ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Омский государственный университет путей сообщения»
(ОмГУПС (ОмИИТ))

Кафедра «Информационная безопасность»

Сканеры уязвимостей

Отчет по лабораторной работе
по дисциплине «Методы выявления нарушений ИБ и аттестация АС на ЖДТ»

Студент гр. 28 с
_____ Ю.Е. Туник
«___» _____2023г.

Руководитель:
преподаватель кафедры ИБ
_____ Я. С. Беспрозванных
«___» _____2023г.

Омск 2023

Цель работы: освоить навыки работы со сканерами уязвимостей.

Задание:

1. Настройте на виртуальной машине ssh-сервер, ftp-сервер и http-сервер.

2. Прочитайте методичку по сканеру безопасности nmap. Выполните следующие сканирования:

   1) Определение доступности хостов в вашей подсети (выбираете любой из методов по инструкции);

   2) Сканирование портов роутера, собственного ПК, виртуальной машины Linux. Выполните сканирования минимум тремя различными методами сканирования. Сравните полученные результаты.

   3) Выполните сканирование роутера, собственного ПК, виртуальной машины Linux с определением версии ОС целевого узла.

   4) Выполните сканирование роутера, собственного ПК, виртуальной машины Linux с определением версий сетевых сервисов.

3. После этого необходимо перенести pcap файлы из виртуальной машины на свою рабочую ОС и проанализировать их в программе wireshark.

Ход работы

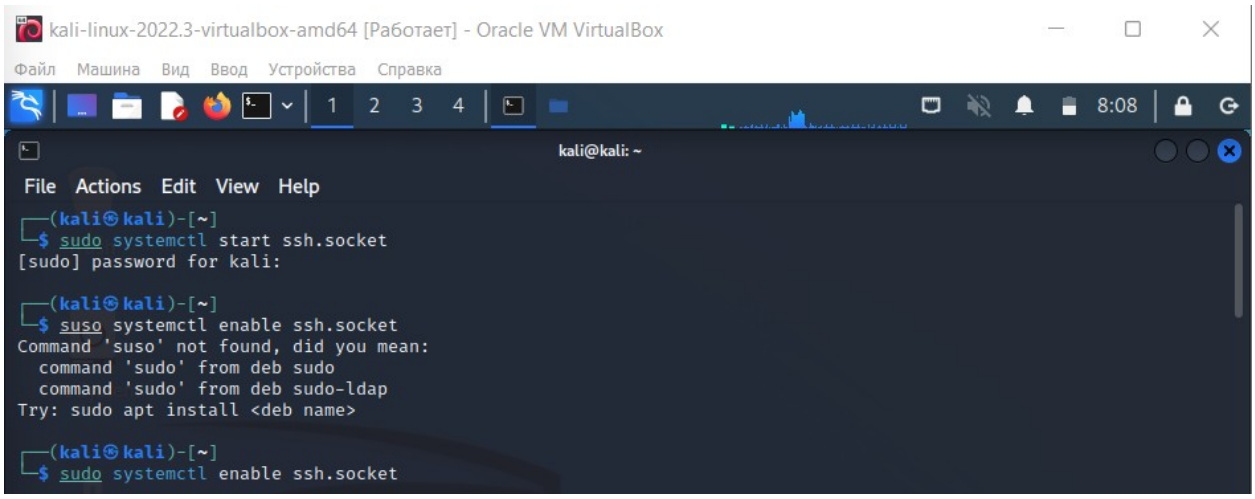
Установили Kali Linux на виртуальную машину, подключили к сети через сетевой мост с хостом и настроили ssh-сервер, ftp-сервер и http-сервер.

