PENETRATION TESTING

NETWORK SCANNING

NETWORK SCANNING

The information gathering phase is over and it allowed us to collect, for instance, a list of IP addresses.

Now it's time to scan each of these IP addresses. What exactly do I mean with "scanning"?

RELEVANT CONCEPT

Each of these IP addresses will expose certain services/ports to the outside world.

RELEVANT CONCEPT

We need to scan them to identify the port corresponding to a certain active service.

NETWORK SCANNING

For example, a Web server will most likely have ports such as 80 or 443 listening, so as to accept requests based on the HTTP, HTTPS protocol.

There are several scanning techniques we can choose. Some of them are silent, others not that much.

Honeypots

NETWORK SCANNING

To see the network scanning techniques in action, we need to expose services on a specific machine in our PenTest laboratory

Another way is to use a "honeypot", i.e., an intentionally vulnerable machine used to attract the attackers and log their activities

When scanning a system always think it might be a honeypot

RELEVANT CONCEPT

Honeypots are deliberately vulnerable machines, which are sometimes used to deceive a potential attacker.

ARPING AND LEVEL 2 NETWORK SCAN

NETWORK SCANNING

The first thing we should mention is that the network can be scanned both at the data link layer and at the network layer of the ISO/OSI model.

NETWORK SCANNING

We start from the one at the data link layer using ARPING

RELEVANT CONCEPT

Scanning at the data link layer (level 2) makes sense only if carried out within a local area network (LAN). In local networks, we will mostly be dealing with MAC addresses and the ARP protocol.

NETWORK SCANNING

Open a terminal on your attacker’s client (e.g., your PC)

Run arping against the OPNsense firewall, e.g., with

```
arping 192.168.122.200 -c 4 -I virbr0
```

where -c 4 limits to 4 requests and -I identifies the interface to be used

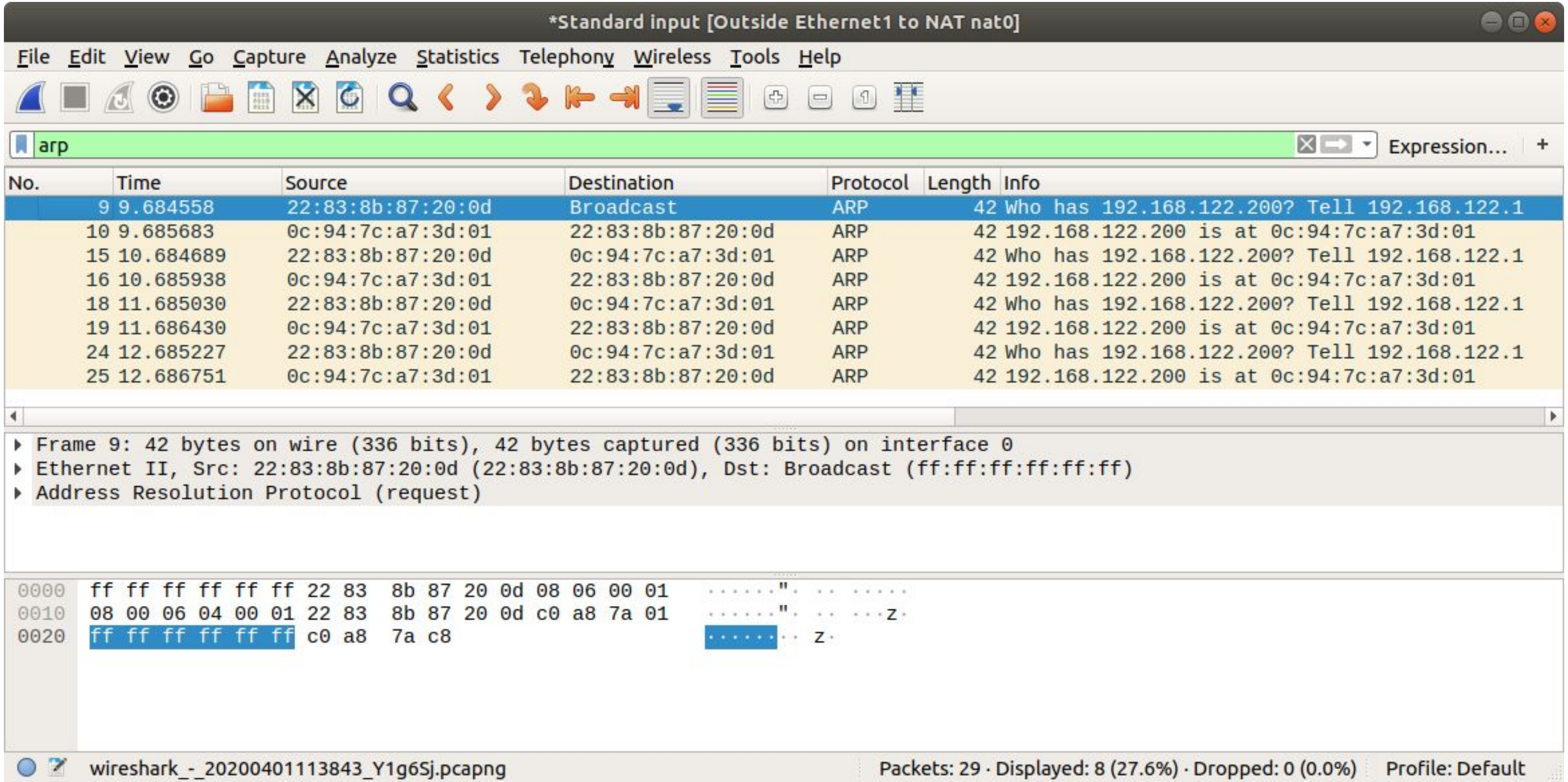
NETWORK SCANNING

```
gabriele@gabriele-XPS-13-9370: ~
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
 gabriele@gabriele-XPS-13-9370  ~  arping 192.168.122.200 -c 4 -I virbr0
ARPING 192.168.122.200 from 192.168.122.1 virbr0
Unicast reply from 192.168.122.200 [0C:94:7C:A7:3D:01]  1.949ms
Unicast reply from 192.168.122.200 [0C:94:7C:A7:3D:01]  1.523ms
Unicast reply from 192.168.122.200 [0C:94:7C:A7:3D:01]  2.233ms
Unicast reply from 192.168.122.200 [0C:94:7C:A7:3D:01]  1.940ms
Sent 4 probes (1 broadcast(s))
Received 4 response(s)
 gabriele@gabriele-XPS-13-9370  ~ 
```

