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, переполнение буфера, черви, IP-спуфинг

Шаг 2: Заполните следующую форму по выбранной сетевой атаке.

Название атаки	
Тип атаки	Фишинг
Даты проведения атак	09.07.2018
Пострадавшие компьютеры/организации	Hola VPN, MyEtherWallet
Принцип действия и результаты	
9-го июля в Twitter компания MyEtherWallet сообщила о том, что вирус «распространялся примерно 5 часов» и попросила пользователей расширения «немедленно перевести средства на новый счет». Представители Hola VPN пояснили, что у них была украдена учетная запись в Google Chrome Store, и хакеры смогли распространить зараженную версию расширения. При попытке зайти на официальный сайт кошелька MyEtherWallet, жертвы направлялись на фишинговую страницу. Если пользователь вводил свой пароль, то хакеры получали доступ к криптовалютным активам жертвы.	

Варианты нейтрализации
Система безопасности должна быть на высоте
Справочные данные и ссылки
https://bitnovosti.com/2018/07/31/myetherwallet-stal-samym-populyarnym-koshelkom-sredi-fisherov/ https://bitnovosti.com/2018/07/11/hakery-vzlomali-hola-vpn-i-atakovali-prilozhenie-myetherwallet/
Графики и иллюстрации (включают ссылки на файл PowerPoint или веб-сайты)
https://bitnovosti.com/wp-content/uploads/2018/07/Screen-Shot-2018-07-11-at-13.43.17.png

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.

Атаки, основанные исключительно на социальной инженерии и бизнес-транзакциях, могут быть совершены даже с помощью простой учетной записи электронной почты от обычного поставщика без каких-либо дополнительных инструментов.

Обычно спам-письмо отправляется клиенту какой-либо организации, оно содержит гиперссылку, которая якобы ссылается на абсолютно безобидный сайт. Однако гиперссылка указывает на IP-адрес вместо имени домена. Когда пользователь нажимает на ссылку, его трафик перенаправляется на вредоносный веб-сайт, который идентичен оригиналу.

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

Наименование инструмента	Microsoft Defender
Разработчик	Microsoft
Тип инструмента (с интерфейсом или символьно-ориентированный)	С интерфейсом
Место использования (сетевое устройство или компьютер)	Компьютер
Стоимость	Входит в стоимость самой ОС(Windows 10 стоит 3500грн)
Описание ключевых особенностей и возможностей продукта или инструмента	
В Microsoft Defender входит ряд модулей безопасности, отслеживающих подозрительные изменения в определённых сегментах системы в режиме реального времени. Также программа позволяет быстро удалять установленные приложения ActiveX. С помощью доступа к сети Microsoft SpyNet есть возможность отправлять сообщения о подозрительных объектах в Microsoft для определения его возможной принадлежности к spyware.	

Справочные данные и ссылки
https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D1%89%D0%B8%D1%82%D0%BD%D0%B8%D0%BA_Windows

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?

   Во первых , сами сотрудникик компаний должны понимать всю ответственность своей работы и не разглашать конфиденциальную информацию.
   Во вторых, не использовать пиратское ПО.
   И в заключение можно сказать, нужно следить за совладельцами организации.

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?

   Да приходилось, работая в техникуме лаборантом(находится на заводе "Антонов"), во время угрозы "Петя" на сам завод, техникум так же пострадал. Ущерба у техникума не было. Только не работоспособность системы примерно 1.5 недели.

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

   Нужно обезательно смотреть куда и что отправляешь, не переходить на подозрительные сайты и ссылки, установка лицензированого антивируса, и не быть наивными, ибо в большенстве случаев мы виноваты сами.

