«هُوَ المَحبوب»

معرفی تکنیک ها و ابزارهای پویش پورت

Introduction To Port Scanning Tools and Techniques

گردآورنده: نیما بازگیر
nmbazgir@gmail.com

فهرست مطالب

مقدمه

تست نفوذپذیری در شبکه ها شامل چندمرحله (گام) می باشد که اولین گام شناسایی مقدماتی هدف بوده و گام دوم پویش و جستجو در شبکه بدنبال رخنه نفوذ (Scanning) یا همان مطلب مورد نظر ما می باشد.

بعد از اینکه نفوذگر ماشینهای فعال شبکه شما و همچنین توپولوژی تقریبی آن را شناسایی کرد، میخواهد بداند هرماشین چه وظیفه ای برعهده دارد و چه خدماتی ارائه می دهد و همچنین هرکدام از سرویسها به چه نحو در اختیار کاربران قرار میگیرند.

یکی از مهمترین قسمتهای گام دوم پویش پورتهای باز روی ماشینهای شبکه می باشد که نفوذگر با استفاده از ابزارهایی که به نام پویشگر پورت (Port Scanner) مشهورند انجام می دهد.

از آنجا که سرویس دهنده های مشهور و استاندارد جهانی دارای پورتهای مشخص و معینی هستند نفوذگر با استفاده از پویش پورت به این موضوع پی خواهد برد که کدام سرویس دهنده بر روی ماشین های شبکه فعال هستند.

نکته: فهرست سرویس دهنده های استاندارد و شماره پورتهای آنها توسط IETF در RFC1700 مشخص شده اند.

از آنجا که منبعی بصورت اختصاصی و با جزئیات نسبتا کامل به این مطالب نپرداخته است در این مقاله سعی شده که به تشریح تکنیکهای رایج پویش پورت ها پرداخته شود بصورتی که یک منبع کلی برای این مطلب در دسترس علاقمندان قرار گیرد و از آنجا که این مطالب بصورت عملی در آزمایشگاه شخصی بصورت تک تک توسط اینجانب آزمایش شده اند خواننده می تواند از آن بعنوان یک منبع کاربردی استفاده کند.

همچنین برای صریح بودن مطالب از دیاگرام های خاص ساده ای استفاده شده که خواننده را در فهم موضوع و اینکه در فرآیند پویش چه اتفاقاتی رخ خواهد داد، کمک کند. از آنجا که این اوراق بصورت کاملا کاربردی و تخصصی به این مطلب می پردازد از دو ابزار بسیار قدرتمند و رایگان پویش پورت با نام های Nmap و Hping3 برای ارائه مثالهای کاربردی استفاده نموده ام، قابل ذکر است که هردو نرم افزار در توزیع های متنوع امنیتی زنده لینوکس مانند Backtrack ، Auditor و... قابل دسترس می باشند و توصیه میکنم برای سهولت از این ابزارها استفاده نمایید، البته در صورت نیاز می توانید ابزارهای ذکر شده را از آدرسهای وب زیر دانلود نمائید:

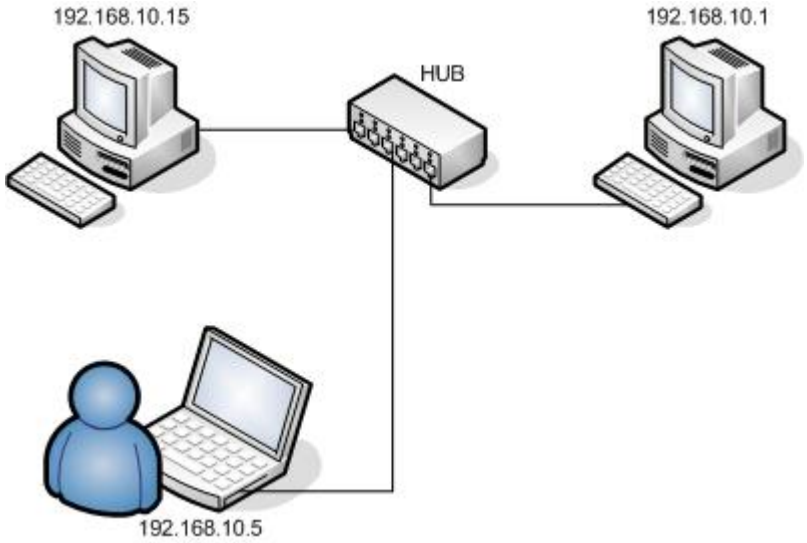
```
http://www.insecure.org/nmap
http://hping.org
```

فرض براین است که خواننده مقاله اطلاعات پایه ای از بسته TCP/IP را دارا می باشد و نیازی به یادآوری (درمورد اینکه TCP/IP چیست، آدرسهای IP چه هستند و چگونه از آنها استفاده می شود، پورت چیست، و پرچم های متفاوت TCP چه نام دارند و شرح حالشان چیست) نخواهد داشت.

تذکر 1 : تمام مطالب این مقاله جنبه آموزشی داشته و عواقب استفاده نادرست از آنها بعهده شخص استفاده کننده خواهد بود و نویسنده هیچ مسئولیتی را برعهده نخواهد داشت.

