**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.

* DoS
* Фишинг
* Рекламное ПО
* Руткиты

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

|  |  |
| --- | --- |
| **Название атаки** | **Petya** |
| **Тип атаки** | Сетевой червь |
| **Даты проведения атак** | Март 2016, лето 2017 |
| **Пострадавшие компьютеры/ организации** | «Хоум Кредит», «Роснефть», энергетические компании, украинские банки, аэропорт Харькова |
| **Принцип действия и результаты** | |
| Программа шифрует файлы на жёстком диске компьютера-жертвы, а также перезаписывает и шифрует MBR — данные, необходимые для загрузки операционной системы. В результате все хранящиеся на компьютере файлы становятся недоступными. Затем программа требует денежный выкуп в биткойнах за расшифровку и восстановление доступа к файлам. | |
| **Варианты нейтрализации** | |
| Petya проверяет наличие файла perfc.dat, находящегося в системной папке только для чтения. Если он обнаружит этот файл, то не будет запускать шифрование программного обеспечения и информации. | |

**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.

* esCLOUD
* METASCAN
* ScanMyServer

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

|  |  |
| --- | --- |
| **Наименование инструмента** | esCLOUD |
| **Разработчик** | eSentire |
| **Тип инструмента (с интерфейсом или символьно-ориентированный)** | С интерфейсом |
| **Место использования (сетевое устройство или компьютер)** | компьютер |