iGNITE Technologies

Nmap for Pentester

PACKET TRACE

WWW.HACKINGARTICLES.IN

Contents

Introduction

Hello, everyone. Today we'll see how to capture network packets using nmap. And we'll use Wireshark to compare its results with nmap. In this article, we mainly focus on what types of network traffic are captured by nmap while we use various nmap ping scans.

A ping scan in Nmap is done to check if the target host is alive or not. As we know, ping by default sends the ICMP echo request and gets an ICMP echo reply if the system is alive. Ping scan by default sends an ARP packet and gets a response to check if the host is up.

NOTE: Nmap scans change their behavior according to the network they are scanning.

- Scanning local network with nmap where nmap sends an ARP packet with every scan.
- If an external network is to be scanned; nmap sends the following request packets:

ICMP echo request

ICMP timestamp request

TCP SYN to port 443

TCP ACK to port 80

Technique involves packet-tracing via nmap.

The nmap module is an interface with nmap's internal functions and data structures. The API offers target host information such as port states and version detection results. It also provides an interface to the Nsock library for effective network I/O.

Nsock is a parallel sockets library used by NSE, service detection (service_scan.cc) and DNS (nmap_dns.cc). **It acts as an abstraction layer above socket operations and is optimised for handling multiple sockets.** "mspool" is defined in "nsock_internal.h" and contains, among other things, a struct event_lists, which is a structure that keeps information on all pending events.

Event creation

Events are represented with the msevent struct (nsock_internal.h) which contains (among other things)

- The callback handler -> nsock_ev_handler (nsock_pool, nsock_event, void *)
- A pointer to a msiod struct -> msiod *iod, which holds all the I/O descriptor (**IOD**) related information.
- Struct filespace iobuf (a buffer usually 1024 bytes which holds the **write/read** bytes)
- The nse_type (nsock.h)
- The nse_status (nsock.h)
- A unique id -> nsock_event_id (**EID**)

Events are created with the the following special functions:

nsock_connect.c

- nsock_connect_tcp
- nsock_connect_udp
- nsock_connect_ssl
- nsock_reconnect_ssl

nsock_read.c

- nsock_readlines
- nsock_readbytes
- nsock_read

nsock_write.c

- nsock_write
- nsock_printf

nsock_timer_create.c

- nsock_timer_create

source: https://sock-raw.org/nmap-ncrack/nsock.html

Nmap Sweep Ping Analysis

Attribute **-sn/ -sP** are used for sweep ping and they try to identify the live host in the network. Using **–packet-trace** along nmap scan we can observe the network packet.

```
nmap -sn 192.168.1.103 --packet-trace
```

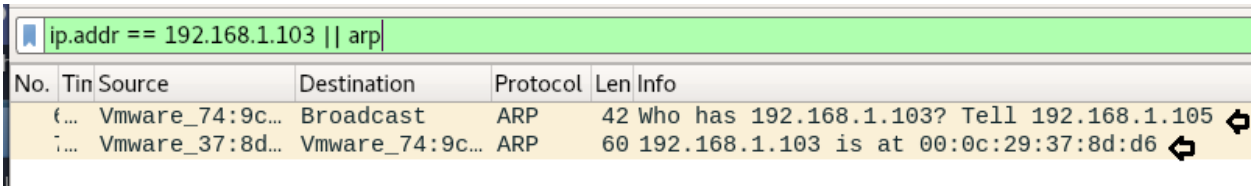
Here you can observe the first two packets SENT/RECD (received), showing an ARP request packet from 192.168.1.105 to 192.168.1.103 and then use NSOCK libraries to state the actual request and response packets travelling between the source and destination router.