تذکر 2 : به خواننده مقاله توصیه می شود که درصورت علاقه به موضوع، مثالها را از طریق یک آزمایشگاه شبکه با چند کامپیوتر خصوصی آزمایش کند، و از استفاده آنها برروی ماشینهای حقیقی در شبکه های عمومی و غیرعمومی جدا خودداری کند.

دیاگرام شبکه ای که این آزمایشات روی آن انجام شده بصورت زیر می باشد:
(البته با استفاده از دو کامپیوتر نیز میتوانید انجام دهید)



ماشین با آدرس 192.168.10.5 بعنوان ماشین مبدا بوده و دو ماشین دیگر بعنوان ماشین های مقصد استفاده شده اند، البته قابل ذکر است که علاقمندان به علوم نفوذگری براحتی میتوانند اکثر آزمایشات خود را با همین امکانات ساده پیاده سازی کنند.

1.0- انواع پویش پورت

1.1- روش TCP Connect()

این نوع از پویش از تابع Connect() استفاده می کند تا بدین وسیله به سیستم عامل اجازه برقرای یک اتصال TCP را بدهد، که این روش معمولا کندتر از پویشهایی هستند که از بسته های raw استفاده می کنند، دلیل کند بودن این نوع از پویش این است که از روش دست تکانی 3طرفه کامل استفاده می کند و با استفاده از این روش پورتهای باز را پیدا می کند.

این بدان معنی است که زمان بیشتر و بسته های بیشتری نسبت به روشی به نام SYN استفاده می شود تا اینکه بفهمیم کدام پورت روی ماشین مقصد باز است.

نکته مهمی که باید بخاطر داشته باشید این است که استفاده از این روش باعث می شود آدرس IP شما بر روی ماشین مقصد ذخیره (Log) شود.

برای انجام این پویش با استفاده از پویشگر Nmap بصورت زیر عمل خواهیم کرد.

```
# nmap -sT 192.168.10.1
Starting Nmap 4.21ALPHA2 ( http://insecure.org )at 2007-03-07 08:49 CST
Interesting ports on 192.168.10.1 (192.168.10.1):
Not shown: 1702 closed ports
PORT STATE SERVICE
80/tcp open http
5190/tcp open aol
Nmap finished: 1 IP address (1 host up) scanned in 1.459 seconds
```

همانطور که در نتیجه پویش سیستمی با آدرس 192.168.10.1 می بینید، دو پورت 80 و 5190 که مربوط به سرویسهای http و aol هستند، باز می باشند. سوئیچ sT– تعیین کننده این است که نوع پویش بصورت TCP Connect() است.

1.2- روش TCP SYN

این نوع پویش بسته های raw SYN را به سیستم مقصد ارسال کرده و منتظر پاسخ می ماند. یک پورت باز با یک بسته SYN/ACK پاسخ خواهد داد، پورت بسته با یک بسته RST پاسخ خواهد داد.
اگر پاسخی برگشت داده نشد، به احتمال زیاد پورت فیلتر شده است. (که در این صورت به این مطلب پی خواهیم برد که در میانه مسیر یک firewall قرار دارد.)

```
Open:
192.168.10.5 -> 192.168.10.1 SYN
192.168.10.5 <- 192.168.10.1 SYN/ACK

Closed:
192.168.10.5 -> 192.168.10.1 SYN
192.168.10.5 <- 192.168.10.1 RST/ACK

Filtered:
192.168.10.5 -> 192.168.10.1 SYN
        <no response>
```

برای انجام این نوع از پویش با استفاده از نرم افزارهای Nmap و Hping3 به صورت زیر عمل می کنیم.

```
# nmap -sS 192.168.10.1
Starting Nmap 4.21ALPHA2 ( http://insecure.org )at 2007-03-07 08:50 CST
Interesting ports on 192.168.10.1 (192.168.10.1):
Not shown: 1702 closed ports
PORT STATE SERVICE
80/tcp open http
5190/tcp open aol
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)
Nmap finished: 1 IP address (1 host up) scanned in 1.616 seconds
```

در دستور بالا سوئیچ sS– نشاندهنده پویش به روش TCP SYN می باشد.

```
# hping3 -c 1 --syn -p 80 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): S set, 40 headers + 0 data
bytes
len=46 ip=192.168.10.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=5840
rtt=1.8 ms
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.7/1.7/1.7 ms
```

```
# hping3 -c 1 --syn -p 81 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): S set, 40 headers + 0 data
bytes
len=46 ip=192.168.10.1 ttl=64 DF id=0 sport=81 flags=RA seq=0 win=0
rtt=1.8 ms
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.7/1.7/1.7 ms
```

در دو دستور مثال بالا که با استفاده از Hping3 آورده شده است، سوئیچ c– تعداد بسته هایی که باید ارسال شود را به نرم افزار می فهماند و عدد بعد از آن یعنی 1 تعداد را مشخص میکند. سوئیچ syn– نشاندهنده نوع اسکن به روش TCP SYN می باشد، سوئیچ p– و عدد بعد از آن تعیین می کند کدام پورت مورد پویش قرار بگیرد که در دو مثال پورت های 80 و 81 مشخص شده اند و در نهایت IP نشاندهنده آدرس ماشین مقصد می باشد که باید مورد پویش قرار بگیرد.

