دانشگاه صنعتی امیرکبیر

(پلی‌تکنیک تهران)

دانشکده مهندسی کامپیوتر

امنیت و اطلاعات شبکه

(پاییز ۱۴۰۱)

تمرین عملی اول

محمد چوپان ۹۸۳۱۱۲۵

۲. ابزار طراحی شده می‌بایست شامل موارد زیر باشد:

- گرفتن ping از آی پی خاص

برای گرفتن ping از کتابخانه subprocess استفاده کردهایم . که با سیستم عامل ارتباط برقرار کرده و ping را می گیرد.

```python
import subprocess


def ping(host):

    p1 = subprocess.Popen(['ping', '-c 8', host], stdout=subprocess.PIPE)

    output = p1.communicate()[0]

    print(output.decode('utf-8'))


inp = input("Enter the IP or Domain: ")
ping(inp)

```

خروجی :

```
mohamad@mamads:/mnt/mamads/uni/7/Securety/HW/HW2$ python3 ping.py
Enter the IP or Domain: google.com
PING google.com (142.250.176.206) 56(84) bytes of data.
64 bytes from lga34s37-in-f14.1e100.net (142.250.176.206): icmp_seq=1 ttl=59 time=695 ms
64 bytes from lga34s37-in-f14.1e100.net (142.250.176.206): icmp_seq=2 ttl=59 time=344 ms
64 bytes from lga34s37-in-f14.1e100.net (142.250.176.206): icmp_seq=3 ttl=59 time=245 ms
64 bytes from lga34s37-in-f14.1e100.net (142.250.176.206): icmp_seq=4 ttl=59 time=327 ms
64 bytes from lga34s37-in-f14.1e100.net (142.250.176.206): icmp_seq=5 ttl=59 time=195 ms
64 bytes from lga34s37-in-f14.1e100.net (142.250.176.206): icmp_seq=6 ttl=59 time=619 ms
64 bytes from lga34s37-in-f14.1e100.net (142.250.176.206): icmp_seq=7 ttl=59 time=286 ms
64 bytes from lga34s37-in-f14.1e100.net (142.250.176.206): icmp_seq=8 ttl=59 time=192 ms

--- google.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7054ms
rtt min/avg/max/mdev = 191.896/362.820/694.943/178.497 ms
```

برای این قسمت با استفاده از nmap و دریافت بازه مد نظر خود عملیات اسکن انجام می شود. خروجی یک dictionary است که قسمت scan آن اطلاعات هر ip را می دهد و می توان به وضعیت هر host دسترسی داشت و تابع create هم وظیفه دارد که ورودی مد نظر تابع active را بسازد.

activeHosts.py > active_hosts

```python
import nmap


def active_hosts(network):
    nm_scan = nmap.PortScanner()
    scan_range = nm_scan.scan(hosts=network)

    for x in nm_scan.all_hosts():
        state = scan_range['scan'][x]['status']['state']
        if state == 'up':
            print(x, '-> Live')


def create_network_string(network, start, last):
    network_parts = network.split('.')
    network = network_parts[0] + '.' + network_parts[1] + '.' + network_parts[2] + '.' + start + '-' + last
    print(network)
    return network


network_inp = input("Enter the Network Address: ")
start_inp = input("Enter the Starting Number: ")
last_inp = input("Enter the Last Number: ")

active_hosts(create_network_string(network_inp, start_inp, last_inp))

```

خروجی :

```
mohamad@mamads:/mnt/mamads/uni/7/Securety/HW/HW2$ python3 activeHosts.py
Enter the Network Address: 89.43.3.0
Enter the Starting Number: 60
Enter the Last Number: 70
89.43.3.60-70
89.43.3.60 -> Live
89.43.3.61 -> Live
89.43.3.62 -> Live
89.43.3.63 -> Live
89.43.3.64 -> Live
89.43.3.65 -> Live
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
```

- اسکن پورت‌های باز یک هاست فعال

با استفاده از کتابخانه nmap میتوان علاوه بر ip پورت هم به تابع داد و پورت هایی که وضعیت باز هستند را نشان داد.

```python
import nmap


def open_ports(ip, ports):
    nm_scan = nmap.PortScanner()
    scan_range = nm_scan.scan(hosts=ip, ports=ports)
    print(scan_range)
    ports_range = scan_range['scan'][ip]['tcp'].keys()
    for i in ports_range:
        port_state = scan_range['scan'][ip]['tcp'][i]['state']
        if port_state == 'open':
            print(i, '-> open')




ip_inp = input("Enter the remote host IP to scan: ")
start_inp = input("Enter the Start port number: ")
last_inp = input("Enter the Last port number: ")

open_ports(ip_inp, start_inp + '-' + last_inp)
```

خروجی :

```
mohamad@mamads:/mnt/mamads/uni/7/Securety/HW/HW2$ python3 openPorts.py
Enter the remote host IP to scan: 89.43.3.170
Enter the Start port number: 0
Enter the Last port number: 500
80 -> open
443 -> open
```

بخش دوم :

پس از انجام بخش اول تمرین، می‌بایست، با ابزارهای namp، netdiscover، hping3 صحت انجام کار خود را بررسی نمایید و پس از آن با استفاده از ابزارهای whatweb، httprint، xprube2 و یا سایت‌های آنلاین، اطلاعات بیشتری درباره هاست‌های فعالی که در محدوده آی‌پی گفته شده یافته‌اید، بدست آورید.

