شروع به کار با دستور nmap :

nmap IP

در این حالت ۱۰۰۰ پرت مشهور tcp را بر روی آی پی مورد نظر بررسی کرده و سپس خروجی را به فرم زیر میدهد :

```
PORT    STATE  SERVICE
20/tcp closed ftp-data
21/tcp closed ftp
```

که در آن اسم پرت و حالت آنکه closed یا opened یا filtered باشد و همچنین اسم سرویس هم چاپ میکند .

برای اسکن کردن چندین آی پی از دستور زیر استفاده میکنیم :

nmap 192.168.10.1 192.168.10.100 192.168.10.101

برای اسکن کردن یک رنج آی پی از روش زیر استفاده میکنیم :

nmap 192.168.10.1-100

شما همچنین میتوانید یک سابنت را اسکن کنید :

nmap 192.168.10.1/24

میتوان از یک فایل که شامل آی پی های ما میباشد استفاده کرد (هر ای پی در یک خط) :

echo 192.168.10.1 > list.txt

سپس بعد از ساختن فایل دستور زیر را میزنیم :

nmap -iL list.txt

شما همچنین میتوانید به صورت تصادفی ای پی های مختلف را اسکن کنید :

nmap -iR 3

که عدد ۳ نشان میدهد ۳ ای پی تصادفی از داخل شبکه شما پیدا کرده و اسکن میکند.

همچنین شما میتوانید یک ای پی یا یک رنج یا یک فایل خاص شامل ای پی ها را از موارد مورد اسکن جدا کنید :

nmap 192.168.10.0/24 --exclude 192.168.10.100

nmap 192.168.10.0/24 --exclude 192.168.10.100-105

ابتدا فایل را میسازیم :

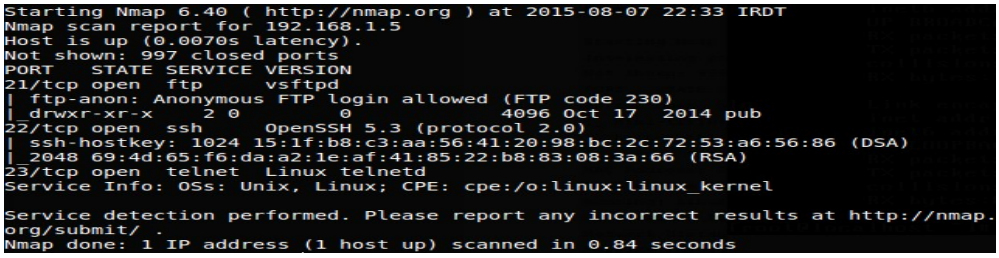
echo 192.168.10.1 > list.txt

سپس آن را از شیکه مورد جستجو جدا میکنیم :

nmap 192.168.10.0/24 --excludefile list.txt

شما همچنین میتوانید به صورت پرخاشگرانه اسکن کنید که تمام سرویس های مقصد را با جزییات قابل توجه ای نشان میدهد (سیستم عامل و دیگر مشخصات هم مشخص می‌شود) :

nmap -A 192.168.1.5



به طور پیشفرض دستور nmap با استفاده از پکت های icmp هاست های فعال را مشخص میکند و اقدام به اسکن انها میکند اما با توجه به اینکه اکثرا icmp روی سرور بسته است بهتر است از روش های دیگر استفاده کنیم :

Feature	Option
Don’t Ping	**-PN**
Perform a Ping Only Scan	**-sP**
TCP SYN Ping	**-PS**
TCP ACK Ping	**-PA**
UDP Ping	**-PU**
SCTP INIT Ping	**-PY**
ICMP Echo Ping	**-PE**
ICMP Timestamp Ping	**-PP**
ICMP Address Mask Ping	**-PM**
IP Protocol Ping	**-PO**
ARP Ping	**-PR**
Traceroute	**--traceroute**
Force Reverse DNS Resolution	**-R**
Disable Reverse DNS Resolution	**-n**
Alternative DNS Lookup	**--system-dns**
Manually Specify DNS Server(s)	**--dns-servers**
Create a Host List	**-sL**

حال کمی به تفسیر پروتکل TCP میپردازیم :

در این پروتکل مفهومی به نام 3ways handshake داریم که ابتدا برای برقراری ارتباط سیستم با سرور کلاینت Syn را ارسال میکند و سرور در جواب syn+ack را برمیگرداند و کلاینت جواب نهایی یعنی ack را میدهد .پس از این عملیات ارتباط برقرار میشود.

