



# A DETAILED GUIDE TO **NMAP SCAN WITH**



# **WIRESHARK**

[WWW.HACKINGARTICLES.IN](http://WWW.HACKINGARTICLES.IN)

Contenido

Introducción.....3

Escaneo TCP .....3

Escaneo sigiloso .....6

Escaneo de aletas .....8

Escaneo nulo.....10

Escaneo UDP .....13

Escaneo de Navidad.....15

## Introducción

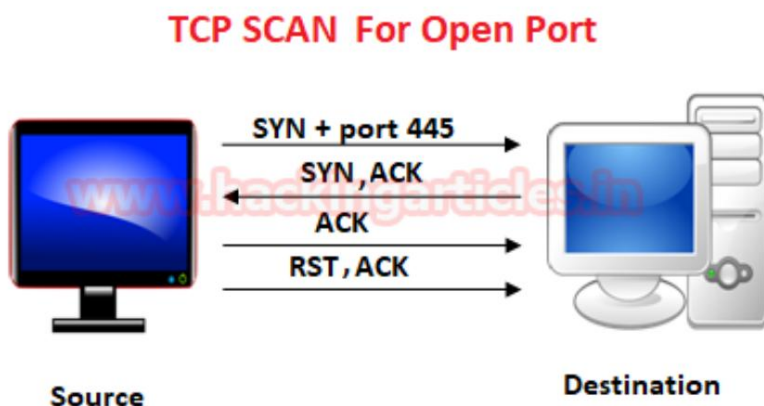
En esta publicación, aprenderá cómo capturar paquetes de red usando Wireshark cuando un atacante está escaneando un objetivo usando el método de escaneo de puertos NMAP. Aquí notará cómo Wireshark capturó diferentes paquetes de tráfico de red para puertos abiertos y cerrados.

Nota: La siguiente práctica se realiza con la misma dirección IP (192.168.1.102), que como notará es común para nuestras máquinas Windows y Linux. Puedes diferenciarlos por sus direcciones MAC en este caso.

¡¡¡Empecemos!!!

## Escaneo TCP

TCP Scan buscará puertos TCP como el puerto 22, 21, 23, 445, etc. y garantizará que el puerto de escucha esté abierto a través de una conexión de protocolo de enlace de 3 vías entre el puerto de origen y el de destino. Si el puerto está abierto, el origen envió un paquete SYN, el destino de la respuesta envió un paquete SYN, el origen envió paquetes ACK y el origen envió paquetes RST y ACK nuevamente.



Escriba el siguiente comando NMAP para el escaneo TCP e inicie Wireshark por otro lado para capturar el paquete enviado.

```
mapanm -st -p 445 192.168.1.102
```

En la imagen proporcionada, puede observar que el puerto 445 está abierto.

```

root@kali:~# nmap -sT -p 445 192.168.1.102

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 02:05 EDT
Nmap scan report for 192.168.1.102
Host is up (0.087s latency).
www.hackingarticles.in
PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 0C:D2:92:82:EE:02 (Intel Corporate)

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

```

Revise la secuencia de transferencia de paquetes entre el origen y el destino capturada a través de Wireshark.

Notarás que ha capturado la misma secuencia de la bandera como se describe arriba:

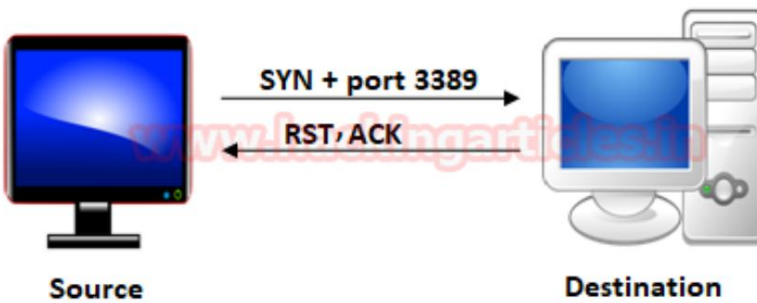
- El origen envió el paquete SYN al destino.
- Destino enviado SYN, ACK a la fuente
- El origen envió el paquete ACK al destino.
- La fuente envió nuevamente RST, ACK al destino

ip.addr == 192.168.1.113						
No.	Time	Source	Destination	Prot	Length	Info
129	37.411...	192.168.1.113	192.168.1.102 T...	TCP	74	52944 → 445 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
132	37.415...	192.168.1.102	192.168.1.113 T...	TCP	74	445 → 52944 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
133	37.415...	192.168.1.113	192.168.1.102 T...	TCP	66	52944 → 445 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TS=0
134	37.415...	192.168.1.113	192.168.1.102 T...	TCP	66	52944 → 445 [RST, ACK] Seq=1 Ack=1 Win=29312 Len=0 TS=0

Averigüemos el tráfico de red para el puerto cerrado. Según la imagen proporcionada, muestra que si el puerto de escaneo está cerrado, entonces no sería posible una conexión de protocolo de enlace de tres vías entre el origen y el destino.

La fuente envió un paquete SYN y si el puerto está cerrado, el receptor recibirá una respuesta a través de RST, ACK.

