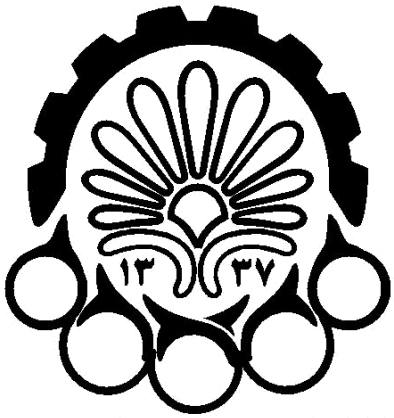


دانشگاه صنعتی امیرکبیر

(پلی تکنیک تهران)

سپهر مقیسه/۹۸۳۱۱۰۳

مبانی امنیت

دکتر شهریاری

پاییز ۱۴۰۱

بخش اول (ابزارنویسی):

در هر سه ابزار نوشته شده در این بخش، با استفاده از سوییچ `-h` برای ابزارها، می‌توان راهنمای آنها را مشاهده کرد. به عنوان مثال `python ping.py -h` خروجی زیر را خواهد داشت.

```
usage: myping [-h] [-n number_of_packets] [-t seconds] [-s bytes] host

positional arguments:
  host

optional arguments:
  -h, --help            show this help message and exit
  -n number_of_packets
  -t seconds, --timeout seconds
  -s bytes, --size bytes
```

ابزار پینگ: برای ساخت این ابزار از کتابخانه ping3 استفاده شده است. در این برنامه پس از دریافت آرگومانها از خط فرمان، به تعداد دفعات مشخص شده پکت ICMP به هوست مشخص شده ارسال می‌شود و نتایج هر کدام نمایش داده می‌شود. خروجی پینگ گوگل و سرویس 8.8.8.8 در شکل زیر آمده است.

```
Pinging google.com
64 bytes from google.com: time=222ms
64 bytes from google.com: time=203ms
64 bytes from google.com: time=202ms
64 bytes from google.com: time=205ms
64 bytes from google.com: time=200ms
5 packet(s) transmitted, 5 received, 0.0% packet loss
```

ابزار یافتن هوست‌های فعال: در این ابزار، با ارسال پکت TCP SYN به پورت ۸۰ هوست‌های مشخص شده، هوست‌های فعال شناسایی می‌شوند (در صورت فعال بودن هوست، پکت RST یا SYN/ACK بازمی‌گردد). نحوه وارد کردن بازه IPهای مورد نظر، مانند ابزار nmap است. به عنوان نمونه، بازههای IP زیر را توسط برنامه اسکن می‌کنیم.

89.43.2.0 - 89.43.2.255

89.43.3.0 - 89.43.3.255

89.43.4.0 - 89.43.4.255

نتیجه هر یک از سه بازه نوشته شده در فایل‌های result_host_scan{1-3}.txt ذخیره شده است.

ابزار یافتن پورتهای باز: برای این بخش روی هر پورت پکت SYN ارسال می‌شود و در صورت باز بودن آن پورت، نتیجه مشخص می‌شود. برای نمونه، سه هوست زیر را با این ابزار بررسی می‌کنیم.

89.43.2.32 89.43.3.64 89.43.4.37

```
Searching for open ports...
89.43.2.32:80 is open.
89.43.3.64:80 is open.
98.43.4.37:80 is open.
```

در این ابزار، تنها پورتهای باز (open) نمایش داده می‌شوند و پورتهای فیلتر شده (filtered) نمایش داده نمی‌شوند.

بخش دوم (بررسی ابزارهای آماده):

از آنجا که به نظر می‌رسد تمام هوست‌ها در بازه IPهای بررسی شده مانند یکدیگر هستند و فقط پورت ۸۰ آنها باز است، در اسکن‌های زیر تنها دو هوست را بررسی می‌کنیم.

ابزار nmap: در اسکن TCP full با برقراری یک اتصال (ساخت socket و فراخوانی متد (connect()) باز بودن پورت بررسی می‌شود. با استفاده از سوییچ sT- این اسکن قابل انجام است (پورتها را نیز می‌توان با سوییچ p- مشخص کرد اما به علت طول کشیدن اسکن، تنها از هزار پورت پیش‌فرض اول استفاده شده است).

