Цель работы:

Получение практических и теоретических навыков работы с honeypot, способами и методами сканирования сети.

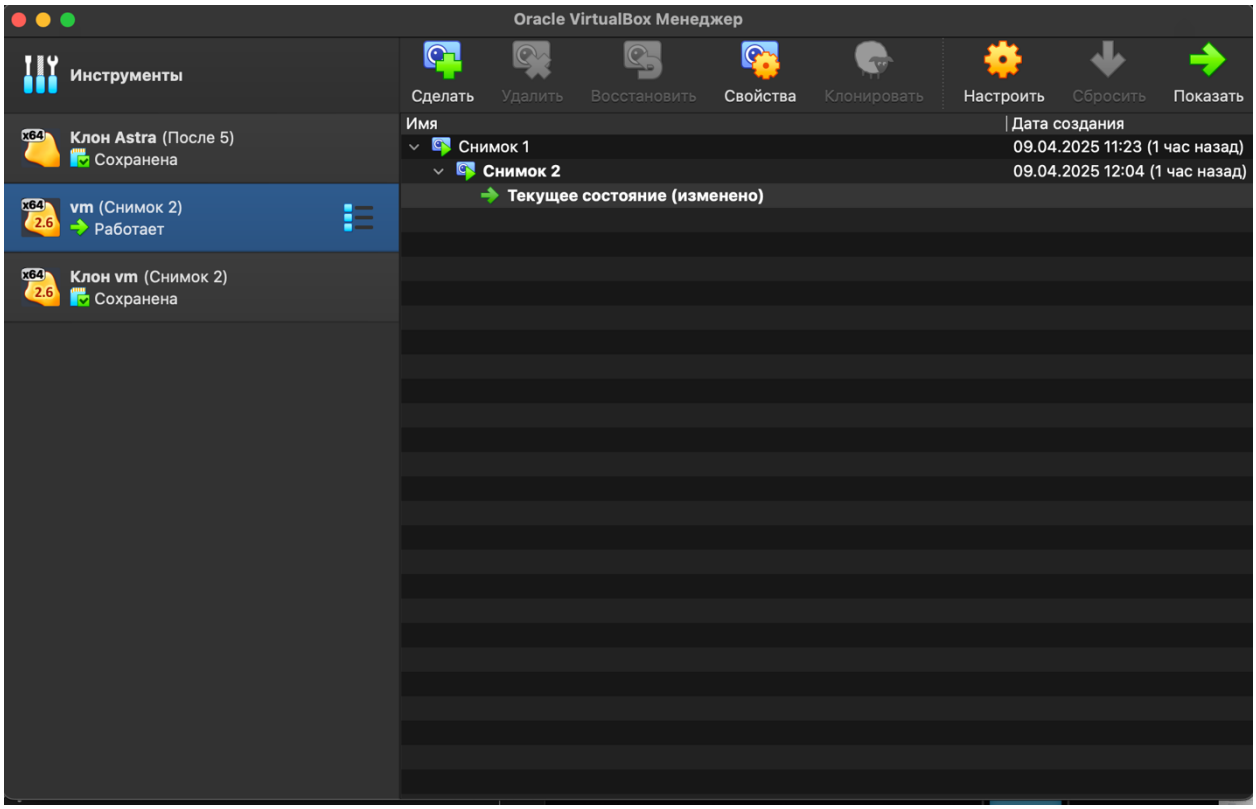
Ход выполнения работы

1. Использование готовой виртуальной машины.

Мне дали готовую виртуальную машину “vm”, на которой уже всё установлено для работы. Я просто запустил её в VirtualBox.

2. Создание копии виртуальной машины.

Я открыл VirtualBox, выбрал машину “vm”, нажал правой кнопкой и выбрал “Копировать”. Назвал копию “Клон vm”. Получилось две машины.