## TCP SACKN For Close Port



Escriba el siguiente comando NMAP para el escaneo TCP e inicie Wireshark por otro lado para capturar el paquete enviado.

```
mapanm -st -p 3389 192.168.1.102
```

En la imagen proporcionada, puede observar que el puerto 3389 está cerrado.

```

root@kali:~# nmap -sT -p 3389 192.168.1.102

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 03:54 EDT
Nmap scan report for 192.168.1.102
Host is up (0.049s latency).

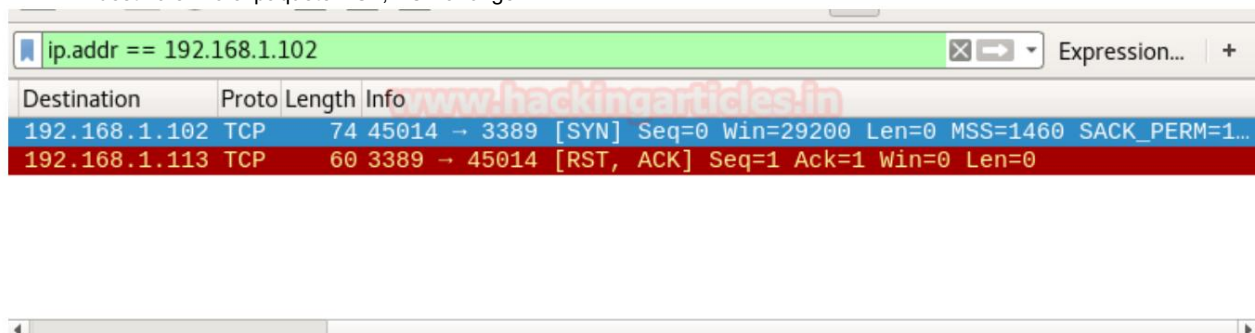
PORT      STATE      SERVICE
3389/tcp  closed    ms-wbt-server
MAC Address: 0C:D2:92:82:EE:02 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds
  
```

Revise la secuencia de transferencia de paquetes entre el origen y el destino capturada a través de Wireshark.

Notarás que ha capturado la misma secuencia de la bandera como se describe arriba:

- El origen envió el paquete SYN al destino.
- El destino envió el paquete RST, ACK al origen.





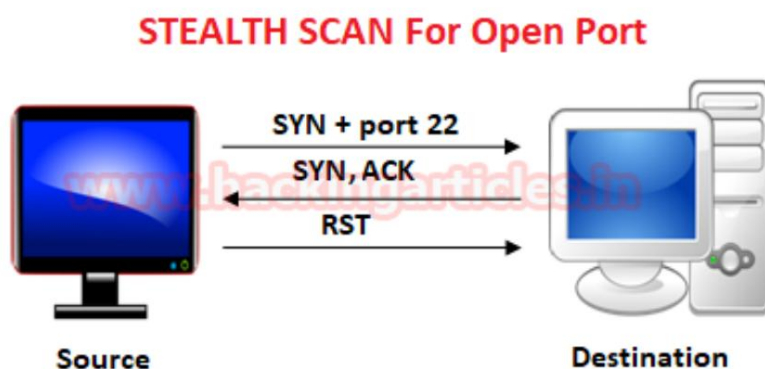
## Escaneo sigiloso

El escaneo SYN es la opción de escaneo predeterminada y más popular por buenas razones. Se puede realizar rápidamente, escaneando miles de puertos por segundo en una red rápida que no se ve obstaculizada por firewalls restrictivos. También es relativamente típico y sigiloso ya que nunca completa las conexiones TCP.

Si se recibe como respuesta un paquete SYN (sin el indicador ACK), el puerto también se considera abierto.

Esta técnica a menudo se denomina "escaneo medio abierto" porque no abre una conexión TCP completa.

Envía un paquete SYN como si fuera a establecer una conexión real y luego espera una respuesta. Un SYN, ACK indica que el puerto está escuchando (abierto).



Escriba el siguiente comando NMAP para el escaneo TCP e inicie Wireshark por otro lado para capturar el paquete enviado.

```
nmap -sS -p 22 192.168.1.102
```

En la imagen dada, puede observar que el puerto 22 está abierto.

```

root@kali:~# nmap -sS -p 22 192.168.1.102

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 04:10 EDT
Nmap scan report for 192.168.1.102
Host is up (0.046s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: AC:E0:10:E0:47:89 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 13.63 seconds
  
```

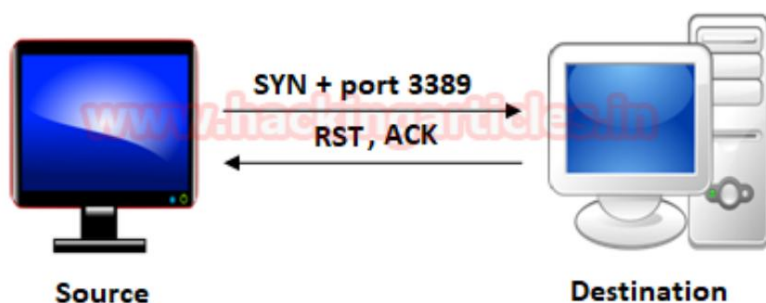
Revise la secuencia de transferencia de paquetes entre el origen y el destino capturados a través de Wireshark

- El origen envió paquetes SYN al destino.
- El destino envió paquetes SYN, ACK al origen
- El origen envió paquetes RST al destino.