در این روش دستور nmap یه پکت syn برای سرور فرستاده و منتظر جواب سرور میشود . این روش زمانی استفاده میشود که پرتکل icmp در روی سرور بلاک شده است .همچنین پیشفرض روی پرت ۸۰ این ارتابط را برقرار کرده و میتوان ان را عوض کرد :

nmap -PS scanme.insecure.org

در روشی مشابه روش بالا ما پکت ای که سمت سرور میرود فلگ ack ان مشخص شده در صورتی که از قبل کانکشنی وجود نداشته پس کانکشنی که از سمت سرور میاد فلگ rst خورده است.مزیت این دو روش bypass کردن فایروال هاست :

nmap -PA 192.168.1.254

در روشی دیگر میتوان از پرتکل udp برای اسکن کردن استفاده کرد.البته در بسیاری از سرور ها این پرت ها بسته است و کارایی نداره اما از مزیت های ان میتوان به رد کردن راحت ترافیک روی فایروال های نام برد چرا که فایروال ها پکت های روی tcp را بررسی میکنند :

nmap -PU 192.168.1.254

پرتکلی دیگری که میتوان از ان استفاده کرد sctp است که ارتقاع یافته پرتکل های مشهوری مثل tcp , udp میباشد.برای اسکن کردن توسط این روش کامپیتور ابتدا فلگ init chunk میفرستد اگر پرت باز باشد مرحله دوم 4ways handsahke sctp رخ میدهد و سرور جواب init-ack را میفرستد و در این زمان کلاینت دستور abort را به نشانه پایان کانکشن میدهد.برای مدیریت این پروتکل نیاز به دسترسی رووت دارید :

nmap -PY 192.168.1.254

برای اسکن کردن توسط پروتکل icmp میتوان از روش echo ping استفاده کرد.به این منظور که ابتدا پکت echo request و جواب echo replay سرور را بررسی میکند.این روش در محیط های درون سازمانی بیشتر کارساز است :

nmap -PE 192.168.1.254

دو دستور زیر مانند دستور بالا عمل میکنند با این تفاوت که از روش های دیگر پرتکل icmp استفاده میکنند.این روش زمانی بکار می ایند که ادمین echo request را در شبکه بسته باشد :

nmap -PP 192.168.1.254

nmap -PM 192.168.1.254

همچنین میتوانیم با پرتکل های دیگر نیز اسکن را انجام دهیم :

اعداد پروتکل ها :

po1 – icmp

po2 – igmp

po3 – ip-in-ip

nmap -PO 10.10.1.48

میتوانیم از پرتکل لایه دو arp استفاده کنیم.این روشی سریع ای است که هاست های زنده را پیدا کنیم.البته این روش یک روش درون سازمانی است :

nmap -PR 192.168.1.254

همچنین میتوان با دستور traceroute عمل اسکن کردن را انجام دهیم اما trace دستور nmap برعکس حالت عادی ttl را بالا گزاشته و هی از ان کم میکند تا به صفر به رسد :

nmap --traceroute scanme.insecure.org

همچنین دستور nmap اجازه اسکن با استغاده از dns را نیز به ما میدهد که این عمل اطلاعاتی در اختیار ما میگزارد :

nmap -R 64.13.134.52

همچنین برای اینکه از dns استفاده نکند و سرعت عمل بیشتری داشته باشد به جای اپشن R- از اپشن n- استفاده کرد.

همچنین میتوانیم از dns مورد نظر خود استفاده کنیم :

nmap --dns-servers 208.67.222.222,208.67.220.220 scanme.insecure.org

همچنین میتوان اطلاعات هاست مورد نظر را بدون فرستادن پکتی از داخل dns ها جستجو کرد :

nmap -sL 10.10.1.1/24

روش های دیگری نیز nmap همراه دارد که باید با سطح دسترسی روت باشد .

