

## بخش اول و دوم

- فایل README.md برای اجرای صحیح کد های Python و bash اسکریپت ها قرار داده شده است. (نوع ورودی گرفتن اسکریپت ها تغییر کرده!)
- خروجی های کد در فایل های با پسوند .txt قرار داده شده اند.
- اسکریپت شات ها رو فایل های با پسوند .png قرار داده شده اند.

## Ping

```
Pinging 82.115.20.167 with 32 bytes of data:
Reply from 82.115.20.167: bytes=32 time=114ms TTL=45
Reply from 82.115.20.167: bytes=32 time=97ms TTL=45
Reply from 82.115.20.167: bytes=32 time=104ms TTL=45

Ping statistics for 82.115.20.167:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 97ms, Maximum = 114ms, Average = 105ms
    '82.115.20.167' is UP.
```

خروجی هر دو اسکریپت نوشته شده با Python و Bash مطابقت داشت که دستور nmap را اجرا میکند. خروجی nmap:

```
keivanipchihagh@Keivan:~/temp$ nmap -sn 82.115.20.167
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-04 22:29 +0330
Nmap scan report for 82.115.20.167
Host is up (0.13s latency).
Nmap done: 1 IP address (1 host up) scanned in 15.14 seconds
```

## ICT - Project 1 – Keivan Ipchi Hagh - 9831073

IP Range

Starting from IP:	<input type="text" value="82.115.20.160"/>	example: 91.19.91.10
Last IP in range:	<input type="text" value="82.115.20.170"/>	example: 91.19.91.170
Port number:	<input type="text" value="80"/> or <input type="text"/>	▼
Timeout (bigger means slower):	<input type="text" value="2 sec"/>	▼
<input type="button" value="Start Scan"/>		
<b>Scanning Complete</b>		
82.115.20.167:80 = open		
82.115.20.163:80 = open		
82.115.20.170:80 = closed		
82.115.20.169:80 = closed		
82.115.20.168:80 = closed		
82.115.20.166:80 = closed		
82.115.20.165:80 = closed		
82.115.20.164:80 = closed		
82.115.20.162:80 = closed		
82.115.20.161:80 = closed		
82.115.20.160:80 = closed		

تصویر بالا مربوط به این [سایت](#) است که برای IP های داده شده ۲ IP باز پیدا کرده که سرور با IP 82.115.20.167 برا من است.

```
82.115.20.163 --> Live
82.115.20.167 --> Live
scanning complete in 123.66918087005615
PS E:\github\AUT-CE-ICT\projects\project 1>
```

تصویر بالا مربوط به اجرای کد Python است که با اتصال socket به پورت 80 آدرس های داده شده، آن ها را چک میکند. همانطور که مشاهده می شود خروجی این دو با یکدیگر مطابقت دارد.

```
keivanipchiagh@Keivan:~/temp$ sudo hping3 -S 82.115.20.167 -p ++1
HPING 82.115.20.167 (eth0 82.115.20.167): S set, 40 headers + 0 data bytes
len=44 ip=82.115.20.167 ttl=44 DF id=0 sport=22 flags=SA seq=21 win=64240 rtt=119.4 ms
len=44 ip=82.115.20.167 ttl=43 DF id=0 sport=80 flags=SA seq=79 win=64240 rtt=135.9 ms
len=44 ip=82.115.20.167 ttl=43 DF id=0 sport=81 flags=SA seq=80 win=64240 rtt=145.2 ms
^C
--- 82.115.20.167 hping statistic ---
265 packets transmitted, 3 packets received, 99% packet loss
round-trip min/avg/max = 119.4/133.5/145.2 ms
```

تصویر بالا مربوط به خروجی hping3 است که برای 82.115.20.167 سه پورت 22، 80 و 81 را باز یافته است.

```
Port Open: --> 22
Port Open: --> 80
Port Open: --> 81
scanning complete in 0.3873305320739746
```

تصویر بالا مربوط به خروجی کد Python که بوسیله باز کردن socket کار میکند است، همانطور که مشاهده میشود سه پورت 22، 80 و 81 را باز یافته است. (برای سرعت یافتن فرایند لیست ۵ پورت را تست کردیم)

خروجی هر دو اسکریپت نوشته شده با Python و Bash مطابقت داشت. در Bash از hping3 و در Python از socket استفاده شده است.

```
Port Closed: --> 62410
Port Open: --> 62411
Port Closed: --> 62412
Port Closed: --> 62413
Port Closed: --> 62414
Port Closed: --> 62415
Port Closed: --> 62416
Port Closed: --> 62417
Port Closed: --> 62418
Port Closed: --> 62419
scanning complete in 189.52499055862427
```

برای اطمینان از کارکرد صحیح کد، پورت 62411 توسط من برای IP به عنوان 82.115.20.167 باز شد. تصویر بالا مربوط به اجرای کد Python برای این IP است. ابزار hping3 نیز این پورت را تایید کرد.

