

## فهرست مطالب

۲	توضیح موارد پیاده‌سازی شده در بخش اول
۲	مورد شماره یک: گرفتن ping از آی‌پی خاص
۲	مورد شماره دو: اسکن یک محدوده آی‌پی و یافتن هاست‌های فعال
۳	مورد شماره سه: اسکن پورت‌های باز یک هاست فعال
۴	نمونه‌های خروجی از کدهای پیاده‌سازی شده توسط بخش اول
۴	نمونه‌های خروجی ping یک آی‌پی خاص
۵	نمونه‌های خروجی اسکن هاست‌های فعال یک محدوده مشخص
۸	نمونه‌های خروجی اسکن پورت‌های باز یک هاست فعال
۸	در کد پیاده‌سازی شده
۹	استفاده از ابزارهای معرفی شده در بخش دوم
۹	nmap
۱۱	netdiscover
۱۱	hping۳
۱۱	استفاده از ابزارهای آنلاین
۱۱	وبسایت <a href="http://ports.my-addr.com/ip-range-port-scanner-tool.php">http://ports.my-addr.com/ip-range-port-scanner-tool.php</a>
۱۲	وبسایت <a href="https://hackertarget.com/whatweb-scan/">https://hackertarget.com/whatweb-scan/</a>
۱۳	وبسایت <a href="https://www.ipfingerprints.com/portscan.php">https://www.ipfingerprints.com/portscan.php</a>
۱۳	وبسایت <a href="https://www.infobyip.com/">https://www.infobyip.com/</a>

## توضیح موارد پیاده‌سازی شده در بخش اول

### مورد شماره یک: گرفتن ping از آی‌پی خاص

برای این مورد در فایل ping.py تابع ping را تعریف می‌کنیم که به کمک کتابخانه OS می‌تواند عمل ping را انجام دهد. یکی از پارامترهای این تابع (علاوه بر آدرس ورودی و مقادیر مربوط به پارامترهای دستور پینگ) پارامتری تحت عنوان log دارد که در صورت true بودن آن، در فایل result\_ping.txt می‌توانیم اطلاعات مربوط به دستور ping را به همراه زمان دقیق اجرای دستور ذخیره کنیم. ساختار کلی این تابع به صورت زیر می‌باشد:

```
def ping(host, count=1, wait=-1, _print=False, log=False):

    # set number of packets
    count_param = '-c {}'.format(count) if platform.system().lower() != 'windows' else '-n {}'.format(count)

    # set waiting time
    wait_param = '' if wait == -1 else '-W {}'.format(wait)

    # making the command
    command = 'ping {}{}{}'.format(count_param, wait_param, host)
    if _print:
        print('> ' + command + '\n...')
    ping_result = os.popen(command).read()
    if log:
        log_ping(command, ping_result)
    return ping_result
```

و برای فراخوانی آن از روش زیر استفاده می‌کنیم:

```
ping(host=input('HOST : '), count=int(input('COUNT: ')), wait=-1, _print=True, log=True)
```

### مورد شماره دو: اسکن یک محدوده آی‌پی و یافتن هاست‌های فعال

شیوه کار این مورد از همان ping تعریف شده در مورد اول استفاده می‌کند:

```

def detect_active_hosts(range_start, range_end):
    active_hosts = []
    detecting_progress = tqdm(range(range_start[3], range_end[3] + 1))
    for i in detecting_progress:
        target_host = '{}.{}.{}.{}'.format(range_start[0], range_start[1], range_start[2], i)
        detecting_progress.set_description('PINGING {}'.format(target_host))
        response = ping(host=target_host, count=1, wait=0.5)
        if '1 packets transmitted, 1 packets received, 0.0% packet loss' in response:
            active_hosts.append(target_host)
    log_active_results(range_start, range_end, active_hosts)
    return active_hosts

```

کاربر ابتدا و انتهای بازه مورد نظر خود را به این تابع میدهد و در آن برای تمام آدرس‌های این بازه می‌تواند از ping استفاده کند. اگر ۵۰٪ زیر یک آدرس با موفقیت انجام شد، آن آدرس به عنوان یک هاست فعال شناخته می‌شود. نحوه فراخوانی این تابع نیز به صورت زیر می‌باشد:

```

detect_active_hosts(
    range_start=list(map(lambda x: int(x), input('START OF RANGE: ').strip().split('.'))),
    range_end=list(map(lambda x: int(x), input('END OF RANGE: ').strip().split('.')))
)

```

اطلاعات مربوط به هاست‌های فعال هر بازه با هر بار فراخوانی تابع در فایل result\_detect\_active\_hosts.txt ذخیره می‌شود.

