root 2091 Mar 16 08:35 digest.bat
-rwxr-xr-x 1 root root 1965 Mar 16 08:35 digest.sh
-rw-r--r-- 1 root root 3460 Mar 16 08:35 setclasspath.bat
-rwxr-xr-x 1 root root 3708 Mar 16 08:35 setclasspath.sh
-rw-r--r-- 1 root root 2020 Mar 16 08:35 shutdown.bat
-rwxr-xr-x 1 root root 1902 Mar 16 08:35 shutdown.sh
-rw-r--r-- 1 root root 2022 Mar 16 08:35 startup.bat
-rwxr-xr-x 1 root root 1904 Mar 16 08:35 startup.sh
-rw-r--r-- 1 root root 50877 Mar 16 08:35 tomcat-juli.jar
-rw-r--r-- 1 root root 419428 Mar 16 08:35 tomcat-native.tar.gz
-rw-r--r-- 1 root root 4576 Mar 16 08:35 tool-wrapper.bat
-rwxr-xr-x 1 root root 5542 Mar 16 08:35 tool-wrapper.sh
-rw-r--r-- 1 root root 2026 Mar 16 08:35 version.bat
-rwxr-xr-x 1 root root 1908 Mar 16 08:35 version.sh
[root@webserver bin]#
[root@webserver bin]# ./startup.sh
Using CATALINA_BASE:   /appl/apache-tomcat-7.0.103
Using CATALINA_HOME:   /appl/apache-tomcat-7.0.103
Using CATALINA_TMPDIR: /appl/apache-tomcat-7.0.103/temp
Using JRE_HOME:         /appl/jdk1.8.0_231
Using CLASSPATH:        /appl/apache-tomcat-7.0.103/bin/bootstrap.jar:/appl/apache-tomcat-7.0.103/bin/tomcat-juli.jar
Tomcat started.
[root@webserver bin]#
```

- HTTP service installation.

We can install HTTP service using yum repository. To do that installation we need to execute below command in Linux terminal.

"yum install httpd"

After install we can start service as below,

Note: I have also configured virtual host with 443 port in HTTP service.

```
CentOS Server
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
16. KALI
18. CentOS Server
[root@webserver bin]#
[root@webserver bin]#
[root@webserver bin]#
[root@webserver bin]#
[root@webserver bin]# systemctl start httpd.service
[root@webserver bin]#
[root@webserver bin]# systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2020-05-03 16:58:52 +0530; 7s ago
     Docs: man:httpd(8)
           man:apachectl(8)
   Main PID: 2981 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           └─2981 /usr/sbin/httpd -DFOREGROUND
             └─2982 /usr/sbin/httpd -DFOREGROUND
               └─2983 /usr/sbin/httpd -DFOREGROUND
                 └─2984 /usr/sbin/httpd -DFOREGROUND
                   └─2985 /usr/sbin/httpd -DFOREGROUND
                     └─2986 /usr/sbin/httpd -DFOREGROUND

May 03 16:58:49 webserver systemd[1]: Starting The Apache HTTP Server...
May 03 16:58:50 webserver httpd[2981]: AH00548: NameVirtualHost has no effect and will be removed in the next release /etc/httpd/conf:1
May 03 16:58:50 webserver httpd[2981]: AH00558: httpd: Could not reliably determine the server's fully qualified domain name, u...message
May 03 16:58:52 webserver systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@webserver bin]#
[root@webserver bin]# netstat -tupln |grep 2981
tcp6      0      0 :::80             :::*               LISTEN    2981/httpd
tcp6      0      0 :::443            :::*               LISTEN    2981/httpd
[root@webserver bin]#
[root@webserver bin]#
[UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net]
```

- Mariadb service installation.

In this service also we are going to install packages using yum repository by executing below command.

“yum install mariadb”

After installed we can start service as below,

```
CentOS Server
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
16. KALI
18. CentOS Server
[root@webserver bin]#
[root@webserver bin]#
[root@webserver bin]#
[root@webserver bin]# systemctl start mariadb.service
[root@webserver bin]#
[root@webserver bin]# systemctl status mariadb.service
● mariadb.service - MariaDB database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2020-05-03 17:35:34 +0530; 10s ago
     Process: 3102 ExecStartPost=/usr/libexec/mariadb-wait-ready $MAINPID (code=exited, status=0/SUCCESS)
     Process: 3067 ExecStartPre=/usr/libexec/mariadb-prepare-db-dir %n (code=exited, status=0/SUCCESS)
   Main PID: 3101 (mysqld_safe)
   CGroup: /system.slice/mariadb.service
           └─3101 /bin/sh /usr/bin/mysqld_safe --basedir=/usr
             └─3264 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib64/mysql/plugin --log-error=/var/lo...