- NSOCK INFO that denotes a new nsock_event_id (**EID**) **8** is generated to represents I/O descriptor **(IOD) #1** for NSOCK UDP connection request to the router on **port 53**.
- NSOCK INFO that denotes another (EID) **18** is generated to represents read request from (IOD) #1.
- NSOCK INFO that denotes another (EID) **27** is generated to represents write request for 44 bytes to (IOD) #1.
- NSOCK INFO that denotes SUCCESSFUL operation when nsock used callback_handler to connect for EID 8.
- NSOCK INFO that denotes SUCCESSFUL operation when nsock used callback_handler to write for EID 27.
- NSOCK INFO that denotes SUCCESSFUL operation when nsock used callback_handler to read for EID 18.
- NSOCK info that IOD #1 is deleted.
- NSOCK info that nevent_delete is deleting on event 34.
- At last Nmap scan report Host is up.

```
root@kali:~# nmap -sn 192.168.1.103 --packet-trace
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-27 16:38 IST
SENT (0.0391s) ARP who-has 192.168.1.103 tell 192.168.1.105
RCVD (0.0393s) ARP reply 192.168.1.103 is-at 00:0C:29:37:8D:D6
NSOCK INFO [0.0900s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0910s] nsock_connect_udp(): UDP connection requested to 192.168.1.1:53 (I
OD #1) EID 8
NSOCK INFO [0.0910s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeout:
-1ms) EID 18
NSOCK INFO [0.0910s] nsock_write(): Write request for 44 bytes to IOD #1 EID 27 [192.16
8.1.1:53]
NSOCK INFO [0.0910s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID
8 [192.168.1.1:53]
NSOCK INFO [0.0910s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27
 [192.168.1.1:53]
NSOCK INFO [0.1050s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18
[192.168.1.1:53] (121 bytes)
NSOCK INFO [0.1050s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeout:
-1ms) EID 34
NSOCK INFO [0.1050s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1050s] nevent_delete(): nevent_delete on event #34 (type READ)
Nmap scan report for 192.168.1.103
Host is up (0.00020s latency).
MAC Address: 00:0C:29:37:8D:D6 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
root@kali:~#
```

You can observe the same traffic we have captured from Wireshark

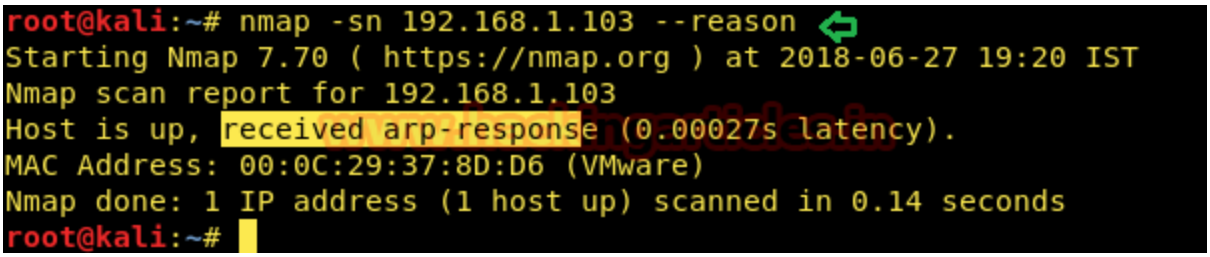
- Arp request packet for 192.168.1.105 to 192.168.1.103
- Arp reply packet from 192.168.1.103 to 192.168.1.105



To enumerate responses from the host network, use the **-reason** option with the nmap command.

nmap -sn 192.168.1.103 --reason

As you can observe, it has clearly shown the host is up when it receives an arp-response.



As we have seen, Nmap sends an ARP packet by default to identify the host status, so we will now trace the Nmap packet when -disable-arp-ping is enabled.

nmap -sn 192.168.1.103 --packet-trace --disable-arp-ping

Here you can notice the following SENT packets from source 192.168.1.105 to destination 192.168.1.103.

- ICMP echo request
- ICMP timestamp request
- TCP SYN to port 443
- TCP ACK to port 80