NETWORK SCANNING

We can capture the traffic and filter the ARP protocol with Wireshark

NETWORK SCANNING



NMAP AND LEVEL 3 NETWORK SCAN

RELEVANT CONCEPT

Nmap is the most widespread as well as the most reliable and versatile network scanning tool. It allows us to perform multiple types of scans, from level 3 onwards.

NETWORK SCANNING

Nmap also contains a whole series of additional features, such as vulnerability scanners and modules for enumerating a system.

In this lesson we will cover a level 3 scan using Nmap. However, Nmap covers several distinct scanning phases.

NETWORK SCANNING

1. Name resolution.
2. Nmap Scripting Engine (NSE) script pre-scan phase.
3. Host discovery/ping scanning. **<= We are now at this stage**
4. Target enumeration
5. DNS reverse resolution.
6. Port or Protocol scan.
7. Service version detection.
8. OS fingerprinting.
9. Traceroute.
10. NSE portrule and hostrule script scanning phase.
11. NSE post-scan phase.

NETWORK SCANNING

For now, let's focus on the host discovery phase. We will have to instruct Nmap not to perform any types of port scan, and to merely check which hosts are active on the network (host enumeration).

RELEVANT CONCEPT

This is a level 2 scan based on the ARP protocol and the MAC address.

Level 3 scans rely on ICMP protocol.

"-sn" is the option you should use to instruct Nmap.

NETWORK SCANNING

```
gabriele@gabriele-XPS-13-9370: ~
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
gabriele@gabriele-XPS-13-9370  ~  nmap -sn 192.168.122.1-255

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-01 12:37 CEST
Nmap scan report for gabriele-XPS-13-9370 (192.168.122.1)
Host is up (0.00054s latency).
Nmap scan report for 192.168.122.123
Host is up (0.0057s latency).
Nmap scan report for 192.168.122.200
Host is up (0.0021s latency).
Nmap done: 255 IP addresses (3 hosts up) scanned in 9.36 seconds
gabriele@gabriele-XPS-13-9370  ~
```

NETWORK SCANNING

192.168.122.1-255 is the range of IP addresses we want to test. We could be dealing with a single address or a subnet.

We can always keep the situation under control with Wireshark and check what happens.

In general, -sn makes a ping sweep using ICMP (+ some other protocols for specific services)

RELEVANT CONCEPT

Level 2 scan is often not very interesting (only in sub-networks)

Outside the LAN, we only use IP addresses and therefore the network scan is set at a higher level, i.e. the network layer "layer 3 scan".