Destination	Proto	Length	Info
192.168.1.102	TCP	58	65008 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.113	TCP	60	22 → 65008 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
192.168.1.102	TCP	54	65008 → 22 [RST] Seq=1 Win=0 Len=0

Ahora calcule el tráfico para el puerto cercano mediante un escaneo sigiloso. Cuando el origen envía un paquete SYN al puerto específico, si el puerto está cerrado, el destino responderá enviando un paquete RST.

### STEALTH SCAN For Close Port



Escriba el siguiente comando NMAP para el escaneo TCP e inicie Wireshark por otro lado para capturar el paquete enviado.

```
nmap -sS -p 3389 192.168.1.102
```

En la imagen proporcionada, puede observar que el puerto 3389 está cerrado.

```

root@kali:~# nmap -sS -p 3389 192.168.1.102

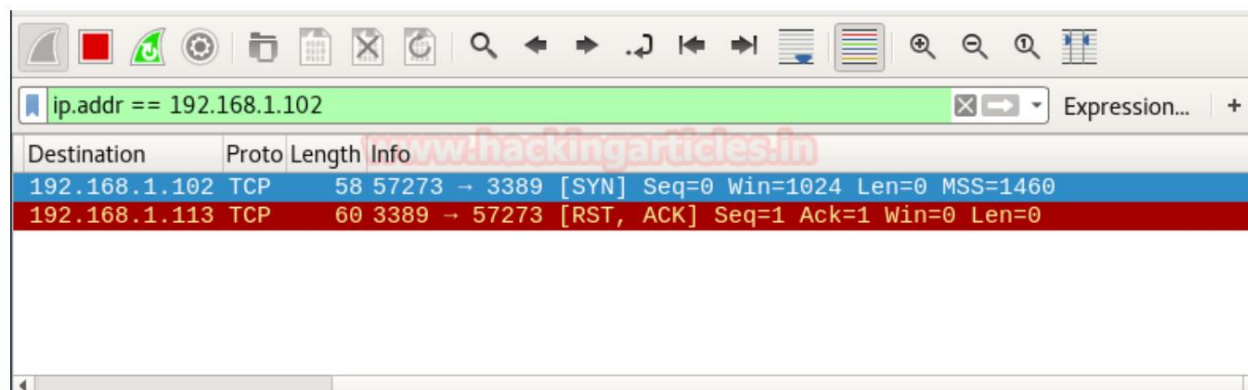
Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 04:07 EDT
Nmap scan report for 192.168.1.102
Host is up (0.043s latency).

PORT      STATE SERVICE
3389/tcp  closed ms-wbt-server
MAC Address: AC:E0:10:E0:47:89 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds
root@kali:~#
  
```

Revise la secuencia de transferencias de paquetes entre el origen y el destino capturadas a través de Wireshark.

- El origen envió paquetes SYN al destino.
- El destino envió paquetes RST, ACK al destino.

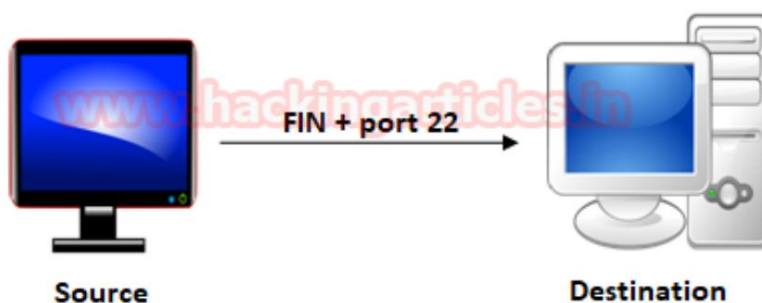


#### Escaneo de aletas

Se utiliza un paquete FIN para finalizar la conexión TCP entre los puertos de origen y de destino, normalmente una vez completada la transferencia de datos. Nmap inicia un escaneo FIN utilizando un paquete FIN en lugar de un paquete SYN. Si el puerto está abierto, no recibirá ninguna respuesta del puerto de destino cuando se envíe un paquete FIN a través del puerto de origen.

Fin-Scan solo funciona en máquinas Linux y no funciona en la última versión de Windows.

### FIN SCAN For Open Port



Escriba el siguiente comando NMAP para el escaneo TCP e inicie Wireshark por otro lado para capturar el paquete enviado.

```
mapanm -sF -p 22 192.168.1.102
```

En la imagen dada, puede observar que el puerto 22 está abierto.



```

root@kali:~# nmap -sF -p 22 192.168.1.102

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 04:20 EDT
Nmap scan report for 192.168.1.102
Host is up (0.085s latency).

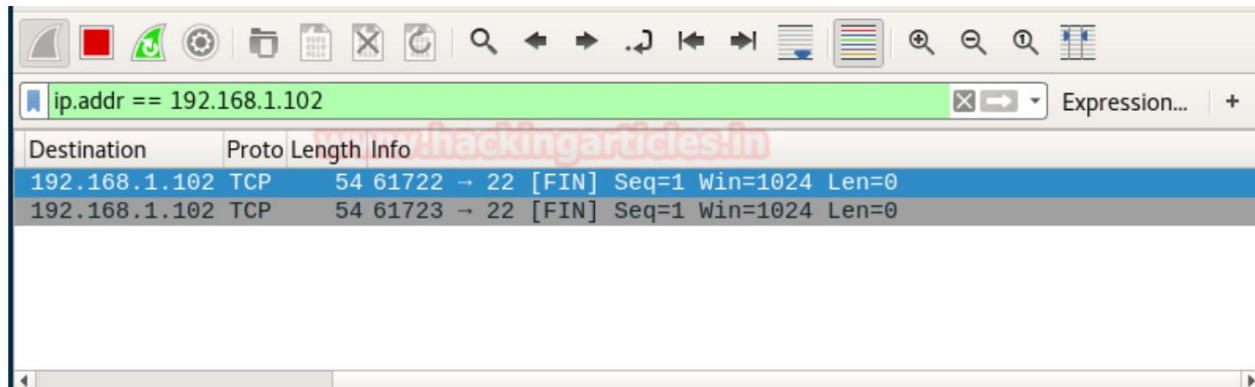
PORT      STATE SERVICE
22/tcp    open|filtered ssh
MAC Address: AC:E0:10:E0:47:89 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 14.29 seconds