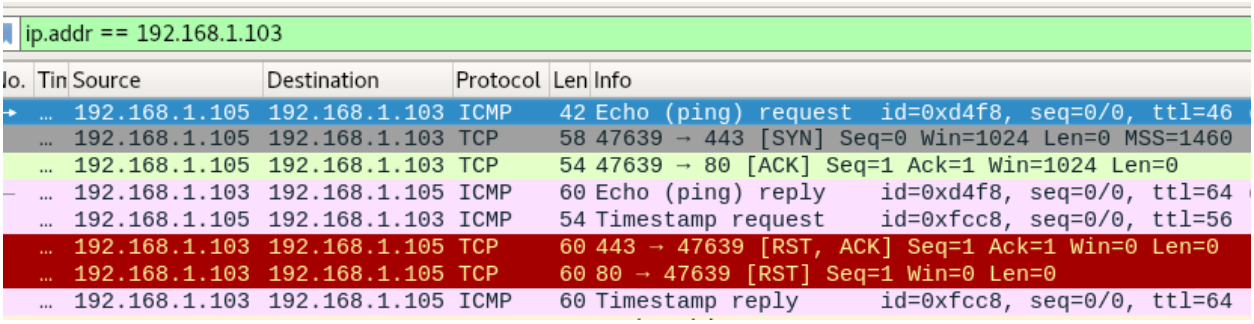
Then RCVD packet ICMP Echo-reply from destination **192.168.1.103** and then used NSOCK libraries to state actual request and response packets travel between source to the destination router.

```
root@kali:~# nmap -sn 192.168.1.103 --packet-trace --disable-arp-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-27 16:40 IST
SENT (0.0462s) ICMP [192.168.1.105 > 192.168.1.103 Echo request (type=8/code=0) id=545
0 seq=0] IP [ttl=46 id=50272 iplen=28 ]
SENT (0.0463s) TCP 192.168.1.105:47639 > 192.168.1.103:443 S ttl=43 id=44313 iplen=44
seq=3811746296 win=1024 <mss 1460>
SENT (0.0463s) TCP 192.168.1.105:47639 > 192.168.1.103:80 A ttl=44 id=58556 iplen=40
eq=0 win=1024
SENT (0.0464s) ICMP [192.168.1.105 > 192.168.1.103 Timestamp request (type=13/code=0)
d=64712 seq=0 orig=0 recv=0 trans=0] IP [ttl=56 id=3924 iplen=40 ]
RCVD (0.0463s) ICMP [192.168.1.103 > 192.168.1.105 Echo reply (type=0/code=0) id=54520
seq=0] IP [ttl=64 id=33592 iplen=28 ]
NSOCK INFO [0.0860s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0860s] nsock_connect_udp(): UDP connection requested to 192.168.1.1:53 (
OD #1) EID 8
NSOCK INFO [0.0860s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeout:
-1ms) EID 18
NSOCK INFO [0.0860s] nsock_write(): Write request for 44 bytes to IOD #1 EID 27 [192.1
8.1.1:53]
NSOCK INFO [0.0860s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID
8 [192.168.1.1:53]
NSOCK INFO [0.0860s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 2
 [192.168.1.1:53]
NSOCK INFO [0.1010s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18
[192.168.1.1:53] (121 bytes)
NSOCK INFO [0.1010s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeout:
-1ms) EID 34
NSOCK INFO [0.1010s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1010s] nevent_delete(): nevent_delete on event #34 (type READ)
Nmap scan report for 192.168.1.103
Host is up (0.00021s latency).
MAC Address: 00:0C:29:37:8D:D6 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
root@kali:~#
```

Demonstrating the workings of Ping Sweep using Wireshark

From the given below image, you can observe the following packet of request and reply between both network IP.

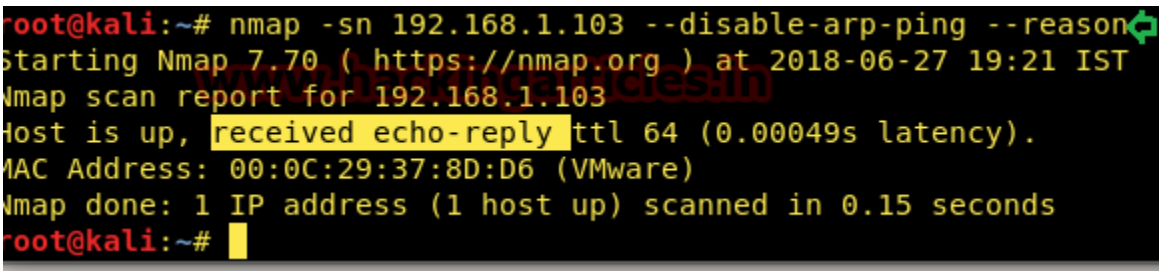
1. ICMP echo request
2. TCP SYN to port 443
3. TCP ACK to port 80
4. ICMP timestamp request
5. ICMP echo reply
6. TCP RST, ACK to port 443
7. TCP RST to port 80
8. ICMP Timestamp Reply



To enumerate responses from the host network, use the -reason option with the nmap command.

nmap -sn 192.168.1.103 --disable-arp-ping --reason

As you can observe it has clearly shown Host is up when received ICMP echo-response.



Nmap TCP-SYN Ping Analysis

Attribute -PS sends TCP SYN packet on port 80 by default; we can change it by specifying the ports with it, like -P22.

nmap -PS -p22 192.168.1.103 --packet-trace

Here you can observe that this scan is the addition of the nmap **ping scan** and the nmap **stealth scan** because, in the beginning, it sends an arp packet, then uses nsock libraries, and at the end, it again implicates TCP half communication.

