شایان به ذکر است که می‌توانستیم از `-p0-` به جای `-p 1-65535` استفاده کنیم.

پورت‌های باز

21/tcp	open	tcpwrapped	
22/tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp	open	http	Apache httpd 2.4.7 ((Ubuntu))
554/tcp	open	rtsp?	
1723/tcp	open	tcpwrapped	
5060/tcp	open	sip?	
9929/tcp	open	nping-echo	Nping echo
31337/tcp	open	tcpwrapped	

برنامه‌های در حال اجرا روی آن‌ها

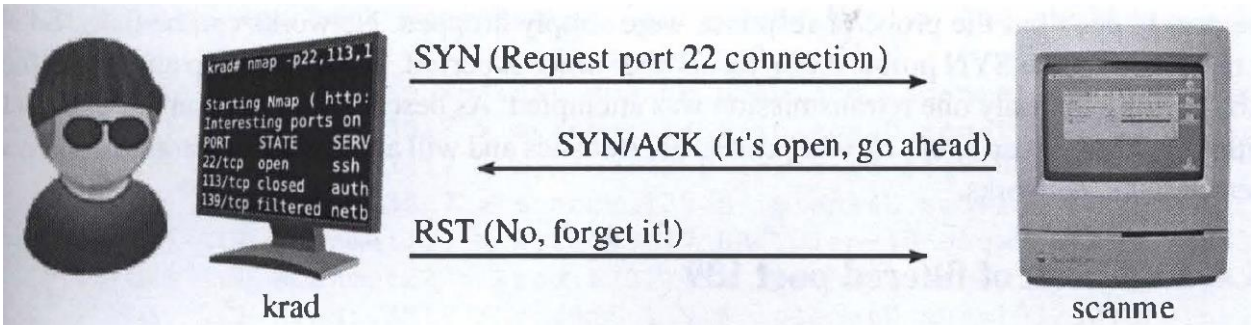
Port	Protocol	State	Service	Version
21	tcp	open	tcpwrapped	
22	tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80	tcp	open	http	Apache httpd 2.4.7 ((Ubuntu))
135	tcp	filtered	msrpc	
136	tcp	filtered	profile	
137	tcp	filtered	netbios-ns	
138	tcp	filtered	netbios-dgm	
139	tcp	filtered	netbios-ssn	
445	tcp	filtered	microsoft-ds	
554	tcp	open	rtsp	
1723	tcp	open	tcpwrapped	
4475	tcp	filtered		
4786	tcp	filtered	smart-install	
5060	tcp	open	sip	
5555	tcp	filtered	freeciv	
7547	tcp	filtered	cwmp	
9929	tcp	open	nping-echo	Nping echo
21002	tcp	filtered		
21020	tcp	filtered		
21111	tcp	filtered		
22001	tcp	filtered	optocontrol	
31337	tcp	open	tcpwrapped	

فرق بین TCP SYN و TCP Connect

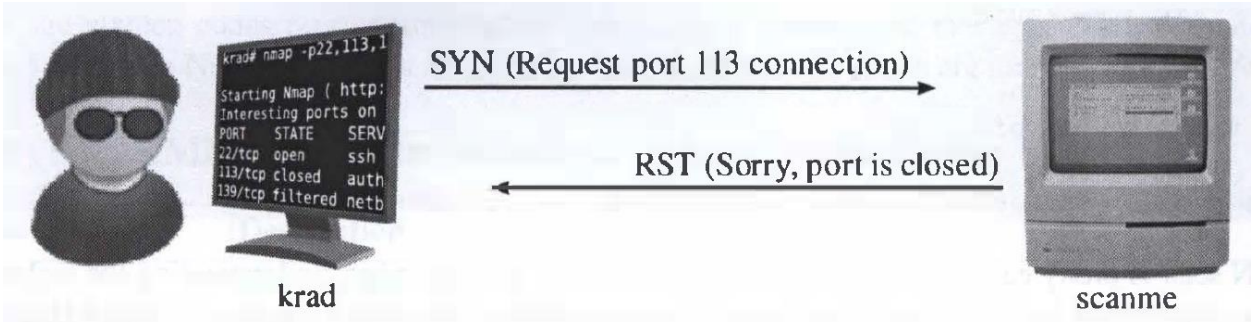
در واقع اِسکن **TCP SYN** معروف‌ترین اِسکن **nmap** است و اِسکن پیشفرض آن نیز هست؛ زیرا نسبت به اِسکن‌های دیگر سریع‌تر است و همچنین احتمال بلاک شدن آن توسط فایروال‌ها کمتر است.