```

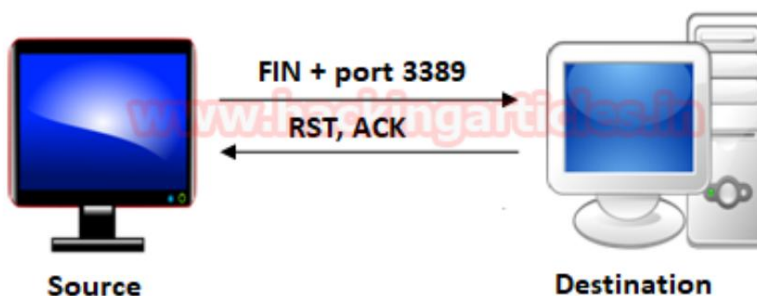
Revise la secuencia de transferencia de paquetes entre el origen y el destino capturados a través de Wireshark

- El origen envió paquetes FIN al destino.
- El destino no envió respuesta a la fuente.



De manera similar, si se realiza un escaneo Fin contra cualquier cierre, entonces el puerto de origen enviará un paquete FIN al puerto específico y el destino responderá enviando paquetes RST y ACK.

### FIN SCAN for Close Port



Escriba el siguiente comando NMAP para el escaneo TCP e inicie Wireshark por otro lado para capturar el paquete enviado.

```
mapanm -sF -p 3389 192.168.1.102
```

En la imagen proporcionada, puede observar que el puerto 3389 está cerrado.

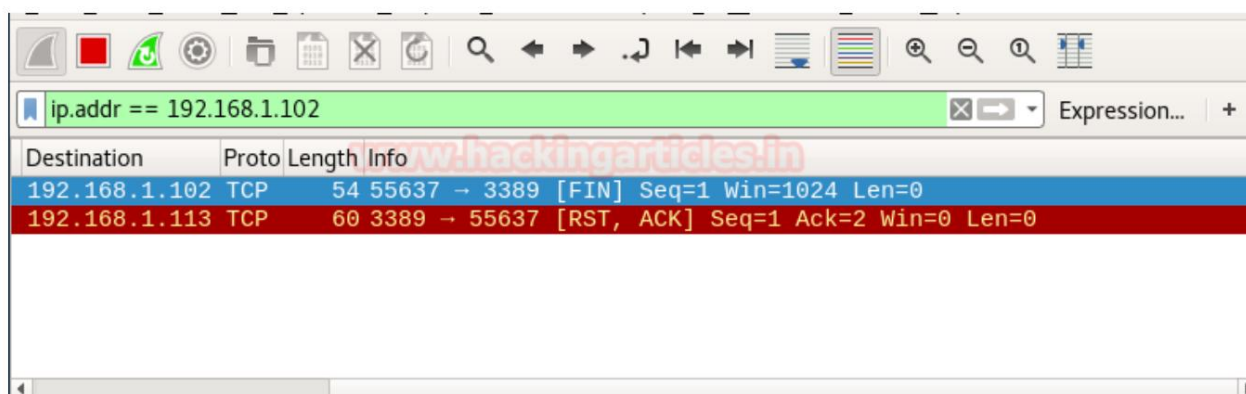
```
root@kali:~# nmap -sF -p 3389 192.168.1.102

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 04:22 EDT
Nmap scan report for 192.168.1.102
Host is up (0.065s latency).
www.hackingarticles.in
PORT      STATE SERVICE
3389/tcp  closed ms-wbt-server
MAC Address: AC:E0:10:E0:47:89 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds
```

Revise la secuencia de transferencias de paquetes entre el origen y el destino capturadas a través de Wireshark.

- El origen envió paquetes SYN al destino • El destino envió paquetes RST al destino

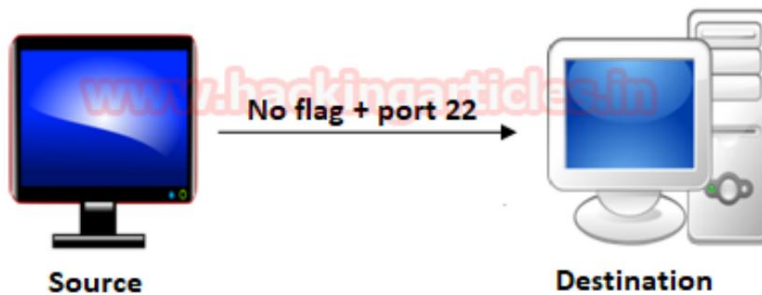


### Escaneo nulo

Una exploración nula es una serie de paquetes TCP que contienen un número de secuencia de "ceros" (0000000) y, como no se establecen indicadores, el destino no sabe cómo responder a la solicitud. Descartará el paquete y no se enviará ninguna respuesta, lo que indica que el puerto está abierto.

