
# به نام خدا

## دانشکده مهندسی کامپیوتر

## گزارش تمرین عملی اول

## درس: مبانی امنیت اطلاعات

**دانشجو: فرشید نوشی – ۹۸۳۱۰۶۸**

# بخش اول

## قسمت اول

برای این بخش با استفاده از زبان پایتون اسکریپتی برای گرفتن پینگ نوشته شد که خروجی به صورت زیر میباشد.

```
 ____  _                    _              _
|  _ \(_)_ __   __ _    ___| |__   ___  ___| | _____ _ __
| |_) | | '_ \ / _` |  / __| '_ \ / _ \/ __| |/ / _ \ '__|
|  __/| | | | | (_| | | (__| | | |  __/ (__|   <  __/ |
|_|   |_|_| |_|\__, |  \___|_| |_|\___|\___|_|\_\___|_|
               |___/

IP/Domain: google.com
PING google.com (172.217.167.78): 56 data bytes
64 bytes from 172.217.167.78: icmp_seq=0 ttl=119 time=445.234 ms
64 bytes from 172.217.167.78: icmp_seq=1 ttl=119 time=634.285 ms
64 bytes from 172.217.167.78: icmp_seq=2 ttl=119 time=859.095 ms

--- google.com ping statistics ---
4 packets transmitted, 3 packets received, 25.0% packet loss
round-trip min/avg/max/stddev = 445.234/646.205/859.095/169.168 ms
IP/Domain: 172.217.167.78
PING 172.217.167.78 (172.217.167.78): 56 data bytes
64 bytes from 172.217.167.78: icmp_seq=0 ttl=119 time=611.779 ms
64 bytes from 172.217.167.78: icmp_seq=1 ttl=119 time=444.501 ms
Request timeout for icmp_seq 2

--- 172.217.167.78 ping statistics ---
4 packets transmitted, 2 packets received, 50.0% packet loss
round-trip min/avg/max/stddev = 444.501/528.140/611.779/83.639 ms
```

**قسمت دوم**

برای این قسمت اسکریپتی نوشته شده است که با اسکن یک محدوده آی پی و یافتن هاست‌های فعال آن‌ها را به ما برمیگرداند. برای اینجا از آی پی 89.43.4.0-255 اسکن انجام داده‌ایم (با استفاده از subnet=24)

خروجی نیز در زیر آورده شده است که همانطور که مشاهده میکنید ۲۵۶ هاست فعال هستند.

```
  ___ ____     ____
 |_ _|  _ \   / ___|  ___ __ _ _ __   _ __    ___ _ __
  | || |_) | \___ \ / __/ _` | '_ \| '_ \ / _ \ '__|
  | ||  __/   ___) | (_| (_| | | | | | | |  __/ |
 |___|_|      |____/ \___\__,_|_| |_|_| |_|\___|_|


Address: 89.43.4.0
Subnet: 24
89.43.4.0: UP
89.43.4.1: UP
89.43.4.10: UP
89.43.4.100: UP
89.43.4.101: UP
89.43.4.102: UP
89.43.4.103: UP
89.43.4.104: UP
89.43.4.105: UP
89.43.4.106: UP
89.43.4.107: UP
89.43.4.108: UP
89.43.4.109: UP
89.43.4.11: UP
```

```
89.43.4.84: UP
89.43.4.85: UP
89.43.4.86: UP
89.43.4.87: UP
89.43.4.88: UP
89.43.4.89: UP
89.43.4.9: UP
89.43.4.90: UP
89.43.4.91: UP
89.43.4.92: UP
89.43.4.93: UP
89.43.4.94: UP
89.43.4.95: UP
89.43.4.96: UP
89.43.4.97: UP
89.43.4.98: UP
89.43.4.99: UP
Scan results saved to                          University/Information Security/Proj 1/results/result_ip scan.txt
Total number of results: 256
```

