دانشگاه صنعتی امیرکبیر
( پلی تکنیک تهران )
دانشکده مهندسی کامپیوتر

# گزارش تمرین عملی اول

## درس مبانی امنیت اطلاعات

هلیا سادات هاشمی‌پور-۹۸۳۱۱۰۶

استاد

دکتر شهریاری

آبان ۰۱

# بخش اول

ابتدا WSL2 را بر روی سیستم خود نصب کردم تا یک محیط خط فرمانی لینوکسی داشته باشم.

- **Ping**

در این بخش ابتدا ابزاری نوشته شد که با دریافت آدرس آیپی یا دامنه (طبق دستور کار باید با آیپی و یا دامنه کار کند) مد نظر کاربر مشخص میکند که آیا پینگ آن آدرس با موفقیت انجام شده است یا خیر (که خروجی به صورت Up و Down به ترتیب در می‌آید) سپس خروجی‌ها را در فایل result_ping.txt ذخیره کردم.

- **کد**

```python
import os

parameter = 2

hostname = input('Please Enter IP/Domain: ')  # example: www.google.com
response = os.system("ping -c " + str(parameter) +
                     " " + hostname)   # ping 2 times

try:
    with open('result_ping.txt', 'w') as f:  # create file
        if response == 0:  # if ping is ok
            f.write(hostname + ' -->  Up\n')  # write to file
        else:  # if ping is not ok
            f.write(hostname + ' --> Down\n')  # write to file

except Exception as e:
    print("Invalid Hostname")
    print(e)

```

- **خروجی**

همانطور که مشاهده میکنیم با زدن دامنه www.google.com همگی پکت‌ها دریافت شده‌اند. خروجی این برنامه همانطور که ذکر شد در result_ping.txt ذخیره میشود.

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo python3 ping.py
[sudo] password for kali:
Please Enter IP/Domain: www.google.com
PING www.google.com (172.217.165.4) 56(84) bytes of data.
64 bytes from yyz12s06-in-f4.1e100.net (172.217.165.4): icmp_seq=1 ttl=128 time=225 ms
64 bytes from yyz12s06-in-f4.1e100.net (172.217.165.4): icmp_seq=2 ttl=128 time=220 ms
64 bytes from yyz12s06-in-f4.1e100.net (172.217.165.4): icmp_seq=3 ttl=128 time=224 ms
64 bytes from yyz12s06-in-f4.1e100.net (172.217.165.4): icmp_seq=4 ttl=128 time=222 ms
64 bytes from yyz12s06-in-f4.1e100.net (172.217.165.4): icmp_seq=5 ttl=128 time=201 ms
64 bytes from yyz12s06-in-f4.1e100.net (172.217.165.4): icmp_seq=6 ttl=128 time=215 ms

── www.google.com ping statistics ──
6 packets transmitted, 6 received, 0% packet loss, time 5011ms
rtt min/avg/max/mdev = 201.150/217.931/224.818/8.153 ms

┌──(kali㉿kali)-[~/Desktop/Security]
└─$ cat result_ping.txt
www.google.com ──>  Up
```

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo python3 ping.py
Please Enter IP/Domain: 89.43.3.229
PING 89.43.3.229 (89.43.3.229) 56(84) bytes of data.
64 bytes from 89.43.3.229: icmp_seq=1 ttl=128 time=394 ms
64 bytes from 89.43.3.229: icmp_seq=2 ttl=128 time=401 ms
64 bytes from 89.43.3.229: icmp_seq=3 ttl=128 time=393 ms
64 bytes from 89.43.3.229: icmp_seq=4 ttl=128 time=406 ms
64 bytes from 89.43.3.229: icmp_seq=5 ttl=128 time=399 ms
64 bytes from 89.43.3.229: icmp_seq=6 ttl=128 time=396 ms

── 89.43.3.229 ping statistics ──
6 packets transmitted, 6 received, 0% packet loss, time 5015ms
rtt min/avg/max/mdev = 393.087/398.180/406.281/4.508 ms
```

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo python3 ping.py
Please Enter IP/Domain: 89.43.3.170
PING 89.43.3.170 (89.43.3.170) 56(84) bytes of data.
64 bytes from 89.43.3.170: icmp_seq=1 ttl=128 time=415 ms
64 bytes from 89.43.3.170: icmp_seq=2 ttl=128 time=435 ms
64 bytes from 89.43.3.170: icmp_seq=3 ttl=128 time=412 ms
64 bytes from 89.43.3.170: icmp_seq=4 ttl=128 time=433 ms
64 bytes from 89.43.3.170: icmp_seq=5 ttl=128 time=424 ms
64 bytes from 89.43.3.170: icmp_seq=6 ttl=128 time=407 ms

── 89.43.3.170 ping statistics ──
6 packets transmitted, 6 received, 0% packet loss, time 5013ms
rtt min/avg/max/mdev = 407.170/421.097/435.370/10.401 ms
```

حال اگر تمامی پکت‌ها loss شود آن آدرس غیرفعال است.

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo python3 ping.py
[sudo] password for kali:
Please Enter IP/Domain: 89.43.3.65
PING 89.43.3.65 (89.43.3.65) 56(84) bytes of data.

── 89.43.3.65 ping statistics ──
6 packets transmitted, 0 received, 100% packet loss, time 5125ms
```

- **IP scanner**

حال برای اینکه محدوده‌ای از آیپی‌ها اسکن شود کافی است که یک حلقه داشته باشیم و در آن تمامی پینگ‌ها را بگیریم سپس در همان حلقه وضعیت فعال را غیرفعال را مشخص کرده و درنهایت نتیجه را در ترمینال چاپ میکنیم، سپس نتایج را در فایل result_ip_scanner.txt ذخیره میکنیم.

- **کد**

```python
import os
import time

# Start time of the scan
start_time = time.time()

# Enter the network address
Domain = input('Enter the Network address: ')

# Enter the starting network number
start_num = int(input('Enter the Starting Number: '))

# Enter the last network number
end_num = int(input('Enter the Last  Number: '))

'''Create a file to save the results '''
with open('result_ip_scanner.txt', 'w') as f:
    # Write scanning in progress in the file
    f.write('Scanning in Progress\n')

'''Loop through the network addresses'''
for i in range(start_num, (end_num + 1)):
    '''Split the network address '''
    Domain_splits = Domain.split('.')

    '''Create the hostname'''
    hostname = Domain_splits[0] + '.' + Domain_splits[1] + \
        '.' + Domain_splits[2] + '.' + str(i)
    # Ping the host
    response = os.system('ping -c 2 ' + hostname)
    '''open the file in append mode'''
    try:
        with open('result_ip_scanner.txt', 'a') as f:
            if response == 0:  # If the host is up
                '''Write the host is live in the file'''
                f.write(hostname + ' --> Live\n')

            else:  # If the host is down
                '''Write the host is down in the file'''
                f.write(hostname + ' --> Down\n')
    except Exception as e:
        print(e)


'''Print the time taken to scan the network addresses'''
print(f'scanning complete in {round(time.time() - start_time, 3)} seconds')
```

- **خروجی**

برای اینکه خروجی زیر را داشته باشیم وی‌پی‌ان را روشن میکنیم و همانطور که گفتم وضعیت فعال را غیرفعال را مشخص کرده و نتایج را در فایل result_ip_scanner.txt ذخیره میکنیم.

