پیاده سازی پینگ

برای پیاده سازی پینگ از کتاب خوانه pythonping استفاده می کنیم، که خروجی آن برای دامنه google.com در زیر دیده می شود:

```
please enter your ip/domain:
google.com
paging google.com[142.251.41.4] with 32 bytes of data:

Reply from 216.239.38.120, 32 bytes in 50.67ms

Round Trip Times min/avg/max is 50.67/50.67/50.67 ms
packets sent: 1
packets returned: 1
packets lost: 0
lost ratio: 0.0
```

پیاده سازی اسکنر[1] محدوده آیپی

برای پیاده سازی اسکنر محدود آیپی از کتابخانه nmap استفاده می کنیم، به این صورت در ابتدا از انواع بسته های پویشگر[2] استفاده می کنیم تا پاسخی از هاست های فعال بگیریم و در صورت عدم دریافت پاسخ از برخی از هاست ها، از سوییچ Pn استفاده می کنیم که ببینیم آیا پورت های سرویس های معروف مانند http و... روی این هاست ها باز هستند یا نه و در صورت باز بودن فرض می کنیم آن ها فعال هستند. خروجی اسکنر در زیر دیده می شود:

[1] Scanner

[2] probe

```
C:\thesisProject\venv\Scripts\python.exe C:/security/scanner/ipScanner.py
Enter the network address:89.43.3.0
Enter the starting number:60
Enter the last number:70
scanning in progress

89.43.3.66--->live
89.43.3.67--->live
89.43.3.68--->live
89.43.3.69--->live
89.43.3.70--->live
scanning complete in 481.0222728252411 seconds
```

همچنین برای تست درستی اسکنر از namp ، whatweb ، netdiscover، httprint و xprobe2 استفاده می کنیم.

