Частное учреждение образования

Колледж бизнеса и права

|  |
| --- |
| УТВЕРЖДАЮ  Ведущий методист колледжа  \_\_\_\_\_\_\_\_\_\_\_Е.В. Паскал  «\_\_\_» 2023 |
| Специальность: 2-40 01 01 «Программное обеспечение информационных технологий» | Учебная дисциплина: «Защита компьютерной информации» | |

# Лабораторная работа №19

Инструкционно-технологическая карта

Тема: применение ПС внутреннего и внешнего аудита сетей.

Цель: научить применять ПС внутреннего и внешнего аудита сетей, научиться обеспечивать более эффективный и точный аудит сетевой инфраструктуры, снижать риски инцидентов в будущем.

Время выполнения: 2 часа.

СОДЕРЖАНИЕ РАБОТЫ

1. Теоретические сведения для выполнения работы
2. Практические задания
3. Контрольные вопросы
4. Литература
5. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ДЛЯ ВЫПОЛНЕНИЯ РАБОТЫ

## Водная информация

Тема "Аудиты сетей" относится к области информационной безопасности и является одним из ключевых направлений в работе специалистов службы безопасности, занимающихся обеспечением безопасности информационных систем и сетей. В современных условиях, когда информационные технологии занимают все более важное место в жизни людей и функционировании бизнеса, безопасность информационных систем и сетей становится все более важным.

Применение ПС (программных средств) внутреннего и внешнего аудита сетей — это один из важных инструментов для обеспечения безопасности и эффективности работы информационных систем и сетей.

Внутренний аудит — это процесс, который проводит внутренний аудитор организации для проверки соответствия деятельности организации установленным правилам, процедурам и стандартам, а также для обнаружения и устранения возможных нарушений в системе безопасности.

Внешние аудиты сетей — это процесс проверки безопасности компьютерных сетей и систем, проводимый компаниями, которые специализируются на предоставлении таких услуг. Внешние аудиты могут выполняться в целях оценки уровня безопасности сети, выявления уязвимостей, а также для проверки соответствия стандартам безопасности и законодательству в области информационной безопасности.

Применение ПС внутреннего и внешнего аудита сетей позволяет автоматизировать процесс сбора, анализа и отчетности по результатам проверок, что повышает эффективность аудита и сокращает время, затрачиваемое на выполнение процедур. При этом необходимо учитывать ограничения безопасности и принимать меры для защиты конфиденциальности и целостности данных.

Использование ПС внутреннего и внешнего аудита сетей помогает выявлять уязвимости и нарушения безопасности в информационных системах и сетях, что позволяет принимать своевременные меры по устранению этих проблем и повышению общего уровня безопасности информационных технологий. Кроме того, использование ПС позволяет оптимизировать процессы внутреннего и внешнего аудита, сокращая время на выполнение процедур и повышая точность и объективность анализа.

Nmap (Network Mapper) – это мощный инструмент сканирования сети, который используется для исследования и анализа устройств, подключенных к сети. Он предоставляет информацию о портах, сервисах, операционных системах и других характеристиках сетевых узлов. Nmap является одним из наиболее популярных инструментов для сканирования сети и широко применяется в области информационной безопасности.

Некоторые основные возможности Nmap включают:

* Определение активных узлов в сети.
* Определение открытых портов и протоколов, работающих на узлах.
* Определение используемой операционной системы.
* Определение версий сервисов, запущенных на узлах.
* Определение наличия фильтров брандмауэра и прокси-серверов.

Zenmap – это графический интерфейс (GUI) для Nmap, созданный с целью упростить использование Nmap для пользователей с минимальными навыками командной строки. Он предоставляет более интуитивный способ взаимодействия с Nmap и позволяет визуализировать результаты сканирования сети.

Некоторые основные возможности Zenmap включают:

* Графическое представление результатов сканирования в виде карты сети.
* Упрощенная настройка и запуск сканирования.
* Просмотр результатов сканирования в удобочитаемом формате.
* Возможность фильтрации и поиска результатов.

Основная разница между Nmap и Zenmap заключается в их интерфейсах. Nmap является инструментом командной строки и предоставляет расширенные возможности для сканирования и анализа сети. Zenmap, с другой стороны, представляет собой графический интерфейс для Nmap, который облегчает использование инструмента и визуализацию результатов. Важно отметить, что оба инструмента используют один и тот же движок сканирования и обеспечивают схожий функционал, просто предоставляя разные способы взаимодействия с ним.

Статусы портов:

1. *Открыт (Open)*: Статус "открыт" указывает на то, что порт открыт и прослушивает подключения. Это означает, что на данном порту находится активный сервис или приложение, готовые принимать входящие соединения. Если порт отмечен как "открыт", это может указывать на наличие работающего сервиса на этом порту.

2. *Закрыт (Closed)*: Статус "закрыт" означает, что порт закрыт и не прослушивает подключения. Это указывает на отсутствие активного сервиса или приложения на данном порту, и попытка подключения к нему может привести к получению сообщения об ошибке или отказу в соединении.

3. *Фильтрован (Filtered)*: Статус "фильтрован" указывает на то, что порт фильтрован, что означает, что невозможно получить точный ответ или определить его состояние из-за наличия фильтрации или блокировки. Это может быть вызвано использованием брандмауэров, межсетевых экранов или других средств сетевой безопасности. Порты, помеченные как "фильтрован", могут быть доступными, но сканирование не предоставляет информации о их точном состоянии.

4. *Открытый-фильтрованный (Open|Filtered)*: Этот статус указывает на то, что сканирование не может однозначно определить состояние порта из-за наличия фильтрации или блокировки, но есть признаки того, что порт может быть открытым. В некоторых случаях это может произойти из-за конфигурации сетевого оборудования или настроек брандмауэра, которые могут препятствовать полному определению состояния порта. Такой статус может указывать на наличие активного сервиса на порту, но существует некоторая форма фильтрации или блокировки, которая влияет на точную классификацию порта.

5. *Закрытый-фильтрованный (Closed|Filtered)*: Этот статус указывает на то, что сканирование не может однозначно определить состояние порта из-за наличия фильтрации или блокировки, но есть признаки того, что порт скорее всего закрыт. В таком случае может быть применена фильтрация на уровне сетевого оборудования или брандмауэра, которая блокирует соединения на этом порту. Хотя точное состояние порта не может быть определено, сканирование указывает на то, что порт не прослушивает соединения и вероятно закрыт.

Сервисы портов (или "приложения") относятся к программным приложениям, которые работают на определенных портах сетевого устройства (например, компьютера или маршрутизатора). Когда клиентское устройство пытается подключиться к определенному порту, серверное устройство, работающее на этом порту, отвечает на соединение и предоставляет соответствующий сервис.

Вот несколько примеров наиболее распространенных сервисов портов и их назначения:

* FTP (File Transfer Protocol): Этот сервис используется для передачи файлов между компьютерами в сети. Порт по умолчанию - 21.
* SSH (Secure Shell): Этот сервис обеспечивает защищенное удаленное управление компьютером через интернет. Порт по умолчанию - 22.
* HTTP (Hypertext Transfer Protocol): Этот сервис используется для передачи веб-страниц и другого веб-контента. Порт по умолчанию - 80.
* HTTPS (Hypertext Transfer Protocol Secure): Этот сервис обеспечивает защищенную передачу веб-страниц и другого веб-контента. Порт по умолчанию - 443.
* DNS (Domain Name System): Этот сервис используется для преобразования доменных имен в IP-адреса и наоборот. Порт по умолчанию - 53.
* SMTP (Simple Mail Transfer Protocol): Этот сервис используется для отправки и получения электронной почты. Порт по умолчанию - 25.
* POP3 (Post Office Protocol version 3): Этот сервис используется для получения электронной почты с сервера. Порт по умолчанию - 110.
* IMAP (Internet Message Access Protocol): Этот сервис используется для получения электронной почты с сервера, но в отличие от POP3 сохраняет копии писем на сервере. Порт по умолчанию - 143.

Знание сервисов портов может помочь администраторам сети понимать, какие программы и сервисы работают на конкретных портах, а также определять и устранять проблемы в сети. Это также может помочь в обеспечении безопасности сети, поскольку знание сервисов портов может позволить определить, какие порты должны быть закрыты или ограничены для доступа из внешней сети.

**Как уставить nmap?**

Установщик по ссылке [здесь](https://nmap.org/download). Рекомендуется следовать рекомендованным настройкам. После установки, у вас будет возможность пользоваться графической утилитой Zenmap или nmap, через консоль.

Чтоб бы вызвать консоль надо: нажать сочетание клавиш win + r и написать в поле “cmd”. Откроется консоль, и вы можете вводить команды.

**Как работать и задавать команды для выполнения работы?**

Для того чтоб запускать nmap, надо: ключевое слово nmap, для запуска программы, опции (если нужны), и домен (важно, что просто домен, без URL).

Знак "-" (минус) перед опцией в командной строке является соглашением для указания опций и их значений. В контексте утилиты командной строки, такой как Nmap, использование знака "-" перед опцией обозначает, что следующий за ним символ или символы являются опцией.

Шаблон любой команды: nmap (обязательно, почти всегда) + опции, как пример это -A и или - p + что сканировать.

