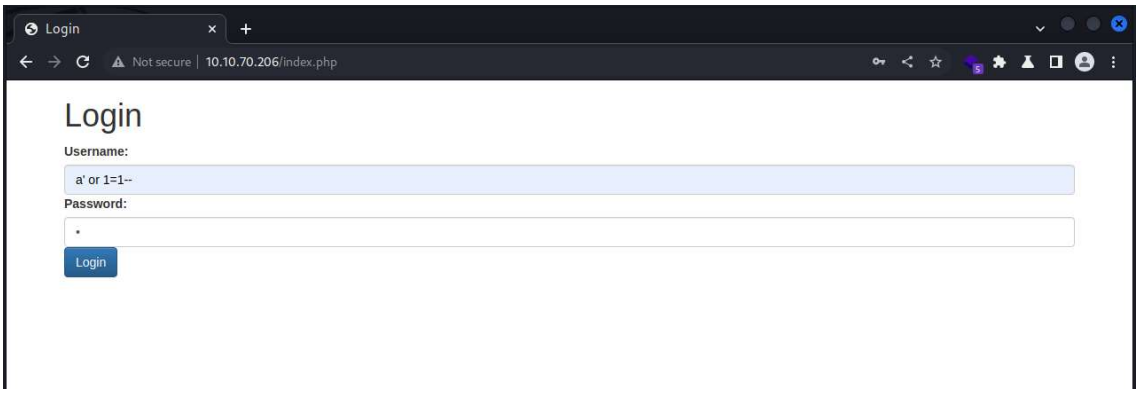
INITIAL SHELL:

NMAP Scan.

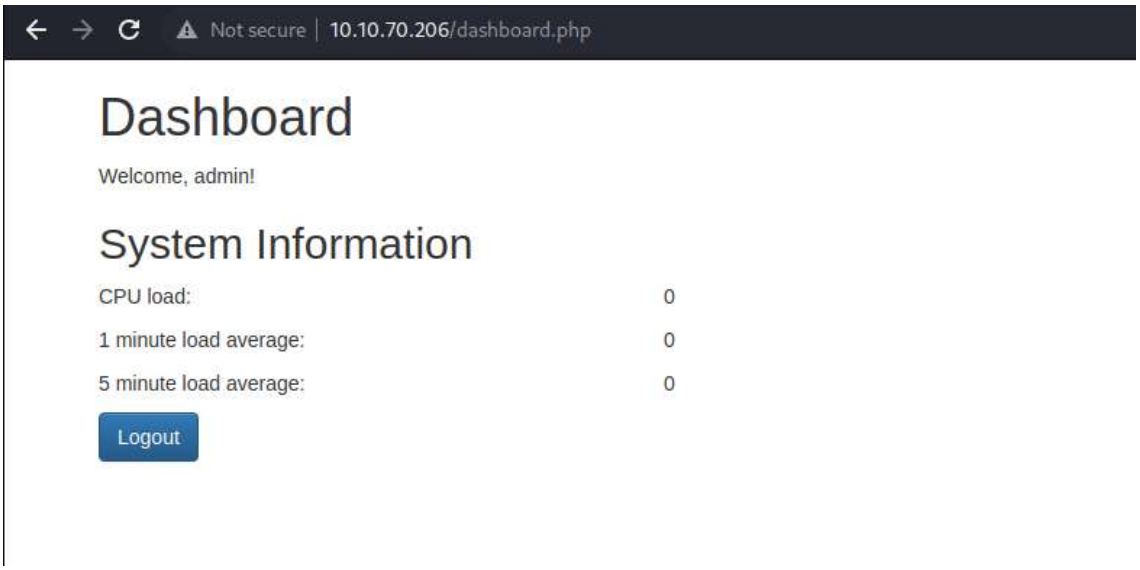
```
┌──(kali㉿kali)-[~/opt/Vulnlab/sync]
└─$ nmap -p- -A 10.10.70.206
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-17 07:45 EDT
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 1.02% done; ETC: 08:06 (0:21:01 remaining)
Stats: 0:05:49 elapsed; 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
```

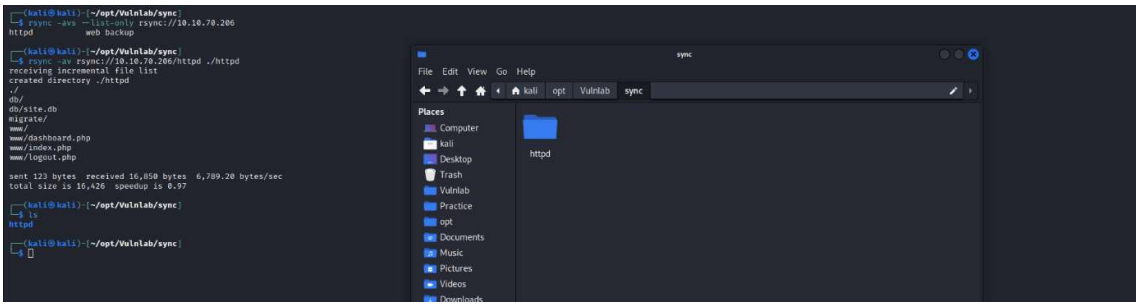
Navigating to port 80 shows a login page which is vulnerable to SQL Injection.