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo python3 ip-scanner.py
Enter the Network address: 89.43.3.0
Enter the Starting Number: 60
Enter the Last  Number: 70
PING 89.43.3.60 (89.43.3.60) 56(84) bytes of data.

── 89.43.3.60 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1026ms

PING 89.43.3.61 (89.43.3.61) 56(84) bytes of data.

── 89.43.3.61 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1025ms

PING 89.43.3.62 (89.43.3.62) 56(84) bytes of data.

── 89.43.3.62 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1019ms

PING 89.43.3.63 (89.43.3.63) 56(84) bytes of data.

── 89.43.3.63 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1029ms

PING 89.43.3.64 (89.43.3.64) 56(84) bytes of data.

── 89.43.3.64 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1032ms

PING 89.43.3.65 (89.43.3.65) 56(84) bytes of data.

── 89.43.3.65 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1031ms

PING 89.43.3.66 (89.43.3.66) 56(84) bytes of data.
64 bytes from 89.43.3.66: icmp_seq=1 ttl=128 time=431 ms
64 bytes from 89.43.3.66: icmp_seq=2 ttl=128 time=432 ms

── 89.43.3.66 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 430.549/431.168/431.788/0.619 ms
PING 89.43.3.67 (89.43.3.67) 56(84) bytes of data.

── 89.43.3.67 ping statistics ──
2 packets transmitted, 0 received, 100% packet loss, time 1018ms

PING 89.43.3.68 (89.43.3.68) 56(84) bytes of data.
64 bytes from 89.43.3.68: icmp_seq=1 ttl=128 time=459 ms
64 bytes from 89.43.3.68: icmp_seq=2 ttl=128 time=422 ms

── 89.43.3.68 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 421.955/440.565/459.176/18.610 ms
PING 89.43.3.69 (89.43.3.69) 56(84) bytes of data.
64 bytes from 89.43.3.69: icmp_seq=1 ttl=128 time=415 ms
64 bytes from 89.43.3.69: icmp_seq=2 ttl=128 time=414 ms

── 89.43.3.69 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 413.986/414.471/414.956/0.485 ms
PING 89.43.3.70 (89.43.3.70) 56(84) bytes of data.
64 bytes from 89.43.3.70: icmp_seq=1 ttl=128 time=411 ms
64 bytes from 89.43.3.70: icmp_seq=2 ttl=128 time=444 ms

── 89.43.3.70 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 411.007/427.747/444.488/16.740 ms
scanning complete in 95.965 seconds
```

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ cat result_ip_scanner.txt
Scanning in Progress
89.43.3.60  Down
89.43.3.61  Down
89.43.3.62  Down
89.43.3.63  Down
89.43.3.64  Down
89.43.3.65  Down
89.43.3.66 ⟶ Live
89.43.3.67  Down
89.43.3.68 ⟶ Live
89.43.3.69 ⟶ Live
89.43.3.70 ⟶ Live
```

- **Port scanner**

ابتدا بازه پورت ها را دریافت کرده سپس آیپی مربوطه را دریافت میکنیم، سپس روی بازه دریافتی با استفاده از سوکت یک کانکشن به پورت‌ها زده تا ببینیم باز است یا خیر و آخر هم نتیجه را چاپ میکنیم همچنین نتایج را در فایل ذخیره کردم.

- **کد**

```python
from socket import *
import time

# Start time of the scan
start_time = time.time()

# Enter the IP address of the remote_host
remote_host = input('Enter the remote host IP scan: ')

# Get the IP address of the remote_host
rh_IP = gethostbyname(remote_host)

# Enter the start port number
start_num = int(input('Enter the start port number:  '))

# Enter the last port number
end_num = int(input('Enter the last port number:  '))
print('***********************************')

'''Print the IP address of the remote_host'''
print('Scanner is working on : ', rh_IP)

print('***********************************')

'''Loop through the ports'''
for i in range(start_num, (end_num + 1)):
    '''Create a socket object'''
    s = socket(AF_INET, SOCK_STREAM)
    '''Check if the port is open'''
    res = s.connect_ex((rh_IP, i))
    # try:
    with open('result_port_scanner.txt', 'a') as f:
        if(res == 0):  # If the port is open
            # Print the open port
            print('Port Open:-->     %d' % (i,))
            f.write('Port Open:-->     %d\n' % (i,))

    # except Exception as e:
    #   print(e)

   # Close the socket
    s.close()

# Print the time taken to scan the ports
print(f'scanning complete in {round(time.time() - start_time, 3)} seconds')
```

- خروجی

```
└─$ sudo python3 port_scanner.py
Enter the remote host IP scan: 89.43.3.170
Enter the start port number:  1
Enter the last port number:  82
*************************************
Scanner is working on :  89.43.3.170
*************************************
Port Open:⟶     1
Port Open:⟶     2
Port Open:⟶     3
Port Open:⟶     4
Port Open:⟶     5
Port Open:⟶     6
Port Open:⟶     7
Port Open:⟶     8
Port Open:⟶     9
Port Open:⟶     10
Port Open:⟶     11
Port Open:⟶     12
Port Open:⟶     13
Port Open:⟶     14
Port Open:⟶     15
Port Open:⟶     16
Port Open:⟶     17
Port Open:⟶     18
Port Open:⟶     19
Port Open:⟶     20
Port Open:⟶     21
Port Open:⟶     22
Port Open:⟶     23
Port Open:⟶     24
Port Open:⟶     25
```

# بخش دوم

برای بررسی صحت خروجی ابزار در بخش اول از ابزارهای hping3, netdiscover, nmap استفاده میکنیم .