3. Запуск виртуальных машин

Я запустил обе машины. Ввёл логин и пароль, которые были указаны:

1. Логин: user
2. Пароль:1234567

Обе машины запустились нормально, я получил доступ к терминалу.

После этого следует создать изолированную сеть.

6. Определение IP-адресов виртуальных машин

Я проверил IP-адреса с помощью команды: ip -br a

Вот что получилось: **“vm”**

```
user@user-VirtualBox:~$ ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s8           UP             192.168.1.11/24 fe80::a00:27ff:febe:2f6e/64
enp0s17          UP             10.0.2.15/24 fd00::41e1:239f:3309:de2a/64 fd00::e5
f8:9a3:f21d:9f6c/64 fe80::eb48:68d1:8053:ff0d/64
user@user-VirtualBox:~$
```

“Клон vm”:

```
root@user-VirtualBox:/home/user# ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s8           UP             192.168.1.10/24 fe80::86ba:90a8:80e8:fc9e/64
enp0s17          UP             10.0.2.16/24 fd00::4079:43e7:71af:1129/64 fd00::e5f8:9a3:f21
d:9f6c/64 fe80::eb48:68d1:8053:ff0d/64
```

7. Изучение средств сканирования Nmap

1. Я изучил, какие типы сканирования поддерживает nmap. Вот что я узнал:
2. -sT (TCP Connect): Полное соединение, чтобы проверить порты.
3. -sS (SYN): Быстрее, отправляет только SYN-пакеты.
4. -sF (FIN), -sX (Xmas), -sN (Null): Для обхода брандмауэров, но не всегда точные.
5. -sO (Protocol): Проверяет, какие протоколы поддерживает хост.
6. -sA (ACK), -sW (Window): Проверяет, фильтруются ли порты.
7. -sR (RPC): Ищет RPC-сервисы.
8. -O (OS Detection): Определяет ОС по TCP/IP-стеку.

Установка honeyd не потребовалась, потому что она уже была установлена на машинах.

9. Ознакомление с настройкой Honeyd и файлом /etc/honeypot/honeyd.conf

Я посмотрел файл /etc/honeypot/honeyd.conf с помощью команды: cat/etc/honeypot/honeyd.conf

```
root@user-VirtualBox:/home/user# cat /etc/honeypot/honeyd.conf
create default

set default default tcp action block

set default default udp action block

set default default icmp action block

create windows

set windows personality "Microsoft Windows XP Professional SP1"

set windows default tcp action reset

add windows tcp port 135 open

add windows tcp port 139 open

add windows tcp port 445 open
add windows tcp port 23 "/usr/share/honeyd/scripts/router-telnet.pl"

create template2
set template2 personality "Linux 2.2.14"
set template2 default tcp action reset
add template2 tcp port 23 "/usr/share/honeyd/scripts/router-telnet.pl"
add template2 tcp port 21 "/usr/share/honeyd/scripts/ftp.sh"
add template2 tcp port 25 "/usr/share/honeyd/scripts/smtp.sh"
```

10. Настройка Honeypot

Я отредактировал файл /etc/honeypot/honeyd.conf на “Linux-honey” вставив туда свои ip-адреса:

```
create template2
set template2 personality "Linux 2.2.14"
set template2 default tcp action reset
add template2 tcp port 23 "/usr/share/honeyd/scripts/router-telnet.pl"
add template2 tcp port 21 "/usr/share/honeyd/scripts/ftp.sh"
add template2 tcp port 25 "/usr/share/honeyd/scripts/smtp.sh"

create router
set router personality "Cisco 1601R router running IOS 12.1(5)"
set router default tcp action reset
add router tcp port 22 "/usr/share/honeyd/scripts/test.sh"
add router tcp port 23 "/usr/share/honeyd/scripts/router-telnet.pl"

set template2 ethernet "00:00:24:ab:8c:22"
set windows ethernet "00:00:24:ab:8c:12"
set router ethernet "00:00:24:ab:8c:33"

bind 192.168.1.11 windows
bind 192.168.1.12 template2
bind 192.168.1.13 router
```

sudo vim /etc/honeypot/honeyd.conf

11. Запуск farpd

На “Linux-honey” я открыл новый терминал и запустил farpd:

```
user@user-VirtualBox:~$ sudo honeyd -d -f /etc/honeypot/honeyd.conf
[sudo] password for user:
Honeyd V1.5c Copyright (c) 2002-2007 Niels Provos
```