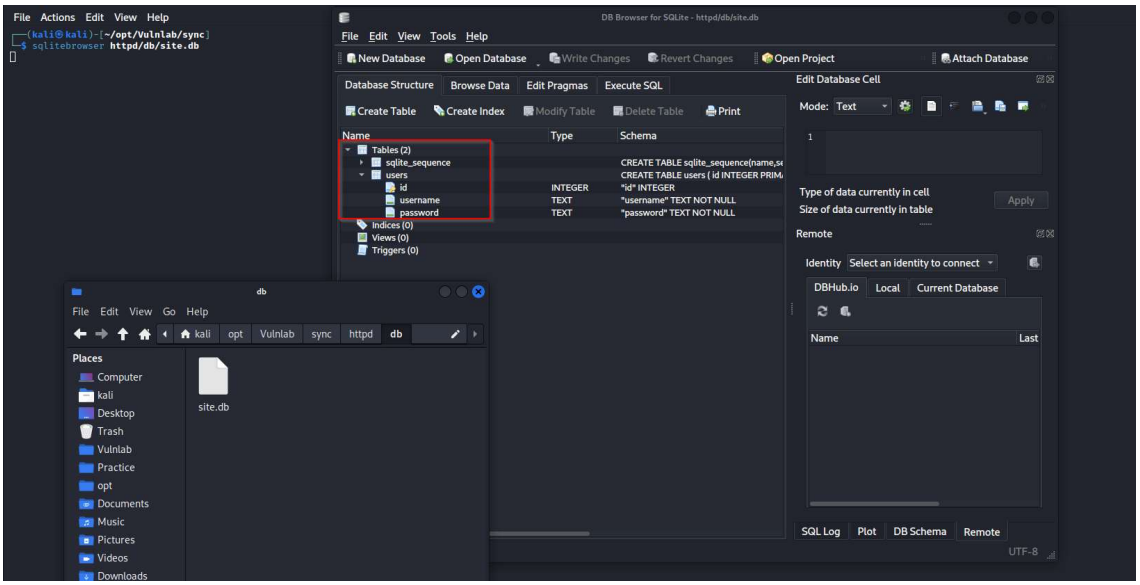
However no further exploitation can be performed.