Feature	Option
TCP SYN Scan	-sS
TCP Connect Scan	-sT
UDP Scan	-sU
TCP NULL Scan	-sN
TCP FIN Scan	-sF
Xmas Scan	-sX
TCP ACK Scan	-sA
Custom TCP Scan	--scanflags
IP Protocol Scan	-sO
Send Raw Ethernet Packets	--send-eth
Send IP Packets	--send-ip

همانند اپشن PS- اپشن sS- نیز از روش 3ways handshake برای برقراری ارتباط استفاده میکند.مزیت این روش بر روش قبلی اش این است که از برقراری یک ارتباط کامل جلو گیری میکند :

nmap -sS 10.10.1.48

هچنین برای کسانی که دسترسی روت ندارند میتوان یک اسکن مستفیم توسط دستور زیر داشته باشیم :

nmap -sT 10.10.1.1

برای دور زدن فایروال میتوان یه کانکشن tcp ایجاد کرد اما در هدر ان چیزی نگزاریم :

nmap -sN 10.10.1.48

همچنین میتوان در پکت tcp خود فلگ fin را فعال کرده.این چون نوعی ارتباط غیر منتظره است میتواند فایروال را دور بزند :

nmap -sF 10.10.1.48

در tcp زمانی که میخواهیم یه فایل حجیم را ارسال کنیم علاوه بر هدر tcp یک buffer به ان اضافه میشود اما زمانی که این بافر اضافه شد سرعت پردازش دیتا پایین میاید .برای همین فلگی به اسم psh وجود دارد که میگوید در لایه ۴ دریافت کننده نیاز به تحلیل برنامه نیست و سریعا ان را به لایه بالاتر خود انتفال داده .همچنین فلگ دیگری به نامه urg وجود دارد که به دریافت کننده میگوید به تعداد بیت هایی که از بیت اول این فلگ اشاره کرده باید الویت بندی شوند و حایز اهمیت هستند.

حال برای اسکن کردن nmap با تلفیق سه فلگ fin,urg,psh امکان اسکن را فراهم میکند :

nmap -sX 10.10.1.48

شما نیز میتوانید از تلفیقی از فلگ های tcp پکت مورد نظر خود را ارسال کنید.جدول فلگ های موجود و دستور به شرح زیر است :

Flag	Usage
SYN	Synchronize
ACK	Acknowledgment
PSH	Push
URG	Urgent
RST	Reset
FIN	Finished

nmap --scanflags SYNURG 10.10.1.127

میتوان با فلگ ack متوجه فیلتر بودن یا نبودن پرت ها شد به این معنی که زمانی که nmap فلگ ack را میفرستد انتظار فلگ rst را دارد اما اگر دریافت نکرد یعنی فایروال مانع این عمل شده است اما اگر rst دریافت کرد یعنی ان پرت فیلتر نیست :

nmap -sA 10.10.1.70

میتوان پروتکل های باز روی سیستم هدف را شناسایی کنیم.این کار باعث میشود بهترین روش اسکن خود را پیدا کنیم :

nmap -sO 10.10.1.41

میتوان با پکت های خام اترنت روی لایه دتیا لینک اسکن مورد نظر رو انجام داد :

nmap --send-eth 10.10.1.51

دستور nmap به طور پیشفرض ۱۰۰۰ پرت مشهور را بررسی میکند اما در برخی از سازمان ها این پرت را عوض میکنند برای همین نیاز به شناسایی ان دارید :

Feature	Option
Perform a Fast Scan	-F
Scan Specific Ports	-p [port]
Scan Ports by Name	-p [name]
Scan Ports by Protocol	-p U:[UDP ports],T:[TCP ports]
Scan All Ports	-p “*”
Scan Top Ports	--top-ports [number]
Perform a Sequential Port Scan	-r

برای اسکن ۱۰۰ پرت توسط دستور زیر عمل میکنیم :

nmap -F 10.10.1.44

همچنین میتوانید پرت های خود را مشخص کنید که میتواند پرت ها جدا گانه باشد یا یک رنج باشد و همچنین میتوان بجای استفاده از شماره پرت اسم ان را اسکن کند :

nmap -p 80 10.10.1.44

nmap -p 25,53,80-200 10.10.1.44

nmap -p smtp,http 10.10.1.44

همچنین میتوان روی پرتکل مشخص پرتی را مشخص کنیم و ان را اسکن کنیم :

nmap -sU -sT -p U:53,T:25 10.10.1.44

اگر نیاز به اسکن کل ۶۵۵۳۵ پرت باشد میتوان طبق زیر عمل کرد :

nmap -p "*" 10.10.1.41

میتوان برای nmap مشخص کرد که از چند پرت مشهور استفاده کند که پیشفرض ۱۰۰۰ است :

nmap --top-ports 500 10 10.10.1.41

با اپشن r- شمارش پرت ها را میتوان به صورت عددی از اول مشخص کرد.پیشفرض تصادفی انتخاب میکند :

nmap -r 10.10.1.48

با دستور nmap همچنین میتوانید سیستم عامل مقصد را نیز مشخص کنید .دستور با استفاده از TCP/IP fingerprinting حدس میزند سیستم عامل چیست.

Feature	Option
Operating System Detection	**-O**
Attempt to Guess an Unknown OS	**--osscan-guess**
Service Version Detection	**-sV**
Perform a RPC Scan	**--version-trace**
Troubleshooting Version Scans	**-sR**

برای پیدا کردن سیستم عامل میتوان به صورت زیر عمل کرد :

```
nmap -O 10.10.1.48
```

اما گاهی اوقات توانایی حدس زدن به دلیل باز یا بسته نبودن حتی یک پرت روی سرور مقصد نیست ولی میتوان دستور را با اپشنی اقدام به گمانه زنی در باره سیستم عامل بکنیم :

```
nmap -O --osscan-guess 10.10.1.11
```

میتوان نسخه سرویس هایی که روی مقصد نصب است را مشخص کرد :

```
nmap -sV 10.10.1.48
```

میتوان اطلاعات بیشتری از سیستم مقصد توسط دستور زیر به دست اورید :

```
nmap -sV --version-trace 10.10.1.48
```

همچنین میتوان از طریق پرتکل rpc که پرتکلی است که شما میتوانید از یک سرویس در کامپیوتر مقصد درخواست کنید :

```
nmap -sR 10.10.1.176
```

در دستور nmap قادر به این هستید مشخص کنید با چه سرعتی عمل اسکن کردن را انجام دهیم :

```
nmap -T4 10.10.1.1
```

به جای عدد ۴ میتوان هر یک از اعداد جدول زیر را قرار داد :

Template	Name	Notes
-T0	paranoid	Extremely slow
-T1	sneaky	Useful for avoiding intrusion detection systems
-T2	polite	Unlikely to interfere with the target system
-T3	normal	This is the default timing template
-T4	aggressive	Produces faster results on local networks
-T5	insane	Very fast and aggressive scan

که به ترتیت از صفر به پنج سریع تر میشود.

میتوان مشخص کرد که در لحظه دستور nmap حداقل چند پرت را اسکن میکند.به طور پیشفرض nmap با توجه به شرایط شبکه این عدد را انتخاب میکند :

nmap --min-parallelism 100 10.10.1.70

همچنین میتوان حداکثر ان را نیز مشخص کرد :

nmap --max-parallelism 1 10.10.1.70

در مثال بالا در لحظه فقط یک پرت بررسی میشود .

برای افزایش سرعت در اسکن میتوانید مشخص کنید که در یک رنج در هر لحظه به طور مساوی چند هاست را بررسی کند.همچنین میتوانید بیشینه و کمینه ان را نیز مشخص کنید.این کار باعث حجم ترافیک در زمان مشخص میشود و حساسیت حس گرد های امنیتی به این کمتر است :

nmap --min-hostgroup 30 10.10.1.0/24

nmap --max-hostgroup 10 10.10.1.0/24

میتوان زمان time out های پکت هایی را که فرستادیم تا پکت بعدی را مشخص کنیم. با افرایش rtt تعداد پکت هایی که دوباره فرستاده میشوند بخاطر time out را کاهش میدهد و با کاهش ان سرعت را افزایش میدهیم اما باید توجه داشت ممکن است نتایج دقیق نباشند :

nmap --initial-rtt-timeout 5000 scanme.insecure.org

میتوان بیشنه زمان صبر برای time out را مشخص کرد.دستور nmap به طور پیشفرض این عمل را به صورت دینامیک و با مقدار ۱۰ ثانیه

انجام میدهد اما میتوان این مقدار را برای افزایش سرعت در بررسی بلوک های بزرگ شبکه انجام داد :

```
nmap --max-rtt-timeout 400 scanme.insecure.org
```

زمانی که یک پرت اسکن ان با موفقیت انجام نمیشود ممکن است که فیلتر باشد یا پکت ما گم شده باشد.در این حال nmap سعی میکند دوباره این پکت هارا بفرستد.سود اینکار در دقت جواب ها است اما باعث افزایش زمان میشود.در بعضی از هاست های حساس باید مقدار ان را خود مشخص کنیم :

```
nmap --max-retries 1 scanme.insecure.org
```

اگر تارگت ما ارتباط ضعیفی با ان داریم و پکت ها به صورت نرمال در ان گم میشوند میتوان با تغییر مقدار ttl ان نتیجه بهتری بگیریم :

```
nmap --ttl 500 scanme.insecure.org
```

