**Create Metasploitable Machine**

### **Project List :**

Task: Download the Metasploitable 2 machine and compromise the target machine using Metasploit

Download metasploitable 2 at: <https://metasploit.help.rapid7.com/docs/metasploitable-2>

Metasploitable 2 Walkthrough: <https://resources.infosecinstitute.com/metasploitable-2-walkthrough/#gref>

**Project Link :**

┌──(root㉿kali)-[~]

└─# ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255

inet6 fe80::a00:27ff:fef0:19 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:f0:00:19 txqueuelen 1000 (Ethernet)

RX packets 31 bytes 5692 (5.5 KiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 24 bytes 3158 (3.0 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 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

┌──(root㉿kali)-[~]

└─# ping 10.0.2.4

PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.

64 bytes from 10.0.2.4: icmp\_seq=1 ttl=64 time=0.929 ms

64 bytes from 10.0.2.4: icmp\_seq=2 ttl=64 time=0.722 ms

64 bytes from 10.0.2.4: icmp\_seq=3 ttl=64 time=0.848 ms

64 bytes from 10.0.2.4: icmp\_seq=4 ttl=64 time=0.764 ms

64 bytes from 10.0.2.4: icmp\_seq=5 ttl=64 time=0.733 ms

64 bytes from 10.0.2.4: icmp\_seq=6 ttl=64 time=0.734 ms

64 bytes from 10.0.2.4: icmp\_seq=7 ttl=64 time=0.804 ms

64 bytes from 10.0.2.4: icmp\_seq=8 ttl=64 time=0.701 ms

64 bytes from 10.0.2.4: icmp\_seq=9 ttl=64 time=0.787 ms

64 bytes from 10.0.2.4: icmp\_seq=10 ttl=64 time=0.743 ms

64 bytes from 10.0.2.4: icmp\_seq=11 ttl=64 time=0.846 ms

64 bytes from 10.0.2.4: icmp\_seq=12 ttl=64 time=0.974 ms

64 bytes from 10.0.2.4: icmp\_seq=13 ttl=64 time=0.725 ms

64 bytes from 10.0.2.4: icmp\_seq=14 ttl=64 time=0.794 ms

64 bytes from 10.0.2.4: icmp\_seq=15 ttl=64 time=0.703 ms

64 bytes from 10.0.2.4: icmp\_seq=16 ttl=64 time=0.695 ms

64 bytes from 10.0.2.4: icmp\_seq=17 ttl=64 time=0.853 ms

64 bytes from 10.0.2.4: icmp\_seq=18 ttl=64 time=0.613 ms

64 bytes from 10.0.2.4: icmp\_seq=19 ttl=64 time=1.10 ms

64 bytes from 10.0.2.4: icmp\_seq=20 ttl=64 time=0.865 ms

64 bytes from 10.0.2.4: icmp\_seq=21 ttl=64 time=0.547 ms

64 bytes from 10.0.2.4: icmp\_seq=22 ttl=64 time=1.00 ms

64 bytes from 10.0.2.4: icmp\_seq=23 ttl=64 time=0.743 ms

64 bytes from 10.0.2.4: icmp\_seq=24 ttl=64 time=0.889 ms

64 bytes from 10.0.2.4: icmp\_seq=25 ttl=64 time=0.642 ms

64 bytes from 10.0.2.4: icmp\_seq=26 ttl=64 time=0.817 ms

64 bytes from 10.0.2.4: icmp\_seq=27 ttl=64 time=1.16 ms

64 bytes from 10.0.2.4: icmp\_seq=28 ttl=64 time=1.51 ms

164 bytes from 10.0.2.4: icmp\_seq=29 ttl=64 time=0.711 ms

064 bytes from 10.0.2.4: icmp\_seq=30 ttl=64 time=0.990 ms

64 bytes from 10.0.2.4: icmp\_seq=31 ttl=64 time=0.447 ms

64 bytes from 10.0.2.4: icmp\_seq=32 ttl=64 time=0.928 ms

64 bytes from 10.0.2.4: icmp\_seq=33 ttl=64 time=0.712 ms

64 bytes from 10.0.2.4: icmp\_seq=34 ttl=64 time=0.771 ms

64 bytes from 10.0.2.4: icmp\_seq=35 ttl=64 time=0.609 ms

64 bytes from 10.0.2.4: icmp\_seq=36 ttl=64 time=0.793 ms

64 bytes from 10.0.2.4: icmp\_seq=37 ttl=64 time=0.766 ms

