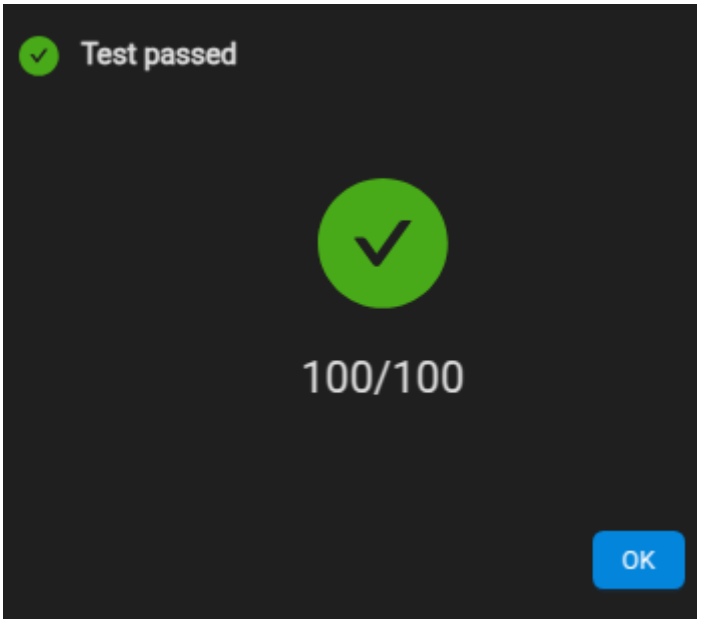


**1. Какое средство обнаружения вторжений (IDS) лучше интегрируется с Windows**
○ Встроенный брандмауэр Windows без дополнительных правил
○ Tường lửa tích hợp sẵn của Windows mà không có quy tắc bổ sung

○ Встроенные средства защиты UserGate
○ Công cụ bảo vệ tích hợp của UserGate

○ Отключить сетевые адаптеры для предотвращения атак
○ Tắt adapter mạng để ngăn chặn tấn công

**✅ Snort с настройкой правил для мониторинга сетевых аномалий**
**✅ Snort với cấu hình quy tắc để giám sát các bất thường mạng**

---

**2. Как настроить систему контроля целостности файлов**
○ Периодически переименовывать файлы вручную
○ Định kỳ đổi tên tệp theo cách thủ công

**✅ Использовать PowerShell + Windows Defender ATP для аудита хэшей критичных файлов**
**✅ Sử dụng PowerShell + Windows Defender ATP để kiểm tra hash của các tệp quan trọng**

○ Удалить все системные логи для экономии места
○ Xoá toàn bộ log hệ thống để tiết kiệm dung lượng

○ Отключить обновление Windows, чтобы файлы не менялись
○ Tắt cập nhật Windows để các tệp không bị thay đổi

---

**3. Как реализовать безопасное хранение логинов/паролей**
○ Использовать шифрование AES со статическим ключом в коде
○ Sử dụng mã hóa AES với khóa tĩnh trong mã nguồn

○ Записать пароли в системный реестр без шифрования
○ Ghi mật khẩu vào registry hệ thống mà không mã hóa

✅ **Хэширование с солью через bcrypt/PBKDF2 и хранение в зашифрованной БД**
✅ **Băm kèm muối bằng bcrypt/PBKDF2 và lưu trong cơ sở dữ liệu được mã hóa**

○ Сохранить пароли в текстовом файле на рабочем столе
○ Lưu mật khẩu trong tệp văn bản trên màn hình nền

---

**4. Какой метод двухфакторной аутентификации (2FA) наиболее безопасен**
✅ **TOTP (Google Authenticator) + резервные коды**
✅ **TOTP (Google Authenticator) + mã dự phòng**

○ Использовать один и тот же код 0000 для всех пользователей
○ Sử dụng cùng một mã 0000 cho tất cả người dùng

○ Отправить пароль по email для подтверждения
○ Gửi mật khẩu qua email để xác nhận

○ SMS-коды, так как они всегда доступны
○ Mã SMS vì chúng luôn sẵn có

---

**5. Как проверить работу IDS на ОС**
✅ **Сгенерировать тестовые атаки (например, через Metasploit) и проверить логи Snort**
✅ **Tạo các cuộc tấn công thử nghiệm (ví dụ qua Metasploit) và kiểm tra log của Snort**

○ Удалить все правила IDS для "ускорения" тестирования
○ Xóa tất cả quy tắc IDS để “tăng tốc” kiểm thử

○ Отключить IDS и убедиться, что система не падает
○ Tắt IDS và kiểm tra xem hệ thống có sập không

○ Проверить ping до локального хоста
○ Kiểm tra ping tới localhost

---

**6. Какие параметры критичны для системы контроля целостности**
○ Отключить контроль после первого успешного сканирования
○ Tắt kiểm tra sau lần quét thành công đầu tiên

○ Игнорировать изменения в папке C:\Windows
○ Bỏ qua các thay đổi trong thư mục C:\Windows

○ Проверять целостность только раз в год
○ Kiểm tra tính toàn vẹn chỉ một lần mỗi năm

✅ **Регулярный аудит хэшей + оповещение при изменении системных файлов**
✅ **Kiểm tra định kỳ hash + cảnh báo khi có thay đổi trong tệp hệ thống**

---

**7. Как защитить базу данных с паролями**
○ Использовать стандартную БД без пароля
○ Sử dụng cơ sở dữ liệu mặc định không có mật khẩu

○ Записать пароли в комментарии к коду приложения
○ Ghi mật khẩu vào chú thích trong mã ứng dụng

○ Хранить БД в публичной папке с доступом для всех пользователей
○ Lưu cơ sở dữ liệu trong thư mục công khai có quyền truy cập cho tất cả người dùng

✅ **Использовать SQLite с шифрованием (SQLCipher) + ограничение прав доступа**
✅ **Sử dụng SQLite với mã hóa (SQLCipher) + giới hạn quyền truy cập**

---

**8. Как интегрировать аппаратный ключ (YubiKey) для 2FA**
○ Привязать ключ к учетной записи администратора без шифрования
○ Gắn khóa vào tài khoản quản trị viên mà không mã hóa

○ Использовать YubiKey как USB-накопитель для хранения паролей
○ Sử dụng YubiKey như USB để lưu mật khẩu

✅ **Настроить FIDO2/U2F через API Windows Hello или специализированные библиотеки**
✅ **Cấu hình FIDO2/U2F qua API của Windows Hello hoặc thư viện chuyên dụng**

○ Ввести серийный номер ключа в текстовое поле пароля
○ Nhập số sê-ri của khóa vào trường mật khẩu dạng văn bản

---

**9. Как реагировать на срабатывание IDS**
✅ **Автоматически блокировать IP + уведомлять администратора через SIEM**
✅ **Tự động chặn IP + thông báo cho quản trị viên qua hệ thống SIEM**

○ Удалить логи, чтобы освободить место на диске
○ Xóa log để giải phóng dung lượng ổ đĩa

○ Отключить IDS до выяснения причин
○ Tắt IDS cho đến khi tìm ra nguyên nhân

○ Игнорировать предупреждения, если система работает стабильно
○ Bỏ qua cảnh báo nếu hệ thống vẫn hoạt động ổn định

---

**10. Что исключить из продвинутых мер защиты**
○ Использовать аппаратные модули безопасности (HSM) для ключей
○ Sử dụng mô-đun phần cứng bảo mật (HSM) cho khóa

✅ **Хранить секреты 2FA в открытом виде в конфигурационных файлах**
✅ **Lưu khóa bí mật 2FA ở dạng rõ ràng trong tệp cấu hình**

○ Настроить автоматическую ротацию ключей шифрования
○ Cấu hình xoay vòng khóa mã hóa tự động

○ Регулярно обновлять правила IDS/IPS на основе актуальных угроз
○ Thường xuyên cập nhật quy tắc IDS/IPS theo mối đe dọa hiện tại

---