Information Assurance & Auditing

4th Year - 1st Semester

Assignment

Registration No: IT17065122

Name: Ranasinghe D.N.

Batch: CSNE-WE

Table of Contents

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.

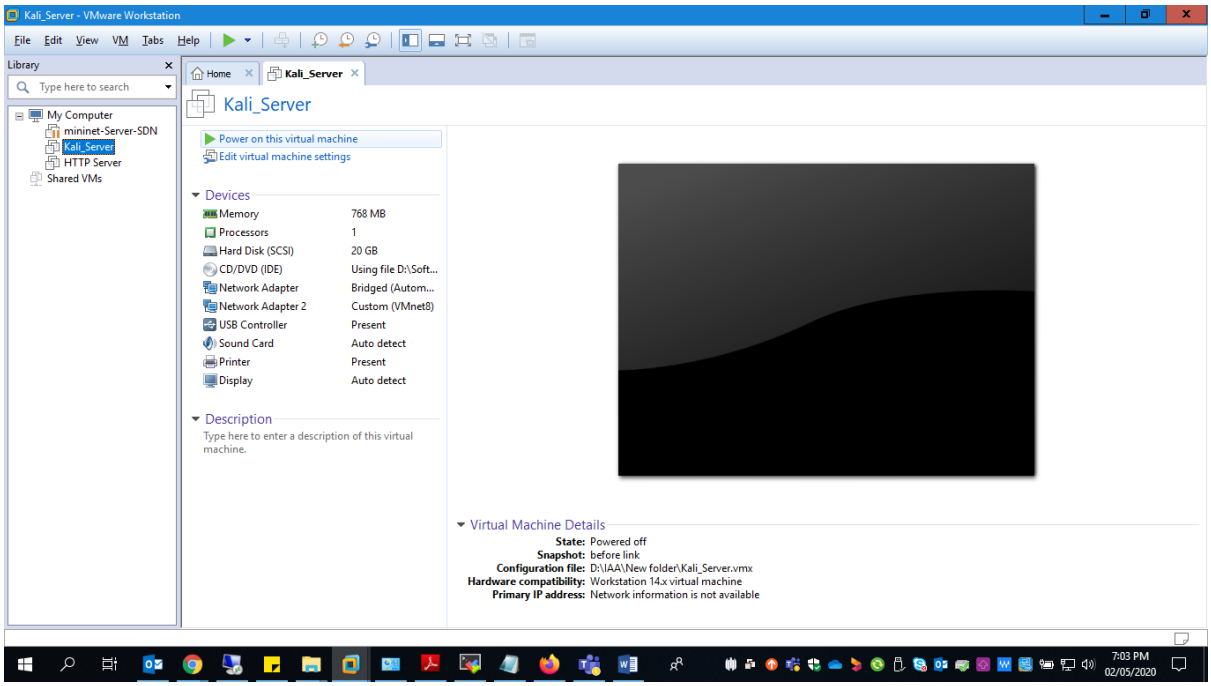
In this Assignment I'm going to use Nessus Manager tool to scan and identify problems are in my remote virtual host. Nessus is a one of best security tool to identify network level and application level bugs. In this report I will explain how to do a vulnerability scan and discuss what are the steps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

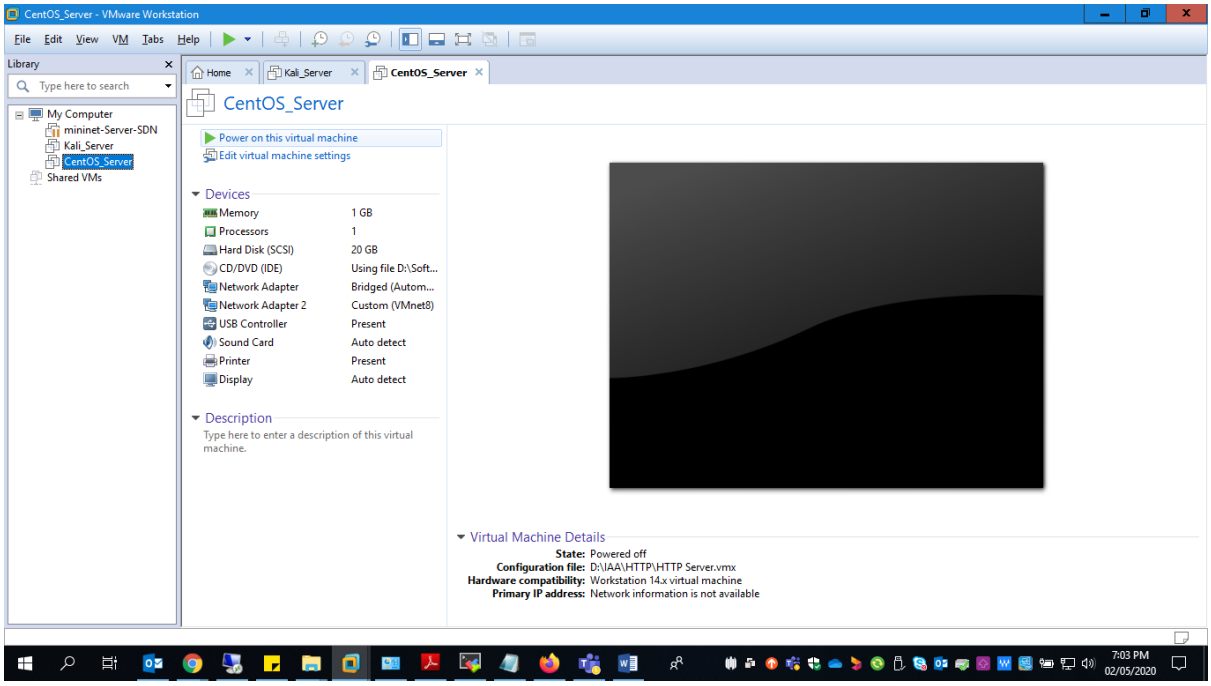
Source virtual machine creation.