May 03 17:35:32 webserver systemd[1]: Starting MariaDB database server...
May 03 17:35:32 webserver mariadb-prepare-db-dir[3067]: Database MariaDB is probably initialized in /var/lib/mysql already, noth... done.
May 03 17:35:32 webserver mysqld_safe[3101]: 200503 17:35:32 mysqld_safe Logging to '/var/log/mariadb/mariadb.log'.
May 03 17:35:32 webserver mysqld_safe[3101]: 200503 17:35:32 mysqld_safe Starting mysqld daemon with databases from /var/lib/mysql
May 03 17:35:34 webserver systemd[1]: Started MariaDB database server.
Hint: Some lines were ellipsized, use -l to show in full.
[root@webserver bin]#
[root@webserver bin]#
[root@webserver bin]# netstat -tupln |grep 3101
[root@webserver bin]# netstat -tupln |grep 3264
tcp        0      0 0.0.0.0:3306        0.0.0.0:*          LISTEN    3264/mysqld
[root@webserver bin]#
[root@webserver bin]#
[UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net]
```


Scan remote server using Nessus.

After start the Nessus process we need to create a user to initial login to the Nessus web UI.

To create new user below command, want to be execute as root user.

“/opt/nessus/sbin/nessuscli adduser”

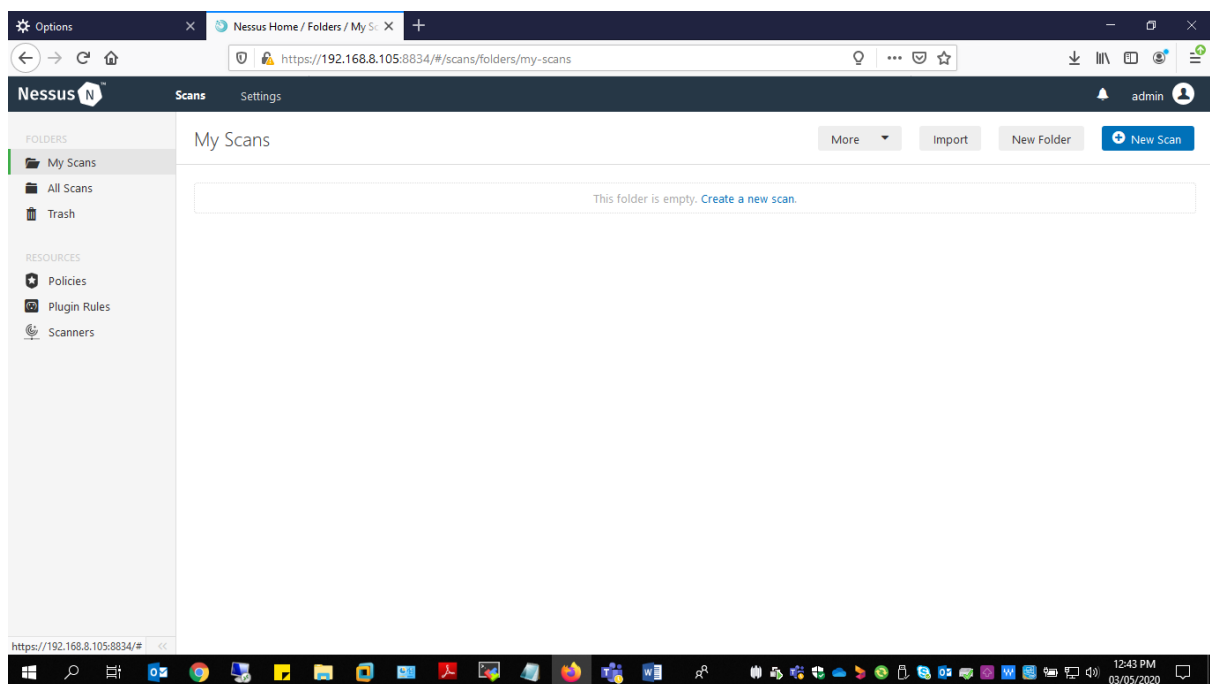
After created user need to restart the Nessus service using below commands.

