Lab 4: Applying User Authentication and Access Controls

Osamudiamen Eweka

CYB-605-Z2 Principles of Cybersecurity

Utica University

Introduction

Today's corporate entities increasingly depend on cloud technologies to manage and disseminate large amounts of customer data efficiently. As reliance on cloud solutions and storage intensifies, the landscape of security threats expands accordingly. This makes cybersecurity a critical concern for companies, especially with the growing complexity of techniques used for unauthorized access. The prevalence of data breaches, along with the emergence of more sophisticated threats and brute-force attacks, has surpassed what many initially anticipated. A holistic approach to cybersecurity, integrating people, processes, and technology across the organization, is essential. The CIA triad, which stands for Confidentiality, Integrity, and Availability, is fundamental in developing a robust cybersecurity framework to protect an organization's essential assets. This framework not only focuses on its core principles but also covers a broad range of aspects including authenticity, precision, ethical standards, identity management, the integrity of individuals, non-denial, accountability, and fostering digital trust (Bruce et al., 2014).

In the corresponding lab activity, attendees will use the Active Directory Users and Computers tool to create several new users and groups. They will then set up a directory structure aligned with these groups and apply permissions to limit access to certain folders based on group membership. Finally, participants will test authentication and access control efforts to enter the assigned folders by logging in as different users.

Objective

After finishing this lab, attendees will develop a thorough knowledge of how to use Microsoft's Active Directory Domain Services to set up a strong framework for authentication and access management. They will become skilled in generating new user accounts and security groups in a Windows setting. Additionally, they will master the creation of access control lists to secure objects and folders from unauthorized entries within the Windows platform. Moreover, the differences between Windows Security permissions and Windows Share permissions will be made clear. The skills learned will also include how to set up access controls on a remote file server by utilizing the strengths of Active Directory Security Groups.

Lab Setup

In this lab, three pivotal software tools are employed to impart practical skills and theoretical knowledge in cybersecurity:

1. **Active Directory Users and Computers**: This tool is essential for managing user accounts and security groups, facilitating an understanding of how access permissions and policies are administered within the Active Directory ecosystem.
2. **PowerShell**: Utilized for its powerful scripting capabilities, PowerShell enables the automation of administrative tasks, illustrating the efficiency and scalability of scripting in system management (Sdwheeler, 2023).
3. **TrueNAS**: Serving as the lab's network-attached storage solution, TrueNAS demonstrates the principles of file sharing, data storage, and the application of access controls, highlighting the importance of data integrity and access management in a networked environment (TrueNAS, 2023).

These tools collectively provide a robust framework for exploring user authentication and access control mechanisms, preparing participants for the complexities of safeguarding digital assets in modern IT infrastructures.

Section 1

Part 1: Create Users and Security Groups

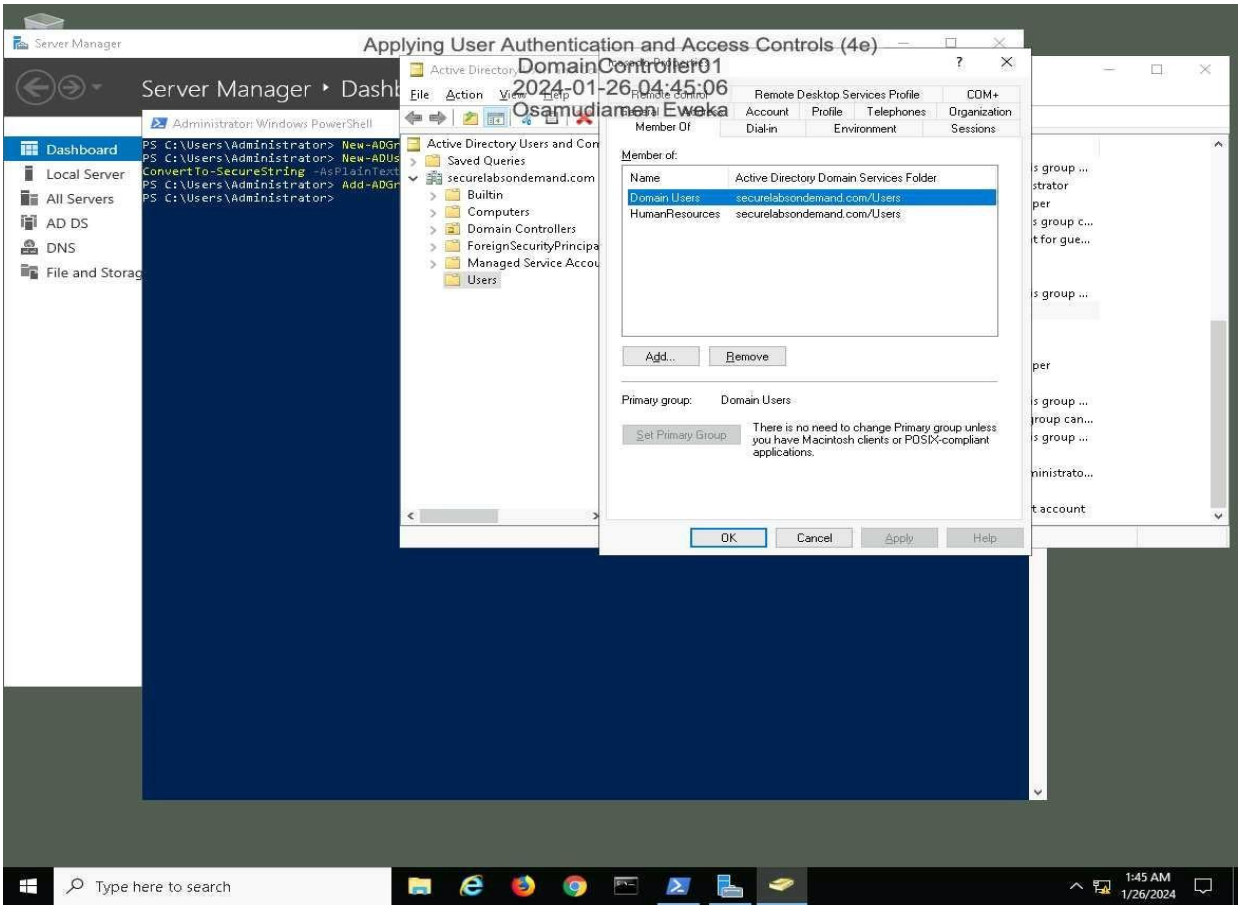
During this lab segment, participants were led through a detailed, step-by-step process aimed at mastering the creation of user accounts and security groups using the ADUC (Active Directory Users and Computers) tool. ADUC acts as a crucial graphical tool for managing Active Directory's central database, which contains essential information about the organization's users and computers. This database is located on a domain controller—a specific type of Windows Server that is crucial for managing the network of user accounts and computers that make up the domain. Active Directory's cooperative features, notably its powerful Group Policy, allow administrators to enforce a wide range of security measures. These include the establishment of password policies, the deployment of antivirus programs, and the management of software updates, among other security protocols.

Given that Active Directory can be a focal point for cyberattacks, the lab emphasized the importance of strengthening it with various security measures. The practical part of the lab involved setting up key security groups—Developers, Managers, and HR (Human Resources) each with a specific function in the organizational framework. Users were also created and thoughtfully placed into these groups, showcasing the critical role Active Directory plays in regulating access based on individuals' job roles and responsibilities. This practical exercise provided a fundamental understanding of the management of users and groups within the Active Directory landscape, as described by (Kim & Solomon, 2021). An accompanying screenshot shows the interface of Active Directory Users and Computers with the newly added users and groups.

Displayed in the image is a list of the users and groups formed in the initial part of the hands-on demo. The groups fashioned were Developers, Managers, and HumanResources, and the individuals created were Sam Carpenter, Carl Prince, and lcasado. Figure 1 is a visual representation of the new user profiles and group categories in Active Directory Users and Computers (Jones & Bartlett, 2024).

Figure 1

Make a screen capture showing the new users and groups in Active Directory Users and Computers.



Section 1

Part 2: Create Folders and Configure Security Permissions

In this phase of the laboratory exercise, participants employ File Explorer to meticulously establish dedicated folders for specific functional groups previously identified, including developers, managers, and HR personnel. This organizational task commences with participants connecting to the vWorkstation system and securely logging in as the domain administrator, a role that confers extensive privileges for adjusting system settings and permissions. The cornerstone of this phase is the sophisticated configuration of security permissions for the LabFiles folder, leveraging the capabilities of NTFS (New Technology File System) permissions. These permissions play a crucial role in determining the range of actions that users or groups can execute on files and folders within the NTFS, thereby ensuring a robust framework for data security and access management.

The process entails a critical step: disabling inheritance of permissions from parent directories, an essential measure to custom-tailor access rights for each functional group according to their specific requirements. Particularly for the HRfiles folder, adjustments are made to empower members of the Human Resources group with the ability to modify folder contents. This strategic maneuver is indicative of a secure approach to managing access within the Active Directory environment, ensuring that HR personnel have the necessary permissions to update and manage sensitive employee information efficiently and securely. Such a bespoke configuration of permissions is instrumental in reinforcing the organization's security posture, highlighting the significance of precise access control in safeguarding sensitive data against unauthorized access or manipulation.

The updated Security permissions for the HRfiles folder, illustrated in Figure 2, exemplify the successful implementation of these advanced security measures. This visualization serves as a concrete demonstration of the application of theoretical security concepts in a practical setting, offering participants a clear understanding of the importance of detailed access control. Through this exercise, participants not only gain hands-on experience in configuring security permissions within an NTFS framework but also appreciate the critical role of customized access rights in maintaining data security and privacy in an organizational context. The careful alignment of permissions with the specific needs of each functional group underscores the necessity of strategic access management in today's information security landscape (Jones & Bartlett, 2024).

Figure 2

Make a screen capture showing the updated Security permissions for the HRfiles folder.