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.

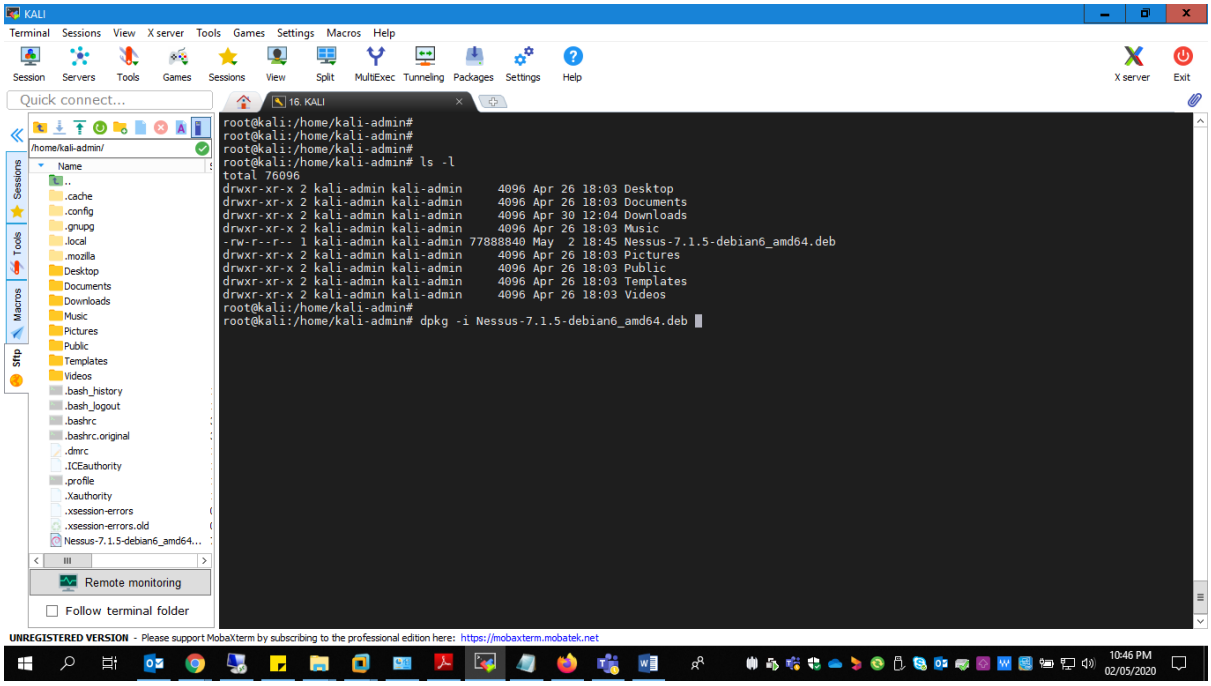
As initial step need to download Nessus application sources using below mention tenable official site.

