|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test 2 Practical** | | | | |
|  | OSSE | 1060 |  |

|  |
| --- |
| Introduction |

* Complete the listed tasks. Provide screenshots proving the work. The screenshot must provide enough proof that the question objective has been met. The quality and validity of the screenshot, as well as the value of the screenshot, is determined by the instructor.

|  |
| --- |
| Objectives |

* Pass the test.

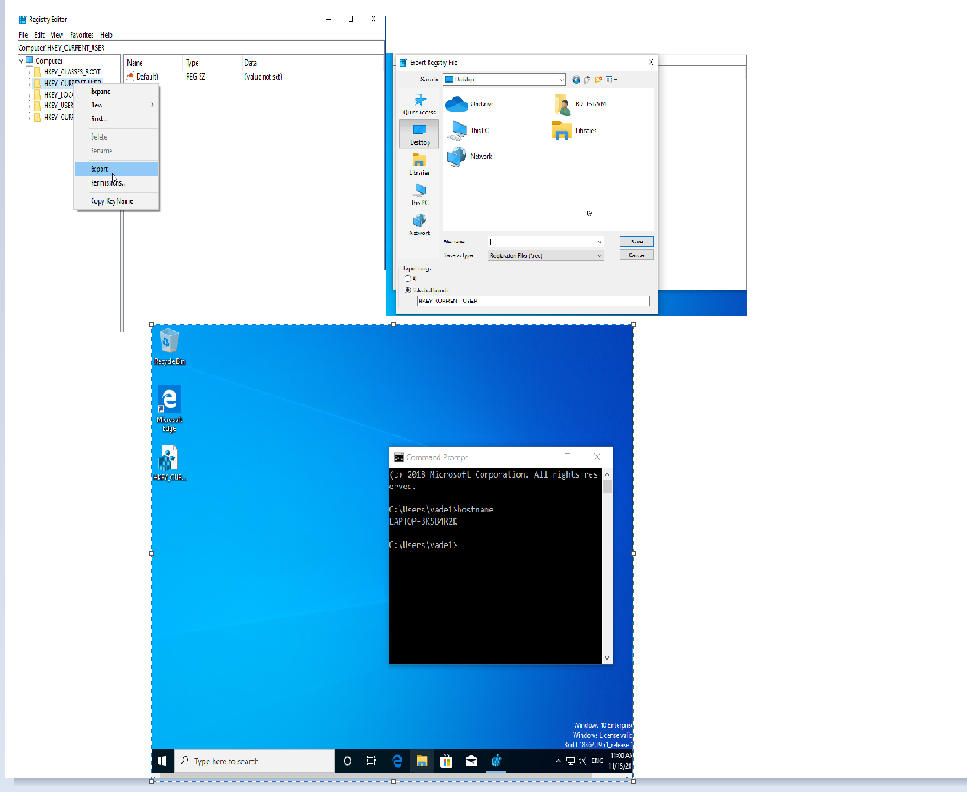
|  |
| --- |
| Test Materials and Setup |

* Newly create Windows 10 VM, approved by the instructor.

