

## CCNA Security

**Лабораторная работа. Изучение сетевых атак, а также инструментов для аудита безопасности и проведения атак**

## Задачи

#### Часть 1. Изучение сетевых атак

* Изучите произошедшие сетевые атаки.
* Выберите сетевую атаку и составьте по ней отчет для представления его аудитории.

#### Часть 2. Изучение инструментов аудита безопасности и проведения атак

* Изучите инструменты аудита безопасности.
* Выберите один из инструментов и составьте его презентацию для класса.

## Исходные данные/сценарий

За многие годы злоумышленники разработали множество инструментов для проведения атак и компрометации сетей. Эти атаки имеют множество форм, но чаще всего они направлены на получение конфиденциальной

информации, уничтожение ресурсов или блокирование доступа легальных пользователей к ресурсам. Когда сетевые ресурсы оказываются недоступны, может страдать продуктивность работника, приводя к упущенной выгоде для всего бизнеса.

Чтобы понять, как защитить сеть от атак, администратор должен определить уязвимости сети. Специальные

программы аудита безопасности, разработанные производителями оборудования и программного обеспечения, помогают определить потенциальные уязвимости. Инструменты, которые применяются для атак на сеть, могут быть использованы и сетевыми специалистами для тестирования способности сети противостоять этим атакам. После определения уязвимостей можно предпринимать меры для защиты сети.

Эта лабораторная работа представляет собой структурированный исследовательский проект, разделенный

на две части: изучение сетевых атак и инструментов аудита безопасности. Сообщите инструктору, какие сетевые атаки и инструменты для аудита безопасности вы выбрали для изучения. Таким образом, участники группы расскажут о целом наборе сетевых атак и инструментов для определения уязвимостей.

В части 1 изучите реально произошедшие сетевые атаки. Выберите одну из этих атак и опишите, каким образом она была совершена, объем урона, нанесенного сети, и время простоя. Затем проанализируйте, каким образом данная атака могла бы быть нейтрализована и какие техники нейтрализации можно реализовать для предотвращения будущих атак. В конце подготовьте отчет по форме, описанной в этой лабораторной работе.

В части 2 изучите инструменты аудита безопасности и проведения атак. Изучите один из инструментов, который можно использовать для определения уязвимостей сетевых устройств или хостов. Составьте отчет на одну страницу по этому инструменту по форме, описанной в этой лабораторной работе. Подготовьте короткую

(на 5-10 минут) презентацию для группы.

Вы можете работать в парах, где один человек рассказывает о сетевой атаке, а другой – об инструментах. Каждый участник группы составляет короткий рассказ о результатах своего анализа. Можно использовать презентации Powerpoint или просто продемонстрировать полученные результаты.

## Необходимые ресурсы

* Компьютер с доступом в Интернет
* Компьютер для проведения презентаций с установленным Powerpoint или другим программным обеспечением для презентаций
* Видеопроектор и экран для демонстраций и презентаций

# Часть 1: Изучение сетевых атак

В части 1 данной лабораторной работы вы изучите реальные сетевые атаки и выберете одну из них для составления отчета. Заполните форму ниже на основе результатов своего анализа.

### Шаг 1: Изучите различные сетевые атаки.

Перечислите несколько атак, которые вы обнаружили в ходе изучения.

Руткиты (Rootkit), Рекламное ПО (Adware), Шпионские программы (Spyware)

Банкеры (Banker).

### Шаг 2: Заполните следующую форму по выбранной сетевой атаке.

|  |  |
| --- | --- |
| **Название атаки** | Рекламное ПО (Adware) |
| **Тип атаки** | Существует два основных типа рекламного ПО в зависимости от способа проникновения на ваш компьютер: вместе с бесплатной или условно-бесплатной программой или через зараженные сайты. |
| **Даты проведения атак** |  |
| **Пострадавшие компьютеры/организации** | Каждый компьютер может пострадать от атаки Adware |
| **Принцип действия и результаты** | |
| Этот тип рекламного ПО, фактически, связан с «угоном» браузера. Заражение происходит при посещении зараженного сайта, в результате чего осуществляется несанкционированная установка рекламного ПО. Затем при просмотре других сайтов вам начинают активно показывать рекламные объявления. Хотя вы думаете, что эта реклама идет с просматриваемого сайта, однако на самом деле они показываются в результате работы рекламного ПО, которое было установлено на вашем устройстве. | |

