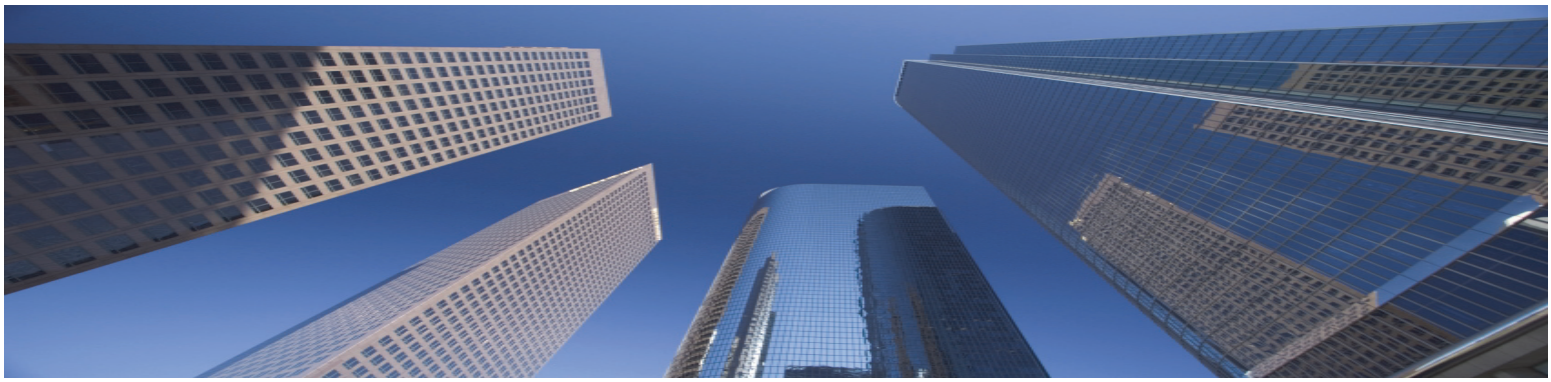
Active Directory Privilege Escalation

The #1 Cyber Security Risk to Organizational Security

In organizations that operate on Microsoft's Windows Server platform, the number **#1** cyber security risk to organizational security is privilege escalation based on the identification and exploitation of unauthorized access grants provisioned in Active Directory.



Introduction

Every IT infrastructure, irrespective of size, is comprised of 4 elemental components – organizational users, the devices they use to engage in computing, the data they create, share, access and act upon, and IT admins that help manage and secure it all.

Users

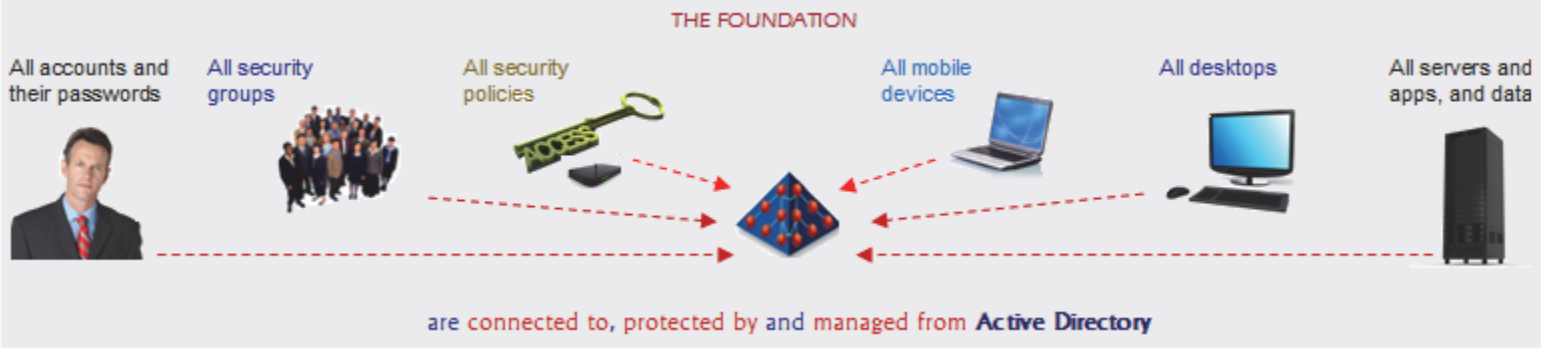
Devices

Data

Admins

The adequate protection of each of these 4 elemental components from unauthorized access is thus essential to cyber security.

In organizations that operate on Microsoft's Windows Server platform, each of these 4 elemental components i.e. all organizational user accounts, devices, data and admin accounts are stored in or connected to, protected by, and managed from Active Directory.



Should an organization's Active Directory deployment be compromised, all organizational IT assets could be at risk of compromise.

The #1 security risk to Active Directory is thus the #1 cyber security risk to organizational security, and that risk is Active Directory Privilege Escalation based on the identification and exploitation of unauthorized access grants provisioned in Active Directory

Executive Summary

Cyber security is about the protection of organizational IT assets from loss of confidentiality, integrity and/or availability. It is made possible by the facilitation of secure (authenticated and authorized) access to all IT assets based on the principle of least-privilege.

Did you know that in Microsoft's Windows Server based IT infrastructures, Active Directory is the bedrock of cyber security because it facilitates secure (authenticated and authorized) access to all organizational IT assets (e.g. data, files, computers, servers etc.) **?**

As the foundation of the Kerberos protocol in a Microsoft Windows Server based IT infrastructure, Active Directory facilitates secure (authenticated and authorized) access to all IT resources, and stores and protects the building blocks of organizational security –

1. All user accounts used to uniquely identify and authenticate users, as well as their credentials (e.g. passwords)
2. All computer accounts used by the organization (e.g. laptops, desktops, file, database, web and application servers)
3. All security groups used to provision and control access to the entirety of the organization's IT assets

In fact, each time an organizational user logs on, accesses data stored on a device or on a server, collaborates via email, or uses a line-of-business application, under the hood, all secure (authenticated and authorized) access is made possible by Active Directory.

Given Active Directory's foundational role in organizational security, ensuring its security, and that of its content, is of paramount importance because should a building block stored in it be compromised, all IT assets protected by that block could be at risk, and should the Active Directory itself be compromised, literally all organizational IT assets could instantly be at risk of compromise.

The security of the Active Directory itself, and that of its content, depends on the security afforded to all Domain Controllers (DC) and the effective access provisioned on all vital Active Directory content, such as all administrative and delegated administrative accounts and security groups stored in Active Directory, as well as configuration data on which the Active Directory relies.

There are numerous avenues that malicious entities could potentially use to compromise Active Directory and its content, such as the compromise of a single DC, administrative or delegated administrative account or security group stored in Active Directory.

However, the easiest avenue to compromising the Active Directory and its content is via a privilege escalation based attack that involves the identification and exploitation of unauthorized access grants in Active Directory to initially or eventually gain control of an administrative account or group in Active Directory, then use that to gain access to any organizational IT asset(s) of choice.

Details

The details of **Active Directory Privilege Escalation** are best understood via the following 8 questions and answers -

Q1. What is the easiest way for a malicious entity to compromise an IT resource (e.g. a file, a server, a user account, an OU etc.)?

Find out which domain user accounts or security groups are delegated or provisioned the required effective access on that IT resource, then compromise the identity of any one of these user accounts or groups to obtain access to that IT resource.

Q2. What then is the easiest way to compromise the identity of a domain user account or a domain security group?

The easiest way to compromise the identity of a domain user account is to reset the account's password. The easiest way to compromise a domain security group is to find out who (i.e. which delegated admins) can effectively modify its membership, then reset the password of any of those delegated admins, login as them and add one's account to the group's membership.

Q3. How might someone use domain account password resets to perform single/multi-step Active Directory privilege escalations?

Find out who (i.e. which delegated admins) can reset the target domain user account's password, then reset the password of any one of those delegated admin accounts, login as them and reset the target account's password. This process can be iterated to identify and exploit multi-step privilege escalation paths, wherein the final target is the user account of ultimate interest, and the initial target is an easily compromisable user account, or a computer onto which that user logs on.

Q4. What makes this risk possible in Active Directory deployments?

In every Active Directory deployment, there are thousands of security permissions that collectively control the effective access protecting all objects stored in Active Directory. Given the sophistication of the underlying access model, and the large number of permissions, it is very difficult to accurately provision effective access on Active Directory objects based on principle of least privilege. As result, in most Active Directory deployments, today, there exist large numbers of unauthorized access grants.

Q5. What makes this the #1 cyber security risk to Active Directory deployments?

This risk makes it easy for anyone with a domain account to potentially compromise any IT resource stored in *or protected by* Active Directory, simply by identifying vulnerabilities (i.e. unauthorized access grants / security permissions) in access control lists (ACLs) protecting Active Directory objects, then exploiting them by performing simple tasks (e.g. password resets) using existing tools to first compromise identities, then IT assets. Unlike other risks, it has no special tool or logon requirements.

Q6. Does the use of 2-factor authentication, 3rd party roles-based administration or Active Directory auditing **not** mitigate this risk?

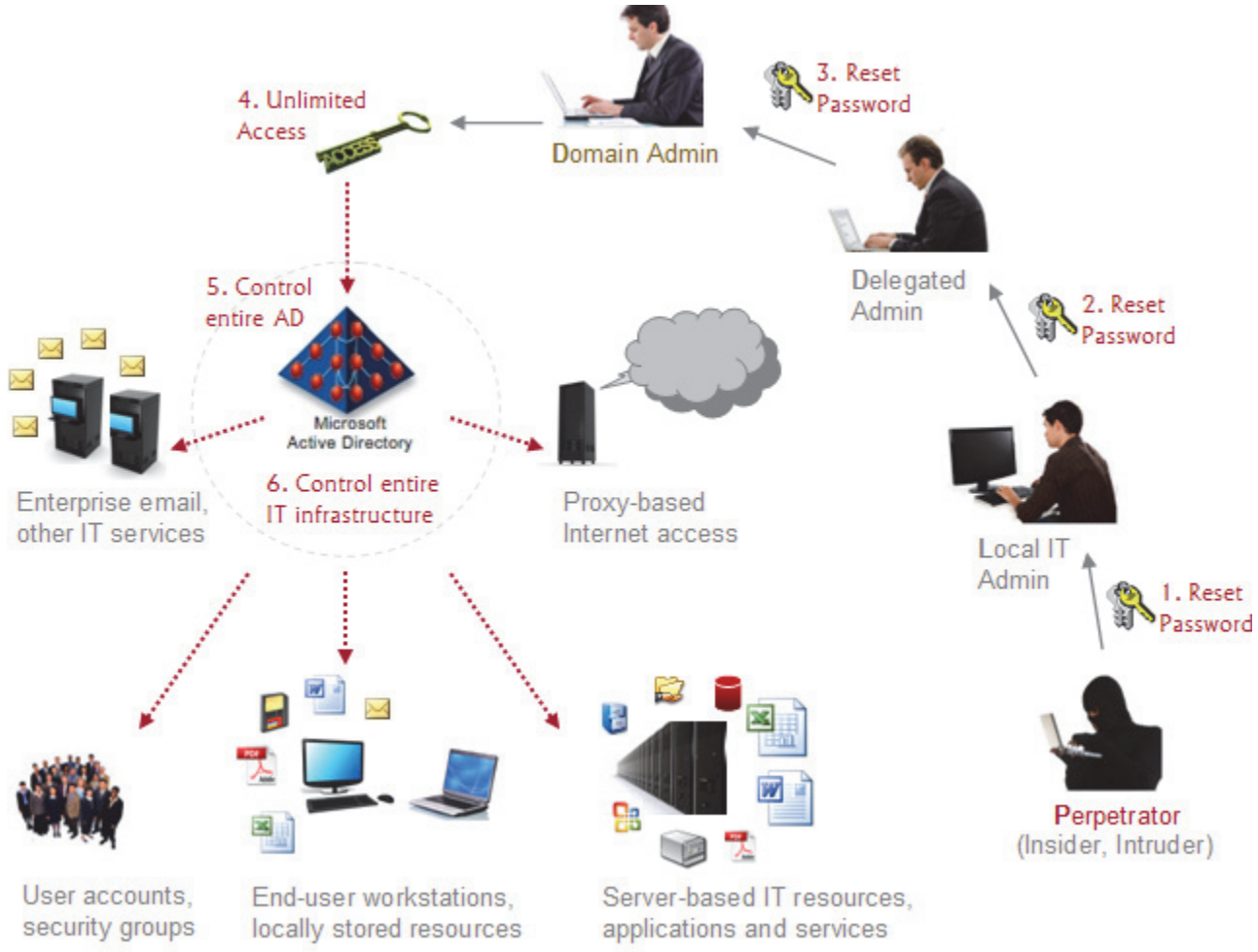
No. This risk still exists, even with either or all of these measures / solutions in place, because of the following reasons –

- Most 2-factor authentication mechanisms are tied to Active Directory and in most cases, can be disabled by modifying an attribute on the user account in Active Directory. Once disabled, authentication will default to being password based.

- Even with a 3rd party roles-based administrative delegation solution in place, the need to provision and manage access directly on objects in Active Directory remains, because many IT services and applications rely on the ability to directly access and/or modify Active Directory content. The provisioning and management of direct access to Active Directory content is outside the scope of any protection afforded by a 3rd party roles-based administrative delegation solution.

- An auditing solution does nothing to mitigate this risk, because it only helps obtain a record of an action that was carried out by someone. It does not provide any insight into who has the ability (i.e. *effective permissions*) to carry out an action. Thus, at best, an auditing solution could help find out who may have escalated their privilege, but by that time, the damage would already have been done. It cannot help find out who can currently escalate their privilege.

Q7. What makes privilege escalation in Active Directory possible, how vast is the attack surface, and how to mitigate this risk?



In every Active Directory domain there are thousands of security permissions that collectively control who has what access.

For example, the security permissions that protect a Domain Admin's user account control who can reset his/her password.

Active Directory lets IT admins precisely provision/delegate access but it lacks the means to help them precisely assess, verify or audit effective provisioned/delegated access. As a result, over time, driven by business needs, the effective state of access in Active Directory changes, and once the state changes, no one really knows who is really provisioned what effective access.

Consequently, this results in a situation wherein over time, unauthorized access grants become pervasive in Active Directory, and the presence of these unauthorized access grants lets anyone who can find them, exploit them to elevate their privilege.

The attack surface is vast because everyone with a domain account already has read access to Active Directory content, and with the right tools (e.g. any *Active Directory Permissions Analysis Tool* or *Active Directory Password Reset Analysis Tool*), anyone can attempt to determine *effective permissions* in an organization's Active Directory and find out exactly who can reset whose passwords, then as illustrated above, identify and exploit privilege escalation paths to instantly compromise delegated/ domain admin accounts. Once identified, it only takes minutes to exploit these paths and perform single/multi-step escalations.

This risk can be mitigated. However, Active Directory auditing solutions cannot mitigate this risk because they cannot identify these escalation paths. To mitigate this risk, IT personnel need to identify and eliminate the underlying unauthorized access grants in Active Directory that pave these escalation paths. This requires the accurate determination of effective access in Active Directory, which can be done manually or with the help of any automated *Active Directory Effective Access Audit Tool*.

One path is all a malicious individual, usually an insider, needs, to gain administrative access, and take over Active Directory.

Q8. Can the existence of this risk in an organization's Active Directory, particularly to admin or executive accounts, be proved?

Yes. This free tool can show how many users can reset anyone's password - www.paramountdefenses.com/goldfinger-mini