“/etc/init.d/nessusd stop”

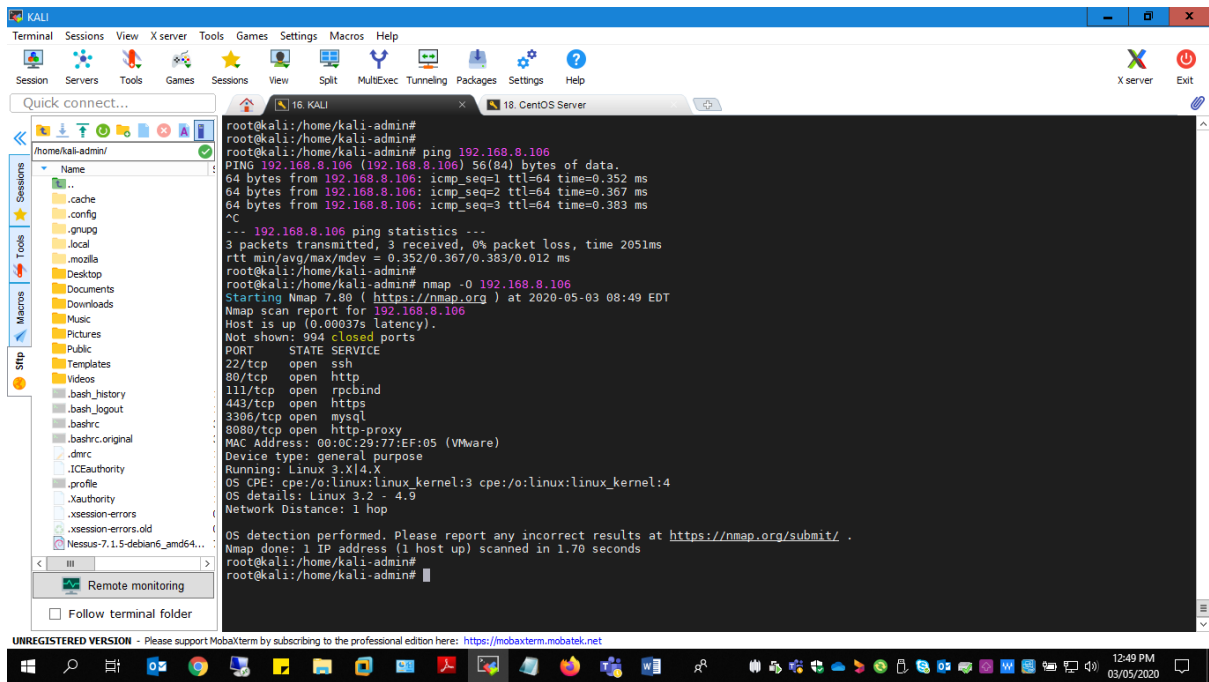
“/etc/init.d/nessusd start”

Then we can login to the Nessus interface using below URL and created user in previous step. After login it will like interface as below.

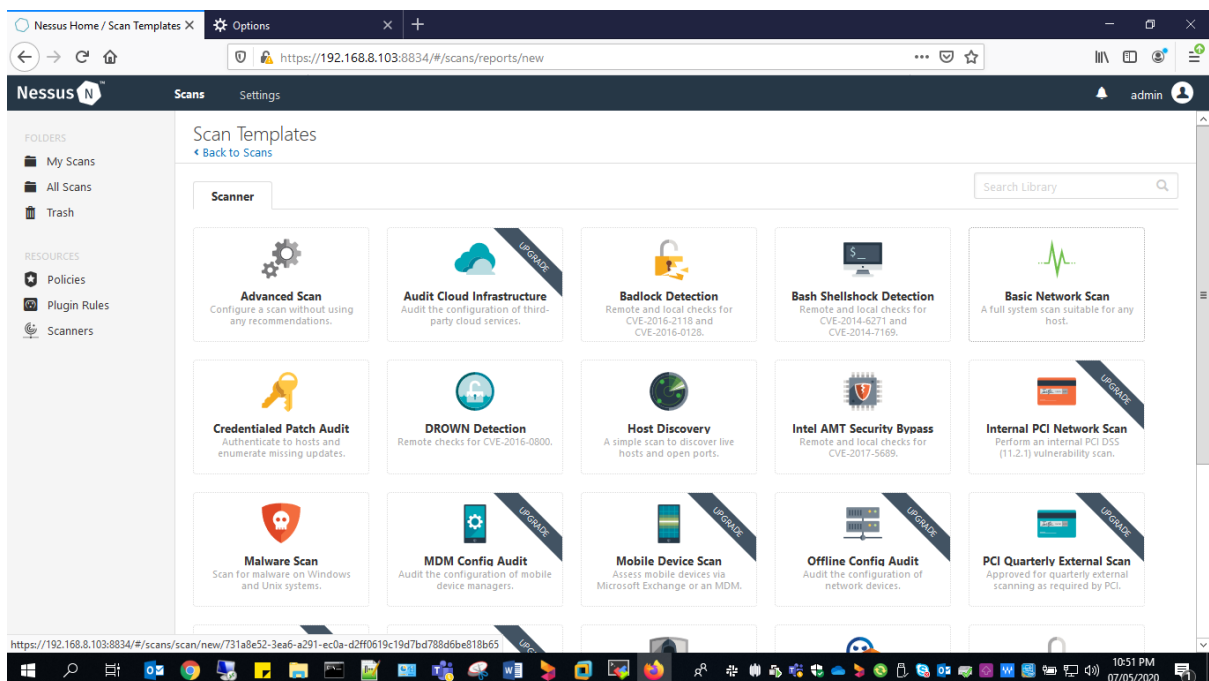
