# 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

очерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

# 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.

## \_Троянкий конь, Червь, DDos атаки, Фишинг, UDP-флуд , вредоносное ПО, уязвимости USB, mail boombing, Dummy dns server , Software vulnerabilities \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

|  |  |
| --- | --- |
| **Название атаки** | Dummy DNS Server |
| **Тип атаки** | Сетевая атака «отказ в обслуживании» |
| **Даты проведения атак** | 1997, 2009, 2012, 2019, 2020 |
| **Пострадавшие компьютеры/организации** | AT&T, Twitter, Godaddy, Сеть Индии |
| **Принцип действия и результаты** | |
| * В декабре 2009 года из-за подмены DNS–записи в течение часа для пользователей был недоступен сервис Twitter. Акция носила политический характер, и вместо интерфейса социальной сети на главной странице ресурса отображались предостережения иранских хакеров по поводу американской агрессии. * В августе 2012 года AT&T подверглась DDoS-атаке, которая вывела из строя DNS-серверы компании в двух территориальных точках. В ходе атаки, которая продлилась по меньшей мере 8 часов, сайт компании AT&T был недоступен для пользователей. Однако наиболее критическое значение имел тот факт, что коммерческие сайты в сети AT&T также были не доступны. * 10 ноября 2012 ujlf компания GoDaddy, крупнейший хостинг-провайдер и регистратор доменных имен, пострадала от атаки типа DNS-флуд, которая нанесла ущерб миллионам доменов в сети интернет. Был недоступен не только домен www.godadddy.com, но и все домены, зарегистрированные через компанию GoDaddy, которые использовали ее имя сервера, DNS записи были также недоступны. * 31 марта хактивисты группы Anonymous угрожали вывести из строя всю сеть Интернет путем атаки на 13 корневых DNS-серверов. Группа планировала использовать технику «усиленного отражения» DNS-запросов, ими была выпущена утилита Ramp, которая была разработана для подключения ресурсов множества интернет-провайдеров и других корпоративных DNS-сервисов для выведения из строя корневых серверов. В конечном итоге, нападение так и не состоялось, но изощренный план (см. ниже раздел «Атака путем отраженных DNS-запросов») обладал разрушительный потенциалом. * 2020: Индия стала лидером по DNS-атакам. В середине июня 2020 года компания по кибербезопасности EfficientIP опубликовала отчет по DNS-атакам, согласно которому Индия стала лидером по этому виду киберугроз. В стране было зафиксировано самое большое количество таких атак, по 12,13 на организацию, а индийские фирмы потеряли по меньшей мере $784 000. Хакеры украли конфиденциальную информацию о клиентах почти 27% индийских компаний, тогда как во всем остальном мире эта доля составила 16%. В результате атак время простоя облачных сервисов в стране достигло 65%. | |
| **Варианты нейтрализации** | |
| Без наличия специальной защиты единственными способами нейтрализовать атаку является повышение мощности NS-серверов.  Кроме того, что постоянное наращивание мощности сервера DNS проблематично, такой сервер сам может использоваться злоумышленниками для организации дальнейших атак на других жертв.  Чаще всего используют программы для защиты.  Программа (защита без раскрытия зоны). В некоторых случаях у клиента нет возможности (например, из соображений безопасности) передавать нашего сервера управления своей доменной зоной. В этом случае достаточно сообщить программе IP-адрес (а) авторитативные серверов (а лучше всего, такого же NS-сервера, данных о котором нет в публичной сети) и указать IP адрес, выделенный, как адрес авторитативные сервера для своего зоны (заменяя или дополняя существующие). При таком подключении NS-сервер будет выступать сервером-рекурсором с кэшем данных о подключенной зоне user. В случае отсутствия у нашего сервера информации о любой записи, он пошлет запрос в upstream-сервера, и сохранит ответ в себе. При этом будут также учитываться все возможные варианты развития вектора атаки. | |
| **Справочные данные и ссылки** | |
| TADVISOR: [сайт]. URL: <https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%90%D1%82%D0%B0%D0%BA%D0%B8_%D0%BD%D0%B0_DNS-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80%D0%B0>  Qrator: [сайт]. URL: <https://qrator.net/ru/solutions/dns>  it-black.ru: [сайт]. URL: <https://it-black.ru/vidy-khakerskikh-atak/>  kiev-security: [сайт]. URL: <http://kiev-security.org.ua/box/15/21.shtml> | |
| **Графики и иллюстрации (включают ссылки на файл PowerPoint или веб-сайты)** | |
| Что такое DNS сервера, зачем они нужны - Ваши финансы | |

# 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.

**Аудит информационной безопасности включает в себя три основных составляющих**:

* Средства и способы проверки (инструменты аудита);
* Результат проверки (оценка текущего состояния системы информационной безопасности);
* Идеал, с которым сравнивается результат проверки.

