

## Scanning with Masscan, Nmap

Scanning with tools MASSCAN and NESSUS tool

**Masscan is port scanner and built to use to scan internet very fast**

<https://github.com/robertdavidgraham/masscan>

Masscan: Open terminal and Type the commands

>> **masscan -p1-65535 192.168.182.129** or (if scanner will take more time stop and run this command)

>> **masscan -p1-65535 --rate 1000 192.168.182.129** (this will scan faster, limited no ports) and another terminal setup Nmap

>> **nmap -T4 -p- 192.168.182 129** or also run specified port know that is open

```
>> nmap -T4 -p 22,80,111,139,443,32768 -A 192.168.182.129
```

## RESULTS with MASSCAN:

```
root@kali:/home/kali# masscan -p1-65535 --rate 1000 192.168.182.129
Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2020-03-27 06:36:06 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 22/tcp on 192.168.182.129 ←
Discovered open port 80/tcp on 192.168.182.129 ←
Discovered open port 32768/tcp on 192.168.182.129 ←
Discovered open port 111/tcp on 192.168.182.129 ←
Discovered open port 139/tcp on 192.168.182.129 ←
Discovered open port 443/tcp on 192.168.182.129 ←
All the port is open
```

RESULTS WITH NMAP:

```
root@kali:/home/kali# nmap -T4 -p- 192.168.182.129
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-27 02:35 EDT
Nmap scan report for 192.168.182.129
Host is up (0.0022s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
32768/tcp open  filenet-tms
MAC Address: 00:0C:29:54:B6:56 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.22 seconds
```

If you are a member of the general public:  
All the port is open to connect

```

root@kali:/home/kali# nmap -T4 -p 22,80,111,139,443,32768 -A 192.168.182.129 | MetHunter | Offense Security
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-27 02:51 EDT
Nmap scan report for 192.168.182.129
Host is up (0.00073s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
|   1024 b8:74:6c:db:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
| sshv1: Server supports SSHv1
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
| http-methods:
|_ Potentially risky methods: TRACE
| http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-title: 400 Bad Request
| ssl-date: 2020-03-25T12:34:42+00:00; -1d18h18m30s from scanner time.
| sslv2:
|_ SSLv2 supported
| ciphers:
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC4_64_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
32768/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:54:B6:56 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X and information on Red Hat Linux, please visit the Red Hat, Inc. website
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_clock-skew: -1d18h18m30s
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT      ADDRESS
1  0.73 ms  192.168.182.129

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.