بعضی از هاست ها ارتباط ضعیفی با ان ها داریم یا توسط فایروال ها محافظت میشوند در این حال باید به دستور nmap یاد بدهیم که اگر پس از مدتی نتوانست اسکن کند ان هاست را رد کند :

```
nmap --host-timeout 1m 10.10.5.11
```

بعضی از هاست ها از سیستم هایی استفاده میکند که جلو اسکن مداوم انها را میگیرد یا فقط پکت های کمی میتوان به ان ارسال کرد یا از IDS (Intrusion Detection Systems) استفاده میکنند. در این حال باید فاصله زمانی بین هر اسکن را مشخص کنیم :

```
nmap --scan-delay 5s scanme.insecure.org
```

دستور nmap به طور دینامیک فاصله بین اسکن هارو تغییر میدهد اما میتوان میزان حداکثری ان را نیز تغییر داد :

```
nmap --max-scan-delay 300 scanme.insecure.org
```

میتوان مشخص کرد که در هر لحظه حداقل و حداکثر چند پکت را دستور nmap بفرستد .افزایش عدد حداقل باعث افزایش سرعت میشود :

nmap --min-rate 30 scanme.insecure.org

nmap --max-rate 30 scanme.insecure.org

بعضی از هاست ها به پکت هایی که حاوی فلگ rst میباشند حساس هستند شما با دستور زیر میتوانید از این محدودیت رها شوید البته ممکن است جواب ها دقیق نباشند :

nmap --defeat-rst-ratelimit scanme.insecure.org

فایروال ها ابزاری هستند که برای جلوگیری از دستور های مثل nmap به وجود امده اند که از به دست اوردن نقشه ای از شبکه شان جلوگیری کنند .

Feature	Option
Fragment Packets	-f
Specify a Specific MTU	--mtu
Use a Decoy	-D
Idle Zombie Scan	-sI
Manually Specify a Source Port	--source-port
Append Random Data	--data-length
Randomize Target Scan Order	--randomize-hosts
Spoof MAC Address	--spoof-mac
Send Bad Checksums	--badsum

میتوان با ارسال پکت های کوچک ۸ بایتی فایروال را دور زد :

nmap -f 10.10.1.48

همچنین میتوان حجم این پکت ها را خود مشخص کنیم (البته باید مضربی از ۸ باشد) :

nmap --mtu 16 10.10.1.48

دستور nmap این قابلیت رو به شما میدهد زمانی که میخواهید به یک هاست حمله کنید طوری به نظر برسد که از طرف چند ip به ان حمله شده است(پکت های جعلی میفرستد) در نیتجه سیتستم های دفاعی ان قادر به شناسایی شما نیستن :

nmap -D RND:10 10.10.1.48

در مثال بالا دستور nmap توسط ۱۰ ای پی رندم اسکن را انجام میدهد.

شما میتوانید یک سیستم دیگر را به عنوان اسکن کننده خود استفاده کنید که به این کار زامبی اتک گفته میشود . در حین انجتم این عمل باید سیستم زامبی idle باشد :

```
nmap -sI 10.10.1.41 10.10.1.252
```

اولین ای پی سیستم زامبی و دومین سیستم هدف است .

میتوانیم سورس پرت خود را برای تمامی اسکن ها عوض کنیم.مزیت این است که فایروال ها معمولا روی بعضی از سورس پرت های خاص حساس هستتد (مانند dhcp , ftp , ...) در نتیجه اسکن ما را متوقف نمیکنند :

```
nmap --source-port 53 scanme.insecure.org
```

دستور nmap میزان مشخصی دیتا در پکت های خود برای اسکن قرار میدهد این روش توسط بعضی از فایروال ها شناسایی شده و جلو ان گرفته میشود.برای دور زدن ان میتوان ان را متغیر فرستاد :

```
nmap --data-length 25 10.10.1.252
```

در مثال بالابه اخر هر بسته ۲۵ بایت اضافه میکند.