64 bytes from 10.0.2.4: icmp\_seq=38 ttl=64 time=0.932 ms

64 bytes from 10.0.2.4: icmp\_seq=39 ttl=64 time=0.857 ms

64 bytes from 10.0.2.4: icmp\_seq=40 ttl=64 time=0.857 ms

64 bytes from 10.0.2.4: icmp\_seq=41 ttl=64 time=1.17 ms

64 bytes from 10.0.2.4: icmp\_seq=42 ttl=64 time=1.04 ms

64 bytes from 10.0.2.4: icmp\_seq=43 ttl=64 time=0.831 ms

64 bytes from 10.0.2.4: icmp\_seq=44 ttl=64 time=0.657 ms

64 bytes from 10.0.2.4: icmp\_seq=45 ttl=64 time=0.909 ms

64 bytes from 10.0.2.4: icmp\_seq=46 ttl=64 time=0.849 ms

64 bytes from 10.0.2.4: icmp\_seq=47 ttl=64 time=0.916 ms

64 bytes from 10.0.2.4: icmp\_seq=48 ttl=64 time=0.953 ms

64 bytes from 10.0.2.4: icmp\_seq=49 ttl=64 time=0.794 ms

64 bytes from 10.0.2.4: icmp\_seq=50 ttl=64 time=0.812 ms

64 bytes from 10.0.2.4: icmp\_seq=51 ttl=64 time=0.774 ms

64 bytes from 10.0.2.4: icmp\_seq=52 ttl=64 time=0.685 ms

64 bytes from 10.0.2.4: icmp\_seq=53 ttl=64 time=0.947 ms

64 bytes from 10.0.2.4: icmp\_seq=54 ttl=64 time=1.06 ms

64 bytes from 10.0.2.4: icmp\_seq=55 ttl=64 time=1.03 ms

64 bytes from 10.0.2.4: icmp\_seq=56 ttl=64 time=0.860 ms

64 bytes from 10.0.2.4: icmp\_seq=57 ttl=64 time=0.770 ms

64 bytes from 10.0.2.4: icmp\_seq=58 ttl=64 time=0.759 ms

64 bytes from 10.0.2.4: icmp\_seq=59 ttl=64 time=0.843 ms

64 bytes from 10.0.2.4: icmp\_seq=60 ttl=64 time=0.873 ms

64 bytes from 10.0.2.4: icmp\_seq=61 ttl=64 time=0.633 ms

^C

--- 10.0.2.4 ping statistics ---

61 packets transmitted, 61 received, 0% packet loss, time 60808ms

rtt min/avg/max/mdev = 0.447/0.832/1.514/0.165 ms

┌──(root㉿kali)-[~]

└─# rpcinfo -p 10.0.2.4

program vers proto port service

100000 2 tcp 111 portmapper

100000 2 udp 111 portmapper

100024 1 udp 53096 status

100024 1 tcp 44858 status

100003 2 udp 2049 nfs

100003 3 udp 2049 nfs

100003 4 udp 2049 nfs

100021 1 udp 42886 nlockmgr

100021 3 udp 42886 nlockmgr

100021 4 udp 42886 nlockmgr

100003 2 tcp 2049 nfs

100003 3 tcp 2049 nfs

100003 4 tcp 2049 nfs

100021 1 tcp 46465 nlockmgr

100021 3 tcp 46465 nlockmgr

100021 4 tcp 46465 nlockmgr

100005 1 udp 45480 mountd

100005 1 tcp 44238 mountd

100005 2 udp 45480 mountd

100005 2 tcp 44238 mountd

100005 3 udp 45480 mountd

100005 3 tcp 44238 mountd

┌──(root㉿kali)-[~]

└─# rlogin -1 root 10.0.2.4

SSH protocol v.1 is no longer supported

┌──(root㉿kali)-[~]

└─# rpcinfo -p 10.0.2.4

program vers proto port service

100000 2 tcp 111 portmapper

100000 2 udp 111 portmapper

100024 1 udp 53096 status

100024 1 tcp 44858 status

100003 2 udp 2049 nfs

100003 3 udp 2049 nfs

100003 4 udp 2049 nfs

100021 1 udp 42886 nlockmgr

100021 3 udp 42886 nlockmgr

100021 4 udp 42886 nlockmgr

100003 2 tcp 2049 nfs

100003 3 tcp 2049 nfs

100003 4 tcp 2049 nfs

100021 1 tcp 46465 nlockmgr

100021 3 tcp 46465 nlockmgr

100021 4 tcp 46465 nlockmgr

100005 1 udp 45480 mountd

100005 1 tcp 44238 mountd

100005 2 udp 45480 mountd

100005 2 tcp 44238 mountd

100005 3 udp 45480 mountd

100005 3 tcp 44238 mountd

┌──(root㉿kali)-[~]

└─# ssh-keygen

Generating public/private rsa key pair.

