**Конспект: Обеспечение безопасности локальной сети**

Обнаружение открытых на ПК портов утилитой Netstat

Шаг 1. Для выполнения практического задания на компьютере предлагается воспользоваться командой «Пуск-Выполнить».

Шаг 2. Откроется окно «Запуск программы», где необходимо ввести команду «cmd».

Шаг 3. Для отслеживания активных подключений TCP и прослушиваемых портов TCP/UDP используется команда «netstat». На экране отобразятся локальные адреса, представляющие компьютер пользователя, и информация о портах.

Виды состояний:

1. режим ESTABLISHED — соединения установлены т.е. сетевые службы работают (используются)
2. TIME\_WAIT - соединение ожидает разрыва

Шаг 4. При запуске браузера количество локальных адресов увеличится.

Команда netstat имеет следующие опции

|  |  |
| --- | --- |
| **Опция (ключ)** | **Назначение** |
| -a | Показывать состояние всех сокетов; обычно сокеты, используемые серверными процессами, не показываются. |
| -A | Показывать адреса любых управляющих блоков протокола, связанных с сокетами; используется для отладки. |
| -i | Показывать состояние автоматически сконфигурированных (auto- configured) интерфейсов. Интерфейсы, статически сконфигурированные в системе, но не найденные во время загрузки, не показываются |
| -n | Показывать сетевые адреса как числа. netstat обычно показывает адреса как символы. Эту опцию можно использовать с любым форматом показа. |
| -r | Показать таблицы маршрутизации. При использовании с опцией - s, показывает статистику маршрутизации. |
| -s | Показать статистическую информацию по протоколам. При использовании с опцией -r, показывает статистику маршрутизации |
| -f семейство\_адресов | Ограничить показ статистики или адресов управляющих блоков только указанным семейством\_адресов, в качестве которого можно указывать:  inet - Для семейства адресов AF\_INET,  unix - Для семейства адресов AF\_UNIX. |
| -I интерфейс | Выделить информацию об указанном интерфейсе в отдельный столбец; по умолчанию (для третьей формы команды) используется интерфейс с наибольшим объёмом переданной информации с момента последней перезагрузки системы. В качестве интерфейса можно указывать любой из интерфейсов, перечисленных в файле конфигурации системы, например, emd1 или lo0. |
| -p | Отобразить идентификатор/название процесса создавшего сокет (-p, --programs display PID/Program name for sockets) |

Программа NetStat Agent

Описание программы:

NetStat Agent представляет собой полезный инструментарий для мониторинга интернет-соединений и диагностики сети.

Функциональность программы:

1. Отслеживание соединений:
   1. NetStat: Мониторит TCP и UDP соединения на ПК, отображая географическое местоположение удаленного сервера и имя хоста.
2. Управление соединениями:
   1. Закрытие нежелательных соединений.
   2. Завершение процессов.
3. Конфигурация сетевых адаптеров:
   1. IPConfig: Отображает свойства сетевых адаптеров и конфигурацию сети.
4. Инструменты диагностики:
   1. Ping: Позволяет проверить доступность хоста в сети.
   2. TraceRoute: Определяет маршрут между компьютером и конечным хостом, отображая IP-адреса маршрутизаторов.
5. DNS и маршрутизация:
   1. DNS Query: Подключается к DNS серверу и предоставляет информацию о домене.
   2. Route: Отображает и позволяет изменять IP маршруты на ПК.
   3. ARP: Отслеживает изменения ARP в локальной таблице.
6. Дополнительные инструменты:
   1. Whois: Получение информации об IP-адресе или домене.
   2. HTTP Checker: Проверка доступности веб-сайтов.
7. Статистика:
   1. Statistics: Показывает статистику сетевых интерфейсов и TCP/IP протоколов.

NetStat Agent предоставляет всесторонний набор инструментов для анализа и управления сетевыми соединениями, а также для диагностики различных аспектов сетевой инфраструктуры.

Сканер портов Nmap (Zenmap)

Общая информация:

Nmap (Zenmap) - популярный сканер портов, применяемый для обследования сети и проведения аудита защиты.

Использовался в фильме "Матрица: Перезагрузка" при взломе компьютера.

Цель использования Nmap:

Задача - не взломать, а защитить ПК.