1.3- روش TCP FIN

این روش پویش می تواند به ما نشان دهد که کدام پورت بسته است، ولی نمی تواند تفاوتی بین پورت باز و فیلتر شده قائل شود زیرا هیچ پاسخی برای ارزیابی و تمایز بین این دو دریافت نخواهد کرد.
ایده اصلی این روش پویش بدین صورت است که یک بسته FIN ارسال می کند، اگر یک بسته RST دریافت شد می فهمیم که پورت بسته است. و اگر پورت بسته نبود (باز یا فیلتر شده بود) ماشین مقصد نباید هیچ بسته ای بعنوان پاسخ ارسال کند.
این روش پویش موجب گمراهی برخی از firewallها می شود. باید توجه داشت که یک مشکل هم وجود دارد و این است که بعضی سیستم ها برای ارتباطات خود از RFC پیروی نمی کند و بسته RST را درصورتی ارسال خواهند کرد که پورت باز باشد، و اگر در این میان Firewall وجود داشته باشد از این طریق نمی توان به نتیجه پویش بر اساس فیلتر بودن یا نبودن پورت مورد نظر اعتماد کرد.

```
Open or filtered:
192.168.10.5 -> 192.168.10.1 FIN
       <no response>

Closed:
192.168.10.5 -> 192.168.10.1 FIN
192.168.10.5 <- 192.168.10.1 RST/ACK
```

پیاده سازی پویش با استفاده از دو نرم افزار Nmap و Hping3 در زیر آمده است:

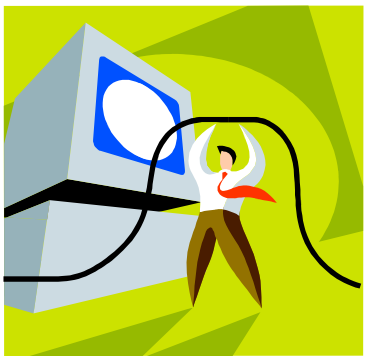
```
# nmap -sF 192.168.10.1
Starting Nmap 4.21ALPHA2 (http://insecure.org) at 2007-03-07 08:51 CST
Interesting ports on 192.168.10.1 (192.168.10.1):
Not shown: 1702 closed ports
PORT STATE SERVICE
80/tcp open|filtered http
5190/tcp open|filtered aol
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)
Nmap finished: 1 IP address (1 host up) scanned in 2.812 seconds
```

همانطور که در مثال واضح است سوئیچ sF– این نوع از پویش را تعیین می کند.

```
# hping3 -c 1 --fin -p 80 192.168.10.1
HPING 192.168.10.1(eth0 192.168.10.1): F set, 40 headers + 0 data bytes
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

# hping3 -c 1 --fin -p 81 192.168.10.1
HPING 192.168.10.1(eth0 192.168.10.1): F set, 40 headers + 0 data bytes
len=46 ip=192.168.10.1 ttl=64 DF id=0 sport=81 flags=RA seq=0 win=0
rtt=1.6 ms
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.6/1.6/1.6 ms
```

در دو دستور بالا از سوئیچ fin– برای تعیین نوع پویش برای پورت های 80 و 81 استفاده شده است. همانطور که در نتیجه می بینید پورت 80 باز یا فیلتر بوده که پاسخی داده نشده، ولی برای پورت 81 در نتیجه حاصل از پویش (خروجی برنامه) می بینید که پرچم RST/ACK فعال شده و بدین معناست که بسته مربوطه برگشت داده شده و همانطور که در توضیحات و دیاگرام آورده شده این نتیجه برای پورت های بسته خواهد بود.



1.4- روش TCP XMAS

این روش همانند روش FIN می باشد، با این تفاوت که بجای یک بسته FIN بصورت منفرد از یک بسته با فلگ های FIN ، URG و PSH استفاده می کند.

نتایج دقیقا بصوت روش FIN تحلیل شده و حالت پورت ها به همان صورت تعیین می شود.

```
Open or filtered:
192.168.10.5 -> 192.168.10.1 FIN/URG/PSH
      <no response>

Closed:
192.168.10.5 -> 192.168.10.1 FIN/URG/PSH
192.168.10.5 <- 192.168.10.1 RST/ACK
```

همانطور که در دیاگرام بالا می بینید، بسته ای که در پاسخ از پورت بسته برگشت داده میشود RST/ACK خواهد بود.

