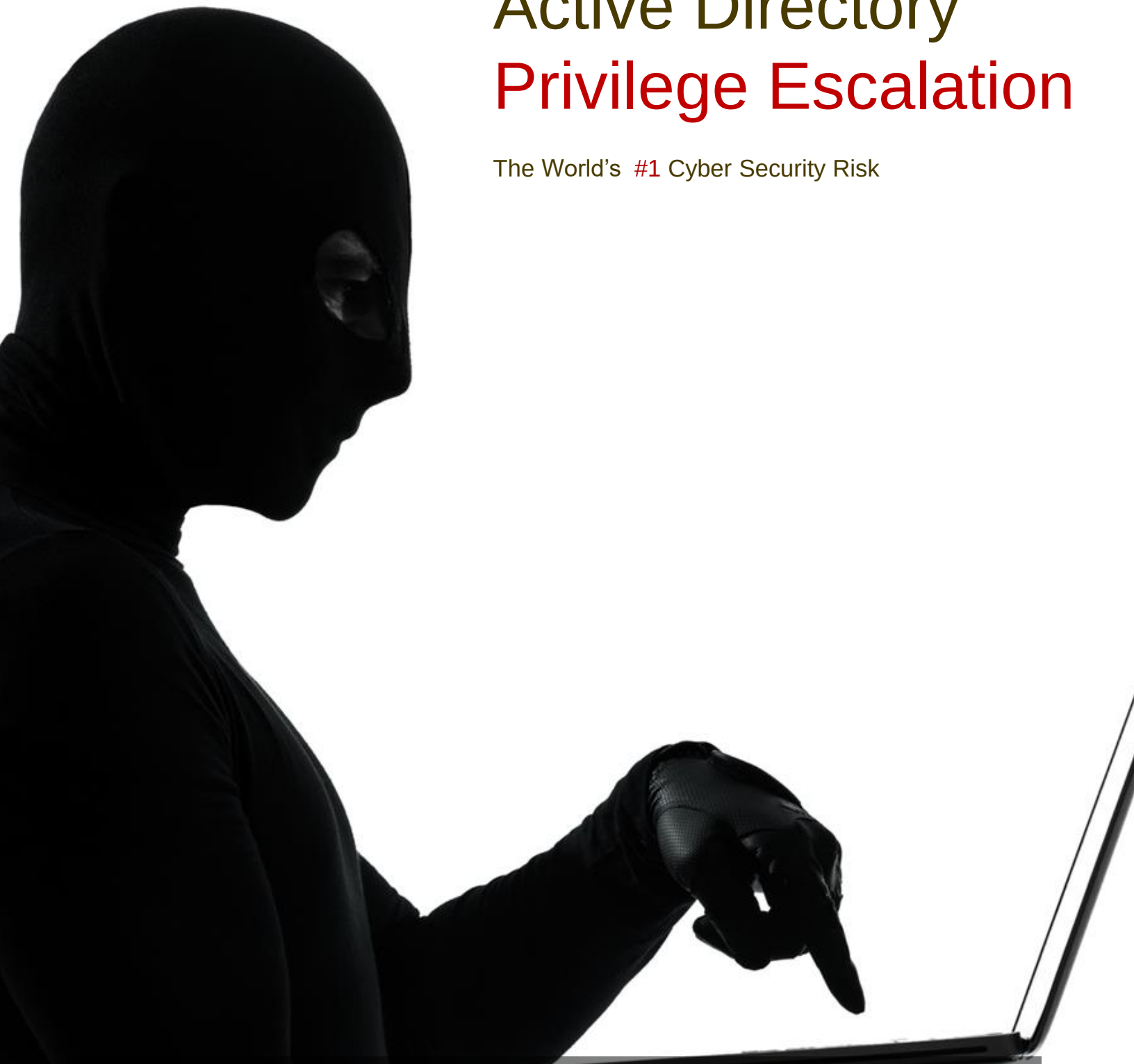
Active Directory Privilege Escalation

The World's #1 Cyber Security Risk



Contents

1. Executive Summary (Non-Technical Audience) 1
2. Executive Summary (Technical Audience) 2
3. Root Cause Example, Top-5 Attack Vectors, Multi-step Escalation ..... 3 – 5
4. Minutes to Compromise, Six Myths, 100% Mitigatable, Risk Mitigation ..... 6 – 9

Active Directory Privilege Escalation

Executive Summary

Microsoft Active Directory is the very foundation of cyber security and privileged access at 85% of organizations, and within Active Directory deployments lie thousands of privilege escalation paths.

Anyone who could identify these privilege escalation paths in Active Directory could easily compromise virtually any IT resource of choice, and in the worst case, the entire foundational Active Directory itself.

This is alarming considering that historically 100% of all major recent cyber security breaches involved the compromise and misuse of a single account that possessed privileged access in Active Directory.

In organizations that operate on the Microsoft Windows Server platform, the entirety of their building blocks of cyber security i.e. all organizational user accounts, computer accounts, and security groups that protect all organizational IT resources, are stored, managed and secured in Active Directory.

These building blocks are represented as Active Directory objects and protected by access control lists (ACLs) within which lie permissions that allow and deny access to a large number of users and groups.

In every Active Directory domain, within ACLs of thousands of Active Directory objects lie hundreds of thousands of permissions and it is their net cumulative resulting effect i.e. effective permissions that govern who has what privileged access on each one of these thousands of Active Directory objects.

Organizations thus require the ability to accurately calculate effective permissions in Active Directory; astonishingly the ability to accurately calculate effective permissions doesn't exist* in Active Directory.

Consequently, organizations have been provisioning access in proverbial dark for years now, and as a result, at organizations worldwide, today there exists an ocean of excessive privileged access within which lie thousands of privilege escalation paths leading to the compromise of all Active Directory content, and anyone who can accurately identify them could easily exploit them to inflict damage.

Active Directory Privilege Escalation

Technical Summary

Active Directory Privilege Escalation is an exploitation technique in which perpetrators identify and exploit unauthorized access in ACLs of Active Directory objects to compromise them and escalate privilege.

Active Directory Privilege Escalation lets perpetrators compromise domain user accounts, computer accounts, security groups and other Active Directory content, including privileged users and groups.

The compromise of a single Active Directory privileged user or group is sufficient to obtain complete command and control over the entire Active Directory, and is tantamount to complete compromise.

In organizations that operate on Microsoft's Windows Server platform, all organizational user accounts, computer accounts, and security groups are stored, managed and secured in their Active Directory.

These building blocks are represented as Active Directory objects and are protected by access control lists within which exist permissions that allow and deny access to a large number of users and groups.

The permissions specified in the ACLs of Active Directory objects determine the effective permissions provisioned on these objects, which in turn govern who can enact various administrative tasks such as resetting passwords and changing group memberships, modifying access etc. on these objects.

Anyone who could enact such tasks on Active Directory objects could gain control over them, in effect escalating privilege, so privilege escalation involves finding and exploiting unauthorized access to do so.

For example, if the effective permissions on the *Domain Admins* security group allow a perpetrator the ability to change its membership, he/she could easily add his/her/any domain user account to the group's membership, and in doing so would have easily escalated privilege to a domain admin.

Active Directory Privilege Escalation

Root Cause Example

Active Directory Privilege Escalation is made possible by the existence of unidentified/unauthorized effective permissions resulting from the security permissions provisioned on Active Directory objects.

Specifically, in the ACL of every Active Directory object reside numerous security permissions, and it is their net resulting effect i.e. effective permissions that determine who actually has what access.

The accurate calculation of Active Directory Effective Permissions is very difficult, and because most organizations do not have accurate effective permissions insight, access changes made over years have resulted in a substantial amount of unidentified/unauthorized access, paving privilege escalation paths.

As an example, assume that the ACL protecting the CEO's domain user account contains one hundred permissions, fifty explicit and fifty inherited, eighty of which allow and twenty deny access, each one specifying various permissions to various users and groups, many of which contain nested groups.

The actual resulting access allowed on the CEO's domain user account will depend on the outcome of the cumulative impact of each one of these one hundred permissions, i.e. on effective permissions.

Based on resulting effective permissions, it so happened that a single permission granted to a single incorrectly nested group resulted in a team of fifty contractors accidentally ending up getting sufficient effective permissions to reset the CEO's password, even though they're not supposed to be able to do so.

This one little technicality ended up creating fifty privilege escalation paths to the CEO's account. In this manner, over time, in every Active Directory, thousands of privilege escalation paths have been created.

Unfortunately, this organization may never discover them as it doesn't have the ability to accurately calculate effective permissions, but any perpetrator who has the ability, could find and exploit them.

Active Directory Privilege Escalation

Top-5 Attack Vectors

Active Directory Privilege Escalation is a very powerful and effective exploitation technique because it can be used to very quickly compromise and gain escalated privileges on any Active Directory object.

Specifically, if a perpetrator has sufficient effective permissions to be able to enact certain administrative tasks on an Active Directory object, all he/she would need to do to escalate privilege is enact the task.

Active Directory Privilege Escalation can be used to target and compromise any domain user account, domain computer account, domain security group, organizational unit, service connection point etc.

The following are the Top-5 most prevalent ways to escalate privilege in Active Directory –

1. Reset a domain user account's password – Resetting a domain user account's password would let the perpetrator instantly take over the account by logging-in using the newly set password.
2. Change a domain security group's membership – Changing a domain security group's membership would let the perpetrator instantly add his/her/any controlled account as a member of the group.
3. Modify the permissions/ACL protecting an object – Modifying the permissions protecting an Active Directory object would let the perpetrator gain complete administrative control over the object.
4. Taking ownership of an object – Taking ownership of an Active Directory object would grant the perpetrator the implicit ability to modify permissions on the object, and gain control over it.
5. Link a malicious GPO to an OU – Linking a single malicious GPO to an OU would ultimately let the perpetrator gain administrative over all computers whose computer accounts reside in that OU.

Smartcard authentication can also be defeated by simply disabling their use on domain user accounts.

Active Directory Privilege Escalation

Multi-step Privilege Escalation Example

Active Directory Privilege Escalation often involves successively escalating privilege multiple times over, gaining additional privileges during each step, to ultimately gain the desired level of privilege.

For instance, a perpetrator could identify and exploit a three-step privilege escalation path starting from a regular domain user account and ultimately leading to domain-admin equivalent access.

Skilled perpetrators often employ multi-step Active Directory Privilege Escalation to gain root access.

Consider that a perpetrator who possesses sufficient skill or tooling to accurately determine effective permissions in Active Directory is able to identify the following three privilege escalation paths –

1. John Doe can change the *Domain Admins* Group Membership – Perpetrator calculates effective permissions on the *Domain Admins* group to uncover that *John Doe* can change its membership.
2. Jane Doe can modify permissions on John Doe's account – Next, perpetrator calculates effective permissions on *John Doe's* account to uncover that *Jane Doe* can modify access on his account.
3. Jim Doe can reset Jane Doe's password – Finally, the perpetrator calculates effective permissions on Jane Doe's account to uncover that *Jim Doe* can reset Jane Doe's domain account's password.

By simply utilizing default read access granted to *Authenticated Users*, and the ability to accurately determine effective permissions on Active Directory objects, the perpetrator has found an easily exploitable three-step privilege escalation path, starting from a minimally protected domain user account leading to the all-powerful *Domain Admins* security group, all achievable within seconds.

In essence, the perpetrator uncovered a multi-step privilege escalation path wherein if he/she could compromise *Jim Doe*'s account, he/she would be literally one password reset, one ACL change and one security group membership change away from gaining all-powerful *Domain Admin* access.

Active Directory Privilege Escalation

Minutes to Compromise

Today, in the ocean of privileged access in Active Directory lie thousands of privilege escalation paths that can be exploited to compromise the vast majority of organizational IT resources within minutes.

Specifically, in virtually every Active Directory deployment today, there exist thousands of privilege escalation paths leading to every single object in Active Directory, including to all their privileged accounts and groups, executive accounts, large OUs, high-value computer accounts, groups etc.

In fact, a single change i.e. just ONE change in one permission in the ACL of one Active Directory object could result in everyone having complete command and control over the entire organization –

1. Just one change to one ACL could be used to compromise all accounts in Active Directory
2. Just one GPO linked to one OU could be used to compromise thousands of computers
3. Just one change to one security group could grant access to all organizational IT resources
4. Just one change to one service connection point (e.g. *AD Azure Connect*) could wreak havoc
5. Just one change in Active Directory could instantly result in a massive cyber security breach

Incidentally, today literally anyone with a domain user account and sufficient expertise/tooling could query their Active Directory and easily find thousands of easily exploitable privilege escalation paths.

Yet, not a single organization in the world knows exactly who can make such changes in their Active Directory, and no one, not their CISOs, not their Auditors, not even their Domain Admins, have a clue.

Active Directory Privilege Escalation

Six Dangerous Myths

Today, most organizations are operating on a dangerously false sense of security, based on the belief that recent cyber security and privileged access management (PAM) solutions can mitigate this risk.

Today every organization, its CISO and Domain Admins must be aware of the following six myths –

1. We analyze Active Directory Permissions – What controls and determines privileged access in Active Directory is not "*who has what permissions*" but "*who has what effective permissions.*"

2. We use Active Directory Auditing – Auditing is merely a reactive measure informing you that a perpetrator has (already) engaged in an action that has (already) compromised your security.

3. We use a Privileged Session Manager – Privileged Session Managers only monitor privileged users' activities. This specific risk can be enacted by anyone who has a domain user account.

4. We use an Enterprise Password Vault/Manager – A mere password reset performed directly on a domain user account in Active Directory can circumvent any password vault/manager.

5. We use Multi-Factor Authentication (MFA) – MFA on domain user accounts can be turned off at a button's click by making a single change directly on the user account in Active Directory.

6. We use Advanced Threat Analytics and/or Threat Intelligence – Both can be easily subverted as recon can be easily disguised and spread over time, and the actual attack takes seconds.

Active Directory Privilege Escalation

100% Mitigatable

The risk posed by Active Directory Privilege Escalation is 100% mitigatable, as doing so only requires the desire and ability to accurately identify, lockdown and maintain least privileged access in Active Directory.

The keys to all privileged access in Active Directory, i.e. the keys to accurately identifying, locking down and maintaining least privileged access in Active Directory lie in Active Directory Effective Permissions.

Active Directory Effective Permissions control all privileged access provisioned in Active Directory.

They control exactly who can–

1. Create, delete and manage all privileged, executive and in fact all user accounts and groups
2. Change the membership of all domain security groups that ultimately protect all IT resources
3. Join computers as well as link GPOs to OUs to ultimately control all domain-joined computers

Unfortunately, for years now, most organizations have incorrectly believed that to assess privileged access in Active Directory, all they need to audit is "*who has what permissions in Active Directory*" when in fact, nothing could be further from the truth, for there's only one correct way to assess privileged access in Active Directory and that's to audit "*who has what effective permissions.*"

In fact, Active Directory Effective Permissions are so important that of the three tabs in Microsoft's native tooling, one is for Effective Permissions. Sadly, that tab remains inaccurate and inadequate.

Today, all CISOs, Auditors and Domain Admins must know what Active Directory Effective Permissions are because without them not a single object in Active Directory can be secured, and it is in effective permissions that lie the keys to correctly and completely mitigating this cyber security risk.

Active Directory Privilege Escalation

Risk Mitigation

This cyber security risk can be reliably mitigated, and all organizations that value foundational cyber security must take this risk seriously and consider making its mitigation a top corporate priority.

Organizations can mitigate this risk by enacting five simple steps –

1. **A**wareness – From the CEO to the Domain Admins, all stakeholders must gain an understanding of why and how this organizational risk impacts the cyber security of the entire organization.
2. **E**xpertise – Organizations must begin by ensuring that their IT personnel have the expertise required to understand and use essential concepts like Active Directory Effective Permissions.
3. **C**apability – Organizations must ensure that they possess/acquire the essential capability needed to accurately and trustworthily calculate effective permissions in Active Directory.
4. **E**mpowerment – IT Teams should be tasked with the objective of assessing and mitigating this risk and ideally simultaneously attaining and maintaining Least Privileged Access (LPA) in Active Directory, and they should be provided the resources required to accomplish their objectives.
5. **A**ccountability – From the CEO to the CISO to the IT Manager to the Domain Admins/IT Teams who manage privileged access in Active Directory, an accountability chain must be established.

From a technical standpoint, mitigating this security risk involves learning how to correctly assess and lockdown privileged access (effective permissions) in Active Directory, and then implementing a high-priority IT project aimed at attaining and maintaining LPA in the organization's Active Directory.

In summary, organizations that possess the desire, expertise and capability required to accurately assess and lockdown privileged access in their Active Directory can easily mitigate this risk today.

Active Directory Effective Permissions

Paramount to Organizational Cyber Security

In every Windows Server based IT infrastructure worldwide, the vast majority of all privileged access as well as the most powerful Domain Admin equivalent privileged access resides in Active Directory.

The keys to all privileged access i.e. the keys to accurately identifying, locking-down and maintaining all privileged access in Active Directory lie in accurately determining Active Directory effective permissions.

Consequently, from the CEO's account to the Domain Admins group, not a single Active Directory object can be secured without being able to accurately determine Active Directory effective permissions.

Does your organization know about and possess the world's most important cyber security capability?

www.paramountdefenses.com/insights/active-directory-effective-permissions

The End.

About the Author

This document is authored by Sanjay Tandon, CEO of Paramount Defenses, and formerly Program Manager for Active Directory Security at Microsoft Corporation.

Microsoft Active Directory is the foundation of cyber security and privileged access at 85% of all organizations worldwide, including 90% of the Fortune 100, and the entire U.S. Government.

Prior to establishing Paramount Defenses, Mr. Tandon was Program Manager for Active Directory Security on the Windows Server Development Team at Microsoft Corporation.

As Microsoft's top subject matter expert on Active Directory Security, he was responsible for all aspects of AD security, including designing features, presenting at conferences, and providing SME guidance to Microsoft Consulting Services and its customers. He also authored Microsoft's 400-page whitepaper titled *Best Practices for Delegating Administrative Authority (Privileged Access) in Active Directory*.

He is the architect of the unique Microsoft-endorsed *Gold Finger* and *Gold Finger Mini*, the world's only accurate privileged access assessment tools for Active Directory, which are used worldwide.

With over two decades of subject matter expertise and experience, he is widely regarded as the world's top subject matter expert in Active Directory Security and Privileged Access in Active Directory.

He also holds the patent that governs the determination of effective access in systems, which today is cited by patents from top cyber security companies including CyberArk, FireEye, Palantir and Microsoft.

He occasionally blogs at – www.cyber-security-blog.com and www.active-directory-security.com.

About Paramount Defenses

Paramount Defenses is the world's only cyber security company that possesses the paramount capability to be able to accurately assess privileged access in Active Directory deployments.

Microsoft Active Directory Domain Services are the foundation of cyber security and the heart of privileged access at 85% of all business and government organizations worldwide.

Paramount Defenses was founded by and is led by former Microsoft Program Manager for Active Directory Security. The company's unique, innovative, patented technology governs the accurate assessment of all access, including privileged access, in IT environments worldwide.

Its unrivaled solutions can accomplish the remarkable feat of being able to automatically and accurately assess privileged access across entire Active Directory domains, at a button's touch.

From the United States of America to Australia, its global customer base spans six continents and includes numerous prominent business and government organizations across the world.

www.paramountdefenses.com


PD