**قسمت سوم**

اسکن پورت‌های فعال یک هاست باز نیز با استفاده از یک اسکریپت به زبان پایتون نوشته شده است و خروجی نمونه اش در زیر نمایش داده شده است. لازم به ذکر است که برای اجرا و کارکردن با تمامی سه اسکریپت گفته شده در این تمرین لازم است که براساس فایل requirements.txt که فایل ارسالی وجود دارد محیط venv برای زبان پایتون بسازید و فایل اسکریپت مربوط به هر بخش تمرین را اجرا کرده و در محیط ترمینال به آن ورودی مربوط را بدهید. در این بخش دو تصویر آمده اند که مربوط به استفاده از vpn و بدون استفاده از vpn هستند. تصویر اول بدون وی پی ان میباشد و دومی با وی پی ان.

```
 ____           _     ____
|  _ \ ___  _ __| |_  / ___|  ___ __ _ _ __  _ __   ___ _ __
| |_) / _ \| '__| __| \___ \ / __/ _` | '_ \| '_ \ / _ \ '__|
|  __/ (_) | |  | |_   ___) | (_| (_| | | | | | | |  __/ |
|_|   \___/|_|   \__| |____/ \___\__,_|_| |_|_| |_|\___|_|


Host IP: 89.43.3.170
Start port: 1
last port: 200
state of the host(): up
protocol: tcp
port: 1, state: closed, service: tcpmux
port: 19, state: closed, service: chargen
open port: 80, service: http
port: 136, state: closed, service: profile
port: 137, state: closed, service: netbios-ns
port: 138, state: closed, service: netbios-dgm
port: 139, state: closed, service: netbios-ssn

Process finished with exit code 0
 ____           _     ____
|  _ \ ___  _ __| |_  / ___|  ___ __ _ _ __  _ __   ___ _ __
| |_) / _ \| '__| __| \___ \ / __/ _` | '_ \| '_ \ / _ \ '__|
|  __/ (_) | |  | |_   ___) | (_| (_| | | | | | | |  __/ |
|_|   \___/|_|   \__| |____/ \___\__,_|_| |_|_| |_|\___|_|


Host IP: 89.43.3.170
Start port: 1
last port: 200
state of the host(170.mobinnet.net): up
protocol: tcp
port: 25, state: closed, service: smtp
open port: 80, service: http
```

## بخش دوم

با ابزارهای nmap، netdiscover و hping 3 به همراه یک ابزار آنلاین موارد خواسته شده را انجام دادیم.

```
farshid @ farshids-MacBook-Pro: ~
$ sudo nmap -sn 89.43.4.0-255
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-06 18:55 +0330
Nmap scan report for 89.43.4.0
Host is up (0.098s latency).
Nmap scan report for 89.43.4.1
Host is up (0.063s latency).
Nmap scan report for 89.43.4.2
Host is up (0.062s latency).
Nmap scan report for 89.43.4.3
Host is up (0.062s latency).
Nmap scan report for 89.43.4.4
Host is up (0.062s latency).
Nmap scan report for 89.43.4.5
Host is up (0.069s latency).
Nmap scan report for 89.43.4.6
Host is up (0.069s latency).
Nmap scan report for 89.43.4.7
Host is up (0.069s latency).
Nmap scan report for 89.43.4.8
Host is up (0.066s latency).
Nmap scan report for 89.43.4.9
Host is up (0.068s latency).
Nmap scan report for 89.43.4.252
Host is up (0.032s latency).
Nmap scan report for 89.43.4.253
Host is up (0.030s latency).
Nmap scan report for 89.43.4.254
Host is up (0.032s latency).
Nmap scan report for 89.43.4.255
Host is up (0.032s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 3.20 seconds
```

خروجی مانند کد است.

**اسکن پورت**

NMAP TCP Full Scan

با استفاده از آرگومان -sT کار را انجام میدهیم.

```
farshid @ farshids-MacBook-Pro: ~
$ sudo nmap -sT 89.43.3.170
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-06 18:58 +0330
Nmap scan report for 89.43.3.170
Host is up (0.011s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
1/tcp    closed tcpmux
19/tcp   closed chargen
25/tcp   closed smtp
80/tcp   open   http
135/tcp  closed msrpc
139/tcp  closed netbios-ssn
445/tcp  closed microsoft-ds
593/tcp  closed http-rpc-epmap
5555/tcp closed freeciv

Nmap done: 1 IP address (1 host up) scanned in 91.00 seconds
```

همانطور که میبینیم خروجی‌ها یکسان هستند. تصویر زیر نیز با وی پی ان است که مانند کد خروجی داده است.

```
farshid @ farshids-MacBook-Pro: ~
$ sudo nmap -sT 89.43.3.170
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-06 19:06 +0330
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (0.26s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE  SERVICE
25/tcp   closed smtp
80/tcp   open   http
443/tcp  open   https
465/tcp  closed smtps
587/tcp  closed submission
5060/tcp open   sip
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 275.41 seconds
```

**NMAP Stealth Scan**

اسکن مخفی نیز یکی از روش‌های اسکن هست که در آن مهاجم میخواهد که عملیات اسکن شدنش از دید فایروال و سیستم‌های اهراز هویت دور بماند و مشخص نشود که دارد اسکن انجام میدهد. روش کلی به این صورت است که به مانند ترافیک عادی شبکه اسکن پورت‌ها انجام می‌شوند.

```
farshid @ farshids-MacBook-Pro: ~
$ sudo nmap -sS 89.43.3.170
Password:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-06 19:13 +0330
Nmap scan report for 89.43.3.170
Host is up (0.043s latency).
Not shown: 991 filtered tcp ports (no-response), 8 filtered tcp ports (admin-prohibited)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 9.01 seconds

farshid @ farshids-MacBook-Pro: ~
$ sudo nmap -sS 89.43.3.170
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-06 19:14 +0330
Nmap scan report for 89.43.3.170
Host is up (0.025s latency).
Not shown: 993 filtered tcp ports (no-response), 6 filtered tcp ports (admin-prohibited)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 5.42 seconds
```

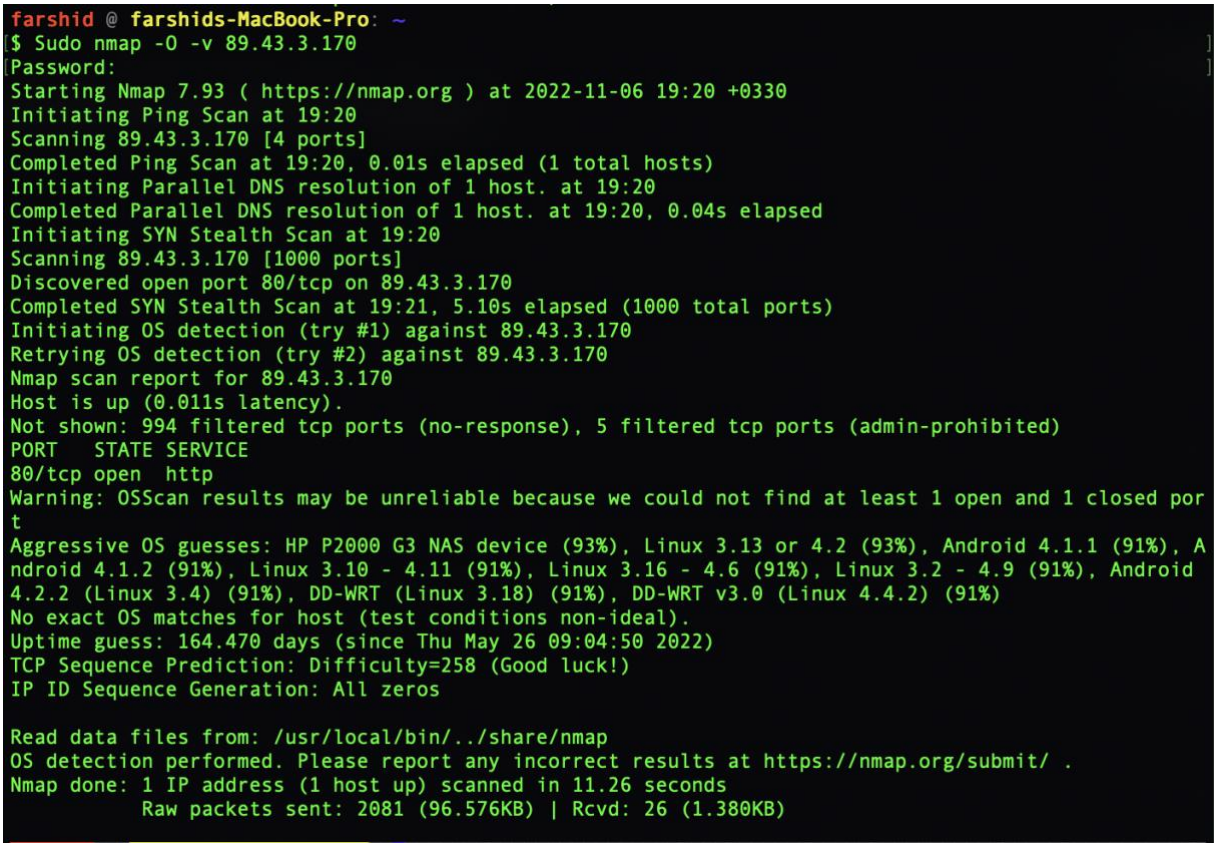
**NMAP UDP Scan**

در این اسکن یک بسته با پروتکل udp برای هر پورت ارسال میشود. در اغلب پورت‌ها این پروتکل بسته بود. برای برخی پورت‌ها یک بسته مخصوص این پروتکل ارسال میشود اما دراینجا همه پورت‌ها همانگونه که در تصویر مشخص است بسته بودند.

```
farshid @ farshids-MacBook-Pro: ~
$ sudo nmap -sU 89.43.3.170
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-06 19:31 +0330
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds

farshid @ farshids-MacBook-Pro: ~
$ sudo nmap -sU 89.43.3.170 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-06 19:33 +0330
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up.
All 1000 scanned ports on 170.mobinnet.net (89.43.3.170) are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 202.70 seconds
```

**NMAP Fingerprint Scan**

در این نوع اسکن همانطور که مشاهده میشود اطلاعات سیستم‌عامل و پورت‌ها و انواع سرویس‌ها نشان داده می‌شوند.