Функциональность Nmap (Zenmap):

Сканирование портов:

1. Nmap позволяет определить открытые порты компьютера.

Безопасность сети:

1. Рекомендуется закрыть доступ к открытым портам с помощью брандмауэра для обеспечения безопасности сети.

Безопасность и защита:

Подчеркивается, что инструмент можно использовать как для защиты, так и для нападения.

Рекомендация - использовать Nmap для определения открытых портов и дальнейшего закрытия их доступа с помощью брандмауэра.

Интерфейс Zenmap:

Zenmap - графический интерфейс для Nmap, что упрощает визуализацию результатов сканирования и управление параметрами.

Nmap (Zenmap) - мощный инструмент для обследования сетей, выявления открытых портов, и аудита защиты. Рекомендуется использовать его в целях защиты, закрывая доступ к выявленным уязвимым точкам сети.

**Использование Nmap и TCPView для мониторинга и защиты сети**

Nmap для сканирования портов компьютера:

* Команда: nmap –p1-65535 IP-адрес\_компьютера
* Альтернативная команда: nmap –sV IP-адрес\_компьютера
* Для сканирования сайта: nmap –sS –sV –O -P0 адрес\_сайта

TCPView - монитор портов:

* Показывает все процессы, использующие интернет-соединения.
* Позволяет узнать, какой порт открыт, и какое приложение его использует.
* Можно мгновенно разорвать соединение при необходимости.

Процедура мониторинга сетевых подключений с TCPView:

* Запустить TCPView для просмотра активных сетевых подключений локального ПК.
* Определить потенциальные угрозы, выявив открытые порты и приложения, использующие их.

Защита от угроз:

* При необходимости, закрыть установленное приложением TCP-соединение или процесс.
* Это позволяет реагировать на потенциальные угрозы и управлять сетевыми подключениями.

Nmap используется для сканирования портов и выявления потенциальных уязвимостей в сети.

TCPView предоставляет визуальный мониторинг активных сетевых подключений, что облегчает обнаружение и реагирование на возможные угрозы.

**Образец офисной политики безопасности:**

*Цель: Обеспечение конфиденциальности, целостности и доступности информации в предприятии.*

1. **Установка программного обеспечения:**
   * Пользователям запрещается устанавливать программное обеспечение на компьютерах и в сети Компании без предварительного разрешения системного администратора.
2. **Электронная почта:**
   * Пользователи не имеют право пересылать электронную почту другим лицам и организациям без явного разрешения отправителя.
3. **Обработка файлов:**
   * Запрещается изменять и копировать файлы, принадлежащие другим пользователям, без предварительного разрешения владельцев файлов.
4. **Управление паролями:**
   * Пользователь несет ответственность за сохранность своих паролей для входа в систему.
   * Запрещается распечатывать, хранить в сети или передавать другим лицам индивидуальные пароли.
5. **Физическая безопасность:**
   * Запрещается оставлять компьютеры в разблокированном состоянии при отсутствии пользователя.
6. **Обнаружение и уведомление о нарушениях:**
   * Пользователям следует немедленно уведомлять системного администратора о любых подозрительных событиях или нарушениях безопасности.
7. **Использование устройств хранения данных:**
   * Переносные устройства хранения данных, такие как флеш-накопители, должны быть предварительно проверены системным администратором перед использованием в компьютерах компании.
8. **Обучение и осведомленность:**
   * Пользователи обязаны пройти обучение по вопросам информационной безопасности и регулярно обновлять свои знания.
9. **Соблюдение законодательства:**
   * Все пользователи обязаны соблюдать действующее законодательство в области информационной безопасности.
10. **Ответственность:**
    * За нарушение политики информационной безопасности могут предусматриваться дисциплинарные меры, включая увольнение или юридическая ответственность в случае утраты или утечки конфиденциальной информации.

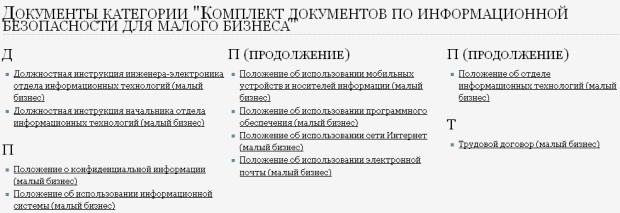


Рисунок 1 - Список документов по информационной безопасности для малого бизнеса