Vulnerability Analysis Lab (Nessus & Nmap)

Created by	Sayf Eddine Ben Salah

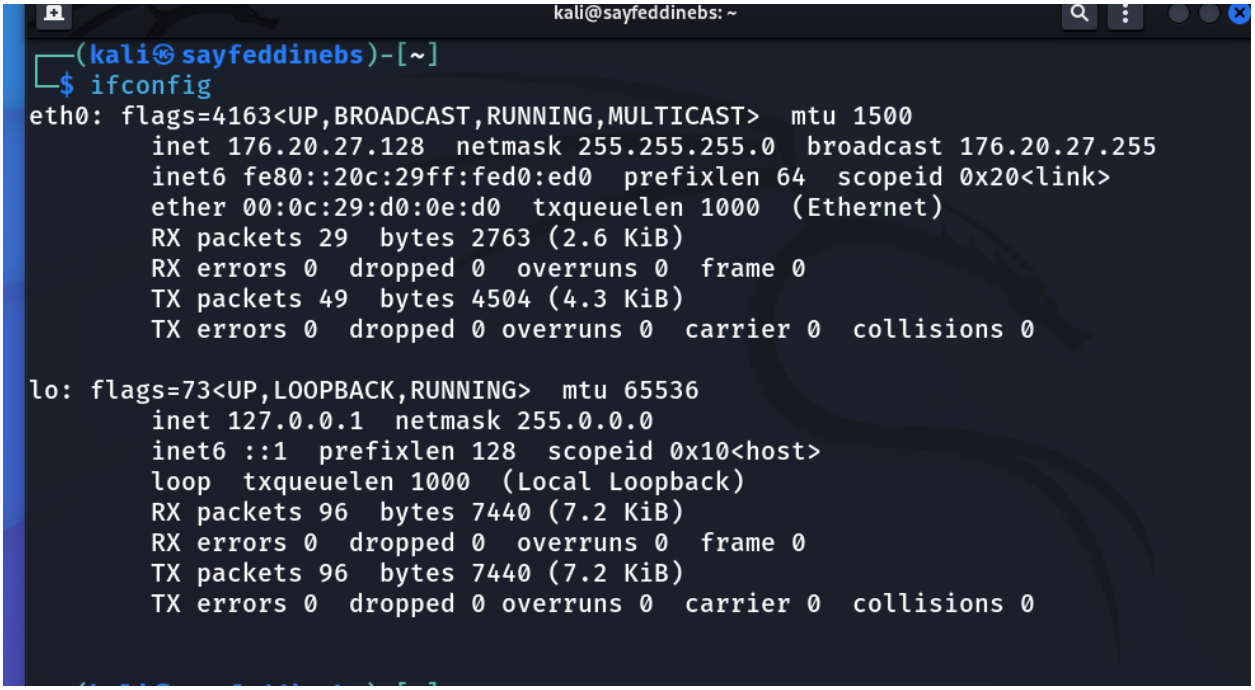
Part 1 : Nmap Scan

> 💡 Nmap is an open source tool that can scan open ports , services and os details on a targeted computer.

> 🎯 The first objective is to check the devices connected to LAN network using the command `nmap -sn <network>/<subnet_mask>` the argument `-sn` means ping scan so the nmap can know what machines are reachable

As u can see before using the nmap command . I needed to determine my LAN network address to do that I used the command `ifconfig` and it’s written in front of the network adapter “eth0”

As you can see what’s in front of `inet` is my LAN address and what in front of `netmask` the my subnet mask.



```
┌──(kali㉿sayfeddinebs)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 176.20.27.128  netmask 255.255.255.0  broadcast 176.20.27.255
        inet6 fe80::20c:29ff:fed0:ed0  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d0:0e:d0  txqueuelen 1000  (Ethernet)
        RX packets 29  bytes 2763 (2.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 49  bytes 4504 (4.3 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 96  bytes 7440 (7.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 96  bytes 7440 (7.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Now I can execute the `nmap -sn 176.20.27.0/255.255.255.0` command

Problems Encountered

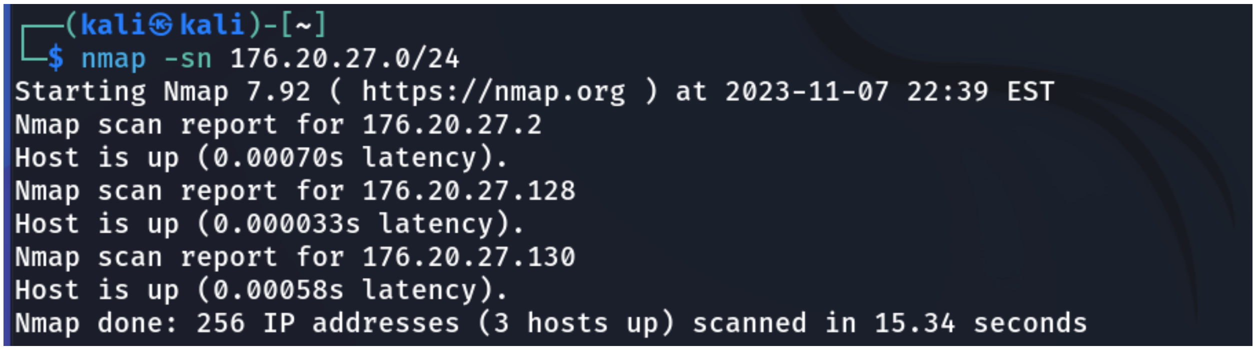
I got an error that’s about the target expression in the nmap command I executed. It seems like I wrote the netmask the wrong way

Solutions

I had to rewrite the command the right way with the netmask written the right way so after I did my research I found that the right command is written the following way : `nmap -sn 176.20.27.0/24`

After executing the right command. I got the following output that’s indicates information about the network scan I did.

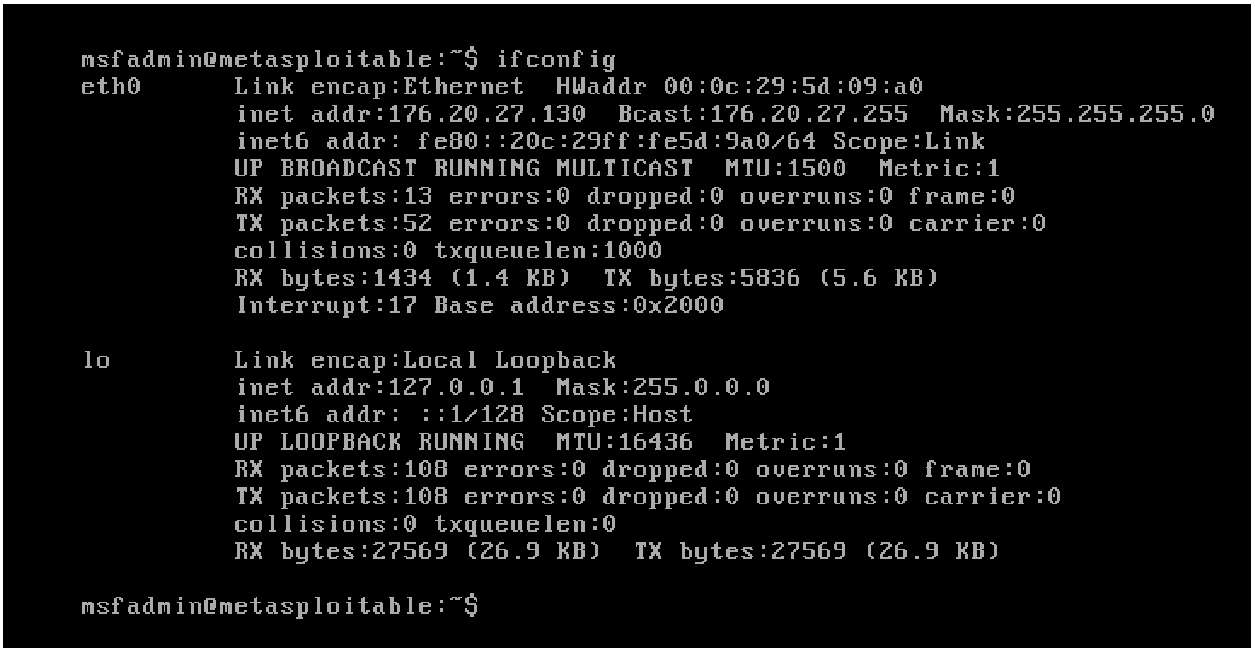
As you can see the final resuls of this nmap scan indicate that 256 IP addresses were scanned and 3 hosts are found up.



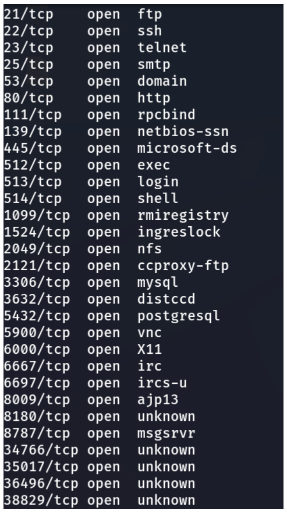
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 176.20.27.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-07 22:39 EST
Nmap scan report for 176.20.27.2
Host is up (0.00070s latency).
Nmap scan report for 176.20.27.128
Host is up (0.000033s latency).
Nmap scan report for 176.20.27.130
Host is up (0.00058s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 15.34 seconds
```