نکته۱: لازم به ذکر است اگر از سایت‌های آنلاین برای بدست آوردن اطلاعات اضافی استفاده می‌کنید، آدرس آن را در گزارش خود قید نمایید.

نکته۲: لازم است هنگام کار با ابزار nmap موارد زیر را در وارد کردن دستورات لحاظ فرمایید:

- TCP full scan
- Stealth scan
- UDP scan
- Fingerprint scan
- Idle scan

صحت سنجی :

با استفاده از ابزار nmap :

tcp full scan:

```
mohamad@mamads:~$ nmap -T4 -sT 89.43.3.170
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-04 23:15 +0330
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (0.44s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
25/tcp   filtered smtp
80/tcp   open     http
443/tcp  open     https
1723/tcp open     pptp
2000/tcp open     cisco-sccp
8291/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 35.63 seconds
```

:Stealth scan

```
mohamad@mamads:~$ sudo nmap -sS 89.43.3.170
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-04 23:18 +0330
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (0.44s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
25/tcp   filtered smtp
80/tcp   open     http
443/tcp  open     https
1723/tcp open     pptp
2000/tcp open     cisco-sccp
8291/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 38.26 seconds
```

UDP scan :

```
mohamad@mamads:~$ sudo nmap -sU 89.43.3.170
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-04 23:18 +0330
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (0.35s latency).
Not shown: 990 open|filtered ports
PORT     STATE  SERVICE
7/udp    closed echo
123/udp  closed ntp
161/udp  closed snmp
177/udp  closed xdmcp
1645/udp closed radius
1812/udp closed radius
2049/udp closed nfs
3283/udp closed netassistant
5351/udp closed nat-pmp
5353/udp closed zeroconf

Nmap done: 1 IP address (1 host up) scanned in 24.29 seconds
```

Fingerprint scan :

```
mohamad@mamads:~$ sudo nmap -O 89.43.3.170
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-04 23:19 +0330
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (0.30s latency).
Not shown: 994 closed ports
PORT     STATE    SERVICE
25/tcp   filtered smtp
80/tcp   open     http
443/tcp  open     https
1723/tcp open     pptp
2000/tcp open     cisco-sccp
8291/tcp filtered unknown
Device type: general purpose|storage-misc
Running (JUST GUESSING): Linux 2.6.X (88%), HP embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/h:hp:p2000_g3
Aggressive OS guesses: Linux 2.6.32 (88%), HP P2000 G3 NAS device (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.14 seconds
```

Idle scan :

```
mohamad@mamads:~$ sudo nmap -Pn -p- -sI 89.43.3.170
Starting Nmap 7.80 ( https://nmap.org ) at 2022-11-04 23:19 +0330
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
```

با استفاده از ابزار net discovery :

```
mohamad@mamads:~$ sudo netdiscover -r 89.43.3.170/24 -c 20 -P -f
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------

-- Active scan completed, 0 Hosts found.
```

```
mohamad@mamads:~$ sudo netdiscover -r 89.43.3.170/8 -c 20 -P -f
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     78:54:2e:d9:6d:24      1      42  D-Link International
```

```
mohamad@mamads:~$ sudo netdiscover -r 89.43.0.0/24 -c 20 -P -f

 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------

-- Active scan completed, 0 Hosts found.
```

```
mohamad@mamads:~$ sudo netdiscover -r 89.43.3.0/24 -c 20 -P -f

 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------

-- Active scan completed, 0 Hosts found.
mohamad@mamads:~$
```

```
mohamad@mamads:~$ sudo netdiscover -r 89.43.0.0/8 -c 20 -P -f

 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
 192.168.1.1     78:54:2e:d9:6d:24      1      42  D-Link International

^Z
[1]+  Stopped                 sudo netdiscover -r 89.43.0.0/8 -c 20 -P -f
```

با استفاده از ابزار hping3 :

با کمک این ابزار می توان بسته تولید کرد و پروتکل TCP/IP را مورد آنالیز قرار داد. پارامتر های مهمی که دارد این ها اند