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-11 20:56 +0330
Nmap scan report for 89.43.2.32
Host is up (0.076s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 16.51 seconds
```

در اسکن stealth که در بخش اول هم از آن استفاده شد، تنها پکت SYN ابتدایی برای برقراری اتصال استفاده می‌شود. این کار با سوییچ sS- امکانپذیر است.

در اسکن UDP (سوییچ sU-) به پورتهای مشخص شده یک پکت UDP ارسال می‌شود و بسته به پاسخ دریافتی (یا عدم دریافت آن)، مطابق جدول زیر وضعیت پورت مشخص می‌شود.

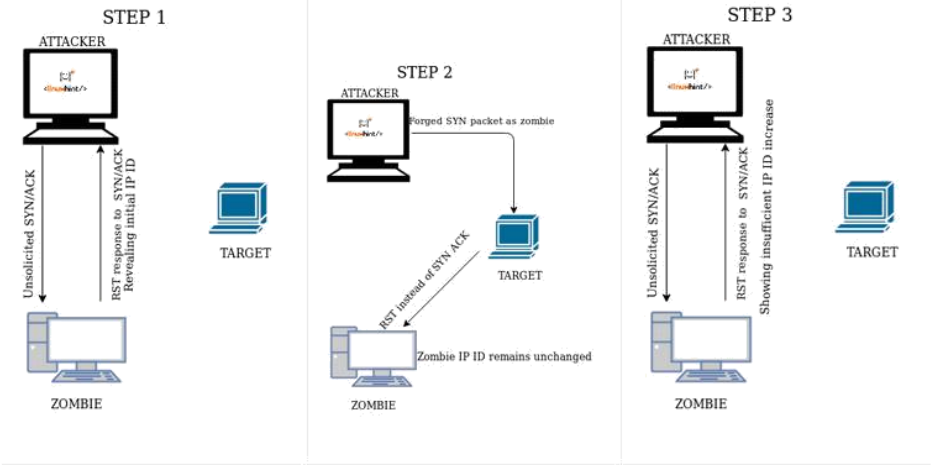
Probe Response	Assigned State
Any UDP response from target port (unusual)	`open`
No response received (even after retransmissions)	`open|filtered`
ICMP port unreachable error (type 3, code 3)	`closed`
Other ICMP unreachable errors (type 3, code 1, 2, 9, 10, or 13)	`filtered`

در اینجا، با ترکیب هر دوی این اسکن‌ها، هزار پورت اول را بر روی هوست‌ها بررسی می‌کنیم.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-11 21:01 +0330
Nmap scan report for 89.43.2.32
```

در اسکن idle (سوییچ `-sI`) اثری از حمله‌کننده روی هدف باقی نمی‌ماند و هدف تنها با یک zombie ارتباط برقرار می‌کند. نحوه انجام این اسکن در صورت باز بودن پورت در شکل زیر آمده است.

STEP 1	STEP 2	STEP 2
Same as above	In this case the target answers the zombie with a RST packet instead of a SYN/ACK, preventing the zombie from sending the RST which may increase its IP ID.	The attacker sends a SYN/ACK and the zombie answers with only increases made when interacting with the attacker and not with the target.



بخش دشوار این اسکن، یافتن یک هوست به عنوان زامبی است. یک نمونه از این اسکن در شکل زیر آمده است که متاسفانه زامبی این ضعف امنیتی را ندارد (آدرس زامبی توسط `nmap -p80 --script ipidseq - iR 10` پیدا شده است).

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-11 21:07 +0330
Idle scan zombie 145.34.117.162 (145.34.117.162) port 80 cannot be used because it has not returned any of our probes -- perhaps it is down or firewalled.
QUITTING!
```

اسکن هوست‌های فعال را نیز می‌توان با سوییچ `-sS` و دادن بازه IP انجام داد.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-11-11 21:04 +0330
Nmap scan report for 89.43.2.0
Host is up (0.099s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 89.43.2.1
Host is up (0.070s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 89.43.2.2
Host is up (0.069s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 89.43.2.3
Host is up (0.084s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 89.43.2.4
Host is up (0.088s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 89.43.2.5
Host is up (0.091s latency).
```

ابزار netdiscover: این ابزار جهت یافتن دستگاههای موجود در شبکه با استفاده از پکت‌های ARP استفاده می‌شود. با استفاده از دستور `netdiscover -r 192.168.1.0/24`، دستگاههای موجود در شبکه داخلی را بررسی می‌کنیم.

```
Currently scanning: 192.168.1.0/24   |   Screen View: Unique Hosts

24 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 1386
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.11                        22    1302                tronics Co.,Ltd
192.168.1.1                          1      42                national
192.168.1.2                          1      42                oration Limited
```

