Evaluating Risks and Mitigation Strategies for Excessive Permissions in Enterprise Identity Access Management(IAM) Environments

Kylen D. Giddens

Master of Science in Cybersecurity

School of Cybersecurity

Old Dominion University

Project Advisor: Dr. Shideh Yavary

CYSE 698

April 17th, 2026

Spring 2026

Abstract

This project explores the topic of privilege escalation creep in identity access management(IAM) environments and the risks associated with it. Privilege escalation creep refers to the gradual increase of excessive permissions accumulated by a user or service accounts over time. This often comes as a result of user error, failing to remove temporary access to a resource, or misconfiguration of an account. From an enterprise standpoint, this creates a security risk for an organization increasing the organization's overall attack surface and exposing critical resources to unauthorized users The objective of this project was to analyze how privilege creep develops over time, evaluate the impact on an organization's security, and identify appropriate mitigation strategies. In order to accomplish this, a controlled virtual environment was created.

For this virtual environment, a simulation enterprise domain was created and consisted of three virtual machines. One machine acted as the domain controller, operating Windows Server 2022 and the remaining two machines acted as regular client machines, operating Windows 10. Using the domain controller, user and service accounts were created and configured with baseline privilege levels. To carry out the simulation, additional excessive privileges were applied to different accounts and were intentionally left assigned to the respective accounts and without ever revoking them. The results of this simulation highlighted how excessive privileges and improper use of access controls can lead to permissions without expiration dates, overprivileged accounts, and dormant administrative accounts, all of which create a security risk. This project was able to demonstrate practical insight to the problem and provide tangible mitigation strategies.

Table of Contents

Introduction

Privilege creep has been identified as a significant security risk in modern digital environments where user and service accounts gradually increase excessive permissions which accumulate over time. This is often a result of administrative oversight, or a lack thereof, changes in job duties, long term and temporary, and account misconfigurations. Over time, unchecked privilege creep increases attack surfaces within an organization and can lead to data breaches, security vulnerabilities, and unauthorized access. Research highlighted causes of privilege creep to include inconsistent enforcement of access control policies and a lack of separation of duties both of which are significant contributors. This is particularly true in situations where inconsistent governance of user permissions is prevalent. (Brickley & Thakur, 2021) Additionally, modern cybersecurity frameworks, namely NIST CSF, CIS Controls, and ISO/IEC 27002, support the idea that improper governance of identity and ineffective access control monitoring are significant factors that weaken an organization's overall security framework. (Bashofi & Salman, 2019) When organizations rely on centralized access control systems, such as Active Directory used in this project, it is necessary for those organizations to understand how privilege creep develops and how impactful it can be, given previously documented risks. (Haimed, Albahar, & Alzubaidi, 2023)

The intent of this project was to analyze how privilege creep develops in a domain where Active Directory is used and evaluate the impact on organizational security. This study sought to demonstrate how improper identity access management practices lead to excessive permission and offer mitigation strategies based on current standards. Previous studies suggest that the enforcement of least privilege and zero trust policies require an environment

where permissions are reviewed continuously and access to resources is structured prevents unnecessary accumulations of privileges. (Carter, 2022) Newer security practices, Zero Trust for example, further reinforces the need to continually monitor and verify access as well as eliminating implicit trust in a network help support the mission of keeping privilege creep to a minimum. (Kang, Liu, Wang, Meng, & Liu, 2023) The research question guiding this study is: How does privilege creep develop in a digital environment, and what security risks are introduced to organizational systems and data. The scope of this project is very limited and controlled to a virtual environment. No real-world enterprise systems, cloud services, or large-scale infrastructures are included. This study focuses specifically on on-premises configurations of Active Directory with controlled simulations focused on user access and permission changes. This allows for direct observation of how privilege escalations patterns emerged in structured testing environments.

Literature review

Privilege creep has been examined in the broader scope of identity access management and enterprise cybersecurity. Recently published research states that excessive permissions and ineffective access controls are key contributors to security vulnerabilities in any environment. A published study from 2021 highlights the importance of enforcing least privilege practices and segregation of duties while noting that failing to properly implement those practices will result in users gaining privileges that aren't appropriate for them to have. This ultimately increases the chances of inside threat actors and unauthorized access to sensitive systems or data. (Brickley & Thakur, 2021) In a similar claim from 2022, research discussed practical applications of least privilege policies emphasizing the need for access audits, continued monitoring and strict governance of user permissions, which in turn prevents potential misuse of access and unwanted escalation. (Carter, 2022)

Current technology and systems used for centralized identity management and access control play an essential role in both allowing and mitigating privilege creep. Enterprise cybersecurity environments often rely on services such as Active Directory and cloud-based services such as Azure Directory, both of which manage authentication and authorization. Both of these systems enable centralized mechanisms for role-based access control through the enforcement of group membership and policy enforcement. Despite being widely used, both systems are highly dependent on being configured correctly and ongoing management in order to be effective. A study published in 2023 demonstrated that improper configurations within Active Directory can be exploited to complete privilege escalation attacks. (Haimed, Albahar, & Alzubaidi, 2023) This suggests that while advanced technologies may be available, they can also be the sole cause of a security lapse when not properly managed.

Current cybersecurity frameworks help provide a structured approach to managing access control and reducing the risks associated with privilege creep. The integration of NIST Cybersecurity Framework , v8 CIS Controls, and ISO/IEC 27002 were examined in a study in 2019. The report highlighted that all three frameworks emphasize identity governance, access control enforcement, and continuous monitoring as components of cybersecurity maturity. (Bashofi & Salman, 2019) Each framework advocates for strong implementation of least-privilege access, regular auditing, and strong policy enforcement. Additionally, Zero Trust security model has gained traction as a modern approach to access control. This model is described as a framework that eliminates implicit trust in a network and requires continuous verification of user access. (Kang, Liu, Wang, Meng, & Liu, 2023) This approach relies on strict access control and aligns with efforts to prevent privilege creep through ensuring permissions are continually validated and evaluated.

Despite the availability of newer, more advanced technologies, and well-established frameworks, there are still gaps to be filled in the research and practical application. Many of the current studies focus on high-level frameworks and cloud-based software but have limited insight on how privilege creep develops and performs in locally based systems. In addition to that, there is a lack of experimental research demonstrating how this situation occurs in real-world situations. Existing studies often emphasize prevention strategies while failing to acknowledge provide sufficient evidence on how privilege creep evolves in practice or in controlled environments. Acknowledging this gap helped guide the focus of this project.

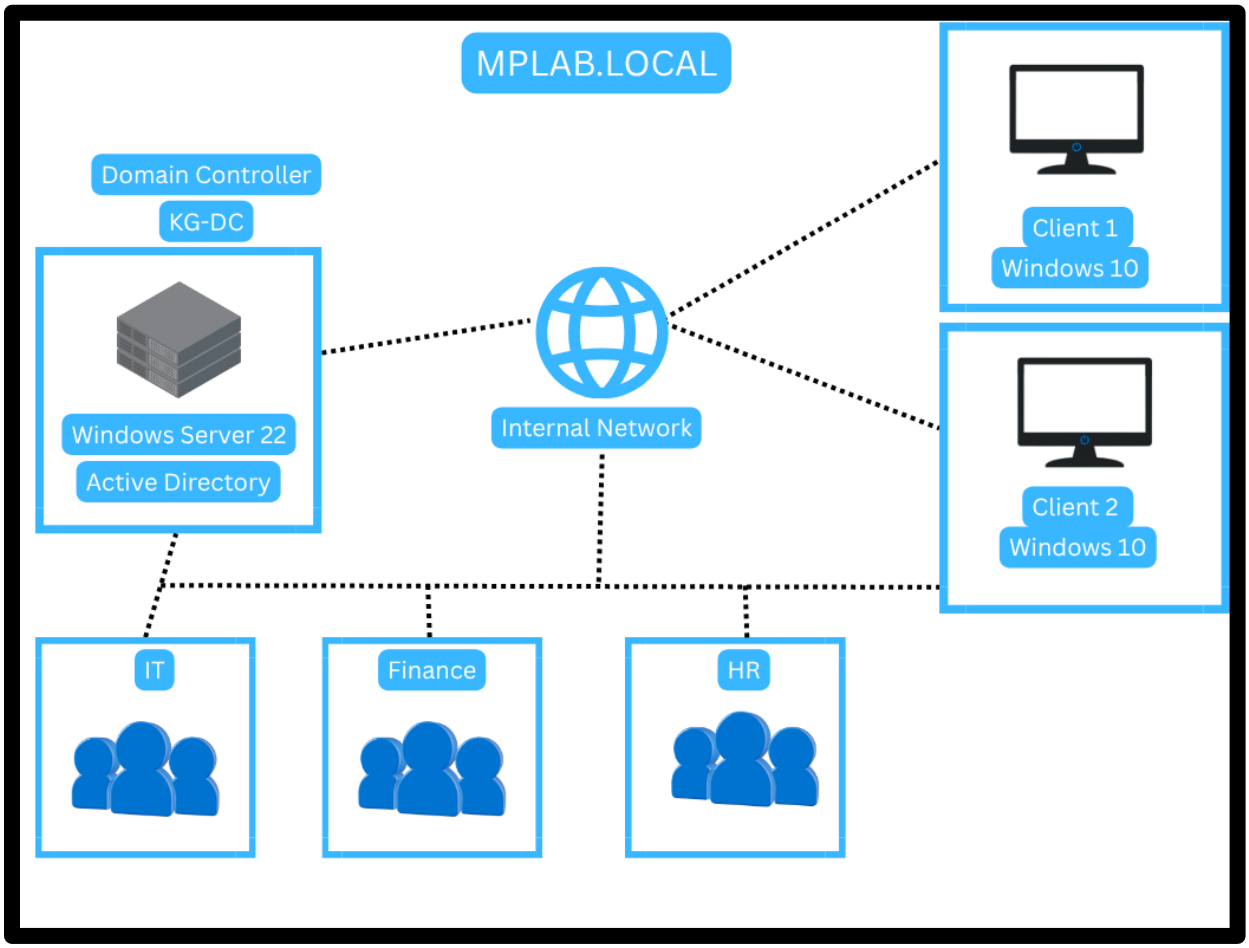
Methodology & Implementation

Through the use of controlled virtual environments and Identity Access Management(IAM) processes, I analyzed the implications of unmonitored access and privilege escalation within a domain. A fictional company environment was created to provide structure and realism to the simulation. The overall structure of this project consisted of a domain tied to the company and included three virtual machines. The first machine acted as a domain controller using Windows 2022 Server with Active Directory Domain Services while the remaining two machines simulated standard client devices within an organization running on Windows 10. All three machines operated on the environment's internal network to ensure proper communication between devices and isolation from external networks, creating a fully maintained controlled environment.

After configuring the virtual infrastructure and creating the domain, the Identity Access Management structure was formed. Organizational units were formed to represent departments within the fictional company including IT, Finance, Human Resources, and service accounts. Security groups were created for each department to include IT Admins, Finance department users, Human Resources users, and shared permission groups. Doing this, established a framework for controlling access amongst shared resources. User accounts were created and assigned to their respective organizational units and security groups. This established baseline access levels while also simulating realistic role-based access controls, where user permissions are granted based on job function. After completing this step, a shared resource folder was created which served as a controlled resource during the study to test access permissions

This folder was shared with the different organizational units and security groups, and each had varying levels of access and permissions. Some were able to fully modify contents of the folder, while others were only able to read contents of the folder, some were not able to do either. This folder contained files that should only be accessible by the intended users. To establish the baseline for this study, each user account was tested by logging into the client machine to verify permissions set for each person and department. This helped identify what users already have access to prior to simulating any changes.

System Structure



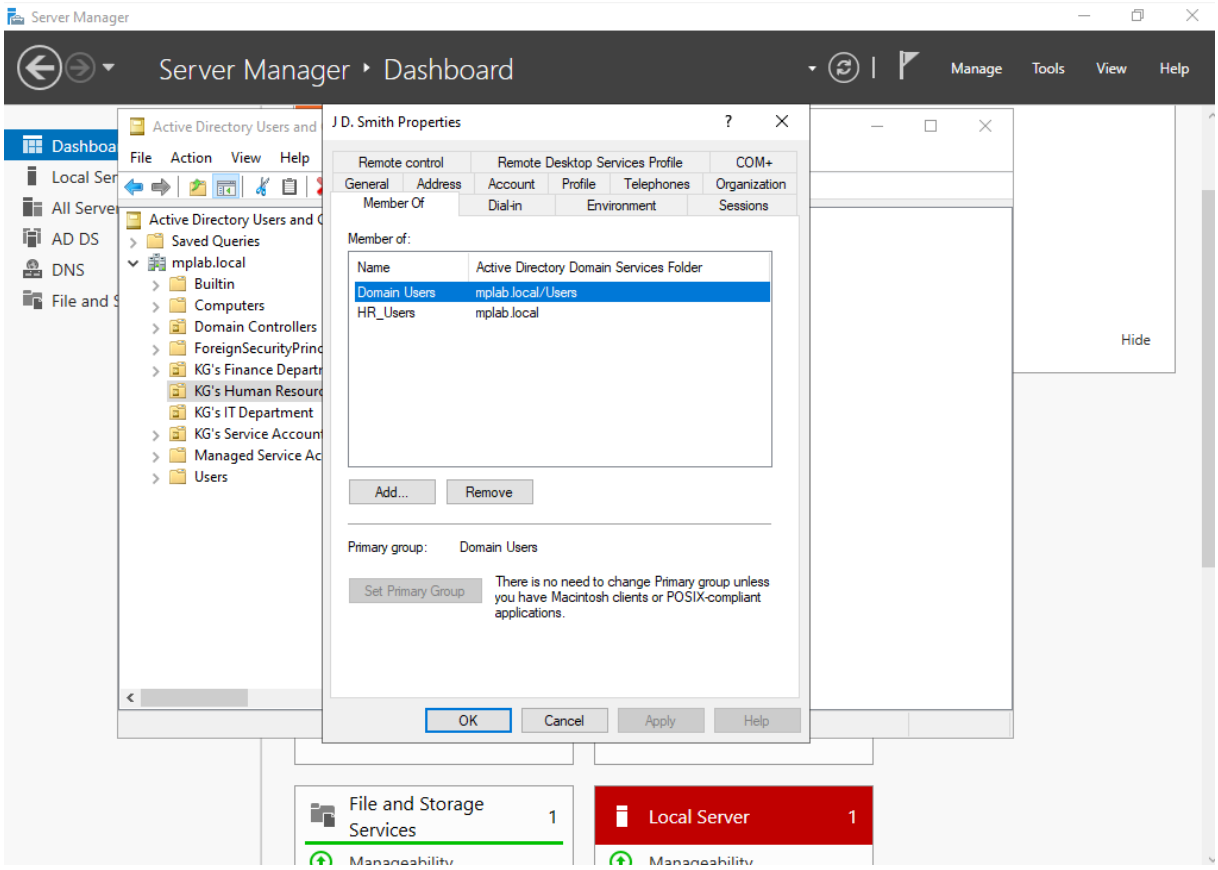
This virtual environment was run by the software Oracle VirtualBox Manager. The virtualization experience was hosted on a Gigabyte x64 based PC with 16GB Ram and an Intel i5 Core processor operating on Windows 11 Home OS. The virtual environment was run solely on the internal network of the environment isolating it from external networks. There were three total devices that ran on the network, one domain controller running Windows Server 2022 and two client machines running Windows 10. All three devices operated under the domain mplab.local. Each account within the domain was password protected.

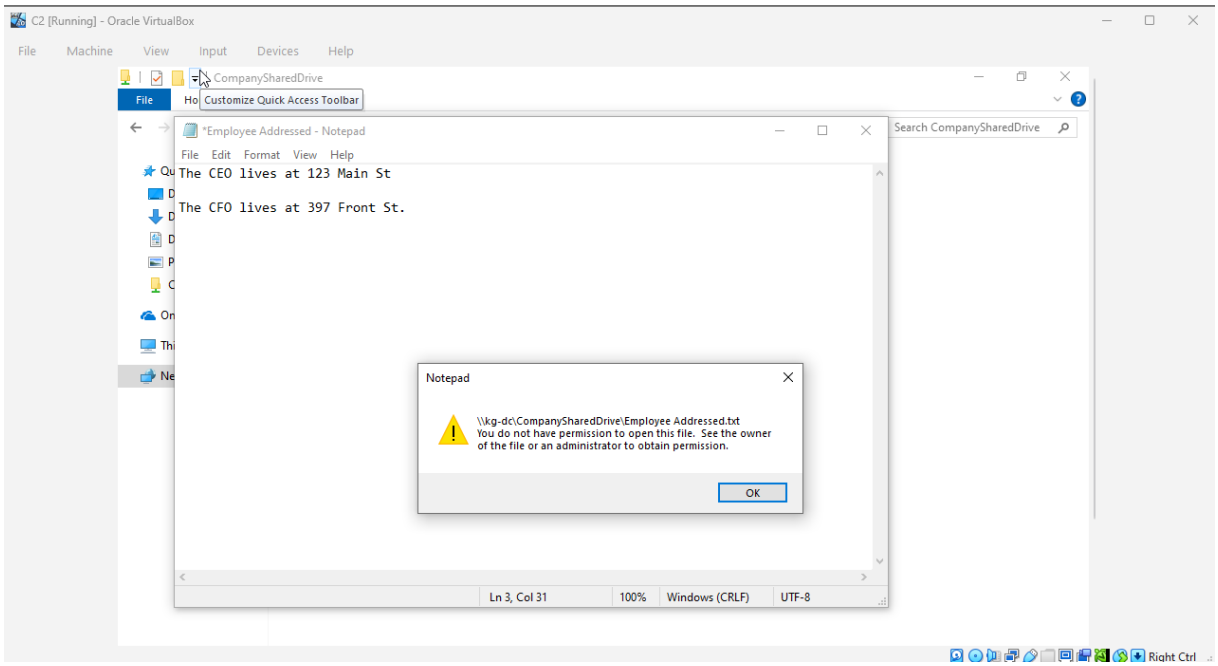
Testing & Evaluation

This project was tested within a controlled virtual environment which assisted with the evaluation of the development and impact of privilege creep when using Active Directory in a domain. The testing procedures began by establishing a baseline configuration where all user accounts were assigned permissions. These permissions were based on respective security groups and organizational units while keeping in mind the principle of least privilege. Each user account was accessed through one of the two client machines to verify initial access levels to the shared resources in the network. Access to the shared resources as well as modification of the resources was attempted to confirm is permissions were enforced correctly. After establishing and verifying the baseline the act of privilege creep was simulated by modifying group membership and allowing additional permissions for certain users and service accounts. Some of the changes included adding basic users to security groups with higher privileges, allowing administrator access to network resources, and setting temporary permissions without revoking them. After modifications were complete access and resource tests were completed again to observe newly gained capabilities and resource access. All changes were documented to show the difference in levels of access before and after. Evaluations of this test included accuracy of the enforcement of access control, the impact of excessive permissions, and the consistency of access control. Also tested in this project was system performance with no notable changes. Finally, security was tested by intentional misconfiguration and excessive permissions simulating realistic vulnerabilities. The results showed that the misconfiguration resulted in unauthorized access to sensitive resources confirming the risks associated with privilege creep.

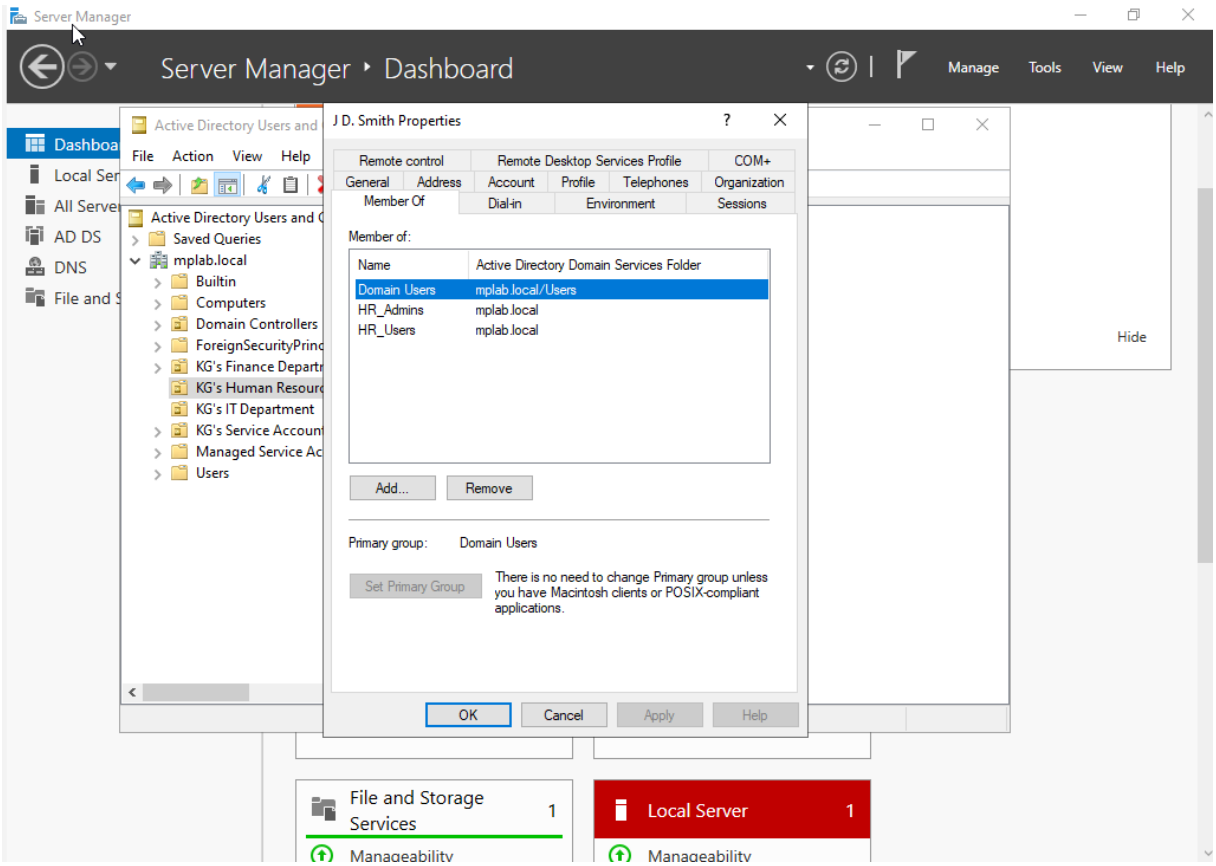
Results & Analysis

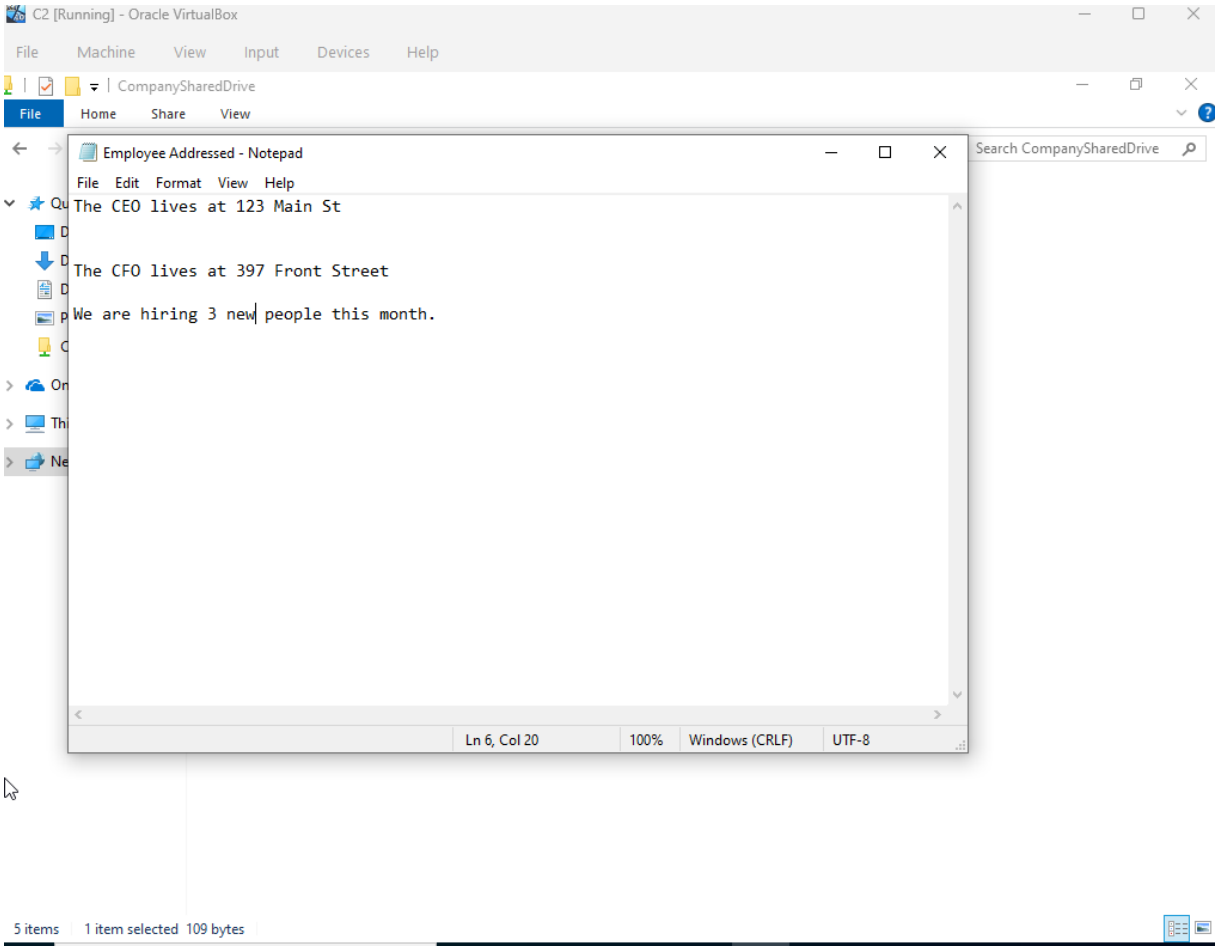
User J.D Smith Account Before Privilege Escalation: Member of HR_Users with no access to modify shared resources.





User J.D Smith Account After Privilege Escalation: Member of HR_Admins & HR_Users with access to modify shared resources.


Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Active Directory Users and
File Action View Help
Saved Queries
mplab.local
Builtin
Computers
Domain Controllers
KG's IT Department
Users
J D. Smith Properties
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
Member Of
Dial-in
Environment
Sessions
Member of:
Name
Active Directory Domain Services Folder
Domain Users
mplab.local/Users
HR_Admins
mplab.local
HR_Users
mplab.local
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help
Hide
File and Storage Services
1
Manageability
Local Server
1
Manageability


C2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
CompanySharedDrive
File Home Share View
Search CompanySharedDrive
Employee Addressed - Notepad
File Edit Format View Help
The CEO lives at 123 Main St
The CFO lives at 397 Front Street
We are hiring 3 new people this month.
Ln 6, Col 20
100%
Windows (CRLF)
UTF-8
5 items
1 item selected 109 bytes

Conclusion

The project examined the development of and impact of privilege creep within an Active Directory managed identity access management domain. Findings showed that even during a simulation, even the smallest of changes to user permissions can quickly result in excessive privileges, whether intentional or not. These changes led to unneeded access to restricted resources, showing how easily the idea of least privilege can be undermined when not actively managed. The results of the test confirmed that privilege creep does in fact increase attack surfaces for an environment and creates opportunity for those seeking it, especially when system oversight and an auditing process are absent. By simulating real-world scenarios, the project was able to clearly provide a tangible example of how excessive privileges become an area of concern over time while impacting security. Additionally, it reinforced the importance of having structure within a network not only with identity access management, but in other aspects as well. Several key issues were addressed. First, the importance of maintaining least privilege practices cannot be understated. Secondly, while effective, group-based access can pose a security risk if not reviewed regularly. Finally, even the smallest misconfiguration can lead to great security risks. Improvement for the future would include regular auditing processes and using automated tools for monitoring and alerting potential risks. In conclusion, this project successfully demonstrated that privilege creep is a persisting problem that can be easily overlooked created an organizational risk if not effectively managed. It underscored the importance of proactive security practices and provided effective suggestion for improving security practices.

Works Cited

Bashofi, I., & Salman, M. (2019). Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002.

Brickley, J., & Thakur, K. (2021). Policy of Least Privilege and Segregation of Duties, their Deployment, Application,. *International Journal of Cyber-Security and Digital Forensics*.

Carter, M. K. (2022). Techniques To Approach Least Privilege.

Haimed, I. B., Albahar, M., & Alzubaidi, A. (2023). Exploiting Misconfiguration Vulnerabilities in Microsoft's Azure Active Directory for Privilege Escalation Attacks.

Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey.