

Workshop 1 : Preparation of the working environment and analysis of vulnerabilities

Goals

- Download and install Kali Linux on your PC.
- Install and download Nessus Tenable.
- Use some network scanning tools.
- Understand the procedures for identifying and remediating vulnerabilities.

Part 1: Preparing the environment

- ✓ 1. ~~Download and install Vmware~~
- ✓ 2. ~~Download and install Kali Linux machine~~
- ✓ 3. ~~Download and install Nessus Tenable~~
- ✓ 4. ~~Download and start the Metasploitable2 VM~~

Part 2: Nmap Scan

Nmap is an open source port scanner. It detects open ports, services hosted and information about the operating system of a target computer.

1. Run a quick machine scan. Use the "Ifconfig" command to get the IP address and network mask.

```
amira@kali: ~/Desktop
File Actions Edit View Help
(amira@kali)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.153.128 netmask 255.255.255.0 broadcast 192.168.153.255
    inet6 fe80::20c:29ff:fe4e:b24e prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:fc:f9:6f txqueuelen 1000 (Ethernet)
    RX packets 206 bytes 16648 (16.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40 bytes 4612 (4.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(amira@kali)-[~/Desktop]
$
```

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4e:b2:4e
          inet addr:192.168.153.129  Bcast:192.168.153.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4e:b24e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:88 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7077 (6.9 KB)  TX bytes:7808 (7.6 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:135 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40109 (39.1 KB)  TX bytes:40109 (39.1 KB)

msfadmin@metasploitable:~$ _
```

2. Identify the operating systems of a target machine.

3. Scan all ports of a target machine.

```
amira@kali: ~/Desktop
File Actions Edit View Help

(amira@kali)-[~/Desktop]
$ nmap 192.168.153.129
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-05 05:12 CDT
Nmap scan report for 192.168.153.129
Host is up (0.0044s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

(amira@kali)-[~/Desktop]
```

4. Check the status of ports 22 and 443 on network machines.

```
(amira@kali)-[~/Desktop]
$ sudo nmap -p 22,443 192.168.153.129
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-05 05:14 CDT
Nmap scan report for 192.168.153.129
Host is up (0.00049s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp    closed https
MAC Address: 00:0C:29:4E:B2:4E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Part 3: Nessus Vulnerability Scanner on Kali Linux

1.Download the package and confirm that it is locally available for installation.

```
(amira@kali)-[~/Desktop]
$ file Nessus-10.7.2-debian10_amd64.deb
Nessus-10.7.2-debian10_amd64.deb: Debian binary package (format 2.0), with control.tar.gz, data compression gz
```

```
(amira@kali)-[~/Desktop]
$ ls
Metasploitable2-Linux      Nessus-10.7.2-debian10_amd64.deb
Nessus-10.7.2-debian10_amd64 metasploitable-linux-2.0.0.zip
```

2.Install Nessus Vulnerability scanner on Kali Linux the command below:

```
cd /home/kali/Downloads/
```

```
sudo dpkg -i Nessus-10.3.0-debian9_amd64.deb
```

```
amira@kali: ~/Desktop
File Actions Edit View Help
(amira@kali)-[~/Desktop]
$ sudo dpkg -i Nessus-10.7.2-debian10_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 398606 files and directories currently installed.)
Preparing to unpack Nessus-10.7.2-debian10_amd64.deb ...
Unpacking nessus (10.7.2) ...
Setting up nessus (10.7.2) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
```

3.Start the service required to run Nessus vulnerability scanner.

```
(amira@kali)-[~/Desktop]
$ systemctl start nessusd.service
(amira@kali)-[~/Desktop]
$
```