## مورد شماره سه: اسکن پورت‌های باز یک هاست فعال

تابع مربوط به این بخش به صورت زیر می‌باشد:

```

def detect_open_ports(ip, range_start, range_end):
    open_ports = []
    port_detecting_progress = tqdm(range(range_start, range_end + 1))
    try:
        for port in port_detecting_progress:
            port_detecting_progress.set_description('checking port {}'.upper().format(port))
            s = socket()
            result = s.connect_ex((ip, port))
            if result == 0:
                open_ports.append(port)
            s.close()
        log_open_ports(ip, range_start, range_end, open_ports)

    except KeyboardInterrupt:
        print("\nanceled...".upper())
    except gaierror:
        print("\nHostname Could Not Be Resolved".upper())
    return open_ports

```

و فراخوانی آن نیز به فرم زیر انجام می‌شود:

```

    detect_open_ports(
        ip=input('TARGET IP ADDRESS: '),
        range_start=int(input('START OF RANGE : ')),
        range_end=int(input('END OF RANGE : '))
)

```

پورت‌های باز مربوط به هاست مورد نظر در فایل result\_detect\_open\_ports.txt ذخیره می‌شوند.

## نمونه‌های خروجی از کدهای پیاده‌سازی شده توسط بخش اول

### نمونه‌های خروجی ping یک آی‌پی خاص

به عنوان مثال ابتدا ping 89.43.3.66 و سپس google.com را می‌کنیم.

```

SELECT AN OPTION:
1) PING AND IP
2) PING AND IP RANGE AND SHOW ACTIVE HOSTS
3) SCAN OPEN PORTS OF AN ACTIVE HOST
-1) EXIT PROGRAM
1
HOST : google.com
COUNT: 1
> ping -c 2 google.com
...
PING google.com (142.250.180.46): 56 data bytes
64 bytes from 142.250.180.46: icmp_seq=0 ttl=51 time=37.239 ms
64 bytes from 142.250.180.46: icmp_seq=1 ttl=51 time=34.793 ms

--- google.com ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 34.793/36.016/37.239/1.223 ms

----- PING PROGRAM -----
SELECT AN OPTION:
1) PING AND IP
2) PING AND IP RANGE AND SHOW ACTIVE HOSTS
3) SCAN OPEN PORTS OF AN ACTIVE HOST
-1) EXIT PROGRAM
1
HOST : 89.43.3.66
COUNT: 1
> ping -c 1 89.43.3.66
...
PING 89.43.3.66 (89.43.3.66): 56 data bytes
64 bytes from 89.43.3.66: icmp_seq=0 ttl=49 time=42.449 ms

--- 89.43.3.66 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 42.449/42.449/42.449/0.000 ms

```

نتایج حاصل از این ping در فایل result\_ping.txt به صورت زیر ذخیره می‌شود:

```

-----
@ 2021-11-16 17:18:48.558032
> ping -c 2 google.com
PING google.com (142.250.180.46): 56 data bytes
64 bytes from 142.250.180.46: icmp_seq=0 ttl=51 time=37.239 ms
64 bytes from 142.250.180.46: icmp_seq=1 ttl=51 time=34.793 ms
--- google.com ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 34.793/36.016/37.239/1.223 ms
-----

@ 2021-11-16 17:19:12.254138
> ping -c 1 89.43.3.66
PING 89.43.3.66 (89.43.3.66): 56 data bytes
64 bytes from 89.43.3.66: icmp_seq=0 ttl=49 time=42.449 ms
--- 89.43.3.66 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 42.449/42.449/42.449/0.000 ms
-----
```

## نمونه‌های خروجی اسکن هاست‌های فعال یک محدوده مشخص

به عنوان نمونه ۱۰۰ عضو اول یکی از بازه‌های خواسته شده را بررسی می‌کنیم.

```

----- PING PROGRAM -----
SELECT AN OPTION:
 1) PING AND IP
 2) PING AND IP RANGE AND SHOW ACTIVE HOSTS
 3) SCAN OPEN PORTS OF AN ACTIVE HOST
 -1) EXIT PROGRAM
2
START OF RANGE: 89.43.3.0
END OF RANGE: 89.43.3.100
PINGING 89.43.3.100: 100%|██████████| 101/101 [01:25<00:00,  1.18it/s]

21 ACTIVE HOST(S):
✓ 89.43.3.66
✓ 89.43.3.67
✓ 89.43.3.68
✓ 89.43.3.69
✓ 89.43.3.70
✓ 89.43.3.75
✓ 89.43.3.76
✓ 89.43.3.77
✓ 89.43.3.80
✓ 89.43.3.81
✓ 89.43.3.82
✓ 89.43.3.85
✓ 89.43.3.87
✓ 89.43.3.88
✓ 89.43.3.89
✓ 89.43.3.92
✓ 89.43.3.95
✓ 89.43.3.96
✓ 89.43.3.97
✓ 89.43.3.98
✓ 89.43.3.100
```