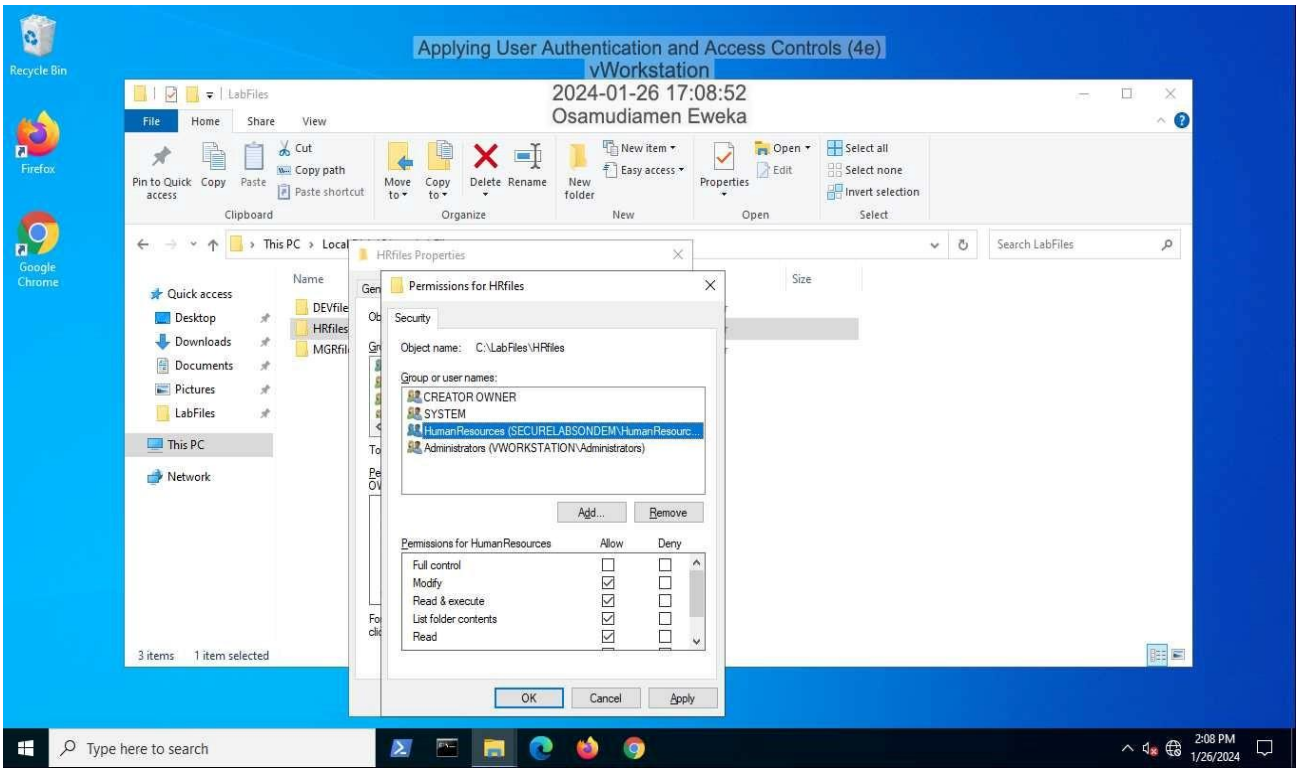
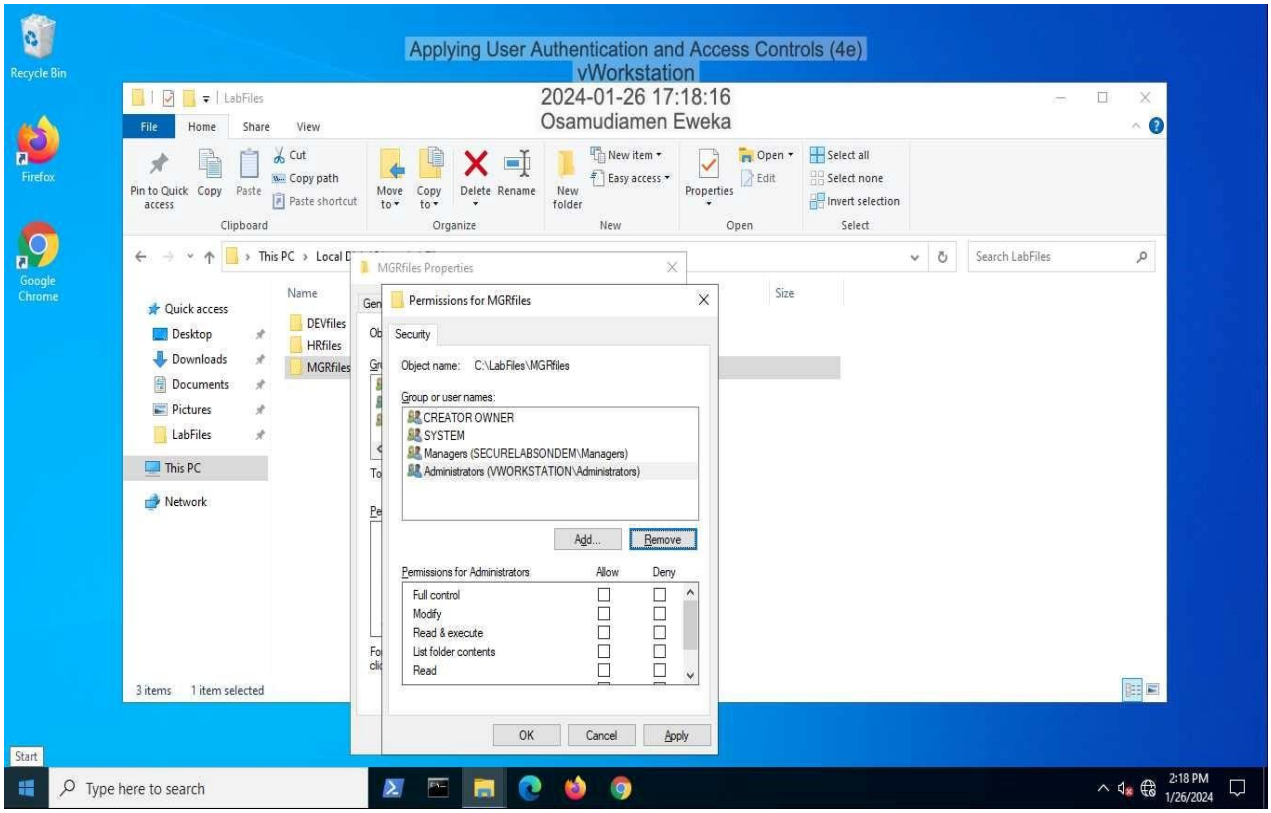


Figure 3 Screenshot below illustrates the revised security settings for the MGRfiles directory (Jones & Bartlett, 2024). In this update, the ability to modify has been granted to individuals in the Managers security group, enabling them to alter files and folders inside the MGRfiles directory.

Figure 3

Make a screen capture showing the updated Security permissions for the MGRfiles folder.



Continuing with the same process, Figure 4 Screenshot displaying the refreshed Security permissions for the DEVfiles folder (Jones & Bartlett, 2024). In this case, the Modification capability has been enabled for members of the Developers security group, allowing them to edit files and folders located within the DEVfiles folder.

Figure 4

Make a screen capture showing the updated Security permissions for the DEVfiles folder.

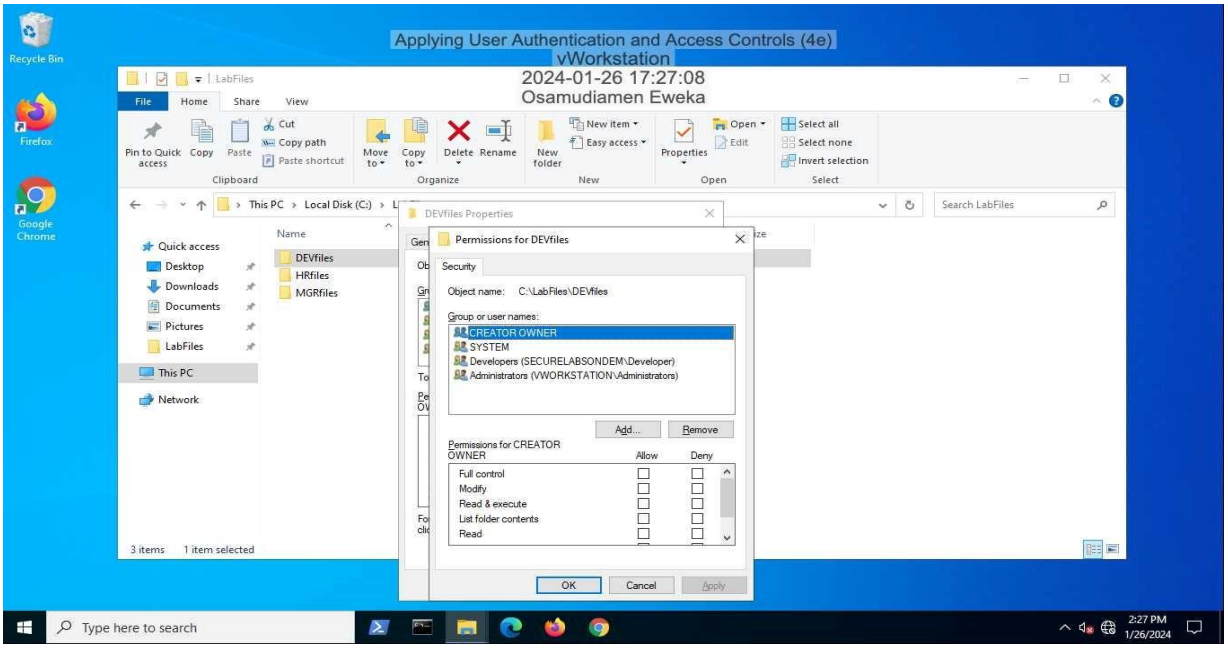


Figure 5

Make a screen capture showing the three folders within the LabFiles folder.

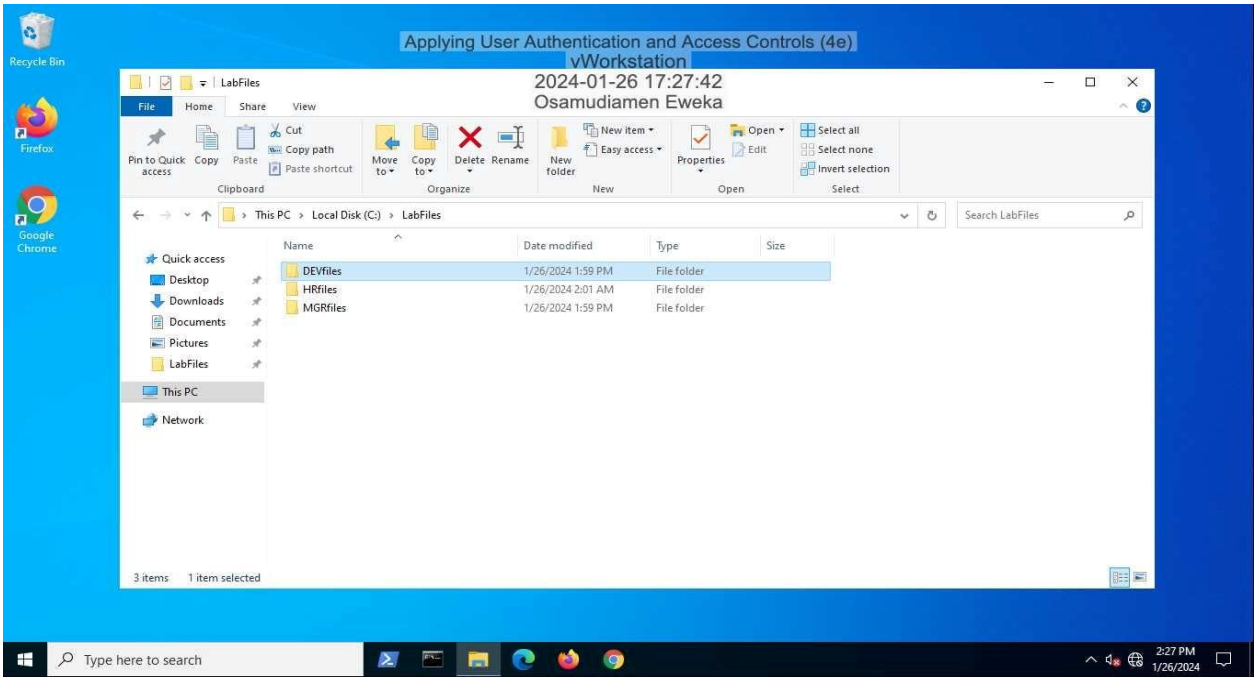


Figure 5 Screenshot above presents the trio of directories within the LabFiles folder. This image explicitly showcases the organization of the LabFiles folder, which houses each department's specific folder: HRfiles, MGRfiles, and DEVfiles (Jones & Bartlett, 2024). The structure depicted in the figure below demonstrates a clear and organized approach to data management, ensuring that each department's files are neatly compartmentalized within the overarching LabFiles directory. This setup not only streamlines file navigation but also reinforces data segregation, allowing for efficient access and management of department-specific documents and resources.

Section 1

Part 3: Verify Authentication and Access Controls

In the final segment of Section 1 of the lab, participants engage in a crucial testing phase to verify the access and modification rights of newly established user accounts within their assigned directories. This verification is accomplished by logging into the vWorkstation with each specific user account, thereby assessing the practical application of access rights in accordance with the Principle of Least Privilege (PoLP). The PoLP is a security concept that restricts users' access rights to only what is strictly necessary for their job functions. Through this hands-on testing, participants determine whether users can appropriately access and contribute files to folders that correlate with their functional roles, such as HRfiles, MGRfiles, and DEVfiles, each earmarked for Human Resources, Managers, and Developers, respectively.

This comprehensive testing process allows participants to directly observe the system's reaction to various access attempts, accurately identifying instances where access is rightly granted or denied based on the pre-configured NTFS permissions. The use of screen captures plays a crucial role in this phase, offering visual evidence of the test outcomes. These captures document both the successful entries and the access denials, thereby providing a clear and tangible proof of the access controls' effectiveness. This methodical verification acts as a critical component in affirming the integrity and security of the implemented permissions, aligning with the overarching goals of the laboratory exercise.