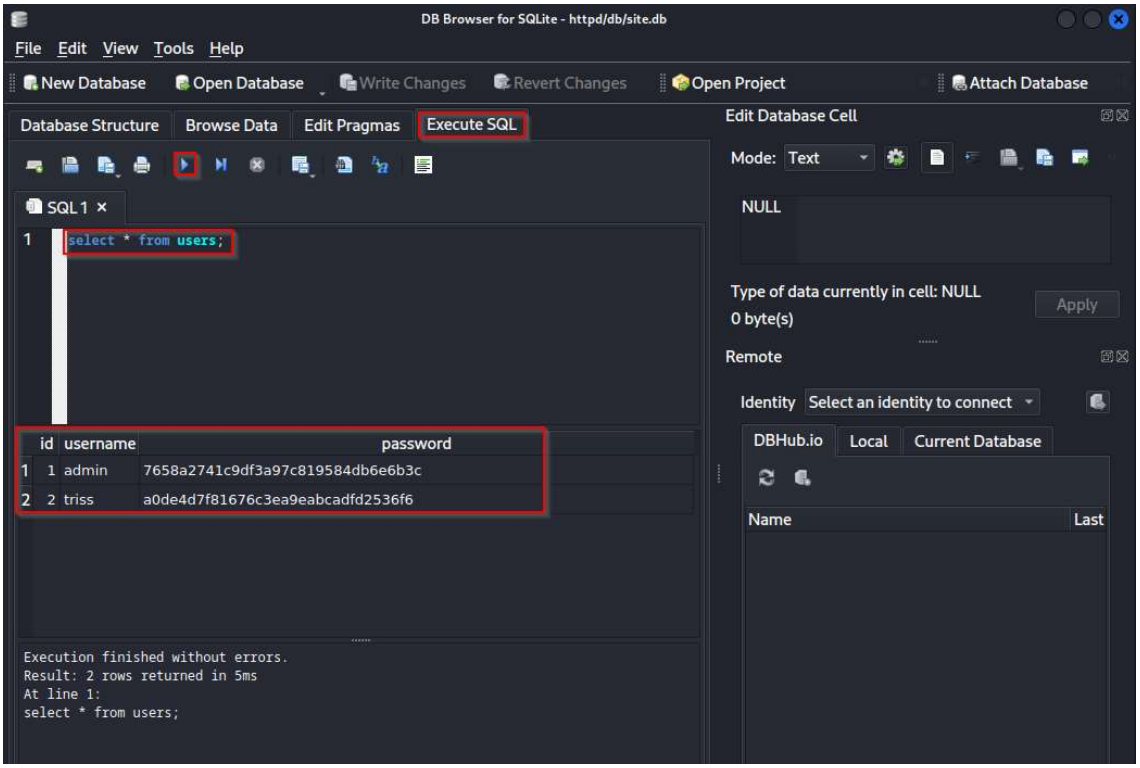


Since port 873 is open, it is possible to enumerate shares using rsync. Transferring the interesting folder “httpd” to kali.

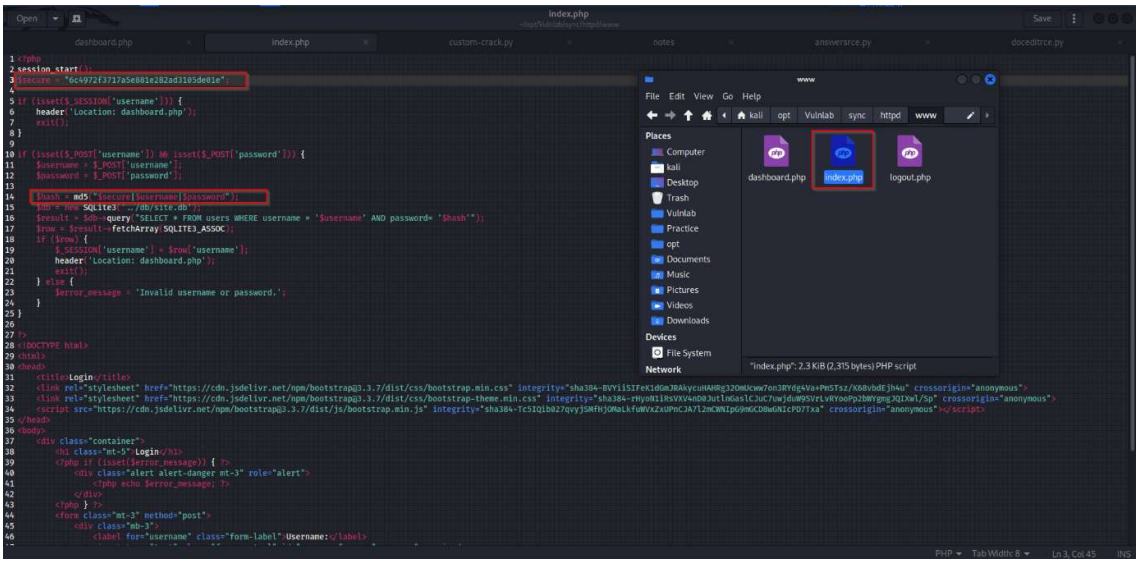


There is a “site.db” file in the transferred folder. Inspecting it using sqlitebrowser reveals usernames and password hash.