در همین حین داخل فایل لگ مربوط به این بخش نیز این اطلاعات ذخیره می‌شود.

```

-----  

@ 2021-11-16 16:57:28.748575  

ACTIVE HOSTS IN RANGE [89.43.3.0 - 89.43.3.100]:  

✓ 89.43.3.66  

✓ 89.43.3.67  

✓ 89.43.3.68  

✓ 89.43.3.69  

✓ 89.43.3.70  

✓ 89.43.3.75  

✓ 89.43.3.76  

✓ 89.43.3.77  

✓ 89.43.3.80  

✓ 89.43.3.81  

✓ 89.43.3.82  

✓ 89.43.3.85  

✓ 89.43.3.87  

✓ 89.43.3.88  

✓ 89.43.3.89  

✓ 89.43.3.92  

✓ 89.43.3.95  

✓ 89.43.3.96  

✓ 89.43.3.97  

✓ 89.43.3.98  

✓ 89.43.3.100  

-----  


```

سپس تمام بازه ها را بررسی می کنیم:

```

----- PING PROGRAM -----  

SELECT AN OPTION:  

  1) PING AND IP  

  2) PING AND IP RANGE AND SHOW ACTIVE HOSTS  

  3) SCAN OPEN PORTS OF AN ACTIVE HOST  

 -1) EXIT PROGRAM  

2  

START OF RANGE: 89.43.2.0  

END OF RANGE: 89.43.2.255  

PINGING 89.43.2.255: 100% [██████] 256/256 [04:19<00:00,  1.01s/it]  

0 ACTIVE HOST(S):  


```

```
----- PING PROGRAM -----
SELECT AN OPTION:
 1) PING AND IP
 2) PING AND IP RANGE AND SHOW ACTIVE HOSTS
 3) SCAN OPEN PORTS OF AN ACTIVE HOST
 -1) EXIT PROGRAM
2
START OF RANGE: 89.43.3.8
END OF RANGE: 89.43.3.255
PINGING 89.43.3.255: 100%|██████████| 256/256 [03:42<00:00,  1.15it/s]

62 ACTIVE HOST(S):
✓ 89.43.3.66
✓ 89.43.3.67
✓ 89.43.3.68
✓ 89.43.3.69
✓ 89.43.3.70
✓ 89.43.3.72
✓ 89.43.3.74
✓ 89.43.3.75
✓ 89.43.3.76
✓ 89.43.3.77
✓ 89.43.3.78
✓ 89.43.3.81
✓ 89.43.3.82
✓ 89.43.3.85
✓ 89.43.3.88
✓ 89.43.3.89
✓ 89.43.3.90
✓ 89.43.3.92
✓ 89.43.3.93
✓ 89.43.3.95
✓ 89.43.3.96
✓ 89.43.3.97
✓ 89.43.3.98
```

```
----- PING PROGRAM -----
SELECT AN OPTION:
 1) PING AND IP
 2) PING AND IP RANGE AND SHOW ACTIVE HOSTS
 3) SCAN OPEN PORTS OF AN ACTIVE HOST
 -1) EXIT PROGRAM
2
START OF RANGE: 89.43.4.8
END OF RANGE: 89.43.4.255
PINGING 89.43.4.255: 100%|██████████| 256/256 [03:37<00:00,  1.18it/s]

49 ACTIVE HOST(S):
✓ 89.43.4.5
✓ 89.43.4.6
✓ 89.43.4.13
✓ 89.43.4.14
✓ 89.43.4.19
✓ 89.43.4.25
✓ 89.43.4.34
✓ 89.43.4.37
✓ 89.43.4.38
✓ 89.43.4.41
✓ 89.43.4.49
✓ 89.43.4.50
✓ 89.43.4.54
✓ 89.43.4.58
✓ 89.43.4.73
✓ 89.43.4.74
✓ 89.43.4.82
✓ 89.43.4.89
✓ 89.43.4.90
✓ 89.43.4.98
✓ 89.43.4.100
✓ 89.43.4.101
✓ 89.43.4.114
```

## نمونه‌های خروجی اسکن پورت‌های باز یک هاست فعال

برای تست پورت‌های فعال خروجی کد پیاده‌سازی شده و nmap را با هم مقایسه می‌کنیم. برای این کار پورت‌های ۱ تا ۱۰۰۰ هاست 89.43.3.170 را مورد بررسی قرار میدهیم.