USEFUL FINDINGS FOR LEVEL 3 NETWORK SCANS

NETWORK SCANNING

- It would be better to use the IP address and not the hostname so as not to have to perform a DNS query and possibly alter the results obtained. We obviously need to set some limits.

NETWORK SCANNING

- When dealing with a Web server that hosts multiple websites, it makes sense to use the hostname and DNS resolution.
- With large networks, it might take longer to complete a scan. For this reason, it is advisable to use a small network sample or dwell only on a small range of doors.
- Nmap also allows for non invasive DNS-based scan using -sL

TCP AND UDP PROTOCOL

NETWORK SCANNING

We have so far mentioned layer 2 (ARP discovery) and layer 3 (IP) scan of the ISO/OSI model. We will now examine the layer 4: transport layer.

RELEVANT CONCEPT

The transport layer has mainly to do with 2 protocols: TCP and UDP.

NETWORK SCANNING

The main difference between these two protocols is that TCP is a connection-oriented protocol, while UDP is connectionless.

Basically, we use TCP when we have to establish a connection between the two parts.

NETWORK SCANNING

They both should want to take part in the connection, otherwise there will be no exchange of information.

From this, we can easily deduce that TCP is a reliable protocol that, besides rare and manageable exceptions, represents the general structure of every connection.

NETWORK SCANNING

On the contrary, with UDP we have no certainty. On the other hand, UDP is a very fast protocol, while TCP is less efficient due to all the additional checks it has to perform to make the connection reliable.

NETWORK SCANNING

Let's look at which fields make up a TCP and a UDP packet.

TCP Segment Header Format

Bit #	0 7	8 15	16 23	24 31
0	Source Port		Destination Port	
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Res	Flags	Window Size
128	Header and Data Checksum		Urgent Pointer	
160...	Options			

UDP Datagram Header Format

Bit #	0 7	8 15	16 23	24 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	

TCP CONTROL FLAG

NETWORK SCANNING

As seen in the previous slides, the TCP protocol performs a connection check.

To do this, it uses a series of additional information within the network packet, and we are interested in the so-called "TCP flags". There are six of them:

NETWORK SCANNING

- SYN (is 1 when the initial synchronization takes place).
- ACK (is 1 when the Acknowledgment field is valid).
- RST (is 1 when the connection must be reset).
- FIN (is 1 when the connection terminates).
- PSH (is 1 when data must be immediately pushed to application layer).
- URG (is 1 when the Urgent Pointer field is set).

RELEVANT CONCEPT

SYN and ACK are the most important TPC flags, because they take part in the "Three-way handshake". This procedure allows the TCP protocol to establish a communication.

THE THREE-WAY HANDSHAKE

NETWORK SCANNING

This connection creation process is based exclusively on the SYN and ACK flags.

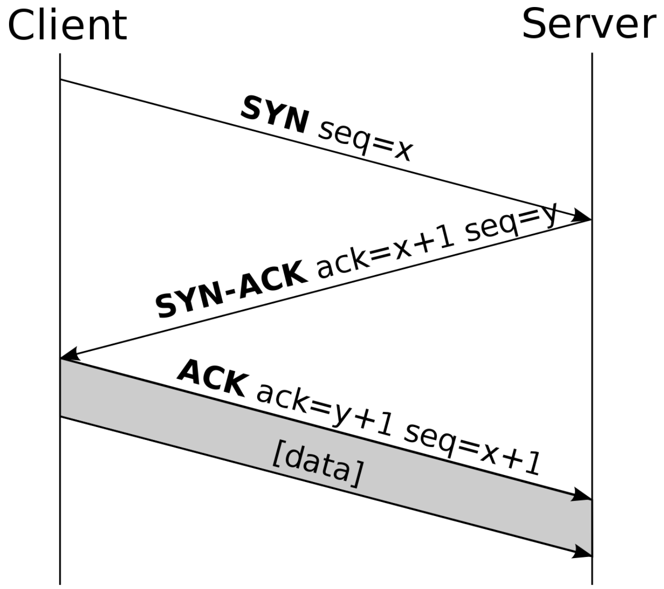
Let’s suppose we have two machines:

- A Client that wants to establish the connection.
- A Server that is waiting for the connection to be established.

NETWORK SCANNING

The exchange takes place as follows:

- Client sets the SYN flag of the packet and sends it to Server.
- Once Server receives it, it sets the SYN and ACK flags of the packet for Client.
- When Client receives the SYN-ACK, it sends the ACK flag to Server.
- If everything went well, the connection is established correctly.