خروجی nmap :

```
C:\Users\Mahdi>nmap -sn -PS -PA -PU -PY -PE -PP -PM -PO 89.43.3.60-70
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-05 10:14 Iran Standard Time
Nmap scan report for 66.mobinnet.net (89.43.3.66)
Host is up (0.073s latency).
Nmap scan report for 67.mobinnet.net (89.43.3.67)
Host is up (0.25s latency).
Nmap scan report for 68.mobinnet.net (89.43.3.68)
Host is up (0.075s latency).
Nmap scan report for 69.mobinnet.net (89.43.3.69)
Host is up (0.072s latency).
Nmap scan report for 70.mobinnet.net (89.43.3.70)
Host is up (0.099s latency).
Nmap done: 11 IP addresses (5 hosts up) scanned in 11.36 seconds
```

```
C:\Users\Mahdi>nmap -Pn 89.43.3.60-66
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-05 13:57 Iran Standard Time
Nmap scan report for mx1.payaco-mnp.ir (89.43.3.60)
Host is up (0.075s latency).
All 1000 scanned ports on mx1.payaco-mnp.ir (89.43.3.60) are filtered

Nmap scan report for 61.mobinnet.net (89.43.3.61)
Host is up (0.088s latency).
All 1000 scanned ports on 61.mobinnet.net (89.43.3.61) are filtered

Nmap scan report for 62.mobinnet.net (89.43.3.62)
Host is up (0.068s latency).
All 1000 scanned ports on 62.mobinnet.net (89.43.3.62) are filtered

Nmap scan report for 63.mobinnet.net (89.43.3.63)
Host is up (0.068s latency).
All 1000 scanned ports on 63.mobinnet.net (89.43.3.63) are filtered

Nmap scan report for 64.mobinnet.net (89.43.3.64)
Host is up.
All 1000 scanned ports on 64.mobinnet.net (89.43.3.64) are filtered

Nmap scan report for 65.mobinnet.net (89.43.3.65)
Host is up.
All 1000 scanned ports on 65.mobinnet.net (89.43.3.65) are filtered

Nmap scan report for 66.mobinnet.net (89.43.3.66)
Host is up (0.074s latency).
Not shown: 990 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   filtered http
800/tcp  filtered mdbs_daemon
801/tcp  filtered device
1723/tcp open     pptp
2000/tcp open     cisco-sccp
8080/tcp open     http-proxy
8291/tcp filtered unknown
8443/tcp open     https-alt
8800/tcp open     sunwebadmin

Nmap done: 7 IP addresses (7 hosts up) scanned in 133.34 seconds
```

```
C:\Users\Mahdi>nmap -O 89.43.3.60-70
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-05 14:21 Iran Standard Time
Nmap scan report for 66.mobinnet.net (89.43.3.66)
Host is up (0.086s latency).
Not shown: 990 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
80/tcp   filtered http
800/tcp  filtered mdbs_daemon
801/tcp  filtered device
1723/tcp open     pptp
2000/tcp open     cisco-sccp
8080/tcp open     http-proxy
8291/tcp filtered unknown
8443/tcp open     https-alt
8800/tcp open     sunwebadmin
Aggressive OS guesses: Linux 3.4 (91%), Linux 2.6.32 (87%), Linux 2.6.32 or 3.10 (87%), Linux 3.5 (87%), Linux 4.2 (87%), Synology DiskStation Manager 5.1 (86%), Linux 2.6.35 (86%), Linux 2.6.39 (86%), Linux 3.10 - 3.12 (86%), Linux 4.4 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops

Nmap scan report for 68.mobinnet.net (89.43.3.68)
Host is up (0.093s latency).
Not shown: 990 closed ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
808/tcp  open     ccproxy-http
3389/tcp open     ms-wbt-server
5357/tcp open     wsdapi
5900/tcp open     vnc
7070/tcp open     realserver
7443/tcp filtered oracleas-https
8291/tcp filtered unknown
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|7|2008 (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_server_2008
Aggressive OS guesses: Microsoft Windows XP SP3 (87%), Microsoft Windows 7 (86%), Microsoft Windows Server 2008 or 2008 Beta 3 (86%), Microsoft Windows Server 2008 SP1 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 19 hops

Nmap scan report for 69.mobinnet.net (89.43.3.69)
Host is up (0.091s latency).
Not shown: 997 closed ports
PORT     STATE    SERVICE
1723/tcp open     pptp
2000/tcp open     cisco-scep
8291/tcp filtered unknown
Aggressive OS guesses: Linux 3.4 (92%), Linux 3.2 - 3.8 (90%), Linux 3.8 (90%), WatchGuard Fireware 11.8 (90%), Linux 3.1 - 3.2 (89%), Linux 2.6.32 - 2.6.39 (88%), Linux 3.5 (88%), Linux 3.0 - 3.2 (87%), Linux 2.6.32 - 3.0 (87%), Kyocera CopyStar CS-2560 printer (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops

Nmap scan report for 70.mobinnet.net (89.43.3.70)
Host is up (0.11s latency).
Not shown: 995 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
1723/tcp open     pptp
6666/tcp open     irc
7443/tcp open     oracleas-https
8291/tcp filtered unknown
Aggressive OS guesses: Linux 3.4 (91%), Linux 4.4 (91%), Linux 4.9 (90%), Linux 3.10 - 3.12 (90%), Linux 4.0 (88%), Linux 3.10 (88%), Linux 3.11 - 4.1 (87%), Linux 2.6.32 (87%), Linux 2.6.32 or 3.10 (87%), Linux 3.5 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 19 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 11 IP addresses (4 hosts up) scanned in 81.38 seconds
```

همانطور که دیده می شود خروجی nmap با خروجی برنامه ما یکسان است و با استفاده از اسکن اثر انگشتی[۳] هم می توانیم با احتمال خوبی حدس بزنیم که سیستم عامل برخی از این هاست ها چی هستند.

حال با استفاده از یک vm به عنوان یک هاست زامبی[۴] و Idle scan، هاست هایی که به نظر می آمدند فعال نبودند را دوباره بررسی می کنیم که مراحل آن در عکس های زیر دیده می شود:

```
C:\Users\Mahdi>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=46ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 46ms, Average = 12ms
```