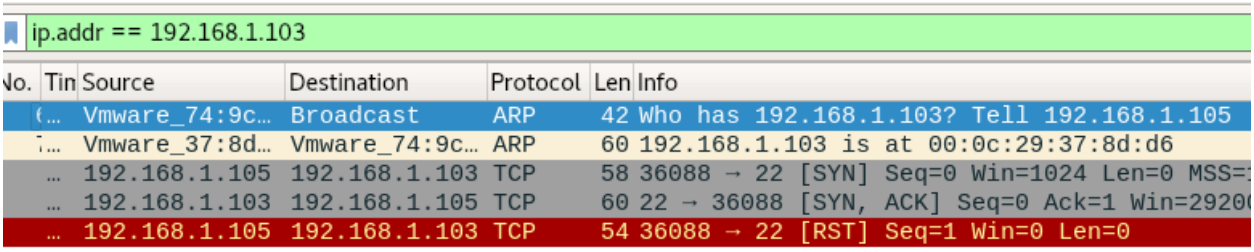
So, you can observe the following information we fetched from nmap:

- SENT/RECD ARP request and reply respectively.
- Nsock libraries details
- TCP-SYN packet from 192.168.1.105:36088 to 192.168.1.103:22.
- TCP-SYN/ACK packet from 192.168.1.103:22 to 192.168.1.105:36088.

```
root@kali:~# nmap -PS -p22 192.168.1.103 --packet-trace
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-27 16:58 IST
SENT (0.0670s) ARP who-has 192.168.1.103 tell 192.168.1.105
RCVD (0.0672s) ARP reply 192.168.1.103 is-at 00:0C:29:37:8D:D6
NSOCK INFO [0.1200s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.1200s] nsock_connect_udp(): UDP connection requested to 192.168.1.1:53 (I
OD #1) EID 8
NSOCK INFO [0.1200s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeout:
-1ms) EID 18
NSOCK INFO [0.1210s] nsock_write(): Write request for 44 bytes to IOD #1 EID 27 [192.16
8.1.1:53]
NSOCK INFO [0.1210s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID
8 [192.168.1.1:53]
NSOCK INFO [0.1210s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27
 [192.168.1.1:53]
NSOCK INFO [0.1360s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18
[192.168.1.1:53] (121 bytes)
NSOCK INFO [0.1360s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeout:
-1ms) EID 34
NSOCK INFO [0.1360s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1360s] nevent_delete(): nevent_delete on event #34 (type READ)
SENT (0.1847s) TCP 192.168.1.105:36088 > 192.168.1.103:22 S ttl=42 id=19516 iplen=44  s
eq=683521233 win=1024 <mss 1460>
RCVD (0.1850s) TCP 192.168.1.103:22 > 192.168.1.105:36088 SA ttl=64 id=0 iplen=44  seq=
642256733 win=29200 <mss 1460>
Nmap scan report for 192.168.1.103
Host is up (0.00022s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:37:8D:D6 (VMware)
```

Similarly, we saw the same pattern of network traffic in Wireshark.



Similar you can also choose –reason option with nmap command to enumerate response from host network.

nmap -PS -p22 192.168.1.103 --reason

Here you can observe port 22 is open and when received SYN/ACK packet from the host.

```
root@kali:~# nmap -PS -p22 192.168.1.103 --reason
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-27 19:24 IST
Nmap scan report for 192.168.1.103
Host is up, received arp-response (0.00044s latency).

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
MAC Address: 00:0C:29:37:8D:D6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```


Now let figure out network traffic when –disable-arp-ping activated.

nmap -PS -p22 192.168.1.103 --packet-trace --disable-arp-ping

So, you can observe the following information we fetched from nmap:

- SENT TCP-SYN packet on port 80
- RCVD TCP-RST/ACK from port 80.
- Nsock libraries details
- TCP-SYN packet from 192.168.1.105:63581 to 192.168.1.103:22.
- TCP-SYN/ACK packet from 192.168.1.103:22 to 192.168.1.105:63851.