پیاده سازی توسط Nmap و Hping3 به صورت زیر خواهد بود:

```
# nmap -sX 192.168.10.1
Starting Nmap 4.21ALPHA2 (http://insecure.org) at 2007-03-07 08:54 CST
Interesting ports on 192.168.10.1 (192.168.10.1):
Not shown: 1702 closed ports
PORT STATE SERVICE
80/tcp open|filtered http
5190/tcp open|filtered aol
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)
Nmap finished: 1 IP address (1 host up) scanned in 2.491 seconds
```

واضح است که از سوئیچ sX– برای تعیین این نوع پویش استفاده شده است، اما با اندکی دقت متوجه خواهیم شد که Nmap در نتیجه پویش این روش و روش قبلی پورت ها را بصورت open|filtered نشان داده است که خود بیانگر این موضوع است که در دو روش ذکر شده مشخص نیست که پورت درحالت باز باشد یا فیلتر شده...

```
# hping3 -c 1 --fin --push --urg -p 80 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): FPU set, 40 headers + 0 data
bytes
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

```
# hping3 -c 1 --fin --push --urg -p 81 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): FPU set, 40 headers + 0 data
bytes
len=46 ip=192.168.10.1 ttl=64 DF id=0 sport=81 flags=RA seq=0 win=0
rtt=2.2 ms
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.7/1.7/1.7 ms
```

واضح است که سوئیچ های fin-- و push-- و urg-- برای تنظیمات فلگ ها برای پویش به روش xmas استفاده شده اند.

در نتیجه خروجی برای پورت 80 بسته ای بعنوان پاسخ برگشت داده نشده (100% packet loss) و برای پورت 81 یک بسته دریافت شده که پرچم RST/ACK بسته نشانده شده است که می فهمیم پورت 80 باز و 81 بسته است.

1.5- روش TCP NULL

این روش نیز همانند FIN و XMAS عمل می کند با این تفاوت که هیچ کدام از پرچم های بسته ارسالی نشانده نمی شوند (برابر با رقم یک منطقی قرار نمیدهد). در واقع یک بسته Null به ماشین مقصد ارسال می کند.

```
Open or filtered:
192.168.10.5 -> 192.168.10.1 (NONE)
      <no response>

Closed:
192.168.10.5 -> 192.168.10.1 (NONE)
192.168.10.5 <- 192.168.10.1 RST/ACK
```

پیاده سازی روش ذکر شده با استفاده از Nmap و Hping3 بصورت زیر خواهد بود:

```
# nmap -sN 192.168.10.1
Starting Nmap 4.21ALPHA2 (http://insecure.org) at 2007-03-07 08:57 CST
Interesting ports on 192.168.10.1 (192.168.10.1):
Not shown: 1702 closed ports
PORT STATE SERVICE
80/tcp open|filtered http
5190/tcp open|filtered aol
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)
Nmap finished: 1 IP address (1 host up) scanned in 2.673 seconds
```

سوئیچ sN– نشان دهنده پویش مورد نظر می باشد.

همانطور که در خروجی برنامه می بینید دو پورت 80 و 5190 پاسخ نداده که Nmap هر دو را بعنوان open|filtered درنظر گرفته است.

```
# hping3 -c 1 -p 80 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): NO FLAGS are set, 40 headers +
0 data bytes
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

# hping3 -c 1 -p 81 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): NO FLAGS are set, 40 headers +
0 data bytes
len=40 ip=192.168.10.1 ttl=64 DF id=0 sport=80 flags=RA seq=0 win=0
rtt=0.1 ms
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.1 ms
```

در دو دستوری که استفاده شده برای تک بسته ای که توسط hping3 به ماشین مقصد ارسال شده هیچ کدام از پرچم ها نشانده نشده، یعنی از سوئیچ هایی که پرچم ها را نشاندهی می کند استفاده نشده است، و این بخودی خود باعث میشود که یه بسته NULL به سمت ماشین مقصد ارسال شود.
اگه نتیجه این روش پویش را با دو روش قبلی مقایسه کنید می بینید که نتایج یکسان بوده ولی پرچم های نشانده شده متفاوت می باشند.

1.6- روش TCP Window

این روش همانند پویش TCP ACK می باشد (درصورت نیاز به قسمت 2.1 مراجعه شود)، با این تفاوت که سعی می کند فرقی بین پورت های باز و بسته قائل شود، که این عمل را با امتحان کردن فیلد Window مربوط به هدر TCP از بسته RST دریافت شده، انجام می دهد.
برخی سیستم ها با مقدار بیشتر از صفر برای پورت های باز و مقدار صفر را در این فیلد برای پورت های بسته استفاده می کنند، و سیستم های معدودی هم دقیقا معکوس مطلب گفته شده عمل می کنند.
پس اگر شما اسکن به این روش را به اتمام رساندید و تعداد زیادی پورت باز پیدا کردید و فقط تعداد کمی پورت بسته وجود داشت، دقیقا با مشکل ذکر شده مواجه شده اید، پس نتیجه را باید معکوس در نظر بگیرید، بدین صورت که تعداد زیادی پورت بسته (که بصورت باز نتیجه داده اند) و تعدادی اندک پورت باز (که بصورت پورت بسته نتیجه داده اند) وجود خواهد داشت.

البته بعضی از سیستم ها هیچ عمل خاصی روی نتیجه انجام نخواهند داد (مانند همین سیستمی که در اینجا اسکن کرده ام)، پس به وضوح می توان نتیجه گرفت که همیشه نمی توان به نتیجه این روش از پویش اعتماد کرد.

```
Open:
192.168.10.5 -> 192.168.10.1 ACK
192.168.10.5 <- 192.168.10.1 RST [Window size > 0]

Closed:
192.168.10.5 -> 192.168.10.1 ACK
192.168.10.5 <- 192.168.10.1 RST [Window size == 0]

Filtered:
192.168.10.5 -> 192.168.10.1 ACK
       <no response>
```

پیاده سازی این نوع از پویش با استفاده از Nmap و Hping3 بصورت زیر خواهند بود.