**NMAP IDLE Scan**

در این روش دریافت اطلاعات مهاجم بدون لو دادن ip دستگاه خودش به قربانی حمله میکند. این کار با یک کانال جانبی انجام میشود که دستگاه سوم که آن نیز یک قربانی است بدون اطلاع درحال کمک به مهاجم برای انجام حمله می‌باشد. در این روش گزارش‌های سیستم‌های دفاعی سیستم سوم را به عنوان مهاجم نشان می‌دهند که اشتباه می‌باشد. این نوع اسکن علاوه بر مخفی بودن امکان کشف روابط اعتماد مبتنی بر IP میان ماشین‌ها را نیز میدهد.

```
farshid @ farshids-MacBook-Pro: ~
$ sudo nmap -sI 89.43.3.170
Password:
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On the other hand, tim
ing info Nmap gains from pings can allow for faster, more reliable scans.
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-06 19:35 +0330
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 2.08 seconds

farshid @ farshids-MacBook-Pro: ~
$ sudo nmap -sI 89.43.3.170 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-06 19:35 +0330
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
```

## HPING

```
farshid @ farshids-MacBook-Pro: ~
$ sudo hping3
Password:
Sorry, this hping binary was compiled without TCL scripting support

farshid @ farshids-MacBook-Pro: ~
$ sudo hping3 --count 1 google.com --icmp
HPING google.com (utun5 142.251.36.46): icmp mode set, 28 headers + 0 data bytes
len=28 ip=142.251.36.46 ttl=116 id=0 icmp_seq=0 rtt=139.3 ms

--- google.com hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 139.3/139.3/139.3 ms

farshid @ farshids-MacBook-Pro: ~
$ sudo hping3 89.43.3.179 -c 20
HPING 89.43.3.179 (utun5 89.43.3.179): NO FLAGS are set, 40 headers + 0 data bytes

--- 89.43.3.179 hping statistic ---
20 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

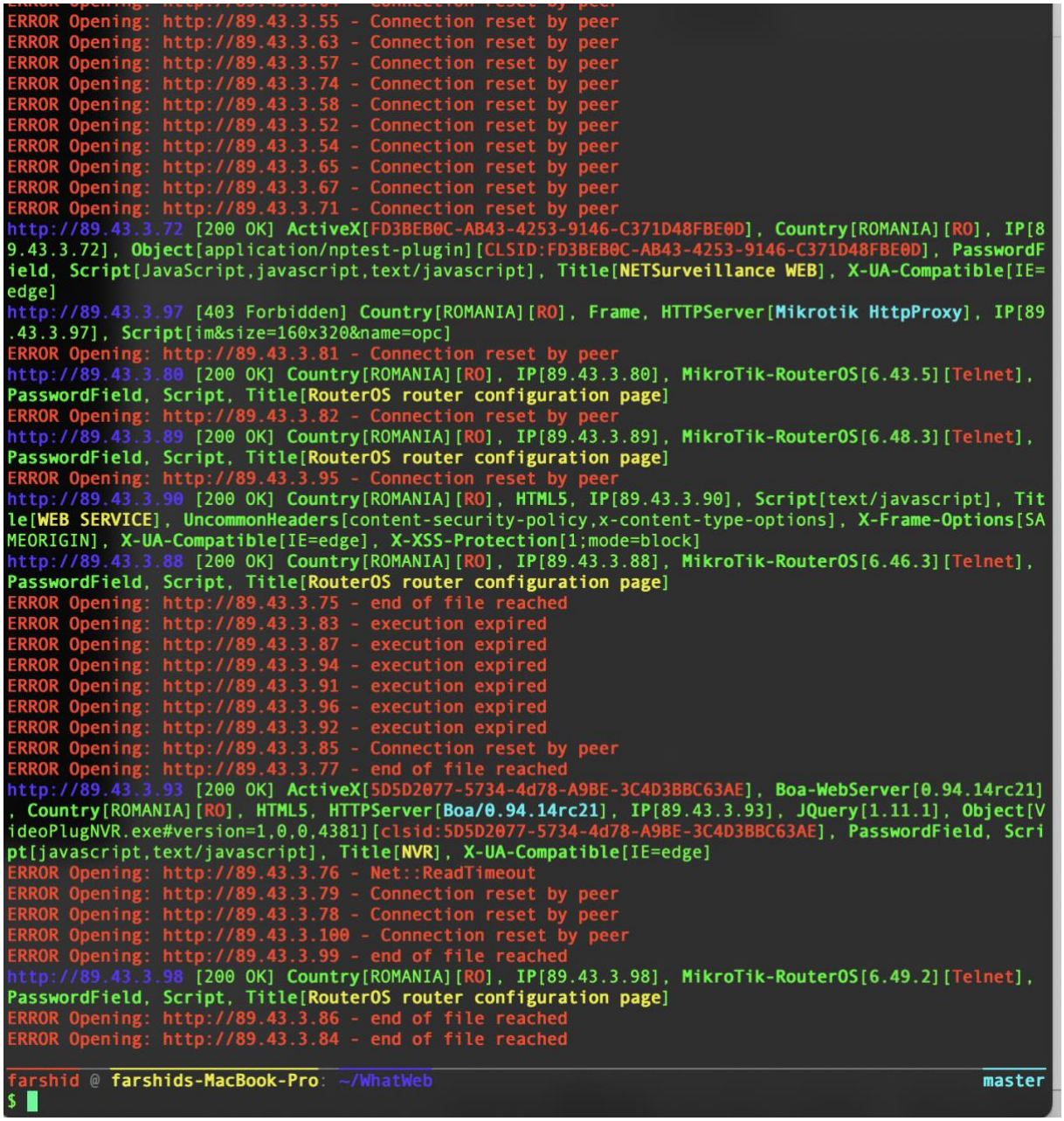
### NetDiscover

این ابزار نصب و اجرا شد و خروجی‌اش حین کار در یزر نمایش داده شده است. سرعت اسکن بسیار پایین بود به طوری که خروجی زیر بعد از حدود یک ساعت اجرا تغییری نکرد. اطلاعاتی از جمله‌هاست‌های درحال اجرا برروی سیستم در اینجا نمایش داده میشوند. که یعنی ipهای اختصاص داده شده لوکال مشاهده میشوند.

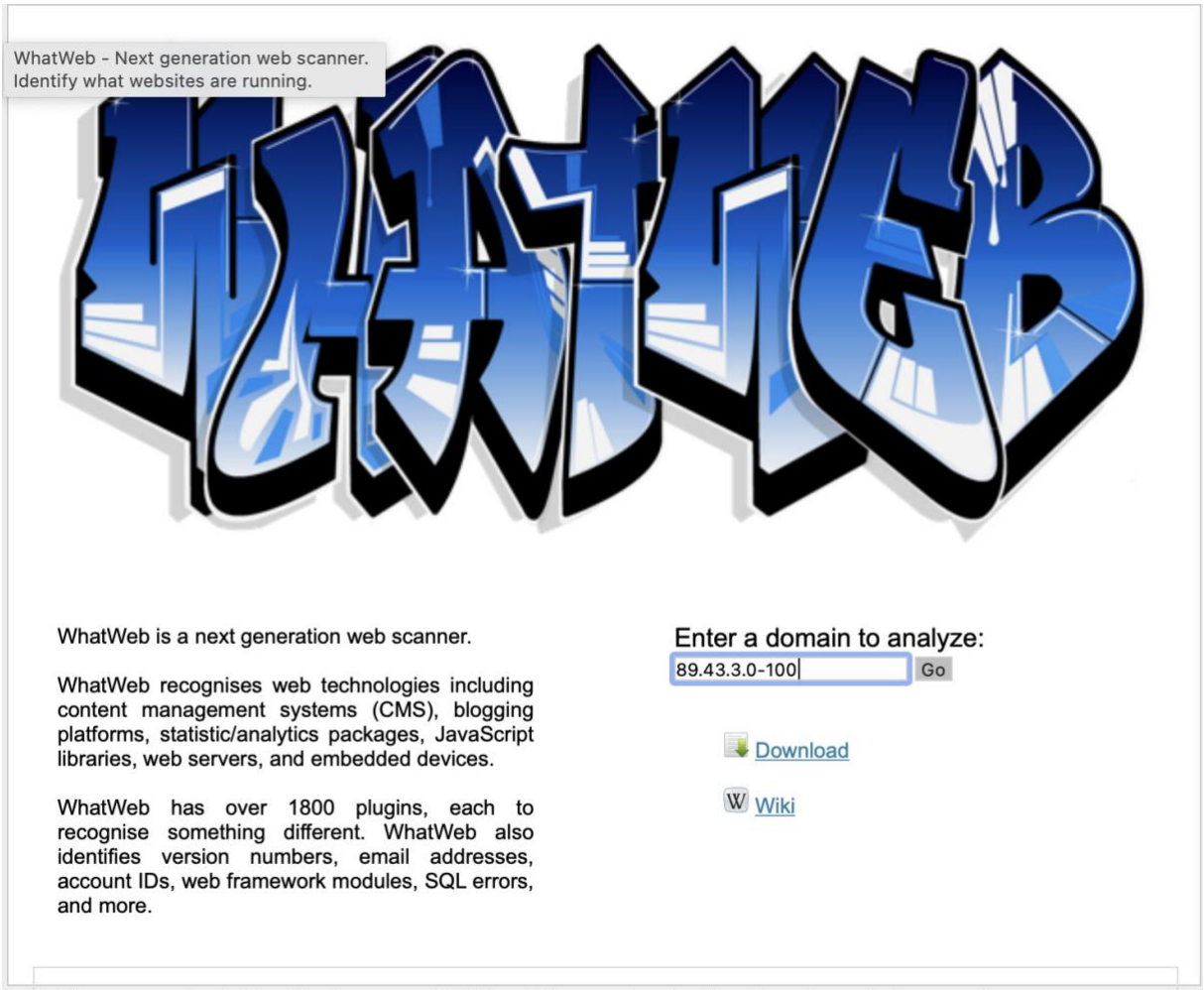
```
netdiscover — farshid@farshids-MacBook-Pro — ~/netdiscover — -zsh — 100×72
Currently scanning: 172.22.146.0/16   |   Screen View: Unique Hosts