🎯 Now among those ip addresses. I’m going to pick the ip address of my target machine and I’m going to scan all of its ports using the command `nmap -p- <ip>` as the argument `-p-` means scan all ports

My target (metasploitable machine) has the following address : `176.20.27.130`



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:5d:09:a0
          inet addr:176.20.27.130  Bcast:176.20.27.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe5d:9a0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
          TX packets:52 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1434 (1.4 KB)  TX bytes:5836 (5.6 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:108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27569 (26.9 KB)  TX bytes:27569 (26.9 KB)

msfadmin@metasploitable:~$
```

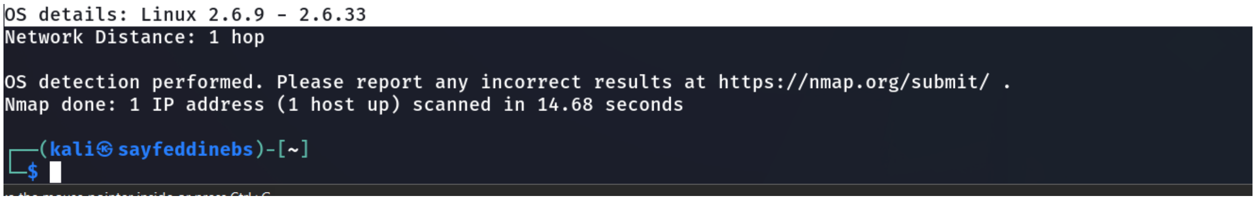


```
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
34766/tcp open  unknown
35017/tcp open  unknown
36496/tcp open  unknown
38829/tcp open  unknown
```

