NMAP

هي أداة فحص (منافذ الإنترنت)، تستخدم من قبل المخترقين الأخلاقيين ومديرو الأنظمة لفحصها والتأكد فيما إذا كانت تتطابق مع معايير الأمان، تطبّق أداة nmap معظم استراتيجيات الفحص للبورتات، يمكن وصفها باختصار بأنها أداة لاكتشاف المنافذ المفتوحة

ينقسم فحص المنافذ لخدمات البروتوكول Tcp إلى نوعان هما:

الفحص الكامل المفتوح

هذه الطريقة تكمن عملها في الفحص للشبكات بواسطة أداةnmap ، حيث تقوم على آلية المصافحة الثلاثية، أي أن المختبر هو من يرسل حزمة SYN مع تحديد عنوان المنفذ، ثم يرد عليه الخادم بحزم SYN و ACK ، بعد ذلك سيرسل جهاز المختبر حزمتي ACK مع RST هذا الرد من الخادم يعني بأن المنفذ مفتوح، أما إذا رد الخادم مباشرة بحزمة RST فهذا يعني أن المنفذ مغلق.

كما تكمن الخطورة في هذه العملية بأن العملية تكون مسجلة بشكل كاملة، أي يتم رصد معلومات من قام بالفحص بشكل كامل.

كذلك يمكن تطبيق هذا الفحص على أداة nmap بالأمر التالي:

-sT

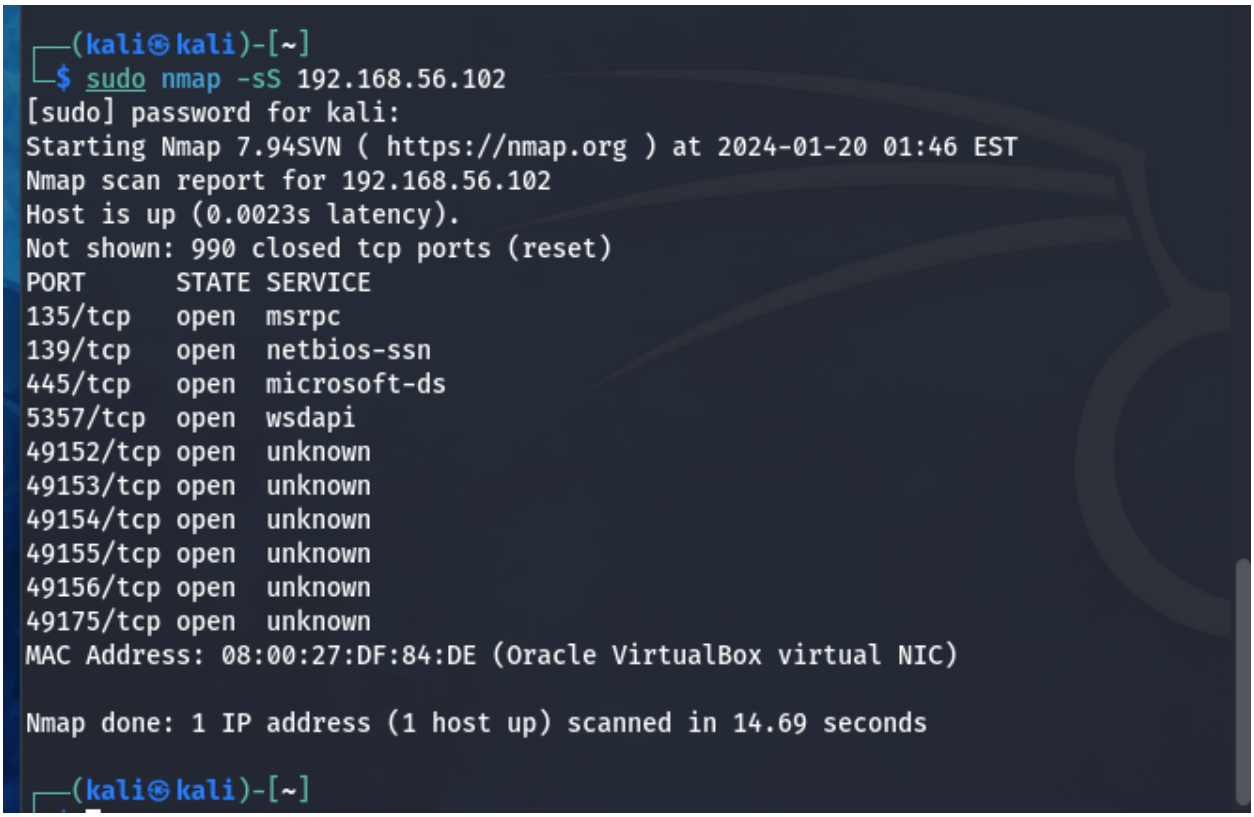
```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 01:44 EST
Nmap scan report for 192.168.56.102
Host is up (0.0020s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49175/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds

┌──(kali㉿kali)-[~]
└─$
```

الفحص نصف المفتوح

يشبه الفحص الكامل لكن بنصف العملية، هذا يعني أن المختبر الذي قام بإرسال الحزم ثم رد عليه الخادم لا يرسل بعدها المختبر ACK معRST ، وإنما يرسل RST فقط، هذه العملية لا تسجّل في الخادم، لكنها تتطلب صلاحيات الجذر.

الجدير بالذكر أن أداة nmap تتخذ هذه التقنية بشكل افتراضي عندما لا يتم تحديد تقنية أخرى، ويمكن تحديدها أيضًا بالأمر:

-sS



تقنيات أخرى لفحص الشبكات

فحصXmas

هذا الفحص يتم فيه إرسال حزمة tcp تحتوي على مجموعة من FIN و URG وPUSH ، يتم في فحص الإكس ماس وضع قيمة مشتركة بين الثلاث المجموعات، ترسل إلى الخادم عبر منفذ معيّن للفحص فإذا لم يرد الخادم هذا يعني أن المنفذ مفتوح أما إذا رد بحزمة RST فهذا يدل بأن المنفذ مغلق، هذه العملية لا يمكن عملها على الويندوز، بل على نظام لينكس فقط.

