Государственное бюджетное образовательное учреждение среднего профессионального образования Новосибирской области

Новосибирский химико- 630102 г. Новосибирск, ул. Садовая, 26,

технологический колледж. Тел./факс: (383) 266-00-44, тел.: (383) 266-00-54,

nhtk@mail.ru, http://nhtk-edu.ru

им. Д.И. Менделеева

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ**

**ПРАКТИЧЕСКОЙ РАБОТЫ**

Выполнил:

Гуров Д.А.

Новосибирск – 2024

**Практическая работа №18 «Nmap, Wireshark, Burpsuite»**

**Вопросы**

1. Что такое Kali linux?

**Kali** **Linux** — это дистрибутив **Linux** на основе Debian с открытым исходным кодом, предназначенный для расширенного тестирования на проникновение, проверки уязвимостей, аудита безопасности систем и сетей. Дистрибутив используют многие специалисты информационной безопасности: сетевые архитекторы и администраторы, инженеры-криминалисты, директора по информационной безопасности, пентестеры.

1. Как связано тестирование программных продуктов и пентестинг?

Тестирование программных продуктов и пентестинг (проверка на проникновение) являются частями процесса обеспечения качества программного обеспечения, однако они имеют различные цели.  
  
Тестирование программных продуктов включает в себя проверку функциональности, производительности, надежности и других аспектов программного продукта с целью обнаружения ошибок и дефектов. Этот процесс обычно проводится разработчиками или специалистами по тестированию для улучшения качества программного продукта.  
  
Пентестинг, с другой стороны, представляет собой процесс исследования информационной безопасности, включающий в себя активное тестирование системы на наличие уязвимостей с целью выявления возможных уязвимостей и оценки уровня защиты системы от несанкционированного доступа.  
  
Хотя тестирование программных продуктов и пентестинг имеют сходные методики и инструменты, связь между ними заключается в том, что тестирование программных продуктов может помочь выявить некоторые уязвимости в программном обеспечении, в то время как пентестинг может использовать результаты тестирования программного продукта для определения уровня защиты системы от потенциальных угроз. Кроме того, пентестинг может быть частью процесса тестирования безопасности программного продукта для обеспечения его защиты от возможных атак.

1. Что такое Wireshark?  
   Wireshark - это программный анализатор сетевого трафика, который позволяет мониторить и анализировать данные, передающиеся по компьютерной сети.
2. Для чего он используется?

Он используется для анализа сетевого трафика, поиска уязвимостей в сети, отслеживания сетевых проблем, обнаружения атак и многих других целей.

1. Что такое Nmap?

Nmap - это утилита сканирования сети, которая используется для определения активных узлов, сервисов и уязвимостей в сети.

1. Как сканирование сети может помочь избежать незащищенности программы, приложения?

Сканирование сети может помочь выявить уязвимости в программе или приложении, так как позволяет обнаружить открытые порты, незащищенные сервисы и другие потенциальные уязвимости, которые могут быть использованы злоумышленниками для атаки.

1. Что такое Burpsuite?

Burp Suite - это инструмент для тестирования безопасности веб-приложений, который позволяет обнаружить уязвимости, проводить атаки на веб-приложения и редактировать сеансовые данные.

1. Как сканирование web-приложения может помочь избежать утечки данных?

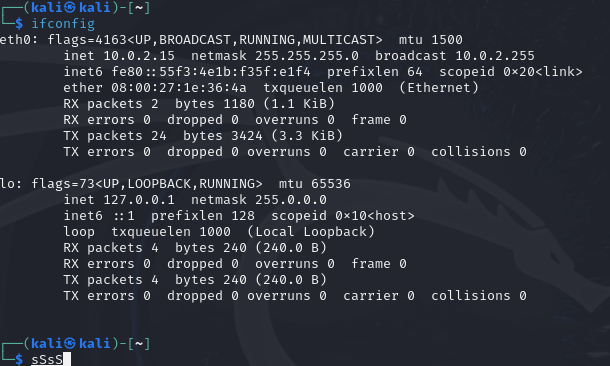
Сканирование web-приложения с помощью Burp Suite может помочь избежать утечки данных, так как позволяет обнаружить уязвимости веб-приложения, связанные с неправильной обработкой ввода данных, перехватывать и анализировать трафик для выявления потенциальных утечек данных и предотвращать атаки на веб-приложения.

