**You should install and configure a basic set of software to protect information from unauthorized access on a virtual machine running the Windows operating system.** The software package includes an antivirus, an encryption tool, and an access control system. The task is completed in 3 stages.

### **Step 1. Install the antivirus protection tool. (up to 3 points)**

1. Select and install one antivirus protection tool (Kaspersky, DrWeb, any free antivirus of your choice).
2. Set up the antivirus for automatic updates and scheduled scanning.
3. Perform a full scan of the system, make sure that it is not infected.
4. Start the test virus detection procedure (for example, with a standard EICAR file).  
    The procedure should be performed both manually (you created the file → antivirus responded) and automatically (the file is created by a script → antivirus responds).

### **Stage 2. Installation and use of the encryption tool (up to 3 points)**

1. Select and install an encryption tool (as examples - BitLocker or VeraCrypt).
2. Create and configure an encrypted data storage container.
3. Move the test data to an encrypted container and demonstrate its encryption/decryption.

### **Stage 3. Setting up the access control system (up to 4 points)**

1. Install and configure an access control system (for example, Active Directory).
2. Create an approximate domain structure with users and groups.
3. Set up access policies for different user groups.
4. Test the created accounts and demonstrate the implementation of access control.

All this must be recorded in a report, and screenshots of all key work steps are required.

In addition, be prepared to demonstrate VMs.

**Bạn cần cài đặt và cấu hình một bộ phần mềm cơ bản để bảo vệ thông tin khỏi truy cập trái phép trên một máy ảo chạy hệ điều hành Windows.** Bộ phần mềm bao gồm: một phần mềm diệt virus, một công cụ mã hóa, và một hệ thống kiểm soát truy cập. Nhiệm vụ được thực hiện qua 3 giai đoạn:

### **Bước 1. Cài đặt phần mềm bảo vệ chống virus (tối đa 3 điểm)**

1. Chọn và cài đặt một phần mềm diệt virus (ví dụ: Kaspersky, DrWeb, hoặc bất kỳ phần mềm diệt virus miễn phí nào bạn chọn).
2. Cấu hình phần mềm diệt virus để tự động cập nhật và quét theo lịch định kỳ.
3. Thực hiện quét toàn bộ hệ thống, đảm bảo rằng hệ thống không bị nhiễm mã độc.
4. Bắt đầu kiểm tra khả năng phát hiện virus (ví dụ bằng file EICAR tiêu chuẩn).  
    Quá trình này cần thực hiện bằng cả hai cách:  
   * **Thủ công:** bạn tạo file → phần mềm diệt virus phát hiện.
   * **Tự động:** file được tạo bởi script → phần mềm diệt virus phát hiện.

### **Bước 2. Cài đặt và sử dụng công cụ mã hóa (tối đa 3 điểm)**

1. Chọn và cài đặt một công cụ mã hóa (ví dụ: BitLocker hoặc VeraCrypt).
2. Tạo và cấu hình một vùng lưu trữ dữ liệu được mã hóa.
3. Di chuyển dữ liệu thử nghiệm vào vùng mã hóa và trình diễn quá trình mã hóa/giải mã.

### **Bước 3. Thiết lập hệ thống kiểm soát truy cập (tối đa 4 điểm)**

1. Cài đặt và cấu hình một hệ thống kiểm soát truy cập (ví dụ: Active Directory).
2. Tạo một cấu trúc tên miền gần đúng với các người dùng và nhóm.
3. Thiết lập các chính sách truy cập cho từng nhóm người dùng khác nhau.
4. Kiểm tra các tài khoản đã tạo và trình diễn cách kiểm soát truy cập hoạt động.

Toàn bộ quá trình cần được ghi lại trong một **báo cáo**, và **ảnh chụp màn hình** của tất cả các bước quan trọng là bắt buộc.

Ngoài ra, bạn cần **chuẩn bị để trình diễn các máy ảo (VMs).**