توضیح حالت های nmap برای اتصال:

- TCP full scan: زمانی است که TCP three-way handshake به کاملی اجرا شود تا باز یا بسته بودن پورت بررسی شود.
- Stealth scan: در این حالت از آنجایی که اتصال TCP هیچگاه به شکل کامل برقرار نمیشود (نیازی به این امر نیست) پس میتوان تعداد زیادی پورت را در هر ثانیه چک کرد. این حالت معروف ترین حالت اسکن است.
- UDP scan: در این حالت بسته UDP به جای TCP ارسال می شود که معمولاً payload ندارد.
- Fingerprint scan: این حالت برای فهمیدن سیستم عامل IP مورد نظر است که با ارسال درخواست به برخی پورت های باز انجام میشود.
- Idle scan: در این حالت درخواست مستقیم از ماشین حمله کننده ارسال نمیشود، بلکه از دستگاه دیگری که معمولاً zombie فراخوانده میشود ارسال میشود تا هویت حمله کننده محفوظ بماند.

## ICT - Project 1 – Keivan Ipchi Hagh - 9831073

```
xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@00o.nu, ofir@sys-security.com, meder@00o.nu

[+] Target is 89.43.3.80
[+] Loading modules.
[+] Following modules are loaded:
[X] [1] ping:icmp_ping - ICMP echo discovery module
[X] [2] ping:tcp_ping - TCP-based ping discovery module
[X] [3] ping:udp_ping - UDP-based ping discovery module
[X] [4] infogather:tll_calc - TCP and UDP based TTL distance calculation
[X] [5] infogather:portscan - TCP and UDP PortScanner
[X] [6] fingerprint:icmp_echo - ICMP Echo request fingerprinting module
[X] [7] fingerprint:icmp_tstamp - ICMP Timestamp request fingerprinting module
[X] [8] fingerprint:icmp_amask - ICMP Address mask request fingerprinting module
[X] [9] fingerprint:icmp_port_unreach - ICMP port unreachable fingerprinting module
[X] [10] fingerprint:tcp_hshake - TCP Handshake fingerprinting module
[X] [11] fingerprint:tcp_rst - TCP RST fingerprinting module
[X] [12] fingerprint:smb - SMB fingerprinting module
[X] [13] fingerprint:snmp - SNMPv2c fingerprinting module
[+] 13 modules registered
[+] Initializing scan engine
[+] Running scan engine
[-] ping:tcp_ping module: no closed/open TCP ports known on 89.43.3.80. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 89.43.3.80. Module test failed
[-] No distance calculation. 89.43.3.80 appears to be dead or no ports known
[+] Host: 89.43.3.80 is up (Guess probability: 50%)
[+] Target: 89.43.3.80 is alive. Round-Trip Time: 0.44765 sec
[+] Selected safe Round-Trip Time value is: 0.89530 sec
[-] fingerprint:tcp_hshake Module execution aborted (no open TCP ports known)
[-] fingerprint:smb need either TCP port 139 or 445 to run
[-] fingerprint:snmp: need UDP port 161 open
[+] Primary guess:
[+] Host 89.43.3.80 Running OS: 0-j0[U (Guess probability: 100%)
[+] Other guesses:
[+] Host 89.43.3.80 Running OS: 0p00[U (Guess probability: 91%)
[+] Host 89.43.3.80 Running OS: 00i0[U (Guess probability: 91%)
[+] Host 89.43.3.80 Running OS: 0-j0[U (Guess probability: 91%)
[+] Host 89.43.3.80 Running OS: 0p00[U (Guess probability: 91%)
[+] Host 89.43.3.80 Running OS: 0p00[U (Guess probability: 91%)
[+] Host 89.43.3.80 Running OS: 0p00[U (Guess probability: 91%)
[+] Host 89.43.3.80 Running OS: 0p00[U (Guess probability: 91%)
[+] Host 89.43.3.80 Running OS: 00i0[U (Guess probability: 91%)
[+] Host 89.43.3.80 Running OS: 00i0[U (Guess probability: 91%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```

خروجی دستور xprobe2 89.43.3.80

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

5 Captured ARP Req/Rep packets, from 1 hosts. Total size: 210

-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
172.17.0.1   00:15:5d:8c:48:4a   5      210  Microsoft Corporation
-----
```

خروجی دستور sudo netdiscover -i eth0 -r 89.43.3.80/16

لینک های استفاده شده:

<http://ports.my-addr.com/check-all-open-ports-online.php>