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.

Фишинг, DoS, DDoS, IP-спуфин, SQL-инъекция,

Шаг 2: Заполните следующую форму по выбранной сетевой атаке.

Название атаки	
Тип атаки	DDoS-атака
Даты проведения атак	Июнь 2020
Пострадавшие компьютеры/организации	Владельцы технологии "Умный дом"
Принцип действия и результаты	
Эта атака достигла значения почти 780 Гбыт/сек. Именно она стала причиной кратковременного отключения 15% всего мирового интернета ы ряда магистральных провайдеров. Источником атак этого типа была сеть скомпрометированых устройств «Умного дома». При этом, в большинстве случаев, доступ к этим устройствам происходил путём взлома паролей.	

Варианты нейтрализации
Более надежные пароли
Справочные данные и ссылки
https://www.ukrinform.ua/rubric-technology/3065103-centr-z-kiberbezpeki-pri-rnbo-viaviv-novij-tip-ddosatak.html
Графики и иллюстрации (включают ссылки на файл PowerPoint или веб-сайты)

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.

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

Наименование инструмента	Barracuda Essentials
Разработчик	
Тип инструмента (с интерфейсом или символьно-ориентированный)	С интерфейсом
Место использования (сетевое устройство или компьютер)	Компъютер. Разветвление: облако, перенаправление записи MX
Стоимость	2,63 доллара США за пользователя в месяц (минимум 10 пользователей)
Описание ключевых особенностей и возможностей продукта или инструмента	

С помощью "Cloud" (облачного) резервного копирования вы можете защитить свои файлы от удаления или повреждения и восстановить каждый из них без проблем. Его надёжная технология шифрования и предотвращения утечек обеспечивает абсолютную безопасность ваших конфиденциальных данных. Входящие фильтры обнаруживают и обеззараживают каждое письмо перед его доставкой для защиты от угроз.
В Barracuda используются такие технологии, как сканирование на вирусы, анализ в реальном времени, оценка спама, проверка репутации, предотвращение ссылок на URL-адреса и т.д., что обеспечивает наилучшую защиту. Круглосуточный глобальный операционный центр по борьбе с угрозами - Barracuda Central постоянно отслеживает новые уязвимости и внедряет технологии фильтрации.[1]

Справочные данные и ссылки
1.https://www.expertinsights.com/reviews/barracuda-essentials

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 узнать конфиденциальную информацию. Например, пароли или счета банковских карт. Обеспечить работников качественным ПО, которое будет фильтровать подозрительные письма. Также провести инструктаж сотрудникам.Чтобы те не переходили по подозрительным ссылкам и в рабочее время не занимались личными делам. Чтобы не оставляли включенную технику, на которой хранится конфиденциальная информация.

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?

   Вовремя атаки випуса Петя ущерб понесли многие компании, в частности бухглтерский отдел. Почти 150 стратегических для экономики страны предприятий, сети которых подключены и контролируются специалистами Государственной службы спецсвязи, в том числе АЭС, а также предприятия, связанные с обеспечением безопасности государства, не пострадали

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

   Установить защитное ПО, не переходить по подозрительным сайтам, не открывать вложенные документы от неизвестных источников, установить дополнительные фильтры на почте и браузерах, использовать надежные пароли и неипользовать один пароль для всех аккаунтов не оставлять включенным ноутбук/компьютер в открытом доступе, если на нем хранится конфиденциальная информация

