**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN 1**

****

**Môn: THỰC TẬP CƠ SỞ**

**BÁO CÁO BÀI THỰC HÀNH SỐ 10**

**Họ và tên sinh viên:**

**Đỗ Tiến Sĩ**

**Mã số sinh viên:**

**B20DCAT153**

**Bài 10: Sao lưu hệ thống.**

**Họ và tên giảng viên:**

**Thầy :Đỗ Xuân Chợ**

**Hà Nội 3/2023 (tháng/năm)**

**Sao lưu tới ổ đĩa mạng**

**I. Tìm hiểu lý thuyết:**

– Giao thức sao chép an toàn (SCP) là một giao thức mạng để truyền các tệp một cách an toàn giữa máy chủ cục bộ và máy chủ từ xa hoặc giữa hai máy chủ từ xa.

– Theo các nhà phát triển OpenSSH vào tháng 4 năm 2019, SCP đã lỗi nthời, không linh hoạt và không dễ sửa chữa; họ khuyến nghị sử dụng các giao thức hiện đại hơn như SFTP và rsync để truyền tệp.

– SCP sử dụng Secure Shell (SSH) để truyền dữ liệu và sử dụng các cơn chế tương tự để xác thực, do đó đảm bảo tính xác thực và tính bảo mật của dữ liệu trong quá trình truyền tải. Máy khách có thể gửi tệp tới máy chủ, đồng thời có thể yêu cầu tải xuống tệp hoặc thư mục từ máy chủ.

– Giao thức truyền tệp (FTP) là một giao thức mạng được sử dụng để truyền tệp từ máy chủ đến máy khách trên mạng máy tính.

– FTP được xây dựng trên kiến​ trúc mô hình máy khách-máy chủ. Người dùng FTP có thể tự xác thực bằng giao thức đăng nhập văn bản rõ ràng, thường ở dạng tên người dùng và mật khẩu, nhưng có thể kết nối ẩn danh nếu máy chủ được định cấu hình cho phép.

– FTP có thể hoạt động ở hai chế độ là chủ động và thụ động:

* Ở chế độ chủ động, máy khách chờ (listen) kết nối từ máy chủ, trên cổng M của máy khách. Máy khách gửi máy chủ thông điệp PORT M để máy chủ biết máy khách đang chờ ở cổng nào. Máy chủ sau đó sẽ tạo kết nối từ cổng 20/21 của máy chủ đến cổng M của máy khách.
* Chế độ thụ động được sử dụng trong trường hợp máy kháchnằm sau tường lửa. Máy khách gửi thông điệp PASV đến máychủ. Máy chủ sau đó gửi địa chỉ IP và cổng FTP đang mở của máy chủ để máy khách tạo kết nối đến máy chủ.

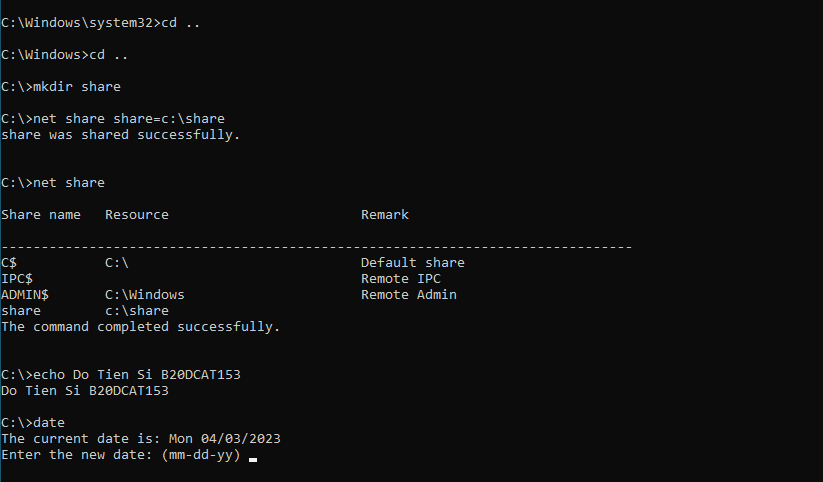
– Mặc định, dữ liệu trên FTP không được mã hoá, bao gồm tên đăng nhập và mật khẩu. Người dùng có thể bật SSL/TLS để mã hoá dữ liệu, tăng cường bảo mật cho quá trình truyền dữ liệu.