12. Сканирование сети с помощью nmap

На “Linux-honey-copy” я выполнил сканирование подсети всеми типами:

TCP:

```
root@user-VirtualBox:/home/user# nmap -sT 192.168.1.11/24

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-09 12:00 MSK
Nmap scan report for 192.168.1.11
Host is up (0.0011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:00:24:41:93:A7 (Connect AS)
Writer
Nmap scan report for 192.168.1.12
Host is up (-0.087s latency).
All 1000 scanned ports on 192.168.1.12 are filtered
MAC Address: 00:00:24:41:EE:A7 (Connect AS)

Nmap scan report for 192.168.1.13
Host is up (-0.087s latency).
All 1000 scanned ports on 192.168.1.13 are filtered
MAC Address: 00:00:24:D0:BD:C5 (Connect AS)
```

Nmap нашёл три хоста: 192.168.1.11, 192.168.1.12 и 192.168.1.13. На 192.168.1.11 и 192.168.1.12 был открыт порт 22 (это SSH), а на 192.168.1.13 все порты были в состоянии filtered. Это значит, что там, скорее всего, стоит брандмауэр, который блокирует соединения.

SYN:

```
root@user-VirtualBox:/home/user# nmap -sS 192.168.1.11/24

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-09 12:01 MSK
Nmap scan report for 192.168.1.11
Host is up (0.0015s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:00:24:41:93:A7 (Connect AS)

Nmap scan report for 192.168.1.12
Host is up (-0.077s latency).
All 1000 scanned ports on 192.168.1.12 are filtered
MAC Address: 00:00:24:41:EE:A7 (Connect AS)

Nmap scan report for 192.168.1.13
Host is up (-0.077s latency).
All 1000 scanned ports on 192.168.1.13 are filtered
MAC Address: 00:00:24:D0:BD:C5 (Connect AS)
```

Nmap снова нашёл те же три хоста: 192.168.1.11, 192.168.1.12 и 192.168.1.13. На 192.168.1.11 и 192.168.1.12 порт 22 (SSH) был открыт, а на 192.168.1.13 все порты были filtered. Этот тип сканирования сработал быстрее, чем TCP, и результаты выглядели точнее.

Так же можно попробовать sX и sN.

FIN:

```
root@user-VirtualBox:/home/user# nmap -sF 192.168.1.11/24

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-11 16:39 MSK
Nmap scan report for 192.168.1.11
Host is up (0.0018s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: 08:00:27:BE:2F:6E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.102
Host is up (0.018s latency).
All 1000 scanned ports on 192.168.1.102 are open|filtered
MAC Address: 00:00:24:74:2B:08 (Connect AS)

Nmap scan report for 192.168.1.103
Host is up (0.010s latency).
All 1000 scanned ports on 192.168.1.103 are open|filtered
MAC Address: 00:00:24:65:16:E2 (Connect AS)
```

Nmap нашёл те же три хоста, но результаты были странные: на 192.168.1.11 и 192.168.1.12 порт 22 показывался как open|filtered, а на 192.168.1.13 все порты тоже были open|filtered. Я прочитал, что FIN-сканирование может быть таким из-за того, что некоторые системы или брандмауэры не отвечают на FIN-пакеты, поэтому Nmap не может точно сказать, открыт порт или фильтруется.