RELEVANT CONCEPT

The three-way handshake is an exchange of packets between two entities that use TCP flags (SYN and ACK) to organize their communication.

NETWORK SCANNING

We can find all the information we need on Wireshark, as you can see from the screenshot here below:

tcp

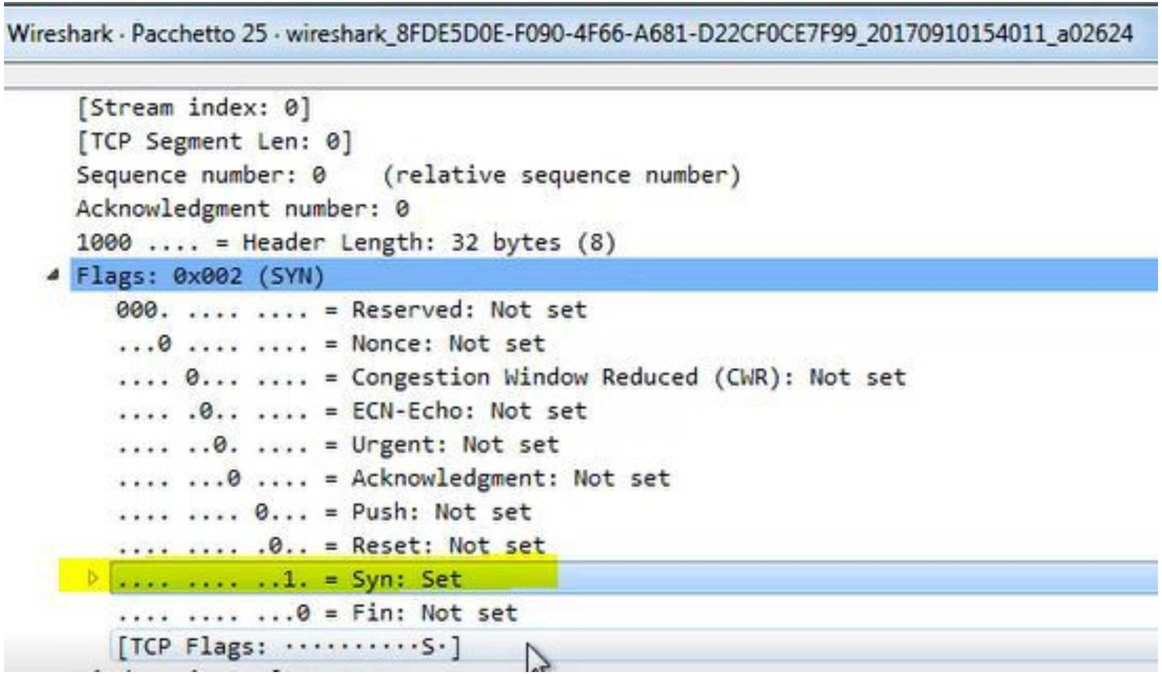
No.	Time	Source	Destination	Protocol	Length	Info
25	77.078202	192.168.1.104	23.12.96.62	TCP	66	1818 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
26	77.365172	23.12.96.62	192.168.1.104	TCP	66	80 → 1818 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM=1 WS=32
27	77.365263	192.168.1.104	23.12.96.62	TCP	54	1818 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0

NETWORK SCANNING

The packet number 25 has the SYN flag active, the 26 one is a copy with SYN and ACK, the 27 one with ACK starts the communication.

Here is a screenshot of the first packet, where the SYN flag is set to 1. This means that it is active:

NETWORK SCANNING



LEVEL 4 NETWORK SCAN - CONNECT SCAN

NETWORK SCANNING

Now we will learn how to perform a level 4 scan: the CONNECT SCAN. This type of scan establishes the TCP connection.

In other words, it completes the three-way handshake, making the scan very noisy and easily identifiable.

