### **Задание 5 – Защита информации при работе с каналами связи.**

Необходимо установить и настроить межсетевой экран (фаервол), средства анализа сетевого трафика, шифрованный канал передачи данных (с использованием OpenVPN или аналога) и цифровую подпись для обеспечения подлинности информации. Работа выполняется на виртуальной машине (рекомендуется использовать ту же ВМ, что и на предыдущих ЛР) и включает три этапа.

### **Этап 1. Установка и настройка межсетевого экрана (до 3 баллов)**

* Установите программное обеспечение для межсетевого экрана (например, iptables для Linux, Windows Firewall для Windows или pfSense).
* Настройте правила фильтрации трафика: (разрешите доступ к портам, необходимым для шифрованного канала (например, 1194 для OpenVPN); заблокируйте входящие подключения ко всем остальным портам, кроме необходимых для тестирования.)
* Проведите тестирование: попробуйте выполнить подключение к заблокированному порту (например, с помощью telnet или nmap) и зафиксируйте результат блокировки.

### **Этап 2. Установка и настройка средств анализа сетевого трафика и шифрованного канала (до 4 баллов)**

* Установите средство анализа сетевого трафика (например, Wireshark, tcpdump или аналоги).
* Настройте фильтры для мониторинга трафика на интерфейсе виртуальной машины (например, фильтр по порту OpenVPN).
* Установите и настройте OpenVPN для создания шифрованного канала: настройте сервер и клиент OpenVPN на одной или двух ВМ; используйте сертификаты для аутентификации (например, через easy-rsa).
* Проведите тестирование: перехватите трафик с помощью средства анализа до и после включения шифрования; продемонстрируйте, что данные в канале зашифрованы (например, сравните содержимое пакетов).

### **Этап 3. Настройка и демонстрация использования цифровой подписи (до 3 баллов)**

* Установите программное обеспечение для создания и проверки цифровой подписи (например, OpenSSL, GPG или встроенные средства Windows).
* Настройте систему: сгенерируйте пару ключей (открытый и закрытый) для цифровой подписи; подпишите тестовый файл (например, текстовый документ) с использованием закрытого ключа.
* Проведите тестирование: проверьте подлинность подписанного файла с использованием открытого ключа; измените файл и убедитесь, что проверка подписи не проходит.

Отчёт должен содержать описание действий, скриншоты и выводы по каждому этапу.

Кроме того быть готовым к демонстрации ВМ на защите работы.

### **Bài 5 – Bảo vệ thông tin khi làm việc với các kênh truyền thông.**

Cần cài đặt và cấu hình tường lửa mạng, công cụ phân tích lưu lượng mạng, kênh truyền dữ liệu được mã hóa (sử dụng OpenVPN hoặc tương tự) và chữ ký số để đảm bảo tính xác thực của thông tin. Bài thực hành được thực hiện trên máy ảo (khuyến nghị sử dụng cùng máy ảo với các bài trước) và gồm ba giai đoạn.

### **Giai đoạn 1. Cài đặt và cấu hình tường lửa mạng (tối đa 3 điểm)**

* Cài đặt phần mềm tường lửa mạng (ví dụ: iptables cho Linux, Windows Firewall cho Windows hoặc pfSense).
* Cấu hình quy tắc lọc lưu lượng: (chỉ cho phép truy cập đến các cổng cần thiết cho kênh mã hóa, ví dụ cổng 1194 cho OpenVPN; chặn tất cả các kết nối đến các cổng còn lại, ngoại trừ những cổng cần thiết cho kiểm thử).
* Thực hiện kiểm thử: thử kết nối đến cổng bị chặn (ví dụ dùng telnet hoặc nmap) và ghi lại kết quả kiểm tra chặn kết nối.

### **Giai đoạn 2. Cài đặt và cấu hình công cụ phân tích lưu lượng mạng và kênh mã hóa (tối đa 4 điểm)**

* Cài đặt công cụ phân tích lưu lượng mạng (ví dụ: Wireshark, tcpdump hoặc tương tự).
* Cấu hình bộ lọc để giám sát lưu lượng trên giao diện máy ảo (ví dụ: lọc theo cổng OpenVPN).
* Cài đặt và cấu hình OpenVPN để tạo kênh mã hóa: cấu hình máy chủ và máy khách OpenVPN trên một hoặc hai máy ảo; sử dụng chứng chỉ để xác thực (ví dụ dùng easy-rsa để tạo chứng chỉ).
* Thực hiện kiểm thử: bắt gói dữ liệu trước và sau khi bật mã hóa bằng công cụ phân tích; chứng minh rằng dữ liệu trên kênh đã được mã hóa (ví dụ: so sánh nội dung các gói tin).

### **Giai đoạn 3. Cấu hình và trình bày việc sử dụng chữ ký số (tối đa 3 điểm)**

* Cài đặt phần mềm tạo và kiểm tra chữ ký số (ví dụ: OpenSSL, GPG hoặc các công cụ tích hợp sẵn trong Windows).
* Cấu hình hệ thống: tạo cặp khóa (khóa công khai và khóa riêng) để ký số; ký một tệp thử nghiệm (ví dụ tệp văn bản) bằng khóa riêng.
* Thực hiện kiểm thử: kiểm tra tính xác thực của tệp đã ký bằng khóa công khai; thay đổi tệp và xác minh rằng việc kiểm tra chữ ký không thành công.

Báo cáo cần chứa mô tả các thao tác đã thực hiện, ảnh chụp màn hình và kết luận cho từng giai đoạn.

Ngoài ra, cần sẵn sàng trình bày trên máy ảo khi bảo vệ bài làm.