[۳] Fingerprint scan

[۴] zombie

```
Ubuntu 19.04 mahdi-VirtualBox tty3

mahdi-VirtualBox login: mahdi
\Password:
Last login: Sun Nov  6 14:44:09 EST 2022 on tty3
Welcome to Ubuntu 19.04 (GNU/Linux 5.0.0-13-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


0 updates can be installed immediately.
0 of these updates are security updates.

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

imahdi@mahdi-VirtualBox:~$ ip r
default via 192.168.1.1 dev enp0s3 proto dhcp metric 20100
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.84 metric 100
mahdi@mahdi-VirtualBox:~$ _
```

```
C:\Users\Mahdi>nmap -sI 192.168.1.1 89.43.3.65
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On t
cans.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-06 23:41 Iran Standard Time
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 6.30 seconds

C:\Users\Mahdi>nmap -sI 192.168.1.1 89.43.3.64
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On t
cans.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-06 23:41 Iran Standard Time
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 6.25 seconds

C:\Users\Mahdi>nmap -sI 192.168.1.1 89.43.3.63
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On t
cans.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-06 23:41 Iran Standard Time
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 6.33 seconds

C:\Users\Mahdi>nmap -sI 192.168.1.1 89.43.3.62
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On t
cans.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-06 23:42 Iran Standard Time
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 6.37 seconds

C:\Users\Mahdi>nmap -sI 192.168.1.1 89.43.3.61
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On t
cans.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-06 23:42 Iran Standard Time
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 6.28 seconds

C:\Users\Mahdi>nmap -sI 192.168.1.1 89.43.3.60
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On t
cans.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-06 23:42 Iran Standard Time
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 6.49 seconds
```

همانطور که دیده می شود با استفاده از idle scan هم این هاست ها به نظر غیر فعال می رسند.

خروجی **netdiscover** :

```
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
-----------------------------------------------------------------------------
```

متاسفانه netdiscover وضعیت هیچ یک از هاست ها را نتوانست تشخیص دهد چرا که از پروتوکل ARP استفاده می کند و این سرور ها به پروتوکل ARP پاسخی نمی دهد.

خروجی **whatweb**:

```
# whatweb -v 89.43.3.60-70
ERROR Opening: http://89.43.3.70 - end of file reached
ERROR Opening: http://89.43.3.61 - execution expired
ERROR Opening: http://89.43.3.62 - execution expired
ERROR Opening: http://89.43.3.65 - execution expired
ERROR Opening: http://89.43.3.64 - execution expired
ERROR Opening: http://89.43.3.63 - execution expired
ERROR Opening: http://89.43.3.67 - execution expired
ERROR Opening: http://89.43.3.69 - execution expired
ERROR Opening: http://89.43.3.68 - execution expired
ERROR Opening: http://89.43.3.60 - execution expired
ERROR Opening: http://89.43.3.66 - execution expired
#
```

با توجه به اینکه نرم افزار whatweb بیشتر برای بررسی website های مشخصی مانند reddit.com و ... است و نه هاست هایی که فقط به عنوان سرور استفاده می شوند، نمی توانیم با استفاده از آن ببینیم که این هاست ها فعال هستند یا نه و همچنین نمی توانیم اطلاعاتی در مورد آن ها به دست آوریم.

خروجی **httprint**:

```
C:\security\httprint_301\win32>httprint -h 89.43.3.60-89.43.3.70 -s signatures.txt
httprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httprint/
httprint@net-square.com

Finger Printing on http://89.43.3.66:80/
Finger Printing on http://89.43.3.68:80/
Finger Printing on http://89.43.3.70:80/
Finger Printing on http://89.43.3.69:80/
Finger Printing Completed on http://89.43.3.69:80/
Finger Printing Completed on http://89.43.3.70:80/
Finger Printing Completed on http://89.43.3.68:80/
Finger Printing Completed on http://89.43.3.66:80/
---------------------------------------------------
Host: 89.43.3.60
ICMP request time out on 89.43.3.60

---------------------------------------------------
Host: 89.43.3.61
ICMP request time out on 89.43.3.61

---------------------------------------------------
Host: 89.43.3.62
ICMP request time out on 89.43.3.62

---------------------------------------------------
Host: 89.43.3.63
ICMP request time out on 89.43.3.63

---------------------------------------------------
Host: 89.43.3.64
ICMP request time out on 89.43.3.64

---------------------------------------------------
Host: 89.43.3.65
ICMP request time out on 89.43.3.65

---------------------------------------------------
Host: 89.43.3.66
Fingerprinting Error: Connection error...

---------------------------------------------------
Host: 89.43.3.67
ICMP request time out on 89.43.3.67

---------------------------------------------------
Host: 89.43.3.68
Fingerprinting Error: Connection error...

---------------------------------------------------
Host: 89.43.3.69
Fingerprinting Error: Connection error...

---------------------------------------------------
Host: 89.43.3.70
Fingerprinting Error: Connection error...

---------------------------------------------------
```

باز هم با توجه به اینکه نرم افزار httprint بیشتر برای website های مشخصی است، با استفاده از آن فقط می توانیم ببینیم که کدام هاست ها فعال هستند(البته هاست x.x.x.67 هم فعال هست ولی httprint ان را غیر فعال نشان داده است) ولی نمی توانیم اطلاعاتی در مورد آن ها به دست آوریم.