4.Confirm that nessusd is started and running

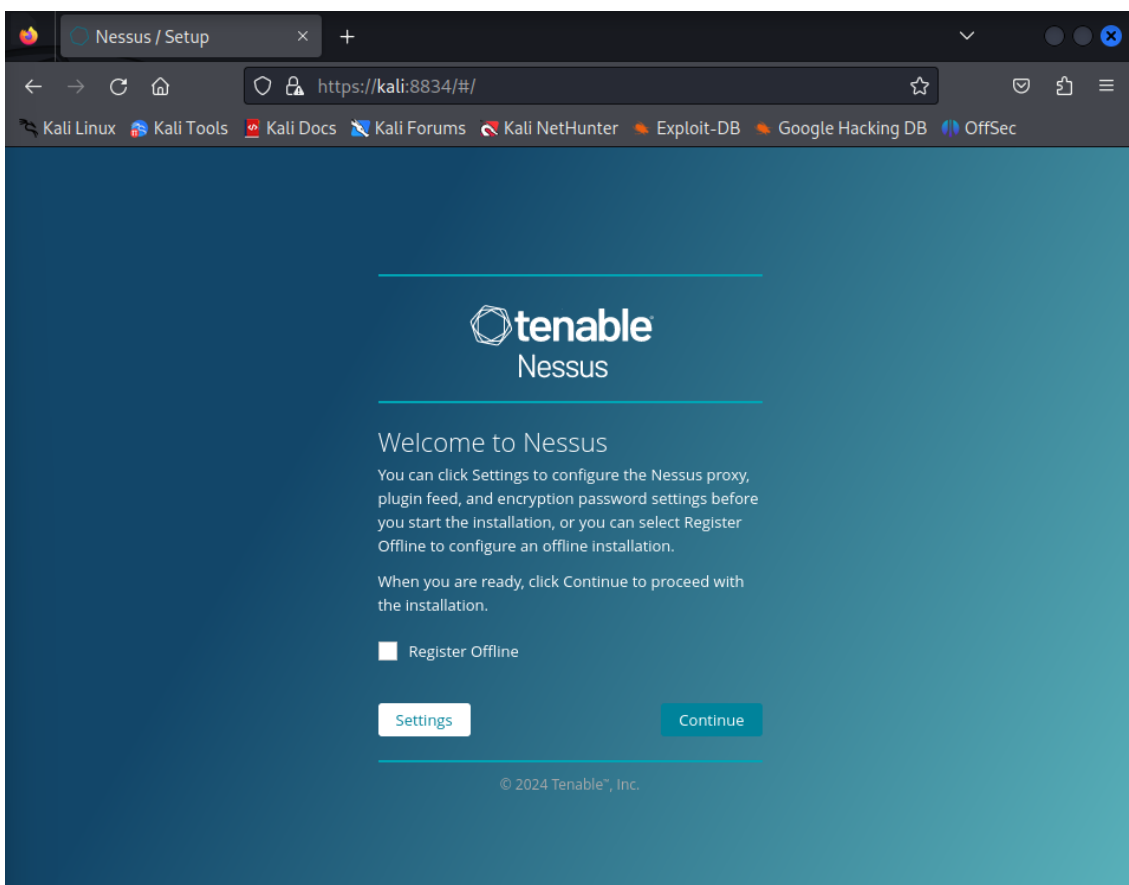
```
(amira@kali)-[~/Desktop]
$ systemctl start nessusd.service

(amira@kali)-[~/Desktop]
$ systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Fri 2024-04-05 05:25:31 CDT; 1min 50s ago
     Main PID: 24428 (nessus-service)
        Tasks: 14 (limit: 9390)
       Memory: 139.2M
          CPU: 45.095s
      CGroup: /system.slice/nessusd.service
              └─24428 /opt/nessus/sbin/nessus-service -q
                 └─24432 nessusd -q

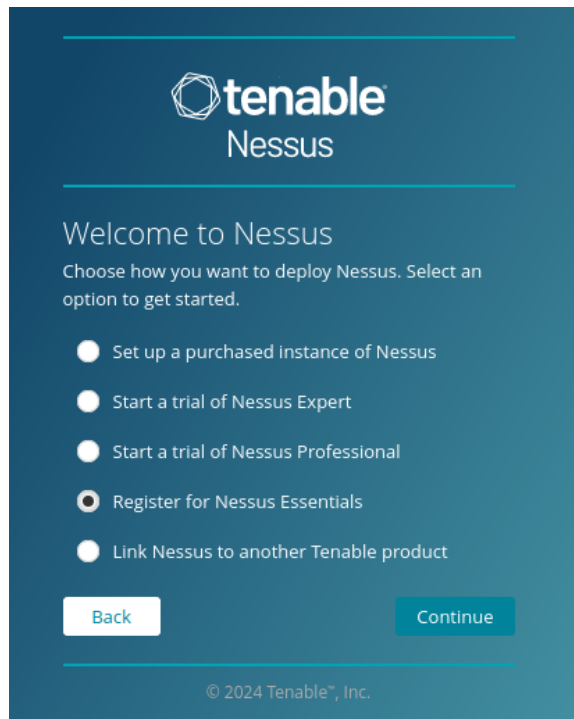
Apr 05 05:25:31 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Apr 05 05:25:32 kali nessus-service[24432]: Cached 0 plugin libs in 0msec
Apr 05 05:25:32 kali nessus-service[24432]: Cached 0 plugin libs in 0msec
```

5. Visit your Nessus web interface on your server IP address, hostname port 8834 to complete Nessus installation and activation.