```
# nmap -sW 192.168.10.1
Starting Nmap 4.21ALPHA2 (http://insecure.org) at 2007-03-07 11:02 CST
All 1704 scanned ports on 192.168.10.1 (192.168.10.1) are closed
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)
Nmap finished: 1 IP address (1 host up) scanned in 1.500 seconds
```

در مثال بالا از سوئیچ sW– برای این منظور استفاده شده است.

```
# hping3 -c 1 --ack -p 80 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): A set, 40 headers + 0 data
bytes
len=46 ip=192.168.10.1 ttl=64 DF id=0 sport=80 flags=R seq=0 win=0
rtt=1.7 ms
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 5.2/5.2/5.2 ms
```

همانطور که ملاحظه می کنید نتایج متفاوت و غیر قابل اعتماد می باشند.

1.7- پویش UDP

اگرچه TCP پروتکلی بشد رایج و فراگیر می باشد، ولی UDP نیز دارای استفاده های خاص خود در شبکه ها می باشد. سرویس هایی نظیر DNS و DHCP از UDP استفاده می کنند.

ایده ای که برای پویش UDP وجود دارد، اینست که ماشین مبدا یک بسته UDP به ماشین مقصد ارسال کرده و منتظر پاسخ می ماند. اگر با ICMP Port Unreachable مواجه شدیم، نتیجه خواهید گرفت که پورت مورد نظر بسته می باشد.

در صورتی که با اشکال دیگری از پیامهای UDP Unreachable مواجه شدیم ممکن است پورت مورد نظر فیلتر شده باشد.

ولی اگر یک پاسخ UDP از سوی ماشین مقصد برگشت داده شد، پورت مورد نظر باز است، و همچنین اگر پاسخی نیز ارسال نشد پورت مورد نظر یا باز و یا فیلتر خواهد بود.

```
Open:
192.168.10.5 -> 192.168.10.1 [UDP]
192.168.10.5 <- 192.168.10.1 [UDP]


Open or filtered:
192.168.10.5 -> 192.168.10.1 [UDP]
      <no response>


Closed:
192.168.10.5 -> 192.168.10.1 [UDP]
192.168.10.5 <- 192.168.10.1 [ICMP Port Unreachable]


Filtered:
192.168.10.5 -> 192.168.10.1 [UDP]
192.168.10.5 <- 192.168.10.1 [Misc. ICMP Unreachable]
```

پیاده سازی پویش UDP با استفاده از دو نرم افزار Nmap و Hping3 بصورت زیر می باشد.

```
# nmap -sU 192.168.10.1
Starting Nmap 4.21ALPHA2 (http://insecure.org) at 2007-03-07 09:18 CST
Interesting ports on 192.168.10.1 (192.168.10.1):
Not shown: 1485 closed ports
PORT STATE SERVICE
53/udp open|filtered domain
67/udp open|filtered dhcps
2049/udp open|filtered nfs
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)
Nmap finished: 1 IP address (1 host up) scanned in 1489.293 seconds
```

همانطور که ملاحظه می کنید برای این نوع از پویش از سوئیچ sU– استفاده شده است. و نتیجه خروجی حاکی از آن است که پورت های 53 و 67 و 2049 به احتمال زیاد باز یا فیلتر شده می باشند.

```
# hping3 -c 1 --udp -p 53 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): udp mode set, 28 headers + 0
data bytes
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms


# hping3 -c 1 --udp -p 54 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): udp mode set, 28 headers + 0
data bytes
ICMP Port Unreachable from ip=192.168.10.1 name=192.168.10.1
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

برای این نوع پویش در نرم افزار Hping3 از سوئیچ udp– استفاده می شود، همانطور که در نتایج می بینید از پورت 53 پاسخی داده نشده و حاکی از آن است که این پورت باز یا فیلتر شده می باشد، ولی از آنجا که برای پورت 54 پاسخ ICMP Port Unreachable دریافت شده است، این نتیجه گرفته می شود که پورت مورد نظر بسته می باشد.

2.0- روشهای دیگر پویش پورت

در این قسمت به روشهایی از پویش پورت می پردازیم که هدف از استفاده آنها معلوم شدن باز یا بسته بودن پورت مورد نظر نمی باشد، بلکه برای مقاصدی خاص می باشند که در ادامه با آنها آشنا می شویم، این روشها مشابه بقیه بوده و هنوز هم بسیار سودمند هستند.

2.1- روش TCP ACK

هنگامی که عمل پویش را در یک شبکه انجام می دهیم وجود فایروالها موجب دریافت نتیجه های ناصحیح و نامعتبر خواهد شد.

بعنوان مثال اگر از روش پویش SYN روی یک هاست که فایروال شده باشد استفاده کنیم، محتملا بسته SYN/ACK یا RST دریافت نخواهیم کرد، از اینرو نخواهیم فهمید که پورت در چه حالتی می باشد و یا چه اتفاقی افتاده است!

