



1. Как настроить OpenVPN для безопасного доступа к VM

- Передавать данные через незащищённый FTP
- Truyền dữ liệu qua FTP không được mã hóa

✓ Использовать сертификаты TLS + шифрование AES-256

✓ Sử dụng chứng chỉ TLS + mã hóa AES-256

- Настроить VPN с паролем "admin" без сертификатов
- Cấu hình VPN với mật khẩu "admin" không có chứng chỉ
- Использовать SSH без проверки ключей
- Sử dụng SSH mà không kiểm tra khóa

2. Как реализовать цифровую подпись документов

- Хранить закрытый ключ в папке "Документы"
- Lưu khóa riêng trong thư mục "Tài liệu"
- Добавлять к файлу комментарий "Подписано мной"
- Thêm bình luận "Đã ký bởi tôi" vào tệp

✓ Использовать утилиту OpenSSL с ГОСТ-ключами

✓ Sử dụng tiện ích OpenSSL với khóa chuẩn GOST

- Отказаться от подписи, так как это замедляет работу
 - Bỏ chữ ký vì làm chậm hiệu suất
-

3. Как проверить работу межсетевого экрана

- Убедиться, что ping до VM проходит
- Đảm bảo rằng lệnh ping tới máy ảo hoạt động
- Проверить, открыт ли доступ к рабочему столу через RDP без пароля
- Kiểm tra xem có thể truy cập RDP vào desktop mà không cần mật khẩu không
- Отключить фаервол и проверить скорость
- Tắt tường lửa và kiểm tra tốc độ

✓ Сканировать порты через Nmap и убедиться, что закрыты ненужные

✓ Quét cổng bằng Nmap và đảm bảo rằng các cổng không cần thiết đã bị đóng

4. Какие настройки критичны для OpenVPN

- Использовать логин/пароль без шифрования
- Sử dụng tên đăng nhập/mật khẩu mà không mã hóa
- Настроить SSH-туннель без аутентификации
- Cấu hình đường hầm SSH mà không xác thực

✓ Конфигурация с TLS-шифрованием + проверка сертификатов

✓ Cấu hình mã hóa TLS + kiểm tra chứng chỉ

- Передавать данные через HTTP
 - Truyền dữ liệu qua HTTP
-

5. Как анализировать сетевой трафик на предмет атак

- Игнорировать предупреждения фаервола
- Bỏ qua cảnh báo của tường lửa
- Проверять только скорость загрузки страниц
- Chỉ kiểm tra tốc độ tải trang

✓ Искать SYN-флуд или необычные DNS-запросы в Wireshark

✓ Tìm SYN flood hoặc truy vấn DNS bất thường trong Wireshark

- Удалить все логи, чтобы не занимать место
 - Xóa toàn bộ log để tiết kiệm dung lượng
-

6. Как обеспечить подлинность сертификатов для VPN

✓ Настроить центр сертификации (CA) и подписывать ключи через него

✓ Thiết lập trung tâm chứng thực (CA) và ký khóa qua nó

- Хранить сертификаты в открытом доступе
- Lưu chứng chỉ ở nơi công khai

- Использовать самоподписанные сертификаты без проверки
 - Sử dụng chứng chỉ tự ký mà không kiểm tra
 - Отказаться от сертификатов, используя только пароли
 - Bỏ qua chứng chỉ, chỉ dùng mật khẩu
-

7. Как проверить валидность цифровой подписи файла

- ✓ **Использовать openssl verify с публичным ключом**
- ✓ **Sử dụng openssl verify với khóa công khai**

- Переименовать файл, добавив “_signed”
 - Đổi tên tệp, thêm hậu tố “_signed”
 - Хранить приватный ключ в коде приложения
 - Lưu khóa riêng trong mã nguồn ứng dụng
 - Сравнить размер файла до и после подписи
 - So sánh kích thước tệp trước và sau khi ký
-

8. Что исключить из мер защиты сети

- ✓ **Передавать пароли в открытом виде через FTP**
- ✓ **Truyền mật khẩu ở dạng rõ qua FTP**

- Использовать HTTPS вместо HTTP
 - Sử dụng HTTPS thay cho HTTP
 - Разрешить все входящие подключения на порт 3389 (RDP) без пароля
 - Cho phép tất cả kết nối đến cổng 3389 (RDP) mà không cần mật khẩu
 - Настроить GeoIP-блокировку подозрительных регионов
 - Cấu hình chặn GeoIP cho các khu vực đáng ngờ
-

9. Какой межсетевой экран лучше использовать для гибкой настройки правил на ОС

- Встроенный Windows Defender без изменений
- Windows Defender tích hợp sẵn mà không chỉnh sửa
- ✓ **pfSense с настройкой правил для блокировки нежелательных портов**
- ✓ **pfSense với cấu hình quy tắc để chặn các cổng không mong muốn**
- Разрешить все входящие подключения для удобства
- Cho phép tất cả kết nối đến để tiện lợi
- Отключить фаервол для “ускорения” сети
- Tắt tường lửa để “tăng tốc” mạng

10. Какое средство анализа сетевого трафика подходит для обнаружения аномалий

- Проверять только ping до шлюза
- Chỉ kiểm tra ping đến gateway
- Отключить сетевой адаптер
- Tắt adapter mạng

☒ **Wireshark с фильтрами для выявления подозрительных пакетов**

☒ **Wireshark với bộ lọc để phát hiện gói tin đáng ngờ**

- Использовать Блокнот для просмотра логов
 - Sử dụng Notepad để xem log
-