بعضی از سیستم های امنیتی در شبکه ها زمانی که شبکه به ترتیب خاص اسکن میشود به ان حساس شده و جلو ان را میگیرند.میتوان برای دستور nmap مشخص کرد که به صورت تصادفی ای پی هارو اسکن کند :

```
nmap --randomize-hosts 10.10.1.100-254
```

برای جلو گیری از شناسایی شدن دستور nmap میتواند مک ادرس های مختلفی تولید کند که به شکل کلی زیر است :

```
nmap --spoof-mac [vendor|MAC|0] [target]
```

مطابق جدول زیر مقادیر ان میتواند تغییر کند :

Argument	Function
0 (zero)	Generates a random MAC address
Specific MAC Address	Uses the specified MAC address
Vendor Name	Generates a MAC address from the specified vendor (such as Apple, Dell, 3Com, etc)

برای مثال :

nmap -sT -PN --spoof-mac 0 192.168.1.1

در tcp در انتهای پکت یک چک سام قرار میگیرد که پکت را تایید میکند و این چک سام توسط مقصد نیز بررسی میگردد. در سیستم هایی که درست پیکره بنده نشده اند میتوان پکت هایی با چک سام اشتباه فرستاد و این کار باعث دور زدن فایروال میشود :

nmap --badsum 10.10.1.41

دستور nmap به شما این امکان را میدهد که نتایج اسکن را در فایل ها به فرمت های دلخواه قرار بدهید و نتایج را مقایسه کنید :

Feature	Option
Save Output to a Text File	**-oN**
Save Output to a XML File	**-oX**
Grepable Output	**-oG**
Output All Supported File Types	**-oA**
Periodically Display Statistics	**--stats-every**
133t Output	**-oS**

میتوان خروجی را در یک فایل خالی ریخت :

nmap -oN scan.txt 10.10.1.1

میتوان به فرمت xml. فایل را تهیه کرد :

nmap -oX scan.xml 10.10.1.1

میتوان فایل را طوری تهیه کرد که دستور grep روی ان کارایی داشته باشد : (دستور grep یک رشته را از فایل بیرون میکشد)

```
nmap -oG scan.txt -F -O 10.10.1.1/24
```

میتوان نتایج را به سه روش بالا ذخیره نمود :

```
nmap -oA scans 10.10.1.1
```

همچنین میتوان تمام جزییات در حال اسکن کردن را حین اسکن دید :

```
nmap --stats-every 5s 10.10.1.41
```

یعنی هر ۵ ثانیه جزییات اسکن را نمایش میدهد.

برای شوخی وخنده میتوان نتایج را به صورت کمدی دید :

```
nmap -oS scan.txt 10.10.1.1
```

میتوان برای مقایسه فایل های اسکن شده از دستور ndiff استفاده کرد.در هرجا که تغییرات باشد دستور ان را نشان میدهد.اگر تغییرات از فایل اول باشد با – و اگر از فایل دوم باشد با + نمایش داده میشود :

```
ndiff scan1.xml scan2.xml
```

میتوان تفاوت هارو به صورت xml مود نمایش داد که برای نمایش توسط نرم افزار های نمایش xml مناسب است:

```
ndiff --xml scan1.xml scan2.xml
```

مشکلات همیشه بخشی از کامپیوتر هستند و دستور nmap نیز از ان مستثنی نیست .

برای دیدن تمام اتفاقات در حال اسکن میتوان به شکل زیر عمل کرد :

```
nmap -v scanme.insecure.org
```

اگر از vv- استفاده کنید اطلاعات بیشتری میگیرید.

همچنین میتوانید برای دیباگ کردن دستور خود یا دنبال مشکل گشتن از دستور زیر استفاده کنید (میتوانید سطح دیباگ را که از ۱-۹ است مشخص کنید) :

```
nmap -d9 scanme.insecure.org
```

میتوان در جواب اسکن دلیل ان را نیز ببینیم که این پرت چرا باز است یا بسته . اگر در دلیل syn-ack باشد معمولا پرت باز است اما اگر جواب هایی مثل conn-refused , reset باشد معمولا بسته هستند :

nmap --reason scanme.insecure.org

میتوان مشخص کرد که فقط پرت های باز را نمایش بده :

nmap --open scanme.insecure.org

یکی از ابزار های مفید برای عیب یابی ان است که رد پکت ها را در شبکه بررسی کنیم که توسط دستور زیر امکان پذیر است :

nmap --packet-trace 10.10.1.1

میتوان تنظیمات عمومی شبکه و همچنین رووت های سیستم لوکال خود را دید :

nmap –iflist

میتوان مشخص کرد که عمل اسکن را از کدام کارت شبکه انجام دهد :

nmap -e eth0 10.10.1.48

دستور nmap ابزار گرافیکی نیز دارد که برای نصب ان توسط دستور های زیر میتوان اقدام کرد :

debian/ubuntu : apt-get install zenmap

fedore/redhta/centOS : yum install zenmap

جدول تمامی دستوراتی که در بالا گفته شده است در زیر امده :