در اینجاست که پویش به روش ACK سودمند واقع خواهد شد، این روش به ما نشان نخواهد داد که فلان پورت باز یا بسته خواهد بود، بلکه با استفاده از این روش خواهیم فهمید که اصلا فایروالی درکار خواهد بود؟ یا خیر؟ که درصورت وجود نداشتن فایروال علت پاسخ ندادن پورت اسکن شده "رد دریافت بسته های SYN" خواهد بود.

و اگر فایروال درکار نبود و فقط یک فیلترینگ بسته های SYN درکار بود، به احتمال زیاد یک بسته ACK مفید واقع شود و دور نخواهد افتاد، زیرا ماشین مقصد اینطور درنظر میگیرد که یک پاسخ برای درخواستی که قبلا داده (که اصلا چنین چیزی وجود نداشته) درحال دریافت می باشد و آن را دور نمی اندازد.

ولی اگر یک پورت (باز یا بسته) یک بسته ACK غیر منتظره دریافت کند، در پاسخ برای ماشین ارسال کننده ACK یک بسته RST ارسال خواهد کرد.

بنابراین اگر از ماشین مقصد یک بسته RST دریافت شد، بدین معنا خواهد بود که فایروالی درکار نیست، اگر پاسخی دریافت نشد، یا ICMP Unreachable دریافت شد، به احتمال زیاد پورت مورد نظر توسط فایروال فیلتر شده خواهد بود.

```
Unfiltered (got through firewall):
192.168.10.5 -> 192.168.10.1 ACK
192.168.10.5 <- 192.168.10.1 RST

Filtered:
192.168.10.5 -> 192.168.10.1 ACK
192.168.10.5 <- 192.168.10.1 [Misc. ICMP Unreachable]
            OR
        <no response>
```

برای پیاده سازی این نوع پویش به روشهای زیر عمل می کنیم.

```
# nmap -sA 192.168.10.1
Starting Nmap 4.21ALPHA2 (http://insecure.org ) at 2007-03-07 09:03 CST
All 1704 scanned ports on 192.168.10.1 (192.168.10.1) are UNfiltered
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)
Nmap finished: 1 IP address (1 host up) scanned in 2.468 seconds


# hping3 -c 1 --ack -p 80 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): A set, 40 headers + 0 data
bytes
```

```
len=46 ip=192.168.10.1 ttl=64 DF id=0 sport=80 flags=R seq=0 win=0
rtt=1.7 ms
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 5.2/5.2/5.2 ms
```

سوئیچ های مورد استفاده در نرم افزارهای مورد نظر sA– و ack– می باشند.

2.2- پویش پروتکل IP

یکی از محبوبترین و یک روش بسیار عالی برای پویش می باشد و بجای جستجو برای پورت های باز به جستجو برای پشتیبانی از پروتکل IP می پردازد. که در نوع خود ایده جالبی است، این روش بسیار شبیه به پویش UDP می باشد، با این تفاوت که یک سری از بسته ها با مقادیر مختلف در فیلد Protocol از سرآیند بسته ارسال کرده و بجای اینکه منتظر پاسخ هایی از نوع ICMP Port Unreachable باشد، منتظر پاسخ های ICMP Protocol Unreachable می ماند تا بعنوان نتیجه بگوید بسته است (از پروتکل مورد نظر پشتیبانی نمیشود)، اگر پاسخی در پروتکل مشابه ارسال شده دریافت شود نتیجه خواهیم گرفت باز می باشد (پشتیبانی می شود)، ولی اگر پاسخ های متفاوتی از نوع ICMP Unreachable دریافت شد، به احتمال زیاد فیلتر شده است.

اما یک رفتار تحلیل نشده دیگر باقی می ماند، و این است که، اگر پاسخی برگشت داده نشد یکی از دو حالت باز و یا فیلتر شده توسط فایروال خواهد بود، که در این روش از پویش فقط برای این نتیجه پاسخی ارسال نخواهد شد.

از آنجا که پروتکل های مختلف دارای پورت های شناخته شده خاص خودشان می باشند براحتی می توان به باز یا بسته بودن پورت ها از این طریق پی برد.

```
Supported:
192.168.10.5 -> 192.168.10.1 [Some IP protocol]
192.168.10.5 <- 192.168.10.1 [Same IP protocol]

Supported or filtered:
192.168.10.5 -> 192.168.10.1 [Some IP protocol]
192.168.10.5 <- 192.168.10.1 [Misc. ICMP Unreachable]
              OR
        <no response>

Unsupported:
192.168.10.5 -> 192.168.10.1 [Some IP protocol]
192.168.10.5 <- 192.168.10.1 [ICMP Protocol Unreachable]
```