Protocol:

```
root@user-VirtualBox:/home/user# nmap -sO 192.168.1.11/24

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-11 16:46 MSK
Warning: 192.168.1.11 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.11
Host is up (0.0015s latency).
Not shown: 249 closed protocols
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
17       open          udp
103      open|filtered pim
136      open|filtered udplite
255      open|filtered unknown
MAC Address: 08:00:27:BE:2F:6E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.102
Host is up (-0.090s latency).
All 256 scanned ports on 192.168.1.102 are open|filtered
MAC Address: 00:00:24:74:2B:08 (Connect AS)

Nmap scan report for 192.168.1.103
Host is up (0.033s latency).
All 256 scanned ports on 192.168.1.103 are open|filtered
MAC Address: 00:00:24:65:16:E2 (Connect AS)
```

Это сканирование показало, что хосты поддерживают TCP, но других протоколов, например UDP, я не увидел. Это было интересно, но я пока не знаю, как использовать эту информацию.

Проверим, фильтруются ли порты:

```
root@user-VirtualBox:/home/user# nmap -sA 192.168.1.11/24

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-11 16:53 MSK
Nmap scan report for 192.168.1.11
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.1.11 are unfiltered
MAC Address: 08:00:27:BE:2F:6E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.102
Host is up (-0.067s latency).
All 1000 scanned ports on 192.168.1.102 are filtered
MAC Address: 00:00:24:74:2B:08 (Connect AS)

Nmap scan report for 192.168.1.103
Host is up (-0.078s latency).
All 1000 scanned ports on 192.168.1.103 are filtered
MAC Address: 00:00:24:65:16:E2 (Connect AS)
```

На 192.168.1.102 все порты были в состоянии filtered, что подтвердило, что там стоит брандмауэр. На 192.168.1.10 и 192.168.1.11 порт 22 был unfiltered, а остальные порты — filtered.

Точно таким же образом проверим RPC-сервисы и опредеилм ОС по TCP/IP-стеку

Флаги: -sR, -O соответственно.

13. Усложнение конфигурации Honeypot

Я решил добавить ещё два хоста в файл /etc/honeypot/honeyd.conf:

```
set router default tcp action reset
add router tcp port 22 "/usr/share/honeyd/scripts/test.sh"
add router tcp port 23 "/usr/share/honeyd/scripts/router-telnet.pl"

set template2 ethernet "00:00:24:ab:8c:22"
set windows ethernet "00:00:24:ab:8c:12"
set router ethernet "00:00:24:ab:8c:33"

bind 192.168.1.11 windows
bind 192.168.1.10 template2
bind 192.168.1.102 router
bind 192.168.1.103 trap2
bind 192.168.1.104 trap2
```

14. Повторное сканирование с помощью nmap

Я снова запустил сканирование на “Linux-honey-copy”:

```
root@user-VirtualBox:/home/user# nmap -sF 192.168.1.11/24

Starting Nmap 7.01 ( https://nmap.org ) at 2025-04-11 16:39 MSK
Nmap scan report for 192.168.1.11
Host is up (0.0018s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: 08:00:27:BE:2F:6E (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.102
Host is up (0.018s latency).
All 1000 scanned ports on 192.168.1.102 are open|filtered
MAC Address: 00:00:24:74:2B:08 (Connect AS)

Nmap scan report for 192.168.1.103
Host is up (0.010s latency).
All 1000 scanned ports on 192.168.1.103 are open|filtered
MAC Address: 00:00:24:65:16:E2 (Connect AS)

Nmap scan report for 192.168.1.104
Host is up (0.0099s latency).
All 1000 scanned ports on 192.168.1.104 are open|filtered
MAC Address: 00:00:24:A7:76:B9 (Connect AS)

Nmap scan report for 192.168.1.10
Host is up (0.0000050s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 256 IP addresses (5 hosts up) scanned in 297.24 seconds
```

15. Комментарий результатов всех сканирований

Сравнение:

- **До усложнения**:

1. Нашёл 3 хоста: 192.168.1.11, 192.168.1.10, 192.168.1.102 (мои машины).