```
root@kali:~# nmap -PS -p22 192.168.1.103 --packet-trace --disable-arp-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-27 17:02 IST
SENT (0.0687s) TCP 192.168.1.105:63595 > 192.168.1.103:80 S ttl=58 id=43386 iplen
=44  seq=3631585945 win=1024 <mss 1460>
RCVD (0.0689s) TCP 192.168.1.103:80 > 192.168.1.105:63595 RA ttl=64 id=35594 iple
n=40  seq=0 win=0
NSOCK INFO [0.1280s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.1280s] nsock_connect_udp(): UDP connection requested to 192.168.1.1
:53 (IOD #1) EID 8
NSOCK INFO [0.1280s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (tim
eout: -1ms) EID 18
NSOCK INFO [0.1280s] nsock_write(): Write request for 44 bytes to IOD #1 EID 27 [
192.168.1.1:53]
NSOCK INFO [0.1280s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS fo
r EID 8 [192.168.1.1:53]
NSOCK INFO [0.1280s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for
EID 27 [192.168.1.1:53]
NSOCK INFO [0.1430s] nsock_trace_handler_callback(): Callback: READ SUCCESS for E
ID 18 [192.168.1.1:53] (121 bytes)
NSOCK INFO [0.1430s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (tim
eout: -1ms) EID 34
NSOCK INFO [0.1430s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1430s] nevent_delete(): nevent_delete on event #34 (type READ)
SENT (0.1948s) TCP 192.168.1.105:63851 > 192.168.1.103:22 S ttl=52 id=8113 iplen=
44  seq=3751894127 win=1024 <mss 1460>
RCVD (0.1952s) TCP 192.168.1.103:22 > 192.168.1.105:63851 SA ttl=64 id=0 iplen=44
  seq=1223132932 win=29200 <mss 1460>
Nmap scan report for 192.168.1.103
Host is up (0.00026s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:37:8D:D6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Similarly, we saw the same pattern of network traffic in Wireshark also.

ip.addr == 192.168.1.103

Tin	Source	Destination	Protocol	Len	Info
…	192.168.1.105	192.168.1.103	TCP	58	63595 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
…	192.168.1.103	192.168.1.105	TCP	60	80 → 63595 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
…	192.168.1.105	192.168.1.103	TCP	58	63851 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
…	192.168.1.103	192.168.1.105	TCP	60	22 → 63851 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len
…	192.168.1.105	192.168.1.103	TCP	54	63851 → 22 [RST] Seq=1 Win=0 Len=0

Nmap ICMP Ping Analysis

-PE sends an ICMP echo request packet [ICMP type 8] and receives an ICMP echo reply packet.

nmap -sP -PE 192.168.1.103 --packet-trace --disable-arp-ping

Here you can notice ICMP Echo-request packets SENT from source 192.168.1.105 to destination 192.168.1.103

Then RCVD packet ICMP Echo-reply from destination 192.168.1.103 and then used NSOCK libraries to state actual request and response packets travelling between the source and the destination router.

```
root@kali:~# nmap -sP -PE 192.168.1.103 --packet-trace --disable-arp-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-27 17:12 IST
SENT (0.0346s) ICMP [192.168.1.105 > 192.168.1.103 Echo request (type=8/code=0) i
d=15512 seq=0] IP [ttl=42 id=10543 iplen=28 ]
RCVD (0.0348s) ICMP [192.168.1.103 > 192.168.1.105 Echo reply (type=0/code=0) id=
15512 seq=0] IP [ttl=64 id=36594 iplen=28 ]
NSOCK INFO [0.0860s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0860s] nsock_connect_udp(): UDP connection requested to 192.168.1.1
:53 (IOD #1) EID 8
NSOCK INFO [0.0860s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (tim
eout: -1ms) EID 18
NSOCK INFO [0.0860s] nsock_write(): Write request for 44 bytes to IOD #1 EID 27 [
192.168.1.1:53]
NSOCK INFO [0.0860s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS fo
r EID 8 [192.168.1.1:53]
NSOCK INFO [0.0860s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for
EID 27 [192.168.1.1:53]
NSOCK INFO [0.1010s] nsock_trace_handler_callback(): Callback: READ SUCCESS for E
ID 18 [192.168.1.1:53] (121 bytes)
NSOCK INFO [0.1010s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (tim
eout: -1ms) EID 34
NSOCK INFO [0.1010s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1010s] nevent_delete(): nevent_delete on event #34 (type READ)
Nmap scan report for 192.168.1.103
Host is up (0.00023s latency).
MAC Address: 00:0C:29:37:8D:D6 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

Similarly, we saw the same pattern of network traffic in Wireshark also.

ip.addr == 192.168.1.103

No.	Tin	Source	Destination	Protocol	Len	Info
→	…	192.168.1.105	192.168.1.103	ICMP	42	Echo (ping) request id=0x3c98, seq=0/0, ttl=42 (
—	…	192.168.1.103	192.168.1.105	ICMP	60	Echo (ping) reply id=0x3c98, seq=0/0, ttl=64 (

Nmap Stealth Scan Analysis

Let's capture the network packet for default nmap scan also called stealth scan which follows TCP half communication

nmap -p22 192.168.1.103