Null Scan solo funciona en máquinas Linux y no funciona en la última versión de Windows.

## NULL SCAN For Open Port



Escriba el siguiente comando NMAP para el escaneo TCP e inicie Wireshark por otro lado para capturar el paquete enviado.

```
nmap -sN -p 22 192.168.1.102
```

En la imagen dada, puede observar que el puerto 22 está abierto.

```
root@kali:~# nmap -sN -p 22 192.168.1.102

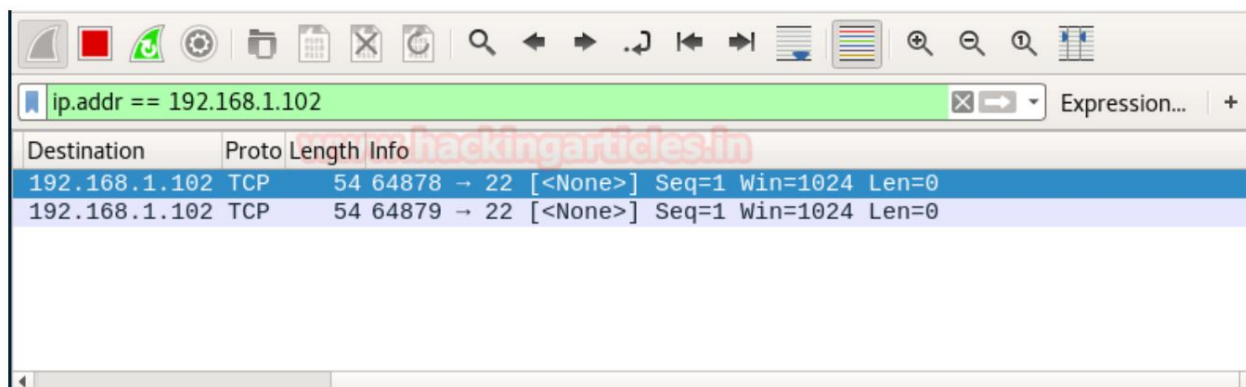
Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 04:26 EDT
Nmap scan report for 192.168.1.102
Host is up (0.071s latency).

PORT      STATE      SERVICE
22/tcp    open|filtered ssh
MAC Address: AC:E0:10:E0:47:89 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 14.17 seconds
```

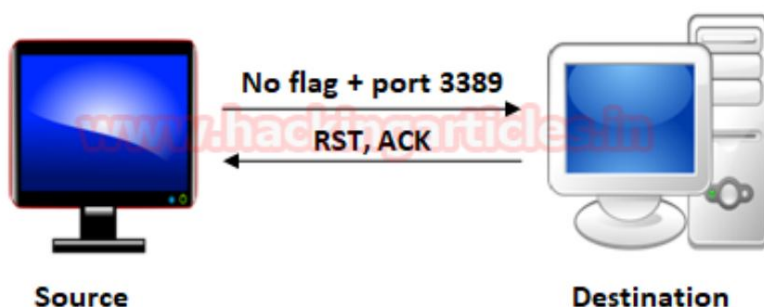
Revise la secuencia de transferencia de paquetes entre el origen y el destino capturados a través de Wireshark

- El origen envió paquetes nulos al destino.
- El destino no envió respuesta a la fuente.



Si el puerto está cerrado, el destino enviará un paquete RST y un ACK en respuesta cuando el origen envíe paquetes nulos en un puerto específico.

### NULL SCAN For Close Port



Escriba el siguiente comando NMAP para el escaneo TCP e inicie Wireshark por otro lado para capturar el paquete enviado.

```
nmap -sN -p 3389 192.168.1.102
```

En la imagen proporcionada, puede observar que el puerto 3389 está cerrado.

```

root@kali:~# nmap -sN -p 3389 192.168.1.102

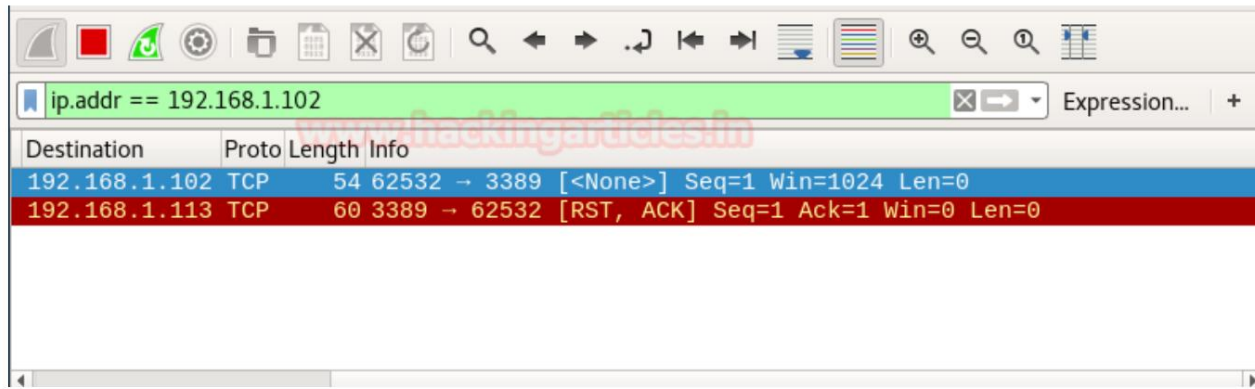
Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 04:30 EDT
Nmap scan report for 192.168.1.102
Host is up (0.063s latency).

PORT      STATE      SERVICE
3389/tcp  closed    ms-wbt-server
MAC Address: AC:E0:10:E0:47:89 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 13.63 seconds
  