- **Nmap**

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ nmap -sn 89.43.3.60-70
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 09:21 EDT
Nmap scan report for mx1.payaco-mnp.ir (89.43.3.60)
Host is up (0.0011s latency).
Nmap scan report for 61.mobinnet.net (89.43.3.61)
Host is up (0.0044s latency).
Nmap scan report for 62.mobinnet.net (89.43.3.62)
Host is up (0.0042s latency).
Nmap scan report for 63.mobinnet.net (89.43.3.63)
Host is up (0.0041s latency).
Nmap scan report for 64.mobinnet.net (89.43.3.64)
Host is up (0.0040s latency).
Nmap scan report for 65.mobinnet.net (89.43.3.65)
Host is up (0.0039s latency).
Nmap scan report for 66.mobinnet.net (89.43.3.66)
Host is up (0.0035s latency).
Nmap scan report for 67.mobinnet.net (89.43.3.67)
Host is up (0.0021s latency).
Nmap scan report for 68.mobinnet.net (89.43.3.68)
Host is up (0.0021s latency).
Nmap scan report for 69.mobinnet.net (89.43.3.69)
Host is up (0.0020s latency).
Nmap scan report for 70.mobinnet.net (89.43.3.70)
Host is up (0.0047s latency).
Nmap done: 11 IP addresses (11 hosts up) scanned in 2.04 seconds
```

همانطور که میبینیم، تمامی IPهای بررسی شده در بخش قبل را up اسکن کرد .

- **گزارش TCP full scan**

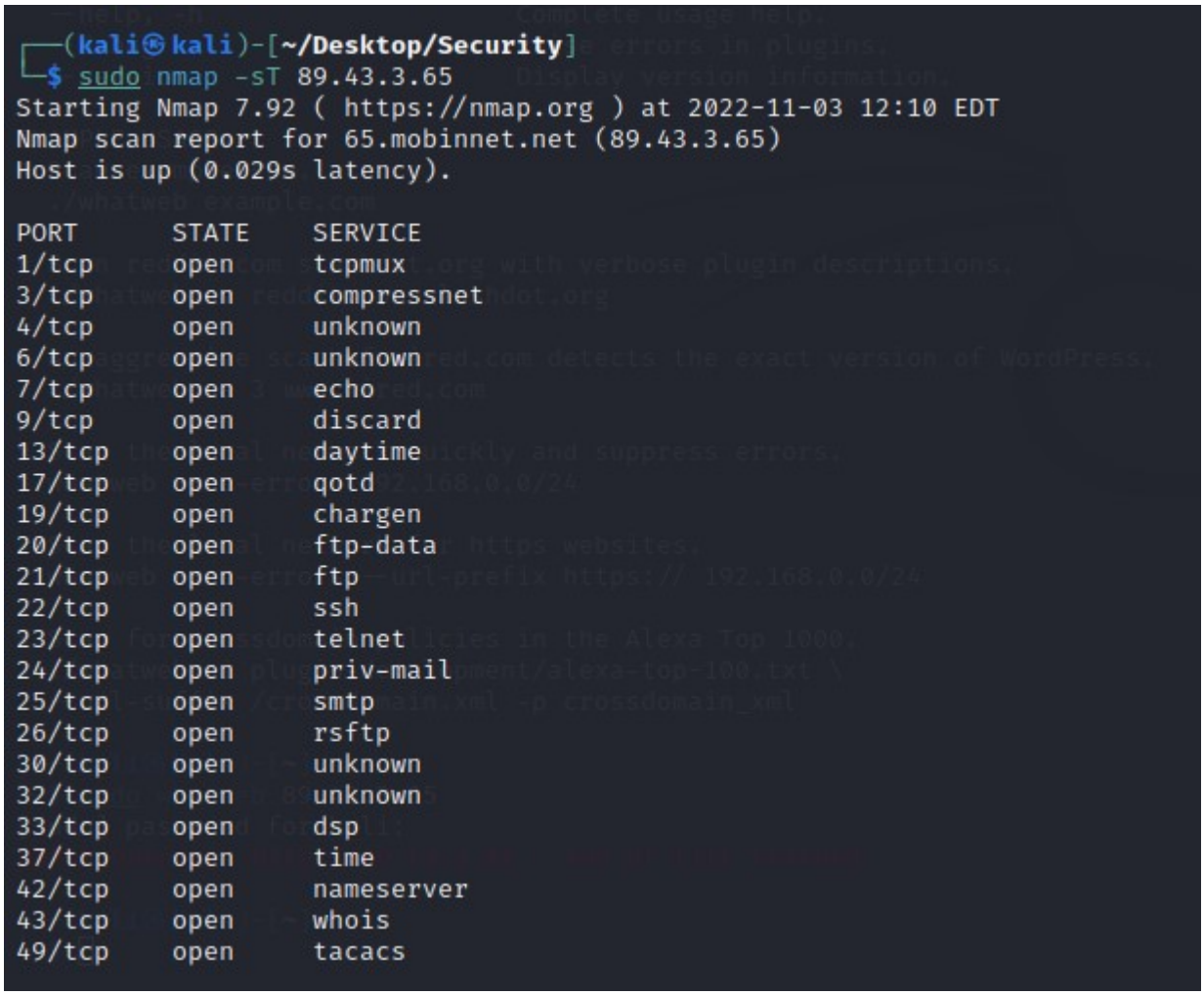
در این بخش پورت‌های TCP را بررسی کردم. در بخش اول هم پورت‌ها اسکن شده بودند بنابراین، نتایج را میتوان با هم مقایسه نمود.

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -sT 89.43.3.229
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 09:42 EDT
Nmap scan report for 229.mobinnet.net (89.43.3.229)
Host is up (0.018s latency).

PORT      STATE    SERVICE
1/tcp     open     tcpmux
3/tcp     open     compressnet
4/tcp     open     unknown
6/tcp     open     unknown
7/tcp     open     echo
9/tcp     open     discard
13/tcp    open     daytime
17/tcp    open     qotd
19/tcp    open     chargen
20/tcp    open     ftp-data
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
24/tcp    open     priv-mail
25/tcp    filtered smtp
26/tcp    open     rsftp
30/tcp    open     unknown
32/tcp    open     unknown
33/tcp    open     dsp
37/tcp    open     time
```