خروجی xprobe2 با توجه به حجم آن در فایل xprobe.png قرار دارد. همان طور که در خروجی دیده می شود، حدس های xprobe2 در مورد سیستم عامل های سرور ها نامشخص است و همچنین در مورد سرور x.x.x.70 هم حدسی نتوانسته بزند، در حالی که با nmap با احتمال خوبی می توانستیم سیستم عامل را حدس بزنیم.

پیاده سازی اسکنر پورت

برای پیاده سازی اسکنر پورت نیز از کتابخانه nmap استفاده می کنیم، به این صورت که از انواع اسکن ها(به غیر از اسکن هایی که نیاز به پارامتر دارند مانند idle scan یا ftp bounce scan) استفاده می کنیم تا ببینیم کدام پورت ها فعال هستند. خروجی اسکنر در زیر دیده می شود:

```
Enter the ip to scan:89.43.3.66
Enter the start port number:1
Enter the last port number:500
unspecified ports are closed
port 22 is open
port 80 is filtered
port 500 is open
```

همچنین برای تست درستی اسکنر از hping3 استفاده می کنیم.

```
# hping3 -8 1-500 89.43.3.66
Scanning 89.43.3.66 (89.43.3.66), port 1-500
500 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
All replies received. Done.
Not responding ports: (1 ) (2 ) (3 ) (4 ) (5 ) (6 ) (7 ) (8 ) (9 ) (10 ) (11 ) (12 ) (13 ) (14 ) (15 ) (16 ) (17 ) (18 )
 (19 ) (20 ) (21 ) (22 ) (23 ) (24 ) (25 ) (26 ) (27 ) (28 ) (29 ) (30 ) (31 ) (32 ) (33 ) (34 ) (35 ) (36 ) (37 ) (38 )
 (39 ) (40 ) (41 ) (42 ) (43 ) (44 ) (45 ) (46 ) (47 ) (48 ) (49 ) (50 ) (51 ) (52 ) (53 ) (54 ) (55 ) (56 ) (57 ) (58 )
 (59 ) (60 ) (61 ) (62 ) (63 ) (64 ) (65 ) (66 ) (67 ) (68 ) (69 ) (70 ) (71 ) (72 ) (73 ) (74 ) (75 ) (76 ) (77 ) (78 )
 (79 ) (80 ) (81 ) (82 ) (83 ) (84 ) (85 ) (86 ) (87 ) (88 ) (89 ) (90 ) (91 ) (92 ) (93 ) (94 ) (95 ) (96 ) (97 ) (98 )
 (99 ) (100 ) (101 ) (102 ) (103 ) (104 ) (105 ) (106 ) (107 ) (108 ) (109 ) (110 ) (111 ) (112 ) (113 ) (114 ) (115 )
 (116 ) (117 ) (118 ) (119 ) (120 ) (121 ) (122 ) (123 ) (124 ) (125 ) (126 ) (127 ) (128 ) (129 ) (130 ) (131 ) (132 )
 (133 ) (134 ) (135 ) (136 ) (137 ) (138 ) (139 ) (140 ) (141 ) (142 ) (143 ) (144 ) (145 ) (146 ) (147 ) (148 ) (149 )
 (150 ) (151 ) (152 ) (153 ) (154 ) (155 ) (156 ) (157 ) (158 ) (159 ) (160 ) (161 ) (162 ) (163 ) (164 ) (165 ) (166 )
 (167 ) (168 ) (169 ) (170 ) (171 ) (172 ) (173 ) (174 ) (175 ) (176 ) (177 ) (178 ) (179 ) (180 ) (181 ) (182 ) (183 )
 (184 ) (185 ) (186 ) (187 ) (188 ) (189 ) (190 ) (191 ) (192 ) (193 ) (194 ) (195 ) (196 ) (197 ) (198 ) (199 ) (200 )