برای این روش پویش بصورت زیر عمل می کنیم:

```
# nmap -sO 192.168.10.1
Starting Nmap 4.21ALPHA2 ( http://insecure.org ) at 2007-03-07 09:03
CST
Interesting protocols on 192.168.10.1 (192.168.10.1):
Not shown: 252 open|filtered protocols
PROTOCOL STATE SERVICE
1 open icmp
2 closed igmp
6 open tcp
17 open udp
MAC Address: 00:0C:E5:4F:0F:AF (Motorola BCS)
Nmap finished: 1 IP address (1 host up) scanned in 5.781 seconds



# hping3 -c 1 --rawip --ipproto 0 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): raw IP mode set, 20 headers + 0
data bytes
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms



# hping3 -c 1 --icmp 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): icmp mode set, 28 headers + 0
data bytes
len=46 ip=192.168.10.1 ttl=64 id=40509 icmp_seq=0 rtt=1.6 ms
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 18.6/18.6/18.6 ms



# hping3 -c 1 --rawip --ipproto 2 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): raw IP mode set, 20 headers + 0
data bytes
ICMP Protocol Unreachable from ip=192.168.10.1 name=192.168.10.1
--- 192.168.10.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

3.0- ابزارهای متداول دیگر

در قسمتهای اول و دوم این مقاله به روشهای اصلی و نکات بسیار مهم در پویش پورت ها با ارائه مثالهایی با استفاده از دو ابزار Nmap و Hping3 پرداختیم. دلیل استفاده از این دو ابزار این بود که اولا

ابزارهای شناخته شده و معروفی برای این منظور هستند، دوما رایگان بوده و براحتی برای همه علاقمندان قابل تهیه (دانلود) از طریق اینترنت می باشند، و سوما ابزار Hping با نمایش پرچم ها، و آمار بسته های دریافت شده و یا دریافت نشدن بسته ها وظیفه نتیجه گیری عمل پویش را بعهده خود کاربر گذاشته و براحتی نکات مربوط به پویش ها را عملا نمایش می دهد.
اما ابزارهای متنوع رایگان و تجاری دیگری برای پویش پورت ها وجود دارد که در ادامه بصورت بسیار مختصر به معرفی آنها پرداخته و درصورت علاقه به مطالعه جزئیات مطالب بدلیل سهولت آنها به عهده خواننده گذاشته شده است.

3.1- ابزار Strobe

Strobe یک ابزار پویش پورت TCP می باشد که توسط Julian Assange نوشته شده و از طریق آدرس وب زیر قابل دریافت می باشد:

```
http://linux.maruhn.com/sec/strobe.html
```

Strobe یکی از سریعترین و قابل اعتمادترین ابزارهای پویش پورت بوده و تحت سیستم عاملهای خانواده Unix قابل استفاده می باشد.

```
# strobe 192.168.10.15
strobe 1.03 (c) 1995 Julian Assange (proff@suburbia.net).
192.168.10.15   echo              7/tcp Echo [95,JBP]
192.168.10.15   discard           9/tcp Discard [94,JBP]
192.168.10.15   sunrpc          111/tcp rpcbind SUN RPC
192.168.10.15   daytime          13/tcp Daytime [93,JBP]
192.168.10.15   chargen          19/tcp ttytst source
192.168.10.15   ftp              21/tcp File Transfer [Control]
192.168.10.15   exec            512/tcp remote process execution;
192.168.10.15   login           513/tcp remote login a la telnet;
192.168.10.15   cmd             514/tcp shell like exec, but automatic
192.168.10.15   ssh              22/tcp Secure Shell
192.168.10.15   telnet           23/tcp Telnet [112,JBP]
192.168.10.15   smtp             25/tcp Simple Mail Transfer [102,JBP]
192.168.10.15   nfs            2049/tcp networked file system
192.168.10.15   lockd          4045/tcp
192.168.10.15   unknown       32772/tcp unassigned
192.168.10.15   unknown       32773/tcp unassigned
```

این ابزار هر پورت TCP که در حالت Listening یا Open باشد را لیست می کند.

توجه داشته باشید که Strobe فقط پورت های TCP را مورد پویش قرار می دهد، ولی نتایج آن بسیار قابل اعتماد می باشند.

3.2- ابزار Netcat

NetCat ابزار چندکاره ای است که در این مقاله فقط به توانایی های پویش پورت آن می پردازیم. این ابزار بسیار فوق العاده توسط Hobbit نوشته شده و بدلیل توانایی های بسیار بالایی که دارد از این ابزار در صنعت امنیت به نام چاقوی چندکاره سوئیسی یاد می شود.
NC پویش ساده پورت های TCP و UDP را فراهم می کند. این ابزار هم برای سیستم عامل های خانواده ویندوز و هم برای سیستم عاملهای خانواده یونیکس قابل تهیه است.
برای راهنمایی بیشتر درمورد سوئیچ های این ابزار می توانید از راهنمای خط فرمان ابزار استفاده کنید.

دستور صادر شده که در زیر میبینید پورت های 1 تا 140 از نوع TCP مربوط به هاست تعیین شده را مورد پویش قرار می دهد.

```
# nc -v -z -w2 192.168.10.15 1-140
[192.168.10.15] 139 (?) open
[192.168.10.15] 135 (?) open
[192.168.10.15] 110 (pop-3) open
[192.168.10.15] 106 (?) open
[192.168.10.15] 81 (?) open
[192.168.10.15] 80 (http) open
[192.168.10.15] 79 (finger) open
[192.168.10.15] 53 (domain) open
[192.168.10.15] 42 (?) open
[192.168.10.15] 25 (smtp) open
[192.168.10.15] 21 (ftp) open
```

دستور صادر شده بعدی پورت های 1 تا 140 از نوع UDP مربوط به همان هاست را مورد پویش قرار می دهد.

نکته مهمی که باید مد نظر داشته باشید این است که پویش UDP در NC تحت ویندوز قابل استفاده نمی باشد و فقط در نسخه تحت خانواده UNIX این امکان فراهم شده است.