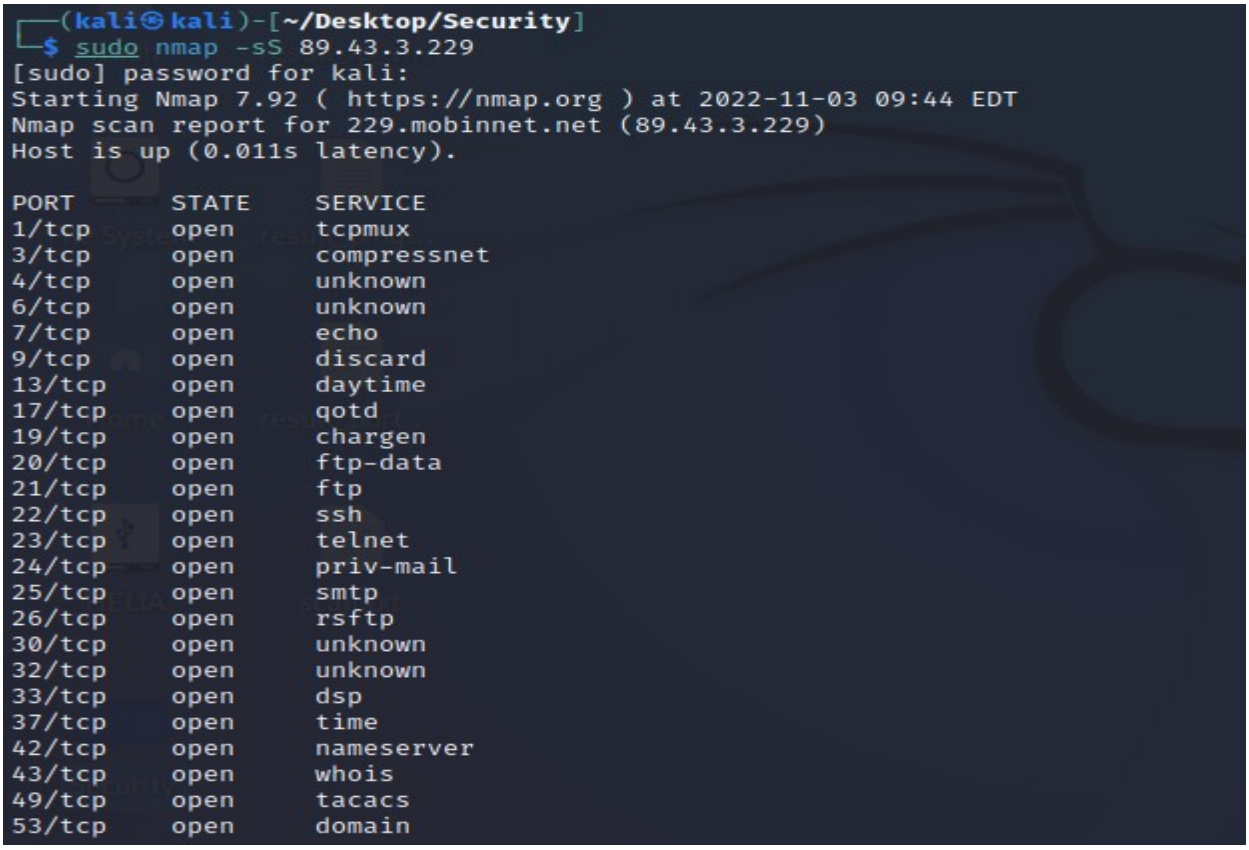
```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -sT 89.43.3.170
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 09:16 EDT
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (0.0035s latency).

PORT      STATE    SERVICE
1/tcp     open     tcpmux
3/tcp     open     compressnet
4/tcp     open     unknown
6/tcp     open     unknown
7/tcp     open     echo
9/tcp     open     discard
13/tcp    open     daytime
17/tcp    open     qotd
19/tcp    open     chargen
20/tcp    open     ftp-data
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
24/tcp    open     priv-mail
25/tcp    open     smtp
26/tcp    open     rsftp
30/tcp    open     unknown
32/tcp    open     unknown
33/tcp    open     dsp
37/tcp    open     time
42/tcp    open     nameserver
43/tcp    open     whois
49/tcp    open     tacacs
```


┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -sT 89.43.3.65
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 12:10 EDT
Nmap scan report for 65.mobinnet.net (89.43.3.65)
Host is up (0.029s latency).
PORT STATE SERVICE
1/tcp open tcpmux
3/tcp open compressnet
4/tcp open unknown
6/tcp open unknown
7/tcp open echo
9/tcp open discard
13/tcp open daytime
17/tcp open qotd
19/tcp open chargen
20/tcp open ftp-data
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
24/tcp open priv-mail
25/tcp open smtp
26/tcp open rsftp
30/tcp open unknown
32/tcp open unknown
33/tcp open dsp
37/tcp open time
42/tcp open nameserver
43/tcp open whois
49/tcp open tacacs

- **گزارش Stealth Scan**

این دستور برای اسکن کامل پورت‌های باز و اطلاعات اضافه راجع به سرویس‌های استفاده شده هر دامین است.



```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -sS 89.43.3.170
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 12:42 EDT
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (1.3s latency).

PORT      STATE SERVICE
1/tcp     open  tcpmux
3/tcp     open  compressnet
4/tcp     open  unknown
6/tcp     open  unknown
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
20/tcp    open  ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
26/tcp    open  rsftp
30/tcp    open  unknown
32/tcp    open  unknown
33/tcp    open  dsp
37/tcp    open  time
42/tcp    open  nameserver
43/tcp    open  whois
49/tcp    open  tacacs
53/tcp    open  domain
```

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -sS 89.43.3.65

Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 09:25 EDT
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 09:25 (0:00:00 remaining)
Nmap scan report for 65.mobinnet.net (89.43.3.65)
Host is up (0.0062s latency).

PORT      STATE SERVICE
1/tcp     open  tcpmux
3/tcp     open  compressnet
4/tcp     open  unknown
6/tcp     open  unknown
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
17/tcp    open  qotd
19/tcp    open  chargen
20/tcp    open  ftp-data
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
26/tcp    open  rsftp
30/tcp    open  unknown
```

همانطور که مشاهده میکنیم همچنین تمامی پورت ها و سرویس‌های مربوط به پورت‌های هر دامین به طور کامل اسکن شده است.

- **گزارش Fingerprint Scan**

در این بخش اطلاعات مربوط به سیستم‌عامل و سرویس‌ها و اطلاعات راجع به پورت ها را نمایش میدهد.

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -O -v 89.43.3.229
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 09:41 EDT
Initiating Ping Scan at 09:41
Scanning 89.43.3.229 [4 ports]
Completed Ping Scan at 09:41, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:41
Completed Parallel DNS resolution of 1 host. at 09:41, 1.98s elapsed
Initiating SYN Stealth Scan at 09:41
Scanning 229.mobinnet.net (89.43.3.229) [1000 ports]
Discovered open port 139/tcp on 89.43.3.229
Discovered open port 143/tcp on 89.43.3.229
Discovered open port 53/tcp on 89.43.3.229
Discovered open port 1720/tcp on 89.43.3.229
Discovered open port 135/tcp on 89.43.3.229
Discovered open port 1025/tcp on 89.43.3.229
Discovered open port 8888/tcp on 89.43.3.229
Discovered open port 110/tcp on 89.43.3.229
Discovered open port 993/tcp on 89.43.3.229
Discovered open port 443/tcp on 89.43.3.229
Discovered open port 8080/tcp on 89.43.3.229
Discovered open port 995/tcp on 89.43.3.229
Discovered open port 3306/tcp on 89.43.3.229
Discovered open port 21/tcp on 89.43.3.229
Discovered open port 80/tcp on 89.43.3.229
Discovered open port 5900/tcp on 89.43.3.229
Discovered open port 111/tcp on 89.43.3.229
Discovered open port 554/tcp on 89.43.3.229
Discovered open port 1723/tcp on 89.43.3.229
Discovered open port 3389/tcp on 89.43.3.229
```