|  |
| --- |
| **Варианты нейтрализации** |
| Если на вашем компьютере установлено рекламное ПО, и вы устали часто закрывать разные вкладки и окна, особенно на мобильных устройствах, где на их показ тратится заряд батареи, то вам необходимо предпринимать меры. Для удаления рекламного ПО на вашем устройстве используйте антивирус, а также специальные программы для удаления рекламного ПО. |
| **Справочные данные и ссылки** |
| <https://www.cloudav.ru/mediacenter/malware/what-is-adware/>  https://zen.yandex.ru/media/merion\_networks/tipy-setevyh-atak-5eb13d248a622c20283c4f00 |
| **Графики и иллюстрации (включают ссылки на файл PowerPoint или веб-сайты)** |
| <https://sun9-25.userapi.com/c846221/v846221480/35c70/N6M1rO_1xe8.jpg>  <https://zillya.ua/sites/default/files/pictures/adware.jpg>  https://www.web-comp-pro.ru/wp-content/uploads/2015/08/kak-udalit-ads-by-offerswizard-vruchnuyu-i-izbavitsya-ot-reklamy.jpg |

**Часть 2: Изучение инструментов аудита безопасности и проведения атак**

Во второй части данной лабораторной работы изучите инструменты для аудита безопасности и проведения атак.

Изучите один из инструментов, который можно использовать для определения уязвимостей сетевых устройств или хостов. Заполните форму ниже на основе полученных результатов.

### Шаг 1: Изучите различные инструменты аудита безопасности и проведения атак.

Перечислите несколько инструментов, которые вы обнаружили в ходе изучения.

Существует два основных типа рекламного ПО в зависимости от способа проникновения на ваш компьютер: вместе с бесплатной или условно-бесплатной программой или через зараженные сайты.

Когда вы скачиваете бесплатную или условно-бесплатную программу, зачастую они содержат встроенное рекламное ПО. Эти бесплатные программы используют рекламное ПО для финансирования разработки и дистрибуции. Такой тип рекламного ПО не имеет злого умысла, но может серьезно раздражать.Часто рекламное ПО путают со шпионским ПО. Шпионы работают аналогичным образом, но они являются отдельной программой. Такие программы скачиваются неосозннано (случайно, без ведома) и они отслеживают ваши предпочтения по поиску в Интернете, чтобы можно было показывать рекламные объявления именно «под вас», а также собирают о вас другую информацию.

### Шаг 2: Заполните следующую форму для выбранного инструмента аудита безопасности/проведения атак.

|  |  |
| --- | --- |
| **Наименование инструмента** | Malwarebytes |
| **Разработчик** | Malwarebytes |
| **Тип инструмента (с интерфейсом или символьно-ориентированный)** | Антивирусная программа |
| **Место использования (сетевое устройство или компьютер)** | Компьютер, смартфон |
| **Стоимость** | 69$ |
| **Описание ключевых особенностей и возможностей продукта или инструмента** | |
| Антивирусная программа, которая находит и удаляет вредоносные программы. Производится корпорацией Malwarebytes, была выпущена в январе 2008 года. Она доступна в виде бесплатной версии, которая ищет и удаляет вредоносные программы по ручному запуску, и платной версии, которая обеспечивает сканирование по расписанию, защиту в реальном времени и сканирование флеш-накопителей. | |

https://ru.malwarebytes.com/

Справочные данные и ссылки

**Вопросы для повторения**

1. В чем заключается воздействие сетевых атак на деятельность организации? Какие ключевые шаги могут предпринять организации для защиты своих сетей и ресурсов?

Чтобы предотвратить загрузку рекламного ПО на ваше устройство, важно проявлять осторожность при работе с любыми сайтами, которые могут выглядеть подозрительными. Вы также должны быть осторожны при загрузке бесплатных или условно-бесплатных программ. Скачивайте программы только с надежных сайтов, которым вы доверяете.

При просмотре сайтов лучше не нажимать на какие-либо рекламные объявления или уведомления. Например, злоумышленники любят показывать уведомления, что якобы ваш ПК заражен, а потому требуется установить антивирус. Это – обман, на который «клюют» многие люди.

В дополнение к этому, вам необходимо следить за тем, чтобы на всех ваших устройствах была обновлена операционная система. Не обновлённые системы являются более уязвимыми: вредоносные программы и вирусы могут использовать их дыры безопасности.

1. Приходилось ли вам работать в организации или слышали ли вы о такой организации, где сеть была скомпро- метирована? Если да, какой ущерб был нанесен организации и какие меры были предприняты в этой ситуации?

Да приходилось, в детстве часто подхватывал такие вирусы, приходилось переустанавливать windows или

запускать антивирусную программу которая могла устранить данные ошибки.

1. Какие меры вы можете предпринять для защиты собственного компьютера или ноутбука?

Для удаления рекламного ПО на устройстве нужно использовать антивирус, а также специальные программы для удаления рекламного ПО