IP адрес хоста – 192.168.56.1

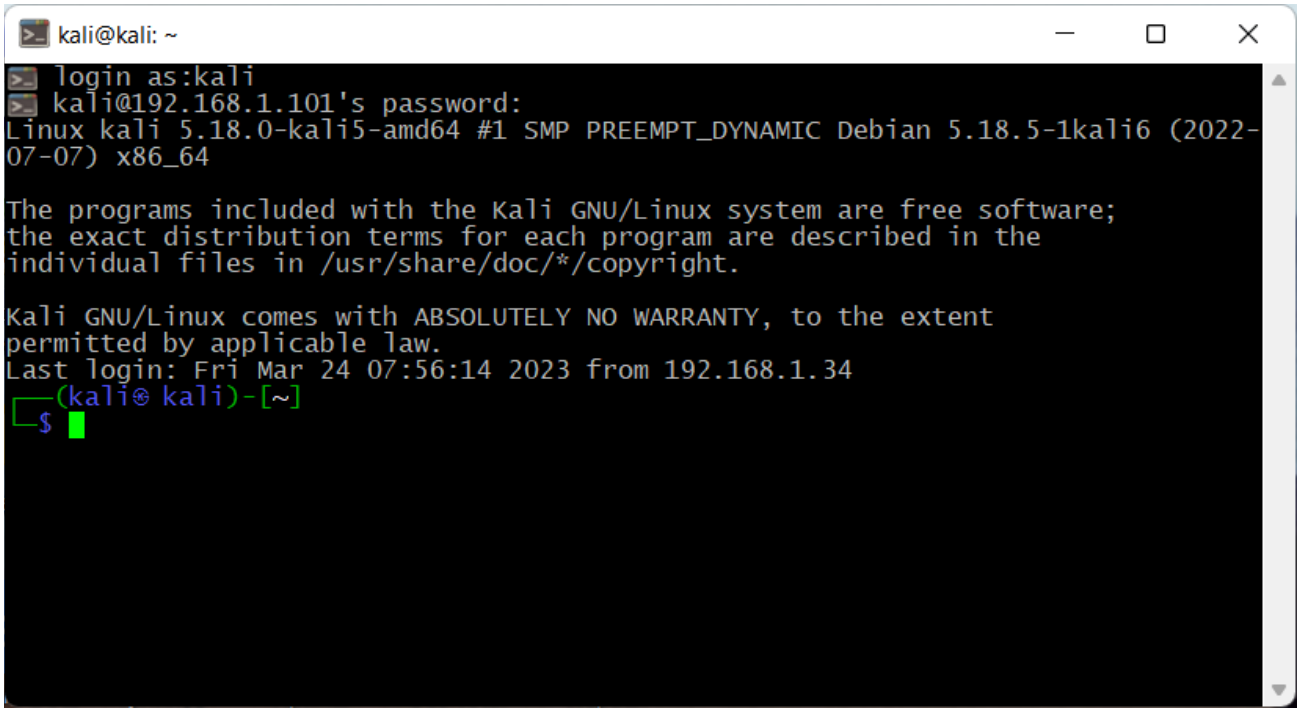
IP адрес Kali Linux – 192.168.1.101

IP адрес роутера – 192.168.1.1

1. Настройка ssh



Проверка подключения по ssh



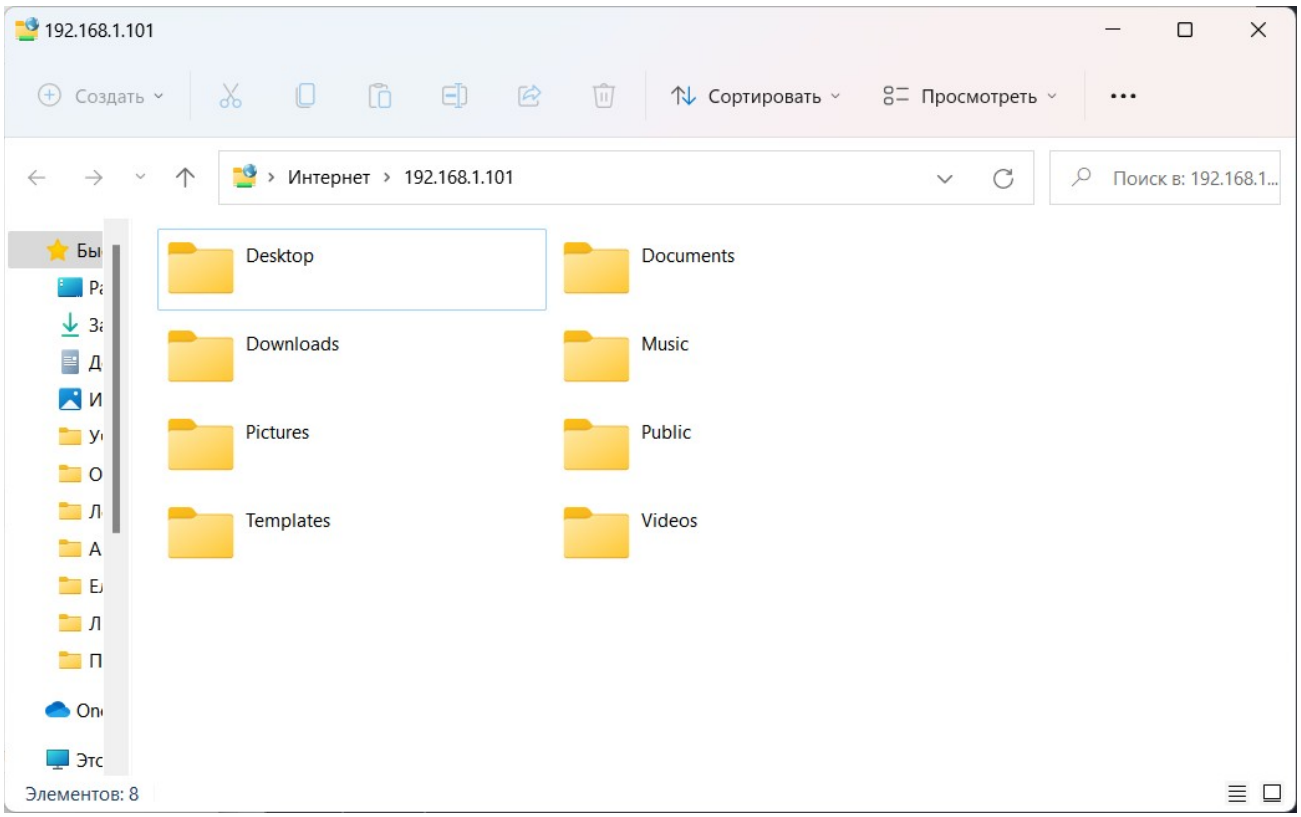
2. Настройка ftp

sudo apt-get update