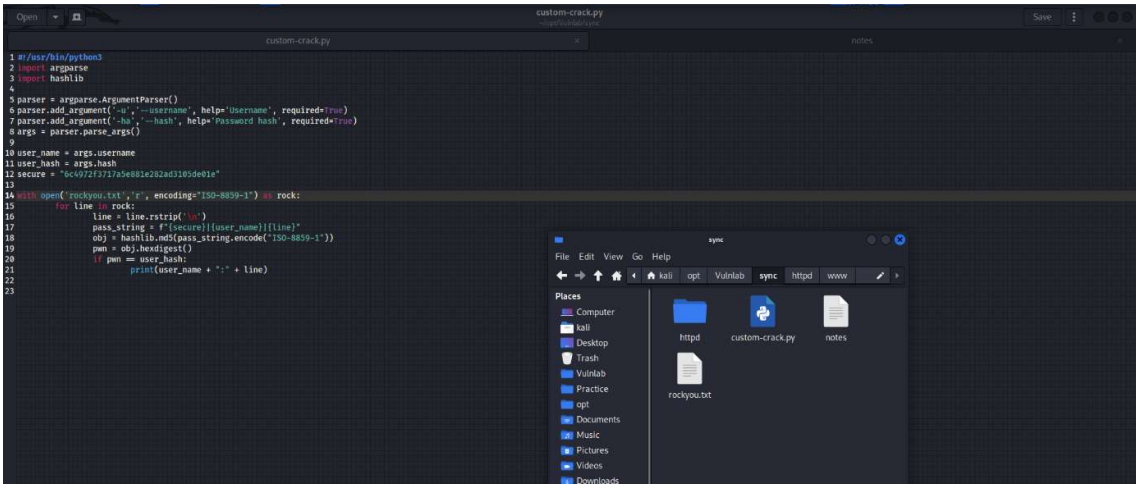




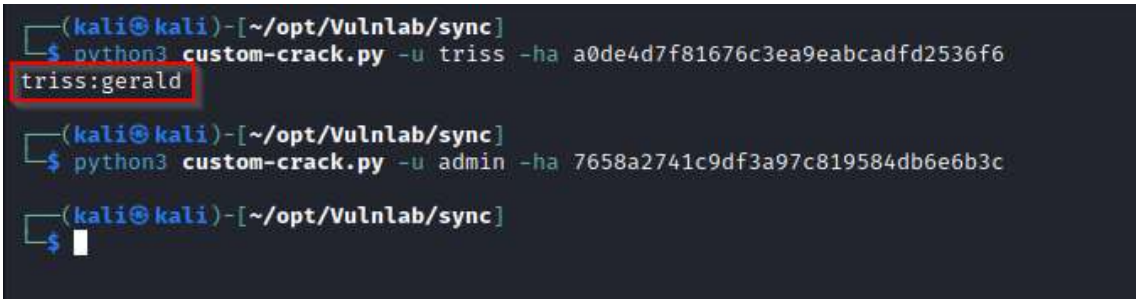
“index.php” which is in “httpd/www/” folder reveals the mechanism for which the hashes are stored in database above.



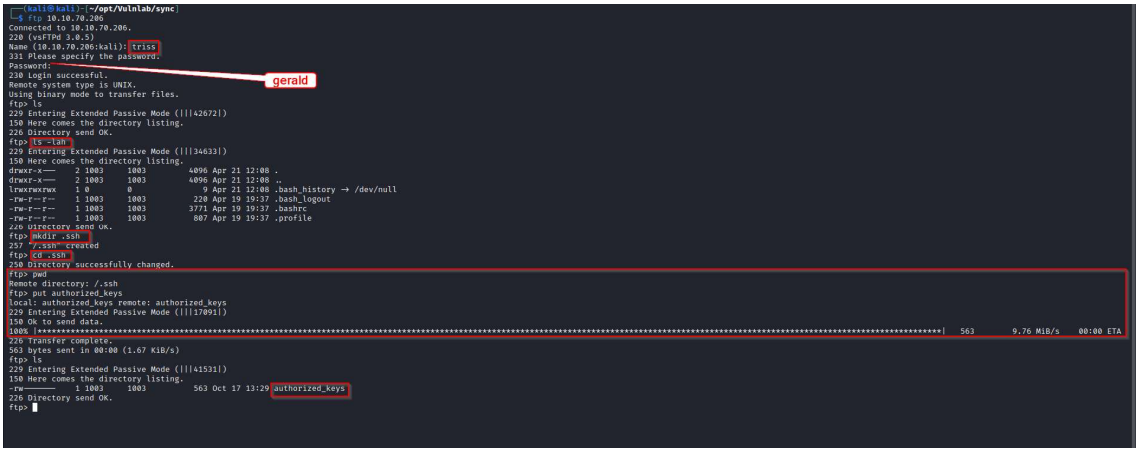
Creating a custom python script to brute force the hashes using the wordlist “rockyou.txt”.

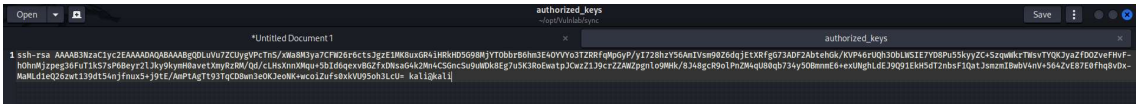


Successfully cracked the password “gerald” for user “triss”

