Active Directory

More like Access Directory

Fun fact: Apple’s GarageBand has had 6 CVE’s averaging 5.1 CVSS Score, reported over the last 13 years.

https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-17800/Apple-Garageband.html

First que es Active Directory?

A directory is a hierarchical structure that stores information about objects on the network. A directory service, such as Active Directory Domain Services (AD DS), provides the methods for storing directory data and making this data available to network users and administrators. For example, AD DS stores information about user accounts, such as names, passwords, phone numbers, and so on, and enables other authorized users on the same network to access this information.

Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information.

Let’s skip to the good stuff

Securing Active Directory

- Avenues to Compromise
- Reducing the Active Directory Attack Surface
- Monitoring Active Directory for Signs of Compromise
- Planning for Compromise

Avenues of Compromise

Initial breach targets

- Gaps in antivirus and antimalware deployments
- Incomplete patching
- Outdated applications and operating systems
- Misconfiguration
- Lack of secure application development practices

Activities that Increase the Likelihood of Compromise

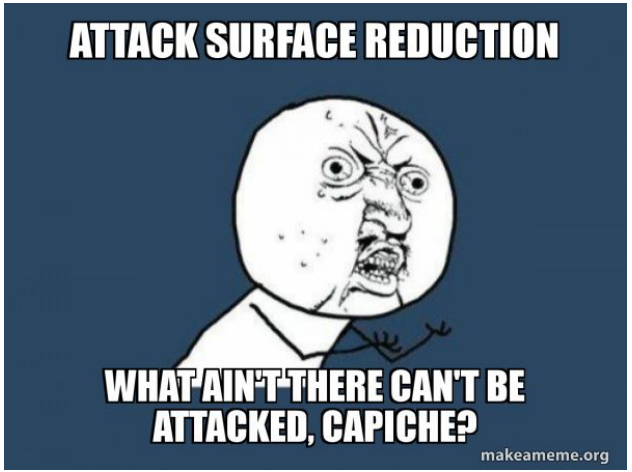
- Browsing the Internet with a highly privileged account
- Configuring local privileged accounts with the same credentials across systems
- Overpopulation and overuse of privileged domain groups
- Insufficient management of the security of domain controllers.
- Logging on to unsecured computers with privileged accounts

Attractive Accounts for Credential Theft

- VIP accounts
- "Privilege-Attached" Active Directory accounts
- Domain controllers
- Perrmanently privileged accounts

Reducing Attack Surface

- Apply Principle of Least Privilege
- Physical Security
- Secure Configuration of Domain Controller
- Segmentation by Permissions, Roles and Groups



Monitoring For Compromise

- Windows Audit Policy - Windows security event logs have categories and subcategories that determine which security events are tracked and recorded.
- Our solution: Windows events are piped to Adlumin.

Best Practices

Best Practice	Tactical or Strategic	Preventative or Detective
Patch applications.	Tactical	Preventative
Patch operating systems.	Tactical	Preventative
Deploy and promptly update antivirus and antimalware software across all systems and monitor for attempts to remove or disable it.	Tactical	Both
Monitor sensitive Active Directory objects for modification attempts and Windows for events that may indicate attempted compromise.	Tactical	Detective
Protect and monitor accounts for users who have access to sensitive data	Tactical	Both
Prevent powerful accounts from being used on unauthorized systems.	Tactical	Preventative
Eliminate permanent membership in highly privileged groups.	Tactical	Preventative
Implement controls to grant temporary membership in privileged groups when needed.	Tactical	Preventative
Implement secure administrative hosts.	Tactical	Preventative
Use application allowslists on domain controllers, administrative hosts, and other sensitive systems.	Tactical	Preventative

Identify critical assets, and prioritize their security and monitoring.	Tactical	Both
Implement least-privilege, role-based access controls for administration of the directory, its supporting infrastructure, and domain-joined systems.	Strategic	Preventative
Isolate legacy systems and applications.	Tactical	Preventative
Decommission legacy systems and applications.	Strategic	Preventative
Implement secure development lifecycle programs for custom applications.	Strategic	Preventative
Implement configuration management, review compliance regularly, and evaluate settings with each new hardware or software version.	Strategic	Preventative
Migrate critical assets to pristine forests with stringent security and monitoring requirements.	Strategic	Both
Simplify security for end users.	Strategic	Preventative
Use host-based firewalls to control and secure communications.	Tactical	Preventative

Use host-based firewalls to control and secure communications.	Tactical	Preventative
Patch devices.	Tactical	Preventative
Implement business-centric lifecycle management for IT assets.	Strategic	N/A
Create or update incident recovery plans.	Strategic	N/A

Stuff We’re Gonna do more of:

Windows Defender on individual computers! Through Group policies. Get rekt everyone else!

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

Sauces

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

https://www.lepide.com/blog/how-to-ensure-your-active-directory-is-secure/

https://blog.netwrix.com/2017/04/20/tutorial-learn-the-basics-of-active-directory/

https://www.windows-active-directory.com/active-directory-ad-fundamentals.html