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

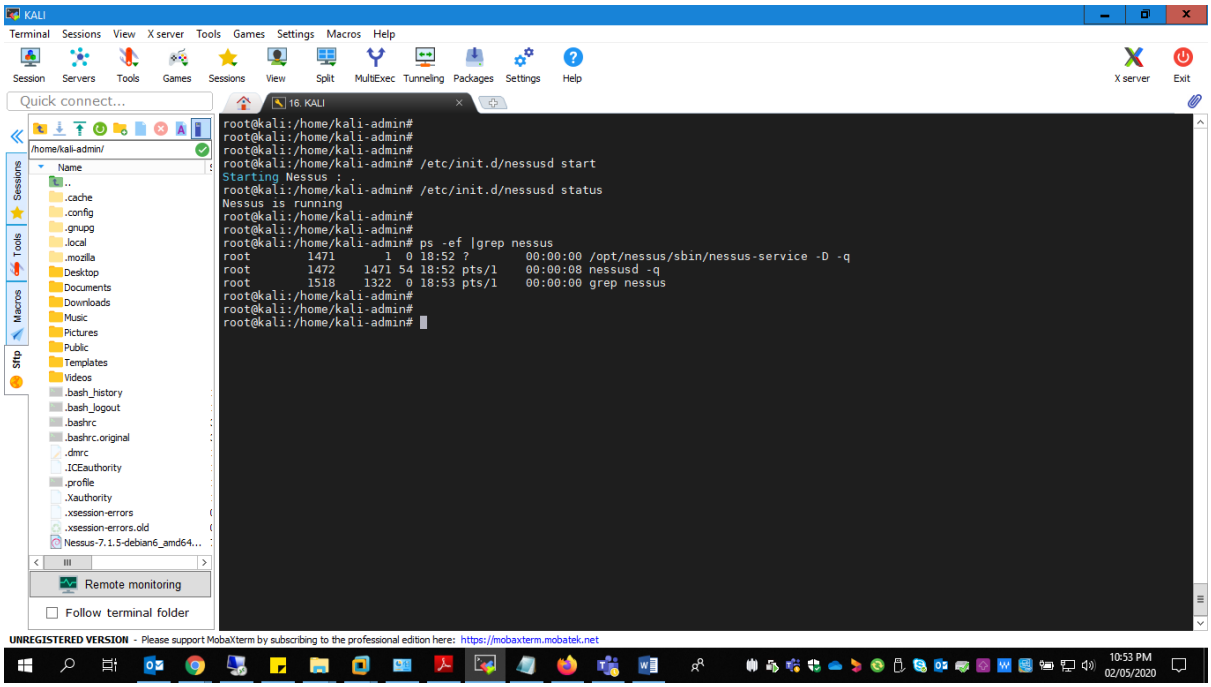
Need to download source relevant and support to operating system also,

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.

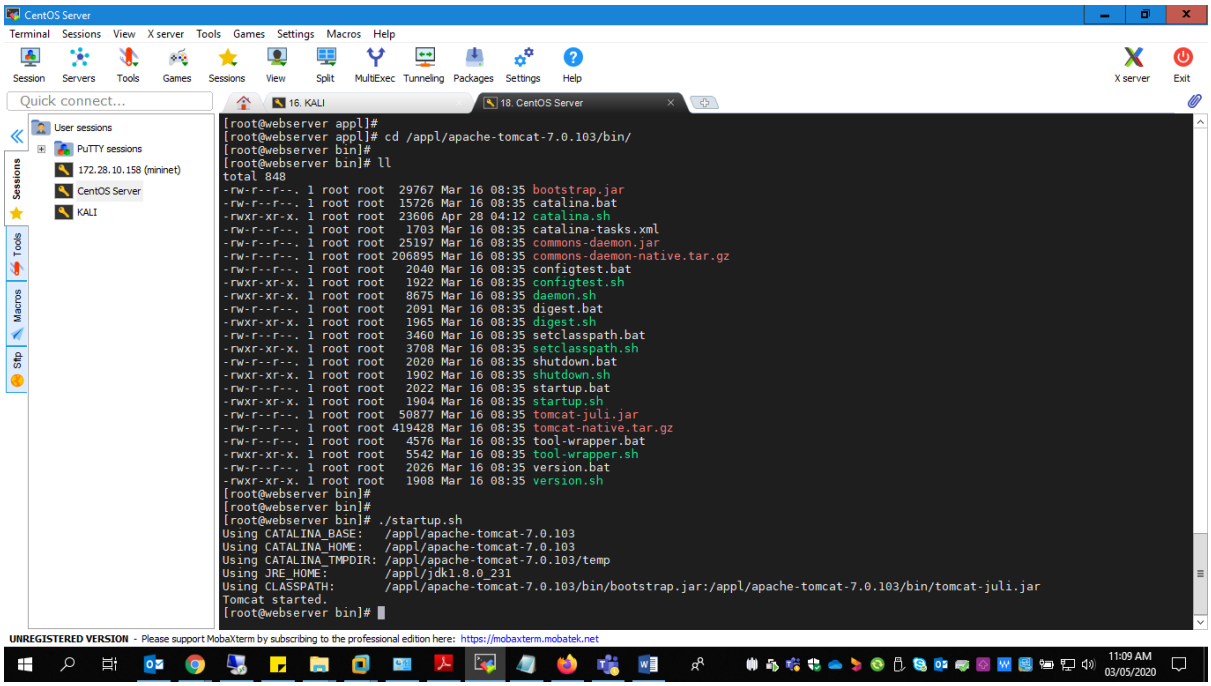
- Apache service installation.

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.



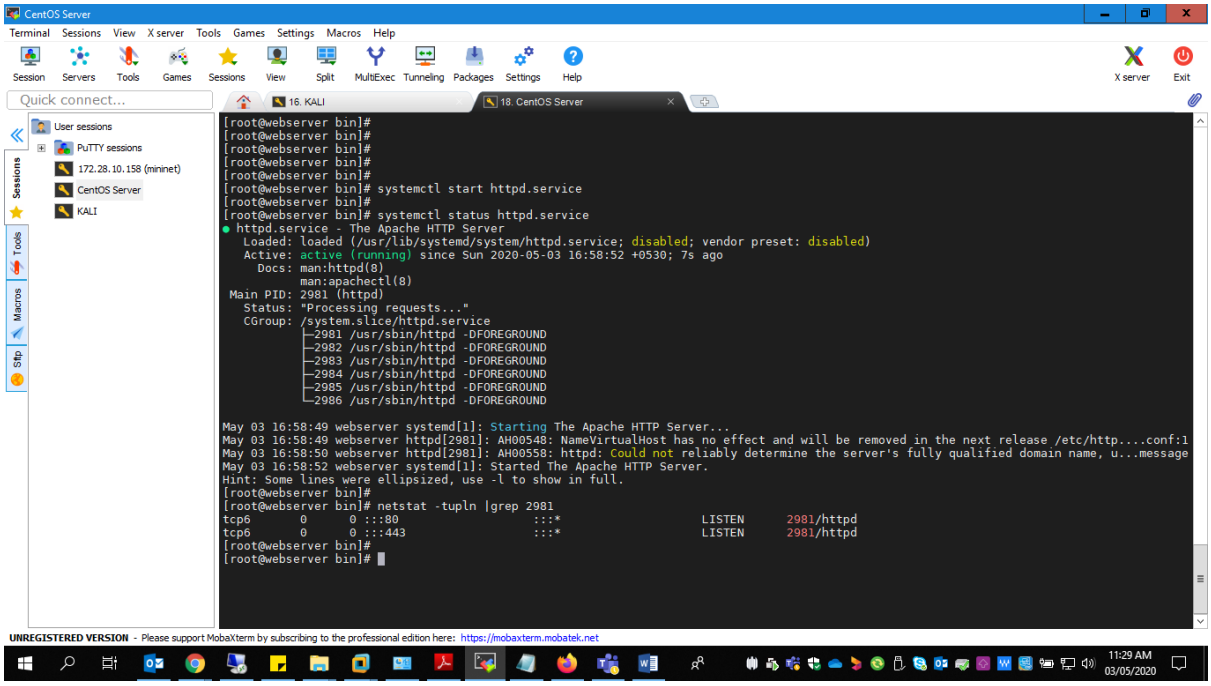
- HTTP service installation.

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.

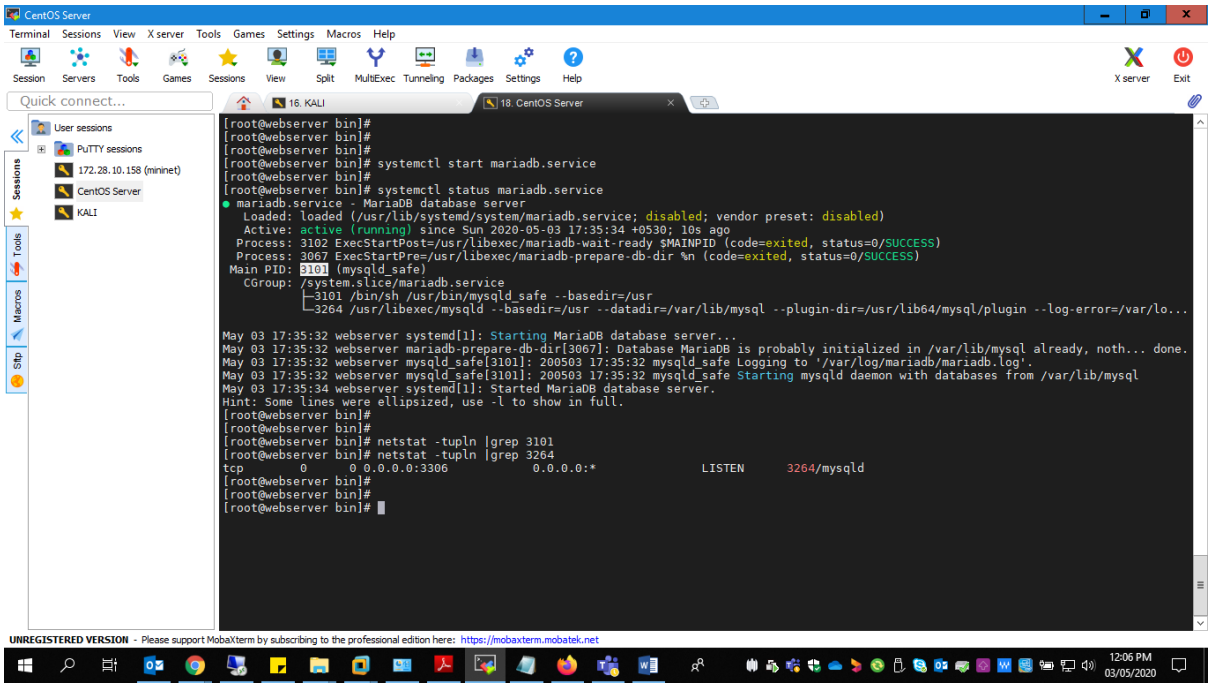


- Mariadb service installation.

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,



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"

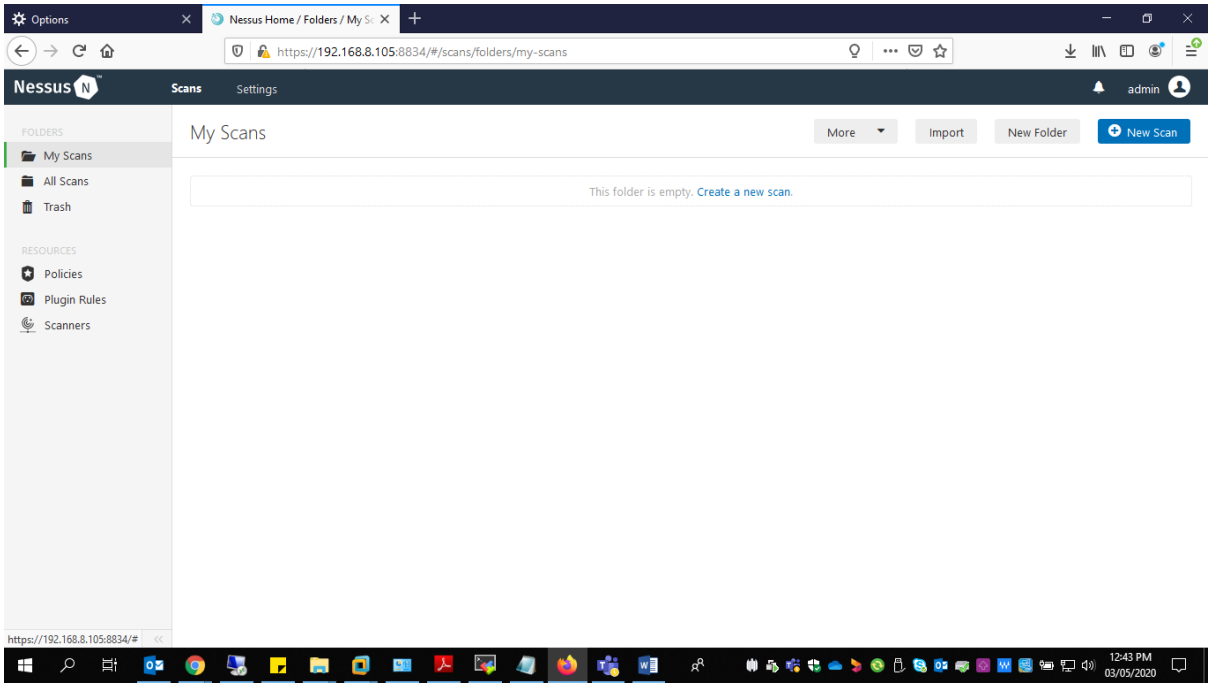
After created user need to restart the Nessus service using below commands.

"/etc/init.d/nessusd stop"

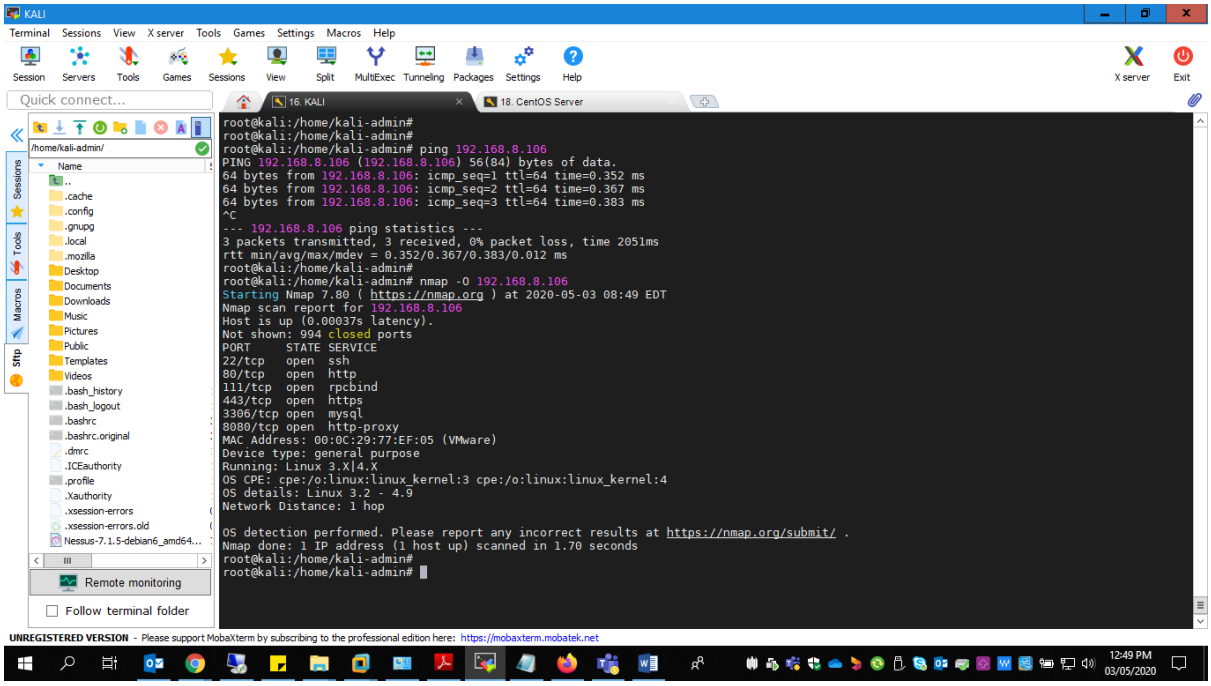
"/etc/init.d/nessusd start"

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.

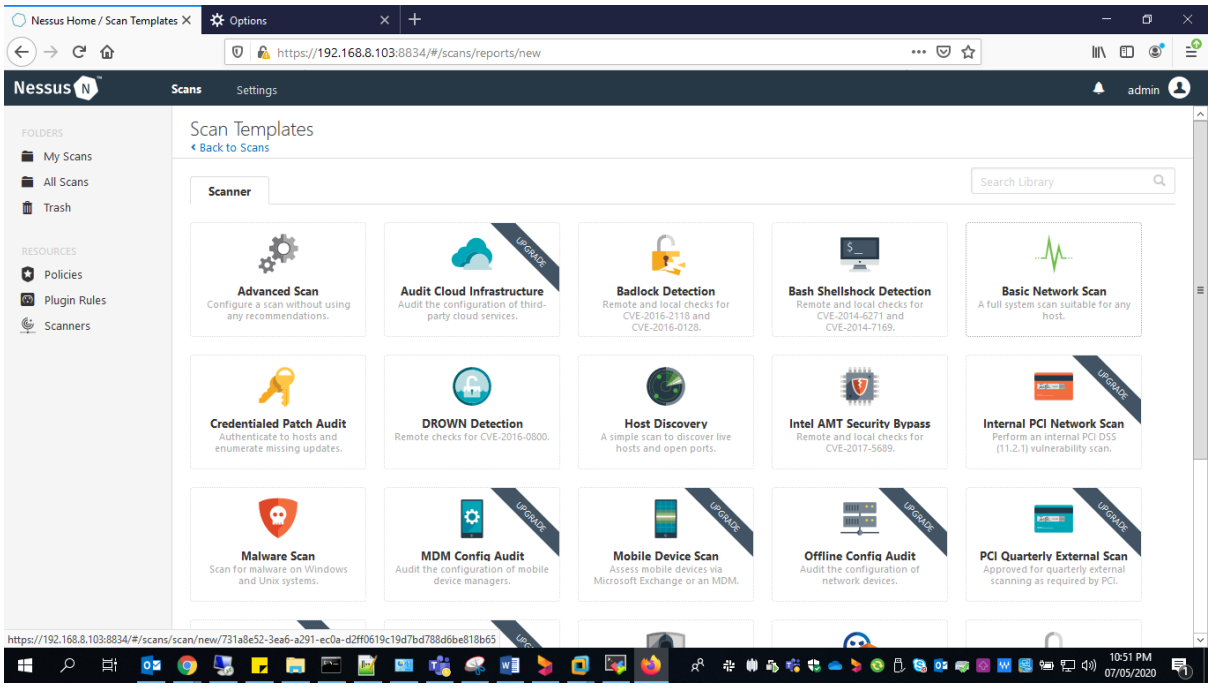
https://< $host_IP >:8834



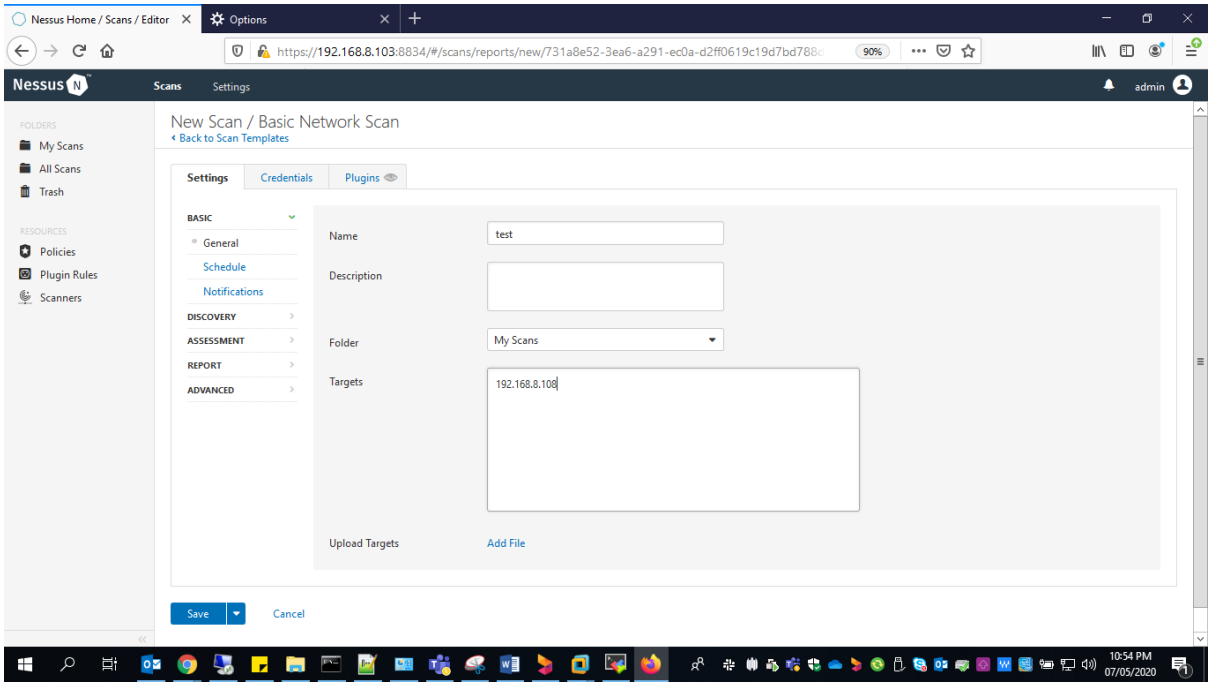
Before start vulnerability scan we need to verify connectivity between our source and target hosts using **ping** command. Also as below we can use **nmap** commands to get more information about remote server.



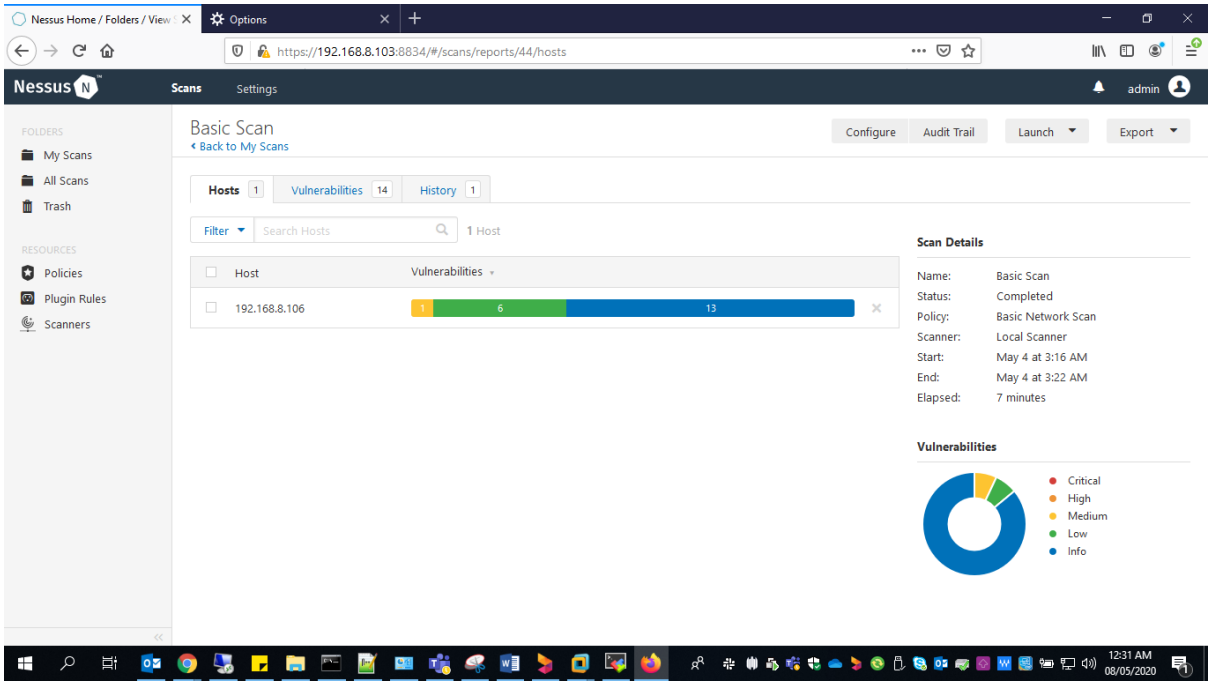
To create new scan, need to click **"New Scan"** in my scan tab. Then we want to select template for scan. There is different type of templates are available in Nessus as below in by default. We are going to use **"Basic Network Scan"** template for our task.



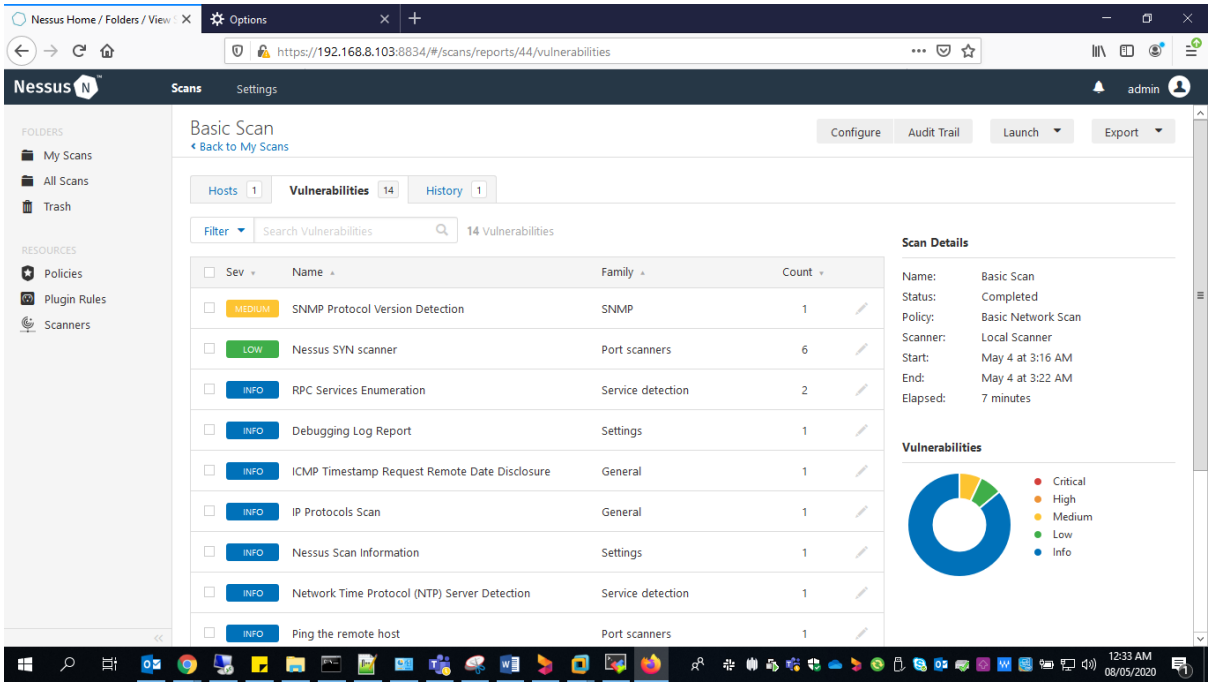
In configuration tab we need to define name for scan and target host IP for targets option. Also we can change port scan types, vulnerability scan types, report options and timeouts for our scan. After complete configuration click **"Save"** button and scan job will create.

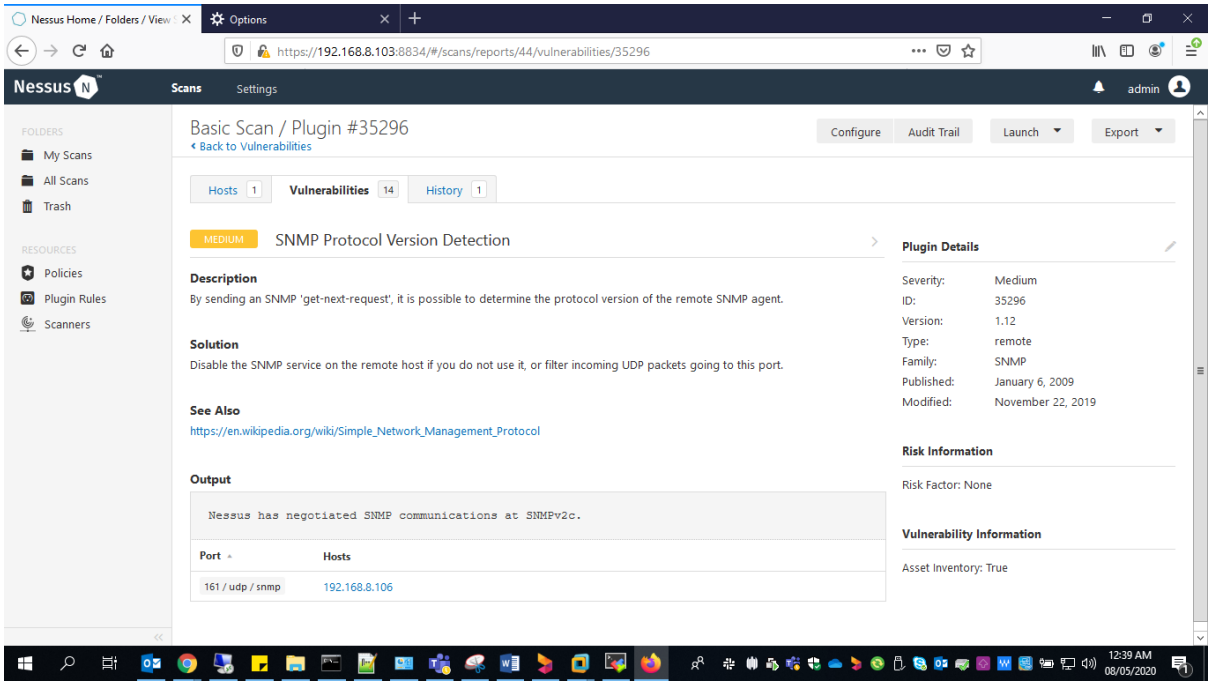


After created need to click **"Launch"** option to start scan. When scan is start it will take about 5 – 10 min time to complete that task. That time may be depending on configurations which are done in scan configuration step. After complete scan we can view vulnerability report using web user interface 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.