[https://<\\$host IP>:8834](https://<$host IP>:8834)



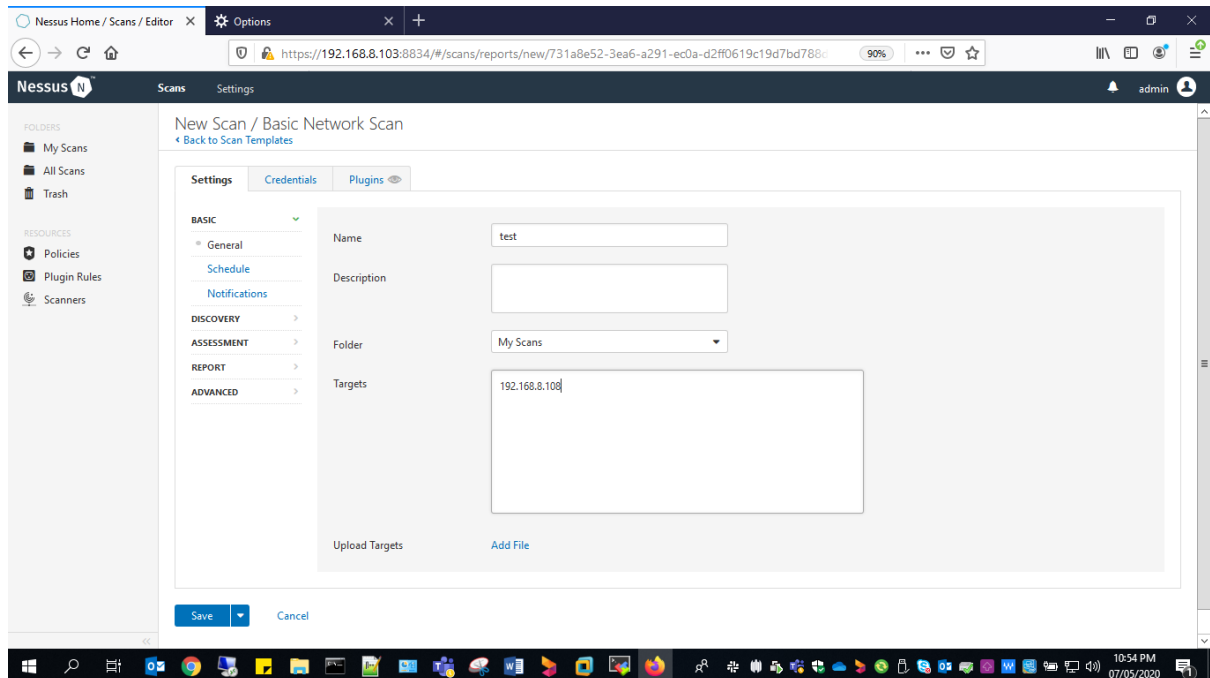
Before start vulnerability scan we need to verify connectivity between our source and target hosts using **ping** command. Also as below we can use **nmap** commands to get more information about remote server.