```
root@kali:~# nmap -p22 192.168.1.103
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-27 16:25 IST
Nmap scan report for 192.168.1.103
Host is up (0.00069s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:37:8D:D6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
root@kali:~#
```

Here you can observe TCP-half communication:

- TCP-SYN packet sent from source 192.168.1.105 to 192.168.1.103 on port 22.
- TCP-SYN, ACK packet received from source 192.168.1.103 to 192.168.1.105.
- TCP-RST packet sent from source 192.168.1.105 to 192.168.1.103.

ip.addr == 192.168.1.103

lo.	Tin	Source	Destination	Protocol	Len	Info
	…	192.168.1.105	192.168.1.103	TCP	58	55598 → 22 [SYN] Seq=0 Win=1024 Len=0
	…	192.168.1.103	192.168.1.105	TCP	60	22 → 55598 [SYN, ACK] Seq=0 Ack=1 Win
	…	192.168.1.105	192.168.1.103	TCP	54	55598 → 22 [RST] Seq=1 Win=0 Len=0

Now let's verify it with parameter -packet-trace and compare the result.

nmap -p22 192.168.1.103 --packet-trace

So you can observe the following information we fetched from nmap, which is similar to TCP-SYN Ping.

- SENT/RECD ARP request and reply respectively.
- Nsock libraries details
- TCP-SYN packet from 192.168.1.105:48236 to 192.168.1.103:22.
- TCP-SYN/ACK packet from 192.168.1.103:22 to 192.168.1.105:48236.

```
root@kali:~# nmap -p22 192.168.1.103 --packet-trace
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-27 16:28 IST
SENT (0.1717s) ARP who-has 192.168.1.103 tell 192.168.1.105
RCVD (0.1722s) ARP reply 192.168.1.103 is-at 00:0C:29:37:8D:D6
NSOCK INFO [0.2290s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.2290s] nsock_connect_udp(): UDP connection requested to 192.168.1.1:53 (IOD #1) EID 8
NSOCK INFO [0.2300s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeout: -1ms) EID 18
NSOCK INFO [0.2300s] nsock_write(): Write request for 44 bytes to IOD #1 EID 27 [192.168.1.1:53]
NSOCK INFO [0.2300s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.1.1:53]
NSOCK INFO [0.2300s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [192.168.1.1:53]
NSOCK INFO [0.2450s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [192.168.1.1:53] (121 bytes)
NSOCK INFO [0.2450s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeout: -1ms) EID 34
NSOCK INFO [0.2450s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.2450s] nevent_delete(): nevent_delete on event #34 (type READ)
SENT (0.2865s) TCP 192.168.1.105:48236 > 192.168.1.103:22 S ttl=38 id=41206 iplen=44  seq=2585637670 win=1024 <mss 1460>
RCVD (0.2870s) TCP 192.168.1.103:22 > 192.168.1.105:48236 SA ttl=64 id=0 iplen=44  seq=2604218680 win=29200 <mss 1460>
Nmap scan report for 192.168.1.103
Host is up (0.00048s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:37:8D:D6 (VMware)
```

Similarly, you can use the nmap command with the "-reason" option to enumerate responses from the host network.

nmap -p22 192.168.1.103 --reason

Here you can observe port 22 is open and when received SYN/ACK packet from the host.

```
root@kali:~# nmap -p22 192.168.1.103 --reason
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-27 16:27 IST
Nmap scan report for 192.168.1.103
Host is up, received arp-response (0.00053s latency).

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
MAC Address: 00:0C:29:37:8D:D6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
root@kali:~#
```

Now let's figure out the behavior of network traffic when –disable-arp-ping activated.

nmap -p22 192.168.1.103 --packet-trace --disable-arp-ping

Here you can notice the following SENT packets from source 192.168.1.105 to destination 192.168.1.103.

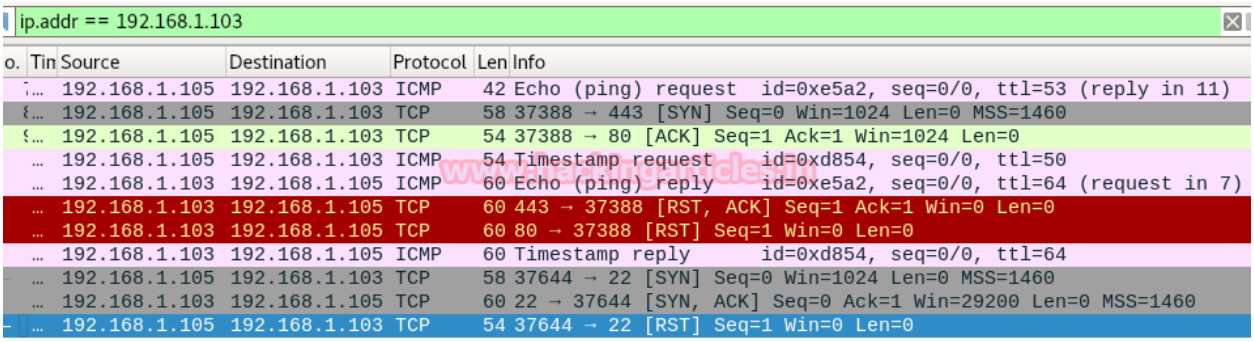
- SENT ICMP echo request
- SENT TCP SYN to port 443
- SENT TCP ACK to port 80
- SENT ICMP timestamp request
- Then RCVD packet ICMP Echo-reply from destination 192.168.1.103
- Then used NSOCK libraries to state actual request and response packets travel between sources to the destination router.
- SENT TCP-SYN request on port 22
- RECV TCP-SYN, ACK reply from port 22.