يمكن تطبيقها في أداة nmap بالأمر التالي:

-sX

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sX 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 01:48 EST
Nmap scan report for 192.168.56.102
Host is up (0.00099s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:DF:84:DE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.51 seconds

┌──(kali㉿kali)-[~]
└─$
```

Null scan: -sN

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sN 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 01:50 EST
Nmap scan report for 192.168.56.102
Host is up (0.00069s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:DF:84:DE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.80 seconds
```

FIN scan: -sF

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sF 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 01:51 EST
Nmap scan report for 192.168.56.102
Host is up (0.00066s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:DF:84:DE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 15.13 seconds
```

الفحص عن طريق الزومبي

هذا الطريقة تكمن في البحث عن جهاز وحيد، غير مضغوط من قبل الشبكة بشكل كبير، بعد ذلك يقوم المخترق بتزييف عنوان الإنترنت لديه إلى عنوان ذلك الجهاز، ثم يقوم بعملية الفحص للسيرفر عن طريق الجهاز الزومبي.

يمكن تطبيقها في أداة nmap بالأمر التالي:

-sI

nmap -sI <zombie host> p- <ports to scan> <target>

قائمة المساعدة في أداة nmap

-sL

استكشاف المضيف.

-sn

لتجريب الإتصال بالهدف بدون إجراء أي فحص نستخدم الأمر `-sn` كالتالي.
ملاحظة: عمل الأمر `sn` يشبه عمل `ping` حيث يستخدم لمعرفة ما إذا كان الهدف يعمل أم لا. مثل تفقد للشبكة.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 02:16 EST
Nmap scan report for 192.168.56.102
Host is up (0.00060s latency).
MAC Address: 08:00:27:DF:84:DE (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds

┌──(kali㉿kali)-[~]
```

-sV

لعمل فحص سريع (ضعيف) يعطي بعض المعلومات فقط و هذه اكثر طريقة مستخدمه لمعرفه بعض المعلومات السطحية عن الهدف نستخدم الأمر `-sV` كالتالي.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 02:19 EST
Nmap scan report for 192.168.56.102
Host is up (0.00093s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49175/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:DF:84:DE (Oracle VirtualBox virtual NIC)
Service Info: Host: USER1-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.18 seconds

┌──(kali㉿kali)-[~]
```

-O

لمعرفه نظام تشغيل رواتر او سيرفر موقع معين نستخدم الأمر `-O` كالتالي.

ملاحظة: الحرف O يكون حرف كبير و نستطيع كتابة دومين الموقع الذي نريد معرفة نظامه بشكل مباشر مكان الآيبي.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 02:21 EST
Nmap scan report for 192.168.56.102
Host is up (0.00068s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49175/tcp open  unknown
MAC Address: 08:00:27:DF:84:DE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:
/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.
1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.85 seconds

┌──(kali㉿kali)-[~]
```

.-F

لعمل فحص سريع نستخدم الأمر `-F` كالتالي مع الإشارة إلى أنه سوف يأخذ أول 100 بورت فقط و يفحصها.

Fragment

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -F 192.168.56.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 02:59 EST
Nmap scan report for 192.168.56.102
Host is up (0.00080s latency).
Not shown: 91 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:DF:84:DE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.59 seconds
```

-P

لفحص بورتات محددة مثلاً البورتات 80 و 139 و 443 نستخدم `-p` كالتالي.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 80,443,139 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 03:01 EST
Nmap scan report for 192.168.56.102
Host is up (0.00077s latency).

PORT    STATE  SERVICE
80/tcp  closed http
139/tcp open   netbios-ssn
443/tcp closed https
MAC Address: 08:00:27:DF:84:DE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.36 seconds
```

-A

لعمل فحص قوي يسمى فحص عدواني, نستخدم الرمز A- كالتالي مع الإشارة إلى أنه يتطلب وقت أكثر في لإتمام المهمة لأنه يفحص كل شي.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-20 03:03 EST
Nmap scan report for 192.168.56.102
Host is up (0.0011s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Home Premium 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49175/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:DF:84:DE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windo
ws_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: USER1-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -18h47m13s, deviation: 2h18m33s, median: -17h27m14s
| smb-os-discovery:
|   OS: Windows 7 Home Premium 7601 Service Pack 1 (Windows 7 Home Premium 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: user1-PC
|   NetBIOS computer name: USER1-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-01-19T18:37:57+04:00
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: USER1-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:df:84:de (Oracle VirtualBox virtual NIC)
| smb2-time:
|   date: 2024-01-19T14:37:57
```

Flag	Role	Command
-sS	TCP syn scan	nmap -sS <target>
-sT	TCP connect() scan	nmap -sT <target>
–sU	UDP scan	nmap -sU <target>
–sA	TCP ack scan	nmap -sA <target>
-sY	SCTP INIT scan	nmap -sY <target>
-sF	FIN Scan	nmap -sF <target>
-sP	Ping Scan	nmap -sP <target>
-sV	Version Detection	nmap -sV <target>
-sI	Idle Scan	nmap -sI <target>
-sW	TCP Window scan	nmap -sW <target>
-sM	TCP maimon scan	nmap -sM <target>
-sZ	SCTP COOKIE ECHO scan	nmap -sZ <target>
-s0	IP protocol scan	nmap -s0 <target>
-Pn	Scan only ports	nmap -Pn <target>