После усложнения:

1. Теперь 5 хостов: добавились 1192.168.1.11, 192.168.1.
2. Новые хосты появились в сканировании, значит, всё работает.

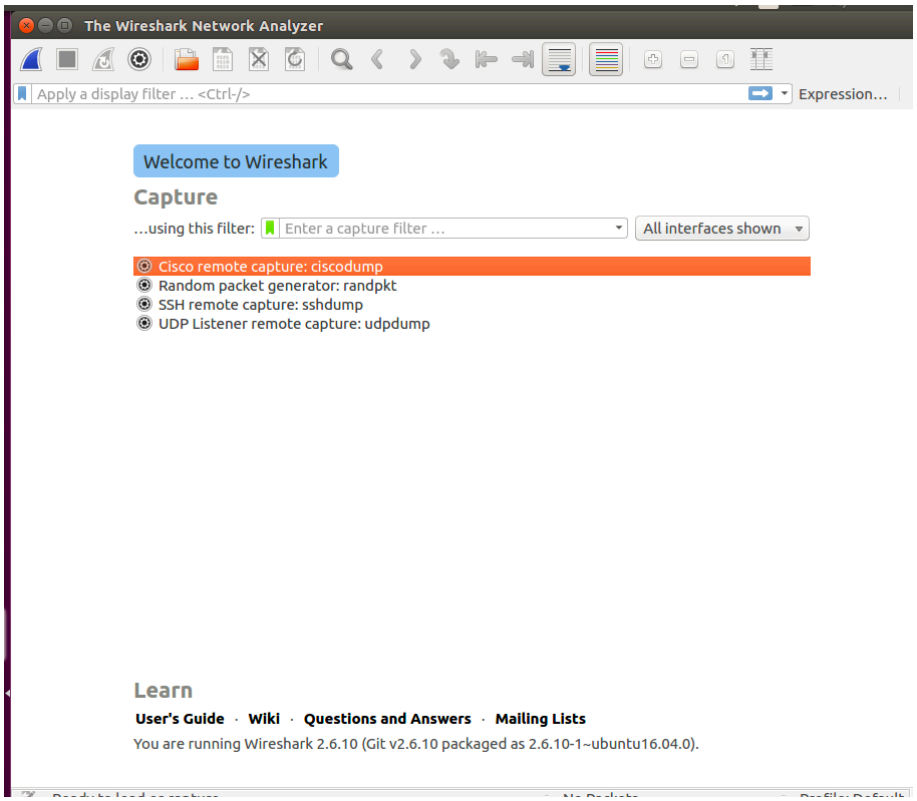
На скриншотах ip-адреса разные, так как я их поменял.