– Ổ đĩa mạng là ổ đĩa gắn trên một máy tính kết nối mạng, được thiết lập để người dùng trên cùng mạng có thể truy cập tài nguyên trên đó.

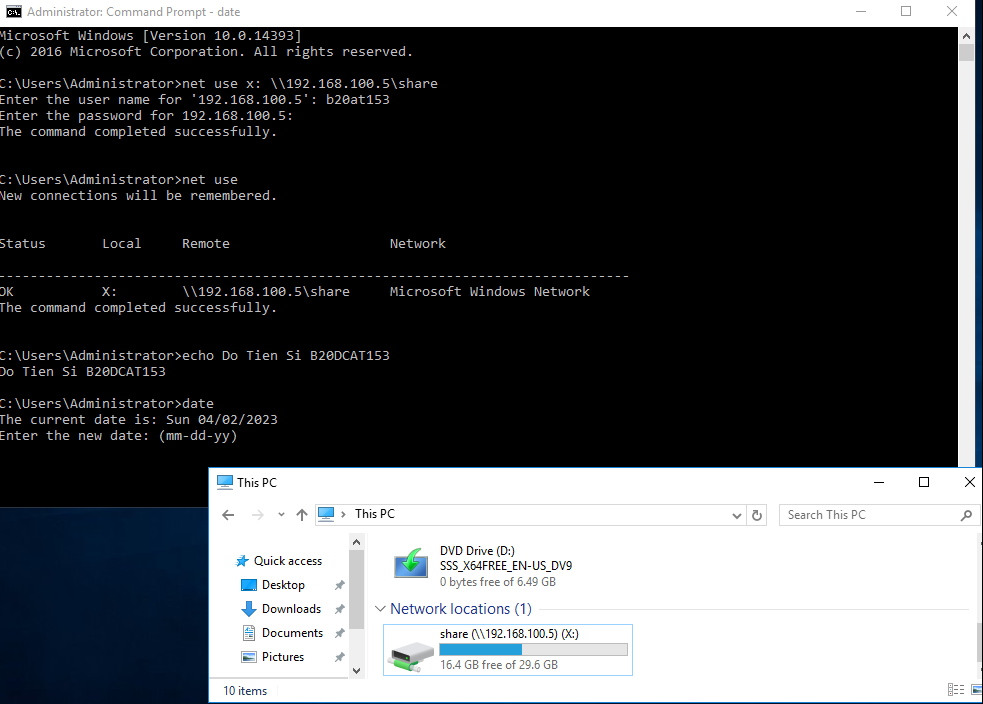
– Ổ đĩa mạng thường được sử dụng trong doanh nghiệp và trường học nhiều hơn là trong hộ gia đình**.**

**II. Mô tả cài đặt & kết quả:**

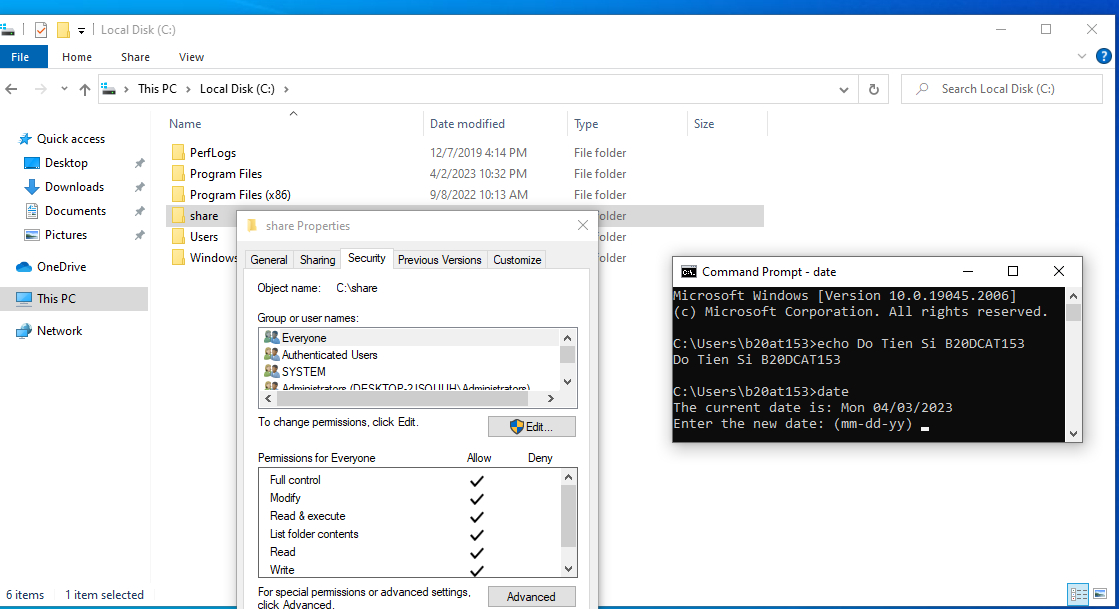
1. Sao lưu tới ổ đĩa mạng:

– Sinh viên chạy lệnh net share share=C:\share để tạo thư mục chia sẻ mới trên Windows 7 attack.

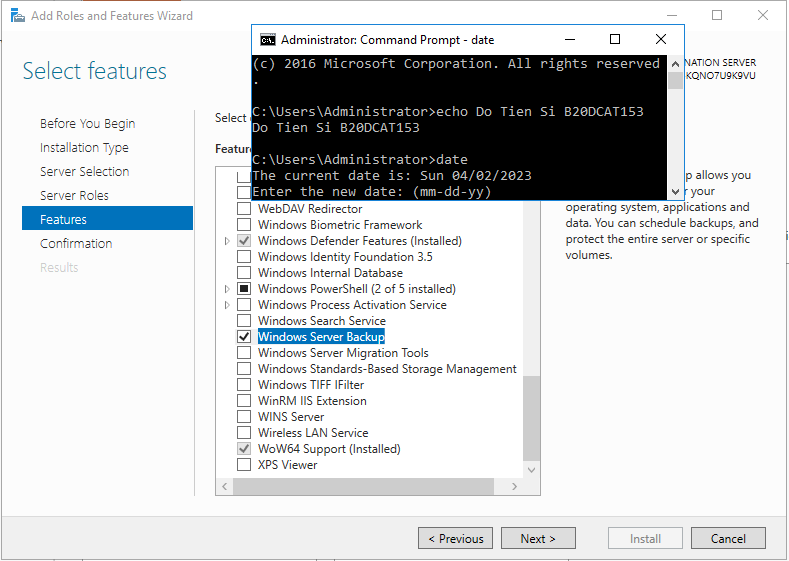
* Trên máy Windows server ở mạng Internal, cấu hình map ổ đĩa mạng trên máy.
* Trên máy Windows attack trong mạng Internal, cấu hình thư mục ở đĩa mạng cho phép sao lưu tệp và thư mục từ máy khác nếu không tạo được thư mục trên máy Windows server



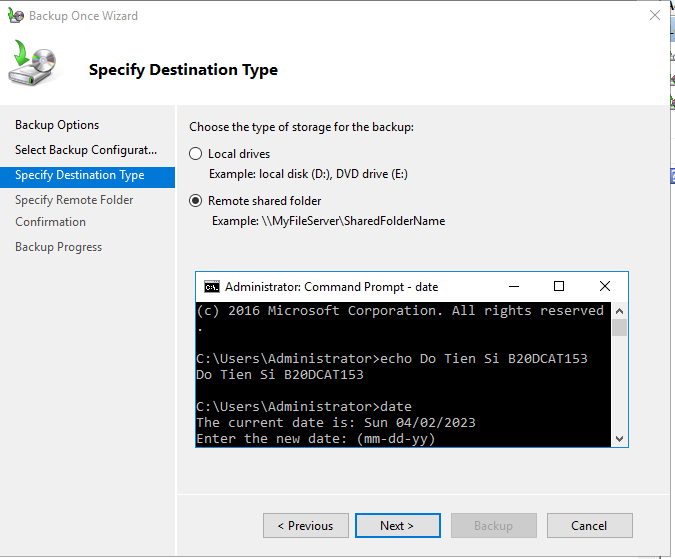
* Cấp quyền full control cho thư mục share