Enter file in which to save the key (/root/.ssh/id\_rsa):

/root/.ssh/id\_rsa already exists.

Overwrite (y/n)? y

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /root/.ssh/id\_rsa

Your public key has been saved in /root/.ssh/id\_rsa.pub

The key fingerprint is:

SHA256:jorULc95qgrRFsuHQdHO3BEy/ufQ8KWdRKRzr+eFKUM root@kali

The key's randomart image is:

+---[RSA 3072]----+

| ooo .. .o |

| . ..o. o |

| o+....o + |

| o =+..+ B o |

|. \* . o S E . |

| o o . \* . . o |

|. . o o o + + . |

| o . = .. = . |

| o.o.=o . |

+----[SHA256]-----+

┌──(root㉿kali)-[~]

└─# telnet 10.0.2.4

Trying 10.0.2.4...

Connected to 10.0.2.4.

Escape character is '^]'.

\_ \_ \_ \_ \_ \_ \_\_\_\_

\_ \_\_ \_\_\_ \_\_\_| |\_ \_\_ \_ \_\_\_ \_ \_\_ | | \_\_\_ (\_) |\_ \_\_ \_| |\_\_ | | \_\_\_|\_\_\_ \

| '\_ ` \_ \ / \_ \ \_\_/ \_` / \_\_| '\_ \| |/ \_ \| | \_\_/ \_` | '\_ \| |/ \_ \ \_\_) |

| | | | | | \_\_/ || (\_| \\_\_ \ |\_) | | (\_) | | || (\_| | |\_) | | \_\_// \_\_/

|\_| |\_| |\_|\\_\_\_|\\_\_\\_\_,\_|\_\_\_/ .\_\_/|\_|\\_\_\_/|\_|\\_\_\\_\_,\_|\_.\_\_/|\_|\\_\_\_|\_\_\_\_\_|

|\_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadminConnection closed by foreign host.

┌──(root㉿kali)-[~]

└─#

┌──(root㉿kali)-[~]

└─# telnet 10.0.2.4

Trying 10.0.2.4...

Connected to 10.0.2.4.

Escape character is '^]'.

\_ \_ \_ \_ \_ \_ \_\_\_\_

\_ \_\_ \_\_\_ \_\_\_| |\_ \_\_ \_ \_\_\_ \_ \_\_ | | \_\_\_ (\_) |\_ \_\_ \_| |\_\_ | | \_\_\_|\_\_\_ \

| '\_ ` \_ \ / \_ \ \_\_/ \_` / \_\_| '\_ \| |/ \_ \| | \_\_/ \_` | '\_ \| |/ \_ \ \_\_) |

| | | | | | \_\_/ || (\_| \\_\_ \ |\_) | | (\_) | | || (\_| | |\_) | | \_\_// \_\_/

|\_| |\_| |\_|\\_\_\_|\\_\_\\_\_,\_|\_\_\_/ .\_\_/|\_|\\_\_\_/|\_|\\_\_\\_\_,\_|\_.\_\_/|\_|\\_\_\_|\_\_\_\_\_|

|\_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin

Password:

Last login: Thu Sep 7 08:29:30 EDT 2023 on tty1

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;

the exact distribution terms for each program are described in the

individual files in /usr/share/doc/\*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by

applicable law.

To access official Ubuntu documentation, please visit:

http://help.ubuntu.com/

No mail.

msfadmin@metasploitable:~$

msfadmin@metasploitable:~$

metasploitable login: msfadmin

Password:

Last login: Thu Sep 7 09:21:23 EDT 2023 from 10.0.2.15 on pts/1

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;

the exact distribution terms for each program are described in the

individual files in /usr/share/doc/\*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by

applicable law.

To access official Ubuntu documentation, please visit:

http://help.ubuntu.com/

No mail.

msfadmin@metasploitable:~$ cal

September 2023

Su Mo Tu We Th Fr Sa

1 2

3 4 5 6 7 8 9

10 11 12 13 14 15 16

17 18 19 20 21 22 23

24 25 26 27 28 29 30

msfadmin@metasploitable:~$ who

msfadmin tty1 2023-09-07 09:14

root pts/0 2023-09-07 09:14 (:0.0)

msfadmin pts/1 2023-09-07 09:21 (10.0.2.15)

msfadmin pts/2 2023-09-07 09:25 (10.0.2.15)

msfadmin@metasploitable:~$