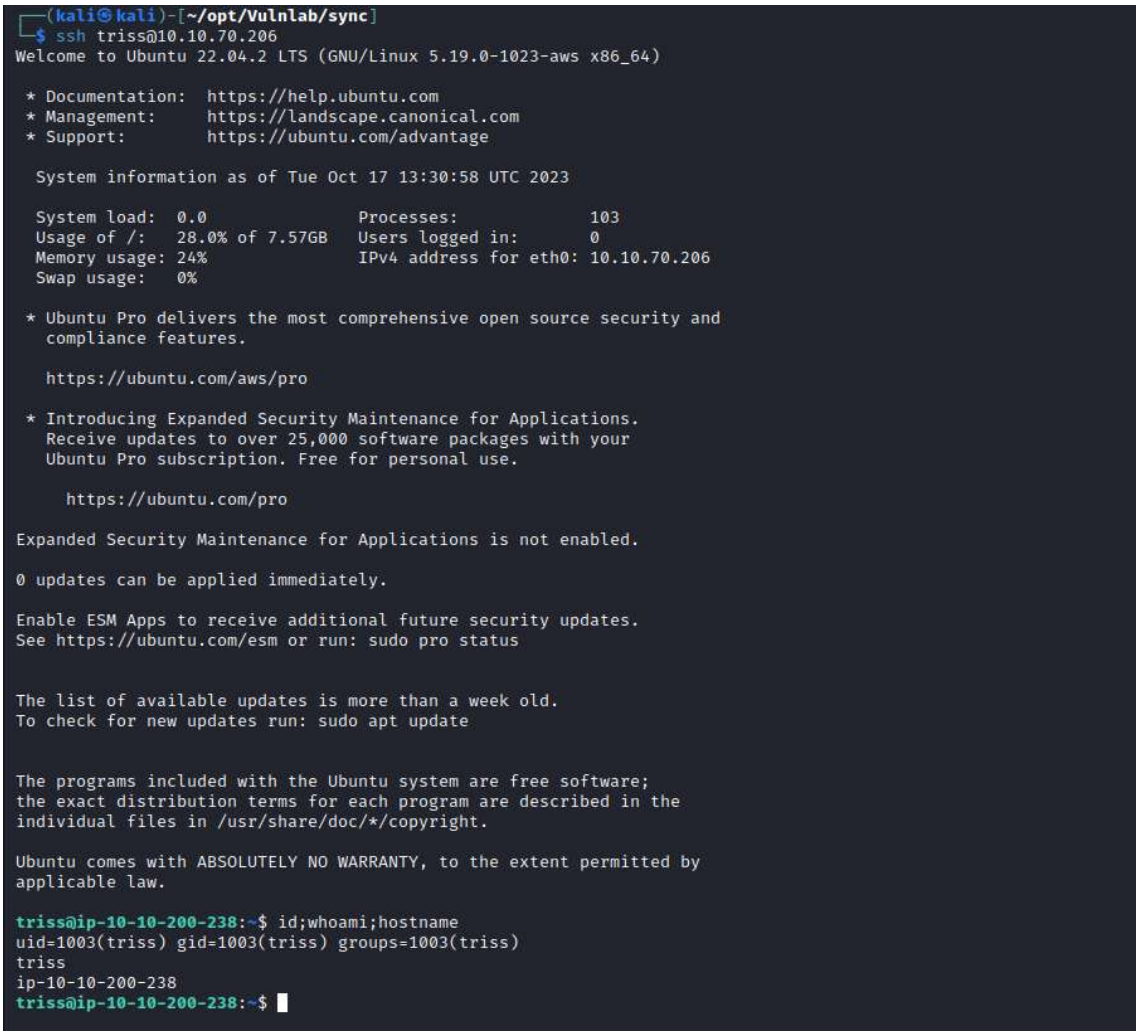


Authenticating to port 21 (ftp) with the above credentials, and listing the contents reveals that we are inside the home folder of “triss” user. Creating “.ssh” folder and uploading “authorized_keys” file containing the public key of kali attack machine (Note: you can generate key pairs in kali using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





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.