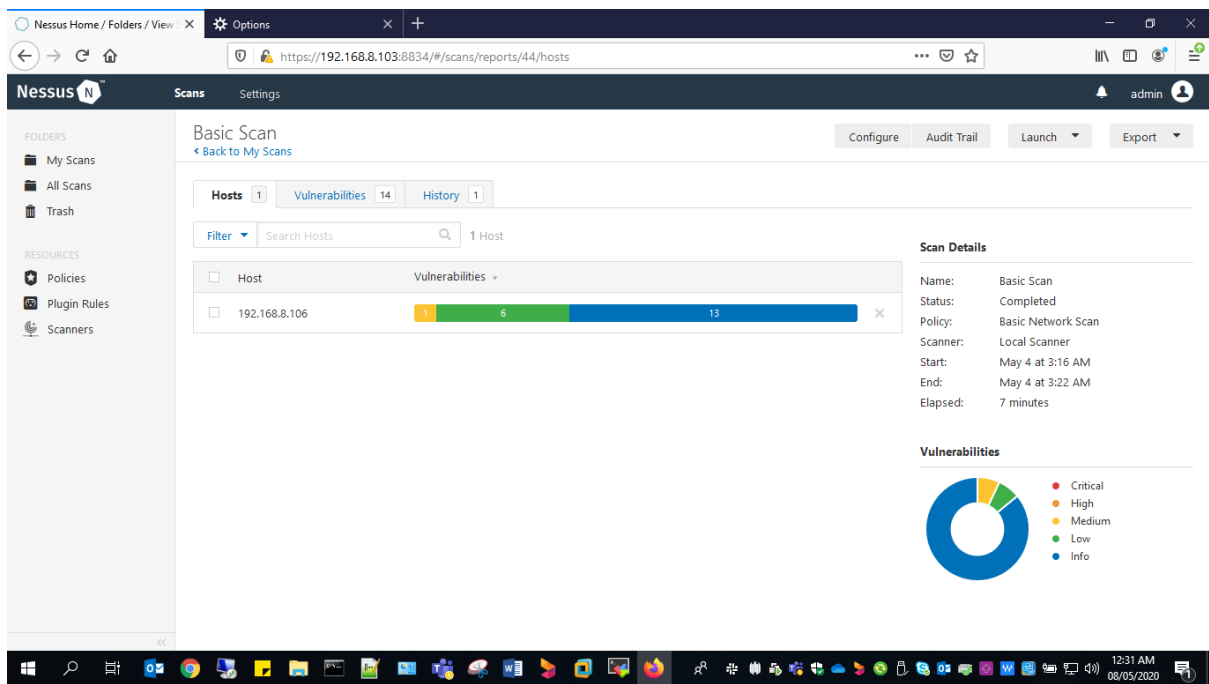
To create new scan, need to click **“New Scan”** in my scan tab. Then we want to select template for scan. There is different type of templates are available in Nessus as below in by default. We are going to use **“Basic Network Scan”** template for our task.



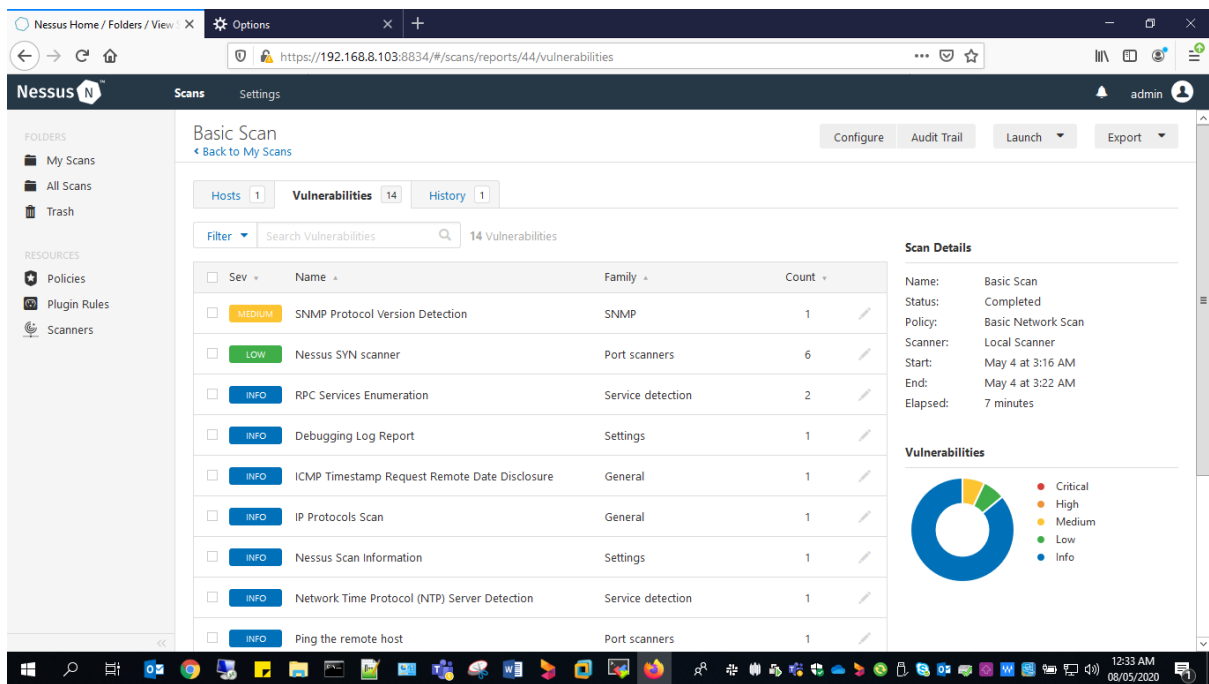
In configuration tab we need to define name for scan and target host IP for targets option. Also we can change port scan types, vulnerability scan types, report options and timeouts for our scan. After complete configuration click **“Save”** button and scan job will create.