Now after executing the command `nmap -p- 172.20.27.130` to scan for all the open ports in my target machine. I found a lot of open ports. Here are the open ports I found.

🎯 My next objective in this lab , is to determine the OS of my target machine using the command `nmap -O <ip_target>`

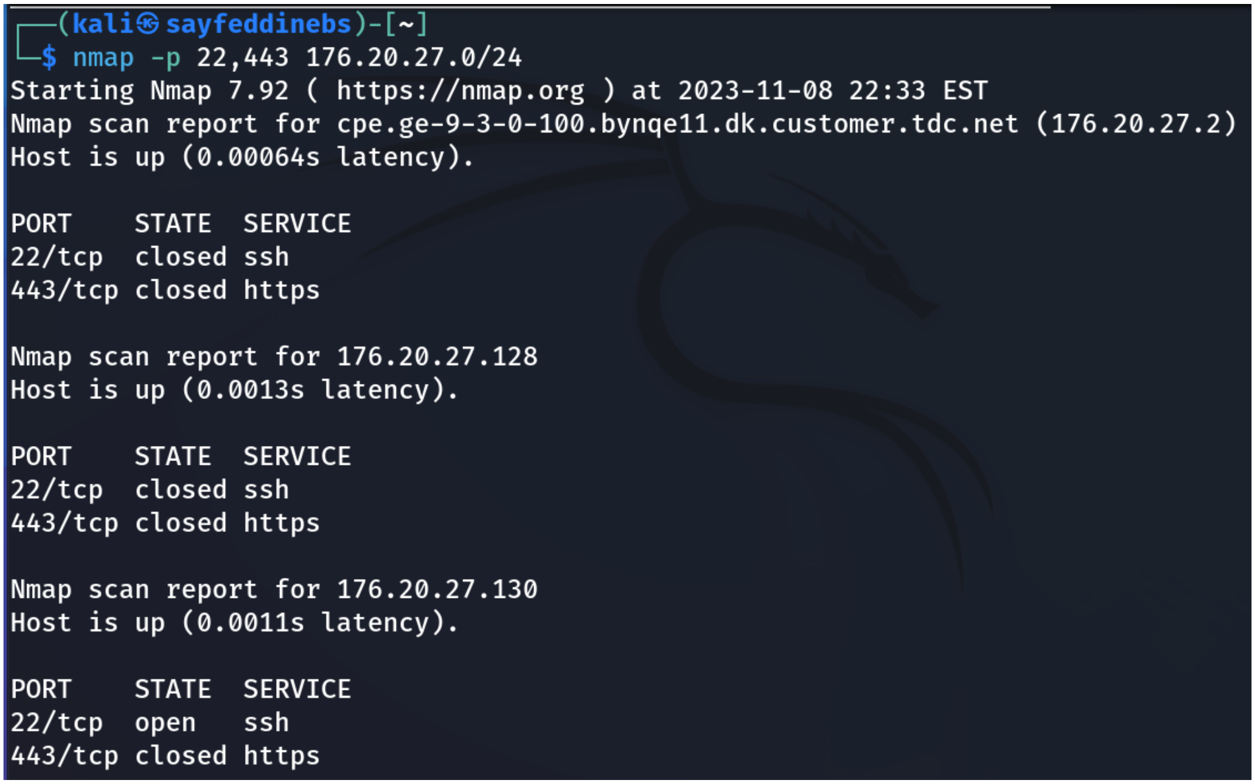
I executed the command nmap -O `176.20.27.130` and discovered that my target machine uses Linux 2.6.9 - 2.6.33



```
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds

┌──(kali㉿sayfeddinebs)-[~]
└─$ 
```

🎯 Now I’m going check the status of the ports 22 and 443 for the the machines in the network I will do that using the command `nmap -p <port_num> <ip_range>`

So I executed the command `nmap -p 22,443 176.20.27.0/24` and I got the following output :



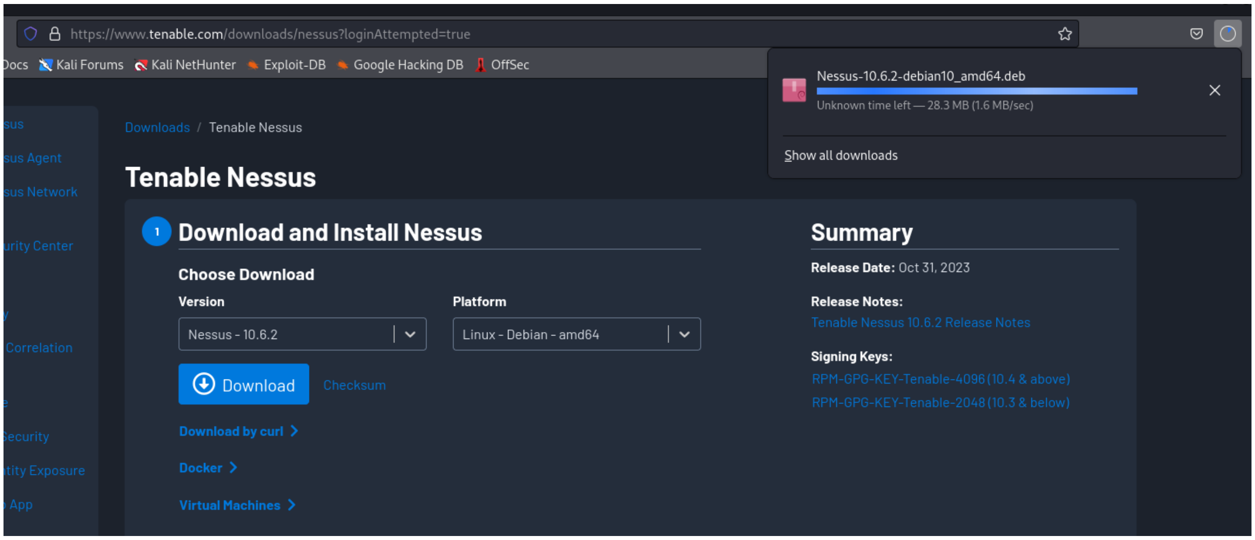
```
┌──(kali㉿sayfeddinebs)-[~]
└─$ nmap -p 22,443 176.20.27.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-08 22:33 EST
Nmap scan report for cpe.ge-9-3-0-100.bynqe11.dk.customer.tdc.net (176.20.27.2)
Host is up (0.00064s latency).

PORT    STATE  SERVICE
22/tcp  closed ssh
443/tcp closed https

Nmap scan report for 176.20.27.128
Host is up (0.0013s latency).

PORT    STATE  SERVICE
22/tcp  closed ssh
443/tcp closed https

Nmap scan report for 176.20.27.130
Host is up (0.0011s latency).

PORT    STATE  SERVICE
22/tcp  open   ssh
443/tcp closed https
```

The only open port was the metasploitable ssh port.

Part 2 : Nessus Vulnerability Scanner on Kali Linux

💡 Nessus is a vulnerability scanner developed by Tenable that helps you scan of vulnerabilities in your network , apps …

🎯 My first objective now is today download Nessus. So I went to the official website of Tenable and I downloaded it.



https://www.tenable.com/downloads/nessus?loginAttempted=true
Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Nessus-10.6.2-debian10_amd64.deb
Unknown time left — 28.3 MB (1.6 MB/sec)
Show all downloads
sus
sus Agent
sus Network
urity Center
Correlation
Security
tity Exposure
App
Downloads / Tenable Nessus

Tenable Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.6.2

Platform: Linux - Debian - amd64

Download
Checksum
Download by curl
Docker
Virtual Machines

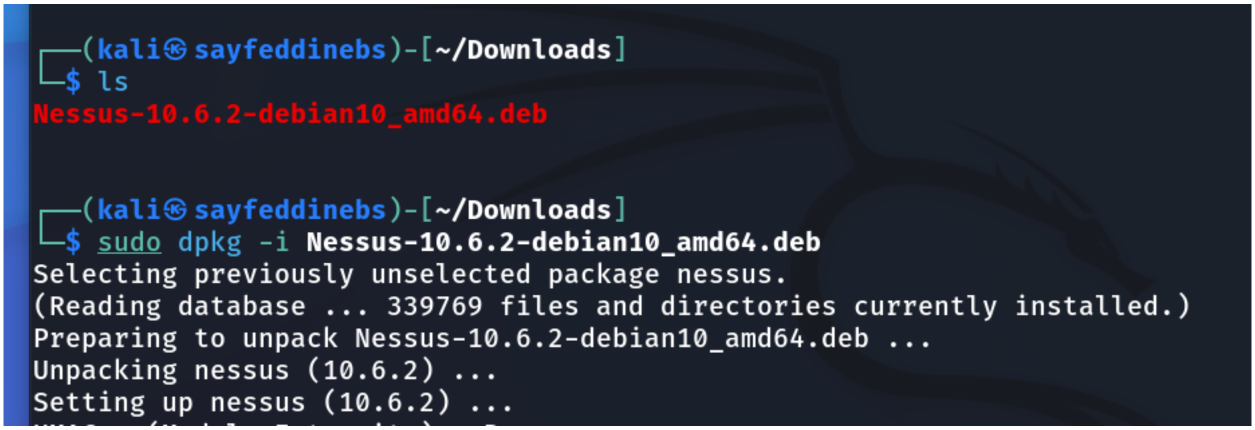
Summary

Release Date: Oct 31, 2023

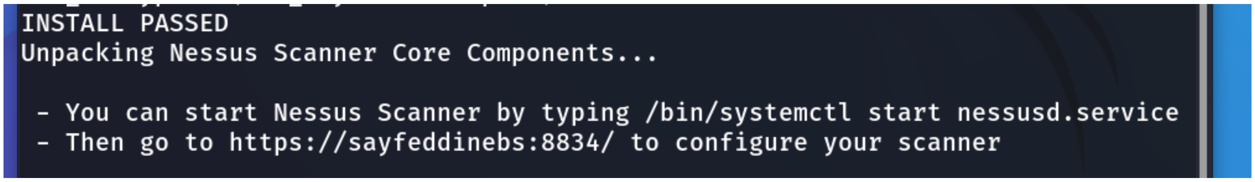
Release Notes:
Tenable Nessus 10.6.2 Release Notes

Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)

🎯 Next I’m going to install Nessus so I moved to its installation path in the terminal and ran the command `sudo dpkg -i <file_name>`