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:Mailing 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
uuidd:x:107:113::/run/uuidd:/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
ftp:x:115:123:ftp daemon,,,:/srv/ftp:/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:/home/triss$ id;whoami
uid=1004(jennifer) gid=1004(jennifer) groups=1004(jennifer)
jennifer
jennifer@ip-10-10-200-238:/home/triss$
```

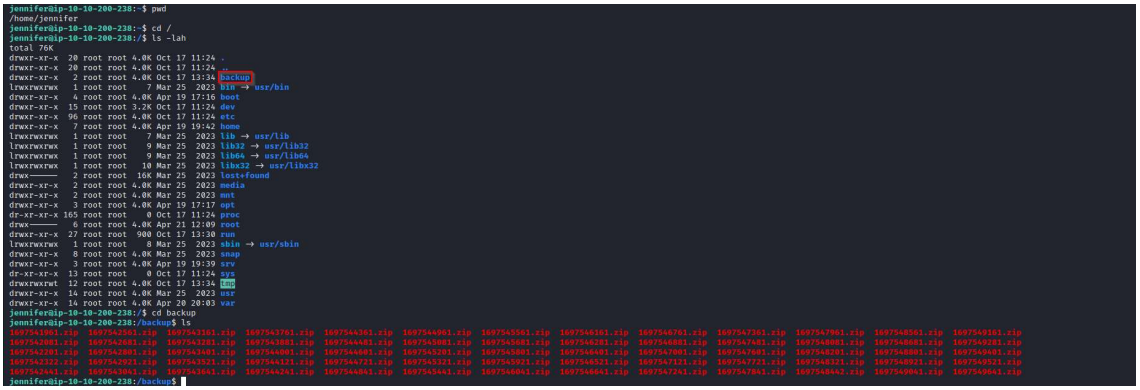
gerald

Obtaining the "user.txt" flag

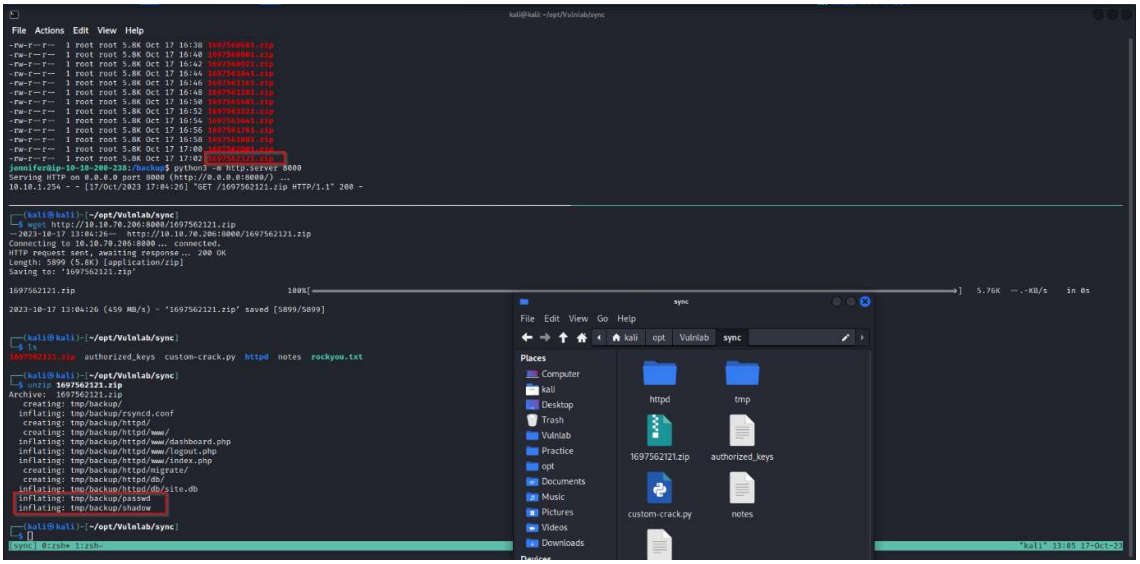
```
jennifer@ip-10-10-200-238:/home/triss$ find / -name user.txt 2>/dev/null
/home/jennifer/user.txt
jennifer@ip-10-10-200-238:/home/triss$ cd /home/jennifer
jennifer@ip-10-10-200-238:~$ pwd
/home/jennifer
jennifer@ip-10-10-200-238:~$ ls
user.txt
jennifer@ip-10-10-200-238:~$ cat user.txt
VL{bcf845cf94864fbba7e016d9fcd3a2db}
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:

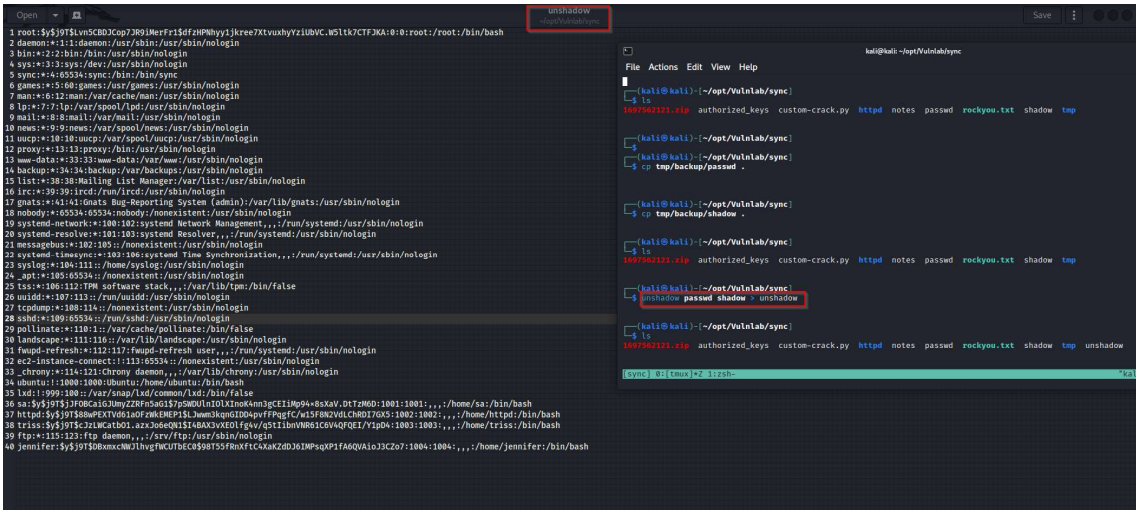
Further exploration of the file system reveals an interesting “/backup” folder which contains a lot of zip files.