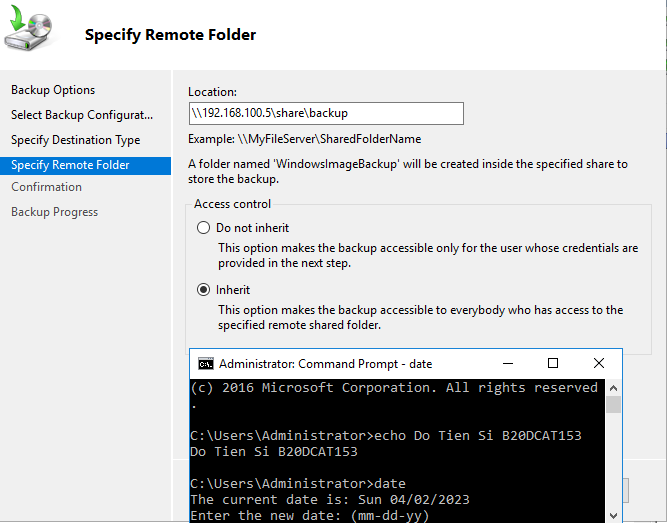


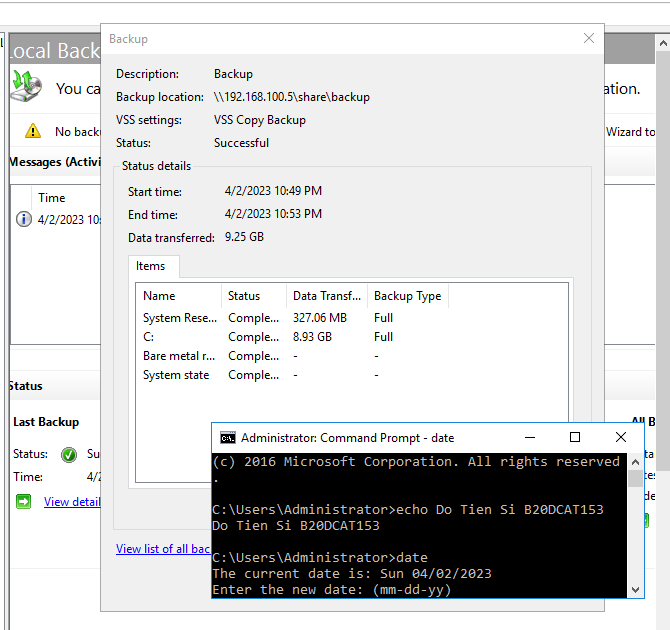
* Cài windows server backup

- Trên máy Windows server ở mạng Internal, sao lưu hệ thống bằng chương trình sao lưu của Windows (ntbackup trong Windows server 2003, nếu sử dụng Win khác thì có thể download ntbackup để sử dụng), sau đó chọn 1 thư mục để sao lưu và đích là thư mục ổ mạng đã chia sẻ trên máy Windows attack trong mạng Internal

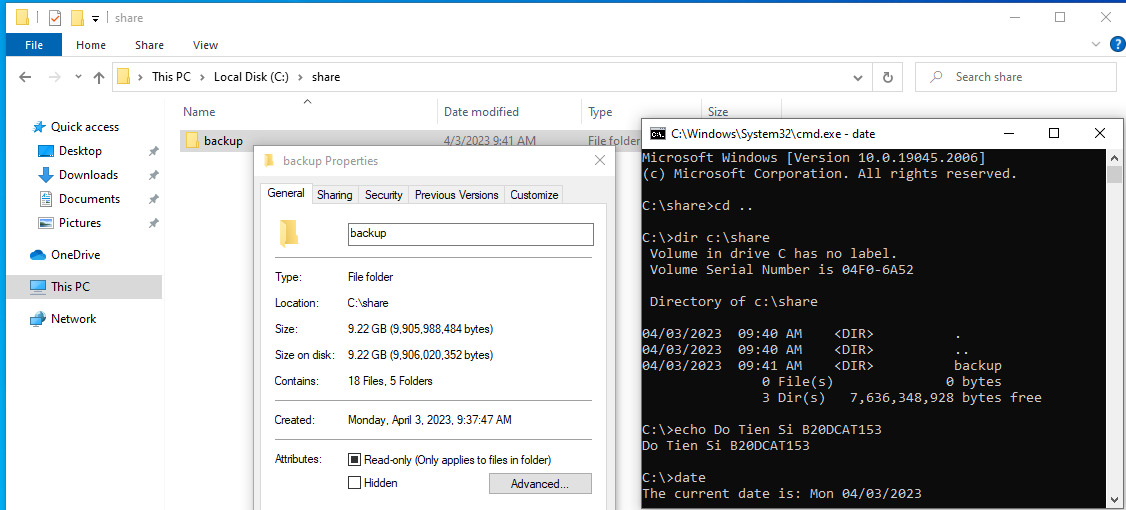
* Chọn chia sẻ file trên 1 hệ thống mạng

