**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.

Червь, троян, перенаправление DNS, DNS снуфинг, DOS

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

| | |
|---|---|
| **Название атаки** | PSP firmware 1.50 hack |
| **Тип атаки** | Buffer overflow |
| **Даты проведения атак** | 2005 |
| **Пострадавшие компьютеры/организации** | Sony Electronics |
| **Принцип действия и результаты** | |
| Ошибка в использовании функции sprintf() из стандартной библиотеки Си позволила запускать неподписаный код на консоли. Принцип работы:<br>В исходном коде прошивки есть строки вида:<br>void foo(void) {<br>  char buffer[260];<br>  sprintf(buffer, "/*аргументы принтф*/", /*какие-то параметры*/);<br>}<br>Хакеры в свою очередь добавили символ % и выйдя за пределы буфера перезаписали адрес возврата функции на тот где хранился неподписанный код. | |

 

| **Варианты нейтрализации** |
|---|
| Выпуск новой прошивки |
| **Справочные данные и ссылки** |
| MISRA C Standard |
| **Графики и иллюстрации (включают ссылки на файл PowerPoint или веб-сайты)** |
| https://www.youtube.com/watch?v=qIxKPu20R58 |

## 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.

Инструменты аудита безопасности Linux
1) Lynis — auditing system hardening testing
2) Lunar — a UNIX security auditing tool
3) Nix Auditor — a CIS Audit made easier
4) Loki — Simple IOC and Incident Response Scanner
5) Linux Security Auditing Tool (LSAT)

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

| **Наименование инструмента** | Lynis |
|---|---|
| **Разработчик** | Open Source |
| **Тип инструмента (с интерфейсом или символьно-ориентированный)** | Command Line Interface |
| **Место использования (сетевое устройство или компьютер)** | Anything running Linux |
| **Стоимость** | 0$ for personal use. 3$ per system for enterprises |
| **Описание ключевых особенностей и возможностей продукта или инструмента** | |
| аудит безопасности (типовой сценарий, задаваемый пользователем); тестирование на соответствие требованиям (например, PCI DSS, HIPAA, SOX404, OpenSCAP, NSA); обнаружение уязвимостей (устаревшее ПО); режим Penetration testing (попытка эскалации привилегий); улучшение системы (незадействованные твики ядра, демонов и прочего). | |

 

| **Справочные данные и ссылки** |
| --- |
| https://cisofy.com/lynis/ |

## 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?

   Последствия могут быть самые разные, от прямых денежных потерь до репутационных и прочих. Для защиты своих сетей организации должны иметь чёткие политики информационной безопасности для сотрудников, а так же регулярно обновлять ПО для защиты(антивирусы и прочее), проводить аудит безопасности регулярно. И самое главное - возможность принять меры при возникновении угрозы

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

   Я проходил учебную практику на ГП Антонов(программист-стажёр) и столкнулся с эпидемий вируса "Петя" который зашифровал многие жёсткие диски в различных ведомствах. Не смотря на отсутствие выхода в интернет на самих машинах, а также запрета неслужебных флешек вирус проник во внутрь, что наводит мысли о саботаже. Ущерб был довольно большим, но как не странно многие вещи были на бумажных носителях, или были бекапы.

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

   Обновлять базу данных антивируса, и не выключать файрвол :P. А так же не скачивать файлы из сомнительных источников

 