```

## Scanning with Metasploit

Command with required run in kali terminal:

```
>> msfconsole
```

```
>> search portscan
```

```
msf5 > search portscan
Matching Modules
=====
If you are a member of the general public:
#  Name                                     Disclosure Date   Rank   Check  Description
--- 
0 auxiliary/scanner/http/wordpress_pingback_access      normal    No    Wordpress Pingback Locator
1 auxiliary/scanner/natpmp/natpmp_portscan            normal    No    NAT-PMP External Port Scanner
2 auxiliary/scanner/portscan/ack                        normal    No    TCP ACK Firewall Scanner
3 auxiliary/scanner/portscan/ftpbounce                normal    No    FTP Bounce Port Scanner
4 auxiliary/scanner/portscan/syn                      normal    No    TCP SYN Port Scanner
5 auxiliary/scanner/portscan/tcp                      normal    No    TCP Port Scanner
6 auxiliary/scanner/portscan/xmas                    normal    No    TCP "XMas" Port Scanner
7 auxiliary/scanner/sap/sap_router_portscanner       normal    No    SAPRouter Port Scanner
```

```
>> use 4 or use auxiliary/scanner/portscan/syn
```

```
msf5 > use 4
msf5 auxiliary(scanner/portscan/syn) >
```

```
>> options # it will ask for requirements but it is already filled actually.
```

```
msf5 auxiliary(scanner/portscan/syn) > options
Module options (auxiliary/scanner/portscan/syn):
=====
Name      Current Setting  Required  Description
---- 
BATCHSIZE  256           yes        The number of hosts to scan per set
DELAY      0              yes        The delay between connections, per thread, in milliseconds
INTERFACE   no             The name of the interface
JITTER     0              yes        The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS      1-10000        yes        Ports to scan (e.g. 22-25,80,110-900)
RHOSTS     [REDACTED]      yes        The target address range or CIDR identifier
SNAPLEN    65535          yes        The number of bytes to capture
THREADS    1              yes        The number of concurrent threads
TIMEOUT    500            yes        The reply read timeout in milliseconds
```

```
>> set rhosts 192.168.182.129 (attacker machine ip address)
```

```
msf5 > set rhosts 192.168.182.129
rhosts => 192.168.182.129
```

```
>> set port 1-65535
```

```
msf5 > set port 1-65535
port => 1-65535
```

```
>> run #this will start the post scanning
```

```
msf5 auxiliary(scanner/portscan/syn) > run
```

```
[+] TCP OPEN 192.168.182.129:22 ←
[+] TCP OPEN 192.168.182.129:80 ← visit the Run
[+] TCP OPEN 192.168.182.129:111 ← Visit server /1
[+] TCP OPEN 192.168.182.129:139 ← Apache-Powered by
[+] TCP OPEN 192.168.182.129:443 ← Apache-Powered by
^C[*] Caught interrupt from the console ...
[*] Auxiliary module execution completed
```

```
>> set threads 100 (or we can set the threads)
```

```
>> run
```

```
msf5 auxiliary(scanner/portscan/syn) > set threads 100
threads ⇒ 100
msf5 auxiliary(scanner/portscan/syn) > run
```

```
You are free to use the image below on an Apache-powered Web server. Thanks for using Apache!
```

```
[+] TCP OPEN 192.168.182.129:22 ← Apache-Powered by APACHE
[+] TCP OPEN 192.168.182.129:80 ← Apache-Powered by Apache
[+] TCP OPEN 192.168.182.129:111 ← Apache-Powered by Apache
[+] TCP OPEN 192.168.182.129:139 ← Apache-Powered by Apache
[+] TCP OPEN 192.168.182.129:443 ← Apache-Powered by Apache
```

## Scanning with Nessus – Part 1

Nessus is called vulnerability scanner, if you do external assessment there is chances that you are use Nessus in the assessment, and kick off the scan,

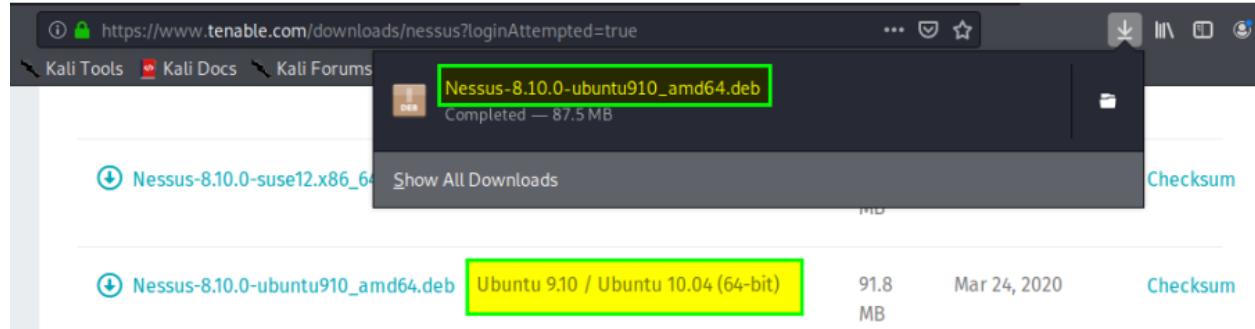
- Information gathering,
- Breach credential try to find juicy on the client

We can scan private ip address and 16 ip we can scan at one time.

---

### DOWLOAD NESSUS:

<https://www.tenable.com/downloads/nessus?loginAttempted=true> (Download 64 bit version debian file)



We can download the file in linux and run below command to install in machine.

```
>>dpkg -i Nessus-8.10.0-ubuntu910_amd64.deb
```

```
root@kali:/home/kali/Downloads# dpkg -i Nessus-8.10.0-ubuntu910_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 257678 files and directories currently installed.)
Preparing to unpack Nessus-8.10.0-ubuntu910_amd64.deb ...
Unpacking nessus (8.10.0) ...
Setting up nessus (8.10.0) ...
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (244-3) ...
```

