A Course Based Project Report on

Windows Domain Hardening

Submitted to the

Department of CSE- (CyS,DS) and AI&DS

in partial fulfilment of the requirements for the completion of course
PLATFORMS AND SYSTEM SECURTIY (A19PC2CS64)
BACHELOR OF TECHNOLOGY

in

Department of CSE-(Cyber Security)

Submitted by

N.V. CHIRUHAS	21071A6238
R.AVINASH	21071A6249
V. BHAVANA	21071A6261
V. LAXMAN REDDY	21071A6263

Under the guidance of

Dr. P.Subhash

(Course Instructor)

Associate Professor, Department of CSE-(CyS,DS) and AI&DS, VNRVJIET

Department of CSE-(CyS,DS) and AI&DS

VALLURUPALLI NAGESWARA RAO VIGNANA JYOTHI INSTITUTE OF ENGINEERING & TECHNOLOGY

An Autonomous Institute, NAAC Accredited with ‘A++’ Grade, NBA

Vignana Jyothi Nagar, Pragathi Nagar, Nizampet (S.O), Hyderabad – 500 090, TS, India

JUNE 2024

VALLURUPALLI NAGESWARA RAO VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

An Autonomous Institute, NAAC Accredited with ‘A++’ Grade, NBA Accredited for CE, EEE, ME, ECE, CSE, EIE, IT B. Tech Courses, Approved by AICTE, New Delhi, Affiliated to JNTUH, Recognized as “College with Potential for Excellence” by UGC, ISO 9001:2015 Certified, QS I GUAGE Diamond Rated
Vignana Jyothi Nagar, Pragathi Nagar, Nizampet(SO), Hyderabad-500090, TS, India

DEPARTMENT OF CSE-(CyS,DS) and AI&DS

TAMASOMA JYOTIRGAMAYA
Estd.1995

CERTIFICATE

This is to certify that the project report entitled “**Windows Domain Hardening**” is a bonafide work done under our supervision and is being submitted by **Mr.N.V.Chiruhas (21071A6238), Mr. R.Avinash (21071A6249), Miss. V.Bhavana (21071A6261), Mr.V.Laxman Reddy (21071A6263)** in partial fulfilment for the award of the degree of **Bachelor of Technology** in **CSE-(Cyber Security),** of the VNRVJIET, Hyderabad during the academic year 2023-2024.

Dr. P.Subhash	**Dr. M. RAJASEKAR**
Associate Professor	Professor & HOD
Dept of CSE-(CyS,DS) and AI&DS	Dept of CSE-(CyS, DS)and AI&DS

Course based Projects Reviewer

VALLURUPALLI NAGESWARA RAO VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

An Autonomous Institute, NAAC Accredited with ‘A++’ Grade,
Vignana Jyothi Nagar, Pragathi Nagar, Nizampet(SO), Hyderabad-500090, TS, India

DEPARTMENT OF CSE-(CyS,DS) and AI&DS

DECLARATION

We declare that the course based project work entitled “**Windows Domain Hardening**” submitted in the Department of **CSE-(CyS,DS) and AI&DS**, Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology, Hyderabad, in partial fulfilment of the requirement for the award of the degree of **Bachelor of Technology in CSE- (Cyber Security)** is a bonafide record of our own work carried out under the supervision of **Dr.P.Subhash, Associate Professor, Department of CSE- (CyS,DS) and AI&DS, VNRVJIET.** Also, we declare that the matter embodied in this thesis has not been submitted by us in full or in any part thereof for the award of any degree/diploma of any other institution or university previously.

Place: Hyderabad.

N.V.Chiruhas	**R.Avinash**	**V.Bhavana**	**V.Laxman Reddy**
(21071A6238)	(21071A6249)	(21071A6261)	(21071A6263)

ACKNOWLEDGEMENT

We express our deep sense of gratitude to our beloved President, Sri. D. Suresh Babu, VNR Vignana Jyothi Institute of Engineering & Technology for the valuable guidance and for permitting us to carry out this project.

With immense pleasure, we record our deep sense of gratitude to our beloved Principal, Dr. C.D Naidu, for permitting us to carry out this project.