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -O -v 89.43.3.170
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 12:12 EDT
Initiating Ping Scan at 12:12
Scanning 89.43.3.170 [4 ports]
Completed Ping Scan at 12:12, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:12
Completed Parallel DNS resolution of 1 host. at 12:12, 1.35s elapsed
Initiating SYN Stealth Scan at 12:12
Scanning 170.mobinnet.net (89.43.3.170) [1000 ports]
Discovered open port 256/tcp on 89.43.3.170
Discovered open port 3306/tcp on 89.43.3.170
Discovered open port 53/tcp on 89.43.3.170
Discovered open port 23/tcp on 89.43.3.170
Discovered open port 8080/tcp on 89.43.3.170
Discovered open port 1025/tcp on 89.43.3.170
Discovered open port 1723/tcp on 89.43.3.170
Discovered open port 554/tcp on 89.43.3.170
Discovered open port 143/tcp on 89.43.3.170
Discovered open port 5900/tcp on 89.43.3.170
Discovered open port 139/tcp on 89.43.3.170
Discovered open port 80/tcp on 89.43.3.170
Discovered open port 1720/tcp on 89.43.3.170
Discovered open port 995/tcp on 89.43.3.170
Discovered open port 111/tcp on 89.43.3.170
Discovered open port 8888/tcp on 89.43.3.170
Discovered open port 3389/tcp on 89.43.3.170
Discovered open port 199/tcp on 89.43.3.170
Discovered open port 443/tcp on 89.43.3.170
Discovered open port 110/tcp on 89.43.3.170
Discovered open port 135/tcp on 89.43.3.170
```

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -O -v 89.43.3.65
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 12:11 EDT
Initiating Ping Scan at 12:11
Scanning 89.43.3.65 [4 ports]
Completed Ping Scan at 12:11, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:11
Completed Parallel DNS resolution of 1 host. at 12:11, 0.20s elapsed
Initiating SYN Stealth Scan at 12:11
Scanning 65.mobinnet.net (89.43.3.65) [1000 ports]
Discovered open port 199/tcp on 89.43.3.65
Discovered open port 23/tcp on 89.43.3.65
Discovered open port 135/tcp on 89.43.3.65
Discovered open port 1720/tcp on 89.43.3.65
Discovered open port 1723/tcp on 89.43.3.65
Discovered open port 111/tcp on 89.43.3.65
Discovered open port 554/tcp on 89.43.3.65
Discovered open port 80/tcp on 89.43.3.65
Discovered open port 1025/tcp on 89.43.3.65
Discovered open port 3389/tcp on 89.43.3.65
Discovered open port 139/tcp on 89.43.3.65
Discovered open port 110/tcp on 89.43.3.65
Discovered open port 256/tcp on 89.43.3.65
Discovered open port 22/tcp on 89.43.3.65
Discovered open port 53/tcp on 89.43.3.65
Discovered open port 21/tcp on 89.43.3.65
Discovered open port 5900/tcp on 89.43.3.65
Discovered open port 3306/tcp on 89.43.3.65
Discovered open port 8080/tcp on 89.43.3.65
Discovered open port 143/tcp on 89.43.3.65
Discovered open port 445/tcp on 89.43.3.65
```

- **گزارش UDP Scan**

این بخش پورت های مربوط به سرویس udp و سرویس‌های استفاده شده روی این پورت ها را بررسی میکند.

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -sU 89.43.3.229
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 12:26 EDT
Nmap scan report for 229.mobinnet.net (89.43.3.229)
Host is up (0.053s latency).
Not shown: 998 open|filtered udp ports (no-response)
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp

Nmap done: 1 IP address (1 host up) scanned in 1601.75 seconds
```

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -sU 89.43.3.170
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 12:27 EDT
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (0.00064s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT   STATE SERVICE
53/udp open  domain
123/udp open  ntp
Nmap done: 1 IP address (1 host up) scanned in 1585.89 seconds
```

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -sU 89.43.3.65
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 09:27 EDT
Nmap scan report for 65.mobinnet.net (89.43.3.65)
Host is up (0.0011s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT   STATE SERVICE
53/udp open  domain

Nmap done: 1 IP address (1 host up) scanned in 1605.78 seconds
```

میتوان دید که در اکثر دامنه‌ها پورتهای udp فیلتر میباشند .

- **گزارش Idle Scan**

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -sI 89.43.3.229
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On the other hand, timing info Nmap gains from pings can allow
for faster, more reliable scans.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 12:13 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.06 seconds
```

---

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -sI 89.43.3.170
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On the other hand, timing info Nmap gains from pings can allow
for faster, more reliable scans.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 12:13 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.07 seconds
```

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo nmap -sI 89.43.3.65
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On the other hand, timing info Nmap gains from pings can allow
for faster, more reliable scans.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-03 10:02 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.06 seconds
```

همانطور که می‌بینیم زامبی مناسبی برای اینکه بتوان حمله بروت فورس را بر روی دامین‌ها انجام داد، یافت نشد. این اسکن پیدا نشد.

- **گزارش Hping3**

این وسیله برای تست پینگ میباشد. همان طور که در میبینیم مثل بخش اول تمامی هاست‌ها را به درستی پینگ میکند . برای مثال به هاست 89.43.2.65 توجه کنید این هاست هم در این بخش و هم در بخش نخست قسمت ۱۰۰ درصد packet lossدارد . در واقع همانطور که مشاهده می شود نتیجه ای hping3با نتیجه ای که در بخش اول داشتیم مطابقت دارد پس ابزار به درستی کار می کند .

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo hping3
hping3> ping www.google.com -c 6
PING www.google.com (172.217.165.4) 56(84) bytes of data.
64 bytes from yyz12s06-in-f4.1e100.net (172.217.165.4): icmp_seq=1 ttl=128 time=207 ms
64 bytes from yyz12s06-in-f4.1e100.net (172.217.165.4): icmp_seq=2 ttl=128 time=215 ms
64 bytes from yyz12s06-in-f4.1e100.net (172.217.165.4): icmp_seq=3 ttl=128 time=213 ms
64 bytes from yyz12s06-in-f4.1e100.net (172.217.165.4): icmp_seq=4 ttl=128 time=204 ms
64 bytes from yyz12s06-in-f4.1e100.net (172.217.165.4): icmp_seq=5 ttl=128 time=222 ms
64 bytes from yyz12s06-in-f4.1e100.net (172.217.165.4): icmp_seq=6 ttl=128 time=230 ms

── www.google.com ping statistics ──
6 packets transmitted, 6 received, 0% packet loss, time 5011ms
rtt min/avg/max/mdev = 203.864/215.207/230.191/8.807 ms
```

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo hping3 -1 89.43.3.229 -c 6
HPING 89.43.3.229 (eth0 89.43.3.229): icmp mode set, 28 headers + 0 data bytes
len=46 ip=89.43.3.229 ttl=128 id=4924 icmp_seq=0 rtt=409.1 ms
len=46 ip=89.43.3.229 ttl=128 id=4925 icmp_seq=1 rtt=413.2 ms
len=46 ip=89.43.3.229 ttl=128 id=4926 icmp_seq=2 rtt=406.6 ms
len=46 ip=89.43.3.229 ttl=128 id=4927 icmp_seq=3 rtt=411.3 ms
len=46 ip=89.43.3.229 ttl=128 id=4928 icmp_seq=4 rtt=405.4 ms
len=46 ip=89.43.3.229 ttl=128 id=4929 icmp_seq=5 rtt=390.2 ms

── 89.43.3.229 hping statistic ──
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 390.2/406.0/413.2 ms
```

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo hping3 -1 89.43.3.170 -c 6
[sudo] password for kali:
HPING 89.43.3.170 (eth0 89.43.3.170): icmp mode set, 28 headers + 0 data bytes
len=46 ip=89.43.3.170 ttl=128 id=21695 icmp_seq=0 rtt=404.7 ms
len=46 ip=89.43.3.170 ttl=128 id=21697 icmp_seq=1 rtt=417.2 ms
len=46 ip=89.43.3.170 ttl=128 id=21698 icmp_seq=2 rtt=417.1 ms
len=46 ip=89.43.3.170 ttl=128 id=21699 icmp_seq=3 rtt=417.1 ms
len=46 ip=89.43.3.170 ttl=128 id=21700 icmp_seq=4 rtt=409.4 ms
len=46 ip=89.43.3.170 ttl=128 id=21702 icmp_seq=5 rtt=409.0 ms

── 89.43.3.170 hping statistic ──
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 404.7/412.4/417.2 ms
```

```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo hping3 -1 89.43.3.65 -c 6
[sudo] password for kali:
HPING 89.43.3.65 (eth0 89.43.3.65): icmp mode set, 28 headers + 0 data bytes

── 89.43.3.65 hping statistic ──
6 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

- **بررسی ابزار netdiscover**

Netdiscover ابزاری برای شناسایی هاست های فعال در یک شبکه است و پروتکل ARPرا شنود می کند

.با دستور ۱۹۲.۱۶۸.۱.۱/۱۶ netdiscover -r میتوان تمامی شبکه‌های روی ۱۹۲.۱۶۸.x.xرا با مشخصاتی همچون مک آدرس مشاهده کرد.

```
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     18:d2:76:6a:b5:ca     53    3180  Unknown vendor
192.168.1.2     50:b7:c3:f5:75:80      2     120  Samsung Electronics CO., LTD
192.168.1.5     00:1b:63:c5:3b:6c      1      60  Apple
192.168.1.150   08:00:27:6d:69:49      1      60  CADMUS COMPUTER SYSTEMS
192.168.1.151   08:00:27:7b:1f:c4      1      60  CADMUS COMPUTER SYSTEMS
```

البته در کل خروجی در این ابزار نداشتیم زیرا باید در شبکه لوکال مربوطه باشم بنابراین نتیجه‌ای نداریم.

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

0 Captured ARP Req/Rep packets, from 0 hosts.   Total size: 0
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
```

- **ابزار آنلاین**

- **گزارش Whatweb**

در دامنه میبینیم که اطلاعاتی مثل HTTPServer، IP وغیره میباشد .

```
┌──(kali㉿kali)-[~]
└─$ sudo whatweb 89.43.3.229
http://89.43.3.229 [200 OK] Country[ROMANIA][RO], HTTPServer[lighttpd/1.4.35], IP[89.43.3.229], PasswordField[password], Script[text/javascri
pt], Title[Setup Login], lighttpd[1.4.35]
```

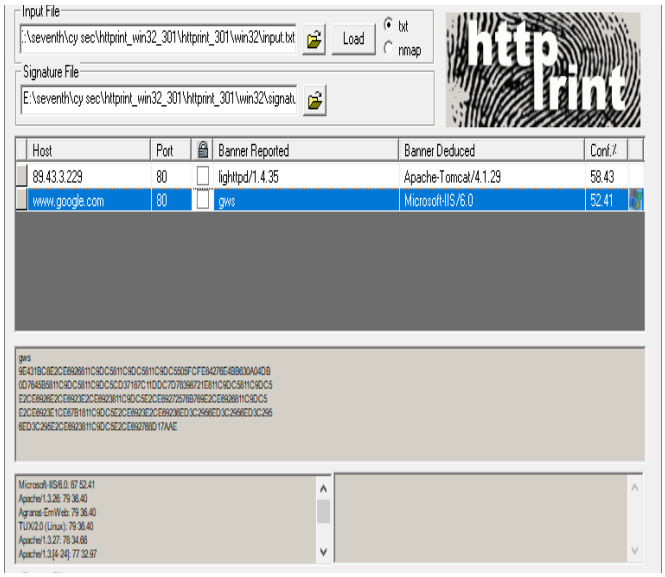
در این ابزار میتوان مشاهده کرد که به دلیل مشکل در وی‌پی‌ان تنها موفق به دریافت اطلاعات همه دامنه‌ها نشده‌ام.

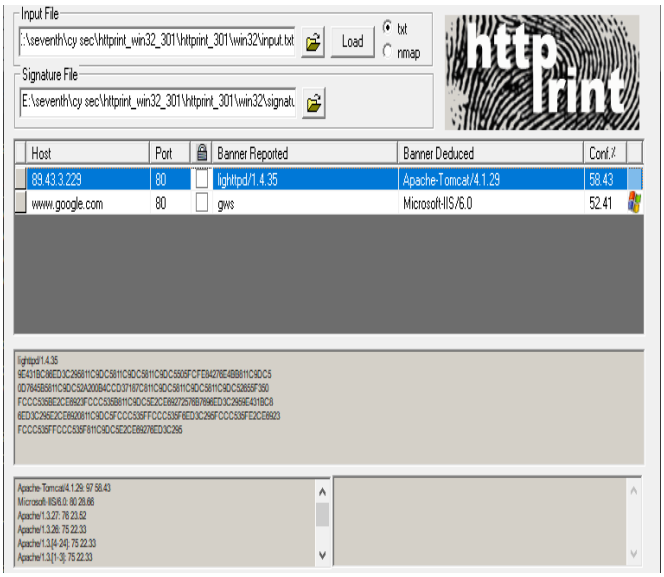
```
┌──(kali㉿kali)-[~/Desktop/Security]
└─$ sudo whatweb 89.43.3.170
ERROR Opening: http://89.43.3.170 - end of file reached
```

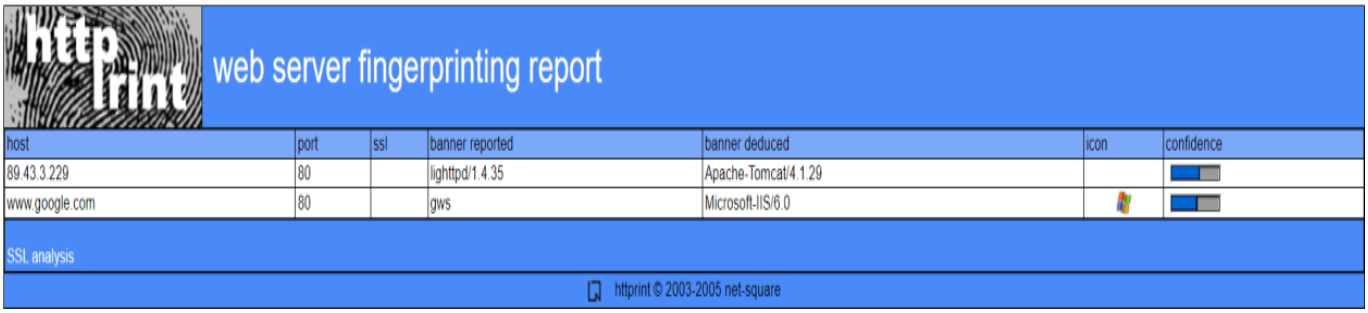
```
┌──(kali㉿kali)-[~]
└─$ sudo whatweb 89.43.3.65
[sudo] password for kali:
ERROR Opening: http://89.43.3.65 - end of file reached
```

## httprint -

با استفاده از httprint اطلاعات بیشتری از دو آدرس ۸۳.۴۹.۳.۲۲۹ و www.google.com بدست می‌آوریم که در ادامه اطلاعات بدست امده را در اسکرین‌شات‌های زیر مشاهده میکنیم .



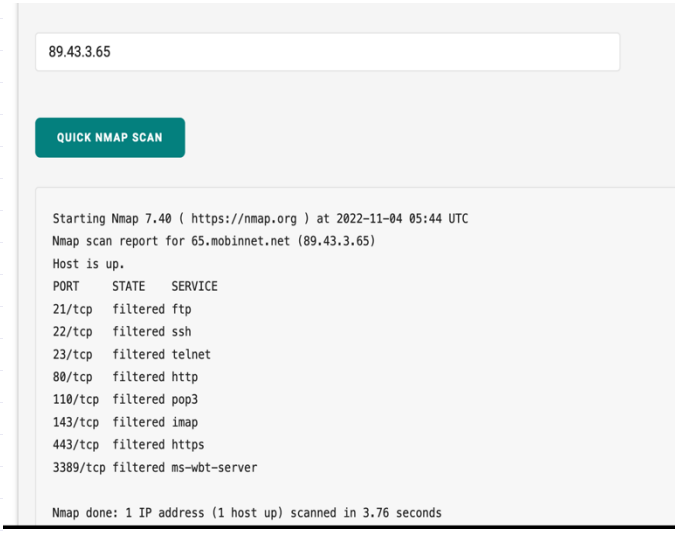



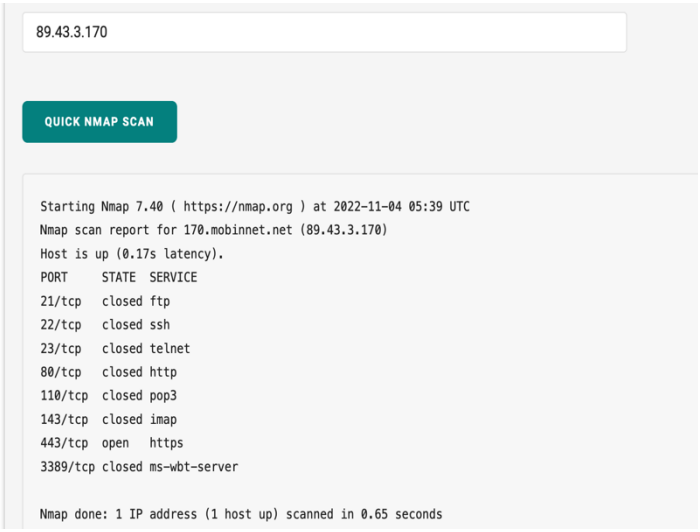



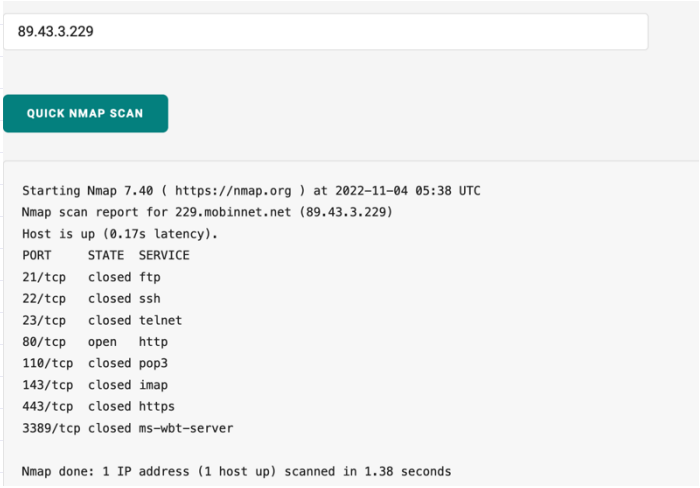
- **سایت‌های آنلاین**

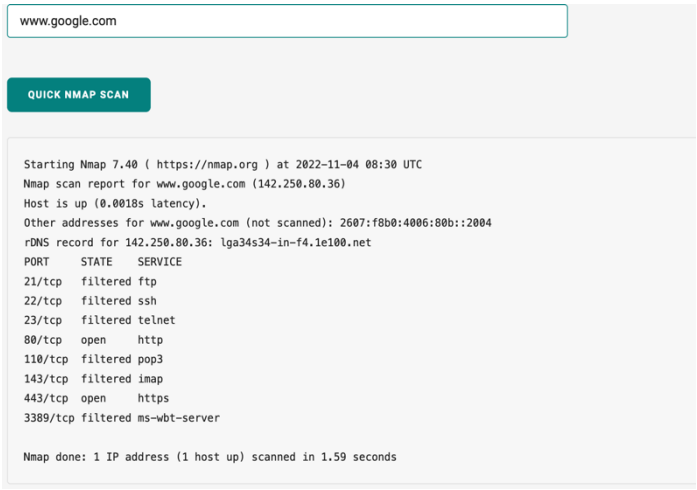
این به شما امکان می دهد اسکن سریعی را با اکثر ده پورت استاندارد زیر با اسکنر پورت NMAP میزبانی شده انجام دهید.

https://hackertarget.com/nmap-online-port-scanner/



## سایت whatweb.net

WhatWeb is a next generation web scanner.

WhatWeb recognises web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices.

WhatWeb has over 1800 plugins, each to recognise something different. WhatWeb also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.

Enter a domain to analyze:

89.43.3.229 Go

Download

Wiki

```
http://89.43.3.229 [200 OK] Country[ROMANIA][RO],
 HTTPServer[lighttpd/1.4.35],
 IP[89.43.3.229],
 PasswordField[password],
 Script[text/javascript],
 Title[Setup Login],
 lighttpd[1.4.35]
```

WhatWeb is a next generation web scanner.

WhatWeb recognises web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices.

WhatWeb has over 1800 plugins, each to recognise something different. WhatWeb also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.

Enter a domain to analyze:

www.google.com Go

Download

Wiki

```
http://www.google.com [200 OK] Cookies[1P_JAR,AEC,NID],
 Country[UNITED STATES][US],
 HTML5, HTTPServer[gws],
 HttpOnly[AEC,NID],
 IP[142.251.32.164],
 Script, Title[Google],
 X-Frame-Options[SAMEORIGIN],
 X-XSS-Protection[0]
```

WhatWeb is a next generation web scanner.

WhatWeb recognises web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices.

WhatWeb has over 1800 plugins, each to recognise something different. WhatWeb also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.

Enter a domain to analyze:

89.43.3.170 Go

Download

Wiki

```
The requested domain is unavailable. Please check the domain and try again.
```

WhatWeb is a next generation web scanner.

WhatWeb recognises web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices.

WhatWeb has over 1800 plugins, each to recognise something different. WhatWeb also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.

Enter a domain to analyze:

89.43.3.65 Go

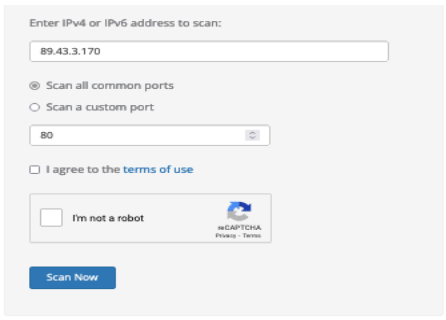
Download

Wiki

```
The requested domain is unavailable. Please check the domain and try again.
```

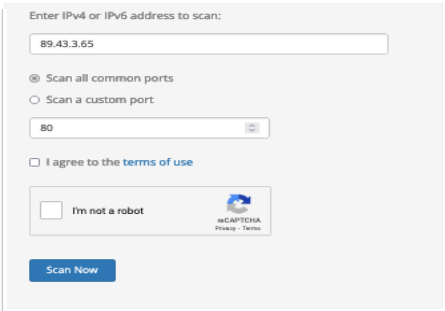
با این اسکنر پورت TCP آنلاین می توانید یک آدرس IP را برای پورت های باز اسکن کنید .از این ابزار اسکن پورت TCP برای بررسی اینکه چه سرویس‌های روی سرور شما اجرا می‌شوند، استفاده کنید، بررسی کنید که آیا فایروال شما درست کار می‌کند یا خیر، پورت‌های TCP باز را مشاهده کنید .این پورت اسکنر اسکن TCP را روی یک آدرس IP با استفاده از اسکنر پورت Nmap اجرا می کند IP هایی را که متعلق به شما نیست اسکن نکنید، این عمل ممکن است توسط سرویس های امنیتی فعال و مسدود شود.

https://www.ipvoid.com/port-scan/



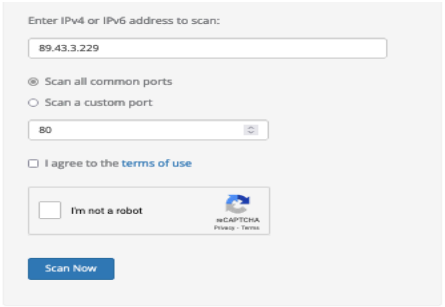

Port Scanning Results

| Port | Type | Status | Service |
|---|---|---|---|
| 21 | TCP | Closed | ftp |
| 22 | TCP | Closed | ssh |
| 23 | TCP | Closed | telnet |
| 25 | TCP | Closed | smtp |
| 53 | TCP | Closed | domain |
| 80 | TCP | Closed | http |
| 110 | TCP | Closed | pop3 |
| 111 | TCP | Closed | rpcbind |
| 135 | TCP | Closed | msrpc |
| 139 | TCP | Closed | netbios-ssn |
| 143 | TCP | Closed | imap |
| 389 | TCP | Closed | ldap |
| 443 | TCP | Open | https |
| 445 | TCP | Closed | microsoft-ds |
| 587 | TCP | Closed | submission |
| 1025 | TCP | Closed | NFS-or-IIS |
| 1080 | TCP | Closed | socks |
| 1433 | TCP | Closed | ms-sql-s |
| 2049 | TCP | Closed | nfs |
| 3306 | TCP | Closed | mysql |
| 3389 | TCP | Closed | ms-wbt-server |
| 5900 | TCP | Closed | vnc |
| 6001 | TCP | Closed | X11:1 |
| 6379 | TCP | Closed | redis |
| 8080 | TCP | Closed | http-proxy |
| 9001 | TCP | Closed | tor-orport |
| 9050 | TCP | Closed | tor-socks |




Port Scanning Results

| Port | Type | Status | Service |
|---|---|---|---|
| 21 | TCP | Filtered | ftp |
| 22 | TCP | Filtered | ssh |
| 23 | TCP | Filtered | telnet |
| 25 | TCP | Filtered | smtp |
| 53 | TCP | Filtered | domain |
| 80 | TCP | Filtered | http |
| 110 | TCP | Filtered | pop3 |
| 111 | TCP | Filtered | rpcbind |
| 135 | TCP | Filtered | msrpc |
| 139 | TCP | Filtered | netbios-ssn |
| 143 | TCP | Filtered | imap |
| 389 | TCP | Filtered | ldap |
| 443 | TCP | Filtered | https |
| 445 | TCP | Filtered | microsoft-ds |
| 587 | TCP | Filtered | submission |
| 1025 | TCP | Filtered | NFS-or-IIS |
| 1080 | TCP | Filtered | socks |
| 1433 | TCP | Filtered | ms-sql-s |
| 2049 | TCP | Filtered | nfs |
| 3306 | TCP | Filtered | mysql |
| 3389 | TCP | Filtered | ms-wbt-server |
| 5900 | TCP | Filtered | vnc |
| 6001 | TCP | Filtered | X11:1 |
| 6379 | TCP | Filtered | redis |
| 8080 | TCP | Filtered | http-proxy |
| 9001 | TCP | Filtered | tor-orport |
| 9050 | TCP | Filtered | tor-socks |




Port Scanning Results

| Port | Type | Status | Service |
|---|---|---|---|
| 21 | TCP | Closed | ftp |
| 22 | TCP | Closed | ssh |
| 23 | TCP | Closed | telnet |
| 25 | TCP | Closed | smtp |
| 53 | TCP | Closed | domain |
| 80 | TCP | Open | http |
| 110 | TCP | Closed | pop3 |
| 111 | TCP | Closed | rpcbind |
| 135 | TCP | Closed | msrpc |
| 139 | TCP | Closed | netbios-ssn |
| 143 | TCP | Closed | imap |
| 389 | TCP | Closed | ldap |
| 443 | TCP | Closed | https |
| 445 | TCP | Closed | microsoft-ds |
| 587 | TCP | Closed | submission |
| 1025 | TCP | Closed | NFS-or-IIS |
| 1080 | TCP | Closed | socks |
| 1433 | TCP | Closed | ms-sql-s |
| 2049 | TCP | Closed | nfs |
| 3306 | TCP | Closed | mysql |
| 3389 | TCP | Closed | ms-wbt-server |
| 5900 | TCP | Closed | vnc |
| 6001 | TCP | Closed | X11:1 |
| 6379 | TCP | Closed | redis |
| 8080 | TCP | Closed | http-proxy |
| 9001 | TCP | Closed | tor-orport |
| 9050 | TCP | Closed | tor-socks |