```
root@kali:~# nmap -p22 192.168.1.103 --packet-trace --disable-arp-ping
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-27 16:33 IST
SENT (0.0744s) ICMP [192.168.1.105 > 192.168.1.103 Echo request (type=8/code=0) id=
58786 seq=0] IP [ttl=53 id=2137 iplen=28 ]
SENT (0.0744s) TCP 192.168.1.105:37388 > 192.168.1.103:443 S ttl=51 id=15499 iplen=
44  seq=3691325058 win=1024 <mss 1460>
SENT (0.0745s) TCP 192.168.1.105:37388 > 192.168.1.103:80 A ttl=51 id=61797 iplen=4
0  seq=0 win=1024
SENT (0.0746s) ICMP [192.168.1.105 > 192.168.1.103 Timestamp request (type=13/code=
0) id=55380 seq=0 orig=0 recv=0 trans=0] IP [ttl=50 id=24463 iplen=40 ]
RCVD (0.0746s) ICMP [192.168.1.103 > 192.168.1.105 Echo reply (type=0/code=0) id=58
786 seq=0] IP [ttl=64 id=33588 iplen=28 ]
NSOCK INFO [0.1230s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.1230s] nsock_connect_udp(): UDP connection requested to 192.168.1.1:5
3 (IOD #1) EID 8
NSOCK INFO [0.1230s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeo
ut: -1ms) EID 18
NSOCK INFO [0.1230s] nsock_write(): Write request for 44 bytes to IOD #1 EID 27 [19
2.168.1.1:53]
NSOCK INFO [0.1230s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for
EID 8 [192.168.1.1:53]
NSOCK INFO [0.1230s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EI
D 27 [192.168.1.1:53]
NSOCK INFO [0.1370s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID
 18 [192.168.1.1:53] (121 bytes)
NSOCK INFO [0.1370s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeo
ut: -1ms) EID 34
NSOCK INFO [0.1370s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1370s] nevent_delete(): nevent_delete on event #34 (type READ)
SENT (0.1770s) TCP 192.168.1.105:37644 > 192.168.1.103:22 S ttl=45 id=45820 iplen=4
4  seq=259118263 win=1024 <mss 1460>
RCVD (0.1774s) TCP 192.168.1.103:22 > 192.168.1.105:37644 SA ttl=64 id=0 iplen=44
seq=3066528596 win=29200 <mss 1460>
Nmap scan report for 192.168.1.103
Host is up (0.00030s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:37:8D:D6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

On the other hand, we saw the same pattern of network traffic in Wireshark too.



Nmap TCP Scan Analysis

From our basic network communication knowledge, we know that a TCP scan performs a three-way-handshake. An nmap TCP scan is done here:

nmap -sT -p22 192.168.1.103 --packet-trace

So you can observe the following information we fetched from nmap which is similar to TCP-SYN Ping.

SENT/RECD ARP request and reply respectively.

Nsock libraries details

Connecting TCP Localhost from destination host 192.168.1.103:22 is in progress.