Описание опций ниже:

* nmap -p хост или диапазон IP – сканирование конкретного порта.
* nmap -p- номер порта и целевой хост или диапазон IP - сканирование всех портов.
* nmap -F хост или диапазон IP - сканирование наиболее распространенных портов.
* nmap -O хост - определение операционной системы целевого хоста.
* nmap -v хост или диапазон IP - вывод подробной информации о сканировании.
* *nmap -oN имя\_файла хост или диапазон IP – сохранение результатов сканирования в файл*.
* nmap -sS хост (TCP SYN сканирование)– это сканирование, которое проверяет, открыт ли порт, отправляя TCP SYN-пакеты.
* nmap -sU хост (UDP сканирование)– это сканирование, которое проверяет, открыт ли порт, отправляя TCP SYN-пакеты, ус.
* nmap -T4 хост – эта опция обозначает скорость сканирования, которая может влиять на скорость с увеличением, но может вызвать сетевые ошибки, работает в следующем диапазоне от Т0 – Т5.
* nmap localhost-x – где x это целое число и является диапазоном IP, которые вы хотите просканировать.
* nmap 192.168.0.0/24 - указывает, что должна быть сканирована вся подсеть с префиксом 192.168.0.0 и длиной префикса 24 бита.
* nmap -sV -p- хост - используя опцию -sV для определения версий сервисов и -p- для сканирования всех портов.

Примеры команд:

* nmap -T4 -A -v localhost
* nmap -sS -sU -T4 -A -v localhost
* nmap -T4 -F localhost
* nmap localhost
* nmap 192.168.0.1-100

1. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

Все нижеперечисленные задания сохранять всё в файлы и при сдаче лабораторной работы показывать файлы с готовым заданием.

Задание 1.

Используя локальное устройство, сканировать все порты своего устройства и результаты сохранить в файл.

Задание 2.

Цель задания, проанализировать сайты в соответствии вашему варианту.

В анализ входит: найти наиболее вероятный ОС хоста, все популярные порты и их статусы, IP-адрес сервера, определить маршрут следования от вашего ПК и до сервера.

|  |  |
| --- | --- |
| Вариант | Сайт |
| 1 | <https://kbp.by> |
| 2 | <https://otdelka.by> |
| 3 | <https://www.slivki.by> |
| 4 | <https://sila.by> |
| 5 | <https://mila.by> |
| 6 | <https://ostrov-shop.by> |
| 7 | <https://myfin.by> |

Задание 3.

Задайте команду в соответствии со словесной задачей по данным вариантам ниже. Выполнить полученную команду и записать информацию и команду из описания команд в отчет.

|  |  |
| --- | --- |
| Вариант | Описание команд |
| 1 | Скорость 3, локальную машину, более подробно |
| 2 | Хост (как пример можно взять любой домен), узнать ОС, использовать TCP сканирование |
| 3 | Скорость 2, используя более подробное сканирование |
| 4 | Сканировать наиболее популярные порты, узнать ОС |
| 5 | Узнать версию ОС, сохранить в файл |
| 6 | Сохранить в файл |
| 7 | Сканирование, которое проверяет, открыт ли порт |

Пример кода, который может получиться: nmap -A -T4 -oN lab19 localhost

Задание 4.

Выполнить поиск нужного сайта, зная адрес (79.137.197.141) и диапазон портов, сказанный в варианте ниже.

Исходя из данных, вам данных узнать:

* статусы самых популярных портов (используя специальную команду);
* версию ОС;
* предоставить страничку на порте;
* узнать по указанному диапазону портов, открытый порт и узнать какой там сервис.

|  |  |
| --- | --- |
| Варианты | Диапазон портов |
| 1 | с 43120 до 47653 |
| 2 | с 47234 до 50123 |
| 3 | с 50021 до 53122 |
| 4 | с 60000 до 64000 |
| 5 | с 60020 до 63300 |

1. КОНТРОЛЬНЫЕ ВОПРОСЫ:
2. Какие бывают статусы портов, опишите каждый из них?
3. Что такое сервисы и что они показывают?
4. Что такое Zenmap и для чего он нужен?
5. Что такое Nmap и для чего нужен?
6. Что можно исследовать и изучать с помощью Nmap?
7. Что такое внутренние и внешние аудиты сетей?
8. Для чего нужны закрытые порты и почему не могут быть только открытые порты?
9. HTTPS – что за он и для чего нужен?

4. ЛИТЕРАТУРА

1. Андресс Д. Защита данных. От авторизации до аудита – Питер, 2021.
2. Козлов С. Защита информации, устройства несанкционированного съема информации и борьба с ними - Академический проект, 2019.
3. М.В. Баранова и В.В. Кучеренко. Шифрование данных в информационных системах
4. А.А. Данилов, С.А. Копылова, И.В. Михайлов. Защита информации в компьютерных системах и сетях"

Преподаватель Д.А. Бунькевич

Рассмотрено на заседании цикловой комиссии

программного обеспечения информационных технологий

Протокол № \_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2023

Председатель ЦК \_\_\_\_\_\_\_\_\_\_\_ К.О.Якимович