```

Revise la secuencia de transferencia de paquetes entre el origen y el destino capturados a través de Wireshark

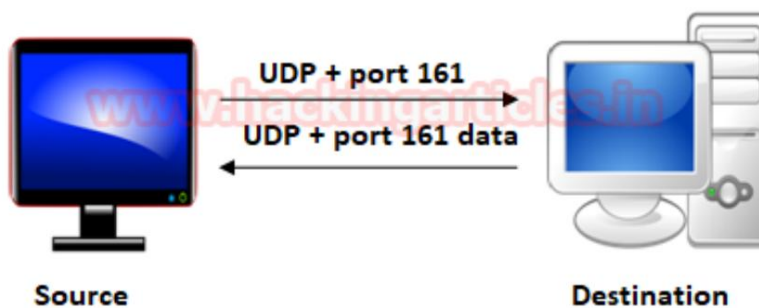
- El origen envió paquetes nulos (ninguno) al destino
- Destino enviado RST, ACK a la fuente



### Escaneo UDP

Un escaneo UDP funciona enviando un paquete UDP a cada puerto de destino; es un protocolo sin conexión. Para algunos puertos comunes, como 53 y 161, se envía una carga útil específica del protocolo para aumentar la tasa de respuesta. Un servicio responderá con un paquete UDP, demostrando que está abierto. Si no se recibe respuesta después de las retransmisiones, el puerto se clasifica como abierto/filtrado. Esto significa que el puerto podría estar abierto o quizás los filtros de paquetes estén bloqueando la comunicación.

### UDP SCAN For Open Port



Escriba el siguiente comando NMAP para el escaneo TCP e inicie Wireshark por otro lado para capturar el paquete enviado.

```
nmap -sU -p 161 192.168.1.119
```

En la imagen proporcionada, puede observar que el puerto 161 está abierto.



```

root@kali:~# nmap -sU -p 161 192.168.1.119

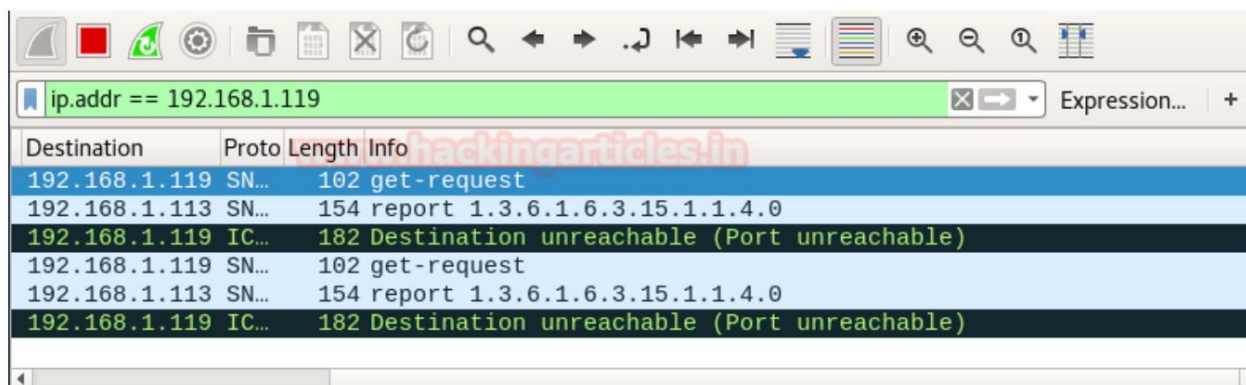
Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 04:32 EDT
Nmap scan report for 192.168.1.119
Host is up (0.0013s latency).
PORT      STATE SERVICE
161/udp   open  snmp
MAC Address: 00:0C:29:95:B8:D0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.64 seconds

```

Revise la secuencia de transferencia de paquetes entre el origen y el destino capturados a través de Wireshark

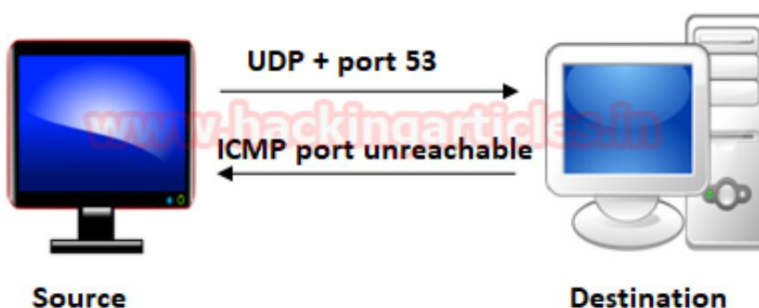
- El origen envió paquetes UDP al destino.
- El destino envió el paquete UDP con algunos datos al origen.