Basic Scanning Techniques	
Scan a Single Target	`nmap [target]`
Scan Multiple Targets	`nmap [target1, target2, etc]`
Scan a List of Targets	`nmap -iL [list.txt]`
Scan a Range of Hosts	`nmap [range of ip addresses]`
Scan an Entire Subnet	`nmap [ip address/cdir]`
Scan Random Hosts	`nmap -iR [number]`
Excluding Targets from a Scan	`nmap [targets] --exclude [targets]`
Excluding Targets Using a List	`nmap [targets] --excludefile [list.txt]`
Perform an Aggressive Scan	`nmap -A [target]`
Scan an IPv6 Target	`nmap -6 [target]`
Discovery Options	
Perform a Ping Only Scan	`nmap -sP [target]`
Don't Ping	`nmap -PN [target]`
TCP SYN Ping	`nmap -PS [target]`
TCP ACK Ping	`nmap -PA [target]`
UDP Ping	`nmap -PU [target]`
SCTP INIT Ping	`nmap -PY [target]`
ICMP Echo Ping	`nmap -PE [target]`
ICMP Timestamp Ping	`nmap -PP [target]`
ICMP Address Mask Ping	`nmap -PM [target]`
IP Protocol Ping	`nmap -PO [target]`
ARP Ping	`nmap -PR [target]`
Traceroute	`nmap --traceroute [target]`
Force Reverse DNS Resolution	`nmap -R [target]`
Disable Reverse DNS Resolution	`nmap -n [target]`
Alternative DNS Lookup	`nmap --system-dns [target]`
Manually Specify DNS Server(s)	`nmap --dns-servers [servers] [target]`
Create a Host List	`nmap -sL [targets]`
Advanced Scanning Functions	
TCP SYN Scan	`nmap -sS [target]`
TCP Connect Scan	`nmap -sT [target]`
UDP Scan	`nmap -sU [target]`
TCP NULL Scan	`nmap -sN [target]`
TCP FIN Scan	`nmap -sF [target]`
Xmas Scan	`nmap -sX [target]`
TCP ACK Scan	`nmap -sA [target]`
Custom TCP Scan	`nmap --scanflags [flags] [target]`
IP Protocol Scan	`nmap -sO [target]`
Send Raw Ethernet Packets	`nmap --send-eth [target]`
Send IP Packets	`nmap --send-ip [target]`

Port Scanning Options	
Perform a Fast Scan	`nmap -F [target]`
Scan Specific Ports	`nmap -p [port(s)] [target]`
Scan Ports by Name	`nmap -p [port name(s)] [target]`
Scan Ports by Protocol	`nmap -sU -sT -p U:[ports],T:[ports] [target]`
Scan All Ports	`nmap -p "*" [target]`
Scan Top Ports	`nmap --top-ports [number] [target]`
Perform a Sequential Port Scan	`nmap -r [target]`
Version Detection	
Operating System Detection	`nmap -O [target]`
Submit TCP/IP Fingerprints	`www.nmap.org/submit/`
Attempt to Guess an Unknown	`nmap -O --osscan-guess [target]`
Service Version Detection	`nmap -sV [target]`
Troubleshooting Version Scans	`nmap -sV --version-trace [target]`
Perform a RPC Scan	`nmap -sR [target]`
Timing Options	
Timing Templates	`nmap -T[0-5] [target]`
Set the Packet TTL	`nmap --ttl [time] [target]`
Minimum # of Parallel Operations	`nmap --min-parallelism [number] [target]`
Maximum # of Parallel Operations	`nmap --max-parallelism [number] [target]`
Minimum Host Group Size	`nmap --min-hostgroup [number] [targets]`
Maximum Host Group Size	`nmap --max-hostgroup [number] [targets]`
Maximum RTT Timeout	`nmap --initial-rtt-timeout [time] [target]`
Initial RTT Timeout	`nmap --max-rtt-timeout [TTL] [target]`
Maximum Retries	`nmap --max-retries [number] [target]`
Host Timeout	`nmap --host-timeout [time] [target]`
Minimum Scan Delay	`nmap --scan-delay [time] [target]`
Maximum Scan Delay	`nmap --max-scan-delay [time] [target]`
Minimum Packet Rate	`nmap --min-rate [number] [target]`
Maximum Packet Rate	`nmap --max-rate [number] [target]`
Defeat Reset Rate Limits	`nmap --defeat-rst-ratelimit [target]`
Firewall Evasion Techniques	
Fragment Packets	`nmap -f [target]`
Specify a Specific MTU	`nmap --mtu [MTU] [target]`
Use a Decoy	`nmap -D RND:[number] [target]`
Idle Zombie Scan	`nmap -sI [zombie] [target]`
Manually Specify a Source Port	`nmap --source-port [port] [target]`
Append Random Data	`nmap --data-length [size] [target]`
Randomize Target Scan Order	`nmap --randomize-hosts [target]`
Spoof MAC Address	`nmap --spoof-mac [MAC|0|vendor] [target]`
Send Bad Checksums	`nmap --badsum [target]`