NETWORK SCANNING

We scan an host using Nmap to establish a TCP connection. For this experiment we need:

- An host to scan (must have a TCP-based service)
- Wireshark to monitor the traffic, filtering by TCP.
- Nmap with the following command: **`nmap -sT -v -p X Y`**

where X is a port number and Y is the IP address of the target host

NETWORK SCANNING

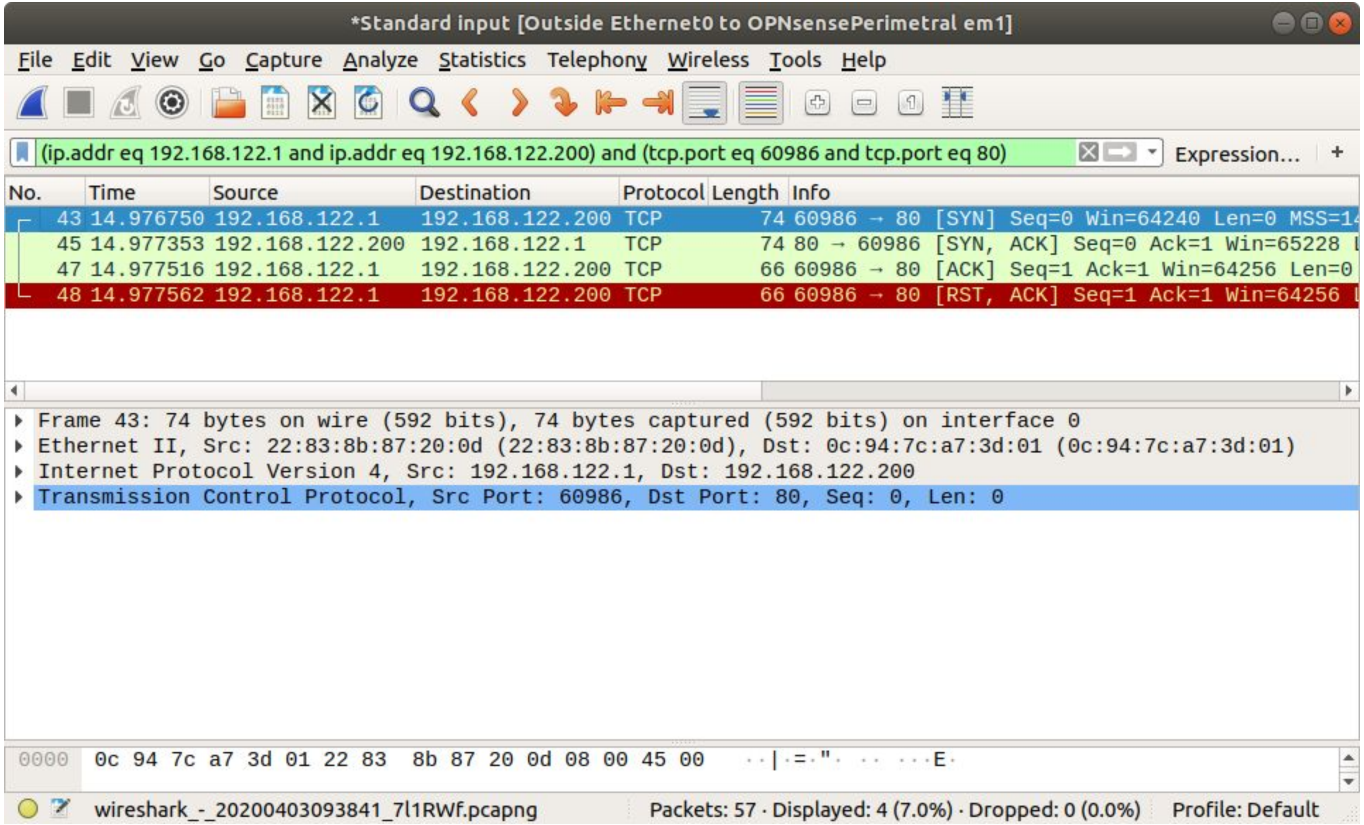
```
gabriele@gabriele-XPS-13-9370: ~
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
gabriele@gabriele-XPS-13-9370  ~  nmap -sT -v -p 80 192.168.122.200

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-03 09:47 CEST
Initiating Ping Scan at 09:47
Scanning 192.168.122.200 [2 ports]
Completed Ping Scan at 09:47, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:47
Completed Parallel DNS resolution of 1 host. at 09:47, 0.00s elapsed
Initiating Connect Scan at 09:47
Scanning 192.168.122.200 [1 port]
Discovered open port 80/tcp on 192.168.122.200
Completed Connect Scan at 09:47, 0.00s elapsed (1 total ports)
Nmap scan report for 192.168.122.200
Host is up (0.00092s latency).

PORT   STATE SERVICE
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
gabriele@gabriele-XPS-13-9370  ~
```

NETWORK SCANNING



LEVEL 4 NETWORK SCAN - SYN SCAN

NETWORK SCANNING

Now let's examine the SYN type scan, which, unlike the CONNECT one, does not complete the three-way handshake completely. We could almost say that it is half done.