Destination	Proto	Length	Info
192.168.1.119	SN...	102	get-request
192.168.1.113	SN...	154	report 1.3.6.1.6.3.15.1.1.4.0
192.168.1.119	IC...	182	Destination unreachable (Port unreachable)
192.168.1.119	SN...	102	get-request
192.168.1.113	SN...	154	report 1.3.6.1.6.3.15.1.1.4.0
192.168.1.119	IC...	182	Destination unreachable (Port unreachable)

De manera similar, si una fuente envió un paquete UDP en un puerto cercano al destino, el destino respondería con un puerto de paquete ICMP inalcanzable con un error apropiado.

### UDP SCAN For ClosePort



Escriba el siguiente comando NMAP para el escaneo TCP e inicie Wireshark por otro lado para capturar el paquete enviado.

```
nmap -sU -p 53 192.168.1.119
```

En la imagen dada, puede observar que el puerto 53 está cerrado.

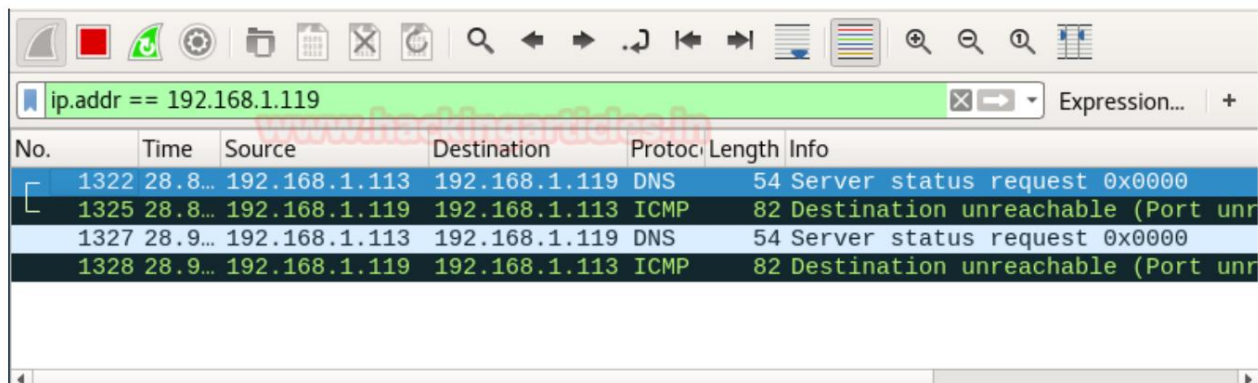
```
root@kali:~# nmap -sU -p 53 192.168.1.119

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 04:38 EDT
Nmap scan report for 192.168.1.119
Host is up (0.0016s latency).
www.hackingarticles.in
PORT      STATE SERVICE
53/udp    closed domain
MAC Address: 00:0C:29:95:B8:D0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.63 seconds
```

Revise la secuencia de transferencia de paquetes entre el origen y el destino capturados a través de Wireshark

- El origen envió paquetes UDP al destino.
- El destino envió el puerto del paquete ICMP inalcanzable para el origen



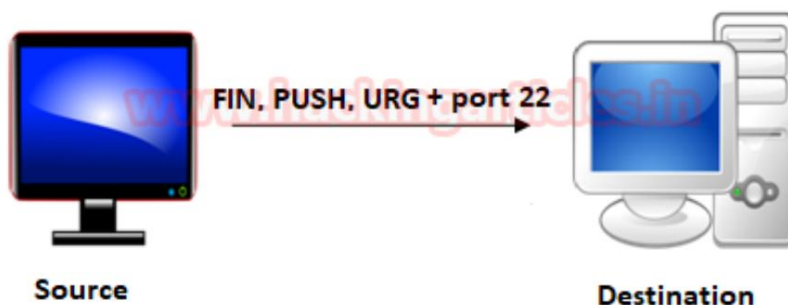
No.	Time	Source	Destination	Protocol	Length	Info
1322	28.8...	192.168.1.113	192.168.1.119	DNS	54	Server status request 0x0000
1325	28.8...	192.168.1.119	192.168.1.113	ICMP	82	Destination unreachable (Port unreachable)
1327	28.9...	192.168.1.113	192.168.1.119	DNS	54	Server status request 0x0000
1328	28.9...	192.168.1.119	192.168.1.113	ICMP	82	Destination unreachable (Port unreachable)

#### Escaneo de Navidad

Estos escaneos están diseñados para manipular los indicadores PSH, URG y FIN del encabezado TCP. Colocaron las banderas FIN, PSH y URG, iluminando el paquete como un árbol de Navidad. Cuando un origen envía paquetes FIN, PUSH y URG a un puerto específico, y si el puerto está abierto, el destino descartará los paquetes y no enviará ninguna respuesta al origen.

Xmas Scan solo funciona en máquinas Linux y no funciona en la última versión de Windows.