```
┌──(kali㉿sayfeddinebs)-[~/Downloads]
└─$ ls
Nessus-10.6.2-debian10_amd64.deb

┌──(kali㉿sayfeddinebs)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.6.2-debian10_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 339769 files and directories currently installed.)
Preparing to unpack Nessus-10.6.2-debian10_amd64.deb ...
Unpacking nessus (10.6.2) ...
Setting up nessus (10.6.2) ...
```



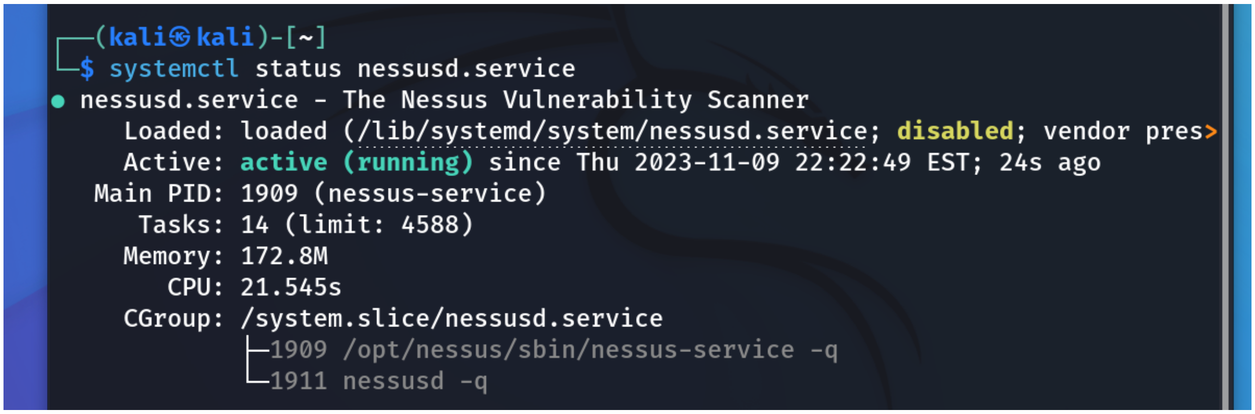
```
INSTALL PASSED
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://sayfeddinebs:8834/ to configure your scanner
```

🎯 Next I’m goinig to start nessus demon so I can start using Nessus I’m going to do that using the command `systemctl start <service>`

I executed the command `systemctl start nessusd.service`

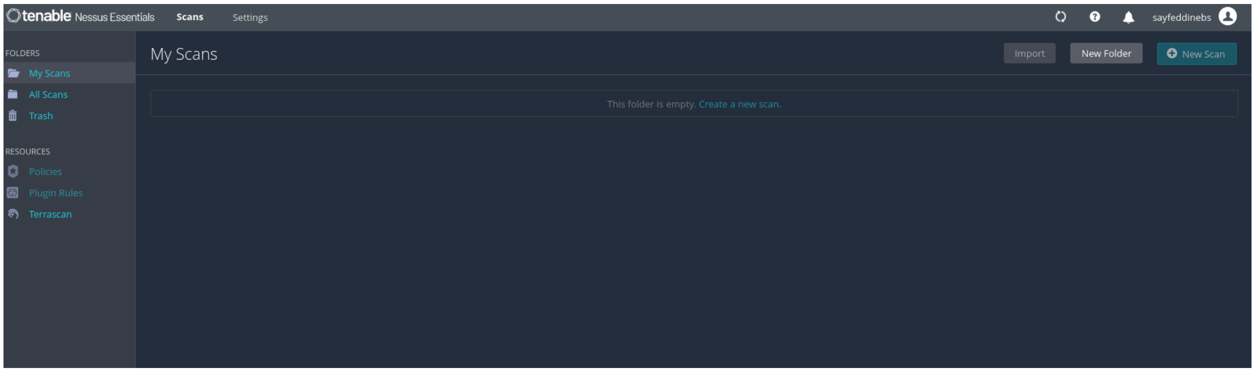
> 🎯 Now I’m going check the status of nessus using the command `systemctl status nessus`

I executed the command systemctl status nessusd.service and you can see that service is running here :