The exchange takes place as follows:

NETWORK SCANNING

- The attacker sends a packet with the SYN flag set.
- The victim responds with a packet with configured SYN and ACK flags.
- The attacker, at this point, does not complete the handshake but sends a packet with the RST flag. This will force a reset of the connection which is not established.

NETWORK SCANNING

This is a relatively "silent" scan. If there is a system in the target network that tracks the established connections, it will not record this attempt.

This is because no connection has been actually established.

To start a SYN scan use: **`nmap -sS -v -p X Y`**

(Notice: may require root privileges)

NETWORK SCANNING

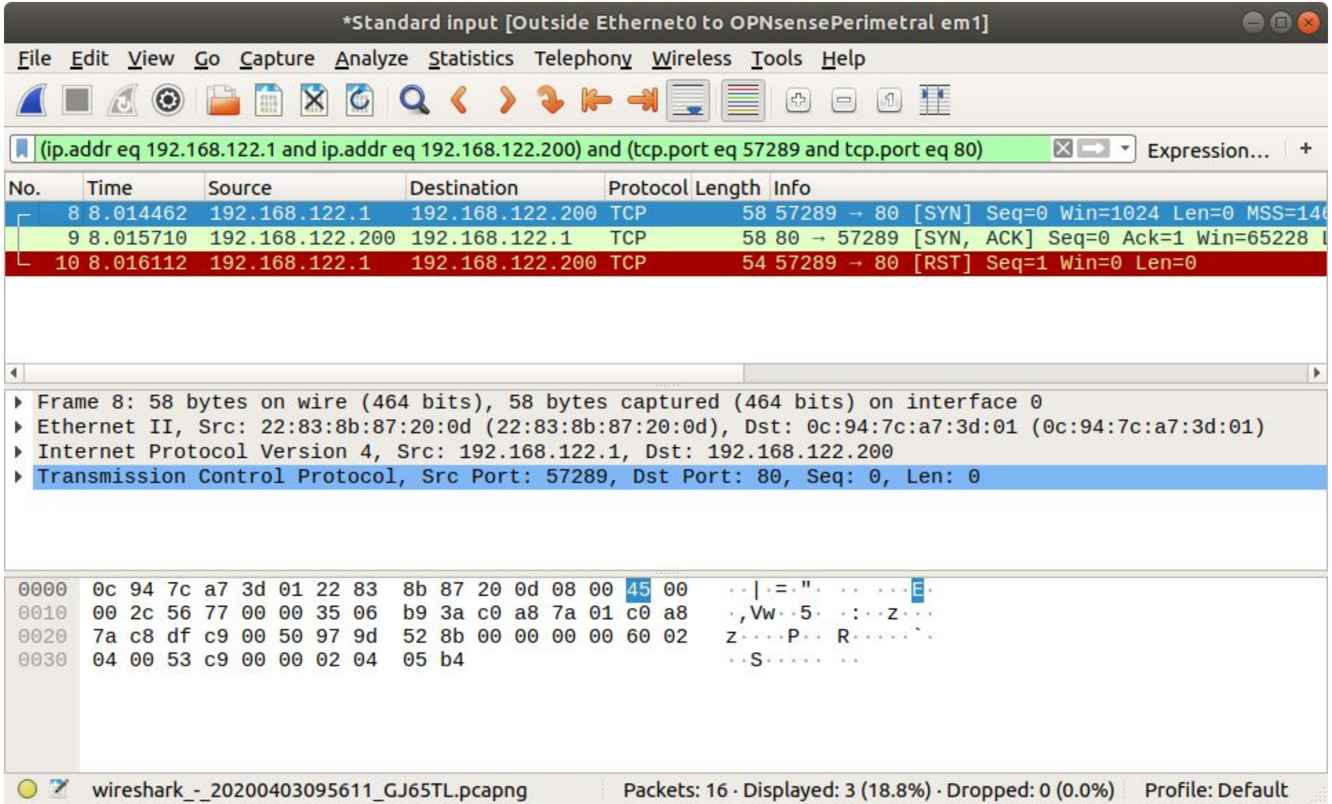
```
gabriele@gabriele-XPS-13-9370: ~
File Modifica Visualizza Cerca Terminale Aiuto
gabriele@gabriele-XPS-13-9370  ~  sudo nmap -sS -v -p 80 192.168.122.200

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-03 09:57 CEST
Initiating ARP Ping Scan at 09:57
Scanning 192.168.122.200 [1 port]
Completed ARP Ping Scan at 09:57, 0.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:57
Completed Parallel DNS resolution of 1 host. at 09:57, 0.00s elapsed
Initiating SYN Stealth Scan at 09:57
Scanning 192.168.122.200 [1 port]
Discovered open port 80/tcp on 192.168.122.200
Completed SYN Stealth Scan at 09:57, 0.22s elapsed (1 total ports)
Nmap scan report for 192.168.122.200
Host is up (0.00055s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 0C:94:7C:A7:3D:01 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
gabriele@gabriele-XPS-13-9370  ~
```