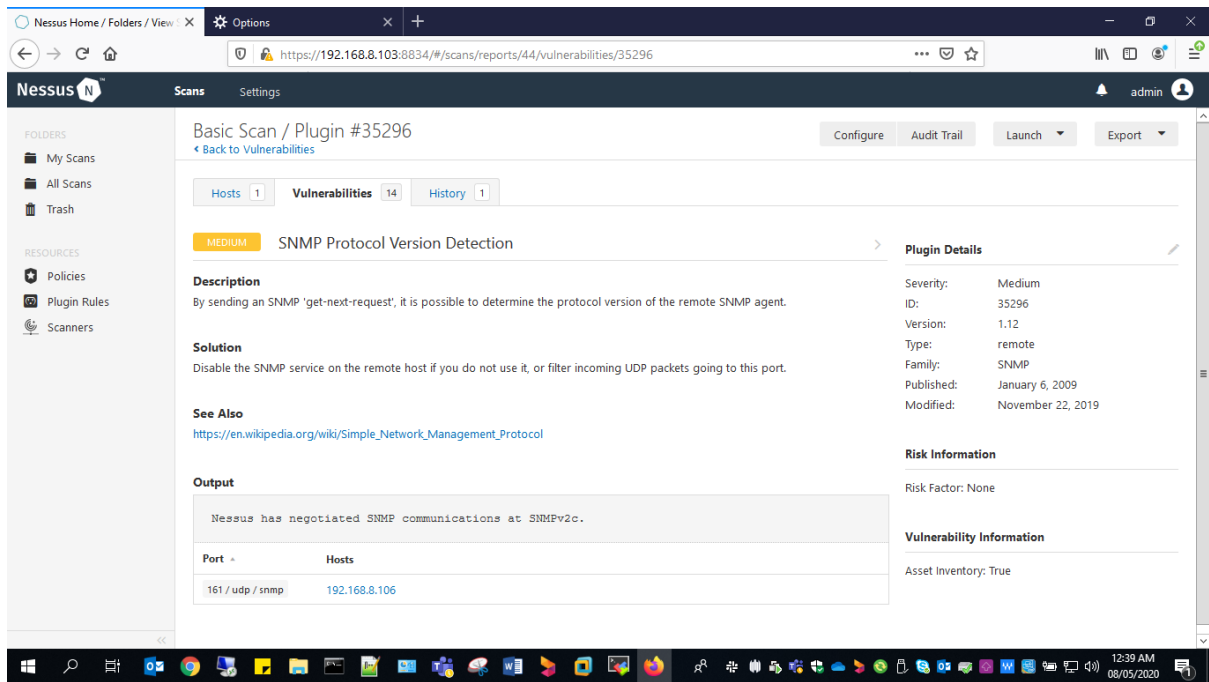


After created need to click **“Launch”** option to start scan. When scan is start it will take about 5 – 10 min time to complete that task. That time may be depending on configurations which are done in scan configuration step. After complete scan we can view vulnerability report using web user interface or download as document using export option. Go to our scan job and it will show as below,



Then switch to the vulnerability tab and it will list down all found vulnerabilities from our target host. Also it gives brief description about each vulnerability and solutions for mitigate those risks from remote host. Below screen captures will show all vulnerabilities and how it describes one of them.





In Nessus scan it divide vulnerabilities under 5 stage considering risk level. Critical, High, Medium, Low and Info are the categorizing levels. Critical level issues have highest risk for applications or services. If there any critical level issues, we need to fix those as possible to minimise attacks coming to the system. Info level problems are having lower risk.