

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



Môn: Thực tập cơ sở

BÀI BÁO THỰC TẬP CƠ SỞ

Bài 4: Cài đặt, cấu hình Windows Server

Họ và tên giảng viên:	TS.Đinh Trường Duy
Họ và tên:	Nguyễn Quốc Khánh
Mã sinh viên:	B20DCAT103
Lớp:	D20CQAT03-B
Số điện thoại:	0964137761

Hà Nội 2023

1. Tìm hiểu lý thuyết

a. Hệ điều hành Windows dành cho máy chủ

Hệ điều hành Windows dành cho máy chủ hay thường gọi là Windows Server là một dòng hệ điều hành mà Microsoft tạo ra cụ thể để sử dụng trên máy chủ. Được thiết kế để xử lý hiệu quả hơn kết nối mạng, lưu trữ internet / mạng nội bộ, cơ sở dữ liệu, hệ thống liên lạc quy mô doanh nghiệp và các chức năng tương tự. Phiên bản Windows Server đầu tiên được phát hành dưới thương hiệu đó là Windows Server 2003. Tuy nhiên, phiên bản máy chủ đầu tiên của Windows là Windows NT 3.1 Advanced Server, tiếp theo là Windows NT 3.5 Server, Windows NT 3.51 Server, Windows NT 4.0 Server và Windows 2000 máy chủ. Windows 2000 Server là phiên bản máy chủ đầu tiên bao gồm Active Directory, máy chủ DNS, máy chủ DHCP, chính sách nhóm, cũng như nhiều tính năng phổ biến khác được sử dụng ngày nay.

Windows Server khác với Windows phiên bản máy trạm:

Windows Server hỗ trợ phần cứng mạnh mẽ hơn

Windows Server không yêu cầu tích hợp giao diện GUI. Nó có thể cài đặt theo hai hình thức - Server Core(không GUI) hoặc có giao diện GUI.

Cung cấp các công cụ dành riêng cho máy chủ: Windows Server có thể hỗ trợ một loạt được thiết kế dành riêng cho các máy chủ, chẳng hạn như Active Directory, DHCP, Server Manager,...

Chi phí bản quyền nhiều hơn phiên bản máy trạm Windows

b. Web Server

Một máy chủ web lưu trữ và cung cấp nội dung cho một trang web - chẳng hạn như văn bản, hình ảnh, video và dữ liệu ứng dụng - cho các máy trạm yêu cầu. Loại trạm hàng phổ biến nhất là chương trình trình duyệt web, yêu cầu dữ liệu từ trang web của bạn khi người dùng nhấp vào liên kết hoặc tải xuống tài liệu trên trang được hiển thị trong trình duyệt.

Một máy chủ web giao tiếp với trình duyệt web bằng giao thức truyền siêu văn bản (HTTP). Nội dung của hầu hết các trang web được mã hóa bằng ngôn ngữ đánh dấu siêu văn bản (HTML). Nội dung có thể tĩnh (ví dụ: văn bản và hình ảnh) hoặc động (ví dụ: giá tính toán hoặc danh sách các mặt hàng mà trạm hàng đã đánh dấu để mua). Để cung cấp nội dung động, hầu hết các máy chủ web đều hỗ trợ các

ngôn ngữ kịch bản bên máy chủ để mã hóa logic kinh doanh vào giao tiếp. Các ngôn ngữ được hỗ trợ thường bao gồm các trang máy chủ hoạt động (ASP), JavaScript, PHP, Python và Ruby. Một máy chủ web cũng có thể lưu trữ nội dung để tăng tốc độ phân phối nội dung yêu cầu. Quá trình này còn được gọi là gia tốc web.

c. FTP Server

Giao thức truyền tệp (FTP) là một giao thức truyền thông tiêu chuẩn được sử dụng để chuyển các tệp máy tính từ máy chủ sang máy trạm trên mạng máy tính. FTP được xây dựng trên kiến trúc mô hình máy trạm-máy chủ bằng cách sử dụng các kết nối dữ liệu và điều khiển riêng biệt giữa máy trạm và máy chủ. Người dùng FTP có thể tự xác thực với giao thức đăng nhập văn bản rõ ràng, thông thường ở dạng tên người dùng và mật khẩu, nhưng có thể kết nối ẩn danh nếu máy chủ được cấu hình để cho phép. Để truyền an toàn để bảo vệ tên người dùng và mật khẩu và mã hóa nội dung, FTP thường được bảo mật bằng SSL/TLS (FTP) hoặc được thay thế bằng Giao thức truyền tệp SSH (SFTP). FTP có thể chạy ở chế độ hoạt động hoặc thụ động, tùy vào cách kết nối dữ liệu được thiết lập:

Trong chế độ chủ động, máy trạm bắt đầu nghe các kết nối dữ liệu đến từ máy chủ. Nó gửi lệnh FTP để thông báo cho máy chủ về cổng nào đang nghe. Sau đó, máy chủ bắt đầu một kênh dữ liệu cho máy trạm từ cổng 20, cổng dữ liệu máy chủ FTP.

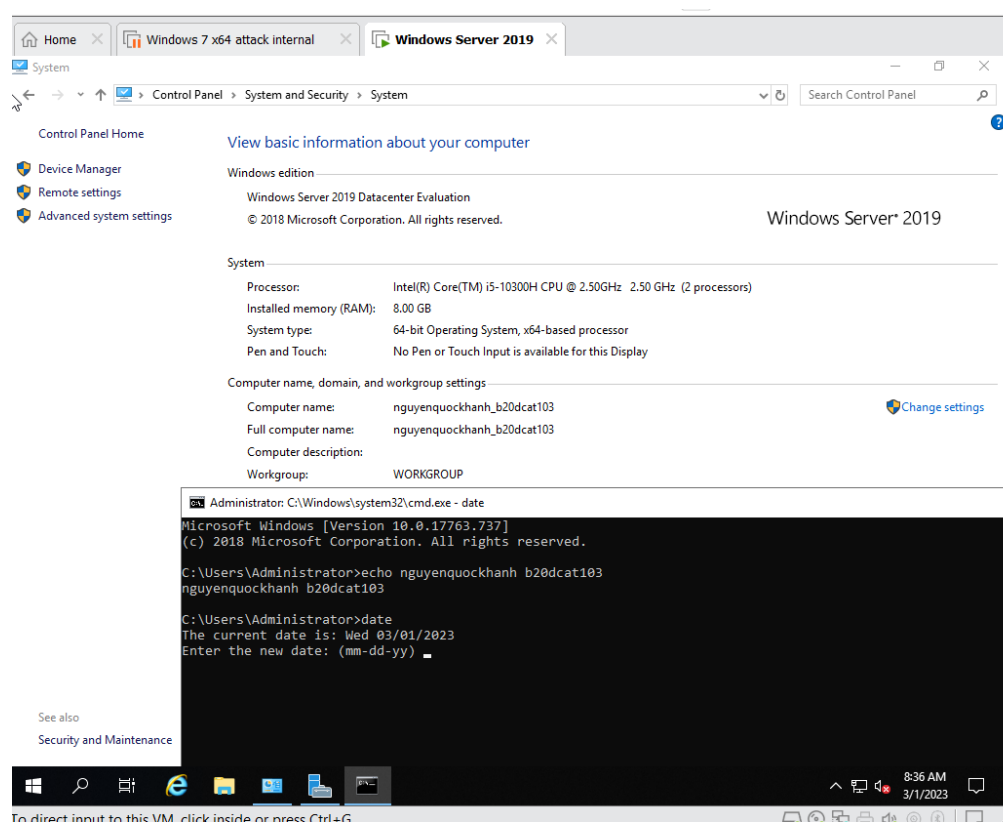
Trong các tình huống mà trạm hàng có tường lửa và không thể chấp nhận các kết nối TCP đến, chế độ thụ động có thể được sử dụng. Trong chế độ này, máy trạm sử dụng kết nối điều khiển để gửi lệnh PASV đến máy chủ và sau đó nhận địa chỉ IP máy chủ và số cổng máy chủ từ máy chủ, mà máy trạm sau đó sử dụng để mở kết nối dữ liệu từ máy trạm tùy ý đến địa chỉ IP máy chủ và số cổng máy chủ nhận được.

d. Remote Desktop Connection

Remote Desktop Connection (RDC), (trước đây có tên là Microsoft Terminal Services Client, MSTSC hoặc TSCClient), cho phép người dùng đăng nhập từ xa vào máy tính được nối mạng chạy máy chủ dịch vụ đầu cuối. RDC trình bày giao diện máy tính để bàn (hoặc ứng dụng GUI) của hệ thống từ xa, giống như đang truy cập cục bộ. Ngoài tên người dùng/mật khẩu thông thường để ủy quyền cho phiên từ xa, RDC cũng hỗ trợ sử dụng thẻ thông minh để ủy quyền. Trên các phiên bản của Windows đều tích hợp sẵn tính năng RDC.

2. Nội dung thực hành

Kiểm tra tên của Server:



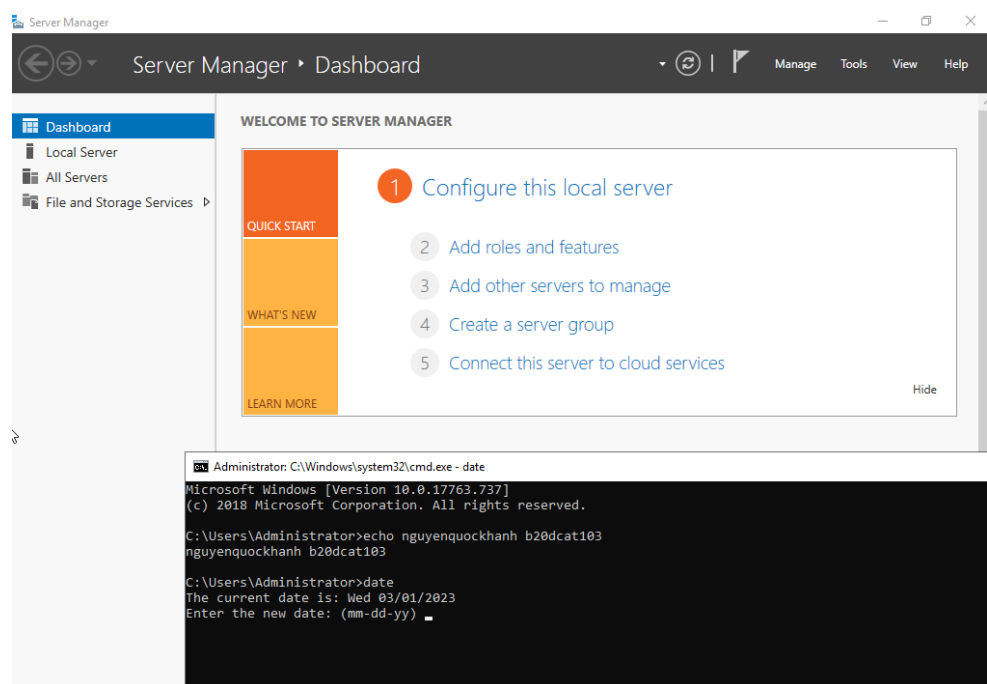
The screenshot shows the Windows Server 2019 Control Panel, specifically the System page. The page displays basic information about the computer, including the Windows edition (Windows Server 2019 Datacenter Evaluation), system type (64-bit Operating System, x64-based processor), and computer name (nguyenquockhanh_b20dcat103). Below this, a command prompt window is open, showing the following commands and output:

```
Administrator: C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>echo nguyenquockhanh b20dcat103
nguyenquockhanh b20dcat103

C:\Users\Administrator>date
The current date is: Wed 03/01/2023
Enter the new date: (mm-dd-yy) _
```

Cài đặt Windows Server và máy trạm Windows từ file đã chuẩn bị:



The screenshot shows the Windows Server Manager Dashboard. The dashboard displays a 'WELCOME TO SERVER MANAGER' message and a list of tasks to configure the local server:

- 1 Configure this local server
- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

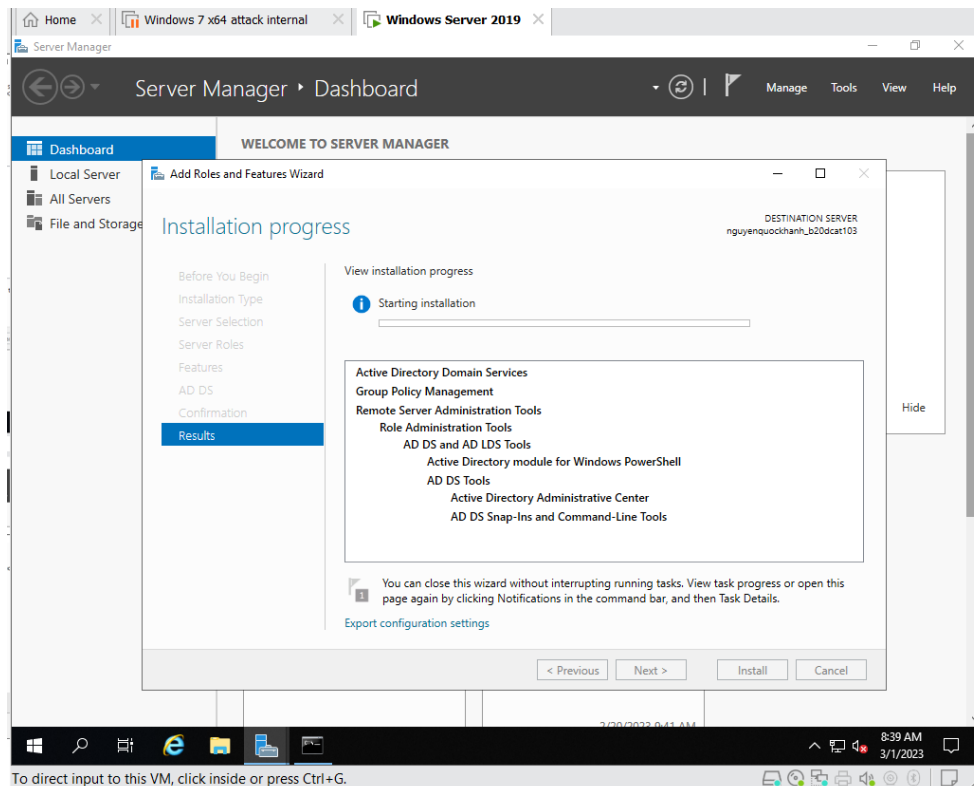
Below the dashboard, a command prompt window is open, showing the same commands and output as in the previous screenshot:

```
Administrator: C:\Windows\system32\cmd.exe - date
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

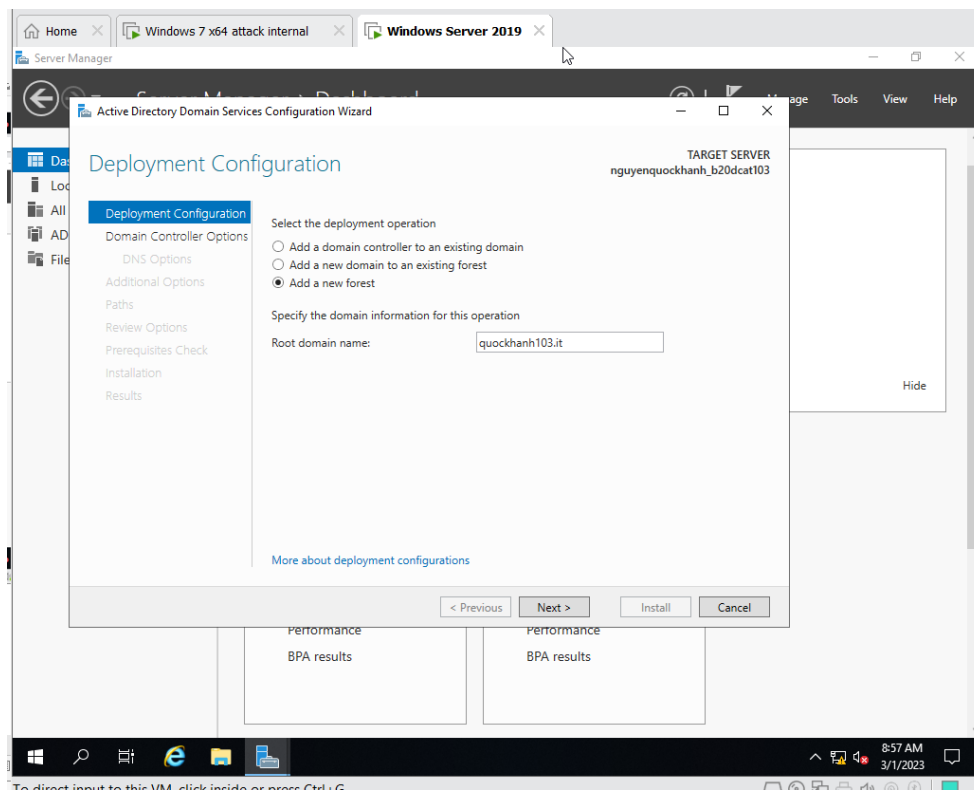
C:\Users\Administrator>echo nguyenquockhanh b20dcat103
nguyenquockhanh b20dcat103

C:\Users\Administrator>date
The current date is: Wed 03/01/2023
Enter the new date: (mm-dd-yy) _
```

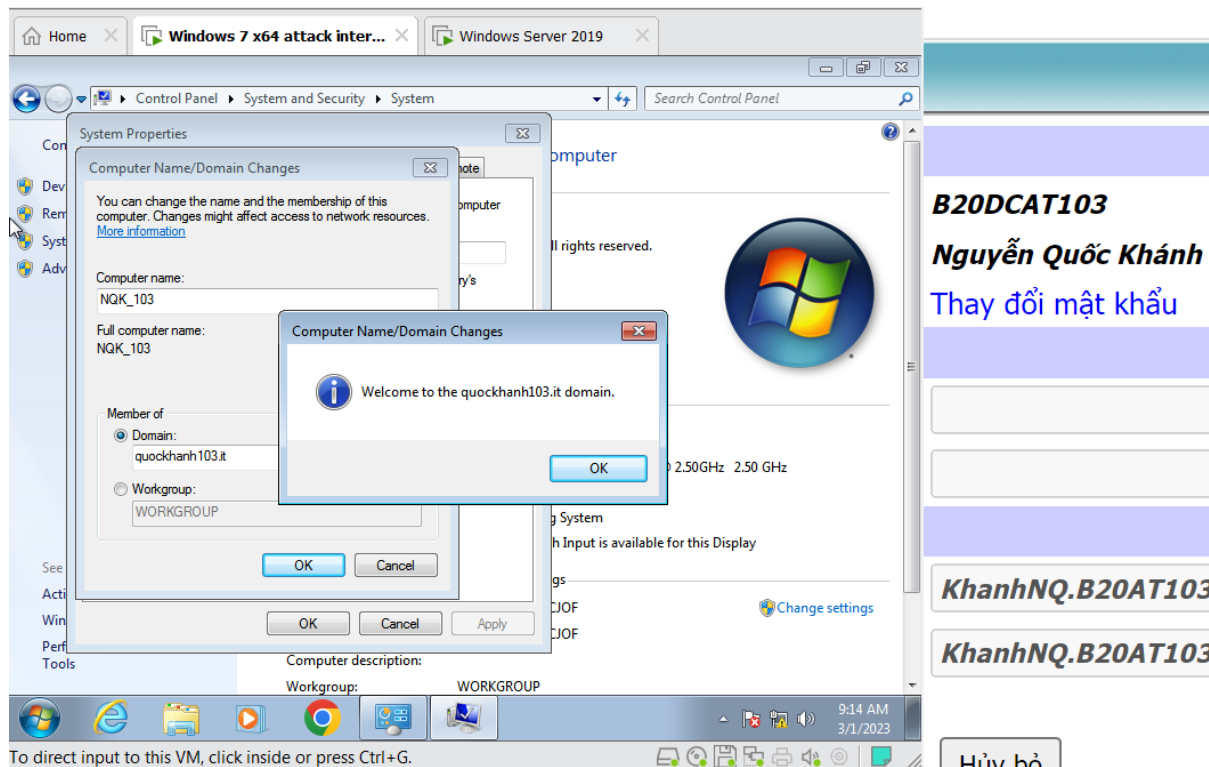
Cài đặt server role trong Server Manager:



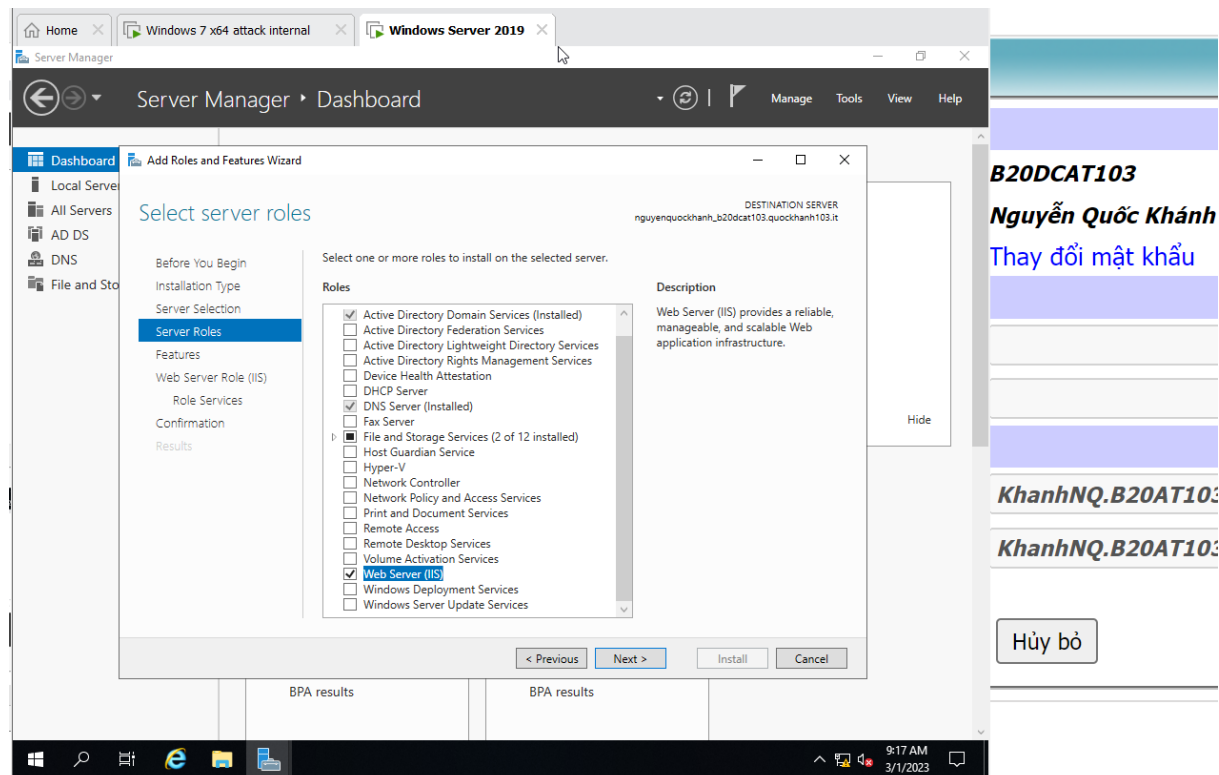
Nâng cấp Server thành Domain Controller:



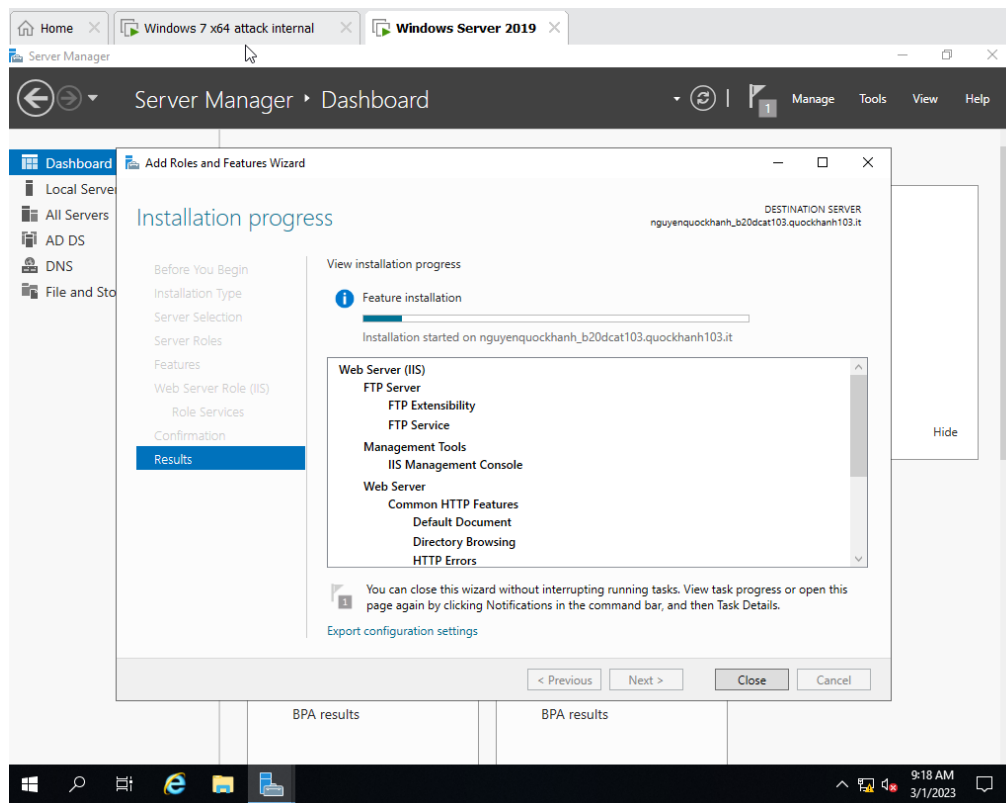
Cấu hình máy trạm Windows gia nhập vào domain vừa tạo được:



Cài đặt Web Server (IIS):



Cài đặt thành công Web Server (IIS):



B20DCAT103

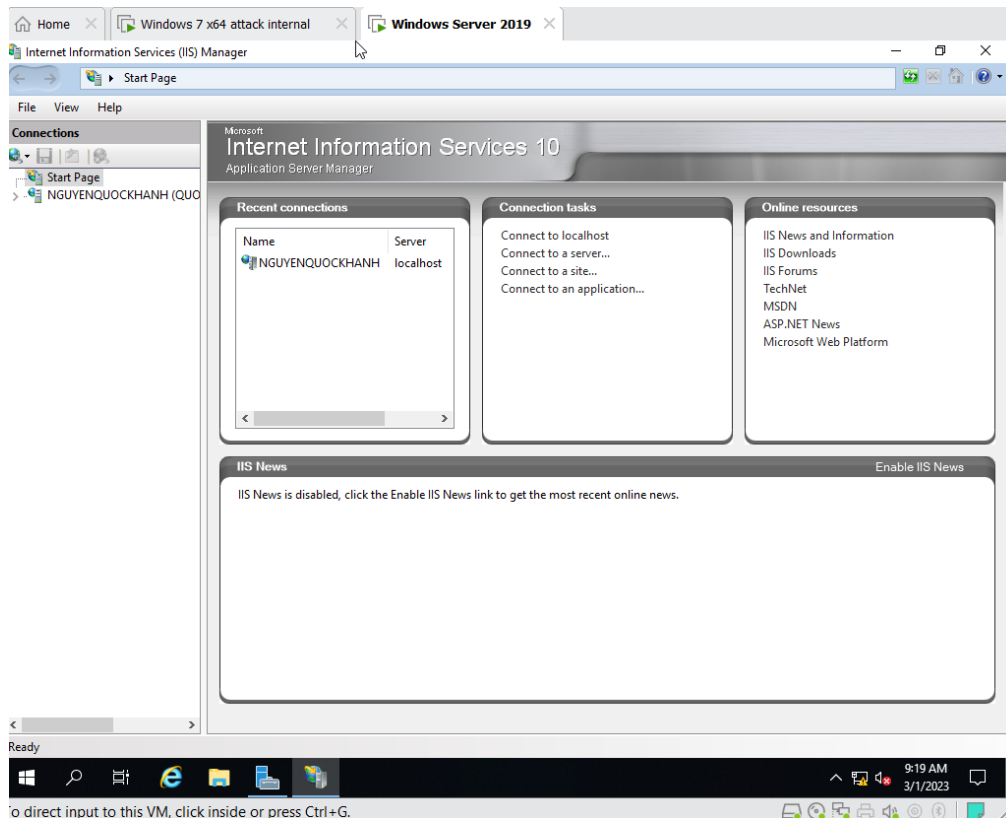
Nguyễn Quốc Khánh

Thay đổi mật khẩu

KhanhNQ.B20AT103

KhanhNQ.B20AT103

Hủy bỏ



B20DCAT103

Nguyễn Quốc Khánh

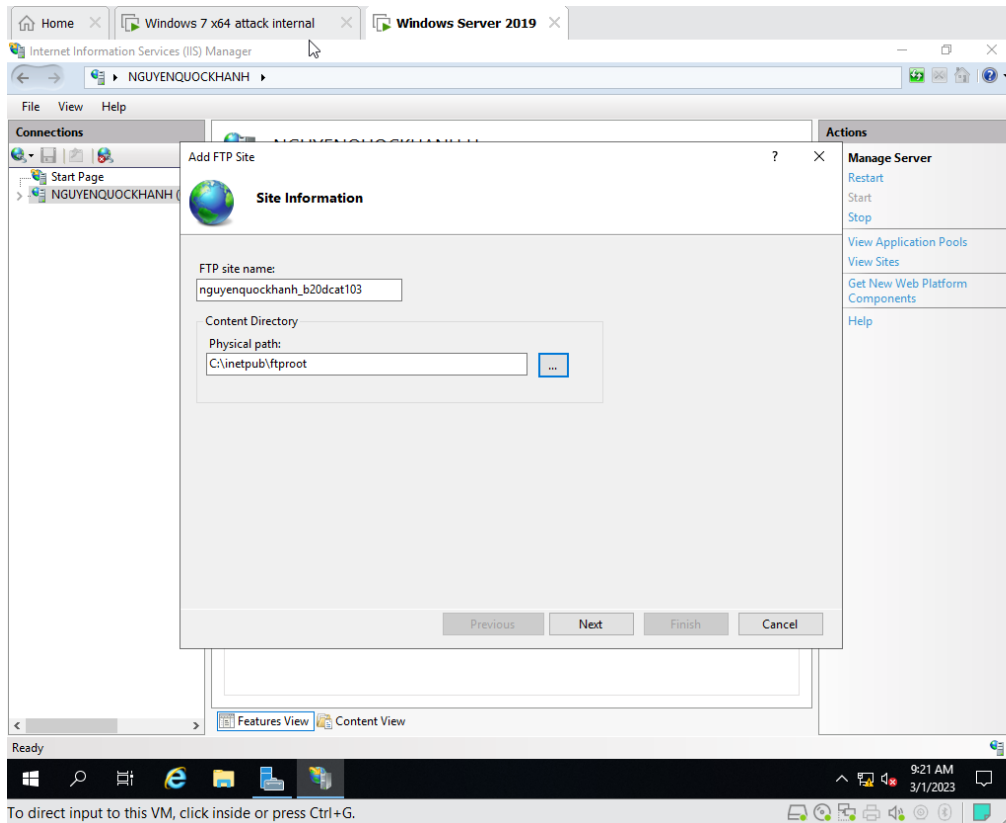
Thay đổi mật khẩu

KhanhNQ.B20AT103

KhanhNQ.B20AT103

Hủy bỏ

Cài đặt và cấu hình thành công FTP Server trong Web Server:



B20DCAT103

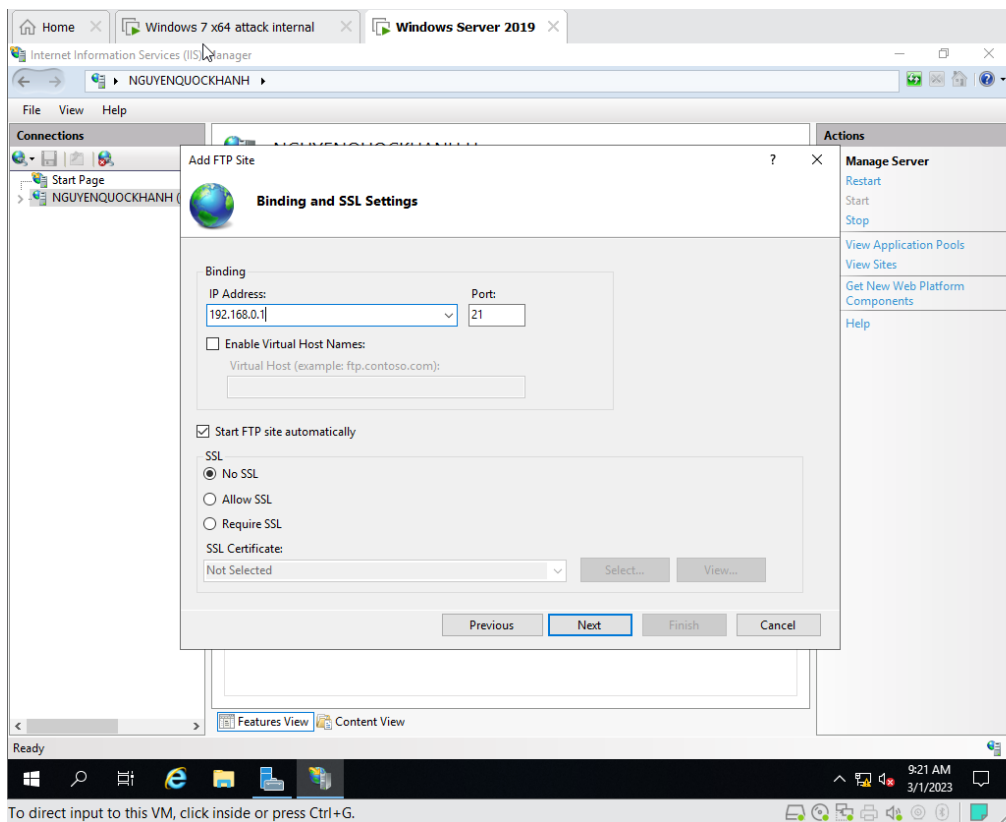
Nguyễn Quốc Khánh

Thay đổi mật khẩu

KhanhNQ.B20AT103

KhanhNQ.B20AT103

Hủy bỏ



B20DCAT103

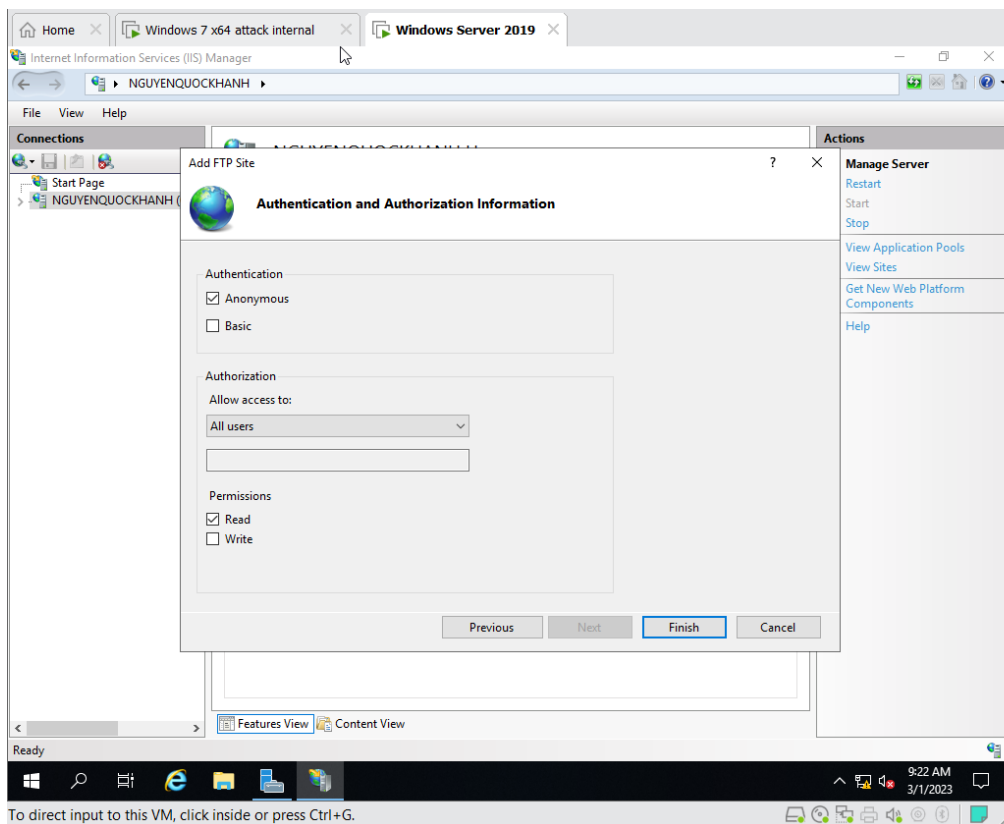
Nguyễn Quốc Khánh

Thay đổi mật khẩu

KhanhNQ.B20AT103

KhanhNQ.B20AT103

Hủy bỏ



B20DCAT103

Nguyễn Quốc Khánh

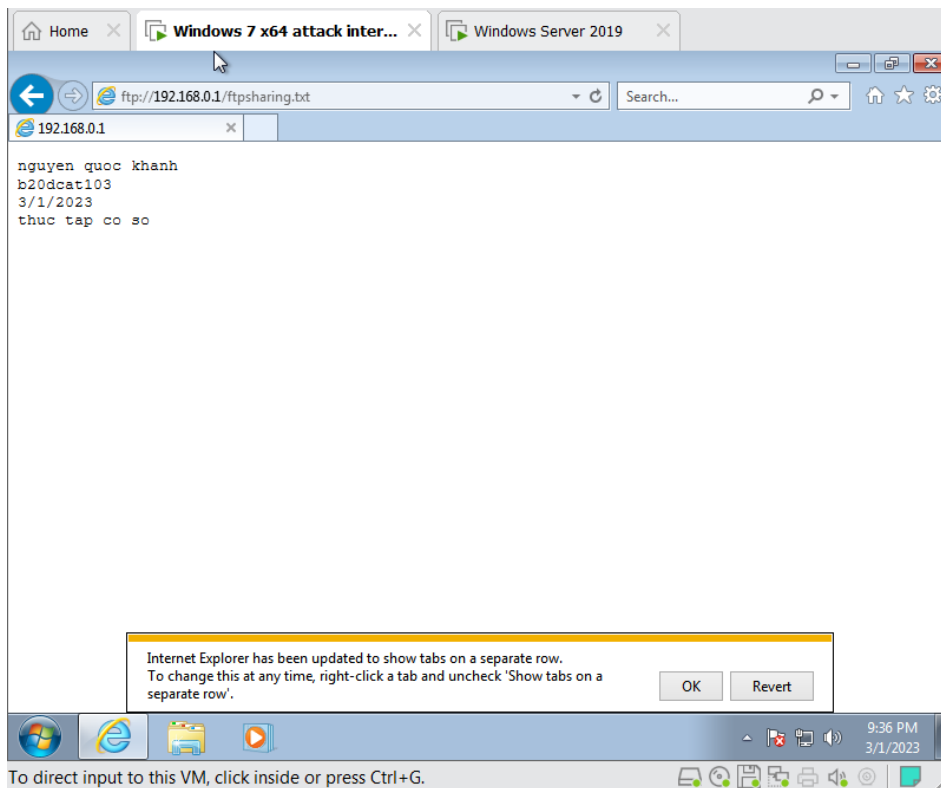
Thay đổi mật khẩu

KhanhNQ.B20AT103

KhanhNQ.B20AT103

Hủy bỏ

Truy cập được file ftpsharing thành công từ FTP Server:



B20DCAT103

Nguyễn Quốc Khánh

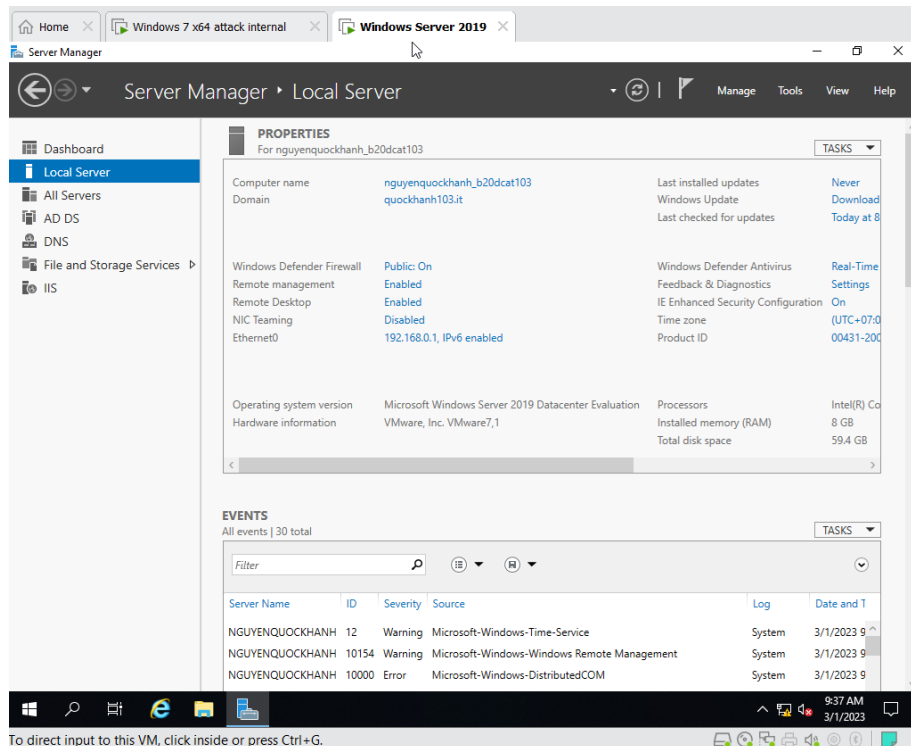
Thay đổi mật khẩu

KhanhNQ.B20AT103

KhanhNQ.B20AT103

Hủy bỏ

Cài đặt Remote Desktop trong Server Manager:



B20DCAT103

Nguyễn Quốc Khánh

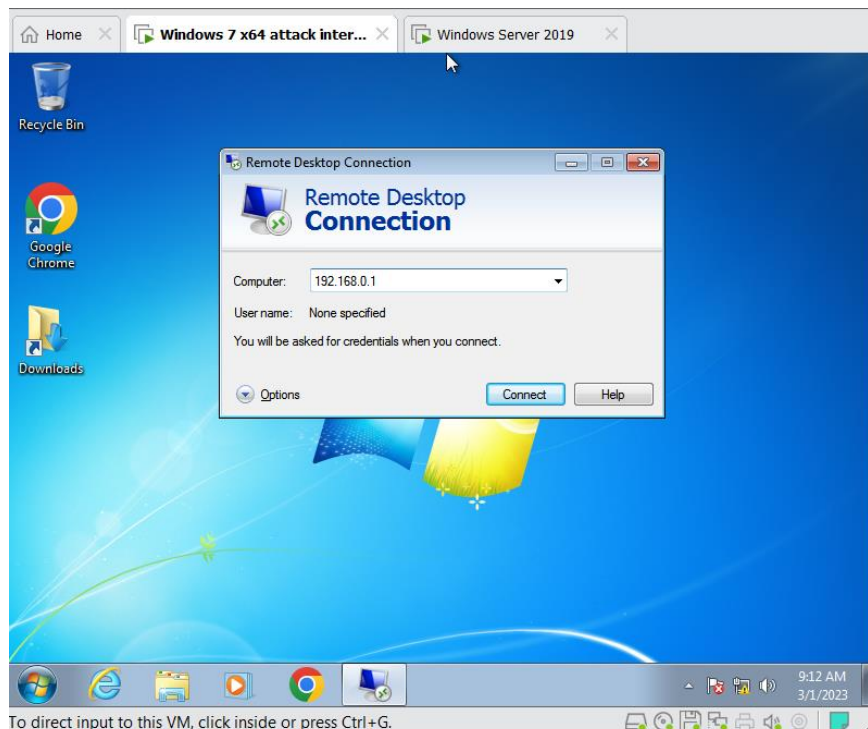
Thay đổi mật khẩu

KhanhNQ.B20AT103

KhanhNQ.B20AT103

Hủy bỏ

Máy trạm sử dụng phần mềm Remote Desktop Connection nhập IP, tài khoản administrator và mật khẩu của máy Server:



B20DCAT103

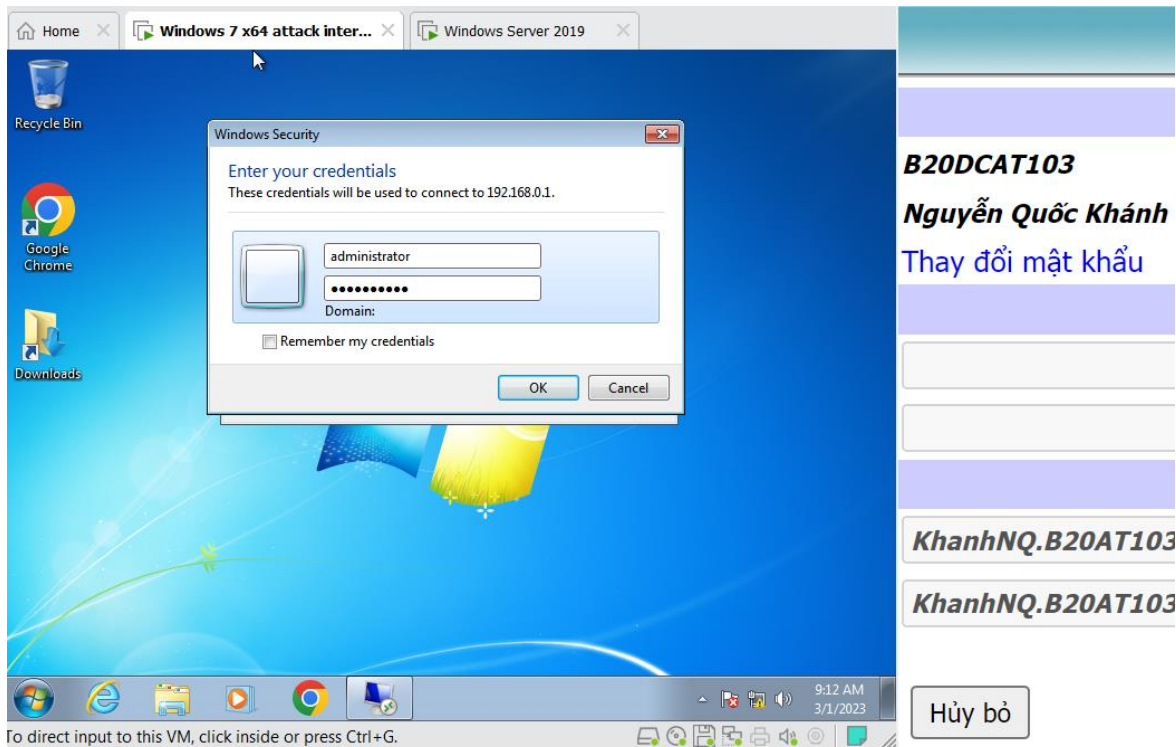
Nguyễn Quốc Khánh

Thay đổi mật khẩu

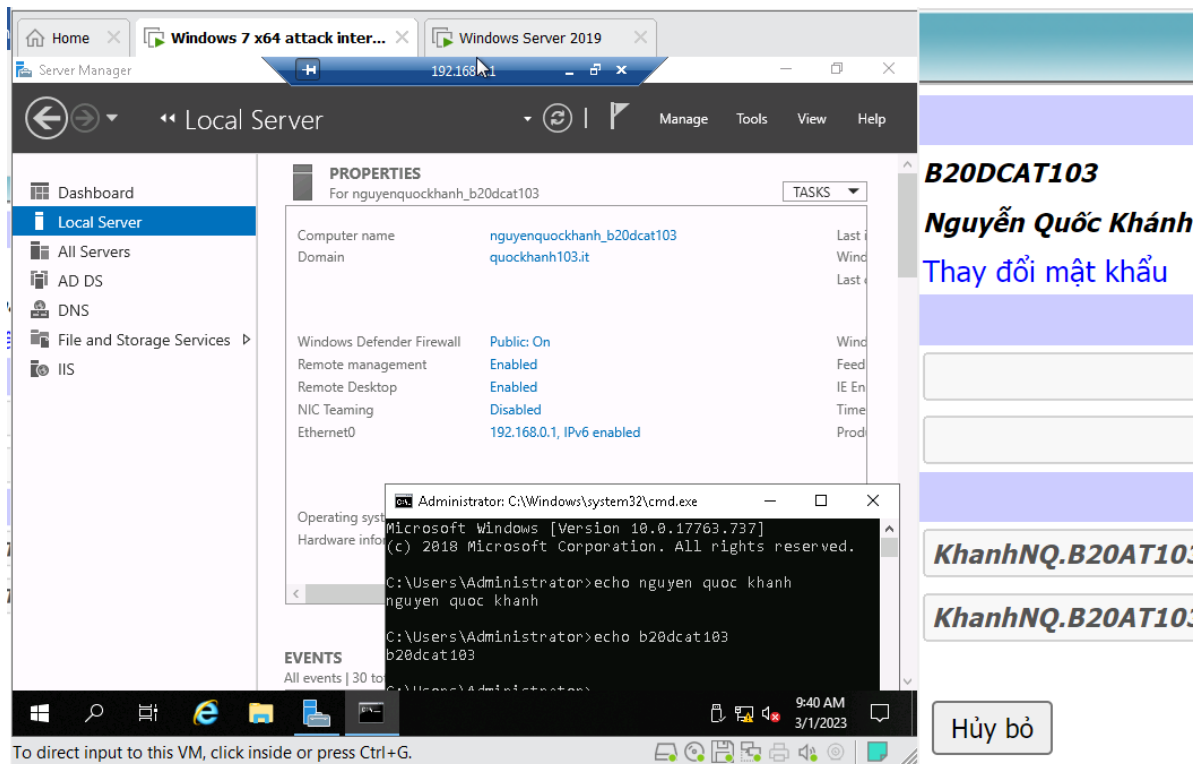
KhanhNQ.B20AT103

KhanhNQ.B20AT103

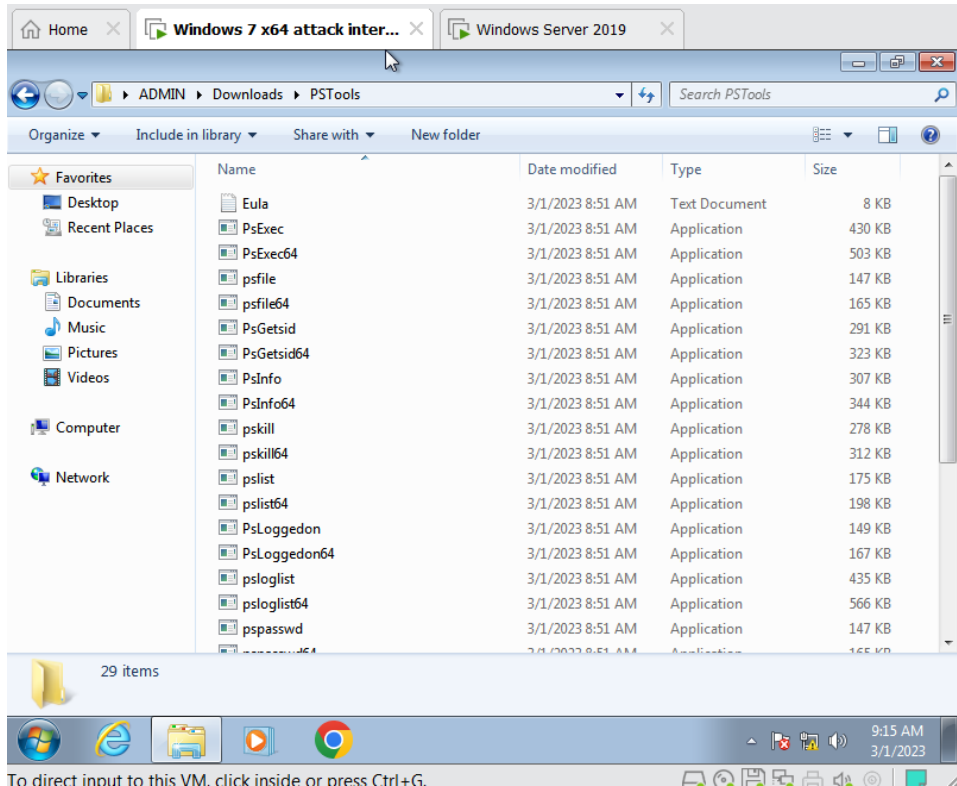
Hủy bỏ



Máy trạm sử dụng remote máy chủ thành công:



Tải công cụ PSTools và giải nén trong máy trạm Windows:



Windows 7 x64 attack inter... Windows Server 2019

ADMIN > Downloads > PSTools

Search PSTools

Organize Include in library Share with New folder

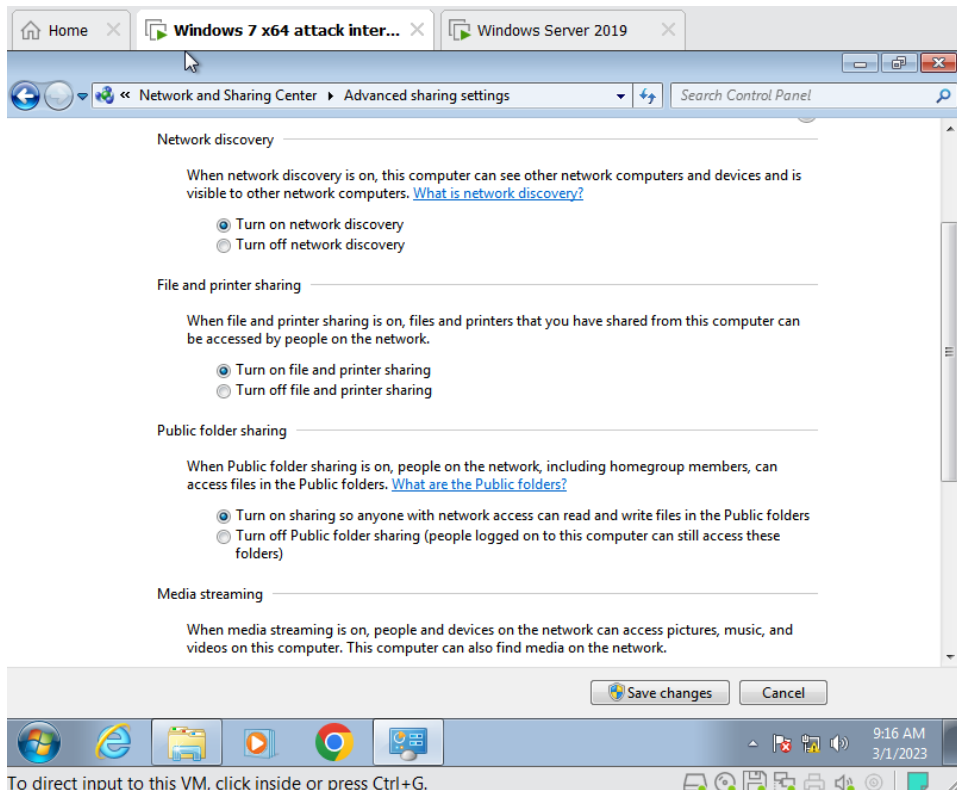
Name	Date modified	Type	Size
Eula	3/1/2023 8:51 AM	Text Document	8 KB
PSEXEC	3/1/2023 8:51 AM	Application	430 KB
PSEXEC64	3/1/2023 8:51 AM	Application	503 KB
psfile	3/1/2023 8:51 AM	Application	147 KB
psfile64	3/1/2023 8:51 AM	Application	165 KB
PsGetsid	3/1/2023 8:51 AM	Application	291 KB
PsGetsid64	3/1/2023 8:51 AM	Application	323 KB
PsInfo	3/1/2023 8:51 AM	Application	307 KB
PsInfo64	3/1/2023 8:51 AM	Application	344 KB
pskill	3/1/2023 8:51 AM	Application	278 KB
pskill64	3/1/2023 8:51 AM	Application	312 KB
pslist	3/1/2023 8:51 AM	Application	175 KB
pslist64	3/1/2023 8:51 AM	Application	198 KB
PsLoggedon	3/1/2023 8:51 AM	Application	149 KB
PsLoggedon64	3/1/2023 8:51 AM	Application	167 KB
psloglist	3/1/2023 8:51 AM	Application	435 KB
psloglist64	3/1/2023 8:51 AM	Application	566 KB
pspasswd	3/1/2023 8:51 AM	Application	147 KB
pspasswd64	3/1/2023 8:51 AM	Application	165 KB

29 items

9:15 AM 3/1/2023

To direct input to this VM, click inside or press Ctrl+G.

Hủy bỏ



Windows 7 x64 attack inter... Windows Server 2019

Network and Sharing Center > Advanced sharing settings

Search Control Panel

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. [What is network discovery?](#)

☒ Turn on network discovery
☐ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

☒ Turn on file and printer sharing
☐ Turn off file and printer sharing

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. [What are the Public folders?](#)

☒ Turn on sharing so anyone with network access can read and write files in the Public folders
☐ Turn off Public folder sharing (people logged on to this computer can still access these folders)

Media streaming

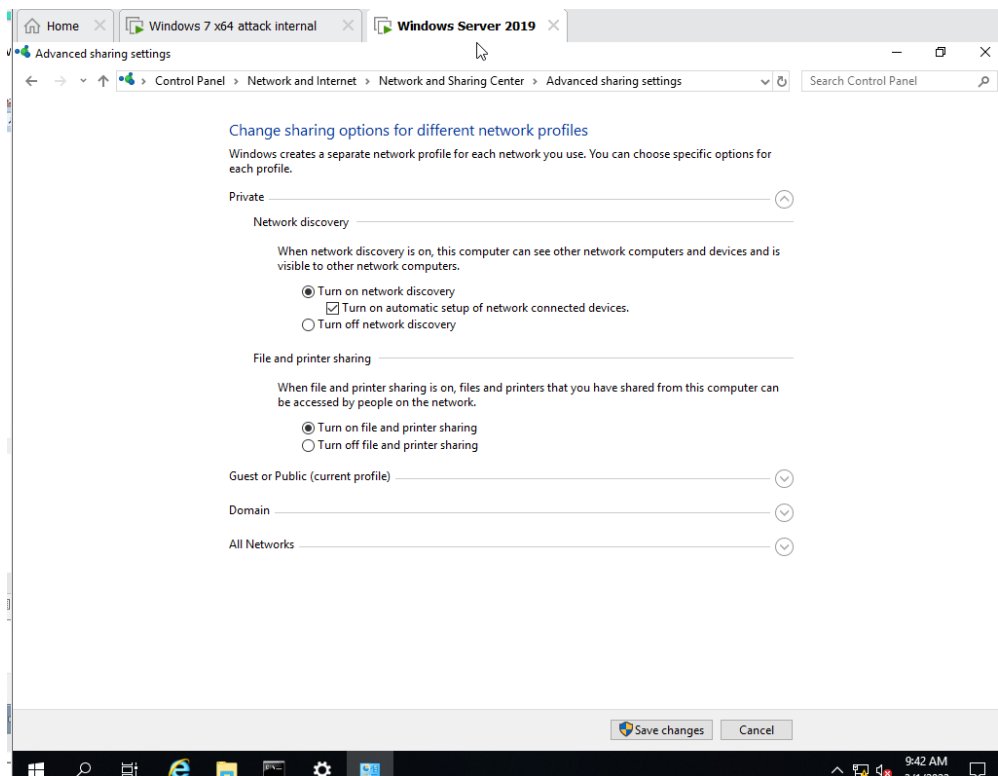
When media streaming is on, people and devices on the network can access pictures, music, and videos on this computer. This computer can also find media on the network.

Save changes Cancel

9:16 AM 3/1/2023

To direct input to this VM, click inside or press Ctrl+G.

Hủy bỏ



B20DCAT103

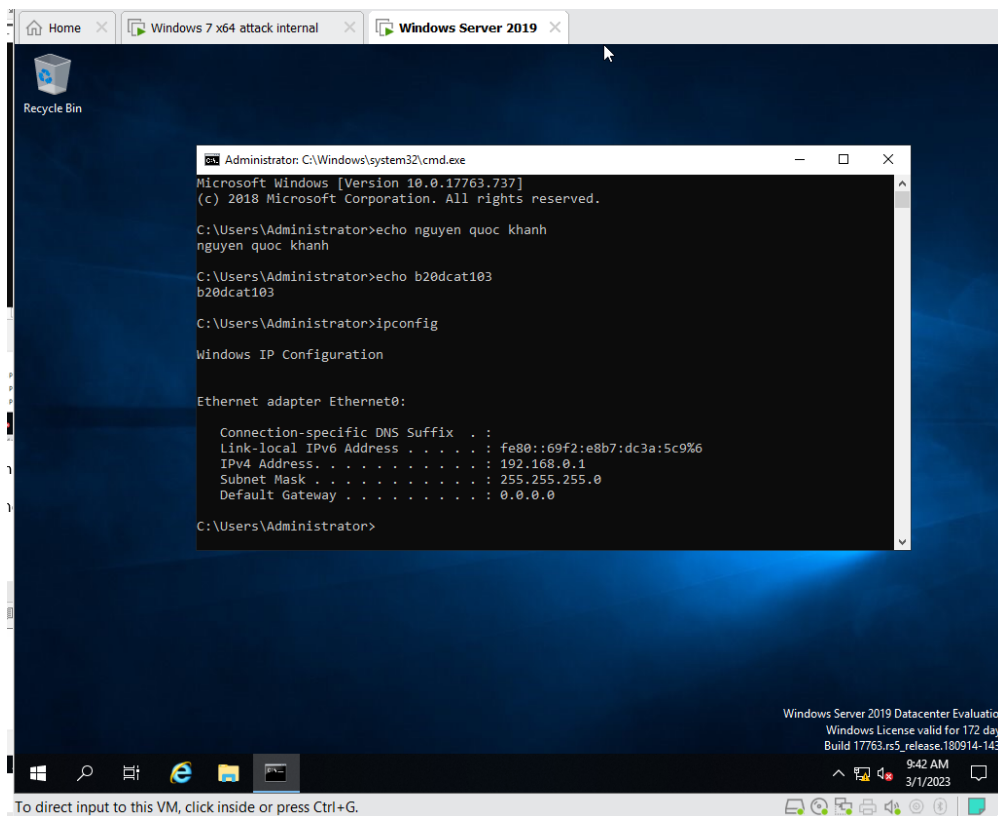
Nguyễn Quốc Khánh

Thay đổi mật khẩu

KhanhNQ.B20AT103

KhanhNQ.B20AT103

Hủy bỏ



B20DCAT103

Nguyễn Quốc Khánh

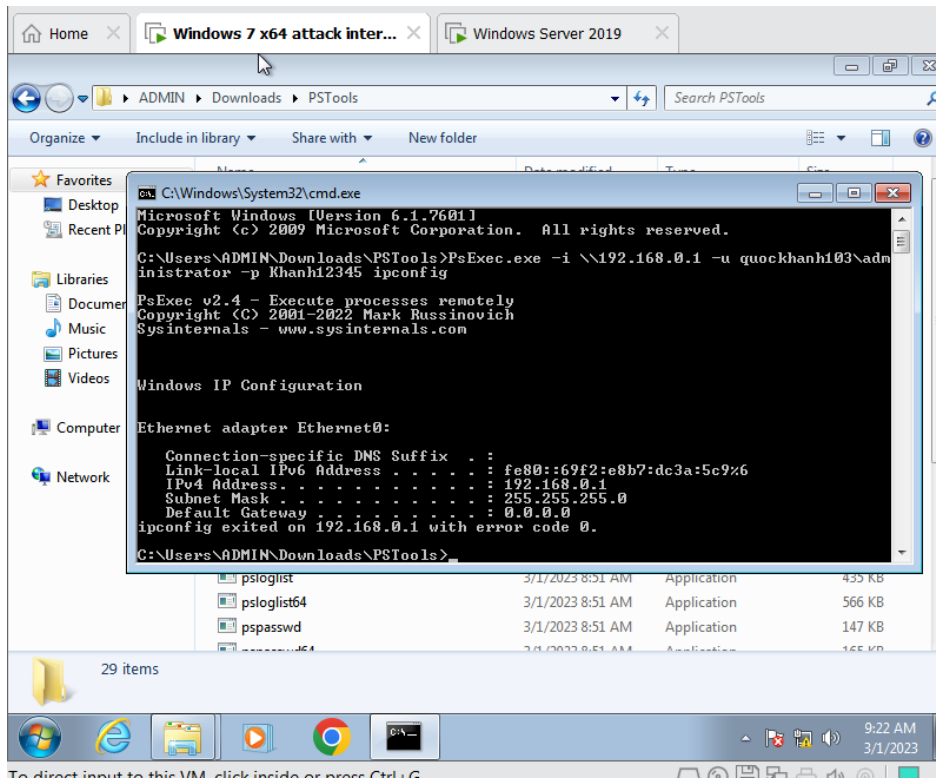
Thay đổi mật khẩu

KhanhNQ.B20AT103

KhanhNQ.B20AT103

Hủy bỏ

Sử dụng công cụ PSTools với cmd để kết nối tới máy Server:



B20DCAT103

Nguyễn Quốc Khánh

Thay đổi mật khẩu

KhanhNQ.B20AT103

KhanhNQ.B20AT103

Hủy bỏ