NETWORK SCANNING



NETWORK SCANNING

Although a TCP connection is not established, the attempt can be logged anyway

Also, aborted connections may be more suspicious that successful ones

LEVEL 4 NETWORK SCAN - UDP SCAN

NETWORK SCANNING

The previous scans are related to the TCP protocol which is possibly the most used.

However, even the UDP protocol can provide interesting results, because it is often underestimated and not adequately protected by network administrators.

Also, UDP is used by certain services of interest, e.g., DNS uses UDP for domain queries (and TCP for zone transfer).

RELEVANT CONCEPT

Keep in mind that the UDP protocol is connectionless and therefore behaves differently from TCP.

NETWORK SCANNING

Even if a scan is launched on a certain port and we receive no response, then we can assume that the port is open.

Otherwise, we will receive an ICMP error message which, in short, means that the port is closed or cannot provide a meaningful answer.

NETWORK SCANNING

We scan the DNS server of our OPNsense router-firewall

DNS service usually runs on port 53

Again, we inspect the traffic with Wireshark

We run nmap with: **`nmap -sU -v -p 53 192.168.122.200`**

(Notice: may need root privileges)

NETWORK SCANNING

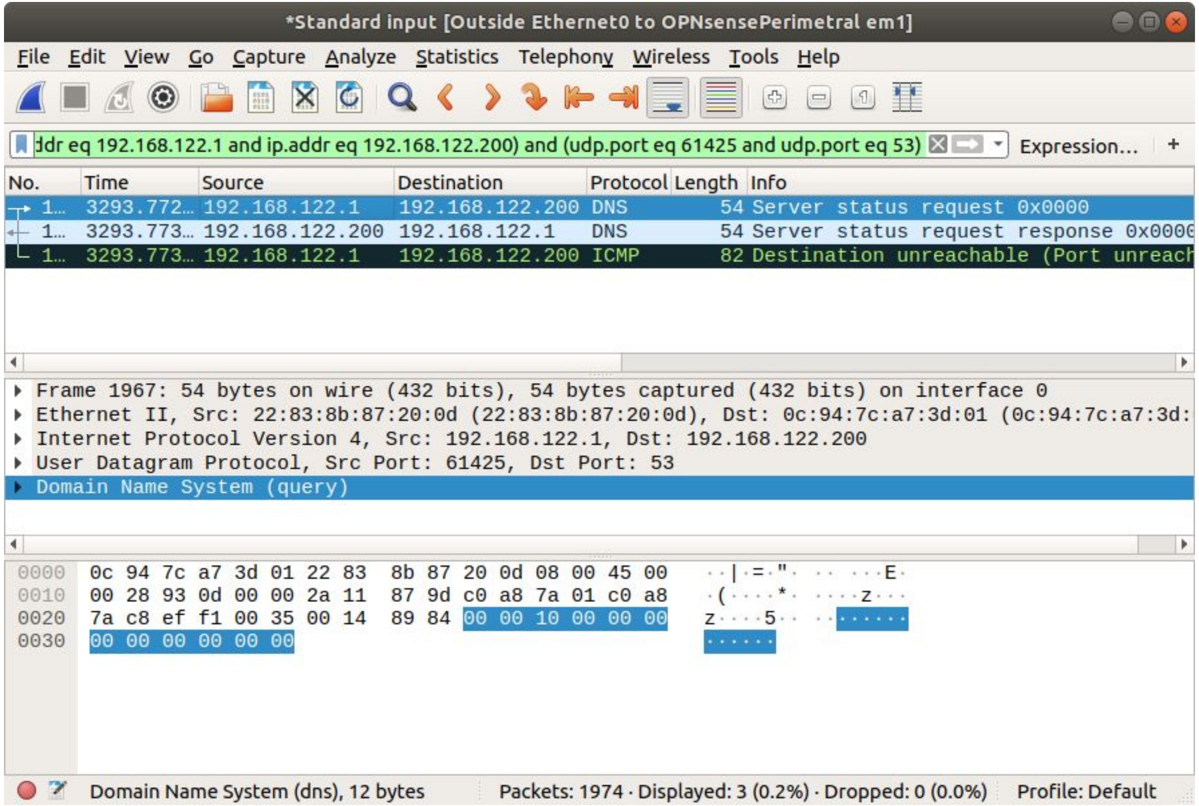
```
gabriele@gabriele-XPS-13-9370: ~
File Modifica Visualizza Cerca Terminale Aiuto
gabriele@gabriele-XPS-13-9370  ~  sudo nmap -sU -v -p 53 192.168.122.200

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-03 10:54 CEST
Initiating ARP Ping Scan at 10:54
Scanning 192.168.122.200 [1 port]
Completed ARP Ping Scan at 10:54, 0.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:54
Completed Parallel DNS resolution of 1 host. at 10:54, 0.00s elapsed
Initiating UDP Scan at 10:54
Scanning 192.168.122.200 [1 port]
Discovered open port 53/udp on 192.168.122.200
Completed UDP Scan at 10:54, 0.23s elapsed (1 total ports)
Nmap scan report for 192.168.122.200
Host is up (0.0016s latency).

PORT   STATE SERVICE
53/udp open  domain
MAC Address: 0C:94:7C:A7:3D:01 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds
           Raw packets sent: 3 (108B) | Rcvd: 3 (108B)
gabriele@gabriele-XPS-13-9370  ~
```