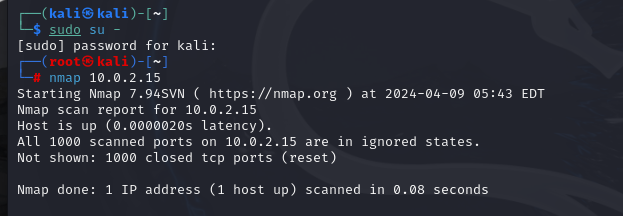
**Порядок выполнения практической работы**

1. Практическая работа выполняется в **отдельном** создаваемом студентом **документе**!
2. Титульный лист с указанием наименования организации, ФИО студента и номер группы
3. Выполнить задания, в отчете написать номер задания, добавить скриншот, описать результат.
4. Ответить на контрольные вопросы (если присутствуют в работе)
5. Вывод

**Практическое задание**

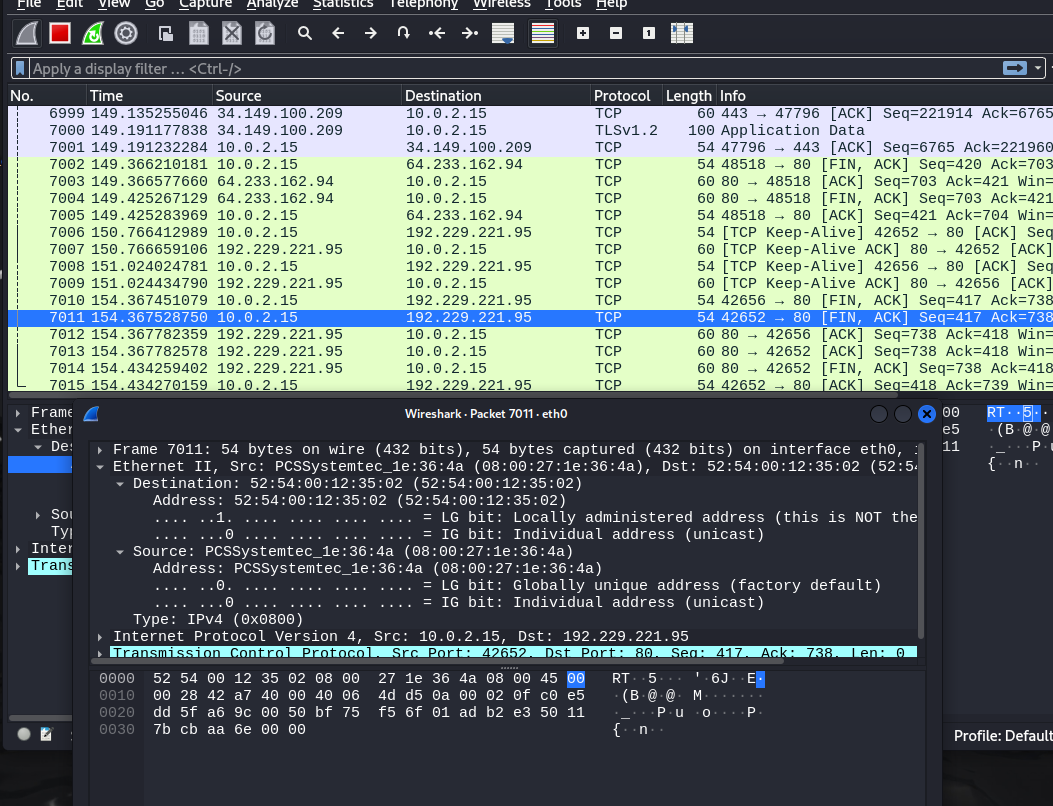
1. Выполнить примеры работы с Nmap: [IntroLabs/IntroClassFiles/Tools/IntroClass/Nmap/Nmap.md at master · strandjs/IntroLabs · GitHub](https://github.com/strandjs/IntroLabs/blob/master/IntroClassFiles/Tools/IntroClass/Nmap/Nmap.md)

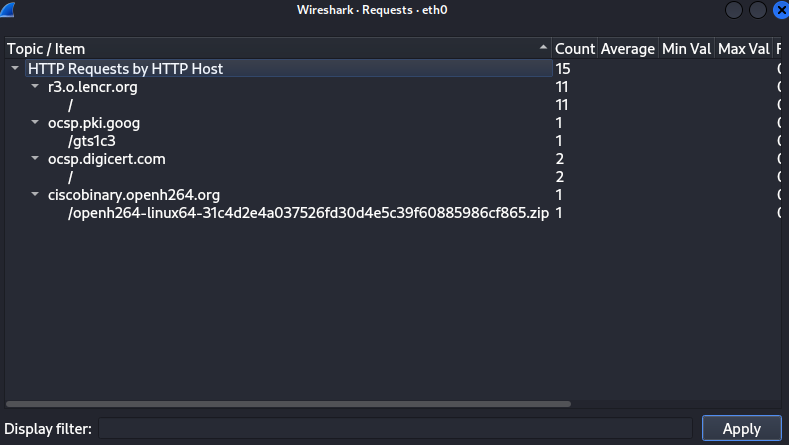


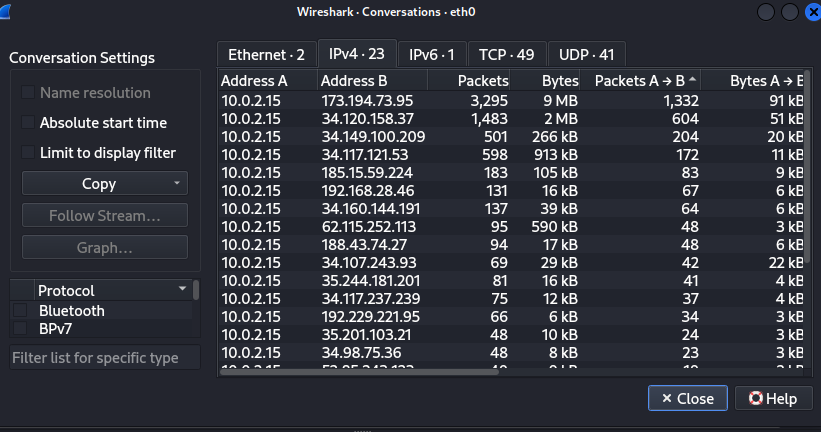


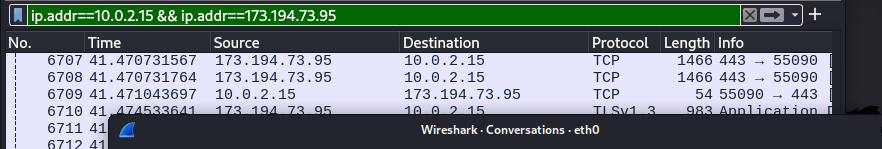
1. Выполнить примеры работы с Wireshark:

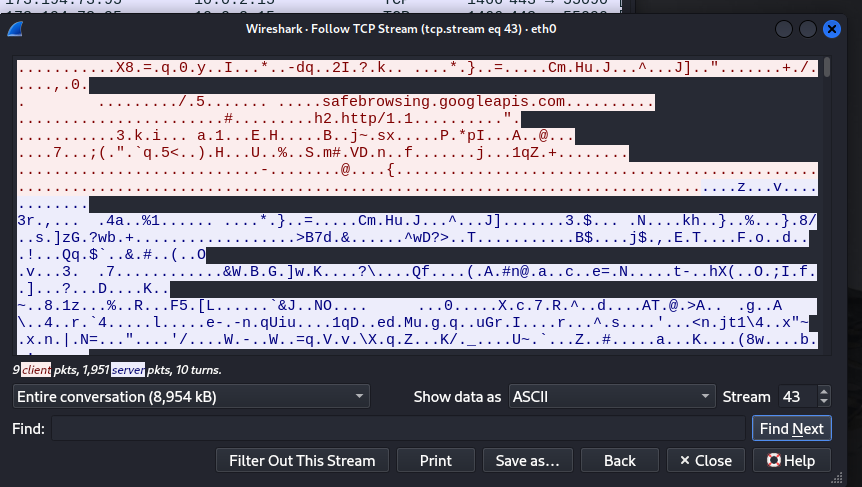
[IntroLabs/IntroClassFiles/Tools/IntroClass/Wireshark/Wireshark.md at master · strandjs/IntroLabs · GitHub](https://github.com/strandjs/IntroLabs/blob/master/IntroClassFiles/Tools/IntroClass/Wireshark/Wireshark.md)