sudo apt-get install vsftpd

sudo service vsftpd start

Проверка ftp



3. Настройка http

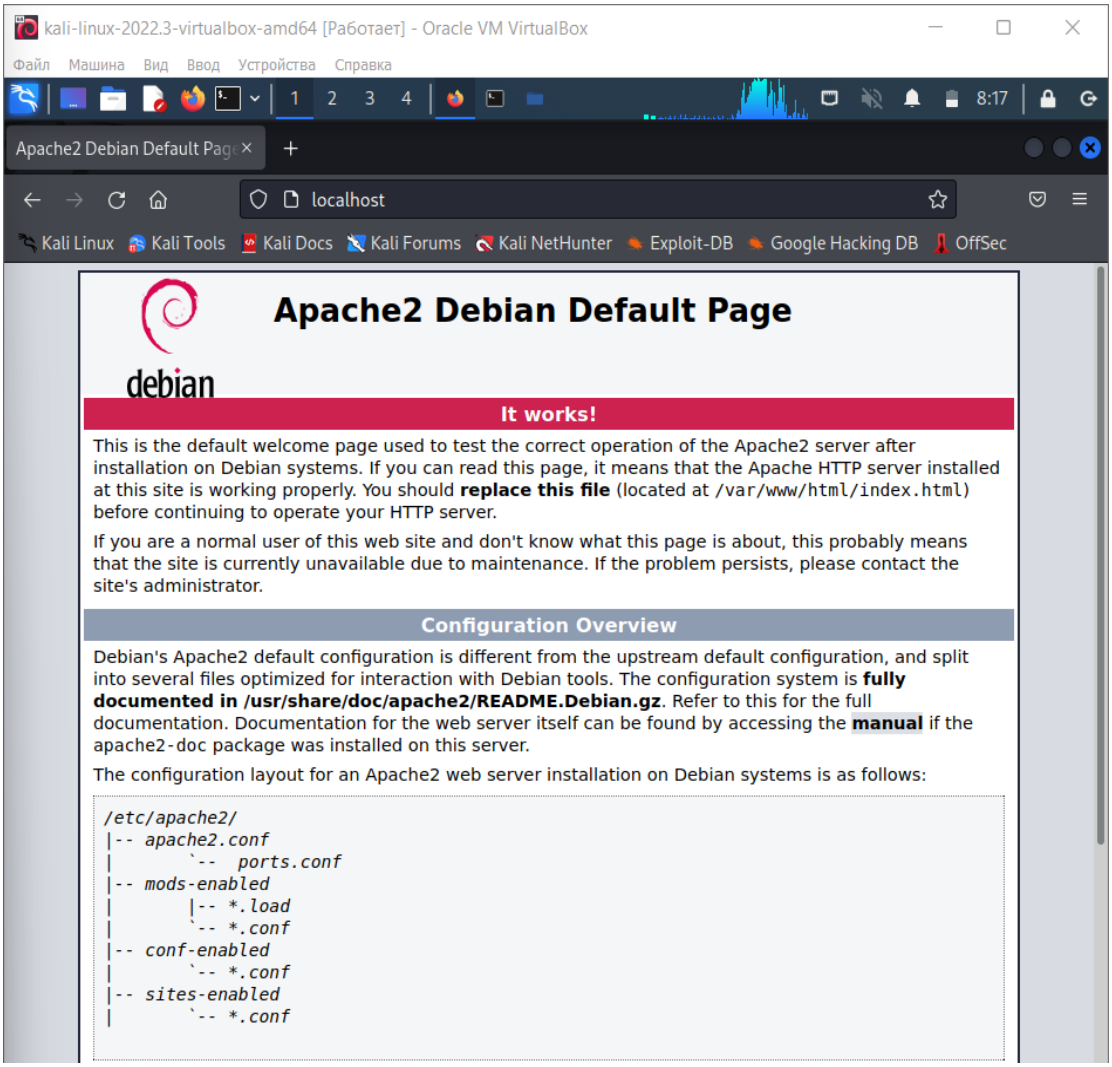
sudo apt-get install apache2

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/sys
temd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start apache2