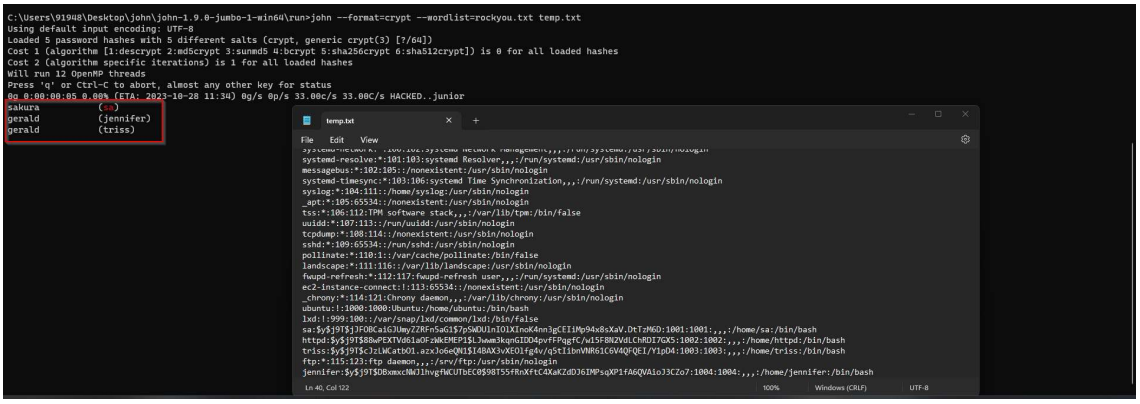
Transferring one of the zip files to the kali attack machine and unzipping it to get the backup copy of “passwd” and “shadow” files of the target system. Note that it is not possible to read the original “/etc/shadow” file in the target as any user other that “root” user of the target .



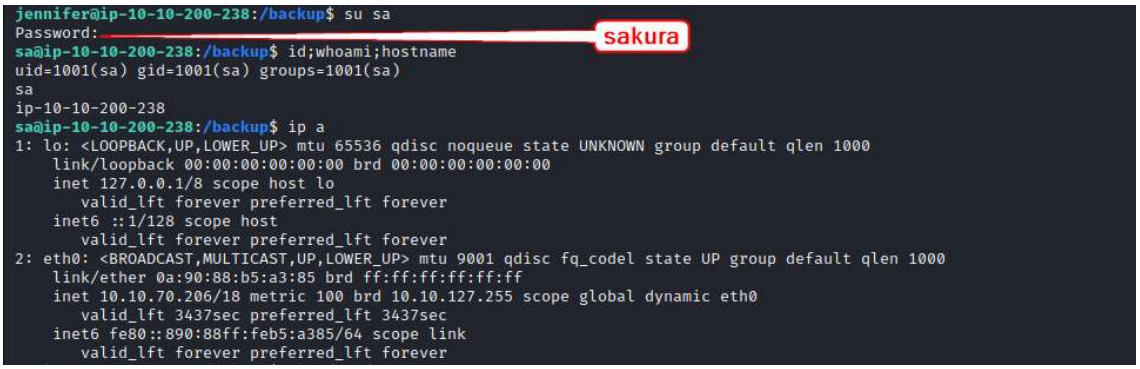
Obtaining traditional Unix password file via “unshadow” command.



Cracking the hash using “john the ripper” tool reveals the password “sakura” for “sa” user.

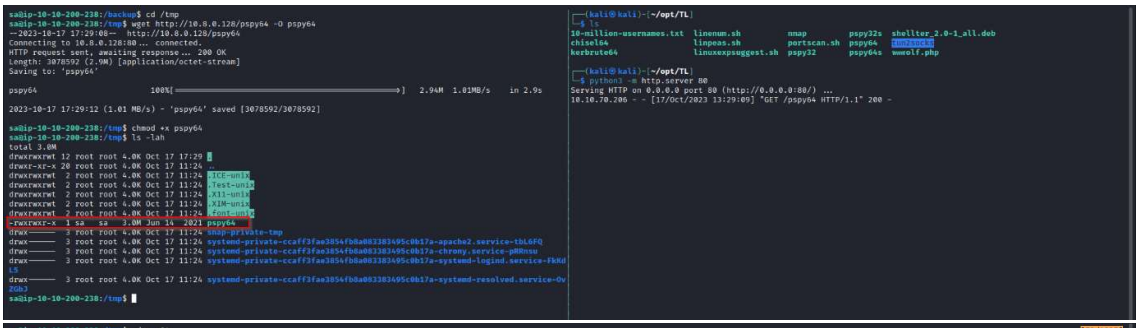


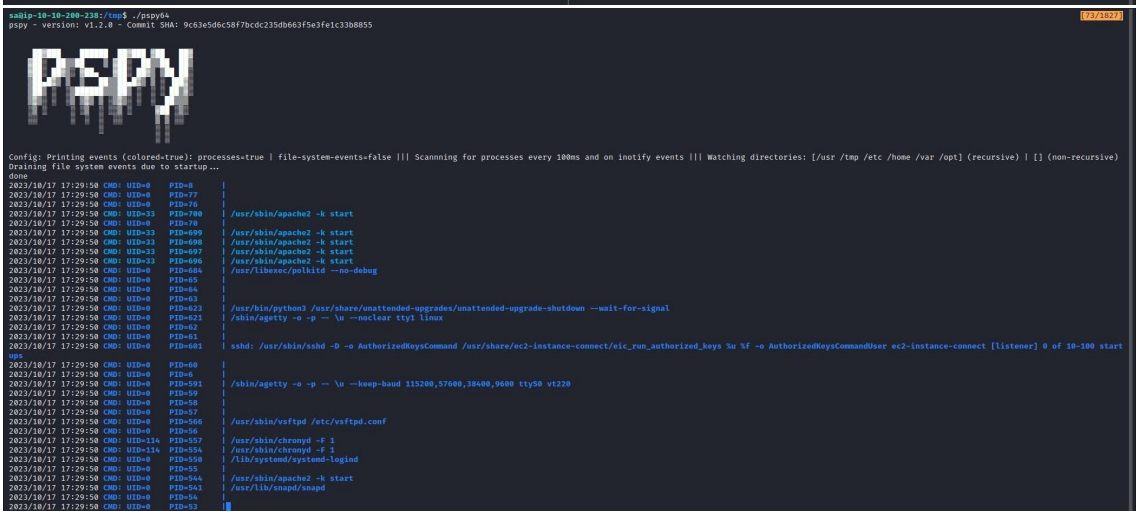
Switching user to “sa”.

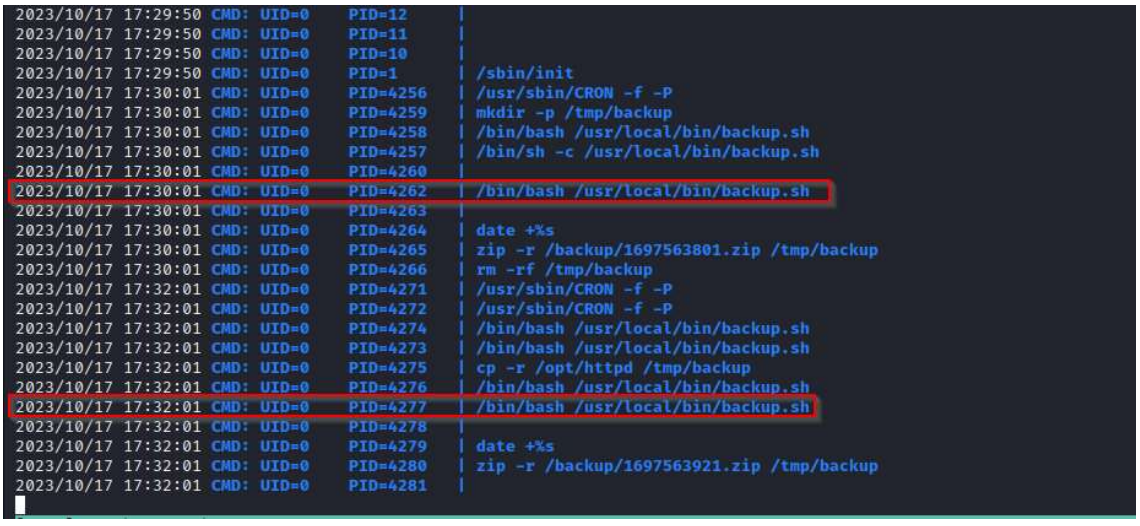


PRIVILEGE ESCALATION III:

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.







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.