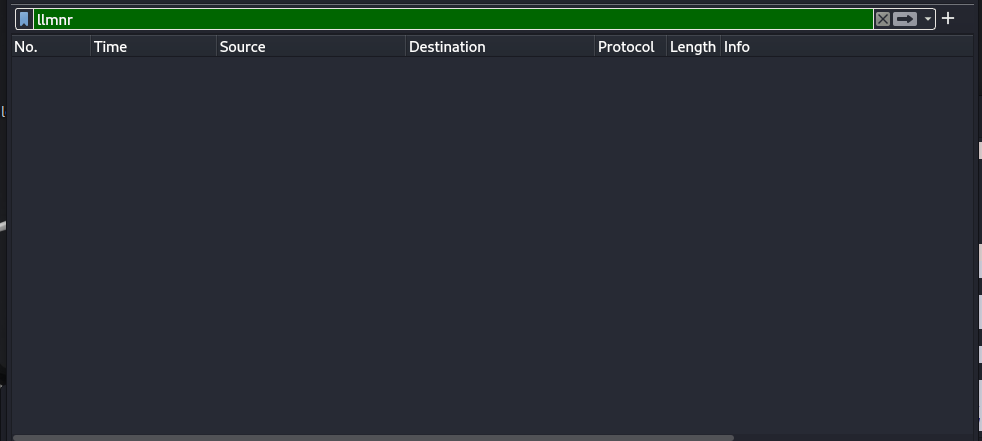


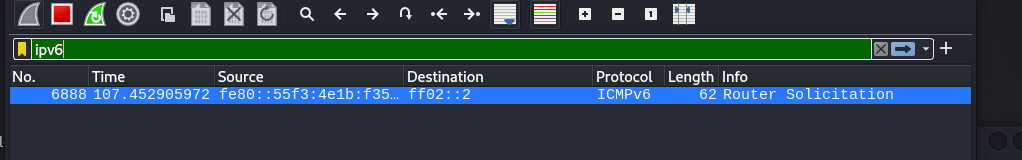


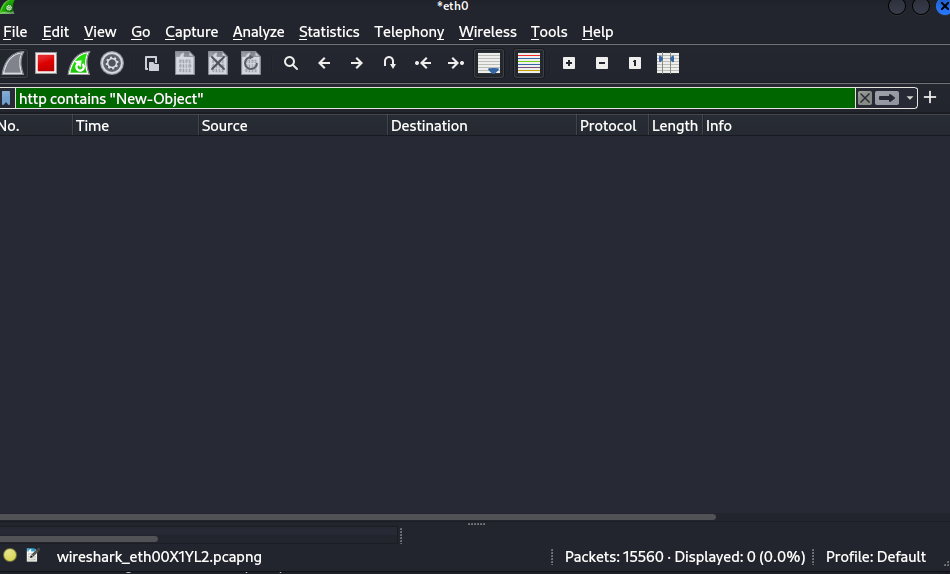












1. Зарегистрироваться

[Web Application Security, Testing, & Scanning - PortSwigger](https://portswigger.net/)

после входа Academy -> all content -> all labs и там выбираем Information disclosure