We express our deep sense of gratitude to our beloved Professor Dr. M.Rajasekar, Professor and Head, Department of CSE-(CyS,DS) and AI&DS,VNR Vignana Jyothi Institute of Engineering & Technology, Hyderabad-500090 for the valuable guidance and suggestions, keen interest and through encouragement extended throughout the period of project work.

We take immense pleasure to express our deep sense of gratitude to our beloved Guide, Dr.P.Subhash, Associate Professor in CSE-(CyS,DS) and AI&DS, VNR Vignana Jyothi Institute of Engineering & Technology, Hyderabad, for his/her valuable suggestions and rare insights, for constant source of encouragement and inspiration throughout my project work.

We express our thanks to all those who contributed for the successful completion of our project work.

Mr. N.V. Chiruhas	(21071A6238)
Mr. R. Avinash	(21071A6249)
Miss. V. Bhavana	(21071A6261)
Mr. V. Laxman Reddy	(21071A6263)

TABLE OF CONTENTS

ABSTRACT

Windows domain environments are integral to managing and securing enterprise IT infrastructures, enabling centralized administration, streamlined access control, and efficient resource allocation. Their critical role and extensive use, however, make them prime targets for cyberattacks. These attacks can range from initial foothold exploits to sophisticated privilege escalations and lateral movements within the network. The document presented here is a comprehensive and curated list of security hardening techniques specifically designed for Windows domains. It draws extensively from expert research, real-world security incidents, and authoritative industry talks, offering IT professionals robust strategies to protect their environments. The primary objective is to equip administrators with actionable measures that significantly enhance their security posture, reduce vulnerabilities, and safeguard against a broad spectrum of cyber threats. By implementing these best practices, organizations can fortify their defenses, ensuring the integrity, availability, and confidentiality of their IT assets. Continuous evaluation and adaptation of these measures are crucial to addressing emerging threats and maintaining a proactive security stance.

CHAPTER-1

INTRODUCTION

In the ever-evolving landscape of cybersecurity, Windows domain environments play a pivotal role in enterprise IT management and security. These domains are essential for maintaining user accounts, enforcing security policies, and managing network resources effectively. The centralized administration provided by Windows domains streamlines operational tasks, reduces complexity, and enhances organizational efficiency. However, their critical function and widespread use make them attractive targets for cyber adversaries, who constantly seek to exploit vulnerabilities within these environments.

The increasing sophistication of cyber threats presents significant challenges to the security of Windows domain environments. Attackers employ various methods to exploit weaknesses, gain unauthorized access, and compromise systems. Common attack vectors include phishing campaigns, malware infections, and credential theft. Once attackers gain an initial foothold, they conduct reconnaissance to map out the domain structure, identify critical assets, and plan further attacks. This reconnaissance allows them to execute lateral movements, escalating their privileges and expanding their reach within the network.

The complexity and scale of Windows domain environments contribute to their vulnerability. Misconfigurations, outdated systems, and inadequate monitoring can create opportunities for attackers. Moreover, the sheer volume of administrative tasks and the diverse range of devices and users increase the risk of oversight and human error. To address these challenges, it is essential to implement a comprehensive and proactive security strategy that encompasses best practices, advanced tools, and continuous monitoring.

This document synthesizes a wealth of knowledge from leading cybersecurity experts, including insights from conference talks, research papers, and real-world incident analyses. It provides a curated list of security hardening techniques specifically tailored for Windows domains. The recommended measures are designed to address various stages of the attack lifecycle, from initial access prevention to advanced threat detection and response. By adopting these techniques, organizations can strengthen their defenses, mitigate risks, and ensure the integrity, availability, and confidentiality of their IT assets.

CHAPTER-2

Problem Definition

Windows domain environments, due to their widespread adoption and critical functions, are frequently targeted by cyber adversaries. These environments manage user authentication, enforce security policies, and control access to network resources, making them highly attractive targets for attackers seeking to disrupt operations or exfiltrate sensitive data. The vulnerabilities in these environments can be attributed to several factors, including outdated operating systems, weak configuration settings, insufficient monitoring, and the inherent complexity of managing a large-scale IT infrastructure.

Attackers employ various methods to exploit these vulnerabilities. Initial foothold attacks often involve phishing campaigns, malware delivery, or exploiting unpatched software vulnerabilities to gain access to the network. Once inside, attackers conduct reconnaissance to gather information about the domain structure, user accounts, and security configurations. This reconnaissance phase is critical for planning further attacks, such as lateral movements and privilege escalations.

Lateral movement techniques allow attackers to traverse the network, compromising additional systems and accounts. They may use tools and tactics such as Pass-the-Hash, Pass-the-Ticket, or exploiting weak network protocols to move between systems. Privilege escalation attacks enable attackers to gain higher-level access, often reaching administrative privileges, which can grant them control over critical systems and data.

The primary challenge for organizations is to implement a comprehensive and effective security strategy that addresses these vulnerabilities without hindering operational efficiency. This requires a multifaceted approach that includes proactive threat detection, stringent access controls, regular system updates, and continuous monitoring. Organizations must balance the need for security with the operational requirements of their IT environments, ensuring that security measures do not impede productivity or usability.

CHAPTER-3

OBJECTIVE

The objective of this document is to provide a detailed and actionable guide for hardening Windows domain environments against cyber threats. By following the curated list of security measures, organizations can achieve several key goals:

1. Enhance Security Posture: Strengthen the overall security of Windows domains to defend against both common and sophisticated attacks. This includes implementing best practices, leveraging advanced security tools, and continuously monitoring for potential threats.

2. Mitigate Attack Vectors: Implement specific techniques to reduce the risk of initial foothold, lateral movement, privilege escalation, and data exfiltration. These techniques are designed to address common vulnerabilities and attack methods, providing a robust defense against a wide range of threats.

3. Practical Implementation: Offer clear, actionable steps that IT administrators can easily deploy within their existing infrastructure. The recommended measures are practical and achievable, ensuring that organizations can implement them without significant disruption to their operations.

4. Incorporate Expert Insights: Leverage best practices and recommendations from leading cybersecurity researchers and practitioners. The curated list of techniques is based on extensive research and real-world experiences, ensuring that the recommendations are both relevant and effective.

5. Promote Continuous Improvement: Encourage regular review and adaptation of security measures to keep pace with evolving threats and technologies. Security is an ongoing process, and organizations must continually refine their strategies to address new challenges and protect their IT environments effectively.

By achieving these objectives, organizations can create a more secure and resilient IT infrastructure. The implementation of these security measures will help protect against a broad spectrum of cyber threats, ensuring the integrity, availability, and confidentiality of critical data and systems.

CHAPTER-4

PROPOSAL

Initial Foothold Mitigation

No hardening effort should compromise upgrading operating systems. Upgrading to the latest versions, such as Windows 10 and Edge, should be prioritized. Deploying the Enhanced Mitigation Experience Toolkit (EMET) to workstations, although it reached the end of life in July 2018, can still be beneficial for older systems like Windows 7. Additionally, use AppLocker to block executable content from running in user locations such as home directories, profile paths, and temporary folders. AppLocker configurations can prevent the execution of unauthorized applications and scripts, which are common vectors for malware and other malicious activities.

To harden against Direct Memory Access (DMA) attacks, consider using techniques recommended by Synacktiv and other security experts. Manage PowerShell execution by using AppLocker or constrained language mode and enable comprehensive logging of PowerShell activities. Blocking Office macros, both on Windows and Mac, for content downloaded from the Internet is crucial to prevent macro-based malware attacks. Deploy security tools that monitor for suspicious behavior and use Windows Event Forwarding (WEF) to send critical events to your Security Information and Event Management (SIEM) system. Limiting the capability to execute certain file types via email or download further reduces the attack surface.

Reconnaissance Prevention

Deploy Windows 10 and limit local group enumeration to prevent attackers from easily discovering network information. Reduce workstation-to-workstation communication to minimize the potential lateral movement paths. Enhance the security of sensitive Group Policy Objects (GPOs) and evaluate the deployment of behavior analytics tools, such as Microsoft Advanced Threat Analytics (ATA), to detect anomalous activities.

Use NetCease to prevent unprivileged session enumeration and SamRi10 to stop unprivileged local admin collection, both of which are critical in hindering attacker reconnaissance. These measures are particularly important for maintaining a secure environment in Windows 10 version 1607 and above.

Lateral Movement Controls

Configure GPOs to prevent local accounts from authenticating over the network by following guidelines like those in KB2871997. Additionally, set specific registry keys to clear credentials of logged-off users after 30 seconds and prevent Wdigest credentials from being stored in memory. Automatically changing local administrator passwords with tools like Microsoft Local Administrator Password Solution (LAPS) and removing extra local admin accounts is essential for reducing the risk of lateral movement. Limit workstation communication through Windows Firewall and regularly test remote administration tools like PsExec to ensure they do not facilitate unauthorized lateral movement.

Privilege Escalation Prevention

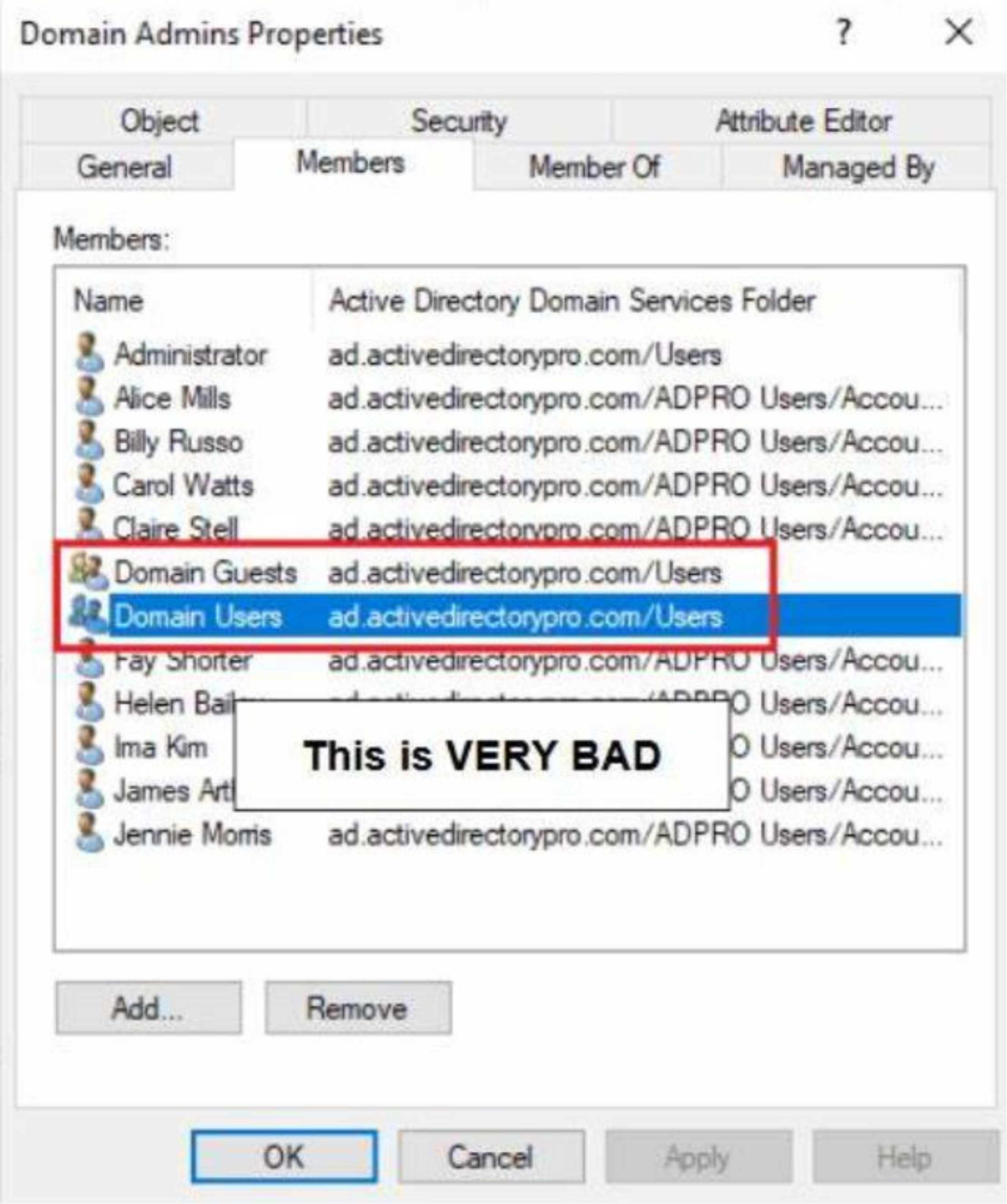
To prevent privilege escalation, remove files with embedded passwords from SYSVOL, including Group Policy Preferences (GPP). Configure GPOs to ensure administrators do not log onto untrusted systems by using "deny" user right assignments. Provide Privileged Access Workstations (PAWs) for highly privileged tasks, ensuring these workstations have no internet access. Use Managed Service Accounts (MSAs) where possible, and for systems that do not support them, deploy a Fine-Grained Password Policy (FGPP) to enforce passwords of over 32 characters. Ensure all systems use NTLMv2 and Kerberos, and deny LM/NTLMv1 authentication protocols to enhance credential security.

Protection of Administrative Credentials

Administrators should only log onto approved admin workstations and servers. Ensure that built-in groups, except for Administrator, are denied access to Domain Controllers via User Right Assignments. Add all admin accounts to the Protected Users group, which requires Windows Server 2012 R2 or later. Control and limit access to admin workstations and servers, disable legacy protocols like NetBIOS over TCP/IP, Link-Local Multicast Name Resolution (LLMNR), and Web Proxy Auto-Discovery Protocol (WPAD) to reduce attack vectors.

Strengthening and Removing Legacy Components

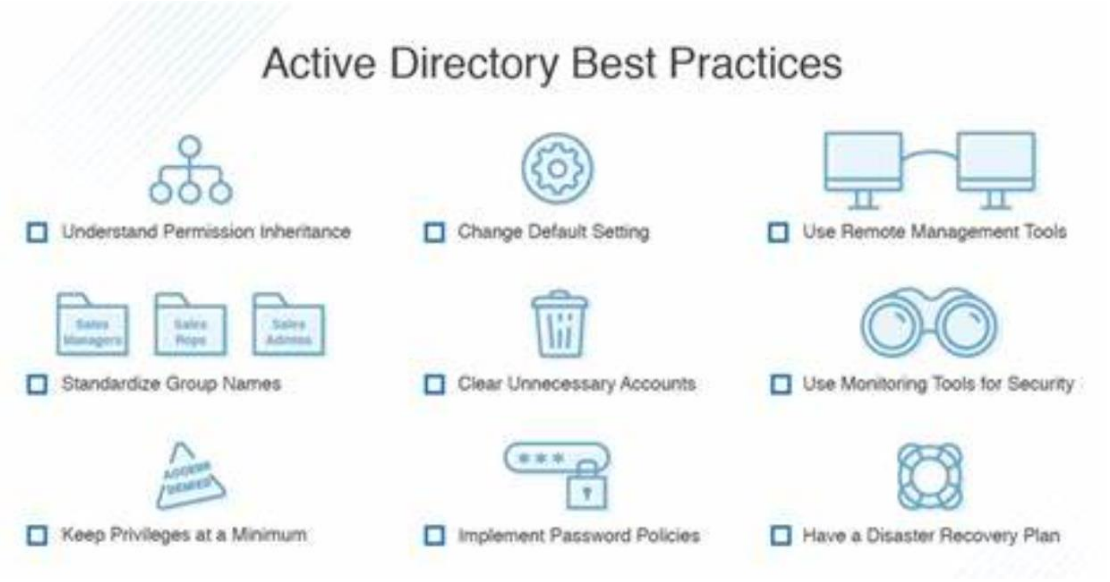
Use tools like PingCastle to audit Active Directory and implement NTLM restrictions and LDAP signing. Enforce SMB signing and encryption where possible. Start with disabling legacy components such as SMB 1.0/CIFS and Windows PowerShell 2.0 in Windows 10. Employ application shims to enable legacy applications to run with required privileges without compromising security.



Members:

Name	Active Directory Domain Services Folder
Administrator	ad.activedirectorypro.com/Users
Alice Mills	ad.activedirectorypro.com/ADPRO Users/Accou...
Billy Russo	ad.activedirectorypro.com/ADPRO Users/Accou...
Carol Watts	ad.activedirectorypro.com/ADPRO Users/Accou...
Claire Stell	ad.activedirectorypro.com/ADPRO Users/Accou...
Domain Guests	ad.activedirectorypro.com/Users
Domain Users	ad.activedirectorypro.com/Users
Fay Shorter	ad.activedirectorypro.com/ADPRO Users/Accou...
Helen Bai	O Users/Accou...
Ima Kim	O Users/Accou...
James Art	O Users/Accou...
Jennie Morris	ad.activedirectorypro.com/ADPRO Users/Accou...

This is VERY BAD



Active Directory Best Practices

□ Understand Permission Inheritance

□ Change Default Setting

□ Use Remote Management Tools

□ Standardize Group Names

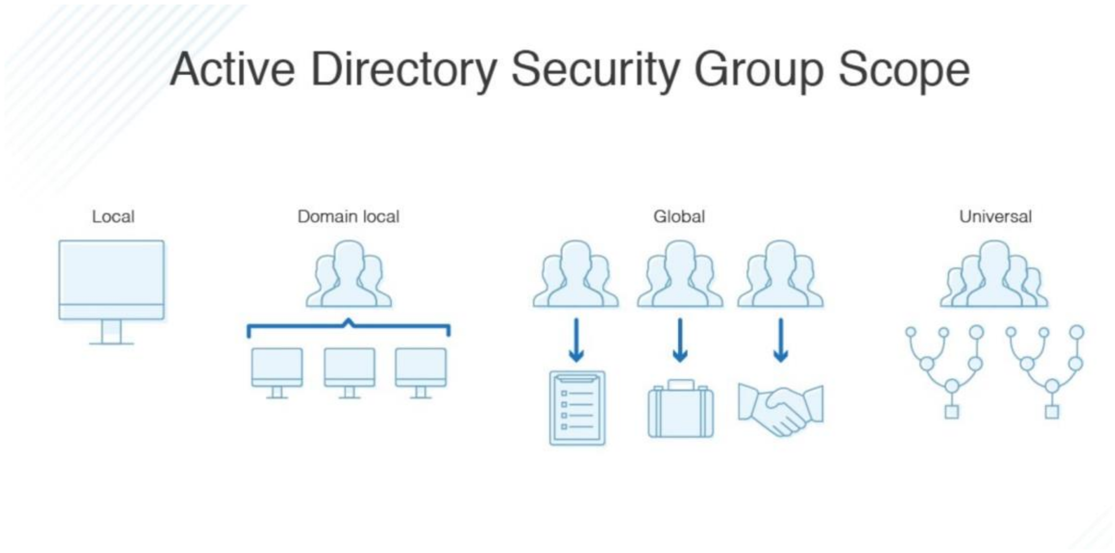
□ Clear Unnecessary Accounts

□ Use Monitoring Tools for Security

□ Keep Privileges at a Minimum

□ Implement Password Policies

□ Have a Disaster Recovery Plan



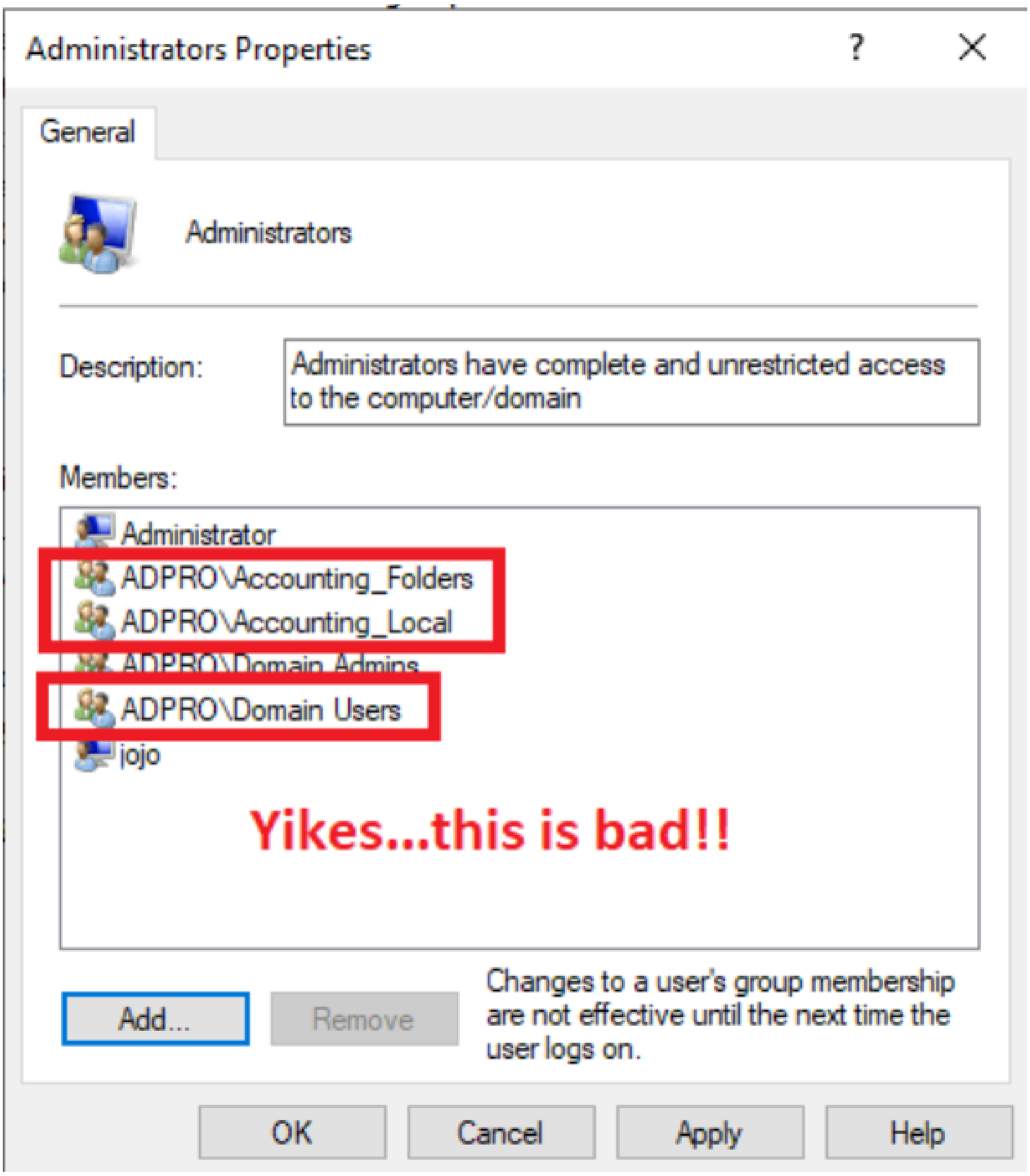
Active Directory Security Group Scope

Local

Domain local

Global

Universal



Administrators Properties

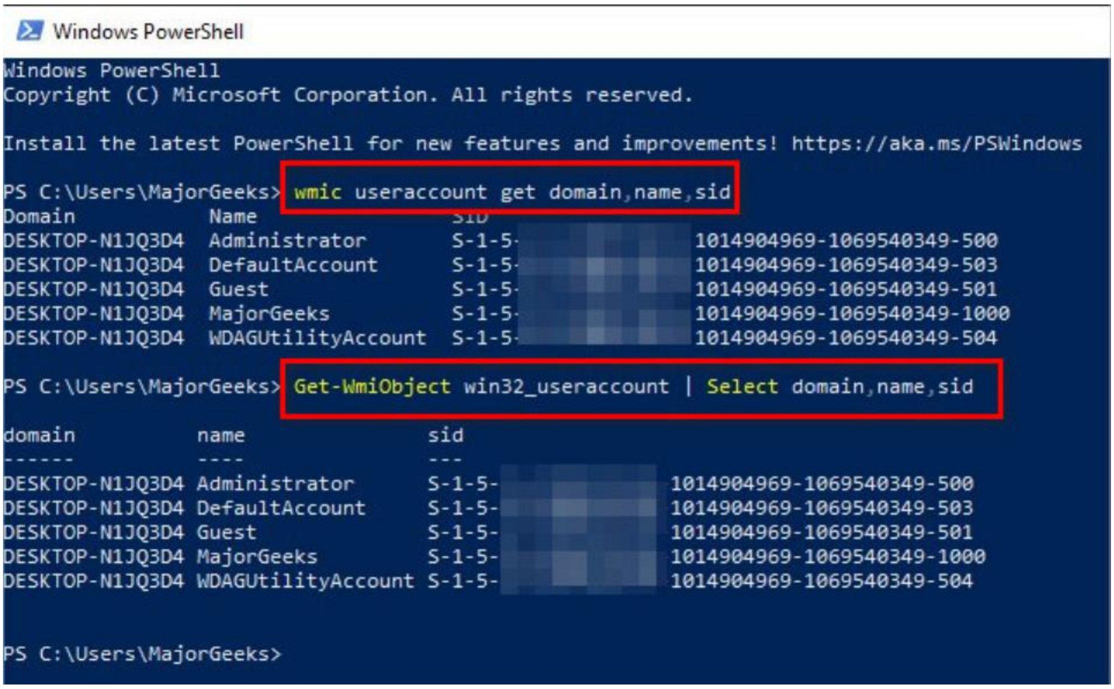
Description: Administrators have complete and unrestricted access to the computer/domain

Members:

- Administrator
- ADPRO\Accounting_Folders
- ADPRO\Accounting_Local
- ADPRO\Domain Admins
- ADPRO\Domain Users
- jojo

Yikes...this is bad!!

Changes to a user's group membership are not effective until the next time the user logs on.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\MajorGeeks> wmic useraccount get domain,name,sid
Domain           Name                 SID
DESKTOP-N1JQ3D4  Administrator        S-1-5-[redacted]1014904969-1069540349-500
DESKTOP-N1JQ3D4  DefaultAccount       S-1-5-[redacted]1014904969-1069540349-503
DESKTOP-N1JQ3D4  Guest                S-1-5-[redacted]1014904969-1069540349-501
DESKTOP-N1JQ3D4  MajorGeeks           S-1-5-[redacted]1014904969-1069540349-1000
DESKTOP-N1JQ3D4  WDAGUtilityAccount   S-1-5-[redacted]1014904969-1069540349-504

PS C:\Users\MajorGeeks> Get-WmiObject win32_useraccount | Select domain,name,sid

domain          name               sid
------          ----               ---
DESKTOP-N1JQ3D4 Administrator      S-1-5-[redacted]1014904969-1069540349-500
DESKTOP-N1JQ3D4 DefaultAccount     S-1-5-[redacted]1014904969-1069540349-503
DESKTOP-N1JQ3D4 Guest              S-1-5-[redacted]1014904969-1069540349-501
DESKTOP-N1JQ3D4 MajorGeeks         S-1-5-[redacted]1014904969-1069540349-1000
DESKTOP-N1JQ3D4 WDAGUtilityAccount S-1-5-[redacted]1014904969-1069540349-504


PS C:\Users\MajorGeeks>
```

CHAPTER 6

CONCLUSION

Implementing comprehensive security hardening techniques for Windows domains is essential for protecting enterprise IT infrastructures from an ever-evolving threat landscape. By following the curated list of recommendations outlined in this document, organizations can significantly enhance their security posture, mitigate attack vectors, and ensure robust protection against a wide range of cyber threats. The strategies proposed focus on key areas such as initial foothold prevention, reconnaissance disruption, lateral movement control, privilege escalation mitigation, and administrative credential protection. Continuous evaluation, adaptation, and refinement of these measures are crucial for maintaining a proactive and resilient security stance.

REFERENCES

1. https://github.com/PaulSec/awesome-windows-domain-hardening?tab=readme-ov-file
2. https://www.pingcastle.com/
3. Ilonen, Timo, Seppo Virtanen, and Jouni Isoaho. "Operating System Hardening Based on Privacy, Security and Performance: Customization of Microsoft Windows." (2024).
4. Dunkerley, Mark, and Matt Tumbarello. *Mastering Windows Security and Hardening: Secure and protect your Windows environment from intruders, malware attacks, and other cyber threats*. Packt Publishing Ltd, 2020.
5. Numminen, Aleksanteri. "Windows technical hardening against the most prevalent threats." (2023).