┌──(kali㉿kali)-[~]
└─$ service apache2 start
Failed to start apache2.service: Access denied
See system logs and 'systemctl status apache2.service' for details.
```

Проверка http


kali-linux-2022.3-virtualbox-amd64 [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Apache2 Debian Default Page
localhost
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Apache2 Debian Default Page
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf

Ход работы

Определение доступности хостов в вашей подсети:

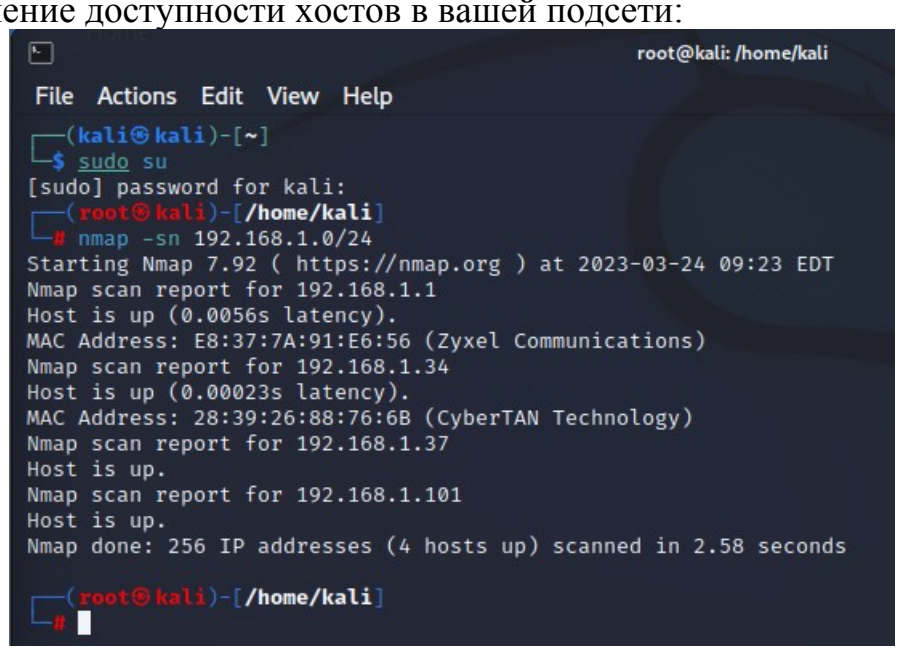


Рисунок 1 – Определение доступности хостов

Сканирование портов роутера, собственного ПК, виртуальной машины Linux:

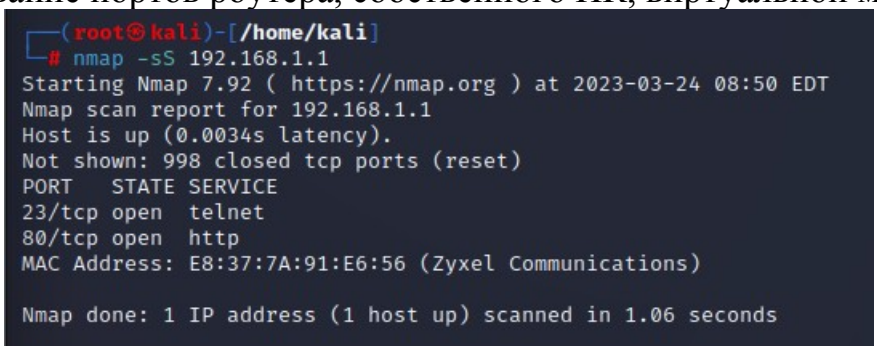


Рисунок 2.1 – Сканирование портов роутера SYN

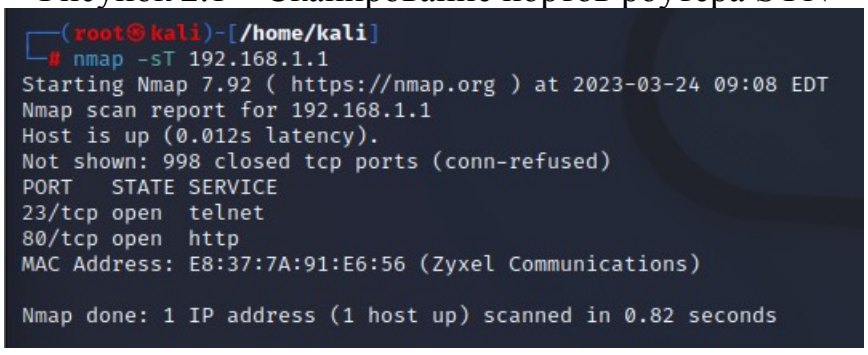


Рисунок 2.2 – Сканирование портов роутера TCP

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-24 09:30 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0028s latency).
Not shown: 954 closed udp ports (port-unreach), 45 open|filtered udp ports (no-response)
PORT   STATE SERVICE
53/udp open  domain
MAC Address: E8:37:7A:91:E6:56 (Zyxel Communications)

Nmap done: 1 IP address (1 host up) scanned in 1030.80 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

Рисунок 2.3 – Сканирование портов роутера UDP

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.56.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-24 09:50 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00035s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
6881/tcp open  bittorrent-tracker
MAC Address: 0A:00:27:00:00:09 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.68 seconds
```

Рисунок 3.1 – Сканирование портов собственного ПК SYN

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.56.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-24 09:53 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00034s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
6881/tcp open  bittorrent-tracker
MAC Address: 0A:00:27:00:00:09 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 19.27 seconds
```

Рисунок 3.2 – Сканирование портов собственного ПК TCP

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.56.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-24 09:54 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.56.1 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)
MAC Address: 0A:00:27:00:00:09 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.40 seconds
```

Рисунок 3.3 – Сканирование портов собственного ПК UDP

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.1.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-24 09:57 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0000040s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
```

Рисунок 4.1 – Сканирование портов виртуальной машины Linux SYN

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.1.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-24 09:59 EDT
Nmap scan report for 192.168.1.101
Host is up (0.000077s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

Рисунок 4.2 – Сканирование портов виртуальной машины Linux TCP

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU 192.168.1.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-24 10:00 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 closed udp ports (port-unreach)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

Рисунок 4.3 – Сканирование портов виртуальной машины Linux UDP

Сканирование роутера, собственного ПК, виртуальной машины Linux с определением версии ОС целевого узла:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-24 10:03 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0029s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
MAC Address: E8:37:7A:91:E6:56 (Zyxel Communications)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.31 - 2.6.35
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 2.49 seconds
```