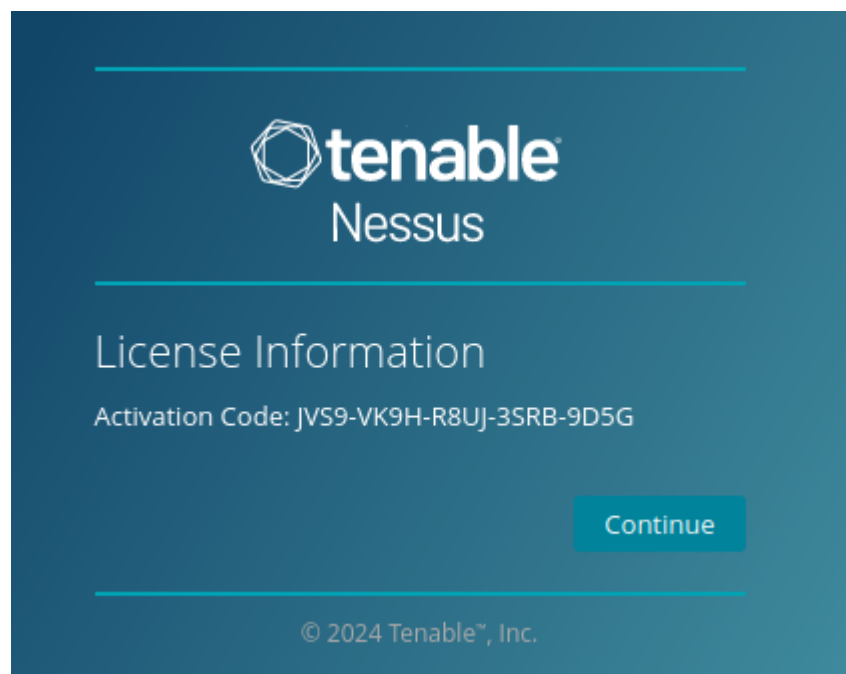
<https://kali:8834/>



6. Activate product: Nessus Essentials license

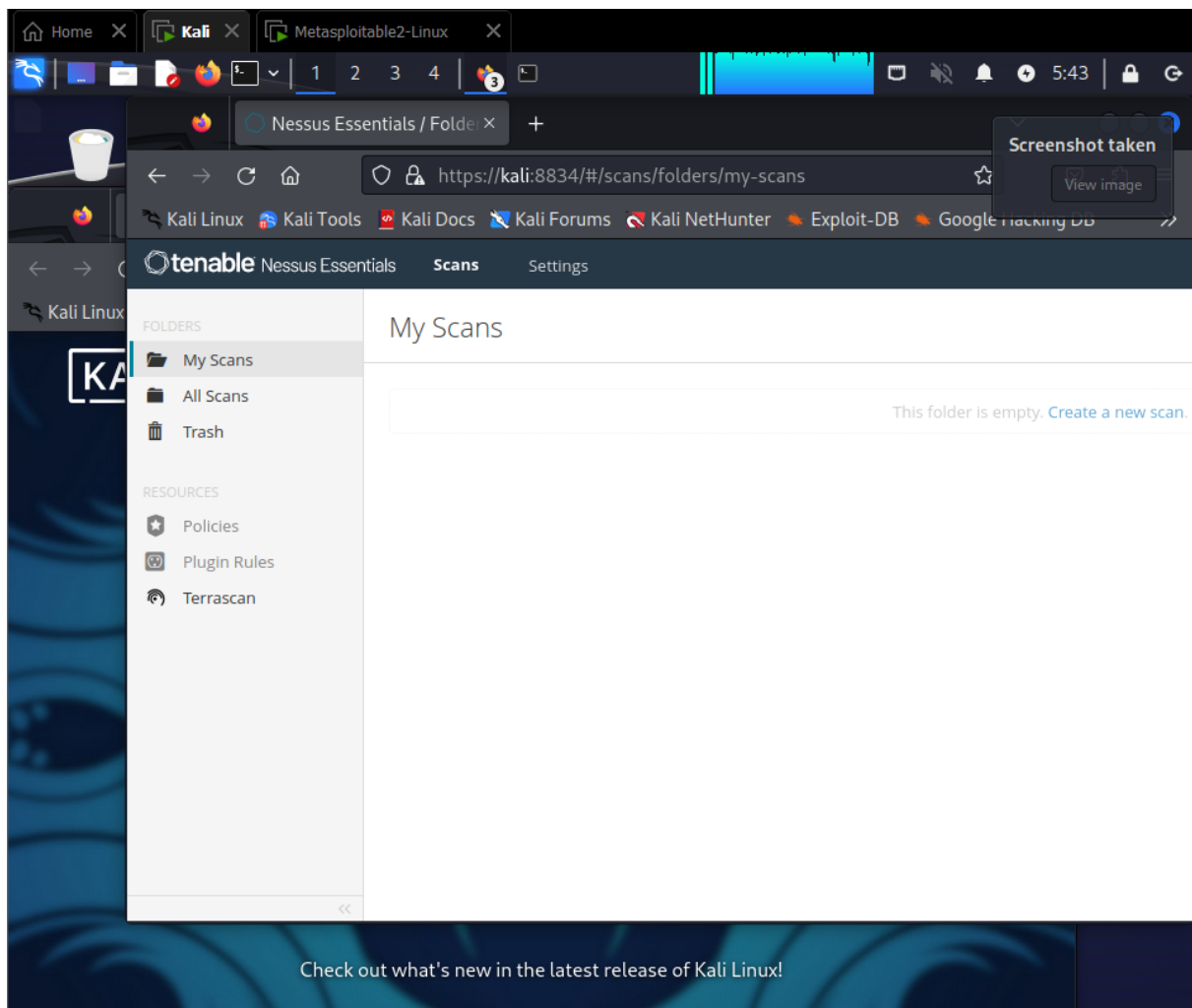