```
# nc -u -v -z -w2 192.168.10.15 1-140
[192.168.10.15] 135 (ntportmap) open
[192.168.10.15] 123 (ntp) open
[192.168.10.15] 53 (domain) open
[192.168.10.15] 42 (name) open
```

این ابزار را می توانید از آدرس وب زیر تهیه کنید:

http://netcat.sourceforge.net

3.3- ابزار SuperScan

یک ابزار ویندوزی با رابط گرافیکی (GUI) می باشد که بدلیل ساده بودن محیط کاری آن، به توضیح درمورد نحوه کار با آن نمی پردازیم. این ابزار را می توانید بهمراه ScanLine از سایت FoundStone دانلود نمائید.

3.4- ابزار ScanLine

یک ابزار کاملا ویندوزی مبتنی بر خط فرمان می باشد که توسط Found Stone ارائه شده است. می توان گفت سریعترین ابزاری که تاکنون برای پویش پورت ساخته شده همین ابزار بوده و از آدرس وب زیر قابل تهیه است:

http://www.foundstone.com

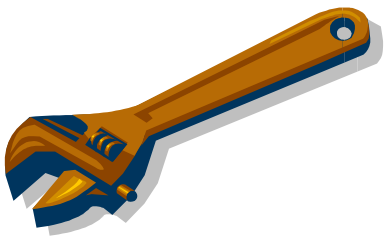
3.5- جدول ابزارهای رایج

در جدول زیر نرم افزارهای رایجی که در محیط های UNIX و Windows بیش از همه مورد استفاده قرار می گیرند آورده شده است. همانطور که می بینید تنها Nmap از ویژگی پویش نهان (Stealth) پشتیبانی می کند.

Scanner	TCP	UDP	Stealth	Resource
UNIX				
Strobe	X			http://linux.maruhn.com/sec/strobe.html
tcp_scan	X			http://wwdsilx.wwdsi.com/saint
udp_scan		X		http://wwdsilx.wwdsi.com/saint
Nmap	X	X	X	http://www.inscure.org/nmap
Netcat	X	X		http://netcat.sourceforge.net/
Windows				
Netcat	X	X*		http://joncraton.org/files/nc111nt.zip
SuperScan	X	X		http://www.foundstone.com/us/resources/termsofuse.asp?file=superscan4.zip
WUPS		X		http://ntsecurity.nu
ScanLine	X	X		http://www.foundstone.com/us/resources/termsofuse.asp?file=scanline.zip

*CAUTION: netcat UDP scanning never works under Windows, so don't rely on it.

Popular Scanning Tools and Features



3.6- جدول خلاصه سوئیچ های مورد استفاده در Nmap

Nmap Port Scanning Option Summary

Scan Option	Name	Packet Sequence	Notes
–sS	TCP SYN	→ SYN ← ACK SYN → ACK RST	Default scan type for privileged (root) user
–sT	TCP connect()	→ SYN ← ACK SYN → ACK → ACK RST	Default scan type for non–privileged user
–sF	FIN	→ FIN ← ACK RST	Usually no reply from open ports, ACK RST from closed ports
–sN	Null	→ No Flags ← ACK RST	
–sX	Xmas	→ FIN PSH URG ← ACK RST	
–sP	Ping	→ Echo Request ← Echo Reply -- and -- → ACK (just port 80) ← RST	Ping sweep with a twist (+ TCP port 80)
–sU	UDP	Null Data	
–sA	ACK	→ ACK ← ACK RST if port opened or closed ← No Reply if port filtered (firewall?)	
–sW	Window	Same as –sA	Window = zero if the port is closed, Window > zero if port is open
–sM	Maimon	→ FIN ACK ← RST (usually) -- or -- ← No Reply (if BSD)	BSD UNIX or not?

4.0 مقابله با پویش پورت

مقابله با پویش پورت شامل دو مرحله: کشف (Detection) و ممانعت (Prevention) می باشد.
برای مطلع شدن از چنین فعالیتی (Detection) درون شبکه باید از سیستم های کشف نفوذ مبتنی بر شبکه (Network-Based IDS) که بعضاً بصورت نرم افزاری ارائه شده اند مثل Snort استفاده کنید، این IDS را می توانید بصورت رایگان از آدرس www.snort.org تهیه کنید. بدلیل ماهیت وجودی و عملکرد سرویسها روی سیستم های مختلف تقریبا کار مشکلی خواهد بود که اجازه ندهید عمل پویش پورت روی سیستمتان انجام شود ولی همانطور که می بینید کشف به راحتی استفاده از یک IDS می باشد، پس قبل از اینکه یک شخص بیگانه پورت های باز روی سیستمتان را پیدا کند خودتان آنها را پیدا کرده و با بستن سرویسهای غیر ضروری خطر نفوذ را کاهش دهید.

موفق و سربلند باشید.
نیما بازگیر
تابستان 90

میخانه اگر ساقی صاحب نظری داشت *** میخواری و مستی ره و رسم دگری داشت