|  |
| --- |
| Activity |

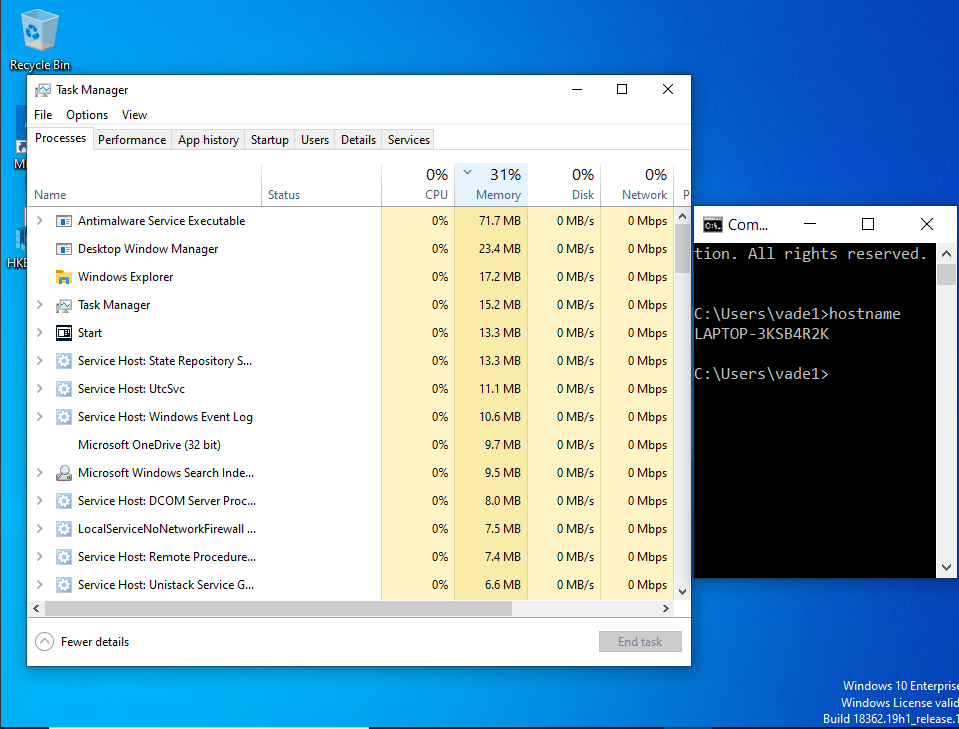
1. Backup the Root Key for the current user. Screenshot: capture/depict the process of backing up the registry root key (take a screenshot that demonstrates the process). Make sure you actually do the backup.

|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |



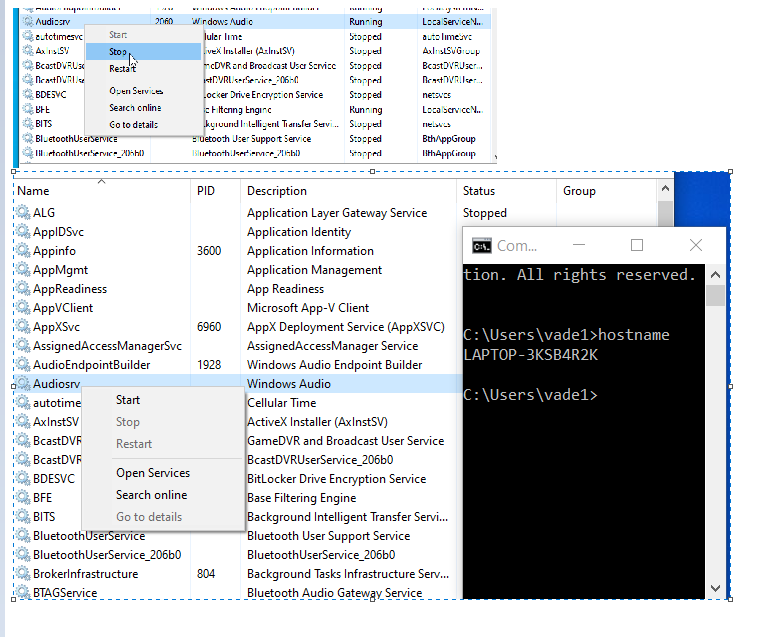
1. Display running processes, in task manager, sorted by Memory usage (highest to lowest).

|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |



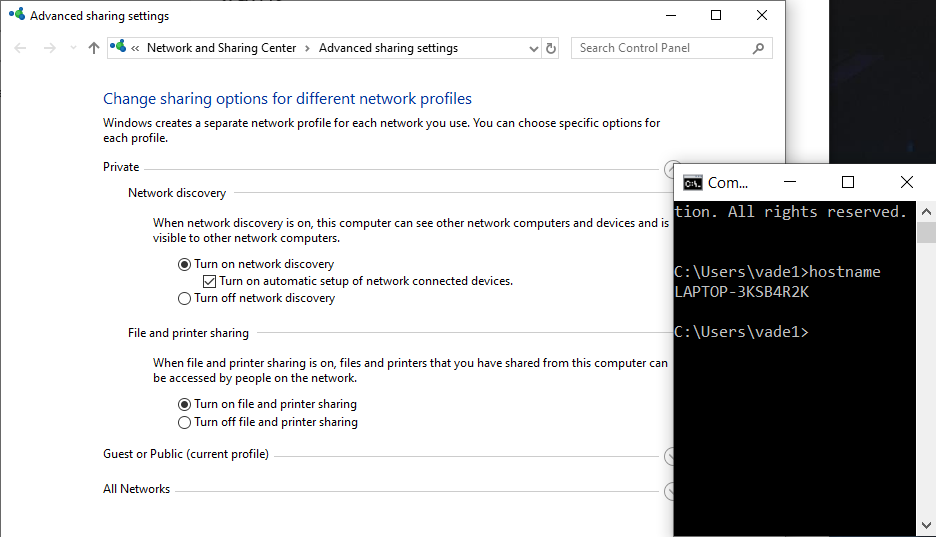
1. Restart the ‘Windows Audio’ service. Screenshot: capture/depict the process of restarting the service.

|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |



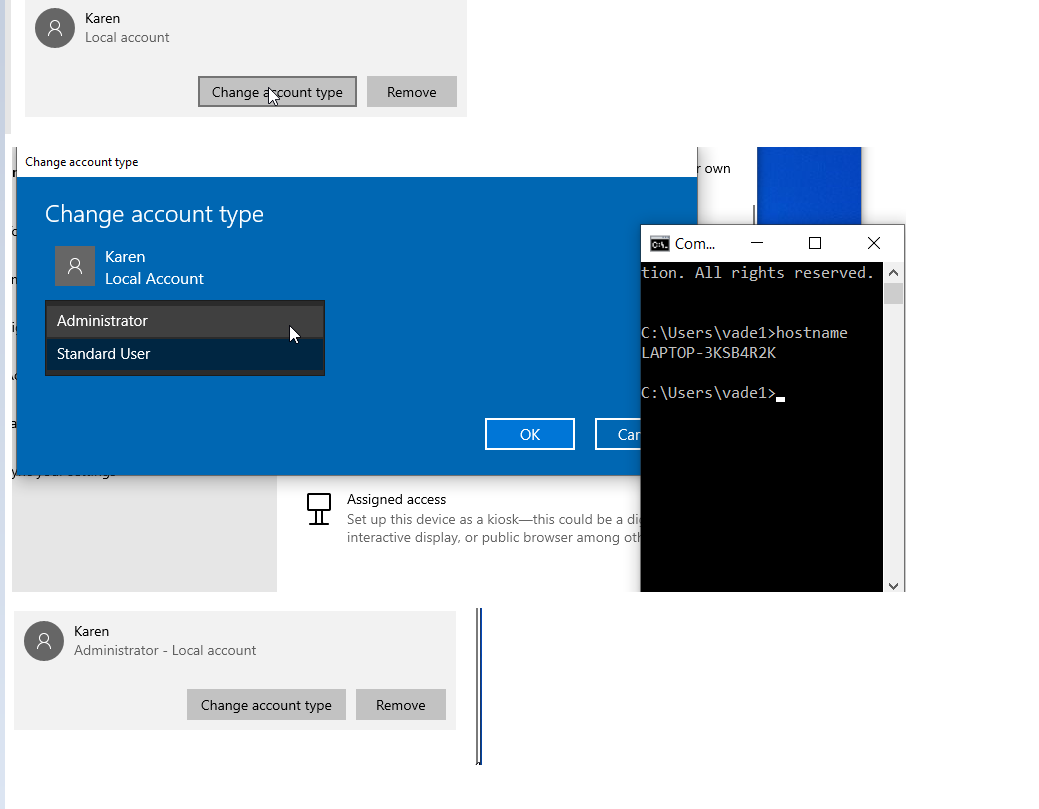
1. Set the current connected network as a ‘Private’ network and turn on ‘network discovery’ and ‘file and print sharing’ for private networks. Screenshot: show the network is set to private and network discovery and file and print sharing is turned on.

|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |



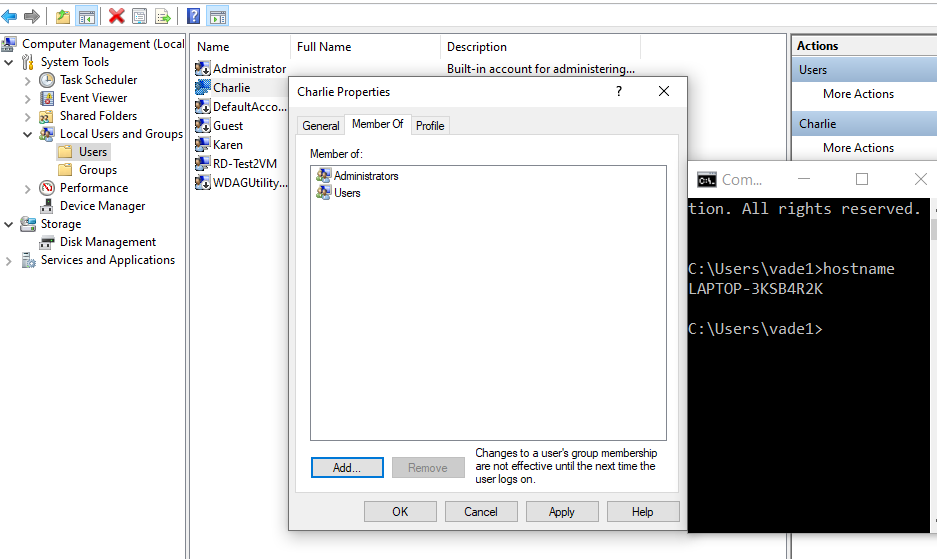
1. Create an administrative user called ‘Karen’ using the ‘Account’s’ Windows App, in Settings. Screenshot: show the *method* of creating an administrative account using the ‘Account’s’ Windows App in Settings.

|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |



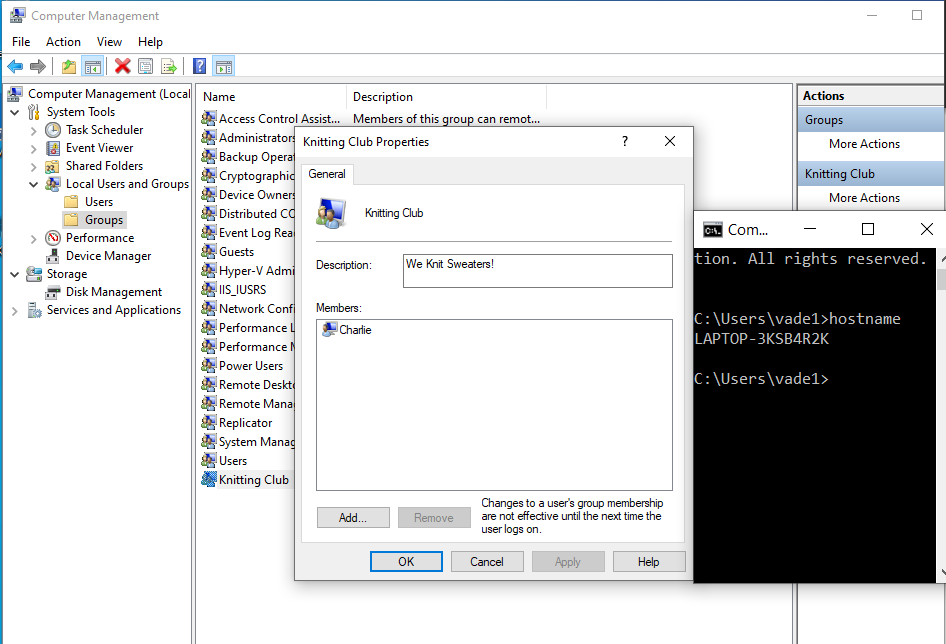
1. Create an administrative user called ‘Charlie’ using the Local Users and Groups Snap-in. Screenshot: prove that the user is an admin user using *only* the Local Users and Groups snap-in.

|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |



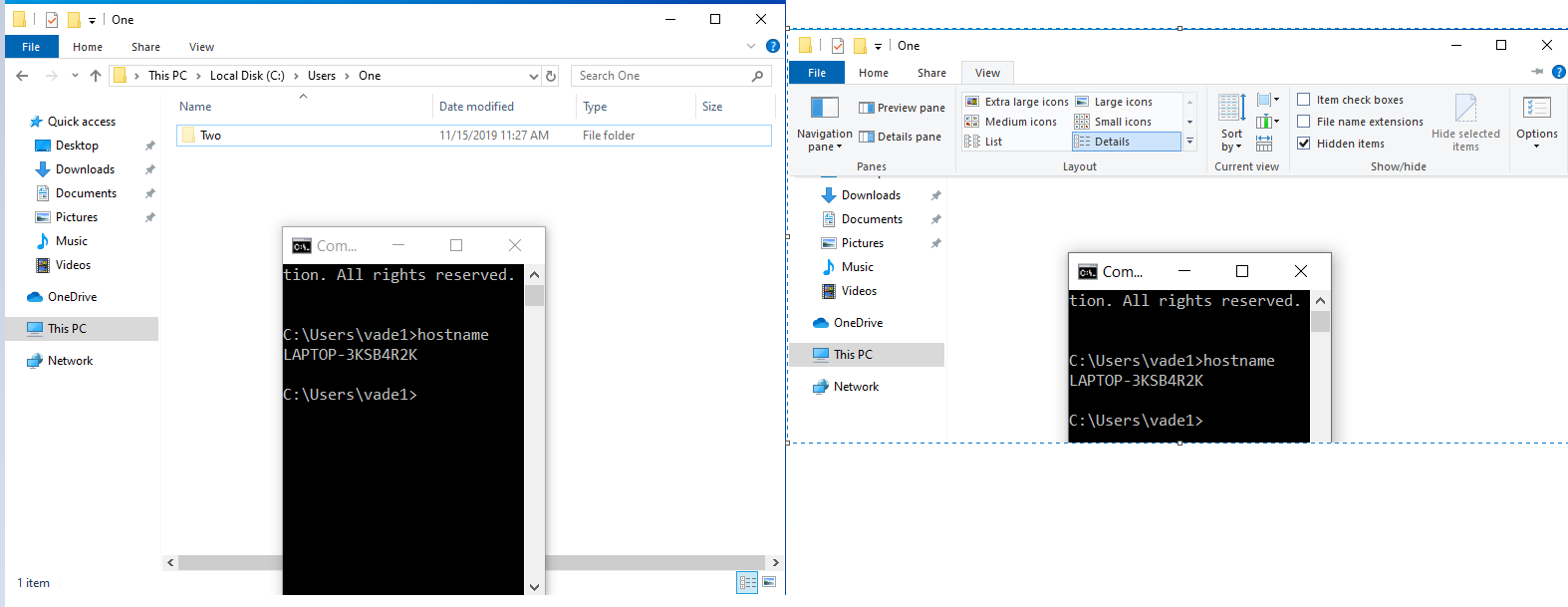
1. Create a group called ‘Knitting Club’. Add Charlie to the Knitting Club group. Screenshot: show that the user is a members of the Knitting club group’.

|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |



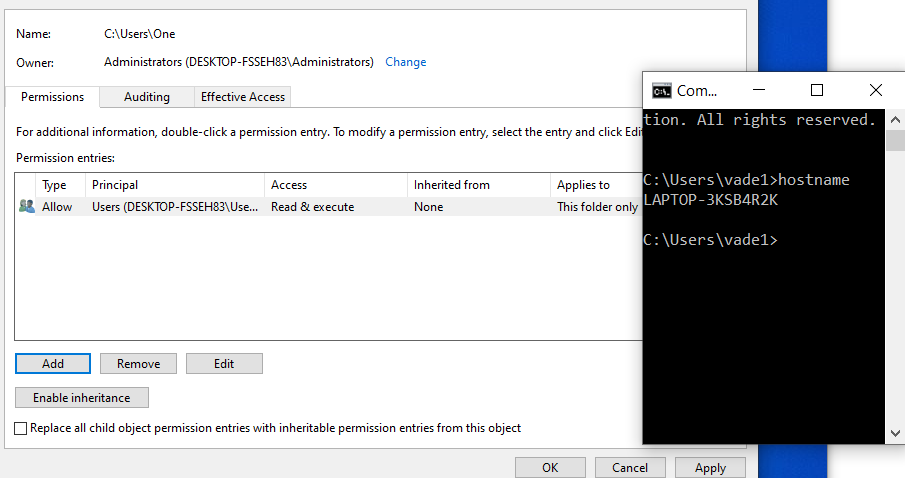
1. Create a folder, within your user folder, called ‘One’. Create a subfolder, within ‘One’, called ‘Two’. *Hide* the ‘Two’ folder from view, within NTFS (file explorer). Display hidden file and folders. Screenshot: prove the ‘Two’ folder is hidden and that hidden folders are now visible in file explorer.

|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |



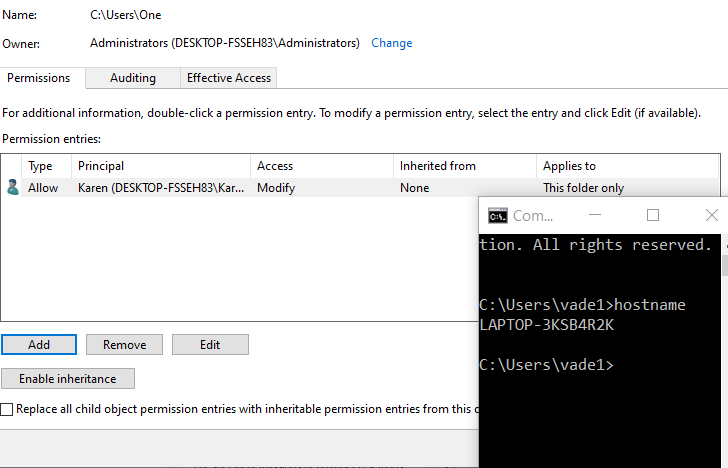
1. Disable inheritance on the ‘One’ folder; convert the inherited permissions to explicit permissions. Screenshot: show that inheritance is off and that the inherited permissions are explicit permissions.

|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |



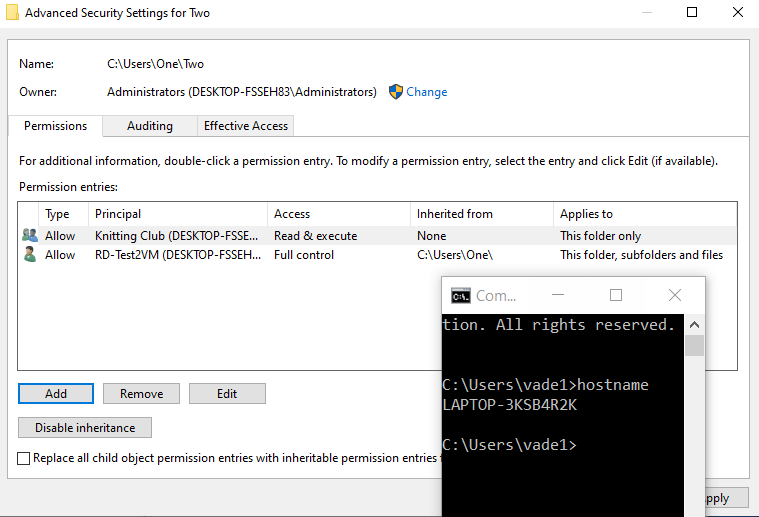
1. Remove all ACE’s from ‘One’, except the initial account. Add Karen as a principal, to the ‘One Folder’. Using only standard permissions, give Karen the ability to Add and Delete files/folders from ‘One’; and to Change the attributes, and contents of files and folders within ‘One’. Screenshot: show the ACL with the appropriate ACEs.

|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |



1. Using only standard permissions, give the group ‘Knitting Club’ the ability to Read and Change the contents of the ‘Two’ folder, explicitly, but not the ‘One’ folder. Screenshot: show the ACL with the appropriate ACEs.

|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |

Share the ‘Two’ folder. Name it anything you like, but make sure the Share is hidden from viewing across the network. Screenshot: show the network path proving the folder is both shared and hidden.

|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |



1. Configure the share permissions so that access to the contents of the share are managed exclusively through NTFS permissions, for everyone. Screenshot: show the share ACL with the appropriate ACEs.

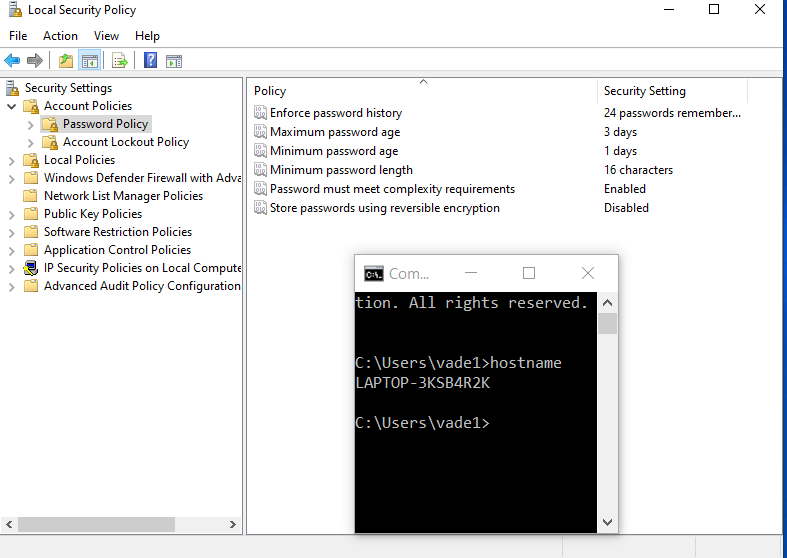
|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |



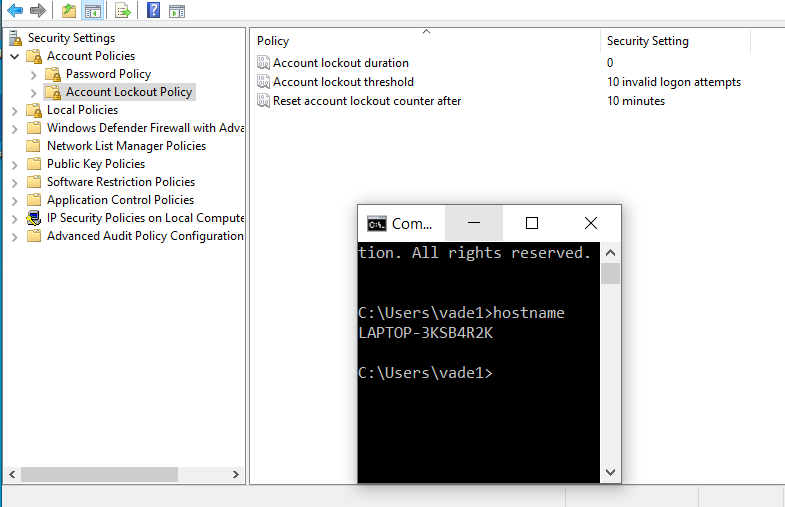
1. Create a Password Policy and Account Lockout Policy that satisfies the following criteria:
   1. Do not allow users to use the same password until they’ve created twenty-four unique passwords.
   2. Force users to change their password every three days.
   3. Allow user to change their password once per day.
   4. Passwords must be sixteen characters or more.
   5. Passwords must meet the complexity requirements as dictated by Microsoft.
   6. If an account violates the password policy, it should remain locked out indefinitely (must be unlocked by an administrator).
   7. The account should lock out after ten invalid authentication attempts.
   8. The users attempt count should reset to zero after 10 minutes.

Screenshots: Take a screen shot of each policy proving the required settings.

|  |  |  |
| --- | --- | --- |
| (0.5 point) | Screenshot submission | *hostname visible;* *Password Policy* |



|  |  |  |
| --- | --- | --- |
| (0.5 point) | Screenshot submission | *hostname visible;* *Account Lockout Policy* |



1. Give Karen the *user* *right* to take ownership of objects, VIA Local Policy. Screenshot: show the policy configured correctly.

|  |  |  |
| --- | --- | --- |
| (1 point) | Screenshot submission | *hostname visible* |