61 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 2562

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.0.1     98:de:d0:60:d7:b1     32    1344  TP-LINK TECHNOLOGIES CO.,LTD.
192.168.0.103   f4:d4:88:79:69:09     27    1134  Apple, Inc.
192.168.0.101   f0:99:bf:4e:71:e5      1      42  Apple, Inc.
192.168.0.104   96:51:ee:e3:c9:8b      1      42  Unknown vendor
```

**Whatweb**

```
farshid @ farshids-MacBook-Pro: ~/WhatWeb                                    master
[$ ./whatweb 89.43.3.0-100                                                        ]
ERROR Opening: http://89.43.3.19 - Connection reset by peer
ERROR Opening: http://89.43.3.21 - Connection reset by peer
ERROR Opening: http://89.43.3.17 - Connection reset by peer
ERROR Opening: http://89.43.3.3 - Connection reset by peer
ERROR Opening: http://89.43.3.20 - Connection reset by peer
ERROR Opening: http://89.43.3.10 - Connection reset by peer
ERROR Opening: http://89.43.3.15 - Connection reset by peer
ERROR Opening: http://89.43.3.12 - Connection reset by peer
ERROR Opening: http://89.43.3.11 - Connection reset by peer
ERROR Opening: http://89.43.3.23 - Connection reset by peer
ERROR Opening: http://89.43.3.18 - Connection reset by peer
ERROR Opening: http://89.43.3.16 - Connection reset by peer
ERROR Opening: http://89.43.3.22 - Connection reset by peer
ERROR Opening: http://89.43.3.14 - Connection reset by peer
ERROR Opening: http://89.43.3.6 - Connection reset by peer
ERROR Opening: http://89.43.3.4 - Connection reset by peer
ERROR Opening: http://89.43.3.13 - Connection reset by peer
ERROR Opening: http://89.43.3.5 - Connection reset by peer
ERROR Opening: http://89.43.3.7 - Connection reset by peer
ERROR Opening: http://89.43.3.1 - Connection reset by peer
ERROR Opening: http://89.43.3.0 - Connection reset by peer
ERROR Opening: http://89.43.3.8 - Connection reset by peer
ERROR Opening: http://89.43.3.2 - Connection reset by peer
ERROR Opening: http://89.43.3.24 - Connection reset by peer
ERROR Opening: http://89.43.3.9 - Connection reset by peer
ERROR Opening: http://89.43.3.41 - end of file reached
ERROR Opening: http://89.43.3.38 - end of file reached
ERROR Opening: http://89.43.3.37 - end of file reached
ERROR Opening: http://89.43.3.44 - Connection reset by peer
ERROR Opening: http://89.43.3.42 - Connection reset by peer
ERROR Opening: http://89.43.3.25 - end of file reached
ERROR Opening: http://89.43.3.27 - end of file reached
ERROR Opening: http://89.43.3.40 - end of file reached
ERROR Opening: http://89.43.3.35 - end of file reached
ERROR Opening: http://89.43.3.39 - end of file reached
ERROR Opening: http://89.43.3.26 - end of file reached
ERROR Opening: http://89.43.3.28 - end of file reached
ERROR Opening: http://89.43.3.29 - end of file reached
ERROR Opening: http://89.43.3.31 - end of file reached
ERROR Opening: http://89.43.3.45 - Connection reset by peer