## XMAS SCAN For Open Port



Escriba el siguiente comando NMAP para el escaneo TCP e inicie Wireshark por otro lado para capturar el paquete enviado.

```
nmap -sX -p 22 192.168.1.102
```

En la imagen dada, puede observar que el puerto 22 está abierto.

```
root@kali:~# nmap -sX -p 22 192.168.1.102

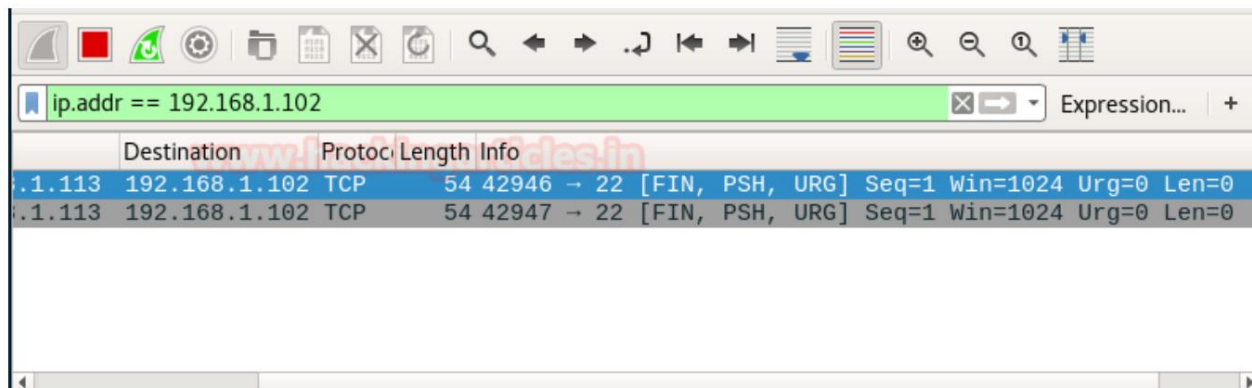
Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 04:42 EDT
Nmap scan report for 192.168.1.102
Host is up (0.028s latency).

PORT      STATE SERVICE
22/tcp    open|filtered ssh
MAC Address: AC:E0:10:E0:47:89 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds
```

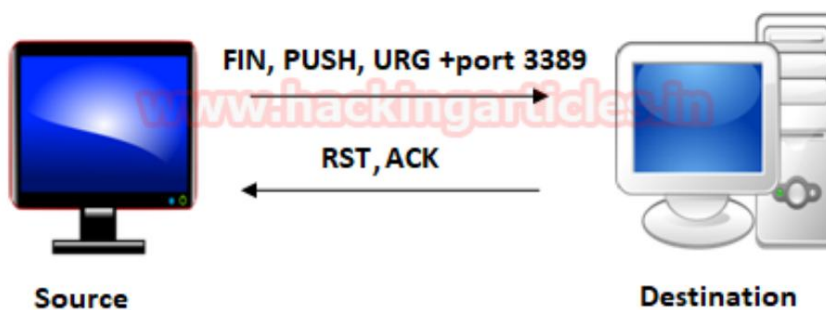
Revise la secuencia de transferencia de paquetes entre el origen y el destino capturados a través de Wireshark

- El origen envió paquetes FIN, PUSH y URG al destino
- El destino no envió respuesta a la fuente.



De manera similar, si un origen envía paquetes FIN, PUSH y URG a un puerto específico y si el puerto está cerrado, el destino enviará paquetes RST y ACK al origen.

### XMAS SCAN For Close Port



Escriba el siguiente comando NMAP para el escaneo TCP e inicie Wireshark por otro lado para capturar el paquete enviado.

```
nmap -sX -p 3389 192.168.1.102
```

En la imagen proporcionada, puede observar que el puerto 3389 está cerrado.

```

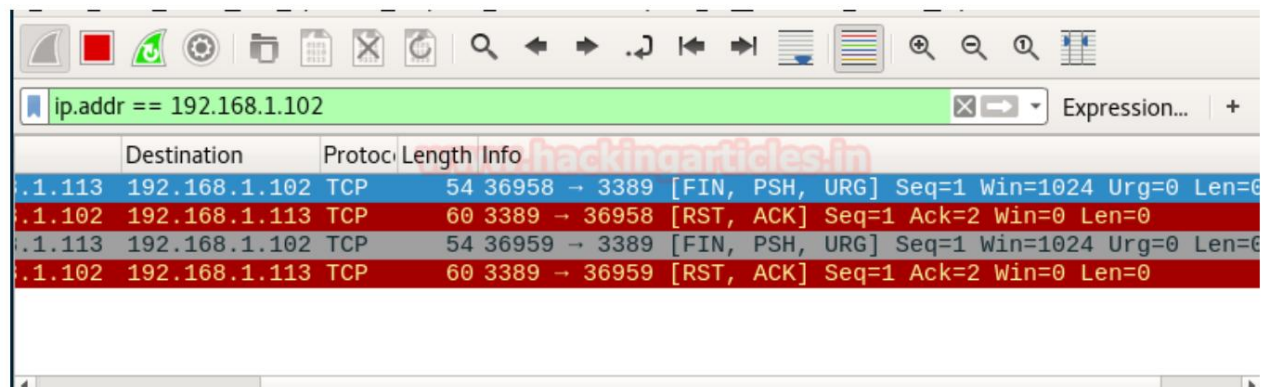
root@kali:~# nmap -sX -p 3389 192.168.1.102

Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-18 04:44 EDT
Nmap scan report for 192.168.1.102
Host is up (0.020s latency).
PORT      STATE      SERVICE
3389/tcp  closed    ms-wbt-server
MAC Address: AC:E0:10:E0:47:89 (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 13.84 seconds
  
```

Revise la secuencia de transferencia de paquetes entre el origen y el destino capturados a través de Wireshark

- El origen envió paquetes FIN, PUSH y URG al destino • Paquete RST, ACK de destino al origen





# ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