NETWORK SCANNING



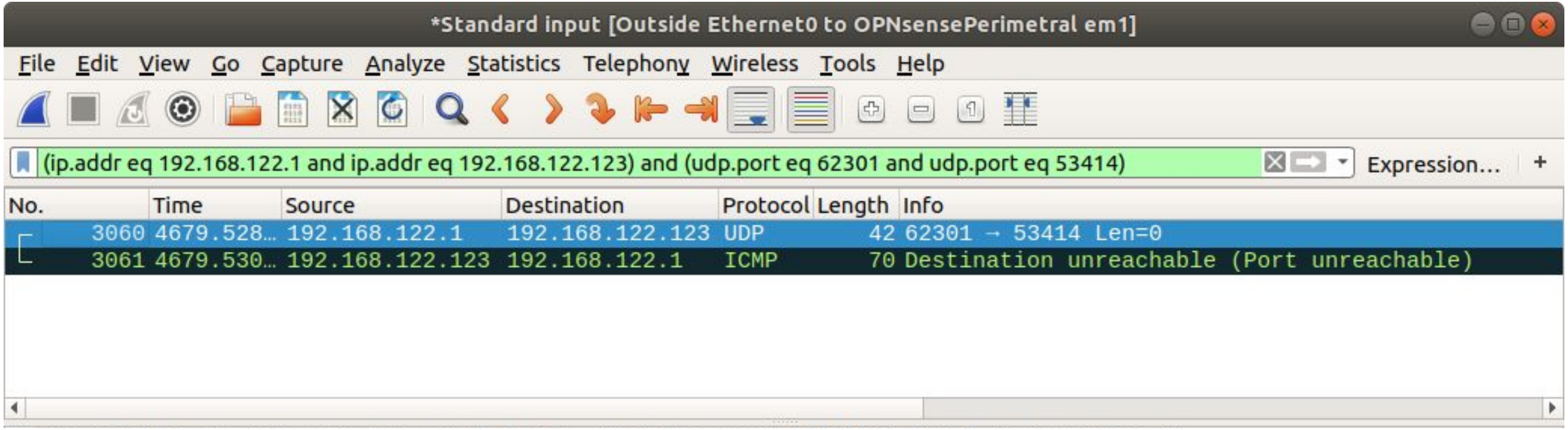
NETWORK SCANNING

The first line shows the UDP packet sent.

Since we received a DNS error message, we know that the scan was successful and that port 53 is actually open.

NETWORK SCANNING

If we try with a random port on some other machine we get a different result



NETWORK SCANNING

As you can see, in this case the ICMP error packet returns immediately, alerting us that the port is unreachable.

The port may be closed or filtered. We actually know that it does not exist.

```
PORT      STATE  SERVICE
53414/udp closed unknown
MAC Address: 0C:94:7C:A7:3D:01 (Unknown)
```

NETWORK SCANNING

Recall that nmap can scan multiple IPs and ports (specified in a range)

nmap -sT -p1-1024 192.168.122.1-255

Tests all the hosts in 192.168.122.* on ports from 1 to 1024