7. Register Nessus now by entering the activation code received by email.
JVS9-VK9H-R8UJ-3SRB-9D5G



8. Create a Nessus administrator account

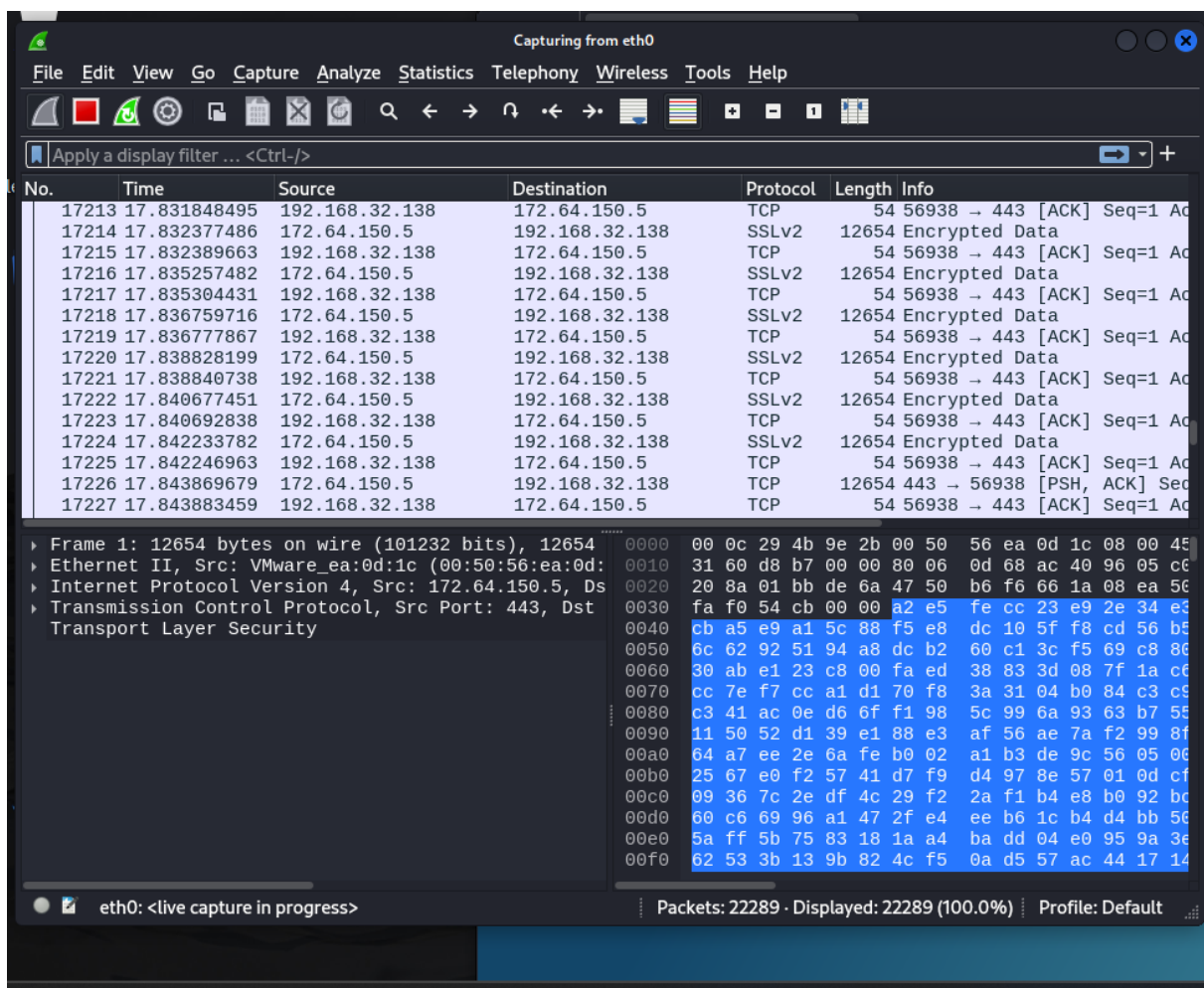
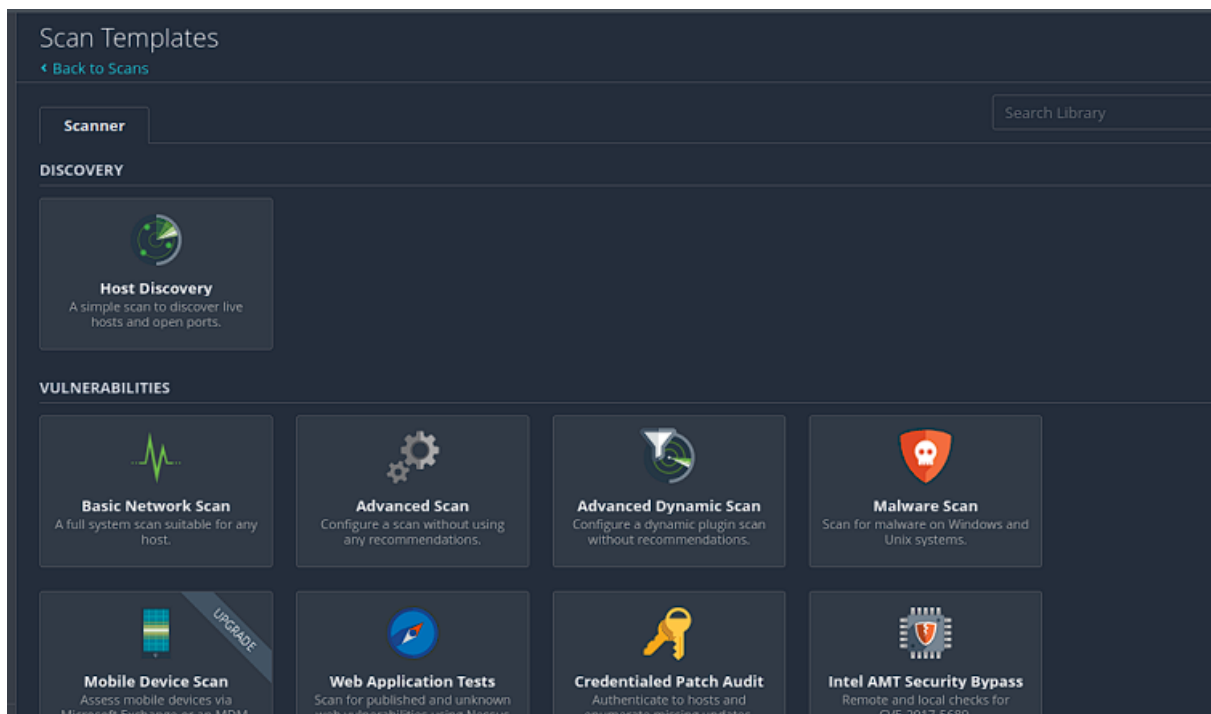
9.The default Nessus page when logging in should look like the one below:



Part 4: Run a Nessus Vulnerability Scan

To create an agent analysis:

1. From the top navigation bar, choose Scans.
2. Choose the New scan.
3. Click on the scan template you want to use.
4. Configure scan settings.
5. Scan immediately: Nessus saves and starts the scan



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
29838	423.397674136	192.168.32.139	192.168.32.1	HTTP	536	HTTP/1.1 302 Found
29839	423.412969500	192.168.32.1	192.168.32.139	HTTP	638	GET /dwa/login.php HTTP/1.1
29842	423.461001960	192.168.32.139	192.168.32.1	HTTP	68	HTTP/1.1 200 OK (text/html)
29844	423.547470387	192.168.32.1	192.168.32.139	HTTP	506	GET /dwa/dwa/css/login.css HTTP/1.1
29846	423.550519684	192.168.32.1	192.168.32.139	HTTP	560	GET /dwa/dwa/images/login_logo.png HTTP/1.1
29848	423.552175084	192.168.32.139	192.168.32.1	HTTP	957	HTTP/1.1 200 OK (text/css)
29861	423.558922570	192.168.32.139	192.168.32.1	HTTP	89	HTTP/1.1 200 OK (PNG)
29953	512.060607010	192.168.32.1	192.168.32.139	HTTP	610	POST /dwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
29955	512.921402105	192.168.32.139	192.168.32.1	HTTP	446	HTTP/1.1 302 Found
29956	512.935858883	192.168.32.1	192.168.32.139	HTTP	670	GET /dwa/index.php HTTP/1.1
29961	512.969377449	192.168.32.139	192.168.32.1	HTTP	638	HTTP/1.1 200 OK (text/html)
29963	513.039506317	192.168.32.1	192.168.32.139	HTTP	505	GET /dwa/dwa/css/main.css HTTP/1.1
29964	513.042231708	192.168.32.1	192.168.32.139	HTTP	492	GET /dwa/dwa/js/dwaPage.js HTTP/1.1
29969	513.043456558	192.168.32.139	192.168.32.1	HTTP	1375	HTTP/1.1 200 OK (text/css)
29973	513.047564999	192.168.32.1	192.168.32.139	HTTP	554	GET /dwa/dwa/images/logo.png HTTP/1.1
29975	513.048151861	192.168.32.139	192.168.32.1	HTTP	1341	HTTP/1.1 200 OK (application/x-javascript)

Source Port: 56747
Destination Port: 80
[Stream index: 17]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 761]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 1335063867
[Next Sequence Number: 762 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment Number (raw): 3404908353
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 510
[calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 8xb70e [unverified]
[Checksum 02:0000 Unverified]

0030 02 01 b7 0e 00 00 50 4f 53 54 20 2f 64 76 77 61 ... PO ST /dwa
0040 2f 6c 0f 67 09 6e 2e 70 68 70 20 48 54 54 50 2f ... /login.p hp HTTP/
0050 31 2e 31 0d 0a 4b 0f 73 74 3a 20 31 39 32 2e 31 ... 1.1. Host: 192.1
0060 36 38 2e 33 32 2e 31 33 39 0d 0a 43 0f 6e 6e 65 ... 68.32.13 9 Conne
0070 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 ... ction: k eep-aliv
0080 65 0d 0a 43 0f 6e 74 65 6e 74 2d 4c 65 6e 67 74 ... e Conte nt-lengt
0090 68 3a 20 34 0d 0a 43 61 63 68 65 2d 43 6f 6e ... h: 44. C ache-Con
00a0 74 72 6f 6e 3a 20 6d 61 78 2d 61 67 65 3d 30 0d ... trol: ma x-age=0
00b0 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 ... Upgrade -Insecur
00c0 72 69 67 69 6e 3a 20 68 74 74 70 3a 2f 31 39 ... e Request: 1.1.0
00d0 32 2e 31 36 38 2e 33 32 2e 31 33 39 0d 0a 43 6f ... rgin: h ttp://19
00e0 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 78 70 6c ... 2.168.32 .139. Co
00f0 69 63 61 74 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f ... ntent-Ty pe: appl
0100 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 55 ... ication/ x-ww-fo
0110 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c ... rm-urle n coded=U
0120 ... ser-Agen t: Mozil

Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (tcp.checksum, 2 byte(s))

Packets: 30090 · Displayed: 30 (0.1%)

Profile: Default