-S : send syn

-p : destination port

-c : number of packets

در قسمت قبل پورت های فعال آن ۸۰ ۴۴۳ هستند برای بررسی میبینیم :

```
mohamad@mamads:~$ sudo hping3 89.43.3.170 -S -p 80 -c 4
HPING 89.43.3.170 (tun0 89.43.3.170): S set, 40 headers + 0 data bytes
len=44 ip=89.43.3.170 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=42340 rtt=655.8 ms

--- 89.43.3.170 hping statistic ---
4 packets transmitted, 1 packets received, 75% packet loss
round-trip min/avg/max = 655.8/655.8/655.8 ms
mohamad@mamads:~$ sudo hping3 89.43.3.170 -S -p 443 -c 4
HPING 89.43.3.170 (tun0 89.43.3.170): S set, 40 headers + 0 data bytes
len=44 ip=89.43.3.170 ttl=64 DF id=0 sport=443 flags=SA seq=0 win=42340 rtt=2231.8 ms
len=44 ip=89.43.3.170 ttl=64 DF id=0 sport=443 flags=SA seq=1 win=42340 rtt=1259.8 ms
len=44 ip=89.43.3.170 ttl=64 DF id=0 sport=443 flags=SA seq=2 win=42340 rtt=1583.6 ms
len=44 ip=89.43.3.170 ttl=64 DF id=0 sport=443 flags=SA seq=3 win=42340 rtt=583.6 ms

--- 89.43.3.170 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 583.6/1414.7/2231.8 ms
mohamad@mamads:~$ sudo hping3 89.43.3.170 -S -p 80 -c 4
HPING 89.43.3.170 (tun0 89.43.3.170): S set, 40 headers + 0 data bytes
len=44 ip=89.43.3.170 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=42340 rtt=1099.6 ms
len=44 ip=89.43.3.170 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=42340 rtt=863.5 ms
DUP! len=44 ip=89.43.3.170 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=42340 rtt=2039.7 ms
DUP! len=44 ip=89.43.3.170 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=42340 rtt=1739.5 ms

--- 89.43.3.170 hping statistic ---
3 packets transmitted, 4 packets received, -33% packet loss
round-trip min/avg/max = 863.5/1435.6/2039.7 ms
mohamad@mamads:~$ sudo hping3 89.43.3.170 -S -p 80 -c 4
HPING 89.43.3.170 (tun0 89.43.3.170): S set, 40 headers + 0 data bytes
len=44 ip=89.43.3.170 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=42340 rtt=1787.8 ms
len=44 ip=89.43.3.170 ttl=64 DF id=0 sport=80 flags=SA seq=1 win=42340 rtt=1187.9 ms
len=44 ip=89.43.3.170 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=42340 rtt=931.7 ms
DUP! len=44 ip=89.43.3.170 ttl=64 DF id=0 sport=80 flags=SA seq=2 win=42340 rtt=1839.7 ms

--- 89.43.3.170 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 931.7/1436.8/1839.7 ms
```

با توجه به وضعیت اینترنت نتایجی میگیریم که تایید میکند .

اطلاعات بیشتر :

برنامه whatweb :

```
mohamad@mamads:~$ whatweb 89.43.3.170 -v
/usr/lib/ruby/vendor_ruby/target.rb:188: warning: URI.escape is obsolete
WhatWeb report for http://89.43.3.170
Status    : 500 Internal Server Error
Title     : <None>
IP        : 89.43.3.170
Country   : ROMANIA, RO

Summary   : UncommonHeaders[x-content-type-options]

Detected Plugins:
[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : x-content-type-options (from headers)

HTTP Headers:
        HTTP/1.1 500 Internal Server Error
        Content-Type: text/plain; charset=utf-8
        X-Content-Type-Options: nosniff
        Date: Fri, 04 Nov 2022 21:13:57 GMT
        Content-Length: 71
        Connection: close
```

برنامه xprobe2 :

```
mohamad@mamads:~$ sudo xprobe2 89.43.3.170 -v

Xprobe2 v.0.3 Copyright (c) 2002-2005 fyodor@o0o.nu, ofir@sys-security.com, meder@o0o.nu

[+] Target is 89.43.3.170
[+] 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:ttl_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 89.43.3.170. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 89.43.3.170. Module test failed
[-] No distance calculation. 89.43.3.170 appears to be dead or no ports known
[+] Host: 89.43.3.170 is up (Guess probability: 50%)
[+] Target: 89.43.3.170 is alive. Round-Trip Time: 0.99522 sec
[+] Selected safe Round-Trip Time value is: 1.99045 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 89.43.3.170 Running OS: ÐYH%V (Guess probability: 91%)
[+] Other guesses:
[+] Host 89.43.3.170 Running OS: ÐYH%V (Guess probability: 91%)
[+] Host 89.43.3.170 Running OS: ÐYH%V (Guess probability: 91%)
[+] Host 89.43.3.170 Running OS: ÐYH%V (Guess probability: 91%)
[+] Host 89.43.3.170 Running OS: ÐYH%V (Guess probability: 91%)
[+] Host 89.43.3.170 Running OS: ÐYH%V (Guess probability: 91%)
[+] Host 89.43.3.170 Running OS: ÐYH%V (Guess probability: 91%)
[+] Host 89.43.3.170 Running OS: ÐYH%V (Guess probability: 91%)
[+] Host 89.43.3.170 Running OS: ÐYH%V (Guess probability: 91%)
[+] Host 89.43.3.170 Running OS: ÐYH%V (Guess probability: 91%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```