### در کد پیاده سازی شده

برای انجام این کار به صورت زیر عمل می‌کنیم:

```
----- PING PROGRAM -----
SELECT AN OPTION:
1) PING AND IP
2) PING AND IP RANGE AND SHOW ACTIVE HOSTS
3) SCAN OPEN PORTS OF AN ACTIVE HOST
-1) EXIT PROGRAM
3
TARGET IP ADDRESS: 89.43.3.170
START OF RANGE : 1
END OF RANGE : 1000
CHECKING PORT 1000: 100% [██████████] 1000/1000 [00:45<00:00, 22.20it/s]

6 OPEN PORT(S):
✓ 21
✓ 22
✓ 23
✓ 53
✓ 80
✓ 443
```

در این حالت نیز پورت‌های باز به صورت زیر می‌باشد:

- ۲۱
- ۲۲
- ۲۳
- ۵۳
- ۸۰
- ۴۴۳

داخل فایل result\_detect\_open\_ports.txt نیز خروجی به صورت زیر به انتهای فایل اضافه می‌شود:

```
15 -----
16 @ 2021-11-16 13:52:45.718225
17 HOST 89.43.3.170 OPEN PORTS FROM 1 TO 1000:
18 ✓ 21
19 ✓ 22
20 ✓ 23
21 ✓ 53
22 ✓ 80
23 ✓ 443
24 -----
```

## استفاده از ابزارهای معرفی شده در بخش دوم

### nmap

برای اسکن‌های مختلف به صورت زیر عمل می‌کنیم:

#### TCP full scan

```
Amirhossein-Macbook-Pro:~ tapsi$ nmap -sT 89.43.3.170
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-16 16:04 +0330
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (0.036s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
53/tcp    open     domain
80/tcp    open     http
443/tcp   open     https
1723/tcp  open     pptp
2000/tcp  open     cisco-sccp
5060/tcp  open     sip
8008/tcp  open     http
8010/tcp  open     xmpp
8291/tcp  filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 3.62 seconds
```

#### Stealth scan

برای این کار به دسترسی root نیاز خواهیم داشت.

```
Amirhossein-Macbook-Pro:~ tapsi$ sudo nmap -sS 89.43.3.170
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-16 16:06 +0330
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (0.026s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
53/tcp    open     domain
80/tcp    open     http
443/tcp   open     https
1723/tcp  open     pptp
2000/tcp  open     cisco-sccp
5060/tcp  open     sip
8008/tcp  open     http
8010/tcp  open     xmpp
8291/tcp  filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 3.30 seconds
```

#### UDP scan

```
Amirhossein-Macbook-Pro:~ tapsi$ sudo nmap -sU 89.43.3.170
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-16 16:36 +0330
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (0.024s latency).
Not shown: 995 closed udp ports (port-unreach)
PORT      STATE    SERVICE
53/udp   open|filtered domain
67/udp   open|filtered dhcps
1701/udp open     L2TP
1900/udp open|filtered upnp
5060/udp open|filtered sip

Nmap done: 1 IP address (1 host up) scanned in 59.65 seconds
```

## Fingerprint scan

```
Amirhossein-Macbook-Pro:~ tapsi$ sudo nmap -sF 89.43.3.170
Password:
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-16 16:14 +0330
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (0.0059s latency).
All 1000 scanned ports on 170.mobinnet.net (89.43.3.170) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.33 seconds
```

## Idle scan

```
Amirhossein-Macbook-Pro:~ tapsi$ 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 2021-11-16 16:16 +0330
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.08 seconds
```

در این مد مهاجم بسته‌های جعلی را به هاست با ترافیک بسیار کم (زامبی) ارسال می‌کند. این اسکن برای هر پورت ابتدا شناسه IP زامبی را ضبط می‌کند سپس بعد از ارسال یک بسته SYN جعلی به قربانی، مجدداً شناسه‌ی آن را بررسی می‌کند. اگر شناسه یک افزایش داشته باشد یعنی پورت باز نیست و اگر دو افزایش داشته باشد یعنی پورت باز است.