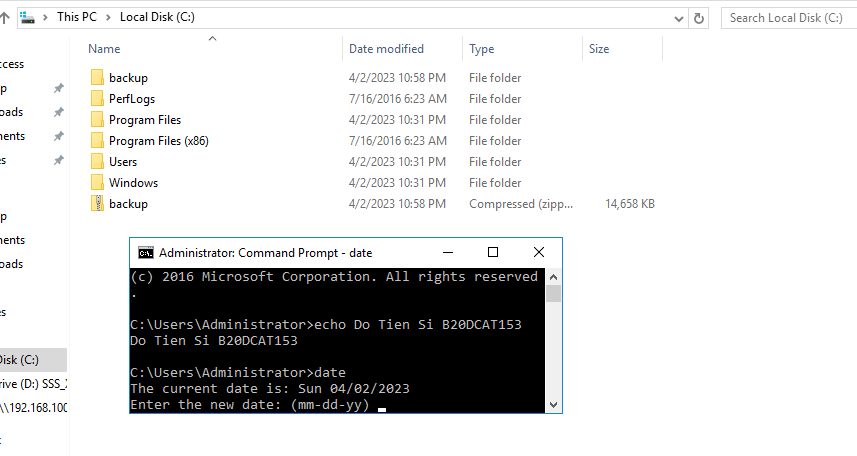




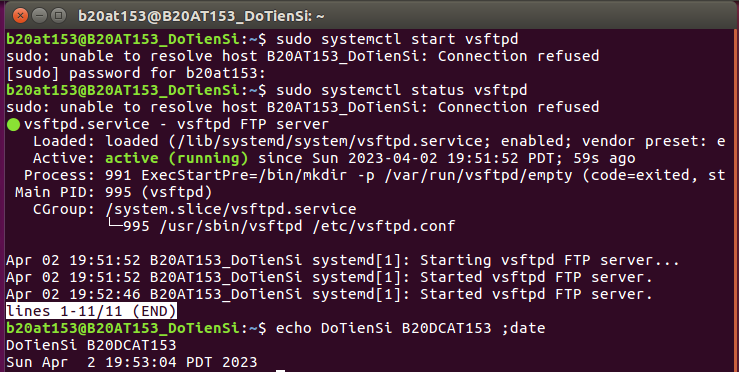


* Kiểm tra

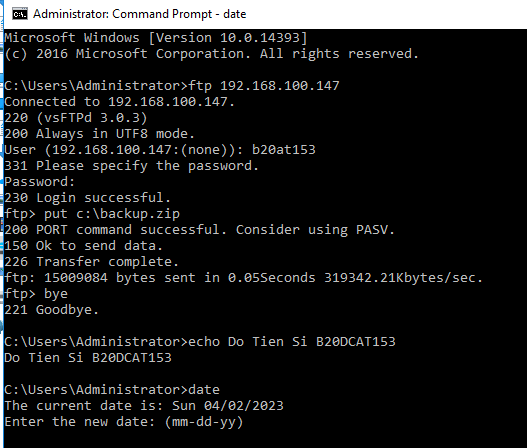




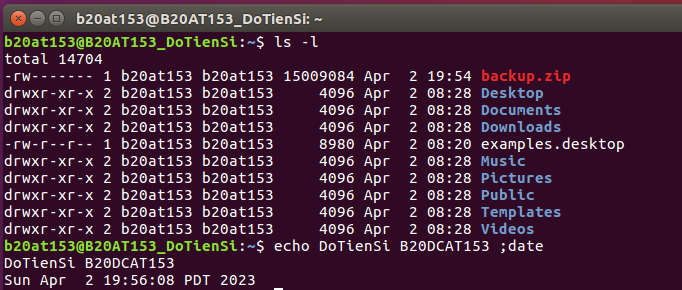
* Sao lưu tệp lên FTP server
* Trên máy Windows victim ở mạng Internal, cài đặt ftp client
* Trên máy Linux trong mạng Internal, cài đặt ftp server



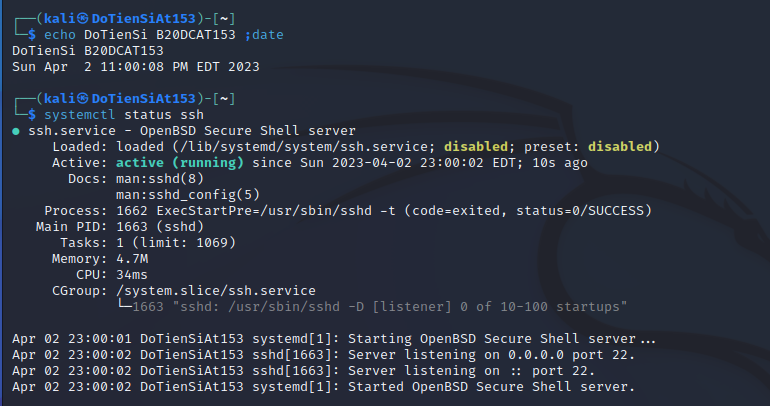
* Sao lưu 1 thư mục trên máy Windows victim tới thư mục /backup trên máy Linux trong mạng Internal sử dụng ftp client, sau khi kết nối tới ftp server