ابزار hping3: این ابزار برای ارسال پکت‌های ICMP، UDP و TCP دلخواه استفاده می‌شود. برای ارسال پکت ICMP و پینگ کردن در این ابزار، می‌توان به شکل زیر عمل کرد.

```
HPING 89.43.4.25 (wlp2s0 89.43.4.25): icmp mode set, 28 headers + 0 data bytes
len=28 ip=89.43.4.25 ttl=242 id=23494 icmp_seq=0 rtt=48.0 ms
len=28 ip=89.43.4.25 ttl=242 id=57150 icmp_seq=1 rtt=35.9 ms
len=28 ip=89.43.4.25 ttl=242 id=16057 icmp_seq=2 rtt=35.6 ms
len=28 ip=89.43.4.25 ttl=242 id=29292 icmp_seq=3 rtt=35.3 ms
len=28 ip=89.43.4.25 ttl=242 id=26768 icmp_seq=4 rtt=34.8 ms
^C
--- 89.43.4.25 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 34.8/37.9/48.0 ms
```

در این ابزار می‌توان فلگ SYN پروتکل TCP را ست کرد (سوییچ syn--) و از طریق آن فعال بودن هوست یا باز بودن پورت را بررسی کرد. در شکل زیر، در دستور اول پکت SYN به پورت ۸۰ یک هوست ارسال شده است و SYN/ACK (SA) بازگردانده شده است که

به معنای باز بودن پورت است. در دستور دوم به پور ت ۴۴۳ پکت SYN را ارسال کردهایم که RST/ACK (RA) بازگردانده شده است. به این معنی که این پورت باز نیست. اما از RST می‌توان دریافت که این هوست فعال است. در دستور آخر نیز، از scan mode استفاده شده است و پکت SYN را برای بازه پورتهای ۱ تا ۱۰۲۳ فرستادهایم

ابزار xprobe2: این ابزار برای حدس زدن نوع سیستم عامل مورد استفاده روی یک هوست از روی برخی رفتارهای آن در برابر پکت‌های دریافتی استفاده می‌شود. با دریافت از این آدرس و کامپایل آن، سیستم عامل یک هوست را بررسی می‌کنیم. همانطور که در شکل زیر می‌بینیم، این دستگاه به احتمال زیاد از Cisco IOS 12.0 استفاده می‌کند. هر چند به نظر می‌رسد این ابزار به علت قدیمی بودن، امکان شناسایی سیستم‌عامل‌های جدید را ندارد.

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

[+] Target is 89.43.4.25
[+] 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 89.43.4.25. Module test failed
[-] ping:udp_ping module: no closed/open UDP ports known on 89.43.4.25. Module test failed
[-] No distance calculation. 89.43.4.25 appears to be dead or no ports known
[+] Host: 89.43.4.25 is up (Guess probability: 50%)
[+] Target: 89.43.4.25 is alive. Round-Trip Time: 0.49149 sec
[+] Selected safe Round-Trip Time value is: 0.98297 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 89.43.4.25 Running OS: "Cisco IOS 12.0" (Guess probability: 100%)
[+] Other guesses:
[+] Host 89.43.4.25 Running OS: "Cisco IOS 12.3" (Guess probability: 100%)
[+] Host 89.43.4.25 Running OS: "Cisco IOS 12.2" (Guess probability: 100%)
[+] Host 89.43.4.25 Running OS: "Cisco IOS 11.3" (Guess probability: 100%)
[+] Host 89.43.4.25 Running OS: "Cisco IOS 11.2" (Guess probability: 100%)
[+] Host 89.43.4.25 Running OS: "Cisco IOS 11.1" (Guess probability: 100%)
[+] Host 89.43.4.25 Running OS: "Linux Kernel 2.2.22" (Guess probability: 93%)
[+] Host 89.43.4.25 Running OS: "Linux Kernel 2.4.15" (Guess probability: 93%)
[+] Host 89.43.4.25 Running OS: "Linux Kernel 2.2.22" (Guess probability: 93%)
[+] Host 89.43.4.25 Running OS: "Linux Kernel 2.4.17" (Guess probability: 93%)
[+] Cleaning up scan engine
[+] Modules deinitialized
[+] Execution completed.
```