 (201 ) (202 ) (203 ) (204 ) (205 ) (206 ) (207 ) (208 ) (209 ) (210 ) (211 ) (212 ) (213 ) (214 ) (215 ) (216 ) (217 )
 (218 ) (219 ) (220 ) (221 ) (222 ) (223 ) (224 ) (225 ) (226 ) (227 ) (228 ) (229 ) (230 ) (231 ) (232 ) (233 ) (234 )
 (235 ) (236 ) (237 ) (238 ) (239 ) (240 ) (241 ) (242 ) (243 ) (244 ) (245 ) (246 ) (247 ) (248 ) (249 ) (250 ) (251 )
 (252 ) (253 ) (254 ) (255 ) (256 ) (257 ) (258 ) (259 ) (260 ) (261 ) (262 ) (263 ) (264 ) (265 ) (266 ) (267 ) (268 )
 (269 ) (270 ) (271 ) (272 ) (273 ) (274 ) (275 ) (276 ) (277 ) (278 ) (279 ) (280 ) (281 ) (282 ) (283 ) (284 ) (285 )
 (286 ) (287 ) (288 ) (289 ) (290 ) (291 ) (292 ) (293 ) (294 ) (295 ) (296 ) (297 ) (298 ) (299 ) (300 ) (301 ) (302 )
 (303 ) (304 ) (305 ) (306 ) (307 ) (308 ) (309 ) (310 ) (311 ) (312 ) (313 ) (314 ) (315 ) (316 ) (317 ) (318 ) (319 )
 (320 ) (321 ) (322 ) (323 ) (324 ) (325 ) (326 ) (327 ) (328 ) (329 ) (330 ) (331 ) (332 ) (333 ) (334 ) (335 ) (336 )
 (337 ) (338 ) (339 ) (340 ) (341 ) (342 ) (343 ) (344 ) (345 ) (346 ) (347 ) (348 ) (349 ) (350 ) (351 ) (352 ) (353 )
 (354 ) (355 ) (356 ) (357 ) (358 ) (359 ) (360 ) (361 ) (362 ) (363 ) (364 ) (365 ) (366 ) (367 ) (368 ) (369 ) (370 )
 (371 ) (372 ) (373 ) (374 ) (375 ) (376 ) (377 ) (378 ) (379 ) (380 ) (381 ) (382 ) (383 ) (384 ) (385 ) (386 ) (387 )
 (388 ) (389 ) (390 ) (391 ) (392 ) (393 ) (394 ) (395 ) (396 ) (397 ) (398 ) (399 ) (400 ) (401 ) (402 ) (403 ) (404 )
 (405 ) (406 ) (407 ) (408 ) (409 ) (410 ) (411 ) (412 ) (413 ) (414 ) (415 ) (416 ) (417 ) (418 ) (419 ) (420 ) (421 )
 (422 ) (423 ) (424 ) (425 ) (426 ) (427 ) (428 ) (429 ) (430 ) (431 ) (432 ) (433 ) (434 ) (435 ) (436 ) (437 ) (438 )
 (439 ) (440 ) (441 ) (442 ) (443 ) (444 ) (445 ) (446 ) (447 ) (448 ) (449 ) (450 ) (451 ) (452 ) (453 ) (454 ) (455 )
 (456 ) (457 ) (458 ) (459 ) (460 ) (461 ) (462 ) (463 ) (464 ) (465 ) (466 ) (467 ) (468 ) (469 ) (470 ) (471 ) (472 )
 (473 ) (474 ) (475 ) (476 ) (477 ) (478 ) (479 ) (480 ) (481 ) (482 ) (483 ) (484 ) (485 ) (486 ) (487 ) (488 ) (489 )
 (490 ) (491 ) (492 ) (493 ) (494 ) (495 ) (496 ) (497 ) (498 ) (499 ) (500))
```

با توجه به خروجی hprint3 همه پورت ها بسته هستند، در حالی که با اسکنر(که در آن از nmap استفاده می کنیم) می توانیم ببینیم که 22 و 500 باز هستند و پورت 80 نیز ممکن است باز باشد.