با مقایسه‌ی این پورت‌های گفته شده در نتیجه‌ی کد پیاده‌سازی شده با پورت‌های محدوده ۱ تا ۱۰۰۰ مربوط به scan می‌توانیم نتیجه بگیریم اسکن ما به درستی انجام شده است.

همچنین در Zenmap می‌توان اطلاعات مربوط به این هاست را به صورت زیر بدست آورد:

The screenshot shows the Zenmap interface with the following details for the host 170.mobinnet.net (89.43.3.170):

- Host Status:** State: up, Open ports: 6, Filtered ports: 0, Closed ports: 994, Scanned ports: 1000, Up time: 526634, Last boot: Wed Nov 10 11:36:34 2021. It features icons of two penguins and a yellow box.
- Addresses:** IPv4: 89.43.3.170, IPv6: Not available, MAC: Not available.
- Hostnames:** Name - Type: 170.mobinnet.net - PTR.
- Operating System:** Name: Linux 3.2 - 3.8, Accuracy: 98%.
- Sequence Analysis:**
  - Ports used
  - OS Classes
  - TCP Sequence
  - IP ID Sequence
  - TCP TS Sequence
  - Comments

## netdiscover

به کمک این ابزار می‌توان بازه آدرس‌های فعال را پیدا کرد. برای این کار از دستور `netdiscover -r XXX.XX/X` میتوانیم استفاده کنیم. به عنوان مثال برای بازه `localhost` خواهیم داشت:

```
Amirhossein-Macbook-Pro:Desktop tapsi$ netdiscover -r 192.168.0.0/16
Currently scanning: Finished! | Screen View: Unique Hosts

14 Captured ARP Req/Rep packets, from 3 hosts. Total size: 852
-----  

IP          At MAC Address      Count      Len  MAC Vendor / Hostname  

-----  

10.100.50.132 8c:a9:82:e0:ab:f0    10     600  Intel Corporate  

10.100.50.112 9a:e3:d4:35:21:24     3      192  Unknown vendor  

10.100.50.67   0c:8f:ff:5c:6d:4a     1       60  HUAWEI TECHNOLOGIES CO.,LTD
```

## hping³

به کمک این ابزار می‌توان عمل ping را تست کرد. در این بخش google.com را باری دیگر مورد بررسی قرار می‌دهیم:

```
Amirhossein-Macbook-Pro:Desktop tapsi$ sudo hping3 --tracerout -V -1 google.com
using wlp2s0, addr: 10.100.50.147, MTU: 1500
HPING google.com (wlp2s0 172.217.169.238): icmp mode set, 28 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=10.100.50.1 name=_gateway
hop=1 hoprtt=12.0 ms
hop=2 TTL 0 during transit from ip=10.10.10.2 name=UNKNOWN
hop=2 hoprtt=7.7 ms
hop=3 TTL 0 during transit from ip=81.91.147.225 name=UNKNOWN
hop=3 hoprtt=23.5 ms
hop=4 TTL 0 during transit from ip=172.25.2.181 name=UNKNOWN
hop=4 hoprtt=51.2 ms
hop=5 TTL 0 during transit from ip=172.21.2.182 name=UNKNOWN
hop=5 hoprtt=27.1 ms
hop=6 TTL 0 during transit from ip=172.21.2.185 name=UNKNOWN
hop=6 hoprtt=11.0 ms
hop=7 TTL 0 during transit from ip=172.20.21.173 name=UNKNOWN
hop=7 hoprtt=14.9 ms
hop=8 TTL 0 during transit from ip=172.20.40.34 name=UNKNOWN
hop=8 hoprtt=18.4 ms
hop=9 TTL 0 during transit from ip=172.17.2.81 name=UNKNOWN
hop=9 hoprtt=6.1 ms
hop=10 TTL 0 during transit from ip=10.202.6.14 name=UNKNOWN
hop=10 hoprtt=17.6 ms
hop=11 TTL 0 during transit from ip=10.201.47.186 name=UNKNOWN
hop=11 hoprtt=25.2 ms
hop=12 TTL 0 during transit from ip=10.21.21.10 name=UNKNOWN
hop=12 hoprtt=20.4 ms
hop=13 TTL 0 during transit from ip=134.0.220.186 name=UNKNOWN
hop=13 hoprtt=43.9 ms
^C
--- google.com hping statistic ---
15 packets transmitted, 13 packets received, 14% packet loss
round-trip min/avg/max = 6.1/21.5/51.2 ms
```

## استفاده از ابزارهای آنلاین

### [وبسایت](http://ports.my-addr.com/ip-range-port-scanner-tool.php)

این وبسایت می‌تواند پورت مخصوصی از یک رنج آدرس را اسکن کند. به علت فیلتر شدن، تمامی این پورت‌ها بسته معرفی می‌باشند:



## [وبسایت](https://hackertarget.com/whatweb-scan/)

این وبسایت اطلاعات مربوط به آدرس هاستهای ورودی خود را در صورت وجود داشتن یا دسترسی در اختیار ما قرار می‌دهد.