**Инструменты аудита безопасности Linux**

* Lynis — auditing system hardening testing.
* Lunar — a UNIX **security** auditing tool.
* Nix Auditor — a CIS Audit made easier.
* Loki — Simple IOC and Incident Response Scanner.
* Linux **Security** Auditing Tool (LSAT)

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

|  |  |
| --- | --- |
| **Наименование инструмента** | Loki |
| **Разработчик** | Florian Roth(Linux) |
| **Тип инструмента (с интерфейсом или символьно-ориентированный)** | это сканер для обнаружения признаков взлома |
| **Место использования (сетевое устройство или компьютер)** | Пк |
| **Стоимость** | Нету точной сумы |
| **Описание ключевых особенностей и возможностей продукта или инструмента** | |
| Loki – это сканер для обнаружения признаков взлома.  Выявление взлома основано на четырех методах обнаружения:   1. Имена файлов (соответствие регулярному выражению полного пути файла); 2. Проверка правилами Yara (поиск на соответствие сигнатурам Yara по содержимому файлов и памяти процессов); 3. Проверка хешей (сравнение просканированных файлов с хешами (MD5, SHA1, SHA256) известных вредоносных файлов); 4. Проверка обратной связи C2 (сравнивает конечные точки технологического соединения с C2 IOC).   Дополнительные проверки:   1. Проверка файловой системы Regin (через **–reginfs**) 2. Проверка аномалии процесса 3. Сканирование распакованных SWF 4. Проверка дампа SAM 5. Проверка DoublePulsar — пытается выявить бэкдор DoublePulsar oна порту 445/tcp и 3389/tc | |
| **Справочные данные и ссылки** | |
| Kali linux: [сайт]. URL: <https://kali.tools/?p=3250>  softpedia: [сайт]. URL: <https://news.softpedia.com/news/elementary-os-0-4-loki-officially-released-it-s-based-on-ubuntu-16-04-lts-508147.shtml>  linux: [сайт]. URL: <https://www.linux.com/topic/desktop/elementary-os-loki-has-arrived/> | |

## 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?

Суть атак , это нанесения вреда устройствам, сетям, информациям, а также изменеи данных или сбор информации. Хотя количество угроз постоянно растет, появляются все новые и новые вирусы, увеличивается интенсивность и частота DDoS-атак, разработчики средств защиты информации тоже не стоят на месте. На каждую угрозу разрабатывается новое защитное ПО или совершенствуется уже имеющееся. Среди средств информационной защиты можно выделить:

* **Физические средства защиты информации.** К ним относятся ограничение или полный запрет доступа посторонних лиц на территорию, пропускные пункты, оснащенные специальными системами. Большое распространение получили HID-карты для контроля доступа. Например, при внедрении этой системы, пройти в серверную или другое важное подразделение компании могут лишь те, кому такой доступ предоставлен по протоколу.
* **Базовые средства защиты электронной информации**. Это незаменимый компонент обеспечения информационной безопасности компании. К ним относятся многочисленные антивирусные программы, а также системы фильтрации электронной почты, защищающие пользователя от нежелательной или подозрительной корреспонденции. Корпоративные почтовые ящики обязательно должны быть оборудованы такими системами. Кроме того, необходима организация дифференцированного доступа к информации и систематическая смена паролей.
* **Анти-DDoS**. Грамотная защита от DDoS-атак собственными силами невозможна. Многие разработчики программного обеспечения предлагают услугу анти-DDoS, которая способна защитить от подобных нападений. Как только в системе обнаруживается трафик необычного типа или качества, активируется система защиты, выявляющая и блокирующая вредный трафик. При этом бизнес-трафик поступает беспрепятственно. Система способна срабатывать неограниченное количество раз, до тех пор, пока угроза не будет полностью устранена.
* **Резервное копирование данных**. Это решение, подразумевающее хранение важной информации не только на конкретном компьютере, но и на других устройствах: внешнем носителе или сервере. В последнее время особенно актуальной стала услуга удаленного хранения различной информации в «облаке» дата-центров. Именно такое копирование способно защитить компанию в случае чрезвычайной ситуации, например, при изъятии сервера органами власти. Создать резервную копию и восстановить данные можно в любое удобное для пользователя время, в любой географической точке.
* План аварийного восстановления данных. Крайняя мера защиты информации после потери данных. Такой план необходим каждой компании для того, чтобы в максимально сжатые сроки устранить риск простоя и обеспечить непрерывность бизнес-процессов. Если компания по каким-то причинам не может получить доступ к своим информационным ресурсам, наличие такого плана поможет сократить время на восстановление информационной системы и подготовки ее к работе. В нем обязательно должна быть предусмотрена возможность введения аварийного режима работы на период сбоя, а также все действия, которые должны быть предприняты после восстановления данных. Сам процесс восстановления следует максимально отработать с учетом всех изменений системы.
* **Шифрование данных** при передаче информации в электронном формате (end-to-end protection). Чтобы обеспечить конфиденциальность информации при ее передаче в электронном формате применяются различные виды шифрования. Шифрование дает возможность подтвердить подлинность передаваемой информации, защитить ее при хранении на открытых носителях, защитить ПО и другие информационные ресурсы компании от несанкционированного копирования и использования.

1. 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?

Множество таких атак на банки организация приписывает двум хакерским группировкам: Cobalt (также известна как Carbanak и FIN7) и Silence. По данным FinCERT, Cobalt нанесла ущерб российской финансовой сфере минимум на 44 млн руб., а Silence – на 14,4 млн руб. Впрочем, это во много раз меньше, чем в 2017 г., отмечается в отчете. В 2017 г. ущерб от атак с использованием программ Cobalt Strike превысил 1 млрд руб.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

\_\_\_\_Всю информацию закидывать на облако, чтобы в разе выявления вируса на пк , данные не стерлись, и не были использовани в плохих целях. Также использую антивирус.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_