```
┌──(kali㉿kali)-[~]
└─$ systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; vendor pres>
     Active: active (running) since Thu 2023-11-09 22:22:49 EST; 24s ago
   Main PID: 1909 (nessus-service)
      Tasks: 14 (limit: 4588)
     Memory: 172.8M
        CPU: 21.545s
     CGroup: /system.slice/nessusd.service
             ├─1909 /opt/nessus/sbin/nessus-service -q
             └─1911 nessusd -q
```

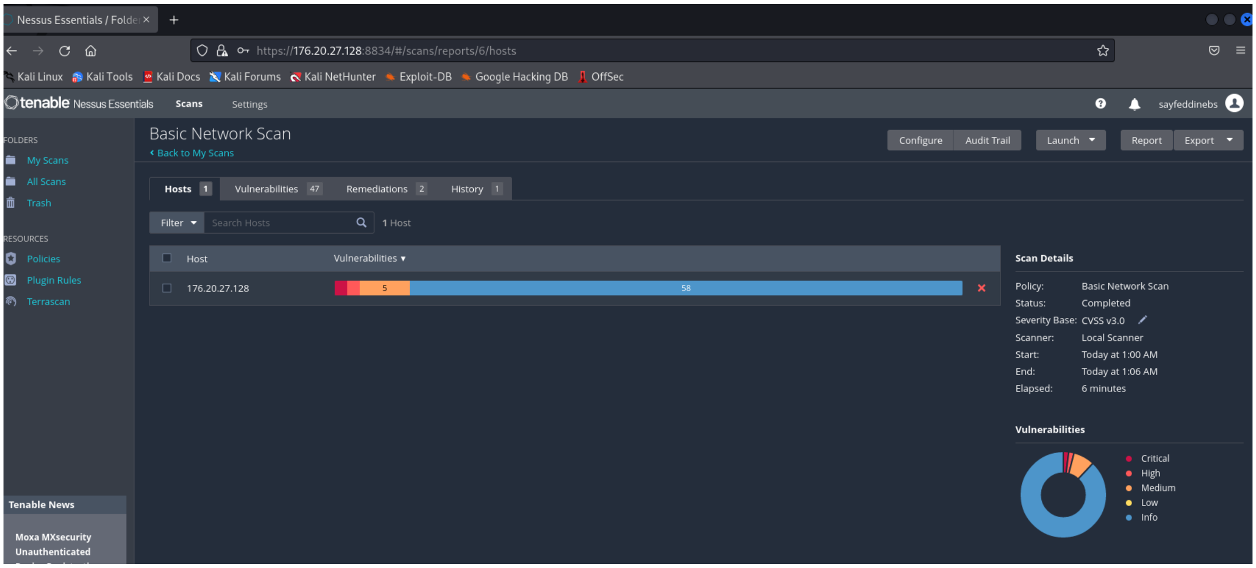
> 🎯 Next I went to the Nessus web interface by entering `https://<ip_address>:8834` and I finalized installation , activated nessus and created an account.



This folder is empty. Create a new scan.

Running a Nessus vulnerability Scan

🎯 In this step I just ran a basic network scan using nessus.



Basic Network Scan

Host	Vulnerabilities ▾
176.20.27.128	5 58

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:00 AM
End: Today at 1:06 AM
Elapsed: 6 minutes

Vulnerabilities