ضمن آن که در هنگام بررسی وضعیت پورت‌ها، **TCP SYN** تعریفی شفاف ارائه می‌دهد.

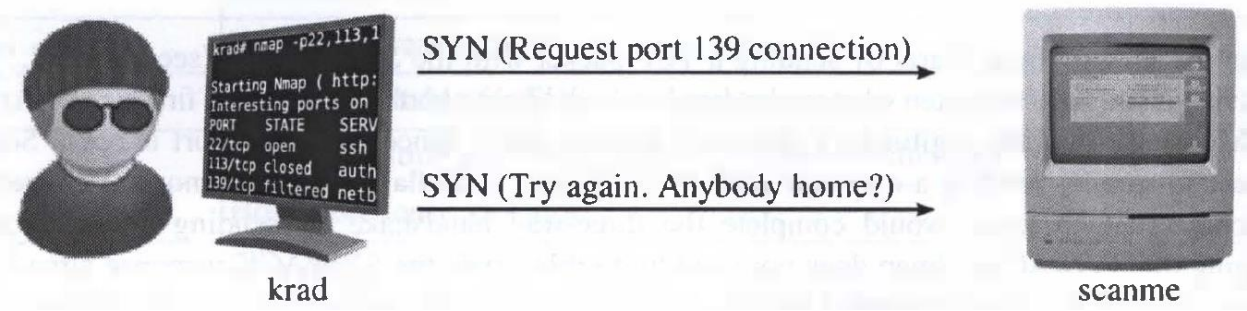
این اِسکن بر پایه‌ی **TCP Three Way Handshaking** است و نیاز به دسترسی `root` به جهت ارسال **raw-packet** است.



نحوه‌ی تشخیص پورت **باز** توسط **TCP SYN**



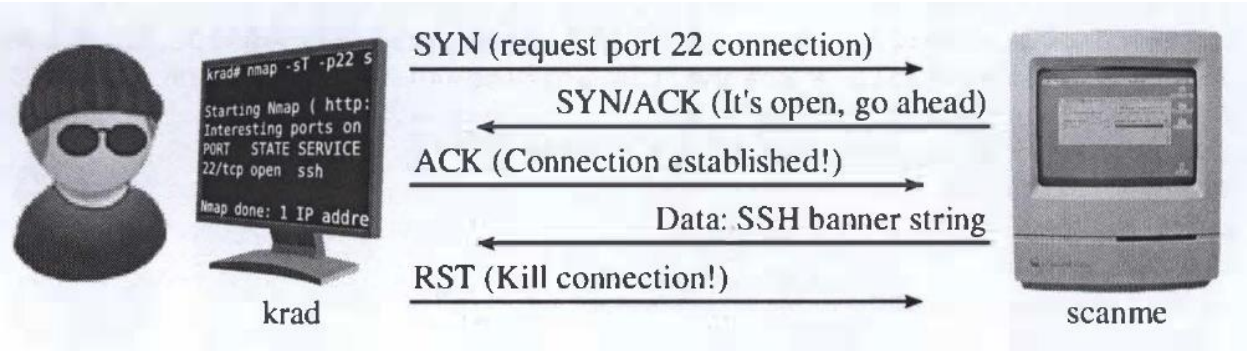
نحوه‌ی تشخیص پورت **بسته** توسط **TCP SYN**