Рисунок 5 – Сканирование портов роутера с определением версии ОС целевого узла

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.56.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-24 10:05 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00034s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
6881/tcp open  bittorrent-tracker
MAC Address: 0A:00:27:00:00:09 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|firewall
Running (JUST GUESSING): FreeBSD 6.X (98%), Microsoft Windows 10|2008 (91%), Juniper JUNOS 12.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:6.2 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:
microsoft:windows_server_2008 cpe:/o:freebsd:freebsd:6.3 cpe:/o:juniper:junos:12.1
Aggressive OS guesses: FreeBSD 6.2-RELEASE (98%), Microsoft Windows 10 (91%), Microsoft Windows Server 2008 or 200
8 Beta 3 (89%), m0n0wall 1.3b11 - 1.3b15 (FreeBSD 6.3) (88%), Juniper SRX-series firewall (JUNOS 12.1) (88%)
No exact OS matches for host (test conditions non-ideal).
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 12.45 seconds
```

Рисунок 6 – Сканирование портов собственного ПК с определением версии ОС целевого узла

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.1.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-24 10:07 EDT
Nmap scan report for 192.168.1.101
Host is up (0.000046s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.18 seconds
```

Рисунок 7 – Сканирование портов виртуальной машины Linux с определением версии ОС целевого узла

Сканирование роутера, собственного ПК, виртуальной машины Linux с определением версий сетевых сервисов:

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-24 10:10 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0070s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE    VERSION
23/tcp open  telnet     Pirelli VDSL router or ZyXEL Keenetic Omni telnetd
80/tcp open  tcpwrapped
MAC Address: E8:37:7A:91:E6:56 (Zyxel Communications)
Service Info: Device: broadband router

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.37 seconds
```

Рисунок 8 – Сканирование портов роутера с определением версий сетевых сервисов

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.56.1
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-24 10:13 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00026s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE           VERSION
6881/tcp open  bittorrent-tracker?
1 service unrecognized despite returning data. If you know the service/version, please submit the following finger
print at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

Рисунок 9 – Сканирование портов собственного ПК с определением версий сетевых сервисов

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-24 10:18 EDT
Nmap scan report for 192.168.1.101
Host is up (0.0000030s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 9.0p1 Debian 1+b1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.56 ((Debian))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.19 seconds
```

Рисунок 10 – Сканирование портов виртуальной машины Linux с определением версий сетевых сервисов

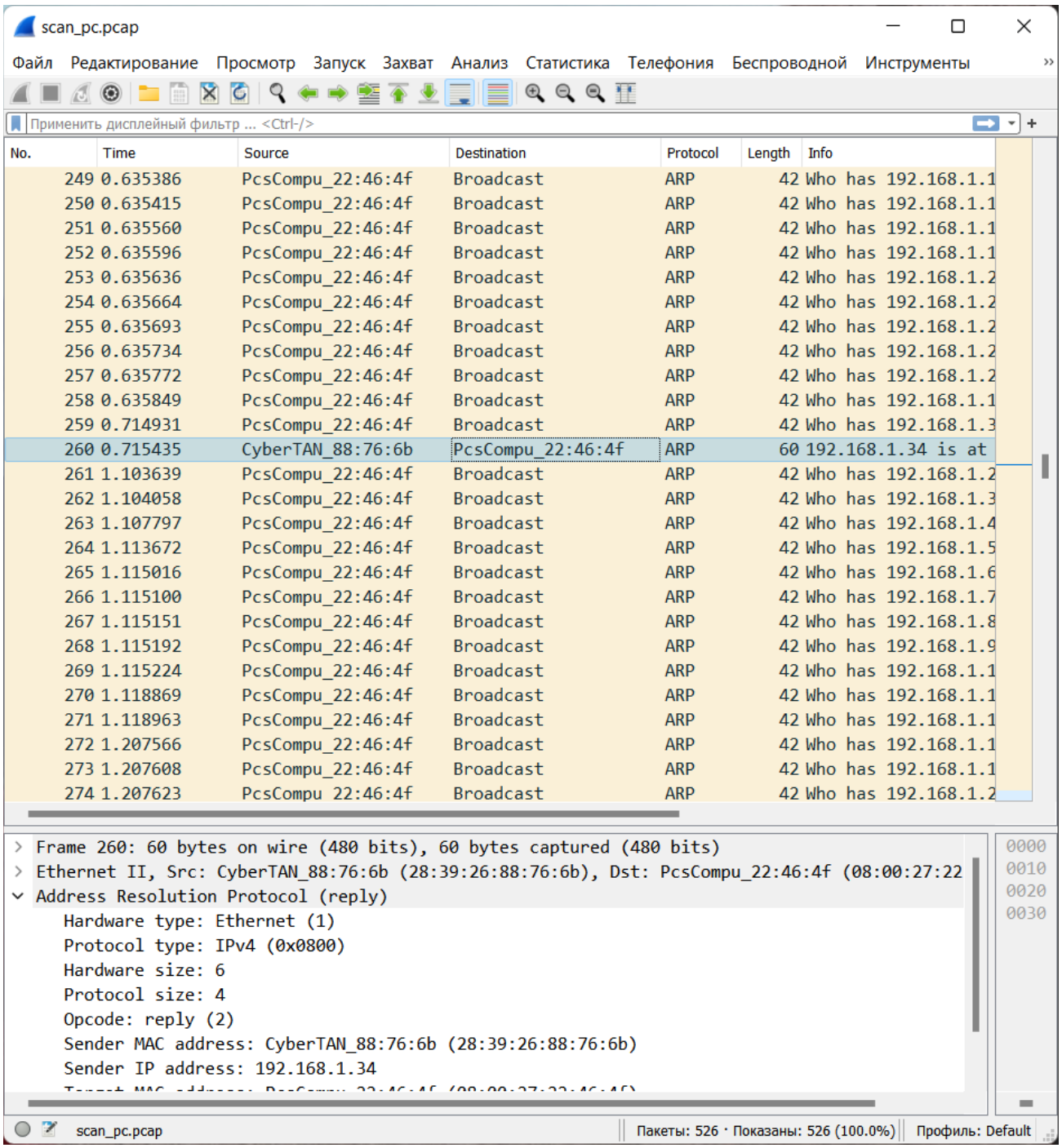


Рисунок 11 – Анализ доступности в Wireshark

Из рисунка 11 видно, что система производила широковещательный запрос на принадлежность к IP из заданного диапазона.