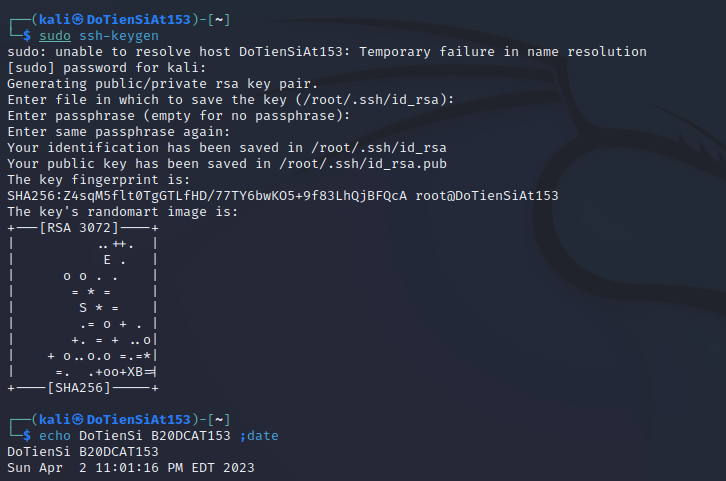
* Kiểm tra



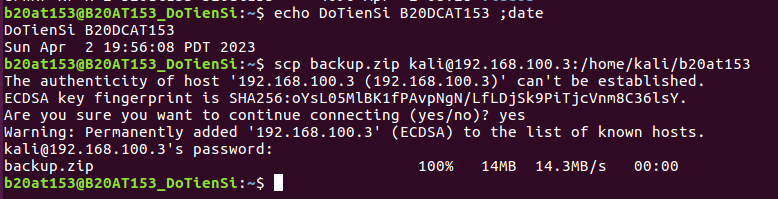
* Sao lưu tệp sử dụng SCP
* Trên máy Kali Linux trong mạng Internal, cấu hình SSH server.



* Tiếp tục, tạo Secure Shell Keys trên máy Kali Linux đó



* Trên máy Linux victim trong mạng Internal, thực hiện sao lưu sử dụng lệnh scp để copy file cần sao lưu tới thư mục root trên máy Kali Linux



* Kiểm tra