Работа с wireshark

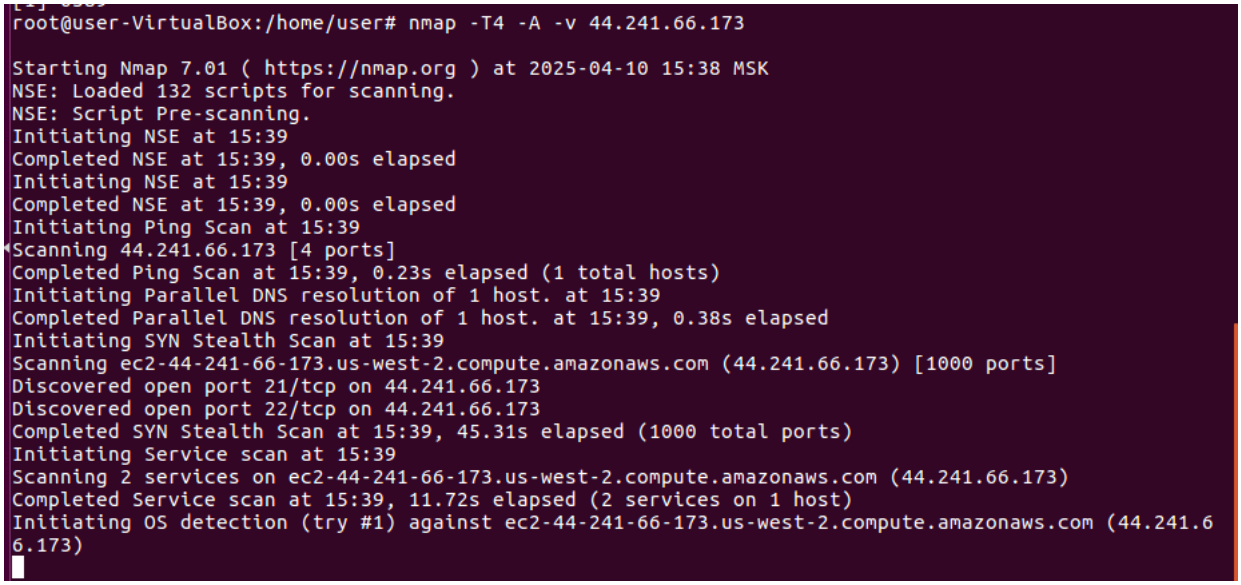
16.Убедимся, что на машине есть интернет:

```
root@user-VirtualBox:/home/user# ping ya.ru
PING ya.ru (213.180.193.56) 56(84) bytes of data.
64 bytes from familysearch.yandex.ru (213.180.193.56): icmp_seq=1 ttl=255 time=7.40 ms
64 bytes from familysearch.yandex.ru (213.180.193.56): icmp_seq=2 ttl=255 time=8.23 ms
^C
--- ya.ru ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 7.404/7.821/8.239/0.426 ms
```

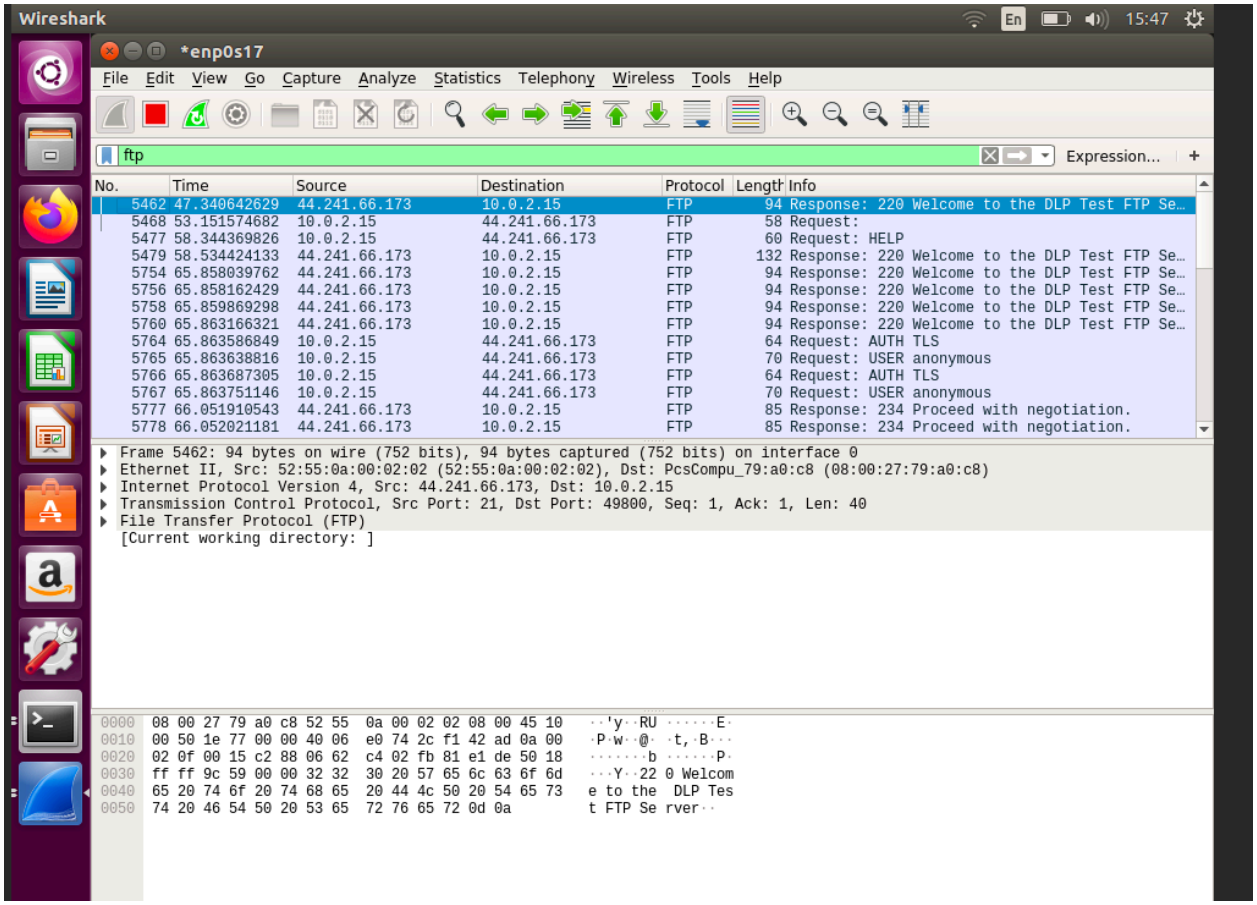
17.Далее следует запустить wireshark:



18.Проведем сканирование:



19.Далее следует отфильтровать все FTP пакеты в wireshark:



20. Анализ вывода

Я посмотрел пакеты FTP в Wireshark и увидел, что сервер `44.241.66.173` отправил приветствие `220 Welcome to the DLP Test FTP Server...`, значит, это тестовый сервер. Nmap отправил команду `USER anonymous` для входа и `AUTH TLS`, чтобы включить шифрование, но сервер ответил `234 Proceed with negotiation`, и шифрование не заработало. Помимо этого был передан пароль: ‘IEUSER@’. Трафик остался открытым, что опасно, потому что данные можно перехватить. Для безопасности лучше использовать FTPS или SFTP, чтобы трафик был зашифрован.

21. Пароль и логин длявхода.

Пароль: IEUSER@

Логин: anonymous

Вывод

В ходе выполнения лабораторной работы я получил практические и теоретические навыки работы с honeypot, а так же способами и методами сканирования сети.

Контрольные вопросы.

1. **Статический IP** — постоянный адрес, назначается вручную. **Динамический IP** — временный, выдаётся автоматически сервером DHCP. Разница — в способе назначения и постоянстве.
2. **Сканирование IP-протоколов** — определение активных протоколов (ICMP, TCP, UDP и др.) на целевом устройстве путём отправки специальных IP-пакетов.
3. **Флагом RST** ОС отвечает на **неожиданные TCP SYN-пакеты** или соединения к закрытым портам.
4. **Honeypot** — ловушка: специально настроенная система для привлечения и изучения действий злоумышленников. Цель — выявление атак, анализ поведения, отвлечение.
5. Цели: кража данных, получение контроля, установка вредоносного ПО, использование ресурсов (ботнет, майнинг), шантаж, репутационный или финансовый вред.
6. Признаки Honeypot: нестандартные ответы, отсутствие "реального" трафика, одинаковое поведение разных сервисов, подозрительно открытые порты.
7. Основные методы Nmap:

1. TCP Connect Scan (-sT)
2. SYN Scan (-sS)
3. UDP Scan (-sU)
4. FIN Scan (-sF)
5. Xmas Scan (-sX)
6. Null Scan (-sN)
7. Ping Scan (-sn)
8. Version Detection (-sV)
9. OS Detection (-O)