ERROR Opening: http://89.43.3.30 - Connection reset by peer
ERROR Opening: http://89.43.3.46 - Connection reset by peer
ERROR Opening: http://89.43.3.36 - Connection reset by peer
ERROR Opening: http://89.43.3.32 - end of file reached
ERROR Opening: http://89.43.3.49 - Connection reset by peer
ERROR Opening: http://89.43.3.43 - Connection reset by peer
ERROR Opening: http://89.43.3.33 - end of file reached
ERROR Opening: http://89.43.3.34 - Connection reset by peer
ERROR Opening: http://89.43.3.48 - Connection reset by peer
ERROR Opening: http://89.43.3.47 - Connection reset by peer
ERROR Opening: http://89.43.3.69 - Connection reset by peer
ERROR Opening: http://89.43.3.70 - Connection reset by peer
ERROR Opening: http://89.43.3.68 - Connection reset by peer
ERROR Opening: http://89.43.3.56 - Connection reset by peer
ERROR Opening: http://89.43.3.73 - Connection reset by peer
ERROR Opening: http://89.43.3.66 - Connection reset by peer
ERROR Opening: http://89.43.3.53 - Connection reset by peer
ERROR Opening: http://89.43.3.62 - Connection reset by peer
ERROR Opening: http://89.43.3.51 - Connection reset by peer
ERROR Opening: http://89.43.3.60 - Connection reset by peer
ERROR Opening: http://89.43.3.50 - Connection reset by peer
ERROR Opening: http://89.43.3.59 - Connection reset by peer
ERROR Opening: http://89.43.3.61 - Connection reset by peer
ERROR Opening: http://89.43.3.64 - Connection reset by peer
ERROR Opening: http://89.43.3.55 - Connection reset by peer
ERROR Opening: http://89.43.3.63 - Connection reset by peer
ERROR Opening: http://89.43.3.57 - Connection reset by peer
ERROR Opening: http://89.43.3.74 - Connection reset by peer
ERROR Opening: http://89.43.3.58 - Connection reset by peer
ERROR Opening: http://89.43.3.52 - Connection reset by peer
```


ERROR Opening: http://89.43.3.55 - Connection reset by peer
ERROR Opening: http://89.43.3.63 - Connection reset by peer
ERROR Opening: http://89.43.3.57 - Connection reset by peer
ERROR Opening: http://89.43.3.74 - Connection reset by peer
ERROR Opening: http://89.43.3.58 - Connection reset by peer
ERROR Opening: http://89.43.3.52 - Connection reset by peer
ERROR Opening: http://89.43.3.54 - Connection reset by peer
ERROR Opening: http://89.43.3.65 - Connection reset by peer
ERROR Opening: http://89.43.3.67 - Connection reset by peer
ERROR Opening: http://89.43.3.71 - Connection reset by peer
http://89.43.3.72 [200 OK] ActiveX[FD3BEB0C-AB43-4253-9146-C371D48FBE0D], Country[ROMANIA][RO], IP[89.43.3.72], Object[application/nptest-plugin][CLSID:FD3BEB0C-AB43-4253-9146-C371D48FBE0D], PasswordField, Script[JavaScript,javascript,text/javascript], Title[NETSurveillance WEB], X-UA-Compatible[IE=edge]
http://89.43.3.97 [403 Forbidden] Country[ROMANIA][RO], Frame, HTTPServer[Mikrotik HttpProxy], IP[89.43.3.97], Script[im&size=160x320&name=opc]