#we can copy the /etc/init/.d.nessusd start and navigate to this URL

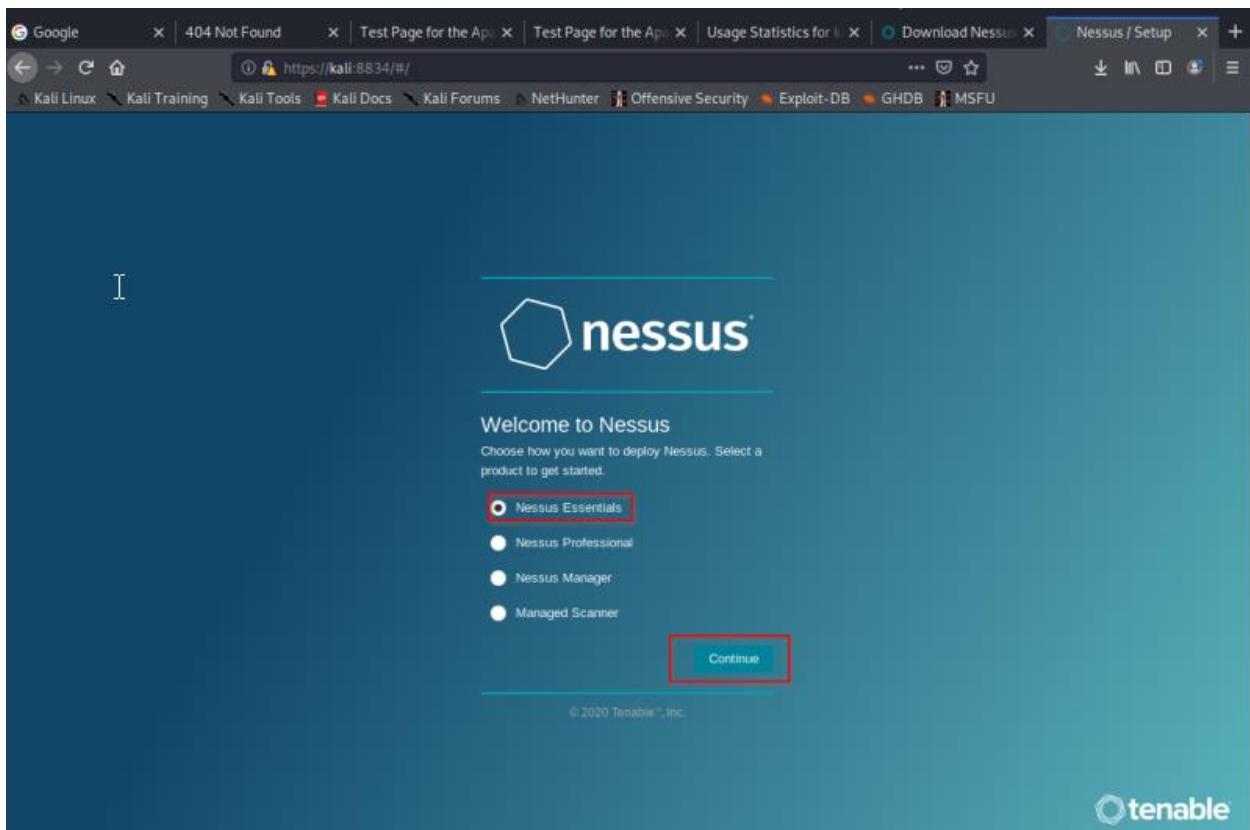
```
>> http://kali:8834/      (paste in the browser)
```

```
root@kali:/home/kali/Downloads# /etc/init.d/nessusd start
Starting Nessus : .
root@kali:/home/kali/Downloads# [Fri Mar 27 06:20:54 2020][20334.1][op=qdb_sync][name=services-udp.db][fd=7][map_sz=0][file_size=13084
9]: complete
[Fri Mar 27 06:20:54 2020][20334.1][op=qdb_sync][name=services-tcp.db][fd=6][map_sz=0][file_size=137898]: complete
[Fri Mar 27 06:20:54 2020][20334.1][op=_qdb_map][name=services-udp.db][fd=-1][map_sz=38575]: complete
[Fri Mar 27 06:20:54 2020][20334.1][op=_qdb_map][name=services-tcp.db][fd=-1][map_sz=40899]: complete
[Fri Mar 27 06:20:54 2020][20334.1][op=_qdb_map][name=services-tcp.db][fd=-1][map_sz=40899]: complete
[Fri Mar 27 06:20:54 2020][20334.1][op=qdb_sync][name=upgrades.db][fd=5][map_sz=0][file_size=20]: complete
[Fri Mar 27 06:20:54 2020][20334.1][op=qdb_sync][name=upgrades.db][fd=5][map_sz=0][file_size=55]: complete
[Fri Mar 27 06:20:55 2020][20334.1][op=qdb_sync][name=plugins-desc.db][fd=8][map_sz=0][file_size=20]: complete
[Fri Mar 27 06:20:55 2020][20334.1][op=qdb_sync][name=plugins-code.db][fd=7][map_sz=0][file_size=20]: complete
[Fri Mar 27 06:20:55 2020][20334.1][op=_qdb_map_lowmem][name=plugins-code.db.15853044552130473316][fd=7][map_sz=0][file_size=20]: comp
lete
[Fri Mar 27 06:20:55 2020][20334.1][op=_qdb_map_lowmem][name=plugins-desc.db.15853044551954417946][fd=8][map_sz=0][file_size=20]: comp
lete
```