نحوه‌ی تشخیص پورت **فیلتر شده** توسط **TCP SYN**

❖ *پورت‌های فیلتر شده، پورت‌هایی هستند که هیچ جوابی از آن‌ها دریافت نمی‌شود. رایج‌ترین دلیل آن بلاک شدن بسته‌ها توسط فایروال است.*

در اِسکن **TCP Connect**، **nmap** از سیستم‌عامل درخواست می‌کند تا یک Connection با سرور مقصد ایجاد کند اما مشکل این اِسکن، زمان‌بر بودن آن و همچنین نیاز آن به تولید تعداد زیادی بسته است. اما از طرفی امکان این که سرور مقصد اجازه‌ی برقراری ارتباط را بدهد، در این اِسکن بیشتر است؛ زیرا همانند دیگر برنامه‌های تحت شبکه (مانند مرورگرها) سعی در برقراری با سرور می‌کند.

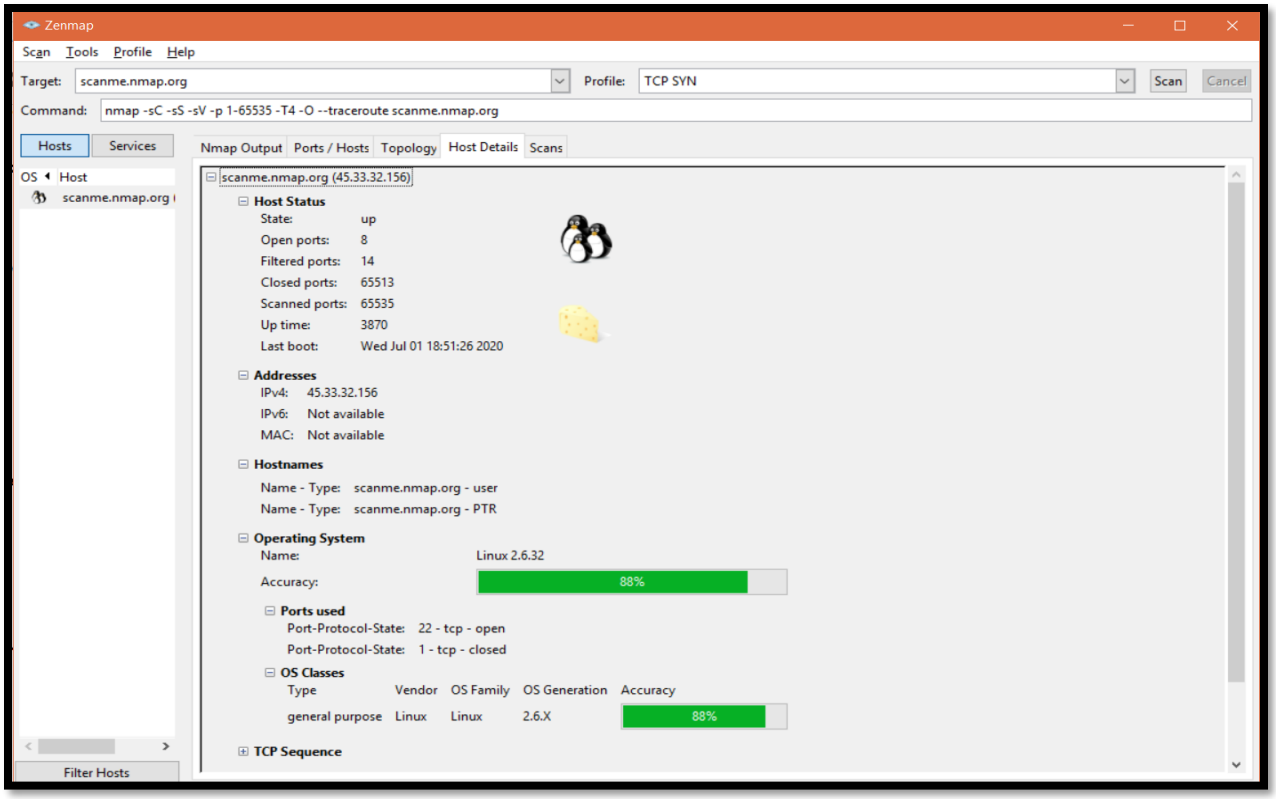


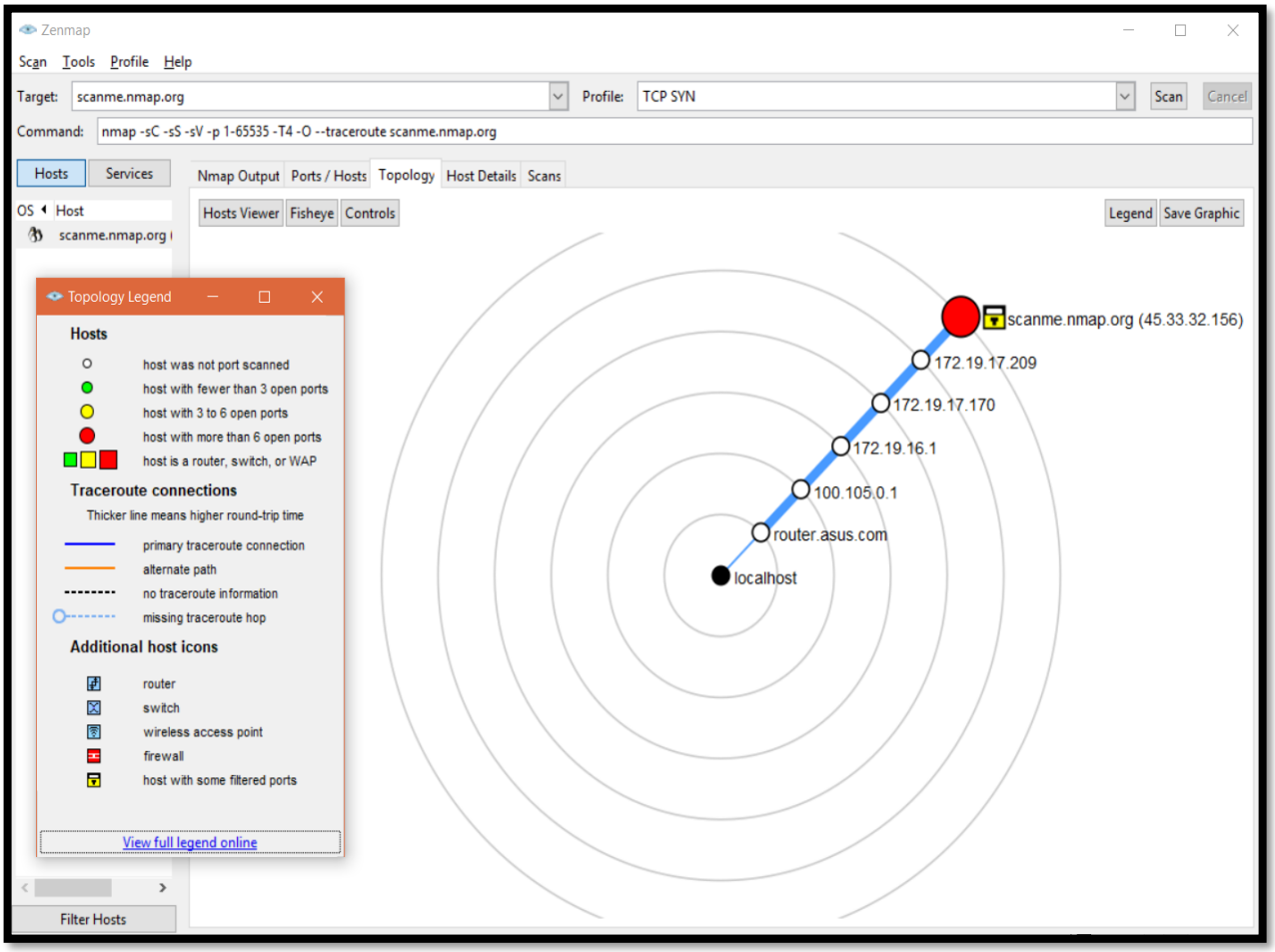
نحوه‌ی تشخیص پورت **باز** توسط **TCP Connect**

پس در نهایت، فرق میان این دو اِسکن آن است که **TCP Connect** یک ارتباط کامل با سرور مقصد برقرار می‌کند (فرایند برقراری ارتباط را کامل طی می‌کند) در حالی که **TCP SYN** تنها نصف این فرایند را طی می‌کند و ارتباطی نصفه‌نیمه برقرار می‌کند.

نتیجه‌ی nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-01 19:44 Iran Daylight
Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.14s latency).
Not shown: 65513 closed ports
PORT STATE SERVICE VERSION
21/tcp open tcpwrapped
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;
protocol | ssh-hostkey:
| 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
| 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_ 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp filtered msrpc
136/tcp filtered profile
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
554/tcp open rtsp?
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
1723/tcp open tcpwrapped
|_pptp-version: ERROR: Script execution failed (use -d to debug)
4475/tcp filtered unknown
4786/tcp filtered smart-install
5060/tcp open sip?
5555/tcp filtered freeciv
7547/tcp filtered cwmp
9929/tcp open nping-echo Nping echo
21002/tcp filtered unknown
21020/tcp filtered unknown
21111/tcp filtered unknown
22001/tcp filtered optocontrol
31337/tcp open tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (88%), HP P2000 G3 NAS device (88%),
Infomir MAG-250 set-No exact OS matches for host (test conditions non-
ideal).
Network Distance: 6 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 1.00 ms router.asus.com (192.168.1.1)
2 55.00 ms 100.105.0.1
3 56.00 ms 172.19.16.1
4 58.00 ms 172.19.17.170
5 61.00 ms 172.19.17.209
6 59.00 ms scanme.nmap.org (45.33.32.156)
OS and Service detection performed. Please report any incorrect results
at https://nmap.org/Nmap done: 1 IP address (1 host up) scanned in 708.50
seconds
```


Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: TCP SYN
Scan
Cancel
Command: nmap -sC -sS -sV -p 1-65535 -T4 -O --traceroute scanme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
scanme.nmap.org
scanme.nmap.org (45.33.32.156)
Host Status
State: up
Open ports: 8
Filtered ports: 14
Closed ports: 65513
Scanned ports: 65535
Up time: 3870
Last boot: Wed Jul 01 18:51:26 2020
Addresses
IPv4: 45.33.32.156
IPv6: Not available
MAC: Not available
Hostnames
Name - Type: scanme.nmap.org - user
Name - Type: scanme.nmap.org - PTR
Operating System
Name: Linux 2.6.32
Accuracy: 88%
Ports used
Port-Protocol-State: 22 - tcp - open
Port-Protocol-State: 1 - tcp - closed
OS Classes
Type Vendor OS Family OS Generation Accuracy
general purpose Linux Linux 2.6.X 88%
TCP Sequence
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: scanme.nmap.org
Profile: TCP SYN
Scan
Cancel
Command: nmap -sC -sS -sV -p 1-65535 -T4 -O --traceroute scanme.nmap.org
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
Topology Legend
Hosts
host was not port scanned
host with fewer than 3 open ports
host with 3 to 6 open ports
host with more than 6 open ports
host is a router, switch, or WAP
Traceroute connections
Thicker line means higher round-trip time
primary traceroute connection
alternate path
no traceroute information
missing traceroute hop
Additional host icons
router
switch
wireless access point
firewall
host with some filtered ports
View full legend online
scanme.nmap.org (45.33.32.156)
172.19.17.209
172.19.17.170
172.19.16.1
100.105.0.1
router.asus.com
localhost
Filter Hosts