ERROR Opening: http://89.43.3.81 - Connection reset by peer
http://89.43.3.80 [200 OK] Country[ROMANIA][RO], IP[89.43.3.80], MikroTik-RouterOS[6.43.5][Telnet], PasswordField, Script, Title[RouterOS router configuration page]
ERROR Opening: http://89.43.3.82 - Connection reset by peer
http://89.43.3.89 [200 OK] Country[ROMANIA][RO], IP[89.43.3.89], MikroTik-RouterOS[6.48.3][Telnet], PasswordField, Script, Title[RouterOS router configuration page]
ERROR Opening: http://89.43.3.95 - Connection reset by peer
http://89.43.3.90 [200 OK] Country[ROMANIA][RO], HTML5, IP[89.43.3.90], Script[text/javascript], Title[WEB SERVICE], UncommonHeaders[content-security-policy,x-content-type-options], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=edge], X-XSS-Protection[1;mode=block]
http://89.43.3.88 [200 OK] Country[ROMANIA][RO], IP[89.43.3.88], MikroTik-RouterOS[6.46.3][Telnet], PasswordField, Script, Title[RouterOS router configuration page]
ERROR Opening: http://89.43.3.75 - end of file reached
ERROR Opening: http://89.43.3.83 - execution expired
ERROR Opening: http://89.43.3.87 - execution expired
ERROR Opening: http://89.43.3.94 - execution expired
ERROR Opening: http://89.43.3.91 - execution expired
ERROR Opening: http://89.43.3.96 - execution expired
ERROR Opening: http://89.43.3.92 - execution expired
ERROR Opening: http://89.43.3.85 - Connection reset by peer
ERROR Opening: http://89.43.3.77 - end of file reached
http://89.43.3.93 [200 OK] ActiveX[5D5D2077-5734-4d78-A9BE-3C4D3BBC63AE], Boa-WebServer[0.94.14rc21], Country[ROMANIA][RO], HTML5, HTTPServer[Boa/0.94.14rc21], IP[89.43.3.93], JQuery[1.11.1], Object[VideoPlugNVR.exe#version=1,0,0,4381][clsid:5D5D2077-5734-4d78-A9BE-3C4D3BBC63AE], PasswordField, Script[javascript,text/javascript], Title[NVR], X-UA-Compatible[IE=edge]
ERROR Opening: http://89.43.3.76 - Net::ReadTimeout
ERROR Opening: http://89.43.3.79 - Connection reset by peer
ERROR Opening: http://89.43.3.78 - Connection reset by peer
ERROR Opening: http://89.43.3.100 - Connection reset by peer
ERROR Opening: http://89.43.3.99 - end of file reached
http://89.43.3.98 [200 OK] Country[ROMANIA][RO], IP[89.43.3.98], MikroTik-RouterOS[6.49.2][Telnet], PasswordField, Script, Title[RouterOS router configuration page]
ERROR Opening: http://89.43.3.86 - end of file reached
ERROR Opening: http://89.43.3.84 - end of file reached
farshid @ farshids-MacBook-Pro: ~/WhatWeb master
$

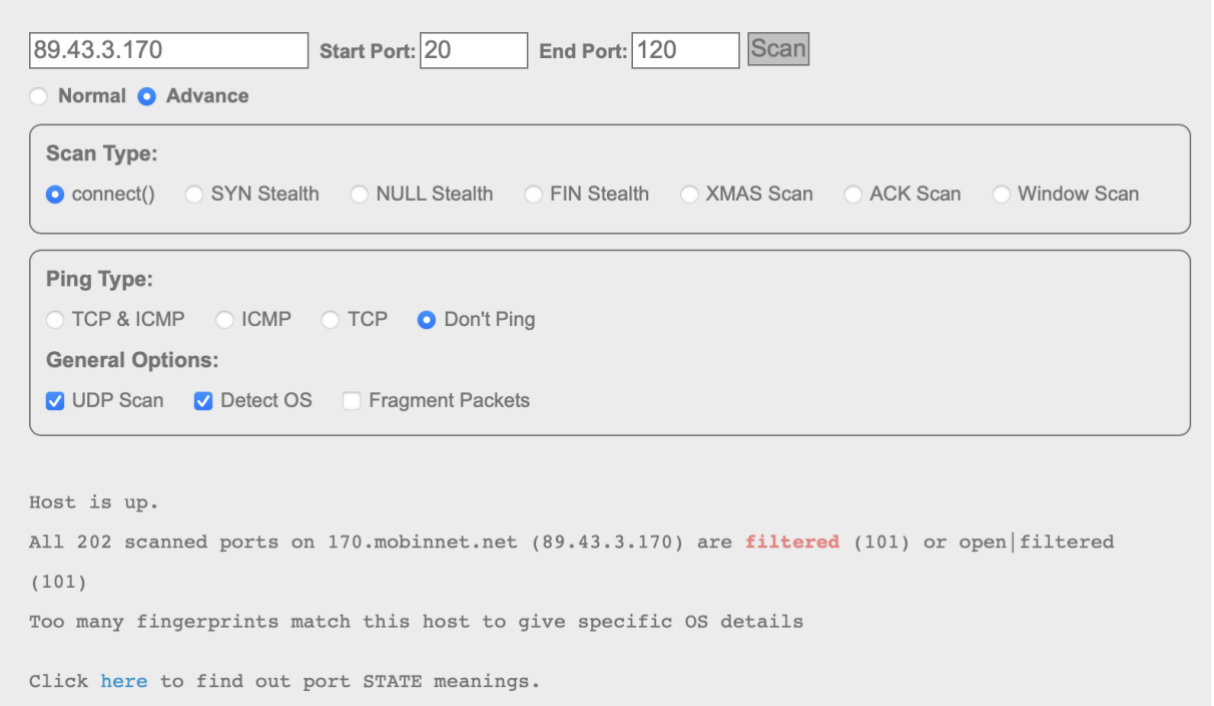
**Whatweb website**




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

https://www.ipfingerprints.com/portscan.php

از ابزار آنلاین بالا برای اسکن و بدست آوردن اطلاعات بیشتر از ۸۹.۴۳.۳.۱۷۰ و رنج پورت‌های ۲۰-۱۰۲۴ استفاده میکنیم.




همانطور که مشاهده میکنیم اطلاعات بدست آمده از اینجا نیز میگویند تعداد بسیار زیادی از پورت‌ها فیلتر هستند برای udp و دیگر بسته‌ها و همینطور os نیز تشخیص داده نشد.