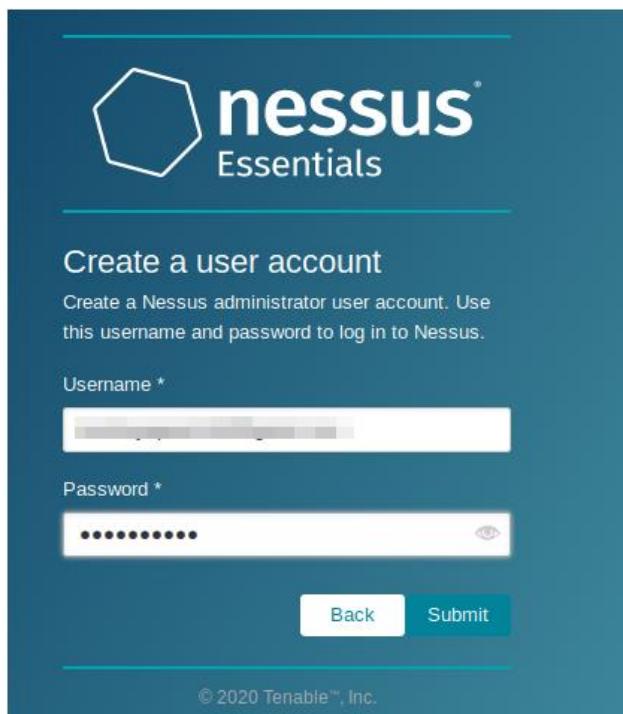
Now open browser, select below option, continue, and set username and last name and email

Enter activation code received on mail

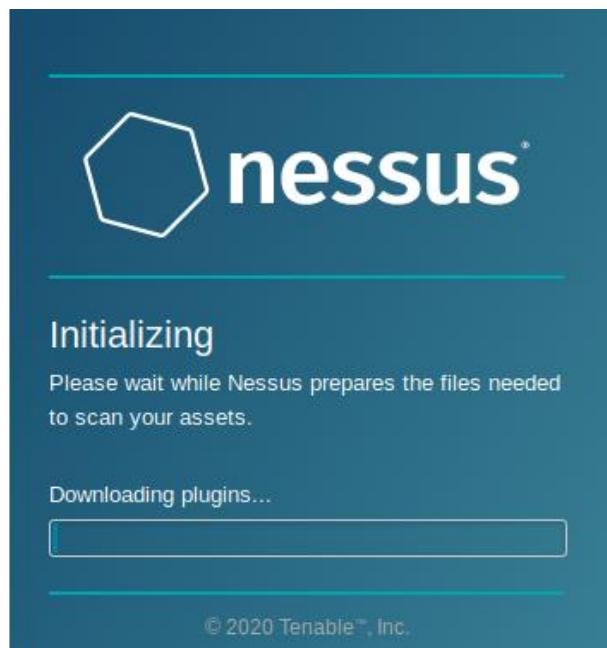
7C42-126F-2D18-FF2B-4CDE like this.



ENTER USERNAME AND PASSWORD – [email7@gmail.com](mailto:email7@gmail.com) , ab@15



This will take some time to install



We now open Nessus with login credentials click on cancel

This folder is empty. [Create a new scan](#).

Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

Close Submit

>> click on new scan on top right side of corner and click on basic network scan.

