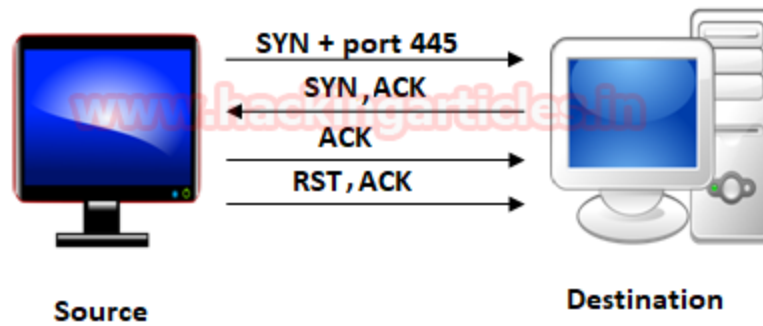


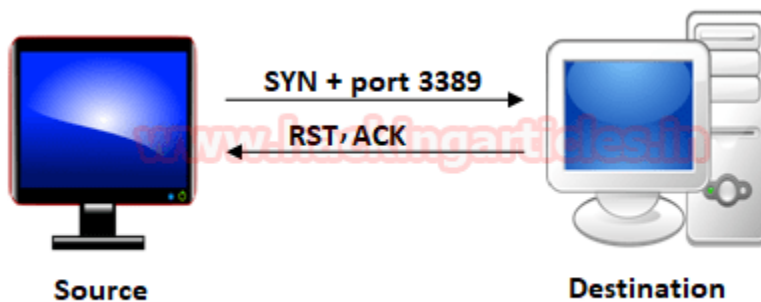
## TYPES OF NMAP SCANNING

### TCP scan for open ports



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

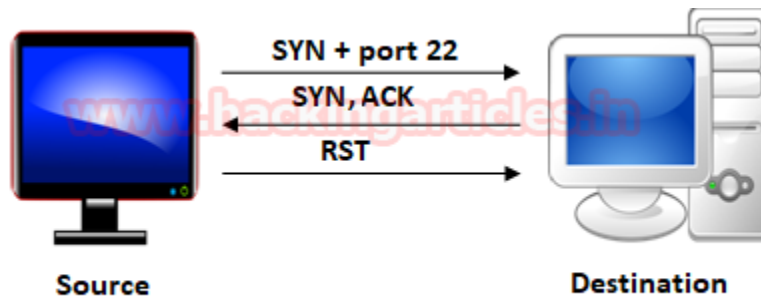
### TCP scan for close ports



ip.addr == 192.168.1.102							Expression...	+
Destination	Proto	Length	Info					
192.168.1.102	TCP	74	45014 → 3389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1...					
192.168.1.113	TCP	60	3389 → 45014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0					

## Stealth scan for open ports

- In stealth scan connection establishment is only done halfway.



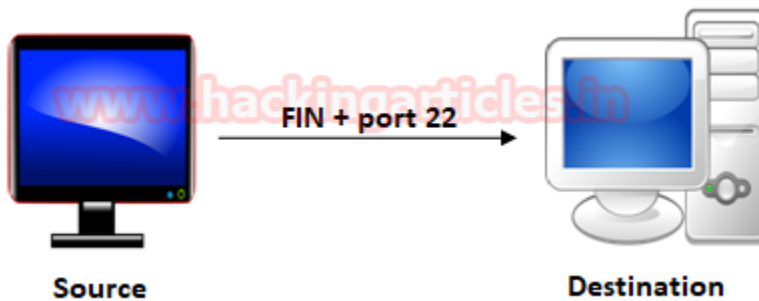
Destination	Proto	Length	Info
192.168.1.102	TCP	58	65008 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.113	TCP	60	22 → 65008 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
192.168.1.102	TCP	54	65008 → 22 [RST] Seq=1 Win=0 Len=0

