**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.

Атака IP spoofing, sniffing (прослушивание канала), нестандартные протоколы, инкапсулированные в IP.

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

|  |  |
| --- | --- |
| **Название атаки** | IP spoofing |
| **Тип атаки** | Подмена исходного IP-адреса |
| **Даты проведения атак** | 2001 г. |
| **Пострадавшие компьютеры/ организации** | 1. Хакерам удалось зарегистрировать подставной домен pаypal.com (xn--pypal-4ve.com в Punycode), где первая буква а — кириллическая. Благодаря публикации на Slashdot.org к проблеме было привлечено внимание общественности, после чего как браузеры, так и администраторы многих доменов верхнего уровня выработали и реализовали контрмеры. 2. Microsoft Security Advisory (2718704) — Unauthorized Digital Certificates Could Allow Spoofing. Довольно интересная вещь была найдена в экземплярах нашумевшего шпионского бота Flamer: по результатам реверс-инжиниринга компонентов этого зловреда был обнаружен участок кода, отвечающий за проведение спуфинг-атак типа фишинг. Имитируя предоставление оригинальных сертификатов крупных компаний, бот проводил MITM-атаку, целью которой был перехват персональных данных пользователей корпоративной сети с последующей отправкой на сервер разработчиков. Этот спуфинг-инцидент получил Security Advisory #2718704 с рангом опасности High. |
| **Принцип действия и результаты** | |
| IP-спуфинг происходит, когда злоумышленник, находящийся внутри корпорации или вне ее выдает себя за санкционированного пользователя. Это можно сделать двумя способами. Во-первых, злоумышленник может воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или авторизованным внешним адресом, которому разрешается доступ к определенным сетевым ресурсам. Атаки IP-спуфинга часто являются отправной точкой для прочих атак. Классический пример - атака DoS, которая начинается с чужого адреса, скрывающего истинную личность злоумышленника. Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами. Для двусторонней связи злоумышленник должен изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Некоторые злоумышленники, однако, даже не пытаются получить ответ от приложений. Если главная задача состоит в получении от системы важного файла, ответы приложений не имеют значения. | |
| **Варианты нейтрализации** | |
| Угрозу спуфинга можно ослабить (но не устранить) с помощью следующих мер: Контроль доступа. Самый простой способ предотвращения IP-спуфинга состоит в правильной настройке управления доступом. Чтобы снизить эффективность IP-спуфигна, настройте контроль доступа на отсечение любого трафика, поступающего из внешней сети с исходным адресом, который должен располагаться внутри вашей сети. Если санкционированными являются и некоторые адреса внешней сети, данный метод становится неэффективным. Фильтрация RFC 2827. Вы можете пресечь попытки спуфинга чужих сетей пользователями вашей сети (и стать добропорядочным "сетевым гражданином"). Для этого необходимо отбраковывать любой исходящий трафик, исходный адрес которого не является одним из IP-адресов вашей организации. Этот тип фильтрации, известный под названием "RFC 2827", может выполнять и провайдер. В результате отбраковывается весь трафик, который не имеет исходного адреса, ожидаемого на определенном интерфейсе. Использование криптографической аутентификации. | |
| **Справочные данные и ссылки** | |
| 1. Боршевников, А. Е. Сетевые атаки. Виды. Способы борьбы / А. Е. Боршевников. — Текст : непосредственный // Современные тенденции технических наук : материалы I Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). — Уфа : Лето, 2011. — С. 8-13. — URL: https://moluch.ru/conf/tech/archive/5/1115/ (дата обращения: 29.09.2020); 2. Актуальные методы спуфинга в наши дни [Електронний ресурс] // Журнал "Хакер". – 2013. – Режим доступу до ресурсу: https://xakep.ru/2013/10/16/relevant-spuffing/ | |

**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.

ADManager Plus (ManageEngine), Lynis — auditing system hardening testing

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

|  |  |
| --- | --- |
| **Наименование инструмента** | Lynis — auditing system hardening testing |
| **Разработчик** | Майкл Боэлен CISOfy |
| **Тип инструмента (с интерфейсом или символьно-ориентированный)** | Символьно-ориентированный |
| **Место использования (сетевое устройство или компьютер)** |  |
| **Стоимость** | Есть и бесплатная и платная версия |
| **Описание ключевых особенностей и возможностей продукта или инструмента** | |
| Утилита сканирует настройки текущего уровня безопасности и определяет состояние защищенности (hardening state) хоста. Найденные тревожные сигналы и важные алерты безопасности, сгруппированные по блокам, выводятся в консоль терминала и отдельно в файл отчета. Кроме сведений о безопасности, Lynis также поможет получить общую информацию о системе, информацию об установленных пакетах и возможных ошибках конфигурации, обновлениях ядра и т.п. | |
| **Справочные данные и ссылки** | |
| Лучшие инструменты аудита безопасности Linux [Електронний ресурс] // SPY-SOFT.NET – Режим доступу до ресурсу: <https://spy-soft.net/linux-hardening-tools/>;  КАКИЕ ПРОГРАММЫ ПОДОЙДУТ ДЛЯ АУДИТА БЕЗОПАСНОСТИ WINDOWS [Електронний ресурс] // ИТ для бизнеса. – 2019. – Режим доступу до ресурсу: https://itfb.com.ua/kakie-programmy-podojdut-dlya-audita-bezopasnosti-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?

Сетевая атака - действие, целью которого является захват контроля (повышение прав) над удалённой/локальной вычислительной системой, либо её дестабилизация, либо отказ в обслуживании, а также получение данных пользователей пользующихся этой удалённой/локальной вычислительной системой.

Ключевые шаги для защиты сетей и ресурсов:

1. Физические средства защиты информации.
2. Базовые средства защиты электронной информации.
3. Резервное копирование данных.
4. План аварийного восстановления данных.
5. Шифрование данных при передаче информации в электронном формате (end-to-end protection).
6. 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 былипредприняты в этой ситуации?

-

1. Какие меры вы можете предпринять для защиты собственного компьютера или ноутбука?
2. Базовые средства защиты электронной информации.
3. Резервное копирование данных.
4. План аварийного восстановления данных.