Now enter details and save all the details

New Scan / Basic Network Scan  
[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Kioptrix

Description: Kioptrix

Folder: My Scans

Targets: 192.168.182.129

>> Now go through schedule the scan weekly daily monthly we can also set this

>> We can also set notification from SMTP server.

>> go to discovery tab we have to select all port scanning

The screenshot shows the 'New Scan / Basic Network Scan' configuration page. At the top, there are three tabs: 'Settings' (selected), 'Credentials', and 'Plugins'. Below these are four main sections: 'BASIC', 'DISCOVERY' (highlighted with a yellow box), 'ASSESSMENT', and 'REPORT'. Under 'DISCOVERY', there is a 'Scan Type' dropdown menu with the following options: 'Port scan (common ports)', 'Port scan (common ports)' (disabled), 'Port scan (all ports)' (highlighted with a yellow box), and 'Custom'. A small note at the bottom right of the dropdown says 'This fact network discovery'.

>> We can go assessment tab and select scan for web vulnerabilities.

The screenshot shows the 'New Scan / Basic Network Scan' configuration page. The 'Assessment' tab is selected. The 'Scan Type' dropdown menu contains the following options: 'Default' (disabled), 'Default' (disabled), 'Scan for known web vulnerabilities' (highlighted with a red box), 'Scan for all web vulnerabilities (quick)', 'Scan for all web vulnerabilities (complex)', and 'Custom'. At the bottom of the dropdown, there is a link 'Disable web application scanning'.

>> In Report and Advanced tab its default setting we can apply and now we can run the scan.

The screenshot shows the 'New Scan / Basic Network Scan' configuration page. At the bottom right, there is a large red-bordered 'Run Scan' button. To its left, there are two status indicators: 'On Demand' and 'N/A'. There are also 'Next' and 'X' buttons.

## Scanning with Nessus part -2

The screenshot shows the Nessus interface for a scan named 'Kioptrix'. The top navigation bar includes 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export' buttons. Below the navigation is a header with tabs for 'Hosts' (1), 'Vulnerabilities' (43), 'Remediations' (3), and 'History' (1). A search bar labeled 'Search Hosts' shows '1 Host'. The main content area displays a table for a host at 192.168.57.134, showing 38 vulnerabilities across severity levels (5 Critical, 36 High, 59 Medium, 10 Low, 67 Info). To the right is a 'Scan Details' panel with the following information:

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	November 25 at 11:53 PM
End:	November 25 at 11:59 PM
Elapsed:	6 minutes

Below this is a 'Vulnerabilities' section featuring a donut chart illustrating the distribution of severity levels.

Now we can check the scan report via severity: we can choose disable groups. Check very critical scan item.

The screenshot shows the Nessus interface displaying a list of 43 vulnerabilities. The columns include 'Sev', 'Name', 'Family', 'Count', and 'Score'. A context menu is open over the fourth row, listing 'Disable Groups' and 'Show Snoozed'.

Sev	Name	Family	Count	Score
MIXED	OpenSSL (Multiple Issues)	Web Servers	48	
MIXED	Openbsd Openssh (Multiple Issues)	Gain a shell remotely	5	
MIXED	Apache HTTP Server (Multiple Issues)	Web Servers	16	
MIXED	Openbsd Openssh (Multiple Issues)	Misc.	15	

However, we cannot add output: supported version information because it is our side to make them do work.

Hosts 1 Vulnerabilities 122 Remediations 3 History 1

**CRITICAL** OpenSSL Unsupported

**Description**

According to its banner, the remote web server is running a version of OpenSSL that is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

**Solution**

Upgrade to a version of OpenSSL that is currently supported.

**See Also**

<https://www.openssl.org/policies/releasestrat.html>  
<http://www.nessus.org/u?4d55548d>

**Output**

Installed version : 0.9.6b
Supported versions : 1.1.0 / 1.0.2
EOC URL : <a href="https://www.openssl.org/policies/releasestrat.html">https://www.openssl.org/policies/releasestrat.html</a>

Port	Hosts
443 / tcp / www	192.168.57.134
80 / tcp / www	192.168.57.134

Installed version 0.9.6b

Supported version 1.1.0 / 1.0.2

Configure Audit Trail Launch Report Export

Nessus Nessus DB

We can download Nessus file and convert them into Excel file with online convertor