## Stealth scan for closed ports

- Same as TCP scan for closed ports

## Fin scan for open ports

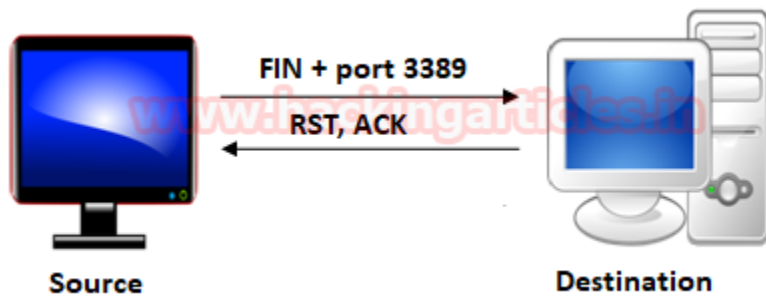
- If the port is open when the port receives packet with fin flag set without connection establishment destination will never reply back.(Destination not replying back for fin means the port is open)



The image shows a Wireshark packet capture window. The filter bar at the top contains the expression `ip.addr == 192.168.1.102`. The packet list below shows two captured packets:

Destination	Proto	Length	Info
192.168.1.102	TCP	54	61722 → 22 [FIN] Seq=1 Win=1024 Len=0
192.168.1.102	TCP	54	61723 → 22 [FIN] Seq=1 Win=1024 Len=0

## Fin scan for closed ports



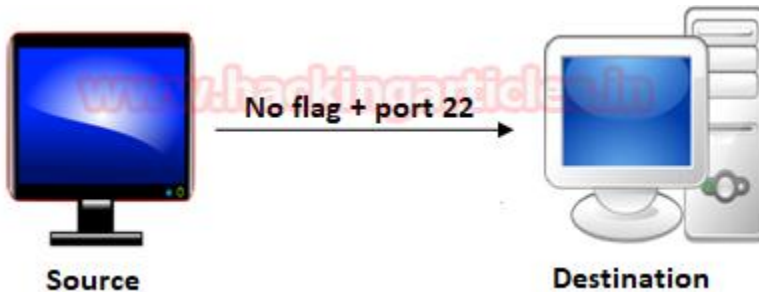
The image shows a Wireshark packet capture window. The filter bar at the top displays `ip.addr == 192.168.1.102`. The packet list shows two packets:

Destination	Proto	Length	Info
192.168.1.102	TCP	54	55637 → 3389 [FIN] Seq=1 Win=1024 Len=0
192.168.1.113	TCP	60	3389 → 55637 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

The first packet is a FIN packet from the source to the destination. The second packet is an RST, ACK response from the destination back to the source. A watermark [www.hackingarticles.in](http://www.hackingarticles.in) is visible across the packet list.

## Null scan for open ports

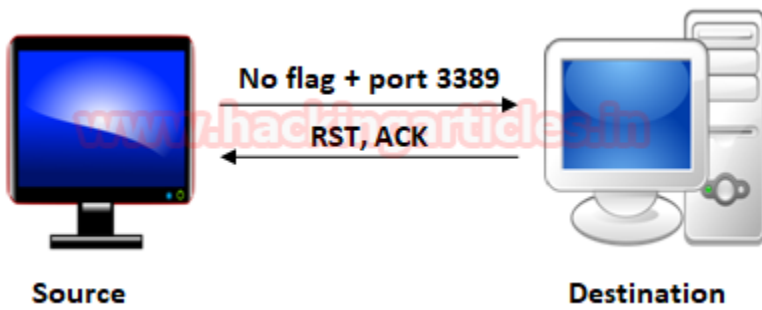
A Null Scan is a series of TCP packets which hold a sequence number of “zeros” (0000000) and since there are none flags set, the destination will not know how to reply the request. It will discard the packet and no reply will be sent, which indicate that port is open.



ip.addr == 192.168.1.102

Destination	Proto	Length	Info
192.168.1.102	TCP	54	64878 → 22 [<None>] Seq=1 Win=1024 Len=0
192.168.1.102	TCP	54	64879 → 22 [<None>] Seq=1 Win=1024 Len=0

## Null scan for closed ports

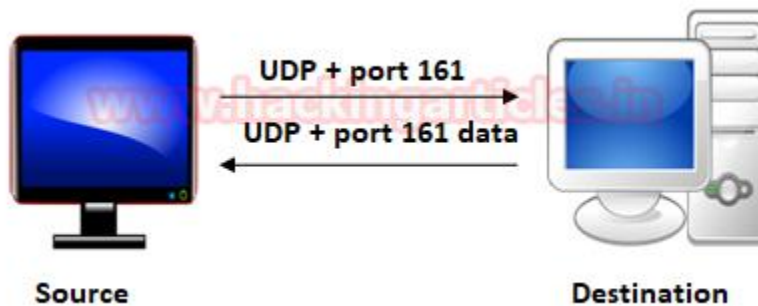


The screenshot shows a Wireshark packet capture. The filter bar at the top displays "ip.addr == 192.168.1.102". The packet list shows two packets:

Destination	Proto	Length	Info
192.168.1.102	TCP	54	62532 → 3389 [ <None> ] Seq=1 Win=1024 Len=0
192.168.1.113	TCP	60	3389 → 62532 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

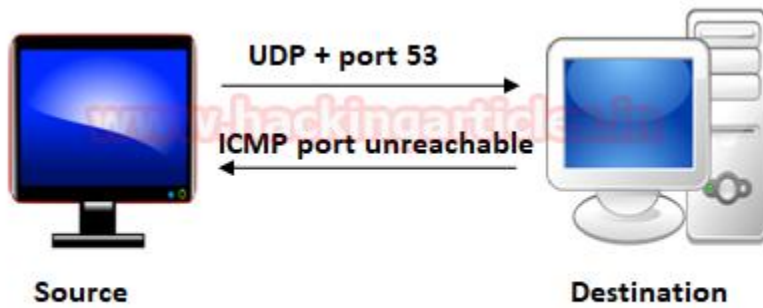
## UDP scan for open port

UDP scan works by sending a UDP packet to every destination port; it is a connection less protocol. For some common ports such as 53 and 161, a protocol-specific payload is sent to increase response rate, a service will respond with a UDP packet, proving that it is open. If no response is received after retransmissions, the port is classified as open|filtered. This means that the port could be open, or perhaps packet filters are blocking the communication.



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)

## UDP scan for closed port



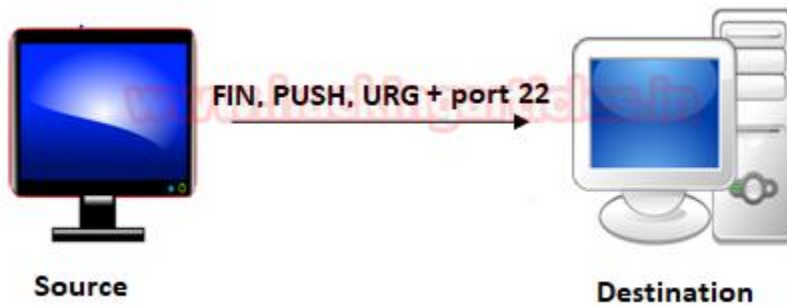
ip.addr == 192.168.1.119

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 unreach)
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 unreach)



## XMAS scan for open ports

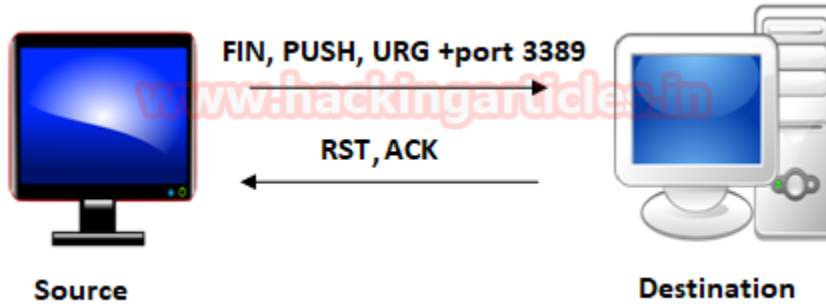
These scans are designed to manipulate the PSH, URG and FIN flags of the TCP header, Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree. When source sent FIN, PUSH, and URG packet to specific port and if port is open then destination will discard the packets and will not sent any reply to source.



The image shows a Wireshark packet capture window. The filter bar at the top contains the expression "ip.addr == 192.168.1.102". The packet list shows two captured packets, both of which are XMAS scans (FIN, PSH, URG) sent to 192.168.1.102.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.113	192.168.1.102	TCP	54	42946 → 22 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2	0.000000	192.168.1.113	192.168.1.102	TCP	54	42947 → 22 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

## XMAS scan for closed ports



	Destination	Protoc	Length	Info
1	192.168.1.113	TCP	54	36958 → 3389 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2	192.168.1.102	TCP	60	3389 → 36958 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
3	192.168.1.113	TCP	54	36959 → 3389 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
4	192.168.1.102	TCP	60	3389 → 36959 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0