Output Options	
Save Output to a Text File	`nmap -oN [scan.txt] [target]`
Save Output to a XML File	`nmap -oX [scan.xml] [target]`
Grepable Output	`nmap -oG [scan.txt] [targets]`
Output All Supported File Types	`nmap -oA [path/filename] [target]`
Periodically Display Statistics	`nmap --stats-every [time] [target]`
133t Output	`nmap -oS [scan.txt] [target]`
Troubleshooting and Debugging	
Getting Help	`nmap -h`
Display Nmap Version	`nmap -V`
Verbose Output	`nmap -v [target]`
Debugging	`nmap -d [target]`
Display Port State Reason	`nmap --reason [target]`
Only Display Open Ports	`nmap --open [target]`
Trace Packets	`nmap --packet-trace [target]`
Display Host Networking	`nmap --iflist`
Specify a Network Interface	`nmap -e [interface] [target]`
Nmap Scripting Engine	
Execute Individual Scripts	`nmap --script [script.nse] [target]`
Execute Multiple Scripts	`nmap --script [expression] [target]`
Script Categories	`all, auth, default, discovery, external, intrusive, malware, safe, vuln`
Execute Scripts by Category	`nmap --script [category] [target]`
Execute Multiple Script Categories	`nmap --script [category1,category2,etc]`
Troubleshoot Scripts	`nmap --script [script] --script-trace [target]`
Update the Script Database	`nmap --script-updatedb`
Ndiff	
Comparison Using Ndiff	`ndiff [scan1.xml] [scan2.xml]`
Ndiff Verbose Mode	`ndiff -v [scan1.xml] [scan2.xml]`
XML Output Mode	`ndiff --xml [scan1.xml] [scan2.xml]`

همچنین مجموعه ای از پرت های مهم ای که موجود است در جدول صفحه بعد امده است :

Port	Type	Usage
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP|UDP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
42	TCP|UDP	Windows Internet Name Service (WINS)
53	TCP|UDP	Domain Name System (DNS)
67	UDP	DHCP Server
68	UDP	DHCP Client
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP|UDP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol 3 (POP3)
119	TCP	Network News Transfer Protocol (NNTP)
123	UDP	Network Time Protocol (NTP)
135	TCP|UDP	Microsoft RPC
137	TCP|UDP	NetBIOS Name Service
138	TCP|UDP	NetBIOS Datagram Service
139	TCP|UDP	NetBIOS Session Service
143	TCP|UDP	Internet Message Access Protocol (IMAP)
161	TCP|UDP	Simple Network Management Protocol (SNMP)
162	TCP|UDP	Simple Network Management Protocol (SNMP) Trap
389	TCP|UDP	Lightweight Directory Access Protocol (LDAP)
443	TCP|UDP	Hypertext Transfer Protocol over TLS/SSL (HTTPS)
445	TCP	Server Message Block (SMB)
636	TCP|UDP	Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
873	TCP	Remote File Synchronization Protocol (rsync)
993	TCP	Internet Message Access Protocol over SSL (IMAPS)
995	TCP	Post Office Protocol 3 over TLS/SSL (POP3S)
1433	TCP	Microsoft SQL Server Database
3306	TCP	MySQL Database
3389	TCP	Microsoft Terminal Server/Remote Desktop Protocol (RDP)
5800	TCP	Virtual Network Computing (VNC) web interface
5900	TCP	Virtual Network Computing (VNC) remote desktop

منابع :

Nmap Cookbook The Fat-free Guide to Network Scanning

nmap.org

wikipedia.com

ترجمه و تهیه توسط :

علی قاسم پور

www.j-22.ir