An illustrative example of the testing outcomes is captured in Figure 6, which depicts the access denial encountered by Sam Carpenter's account when attempting to enter the HRfiles folder. As Carpenter's account lacks the requisite permissions for this directory, the system

generates and displays an error message, visually confirming the operational success of the access restrictions (Jones & Bartlett, 2024).

This specific instance underscores the lab's commitment to enforcing stringent access control measures, thereby enhancing the security framework of the Active Directory environment. The meticulous documentation and analysis of these test results contribute significantly to the lab's objective of establishing a secure and functional access control system.

Figure 6

Make a screen capture showing the unsuccessful access error message for the HRfiles folder as scarpenter.

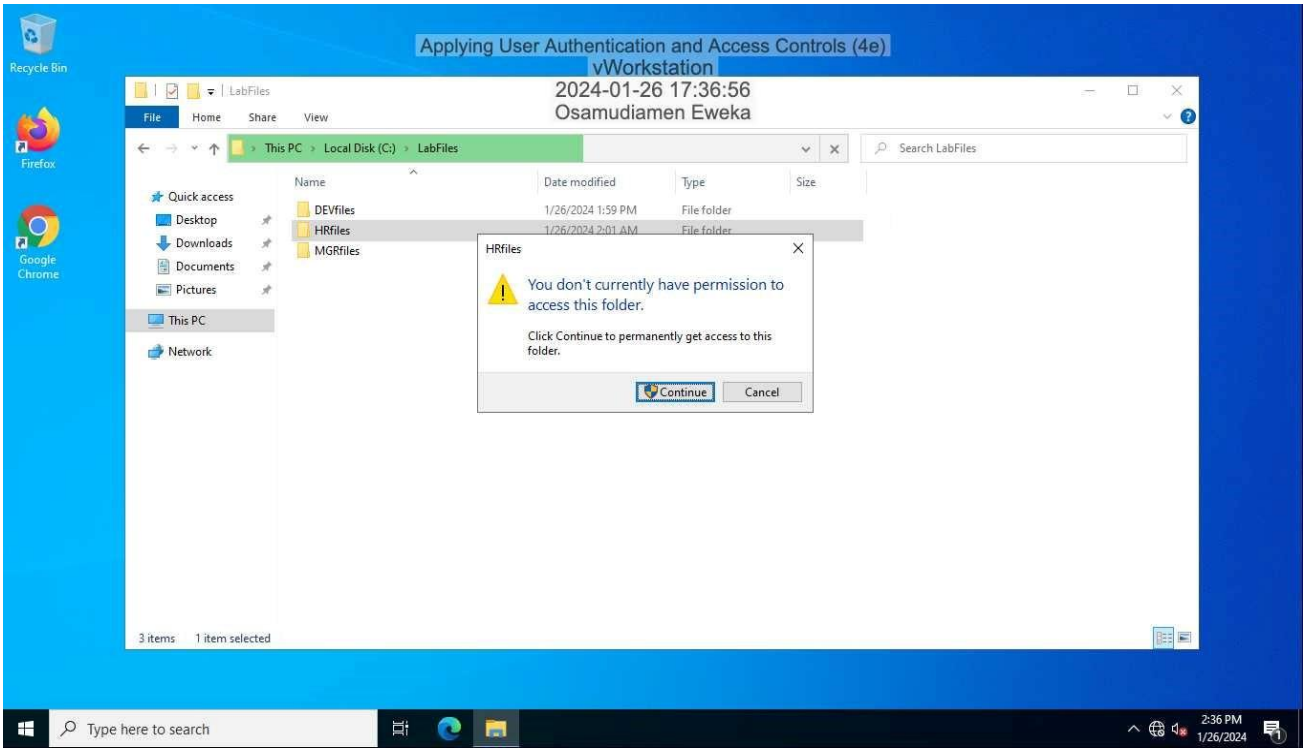
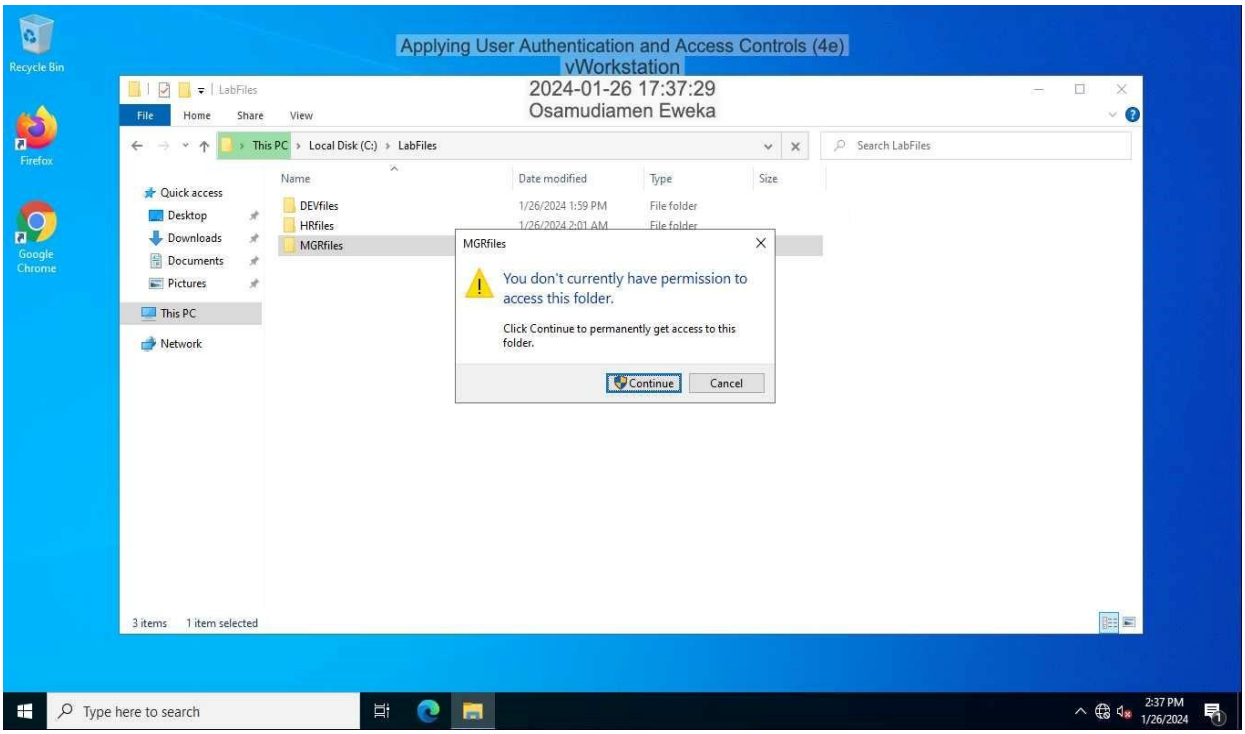


Figure 7

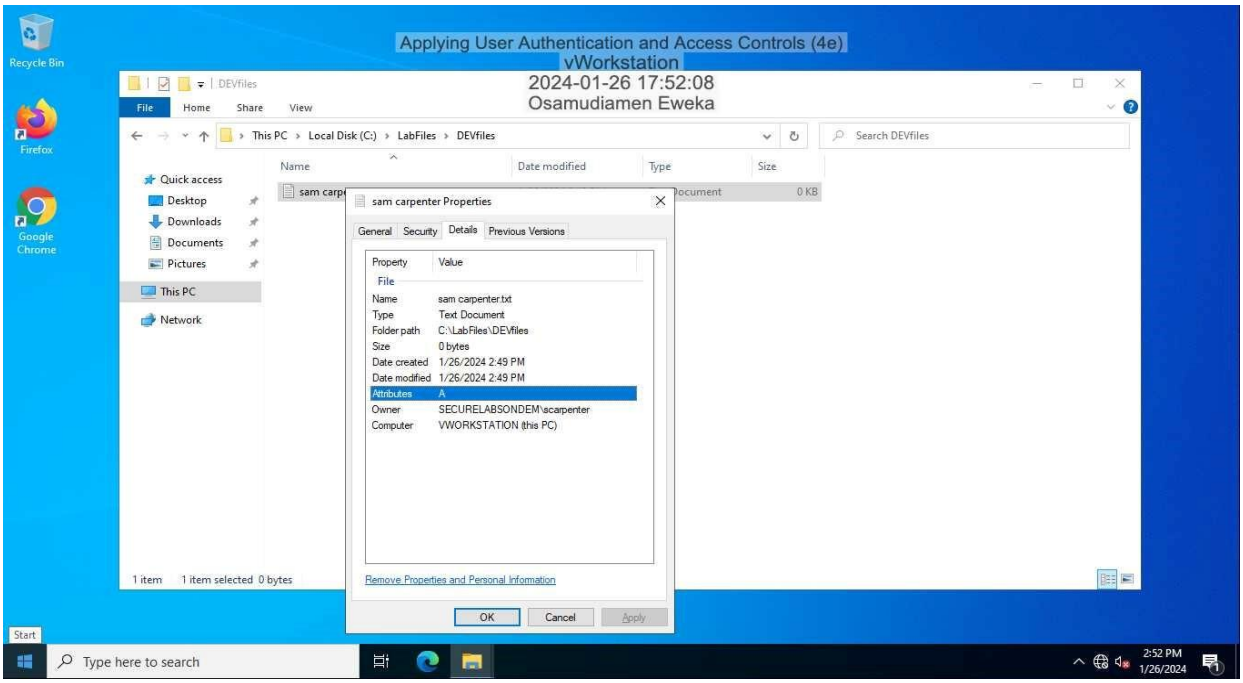
Make a screen capture showing the unsuccessful access error message for the MGRfiles folder as scarpenter.



Note. Figure 7 illustrates a screen capture depicting an error message due to failed access to the MGRfiles folder by the user scarpenter. This indicates that Sam Carpenter's account lacks the necessary permissions to enter the MGRfiles directory, resulting in the display of an error notification (Jones & Bartlett, 2024).

Figure 8

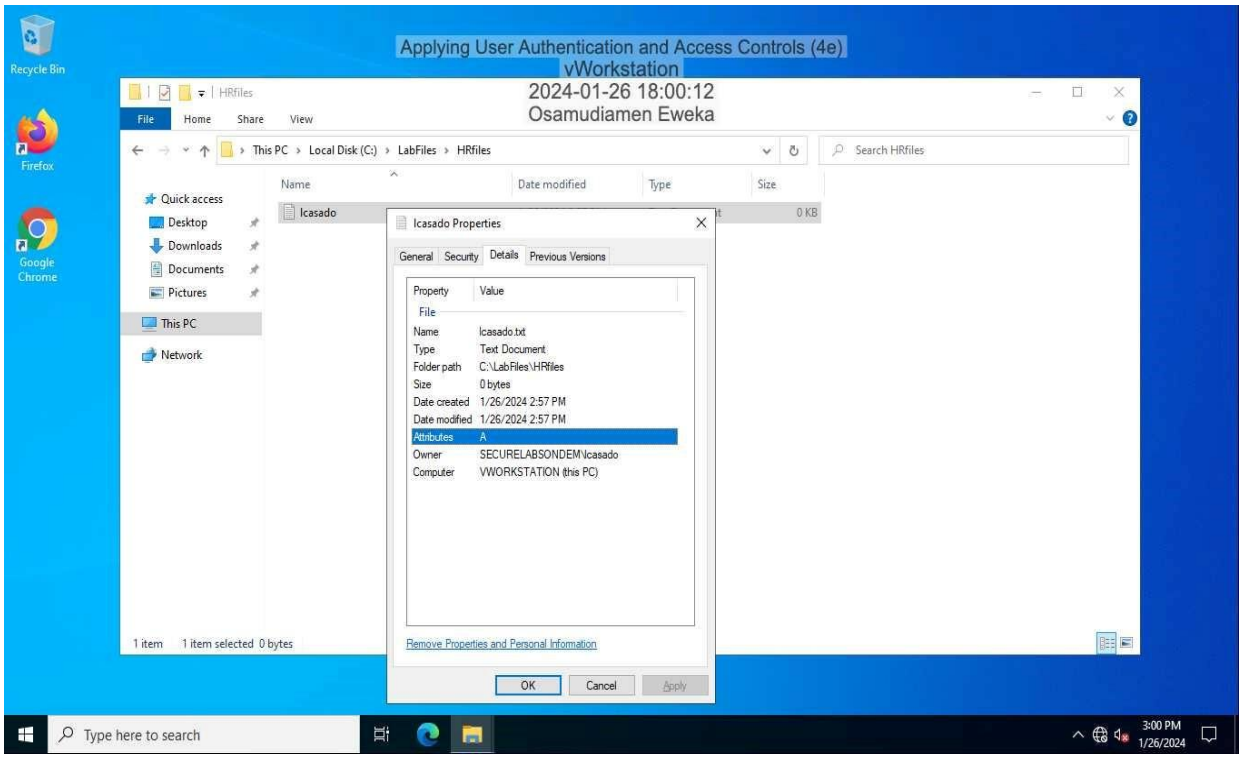
Make a screen capture showing the Properties dialog box for the file created in the DEVfiles folder by scarpenter.



*Note***.** Figure 8 presents a screen capture of the Properties dialog box for a file located in the DEVfiles folder, attributed to the user scarpenter. This indicates that Sam Carpenter is a member of the Developers security group, granting him the appropriate access permissions to the DEVfiles directory. The image exemplifies Sam Carpenter's successful access to the DEVfiles folder (Jones & Bartlett, 2024).

Figure 9

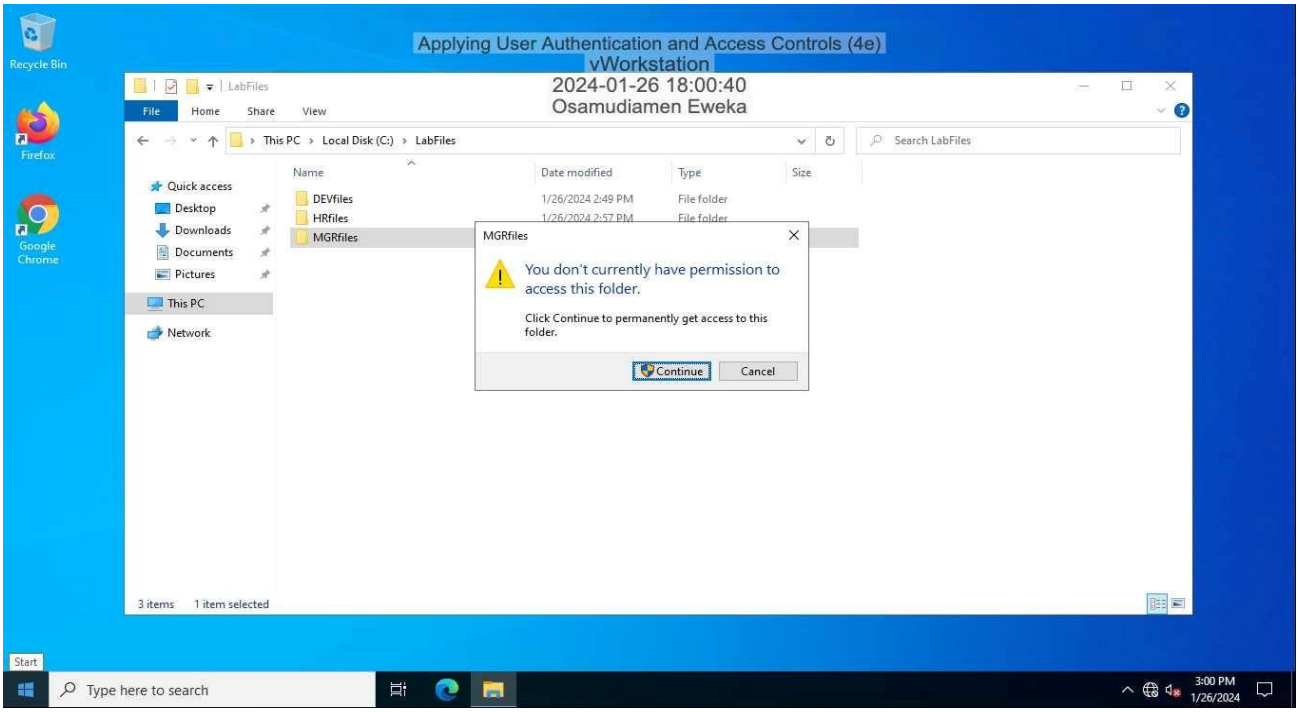
Make a screen capture showing the Properties dialog box for the file created in the HRfiles folder by lcasado.



*Note***.** Figure 9 displays a screen capture of the Properties dialog box for a file situated in the HRfiles folder, created by the user lcasado (Jones & Bartlett, 2024). This demonstrates that lcasado is affiliated with the Human Resources department, thereby possessing the necessary permissions to access the HRfiles folder. The image below confirms lcasado's ability to access

Figure 10

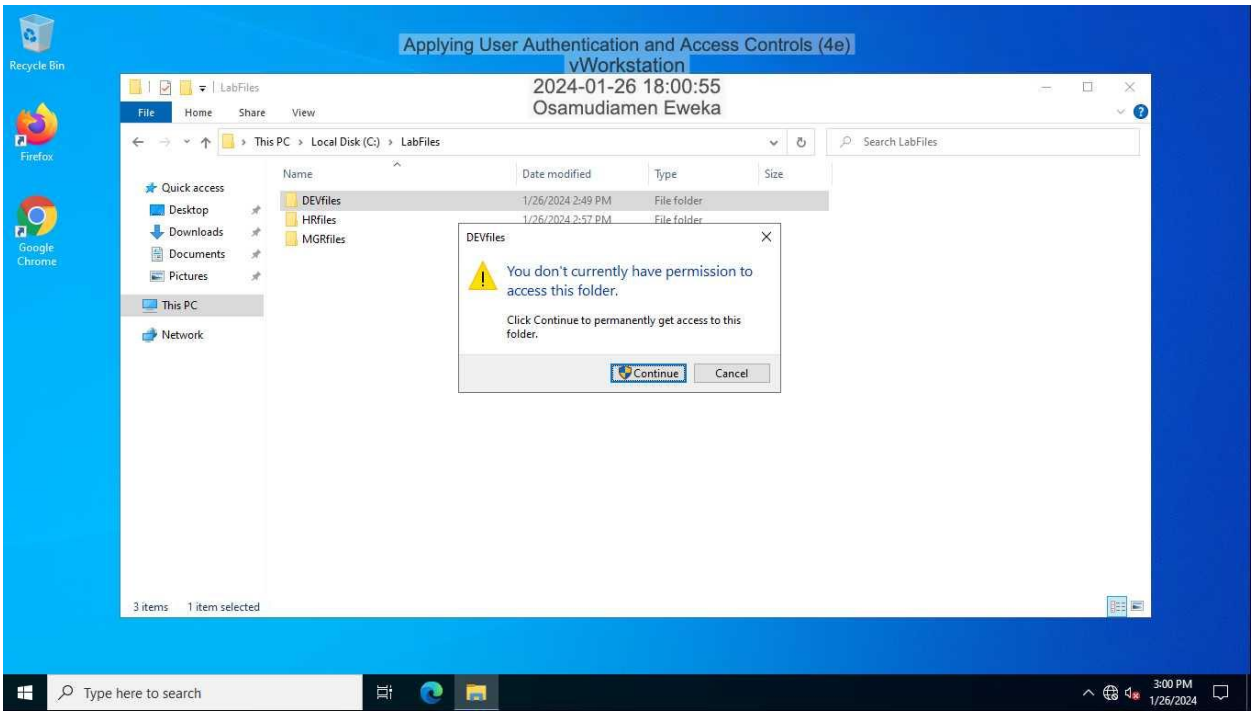
Screen capture showing the unsuccessful access error message for the MGRfiles folder as lcasado



Note. Figure 10 illustrates a screen capture depicting an error message encountered by the user lcasado when attempting to access the MGRfiles folder (Jones & Bartlett, 2024). This error message is indicative of lcasado's affiliation with the Human Resources department, which does not grant him permission to access the MGRfiles directory. The figure below visually confirms that access to the MGRfiles folder is restricted for lcasado.

Figure 11.

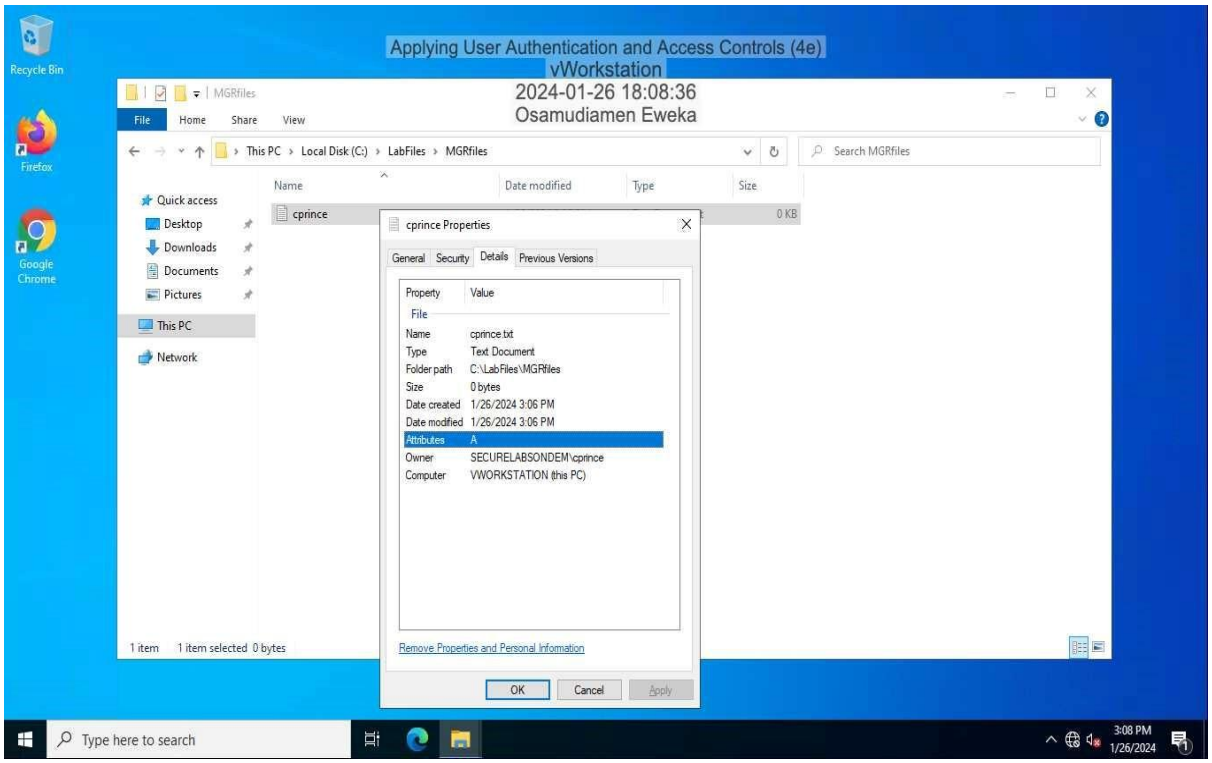
Make a screen capture showing the unsuccessful access error message for the DEVfiles folder as lcasado.



*Note***.** Figure 11 features a screen capture that shows an error message received by lcasado when trying to access the DEVfiles folder (Jones & Bartlett, 2024). This specific folder is accessible only to members of the Developers group. Given lcasado's association with the Human Resources department, he lacks the required permissions to enter the DEVfiles directory. The image below effectively illustrates the denied access for lcasado to the DEVfiles folder.

Figure 12

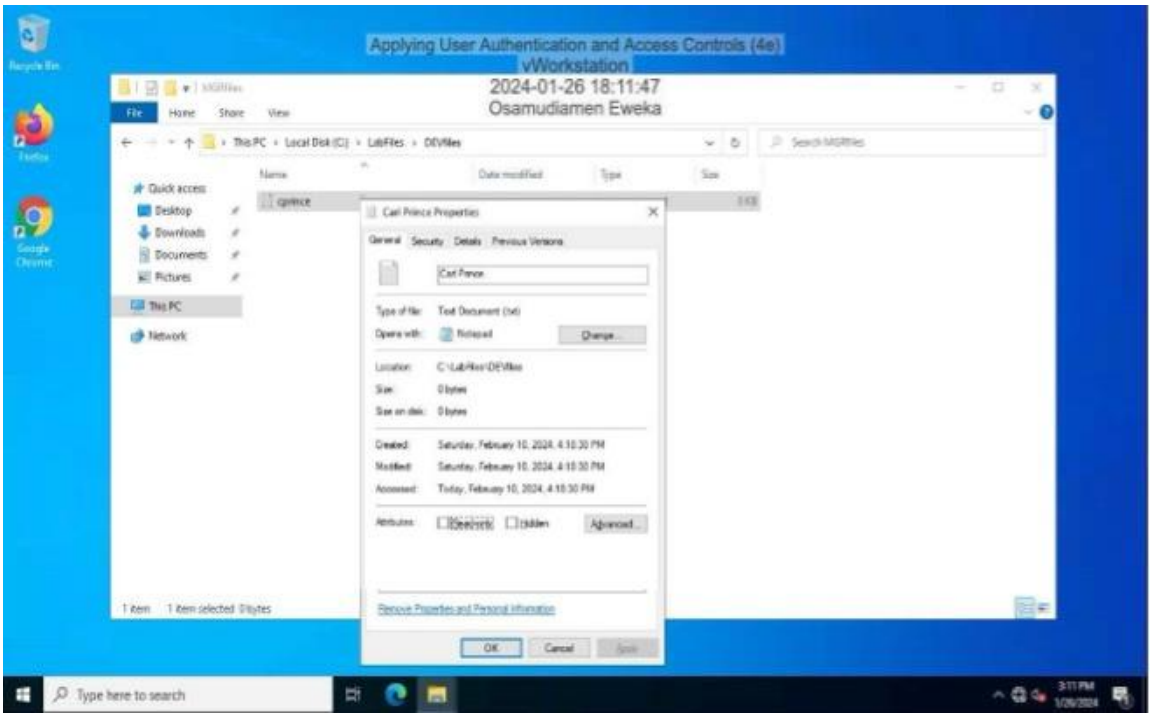
Make a screen capture showing the Properties dialog box for the file created in the MGRfiles folder by cprince.



Note. the figure above displays a screen capture of the Properties dialog box for a file located within the MGRfiles folder, created by the user cprince, also known as Carl Prince (Jones & Bartlett, 2024). Given that Carl Prince has the necessary permissions to access both the MGRfiles and DEVfiles folders, he is able to enter the MGRfiles directory without encountering any restrictions. The image below serves as confirmation of Carl Prince's unrestricted access to the MGRfiles folder.

Figure 13

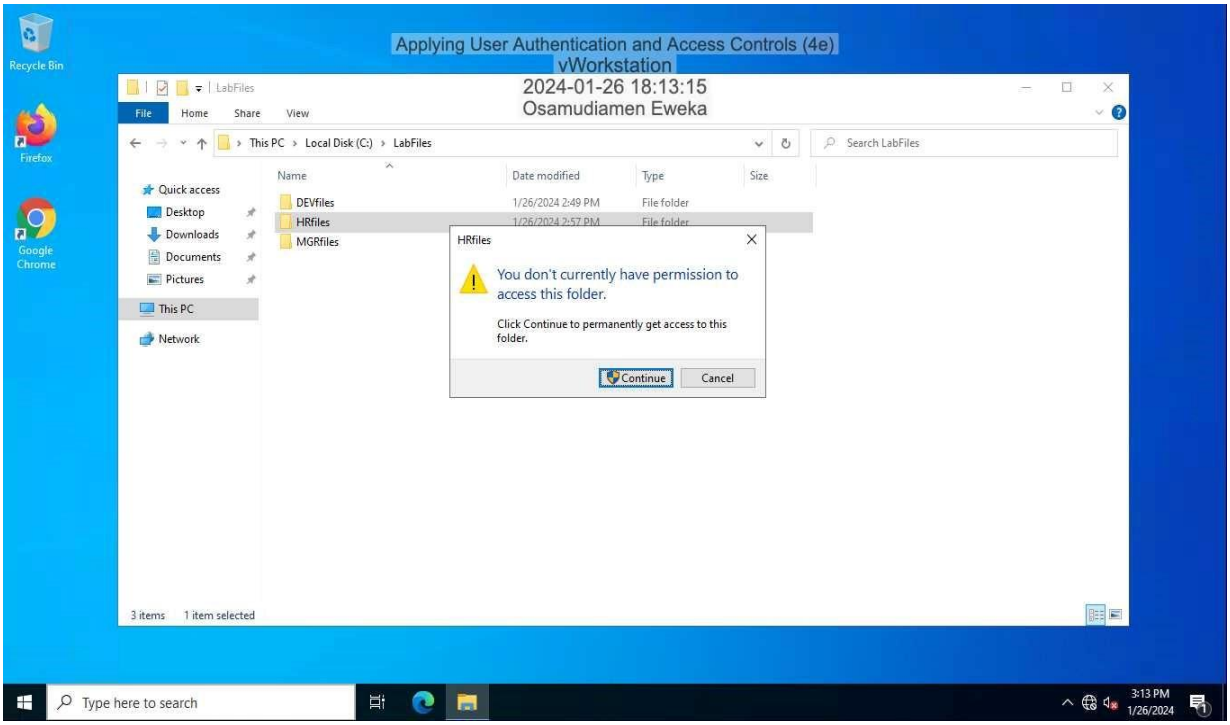
Make a screen capture showing the Properties dialog box for the file created in the DEVfiles folder by cprince.



Note. The figure showcases a screen capture of the Properties dialog box for a file in the DEVfiles folder, attributed to the user cprince, or Carl Prince (Jones & Bartlett, 2024). As Carl Prince is granted access rights to both the MGRfiles and DEVfiles folders, he can access the DEVfiles directory without facing any limitations. The above image verifies Carl Prince's unrestricted ability to access the DEVfiles folder.

Figure 14

Screen capture showing the unsuccessful access error message for the HRfiles folder as cprince



Note. Figure 14 illustrates a screen capture displaying an error message encountered by cprince, or Carl Prince, when attempting to access the HRfiles folder (Jones & Bartlett, 2024). This error underscores that Carl Prince's permissions are limited to the MGRfiles and DEVfiles folders, excluding him from accessing the HRfiles directory. The image below serves as clear evidence of Carl Prince's restricted access to the HRfiles folder.

Section 2

Part 1: Create an SMB Share

In this advanced segment of the laboratory exercise, the emphasis transitions to the meticulous configuration of permissions on a TrueNAS file server, leveraging the user and group frameworks established in the initial section. TrueNAS, an open-source suite, offers Network-Attached Storage (NAS) solutions, facilitating the remote engagement with storage systems as though they were directly connected. The integration with Samba, which represents Microsoft's adaptation of the Server Message Block (SMB) protocol, enables a seamless interface between Windows-operated machines and NAS units, thereby allowing for the remote mapping of drives. This arrangement is meticulously orchestrated via Active Directory, which oversees the authentication and authorization processes essential for connecting to NAS devices.

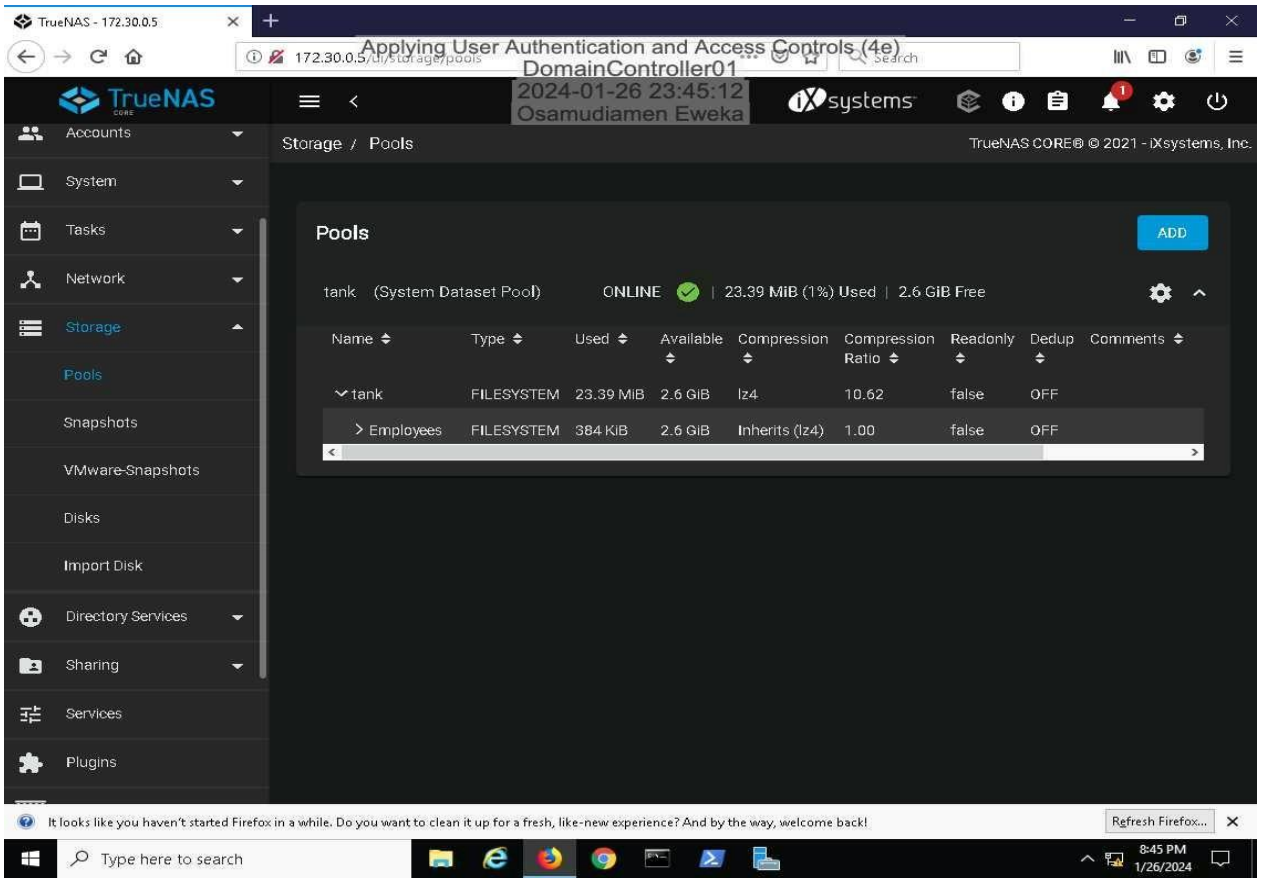
The technical procedure unfolds with a secure login to the TrueNAS console, followed by the activation of Active Directory services. Subsequently, a new dataset is meticulously crafted within the storage pool, setting the stage for the configuration of an SMB network share. Access Control Lists (ACLs) are strategically utilized to delineate permissions for the shared dataset, thereby ensuring a fortified access framework. This procedural execution lays down a robust infrastructure for efficient collaboration across Windows platforms and the TrueNAS ecosystem, significantly enhancing the utility of storage resources while upholding rigorous security protocols.

Figure 15 illustrates a screen capture that highlights the addition of a new dataset, aptly named "Employees," to the TrueNAS pool page (Jones & Bartlett, 2024). This addition, facilitated through access to the TrueNAS server, exemplifies the practical application of the

discussed configurations, showcasing the seamless integration of storage solutions within the network infrastructure.

Figure 15

Make a screen capture showing the Employee's dataset on the TrueNAS Pools page.



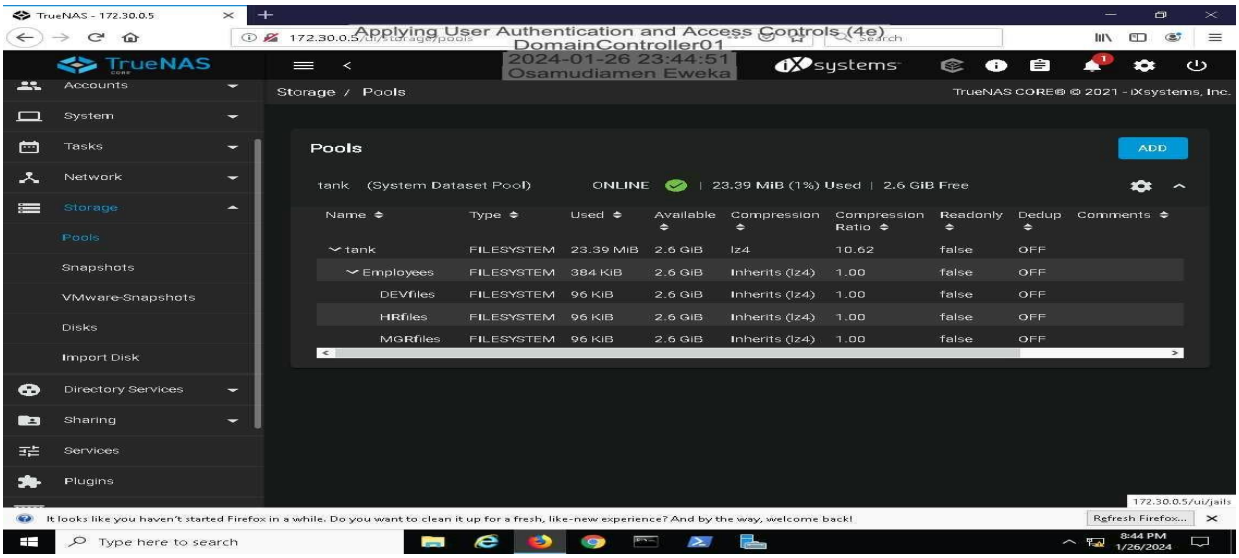
Section 2

Part 2: Create Shared Folders and Configure ACLs

In this section of lab, the focus is on creating additional datasets on a TrueNAS file server, which align with previously established security groups from Section 1. Each dataset is designated for a specific security group, namely developers, managers, and human resources. For each dataset, Access Control Lists (ACLs) are configured to permit read/write access, effectively sharing these datasets with the corresponding security group. This process involves using the TrueNAS interface to add datasets within storage pools and setting up ACLs to manage access rights, demonstrating practical skills in managing file storage and access permissions in a networked environment. This activity emphasizes the importance of precise access control in securing data and ensuring that only authorized users can access specific datasets, reflecting real-world IT security and management practices, Figure 16 shows the three new datasets on the TrueNAS Pools page, Three datasets (DEVfiles, HRfiles, and MGRfiles) are added within the Employees dataset (Jones & Bartlett, 2024).

Figure 16

Make a screen capture three new datasets on the TrueNAS Pools page.



Section 2

Part 3: Verify Access Controls

In this critical phase of the lab, participants embark on a procedural verification of Access Control Lists (ACLs) for the newly established shared folders, employing a remote connection to the FileServer01 system from the vWorkstation. This verification necessitates participants to authenticate as users belonging to distinct security groups, followed by attempts to access the shared folders designated for their respective groups. The process initiates with participants signing out of the Administrator account on vWorkstation and returning to the login interface. The first step involves logging in with the 'scarpenter' account. Once logged in, participants use File Explorer to navigate to the Employees folder located on FileServer01, with a focus on accessing the DEVfiles folder, which is specifically visible to this user account.

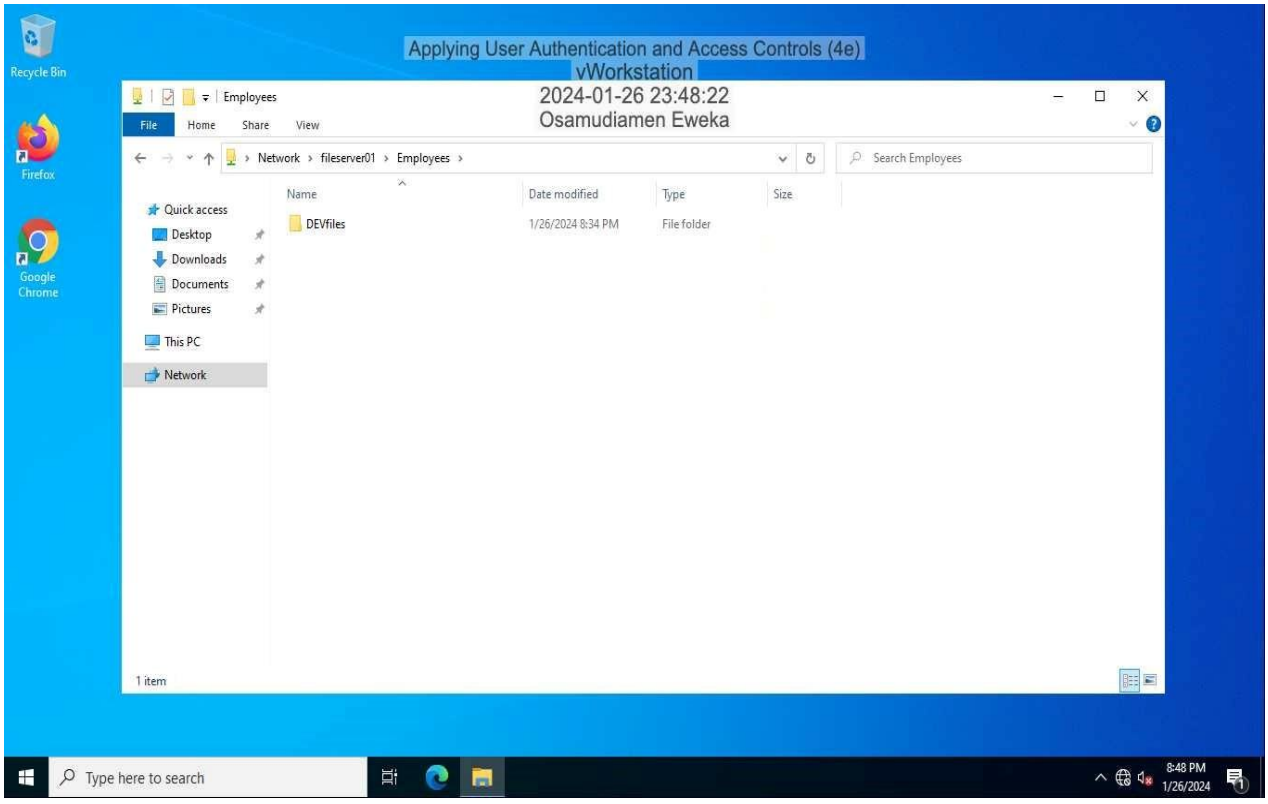
To ensure comprehensive documentation of this verification process, a screenshot is captured to record the view from the 'scarpenter' account perspective. This procedure is systematically replicated for the 'lcasado' and 'cprince' accounts, with an additional verification step for 'cprince' to confirm access to both the DEVfiles and MGRfiles folders. Capturing screenshots from the viewpoint of each user account is essential for this step, providing a visual corroboration of the ACLs effectiveness for the shared folders.

This meticulous verification offers tangible, visual evidence of the applied ACLs' success, confirming the appropriateness of access for each user according to their assigned security group.

Figure 17 vividly demonstrates the Employees folder as viewed when logged in as scarpenter (Jones & Bartlett, 2024). Given the configuration of permissions associated with the SMB share, folders that the participant's user account is authorized to access will be displayed. Therefore, in this specific scenario, the participant is expected to see only the DEVfiles folder, aligning with the security permissions set for the 'scarpenter' account. This step is crucial in validating the precision of access control measures implemented, ensuring each user's access rights are in strict accordance with their security group affiliations.

Figure 17

Make a screen capture showing the Employees folder while signed in as scarpenter.



In the structured exploration of ACLs within the lab, Figure 18 below provides a visual documentation showcasing the Employees folder as accessed by the user logged in as lcasado (Jones & Bartlett, 2024). Following the precise configuration of permissions, lcasado is granted

visibility to the HRfiles folder. This outcome is clearly depicted in the figure below, serving as a testament to the effective application of access controls tailored to the unique requirements of the HR department. This visual evidence supports the lab's objective of ensuring that access privileges are accurately aligned with each user's role and security group, thereby reinforcing the lab's adherence to best practices in access management and security protocols.

Figure 18

Make a screen capture showing the Employees folder while signed in as lcasado.

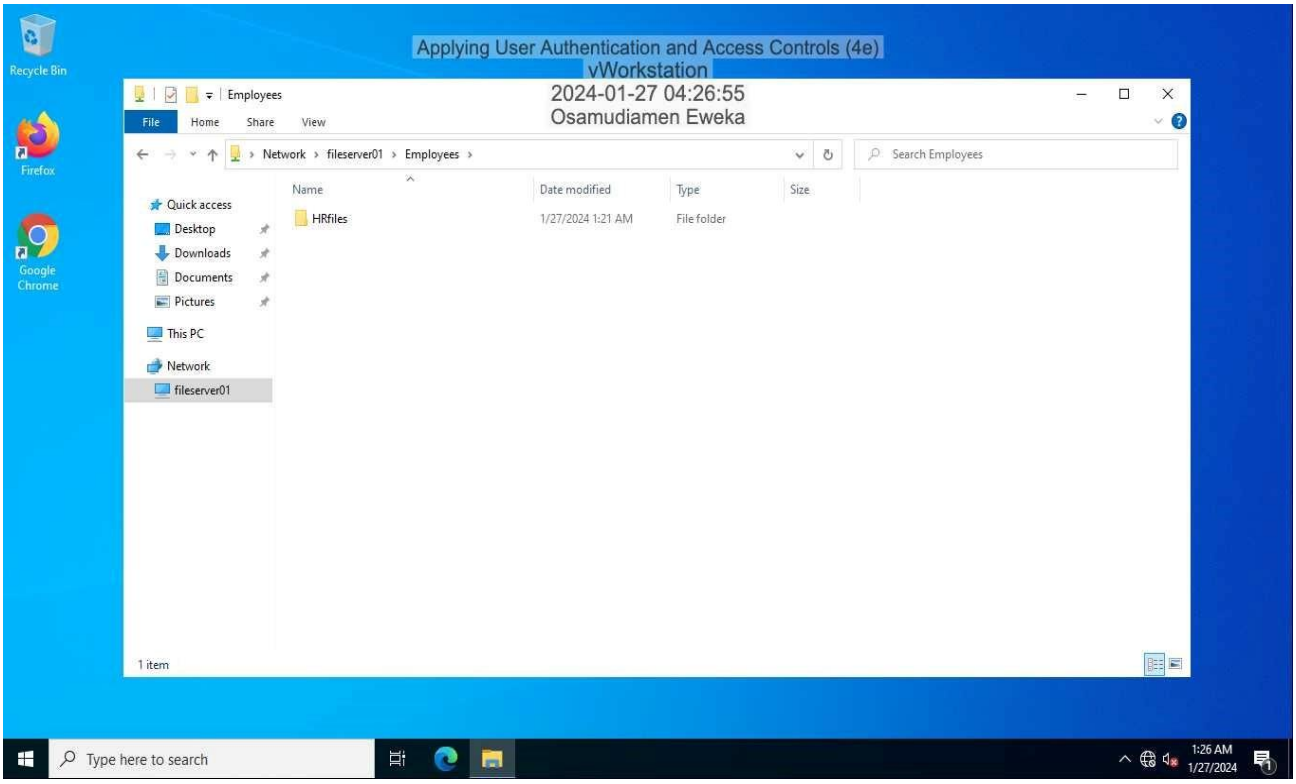
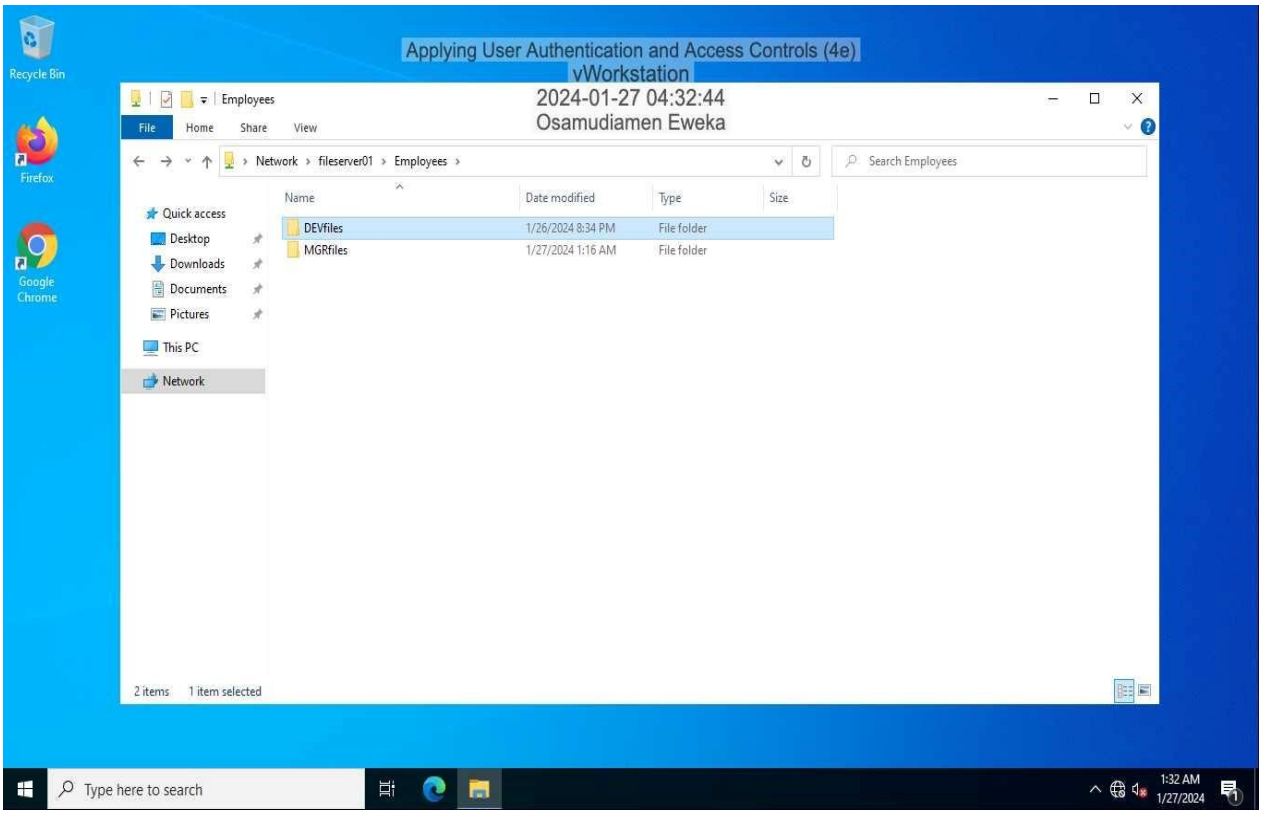


Figure 19 below captures a screen display of the Employees folder from the perspective of the user logged in as cprince (Jones & Bartlett, 2024). Consistent with the account's permissions setup, cprince is expected to have access to both the DEVfiles and MGRfiles folders. The image below confirms this expectation, demonstrating cprince's ability to view both folders. This visual confirmation serves as evidence of the successful implementation of ACLs, ensuring

that the access rights for cprince are in perfect alignment with his roles across the Developers and Managers groups. This access facilitation underscores the lab's commitment to enforcing precise and role-appropriate access controls within the networked environment.

Figure 19

Screen capture showing the Employees folder while signed in as cprince



Section 3

Challenge and Analysis

Part 1: Create Users and Security Groups

In this section of the lab, the narrative centers on streamlining the incorporation of GG Studios' workforce into the Active Directory framework of Secure Labs on Demand, an initiative sparked by a recent corporate amalgamation. The foundational step in this process was the establishment of specific global security groups, identified as GG-Developers and GG-Marketing, through the adept utilization of the Active Directory Users and Computers interface. This methodical classification fosters a compartmentalized management ethos, significantly enhancing the Security team's capability to meticulously oversee access rights and permissions amidst the transitional phase.

The lab's scope further extended to the crafting of user profiles for pivotal figures from GG Studios, encompassing Abernathy Bobbleshaw, the esteemed lead developer, and Leslie Wu, the Director of Marketing. These profiles were diligently affiliated with their respective security clusters, mirroring the pre-defined corporate hierarchy, and facilitating a fluid integration journey. To encapsulate this phase's essence, visual evidence was captured, spotlighting the Membership specifics under the Member Of tab located within the Properties dialog box for both Abernathy Bobbleshaw and Leslie Wu. This visual documentation strategy enhances the clarity and organization of the access and permission management protocol for GG Studios' departmental units, ensuring a structured and transparent integration endeavor.

Figure 20 furnishes a visual insight into the Member Of tab within the Properties dialog box for Abernathy Bobbleshaw (Jones & Bartlett, 2024). The image delineated below provides a

glimpse into the structured membership profile of Abernathy Bobbleshaw, showcasing the strategic group affiliations instrumental in the integration process.

Figure 20

Make a screen capture showing the Member Of tab of the Properties dialog box for Abernathy Bobbleshaw.

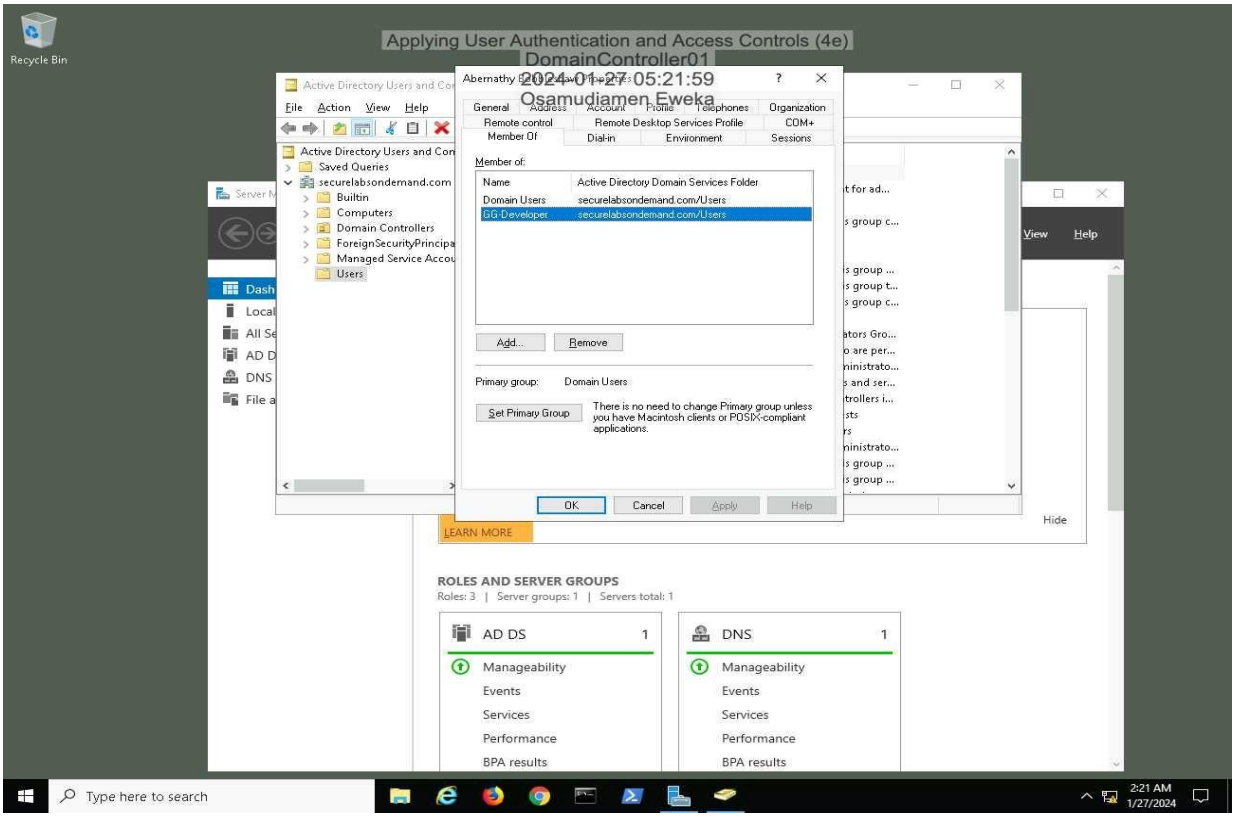
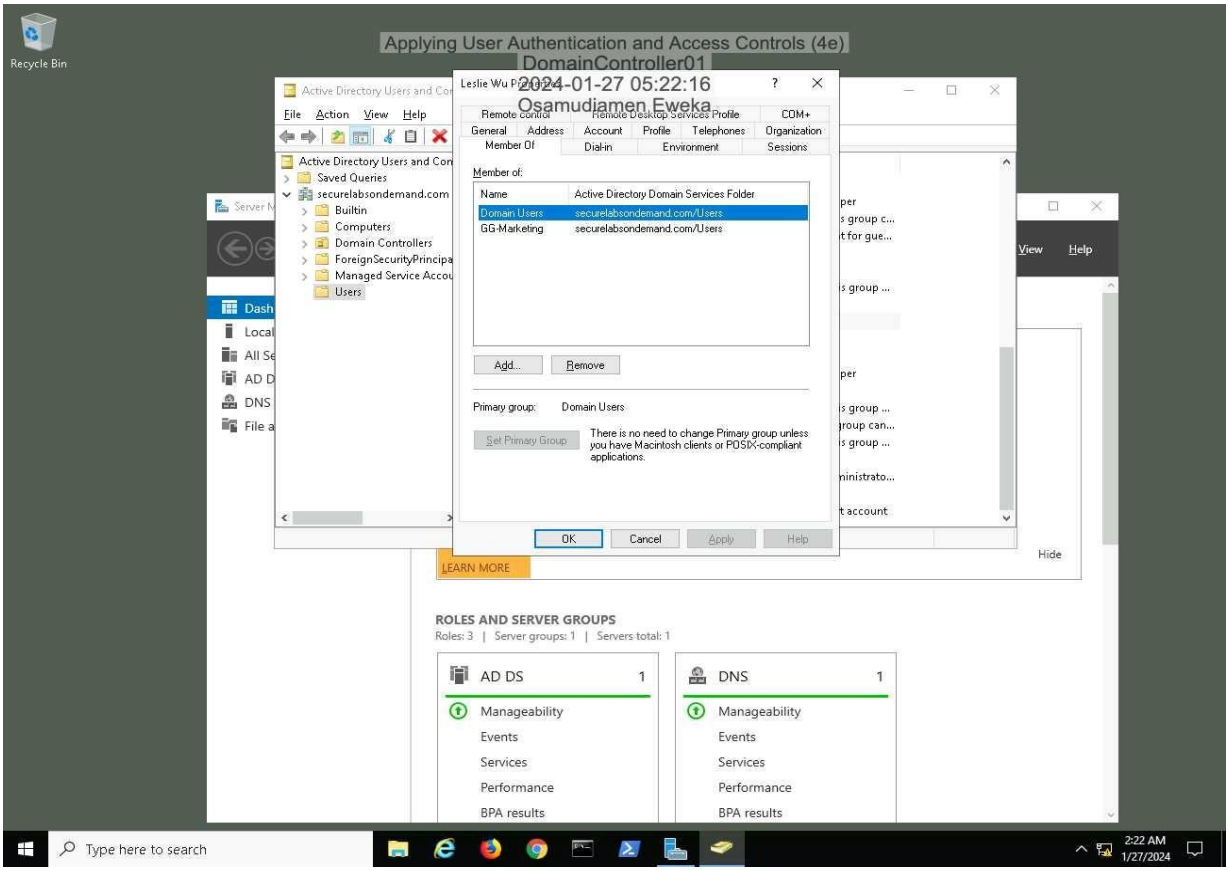


Figure 21

Make a screen capture showing the Member Of tab of the Properties dialog box for Leslie Wu.



Note. Figure 21 illustrates the "Member Of" section within the Properties dialogue for Leslie Wu, akin to the depiction provided in figure 20 (Jones & Bartlett, 2024). This section showcases Leslie Wu's affiliations or group memberships as specified in the system's settings, offering insight into the user's network or organizational structure permissions.

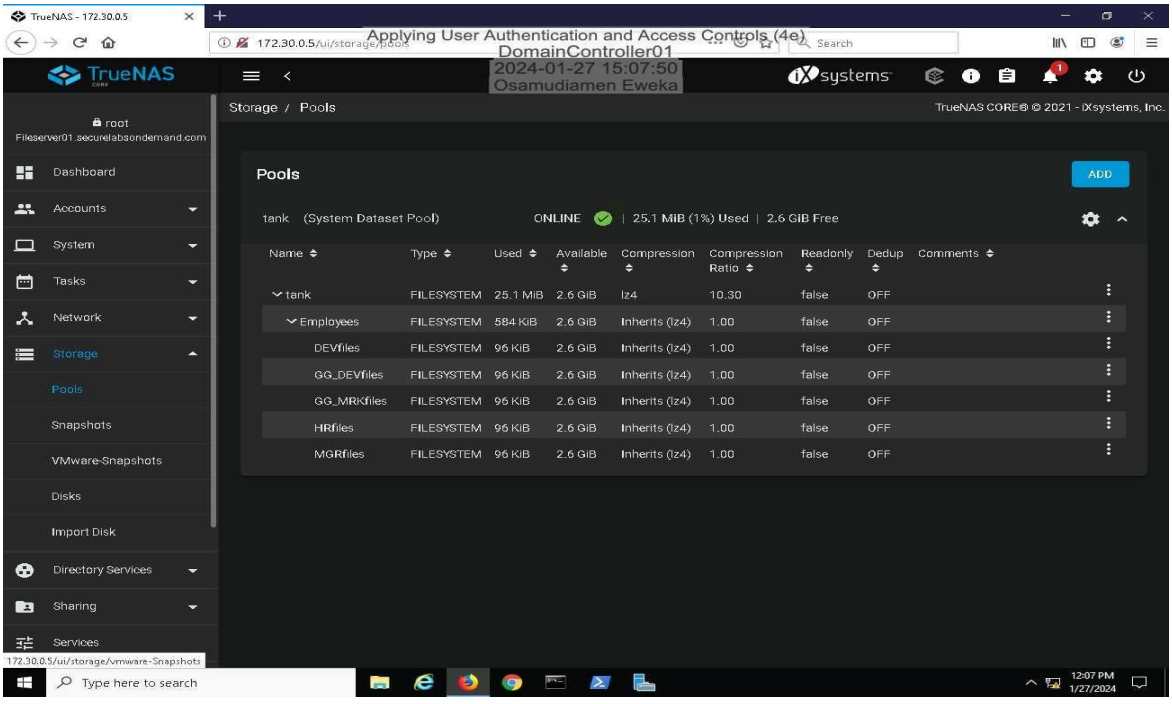
Section 3

Part 2: Create Shared Folders and Configure ACLs

In this lab section, the objective is to configure access for the GG Studios team to the Secure Labs on Demand NAS server using a TrueNAS server. The task includes creating two specific datasets within the Employees dataset on the tank pool, named GG_DEVfiles and GG_MRKfiles, and assigning Full Control permissions to the GG-Developers and GG-Marketing Active Directory groups. This involves rejoining the Secure Labs on Demand domain with detailed steps that include leaving and re-entering the domain with the provided credentials. This process is crucial for ensuring the GG Studios team's files are properly backed up and accessible. Figure 22 then visualizes the successful creation of these new GG Studios datasets within the TrueNAS Pools page, indicating the implementation of the lab segment's task (Jones & Bartlett, 2024).

Figure 22

Make a screen capture showing the new GG Studios datasets on the TrueNAS Pools page.



Section 3

Part 3: Verify Authentication and Access Controls

The final step in this laboratory section necessitates verifying the accuracy of the permissions configured in TrueNAS. This verification is performed by logging into the vWorkstation with the newly created user accounts and accessing the Employee's file share. The goal is to ensure that each user has access exclusively to the shared folder relevant to their department. This process is documented through screenshots captured while accessing the Employees folder as different users, including abobbleshaw and lwu, to demonstrate the effective application of the permissions. Figure 23 presents a screenshot capturing the access permissions in action, specifically showing the files accessible to abobbleshaw when signed into the system.

Figure 23

Make a screen capture showing the Employees folder while signed in as abobbleshaw.

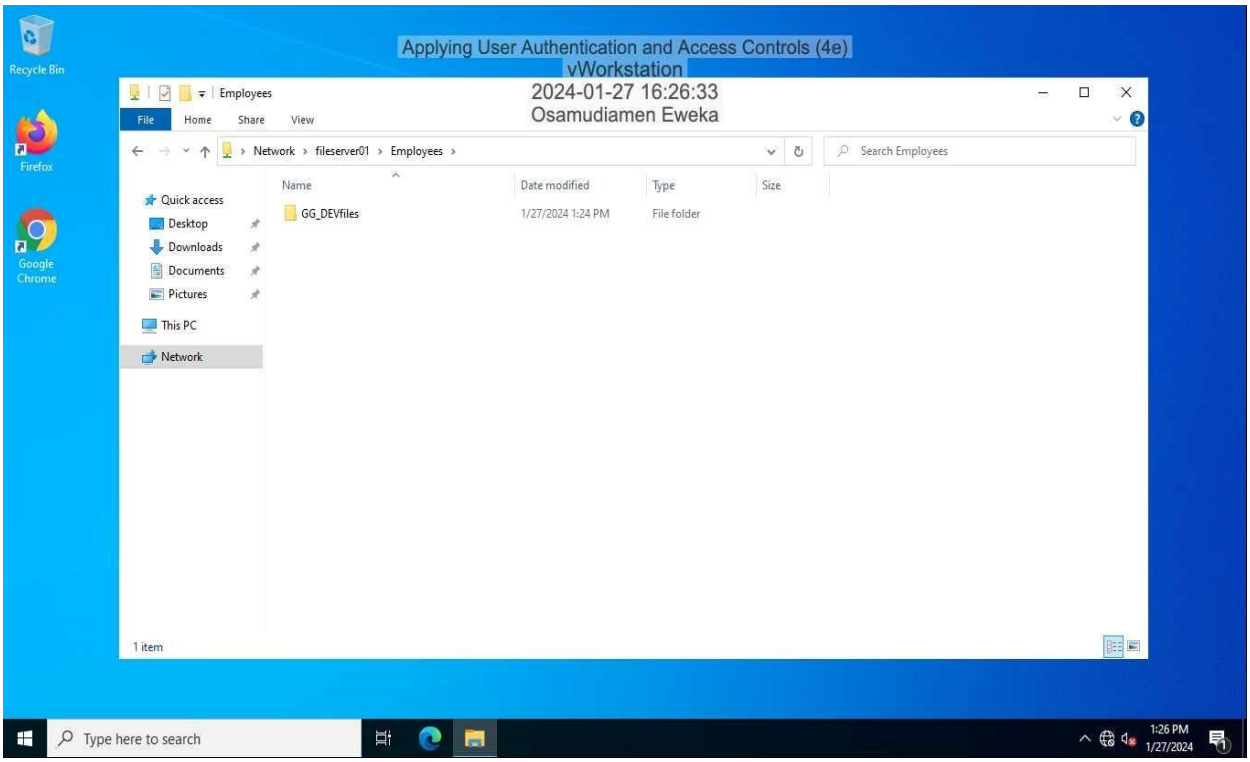
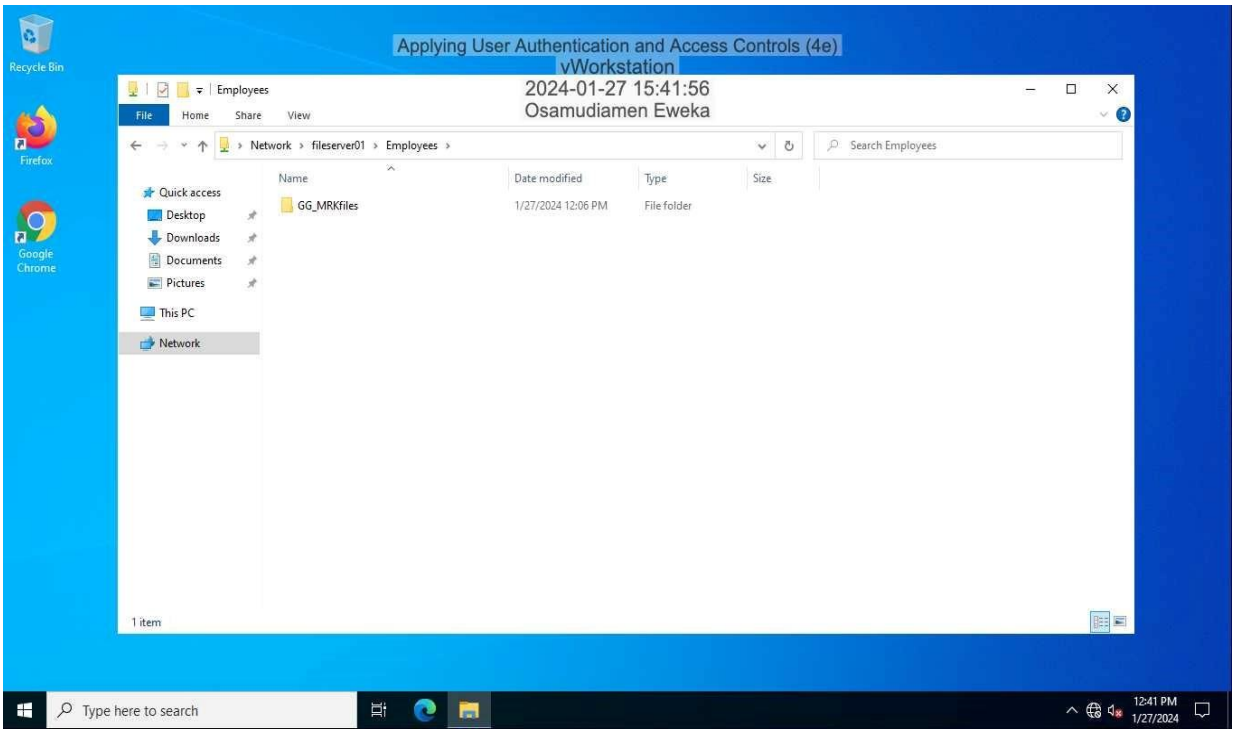


Figure 24

Make a screen capture showing the Employees folder while signed in as lwu



*Note***.** Figure 24 illustrates a screenshot of the Employees folder as accessed by lwu, showcasing the specific files that lwu is permitted to view upon logging in (Jones & Bartlett, 2024). This visualization confirms the effective restriction and customization of access based on departmental roles within the TrueNAS system.

Conclusion

This comprehensive lab report outlines a multi-faceted strategy to enhance the security framework of an organizational network. Initially, it demonstrates the setup of user accounts, security groups, and access controls using Active Directory, emphasizing role-based permissions for improved security management. The subsequent section delves into configuring TrueNAS and Samba for secure network-attached storage, including the creation of shared folders with specific access control lists. The report further explores integrating security measures for newly acquired company groups, adhering to the Principle of Least Privilege through meticulous access control verifications, culminating in a final validation of TrueNAS permissions. This methodical approach underscores the lab's commitment to bolstering the organization's security posture in line with industry standards.

Reference

Bruce, N., Lee, H. J., & Lee, S. (2014). Security analysis and improvements of authentication and access control in the internet of things. *Sensors*, *14*(8), 14786–14805. https://doi.org/10.3390/s140814786

Jones & Bartlett (2024). Applying User Authentication and Access Controls (Figures). *Jones and BartlettLearning Virtual Lab*. URL: https://jbl-lti.hatsize.com/startlab

Kim, D., & Solomon, M. G. (2021,) *Applying User Authentication and Access Controls*. Jones & Bartlett Learning. https://jbl-lti.hatsize.com/labguide

Sdwheeler. (2023, June 28). *What is PowerShell? - PowerShell*. Microsoft Learn. https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.4

TrueNAS, T. (2023). *TrueNAS core - world's most popular open storage OS*. https://www.truenas.com/truenas-core/