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.

Фрагментация данны,Ping flooding,DNS spoofing,IP spoofing

Шаг 2: Заполните следующую форму по выбранной сетевой атаке.

Название атаки	Password attacks
Тип атаки	Атака Password attacks
Даты проведения атак	11 июля 2011
Пострадавшие компьютеры/организации	Booz Allen Hamilton
Принцип действия и результаты	
Большой американской консалтинговой фирмы, выполняющей существенный объём работ для Пентагона, были взломаны Anonymous`ом и подверглись утечке в один день. «Утечка, названная 'Военный Кризисный Понедельник' включает 90 000 логинов военнослужащих, в том числе сотрудников Центрального командования США, командования специальных операций США, морской пехоты, различных объектов ВВС, Национальной безопасности, Государственного департамента по персоналу, и, похоже, частных подрядчиков сектора». Эти пароли были захешированы с помощью SHA-1, и позже были расшифрованы и проанализированы командой ADC в Imperva, подтверждая, что даже военнослужащие используют ярлыки и способы обойти требования к паролям.	

Варианты нейтрализации
Хорошая защита к доступам к ресурсов
Справочные данные и ссылки
https://www.cnews.ru/reviews/free/security/part7/net_attack.shtml https://ru.wikipedia.org/wiki/%D0%92%D0%B7%D0%BB%D0%BE%D0%BC_%D0%BF%D0%B0%D1%80%D0%BE%D0%BB%D1%8F
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.

анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС

оценка текущего уровня защищенности ИС;

локализация узких мест в системе защиты ИС;

оценка соответствия ИС существующим стандартам в области информационной безопасности;

выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

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

Наименование инструмента	Bitdefender
Разработчик	Bitdefender SRL
Тип инструмента (с интерфейсом или символьно-ориентированный)	С интерфейсом
Место использования (сетевое устройство или компьютер)	Компьютер,мобильных устройств на базе iOS и Android
Стоимость	от 331грн до 787 грн
Описание ключевых особенностей и возможностей продукта или инструмента	
румынская компания, разрабатывающая и выпускающая антивирусы, файрволы и антиспамовые решения. Компания предлагает свои решения самому широкому кругу клиентов. Программные продукты компании доступны для различных операционных систем, включая Microsoft Windows, различные дистрибутивы Linux и FreeBSD. А также мобильных устройств на базе iOS и Android — как для пользователей, так и для корпоративной защиты BYOD. Антивирусная защита для виртуальной инфраструктуры поддерживает практически любые платформы виртуализации: VmWare, HyperV, Citrix, Linux, Nutanix, KVM, Red Hat и пр.	

Справочные данные и ссылки
https://ru.wikipedia.org/wiki/Bitdefender

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?

   _внедрение мер безопасности и противодействия для устранения уязвимостей и предотвращения угроз

   формирование финансовых резервов в случае, если стоимость реализации мер безопасности превышает

   отказ от чрезмерно рисковой деятельности_____

   _____

   _____

   _____

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?

   _Нет_____

   _____

   _____

   _____

   _____

   _____

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

   _Такие меры защиты:_____

   _Укрепление шифрования_____

   _Защита аккаунтов_____

   _Использоватние особой защиту_____

   _Смотреть что скачиваешь и на что соглашаешься_____

   _____