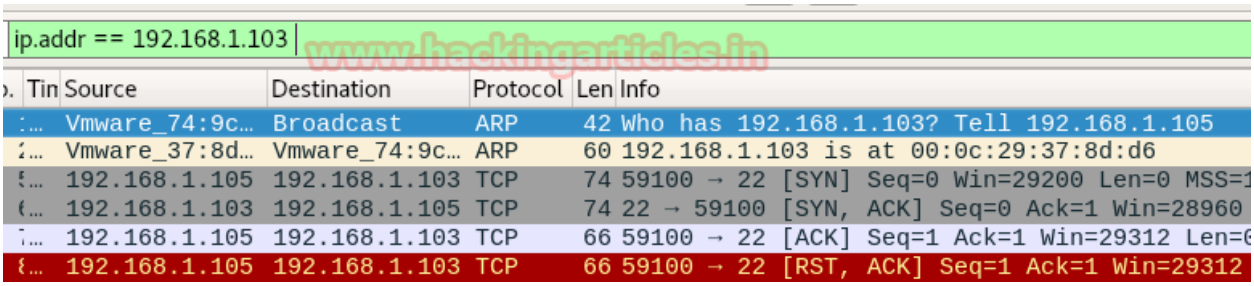
Connected TCP Localhost from destination host 192.168.1.103:22 successfully.

```
root@kali:~# nmap -sT -p22 192.168.1.103 --packet-trace
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-27 19:30 IST
SENT (0.0661s) ARP who-has 192.168.1.103 tell 192.168.1.105
RCVD (0.0663s) ARP reply 192.168.1.103 is-at 00:0C:29:37:8D:D6
NSOCK INFO [0.1140s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.1140s] nsock_connect_udp(): UDP connection requested to 192.168.1.1
:53 (IOD #1) EID 8
NSOCK INFO [0.1140s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (tim
eout: -1ms) EID 18
NSOCK INFO [0.1140s] nsock_write(): Write request for 44 bytes to IOD #1 EID 27 [
192.168.1.1:53]
NSOCK INFO [0.1140s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS fo
r EID 8 [192.168.1.1:53]
NSOCK INFO [0.1140s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for
EID 27 [192.168.1.1:53]
NSOCK INFO [0.1290s] nsock_trace_handler_callback(): Callback: READ SUCCESS for E
ID 18 [192.168.1.1:53] (121 bytes)
NSOCK INFO [0.1290s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (tim
eout: -1ms) EID 34
NSOCK INFO [0.1290s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1290s] nevent_delete(): nevent_delete on event #34 (type READ)
CONN (0.1300s) TCP localhost > 192.168.1.103:22 => Operation now in progress
CONN (0.1306s) TCP localhost > 192.168.1.103:22 => Connected
Nmap scan report for 192.168.1.103
Host is up (0.00032s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:37:8D:D6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

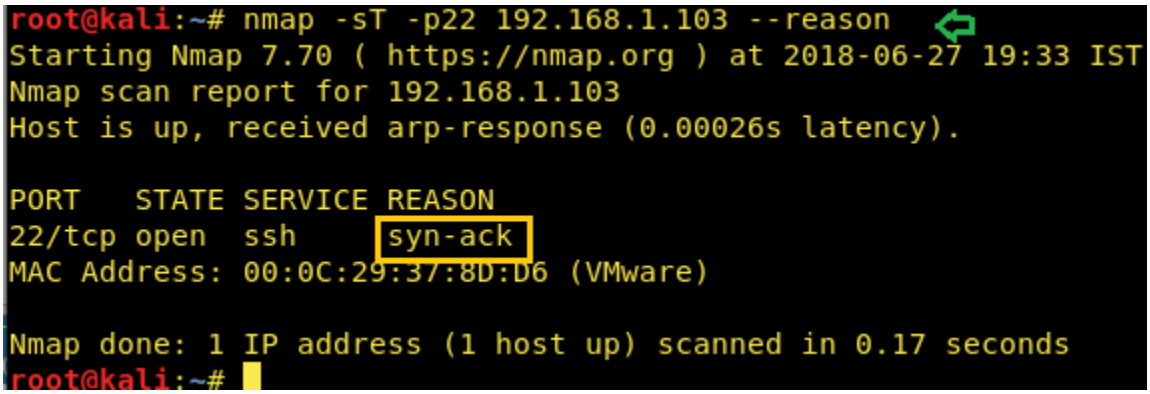
Similarly, we saw the same pattern of network traffic in Wireshark too.



Similarly, you can use the nmap command with the "-reason" option to enumerate responses from the host network.

nmap -sT -p22 192.168.1.103 --reason

Here you can observe port 22 is open and when received SYN/ACK packet from the host.



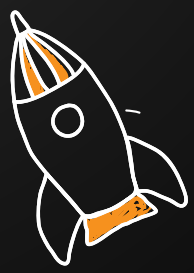
iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

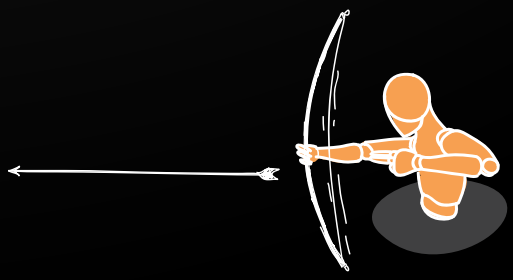
- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials



ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT



- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux