Tyler Sauter

Windows Fundamentals Skills Assessment

Documentation

1/22/2025

This documentation provides a step-by-step guide for setting up shared folders, creating and managing user accounts and security groups, and configuring permissions to ensure secure and organized access. Additionally, it covers how to use PowerShell for basic system management tasks.

Each step in this documentation is accompanied by a corresponding image to visually illustrate the process and provide clarity on what was done. These images serve as a practical reference, ensuring that the written instructions are easy to follow and accurately reflect the actions taken during setup. By combining detailed explanations with visual aids, this documentation ensures both precision and accessibility, making it suitable for professional environments.

1. Since this is a Windows machine, we first need to establish an RDP connection using the xfreerdp command. This involves entering the valid IP address and the correct user credentials to access the system.

2. Next, create a shared folder named Company_Data and enable sharing for this folder. Ensure proper configurations are set, including defining share permissions to control access.

3. Create a new user named Jim by navigating to compmgmt.msc, which provides access to various system tools, including user and group management. Locate the Users folder, and from there, add a new user by specifying the required details and setting appropriate options, such as unchecking "User must change password at logon."

4. Create a security group named HR using the same application (compmgmt.msc). Navigate to the Groups section, create a new group named HR, and add Jim as a member of this group to ensure appropriate permissions and access management.

5. Navigate back to the Company_Data folder and add the HR group to the share permissions. Assign the group the Change and Read permissions to control access effectively.

6. Now, add the HR security group to the Company_Data folder's permissions. Navigate to the folder's Properties, go to the Security tab, and add the HR group. Assign the following NTFS permissions to the group:
    - Modify
    - Read & Execute
    - List folder contents
    - Read
    - Write

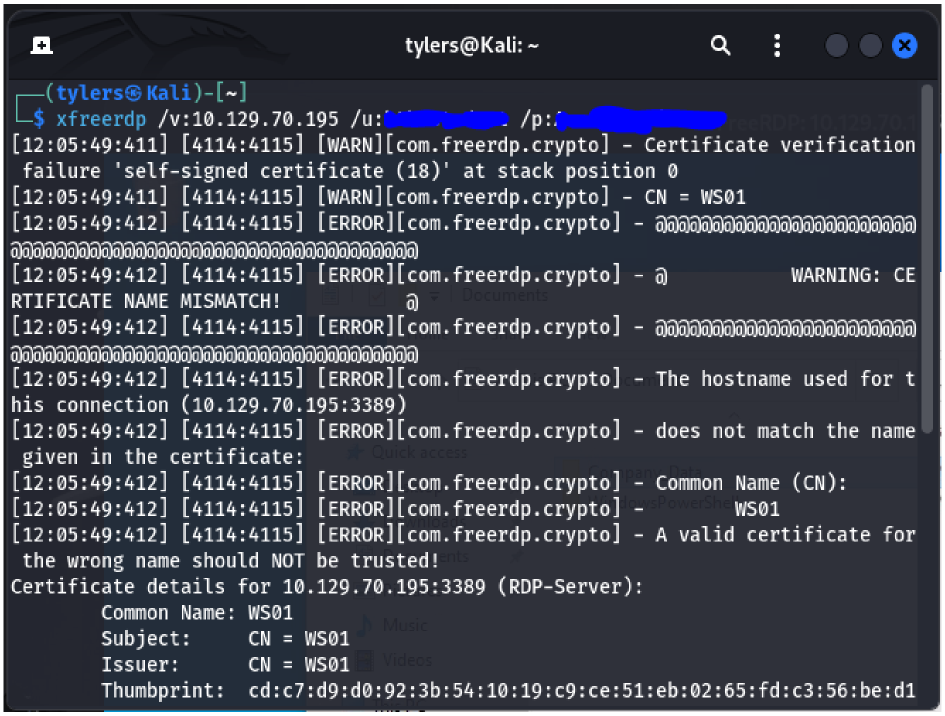
7. Next, disable inheritance on the Company_Data folder. This allows for more granular control over permissions, ensuring that only explicitly defined access rules apply. Disabling inheritance is especially critical for securing files with sensitive information.

8. Repeat the same process for the HR subfolder within the Company_Data folder. Add the HR security group, assign the appropriate NTFS permissions, and disable inheritance to ensure precise control over the folder's access and security.

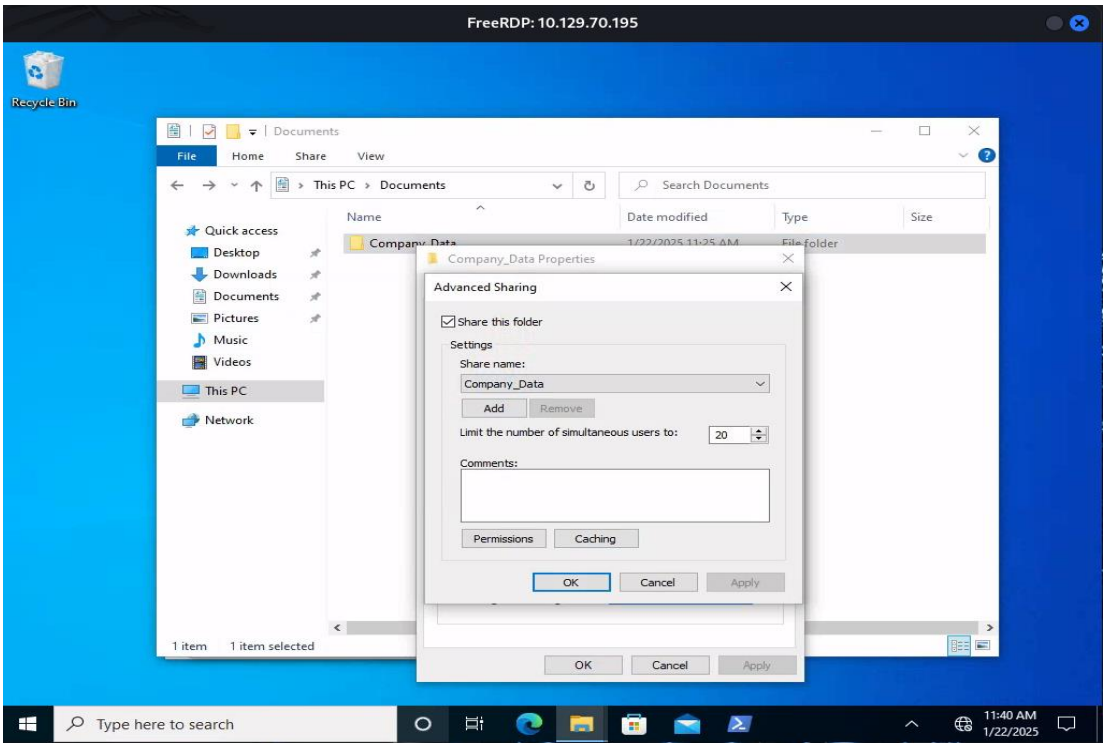
9. Using PowerShell, you can easily retrieve the SIDs for both the user Jim and the security group HR we created. To find the SID for Jim, run the command Get-LocalUser -Name Jim | Select-Object Name, SID. Similarly, to find the SID for the HR group, use Get-LocalGroup -Name HR | Select-Object Name, SID. These commands are valuable in identifying users or groups, managing access control, and troubleshooting permissions. They ensure precise and efficient management of system resources in professional environments.

This documentation demonstrated how to set up shared folders, configure user and group permissions, and manage secure access effectively. These tasks are critical in a professional environment to ensure that resources are accessible to the right people while maintaining data security and compliance. Properly managing permissions, users, and groups lays the foundation for efficient collaboration, reduces the risk of unauthorized access, and streamlines administrative control in live enterprise systems.

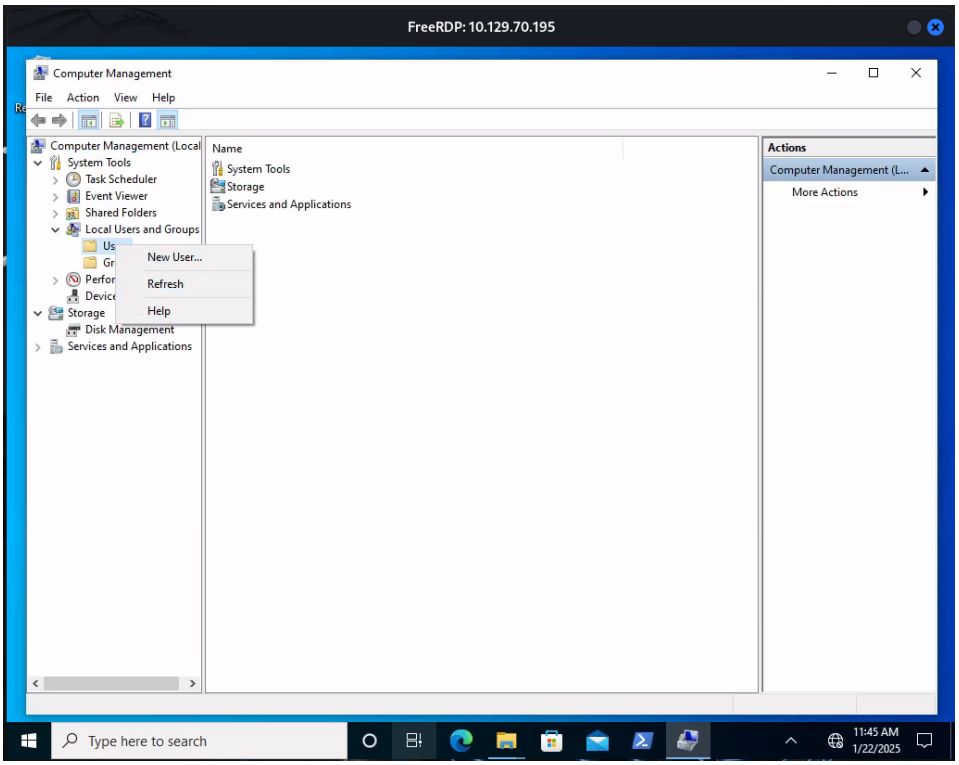
[1]

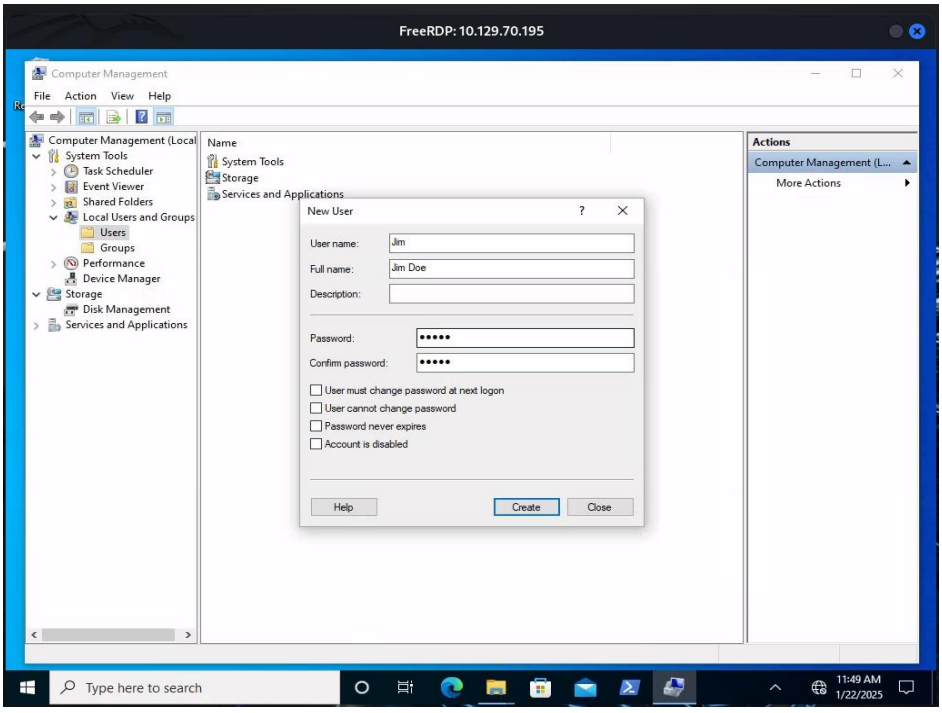

tylers@Kali: ~
┌──(tylers㉿Kali)-[~]
└─$ xfreerdp /v:10.129.70.195 /u:[redacted] /p:[redacted]
[12:05:49:411] [4114:4115] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[12:05:49:411] [4114:4115] [WARN][com.freerdp.crypto] - CN = WS01
[12:05:49:412] [4114:4115] [ERROR][com.freerdp.crypto] - @@@
[12:05:49:412] [4114:4115] [ERROR][com.freerdp.crypto] - @ WARNING: CERTIFICATE NAME MISMATCH! @
[12:05:49:412] [4114:4115] [ERROR][com.freerdp.crypto] - @@@
[12:05:49:412] [4114:4115] [ERROR][com.freerdp.crypto] - The hostname used for this connection (10.129.70.195:3389)
[12:05:49:412] [4114:4115] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[12:05:49:412] [4114:4115] [ERROR][com.freerdp.crypto] - Common Name (CN):
[12:05:49:412] [4114:4115] [ERROR][com.freerdp.crypto] - WS01
[12:05:49:412] [4114:4115] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 10.129.70.195:3389 (RDP-Server):
Common Name: WS01
Subject: CN = WS01
Issuer: CN = WS01
Thumbprint: cd:c7:d9:d0:92:3b:54:10:19:c9:ce:51:eb:02:65:fd:c3:56:be:d1

[2]

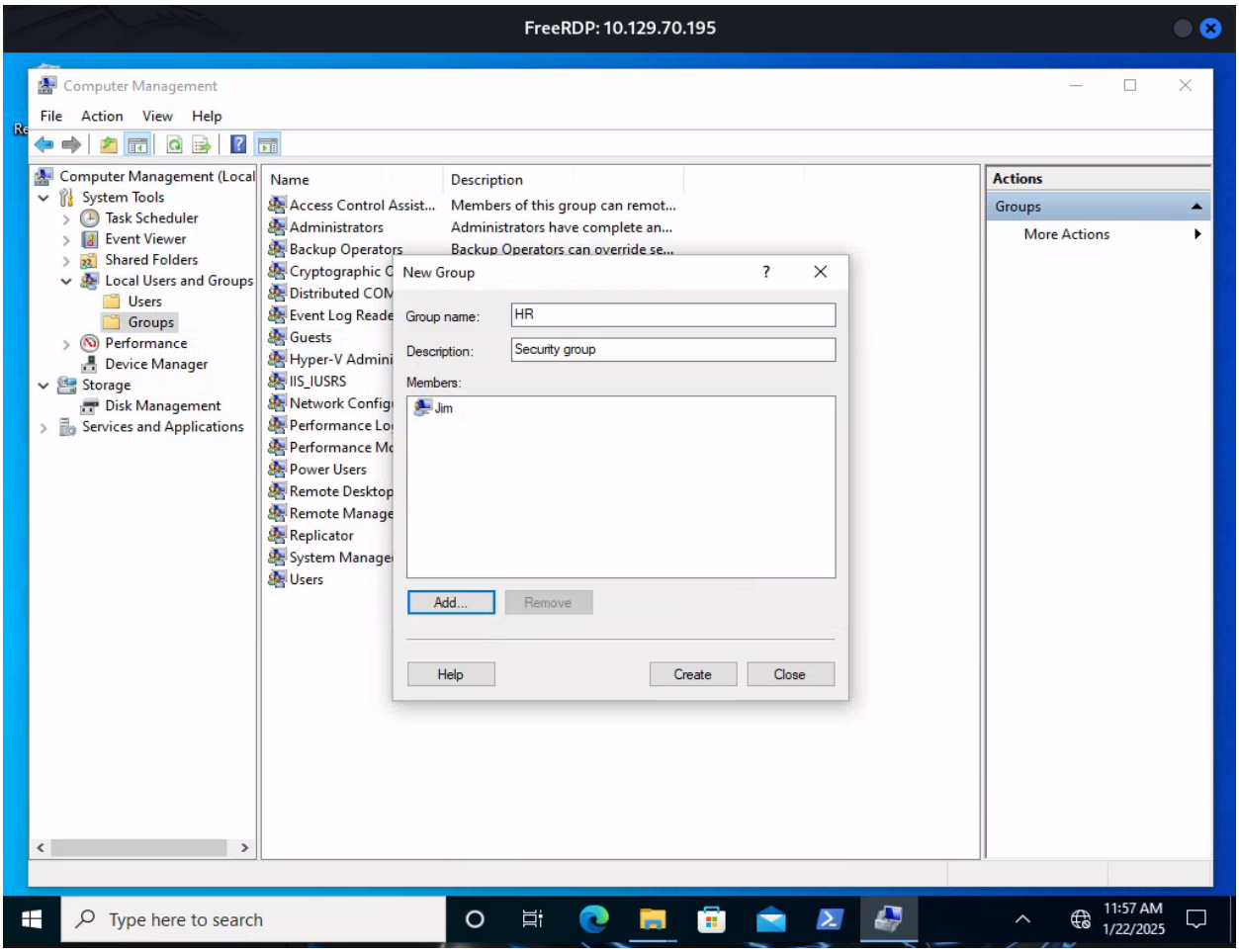

FreeRDP: 10.129.70.195
Recycle Bin
Documents
File
Home
Share
View
This PC › Documents
Search Documents
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Network
Name
Date modified
Type
Size
Company_Data
1/22/2025 11:35 AM
File folder
1 item
1 item selected
Company_Data Properties
Advanced Sharing
Share this folder
Settings
Share name:
Company_Data
Add
Remove
Limit the number of simultaneous users to:
20
Comments:
Permissions
Caching
OK
Cancel
Apply
OK
Cancel
Apply
Type here to search
11:40 AM
1/22/2025

[3]

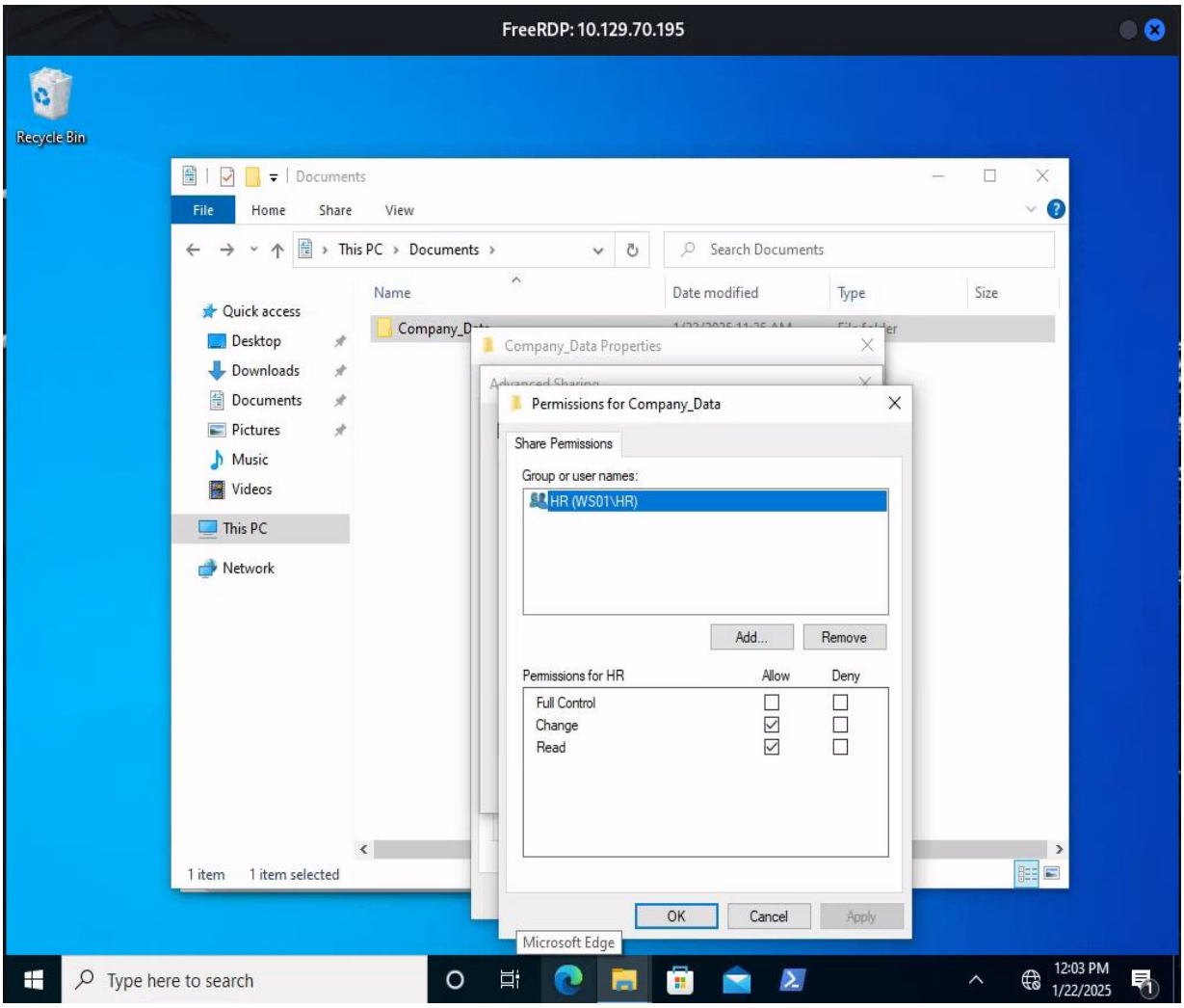

FreeRDP: 10.129.70.195
Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
New User...
Refresh
Help
Storage
Disk Management
Services and Applications
Name
System Tools
Storage
Services and Applications
Actions
Computer Management (L...
More Actions
Type here to search
11:45 AM
1/22/2025


FreeRDP: 10.129.70.195
Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
System Tools
Storage
Services and Applications
New User
User name: Jim
Full name: Jim Doe
Description:
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
Help
Create
Close
Actions
Computer Management (L...
More Actions
Type here to search
11:49 AM
1/22/2025

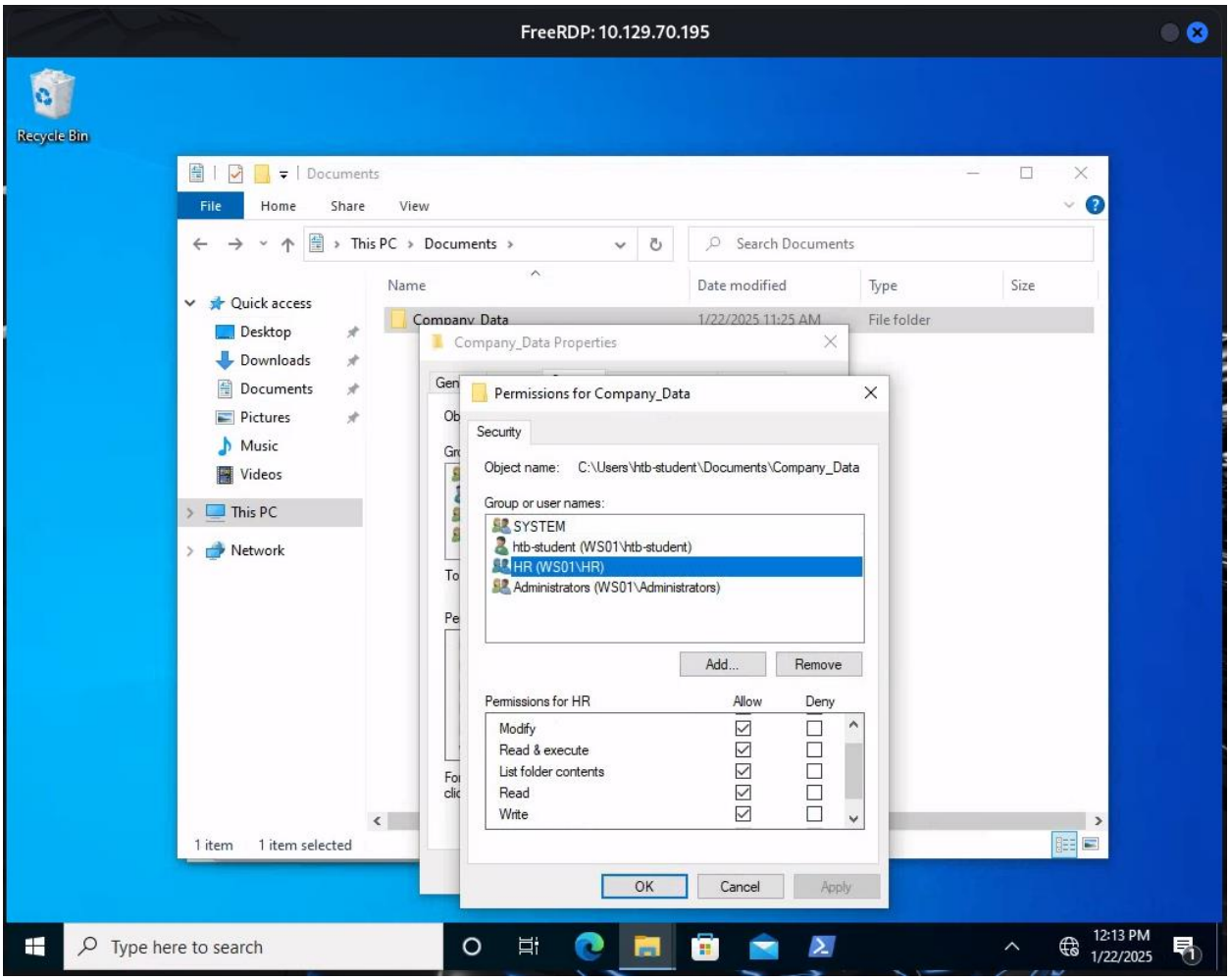
[4]


FreeRDP: 10.129.70.195
Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Description
Access Control Assist...
Members of this group can remot...
Administrators
Administrators have complete an...
Backup Operators
Backup Operators can override se...
Guests
IIS_IUSRS
Power Users
Replicator
Users
New Group
Group name:
HR
Description:
Security group
Members:
Jim
Add...
Remove
Help
Create
Close
Actions
Groups
More Actions
Type here to search
11:57 AM
1/22/2025

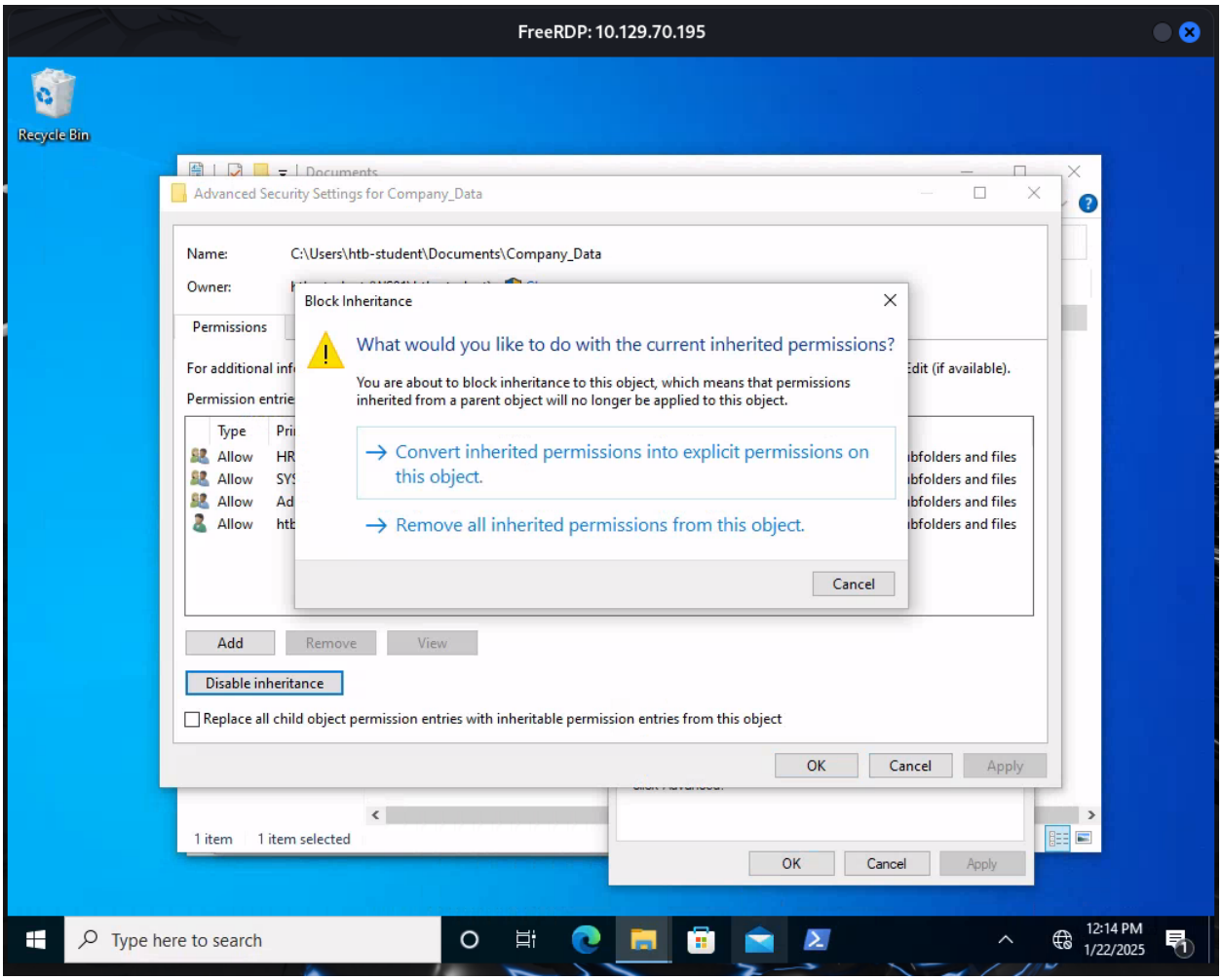
[5]


FreeRDP: 10.129.70.195
Recycle Bin
Documents
File
Home
Share
View
This PC › Documents ›
Search Documents
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Network
Name
Date modified
Type
Size
Company_Data Properties
Permissions for Company_Data
Share Permissions
Group or user names:
HR (WS01\HR)
Add...
Remove
Permissions for HR
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply
1 item
1 item selected
Microsoft Edge
Type here to search
12:03 PM
1/22/2025

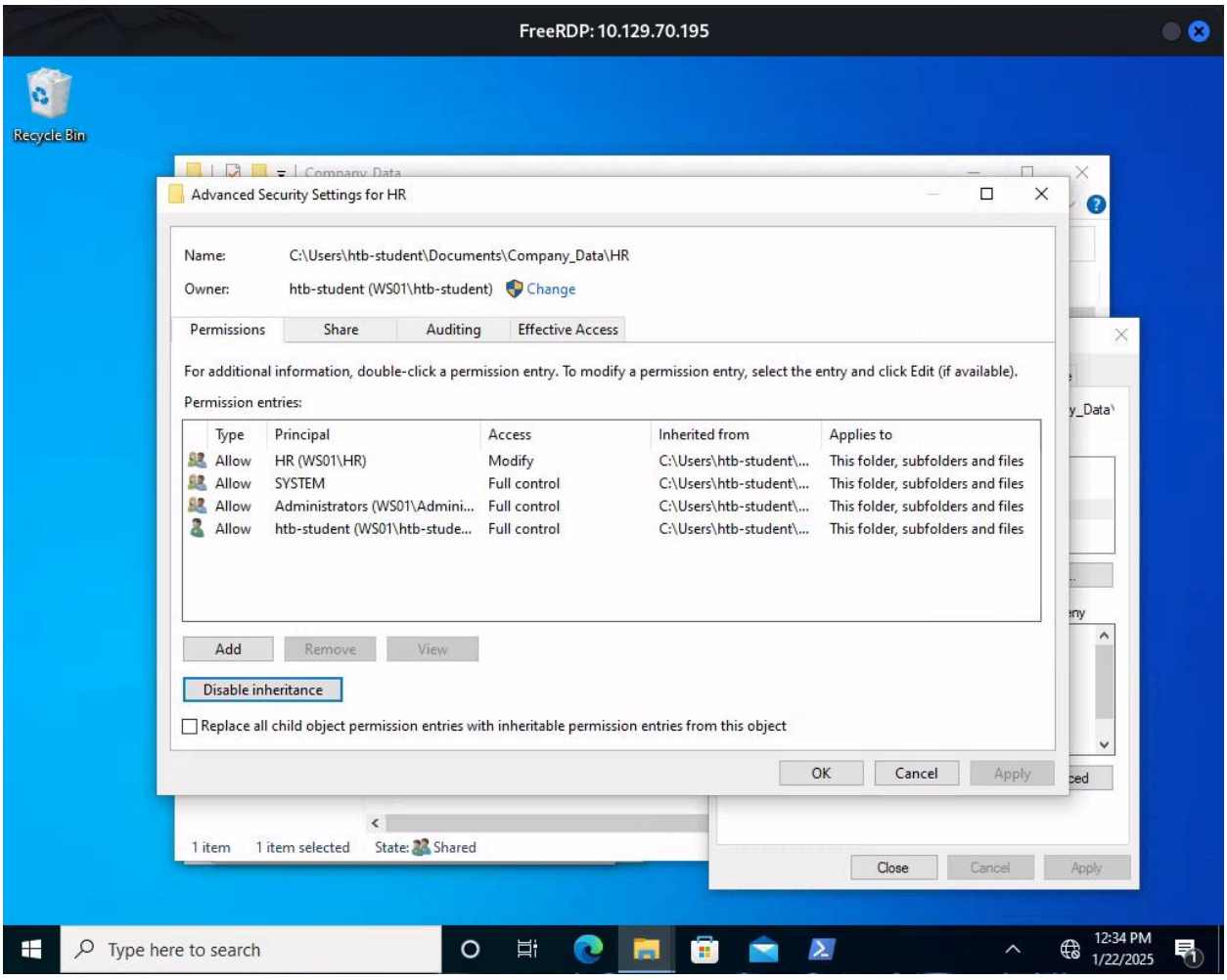
[6]


FreeRDP: 10.129.70.195
Recycle Bin
Documents
File
Home
Share
View
This PC
Documents
Search Documents
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Network
Name
Date modified
Type
Size
Company_Data
1/22/2025 11:25 AM
File folder
1 item
1 item selected
Company_Data Properties
Permissions for Company_Data
Security
Object name: C:\Users\htb-student\Documents\Company_Data
Group or user names:
SYSTEM
htb-student (WS01\htb-student)
HR (WS01\HR)
Administrators (WS01\Administrators)
Add...
Remove
Permissions for HR
Allow
Deny
Modify
Read & execute
List folder contents
Read
Write
OK
Cancel
Apply
Type here to search
12:13 PM
1/22/2025

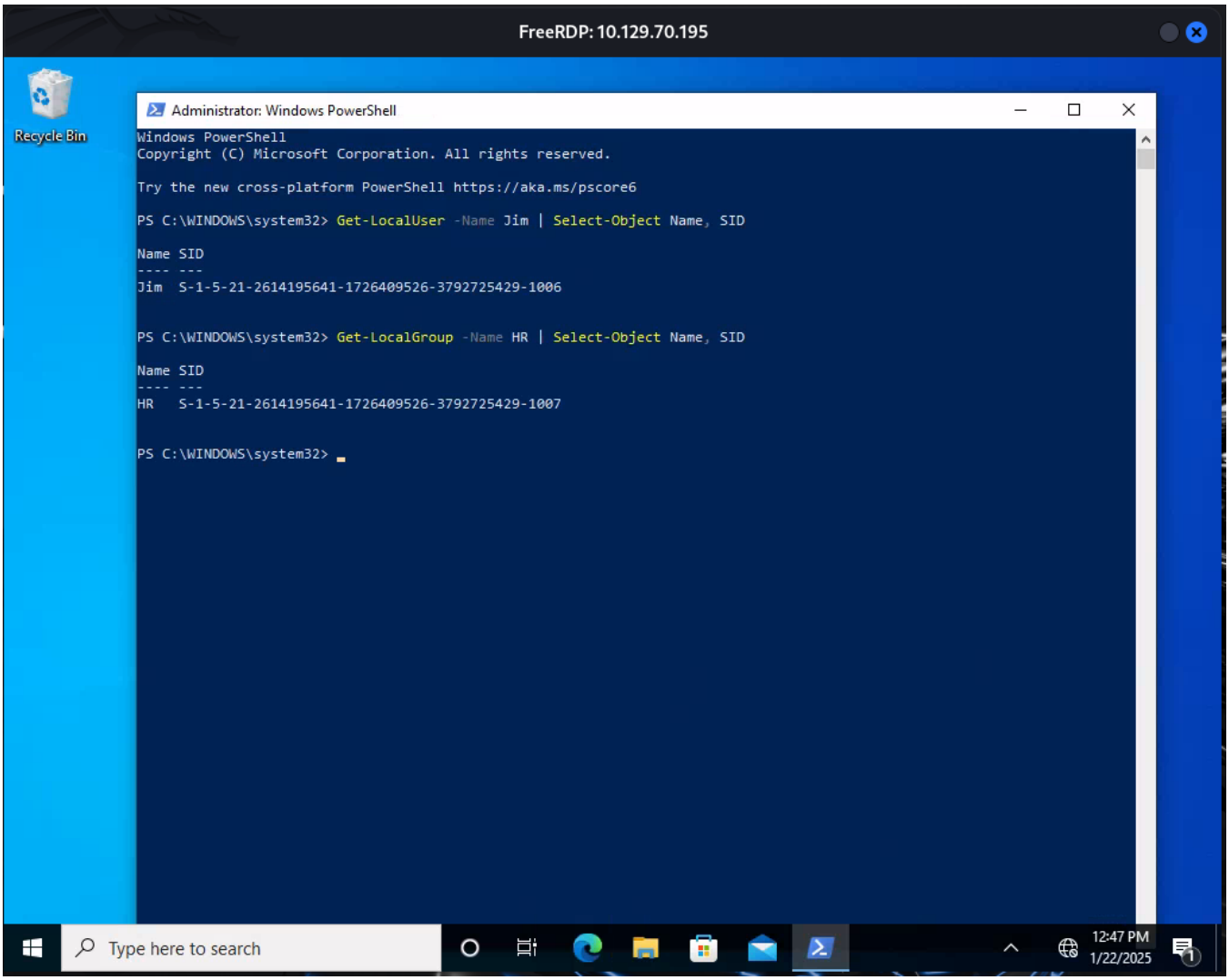
[7]


FreeRDP: 10.129.70.195
Recycle Bin
Advanced Security Settings for Company_Data
Name: C:\Users\htb-student\Documents\Company_Data
Owner:
Permissions
Block Inheritance
What would you like to do with the current inherited permissions?
You are about to block inheritance to this object, which means that permissions inherited from a parent object will no longer be applied to this object.
Convert inherited permissions into explicit permissions on this object.
Remove all inherited permissions from this object.
Cancel
Add
Remove
View
Disable inheritance
Replace all child object permission entries with inheritable permission entries from this object
OK
Cancel
Apply
1 item
1 item selected
Type here to search
12:14 PM
1/22/2025

[8]


FreeRDP: 10.129.70.195
Recycle Bin
Company_Data
Advanced Security Settings for HR
Name: C:\Users\htb-student\Documents\Company_Data\HR
Owner: htb-student (WS01\htb-student) Change
Permissions Share Auditing Effective Access
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).
Permission entries:
Type Principal Access Inherited from Applies to
Allow HR (WS01\HR) Modify C:\Users\htb-student\... This folder, subfolders and files
Allow SYSTEM Full control C:\Users\htb-student\... This folder, subfolders and files
Allow Administrators (WS01\Admini... Full control C:\Users\htb-student\... This folder, subfolders and files
Allow htb-student (WS01\htb-stude... Full control C:\Users\htb-student\... This folder, subfolders and files
Add Remove View
Disable inheritance
Replace all child object permission entries with inheritable permission entries from this object
OK Cancel Apply
1 item 1 item selected State: Shared
Close Cancel Apply
Type here to search
12:34 PM
1/22/2025

[9]


FreeRDP: 10.129.70.195
Recycle Bin
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\WINDOWS\system32> Get-LocalUser -Name Jim | Select-Object Name, SID
Name SID
---- ---
Jim S-1-5-21-2614195641-1726409526-3792725429-1006
PS C:\WINDOWS\system32> Get-LocalGroup -Name HR | Select-Object Name, SID
Name SID
---- ---
HR S-1-5-21-2614195641-1726409526-3792725429-1007
PS C:\WINDOWS\system32>
Type here to search
12:47 PM
1/22/2025