Анализ в Wireshark приведен для каждого из сканирования, но к одному устройству, для других устройств принцип работы Nmap будет аналогичен нижеприведенным.

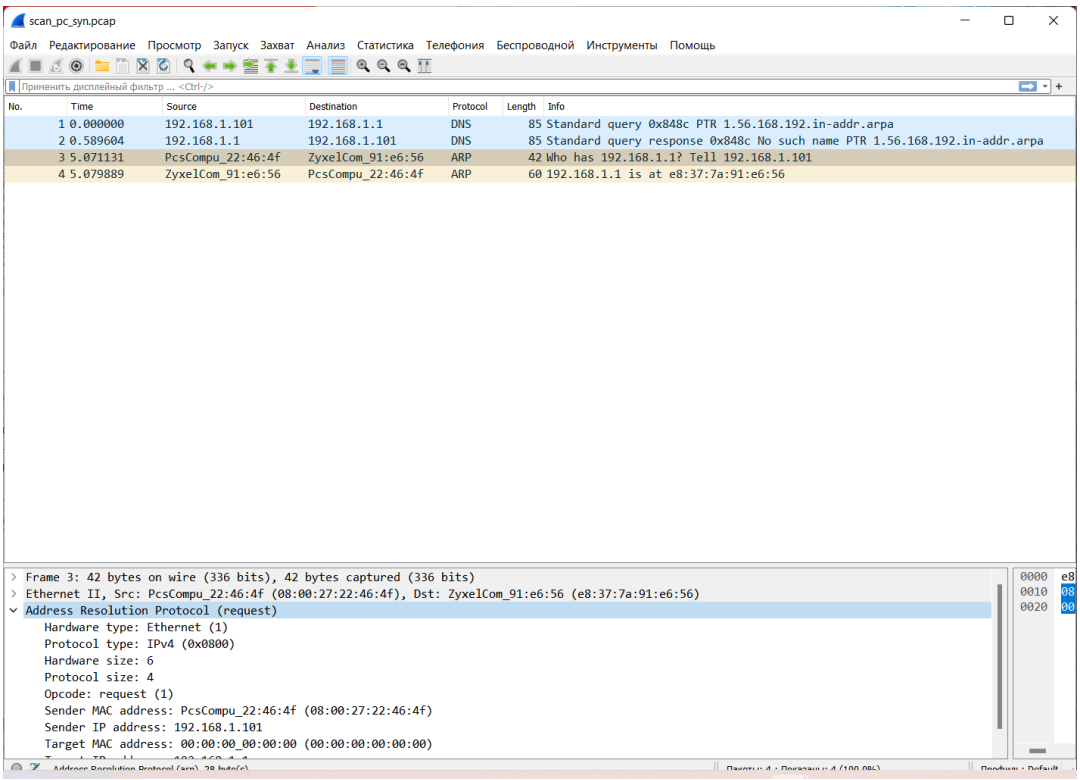


Рисунок 12 – Анализ сканирования портов собственного ПК SYN в Wireshark

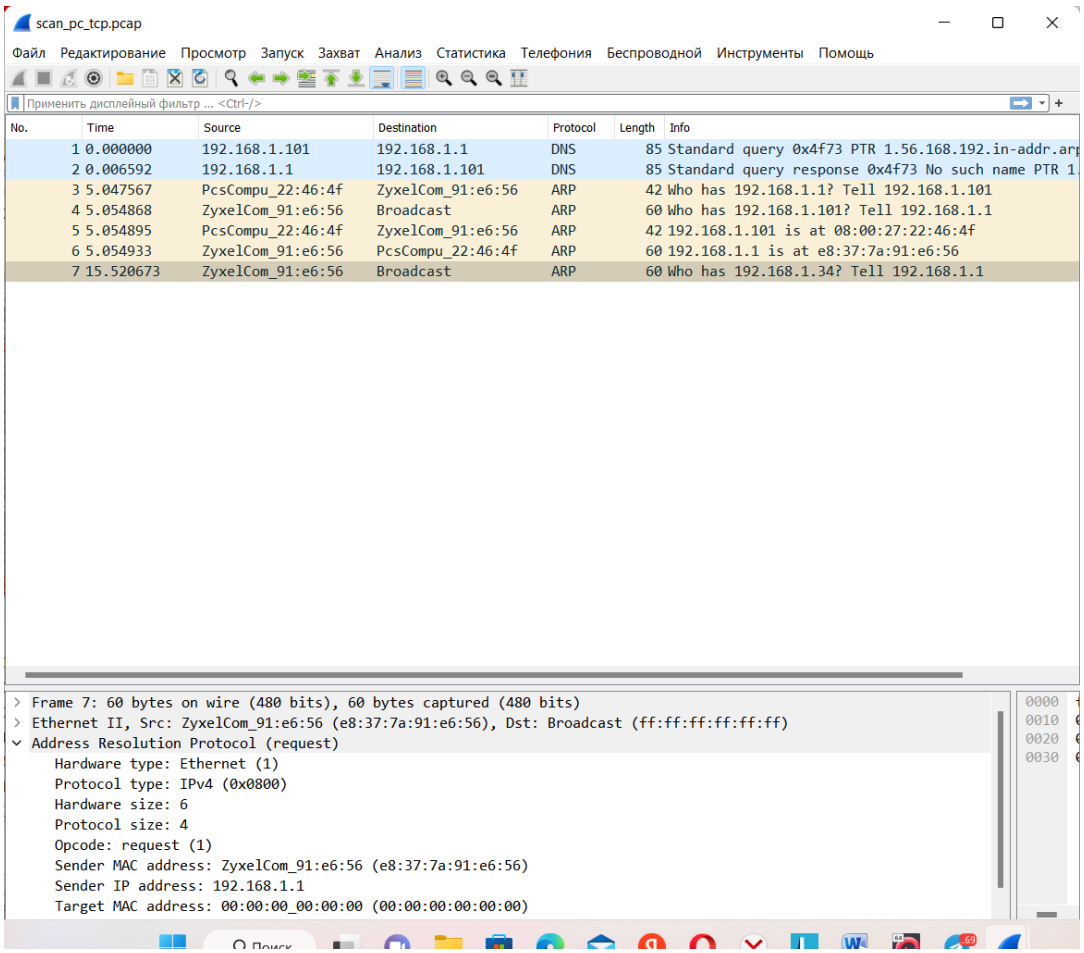


Рисунок 13 – Анализ сканирования портов собственного ПК TCP в Wireshark

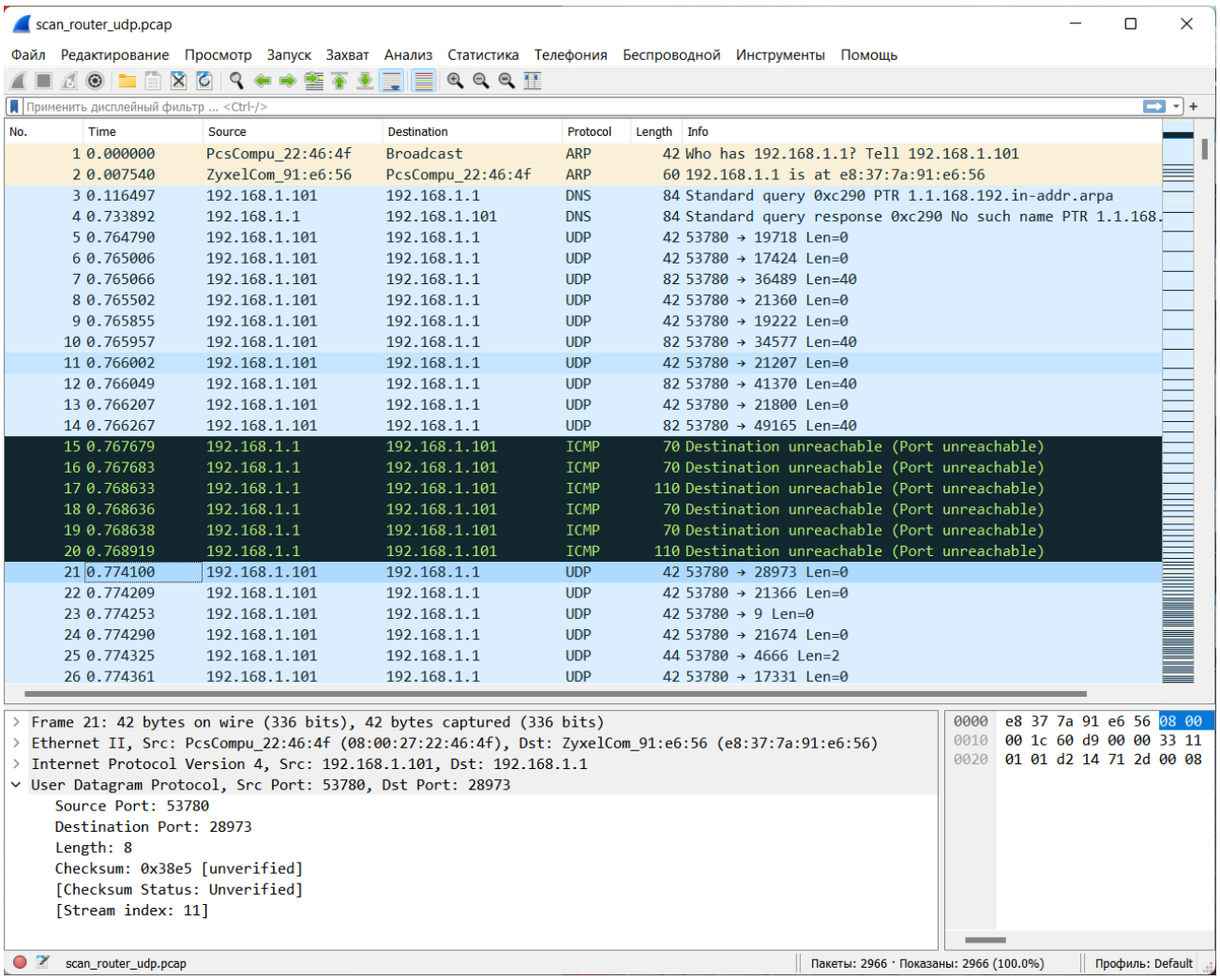


Рисунок 14 – Анализ сканирования портов роутера UDP в Wireshark

UDP сканирование работает путем посылки пустого (без данных) UDP заголовка на каждый целевой порт. Если в ответ приходит ICMP ошибка о недостижимости порта, значит, порт закрыт. Другие ICMP ошибки недостижимости указывают на то, что порт фильтруется. Иногда, служба будет отвечать UDP пакетом, указывая на то, что порт открыт. Если после нескольких попыток не было получено никакого ответа, то порт классифицируется как открыт/фильтруется. Это означает, что порт может быть открыт, или, возможно, пакетный фильтр блокирует его.

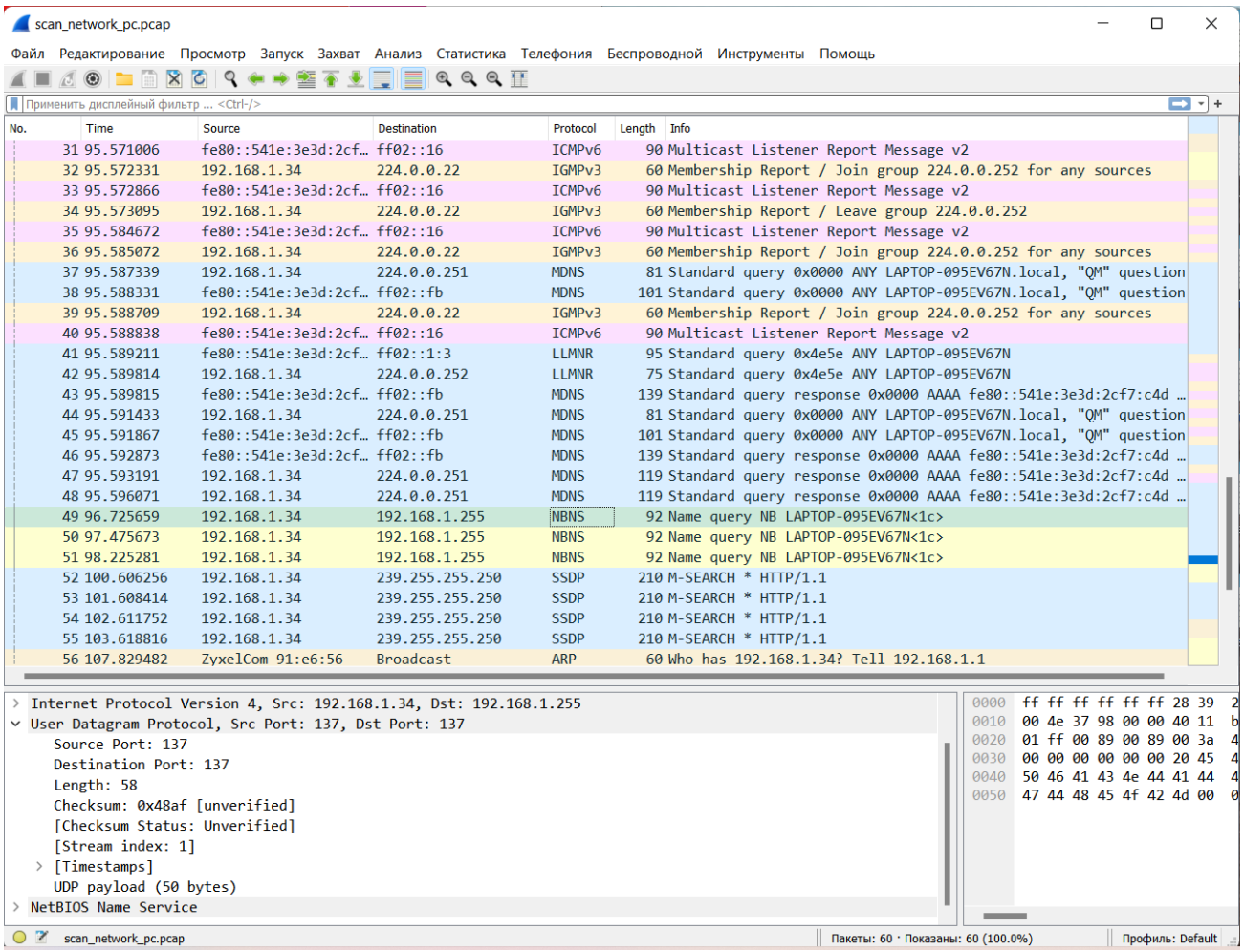


Рисунок 15 – Анализ сканирования портов собственного ПК с определением версий сетевых сервисов в Wireshark

В данном случае TCP или UDP не были обнаружены, но после того как какие-либо TCP и/или UDP будут обнаружены, Nmap начнет опрашивать эти порты, чтобы определить, какие службы их действительно используют. База данных nmap-service-probes содержит запросы для обращения к различным службам и соответствующие выражения для распознавания и анализа ответов. Nmap пытается определить протокол службы, имя приложения, номер версии, имя хоста, тип устройства, семейство ОС и иногда различные иные детали.

Вывод: изучила и освоила навыки работы со сканерами уязвимостей.