The screenshot shows the 'Hackertarget' website interface. At the top, there is a navigation bar with links for SCANNERS, TOOLS, RESEARCH, SERVICES, ABOUT, PRICING, and LOG IN. Below the navigation bar, there is a list of targets:

- 89.43.3.170
- 89.43.2.20
- 185.211.88.131
- 142.250.180.46

On the right side, there is a section titled 'Valid Target(s)' with the following information:

- www.example.com
- https://example.com/
- 192.16.1.1

A note below the targets states: "This is a passive scan that does not send intrusive requests to the target."

Under the 'SELECT ANALYSIS TOOL' dropdown, 'Passive Web Site Analysis (WhatWeb)' is selected. A 'Start Scan' button is located below the dropdown.

The main content area displays the results of the scan:

```

http://185.211.88.131 [403 Forbidden] Apache, HTTPServer[Apache], IP[185.211.88.131], Title[403 Forbidden]

http://142.250.180.46 [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[gws], IP[142.250.180.46], RedirectLocation[http://www.google.com/], Title[301 Moved], UncommonHeaders[bfccache-opt-in], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]

http://www.google.com/ [200 OK] Cookies[1P_JAR], Country[UNITED STATES][US], Email[robert@broofa.com], HTML5, HTTPServer[gws], IP[142.250.98.103], Script, Title[Google], UncommonHeaders[bfccache-opt-in], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]

http://89.43.2.20 [ Unassigned]

http://89.43.3.170 [200 OK] Country[ROMANIA][RO], IP[89.43.3.170], MikroTik-RouterOS[6.48.3][Telnet], PasswordField, Script, Title[RouterOS router configuration page]

```

## وبسایت <https://www.ipfingerprints.com/portscan.php>

در این قسمت می‌توان آدرس هاست مورد نظر را وارد کرد و نتایج را مشاهده کرد:

89.43.3.170 Start Port: 0 End Port: 100 Scan  
 Normal  Advance

Note: Host seems down. If it is really up, but blocking our ping probes, try "Don't Ping" in advance mode.

همانگونه که گفته شده اگر از پروتکلی به غیر از ICMP برای شناسایی آن استفاده کنیم نتیجه متفاوت خواهد بود:

89.43.3.170 Start Port: 0 End Port: 100 Scan  
 Normal  Advance

**Scan Type:**  
 connect()  SYN Stealth  NULL Stealth  FIN Stealth  XMAS Scan  ACK Scan  Window Scan

**Ping Type:**  
 TCP & ICMP  ICMP  TCP  Don't Ping

**General Options:**  
 UDP Scan  Detect OS  Fragment Packets

Host is up.  
All 100 scanned ports on 170.mobinnet.net (89.43.3.170) are filtered

## وبسایت <https://www.infobyip.com/>

این سایت اطلاعات خیلی کاملی از آدرس مورد نظر در اختیار ما قرار می‌دهد.

89.43.3.170

**IP: 89.43.3.170**

IP data	
Domain	170.mobinnet.net
ISP	Mobin Net Communication Company (Private Joint Stock)
ASN	50810
Tools	<a href="#">whois</a> <a href="#">ping</a> <a href="#">traceroute</a> <a href="#">mtr</a> <a href="#">dns</a>



Get info

**Geographical Data**

Continent	Asia (AS)
Country	 Iran (IR)
Lat / Long	35.698 / 51.4115

Location



Antipode



**IP representations**

Decimal	1495991210
Binary	01011001 00101011 00000011 10101010
Hex	0x592b03aa

**IP online tools**

Whois	<a href="#">whois 89.43.3.170</a>
Ping	<a href="#">ping 89.43.3.170</a>
Traceroute	<a href="#">traceroute 89.43.3.170</a>
MTR report	<a href="#">mtr report 89.43.3.170</a>
DNS records	<a href="#">DNS lookup 89.43.3.170</a>
Check spam databases	<a href="#">stopforumspam</a> <a href="#">spamhaus</a>