Active Directory Hardening

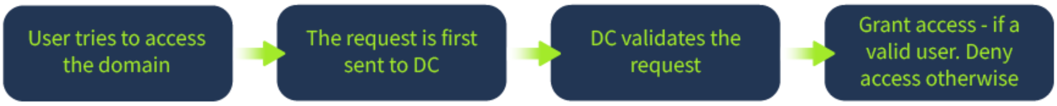
Assignee	J Jude Ghang
Status	Done
Priority	High
Tags	Cybersecurity

Domain

- The domain acts as a core unit regarding the logical structure of the Active Directory. It initially stores all the critical information about the objects that belong to the domain only.

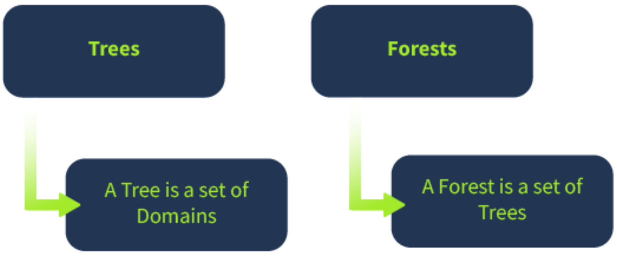
Domain Controller

- A Domain Controller is an Active Directory server that acts as the brain for a Windows server domain; it supervises the entire network. Within the domain, it acts as a gatekeeper for users' authentication and IT resources authorization.


User tries to access the domain → The request is first sent to DC → DC validates the request → Grant access - if a valid user. Deny access otherwise

Trees and Forests

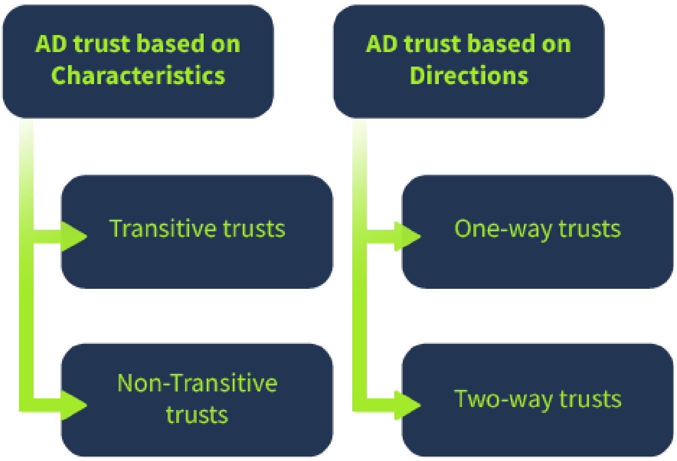
- Trees and Forests are the two most critical concepts of the Active Directory.



  - **Trees** are responsible for sharing resources between the domains. The communication between the domains inside a tree is possible by either one-way or two-way trust. When a domain is added to the Tree, it becomes the Offspring domain of that particular domain to which it is added – now a Parent domain.
  - **Forest** When the sharing of the standard global catalogue, directory schema, logical structure, and directory configuration between the collections of trees is made successfully, it is called a Forest. Communication between two forests becomes possible once a forest level trust is created.

Trust in Active Directory

AD trust is the established communication bridge between the domains in Active Directory. When we say one domain trusts another in the AD network, it means its resources can be shared with another domain. However, one domain's resources are not directly available to every other domain, as it is not safe. Thus, the resource sharing availability is governed by Trusts in AD. The AD trusts are of two categories, which are classified based on their characteristics or the current direction.



LAN Manager Hash

The user account password for Windows isn't stored in clear text; instead, it stores passwords with two types of hash representation. When the password for any user account is changed or set with fewer than 15 characters, both LM hash (LAN Manager hash) and NT hash (Windows NT hash) are generated by Windows and can be stored in AD. The LM hash is relatively weaker than the NT and is prone to a fast brute-force attack. The best recommendation is to prevent Windows from storing the password's LM hash. You can access it through the following:

`Group Policy Management Editor > Computer Configuration >Policies > Windows Settings > Security Settings > Local Policies > Security Options > double click Network security - Do not store LM hash value on next password change policy > select "Define policy setting"`

SMB Signing

SMB stands for Server Message Block. Generally, Microsoft-based networks utilize this protocol for file and print communication. Moreover, it allows secure transmission over the network. Configuring SMB signing through group policy is crucial to detect Man in the Middle (MiTM) attacks that may result in modification of SMB traffic in transit. SMB signing ensures the integrity of data for both client and server. All supported Windows versions have an SMB packet signing option.

`Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > double click Microsoft network server: Digitally sign communication (always) > select Enable Digitally Sign Communications`

LDAP Signing

Light Weight Directory Access Protocol (LDAP) enables locating and authenticating resources on the network. Hackers may introduce replay or MiTM attacks to launch custom LDAP requests. Therefore, LDAP signing is a Simple Authentication and Security Layer (SASL) property that only
accepts signed LDAP requests and ignores other requests (plain-text or non-SSL). We can enable LDAP signing through the following:

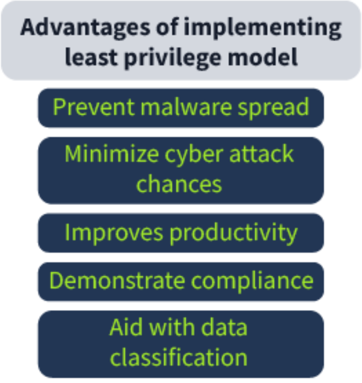
`Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies >`

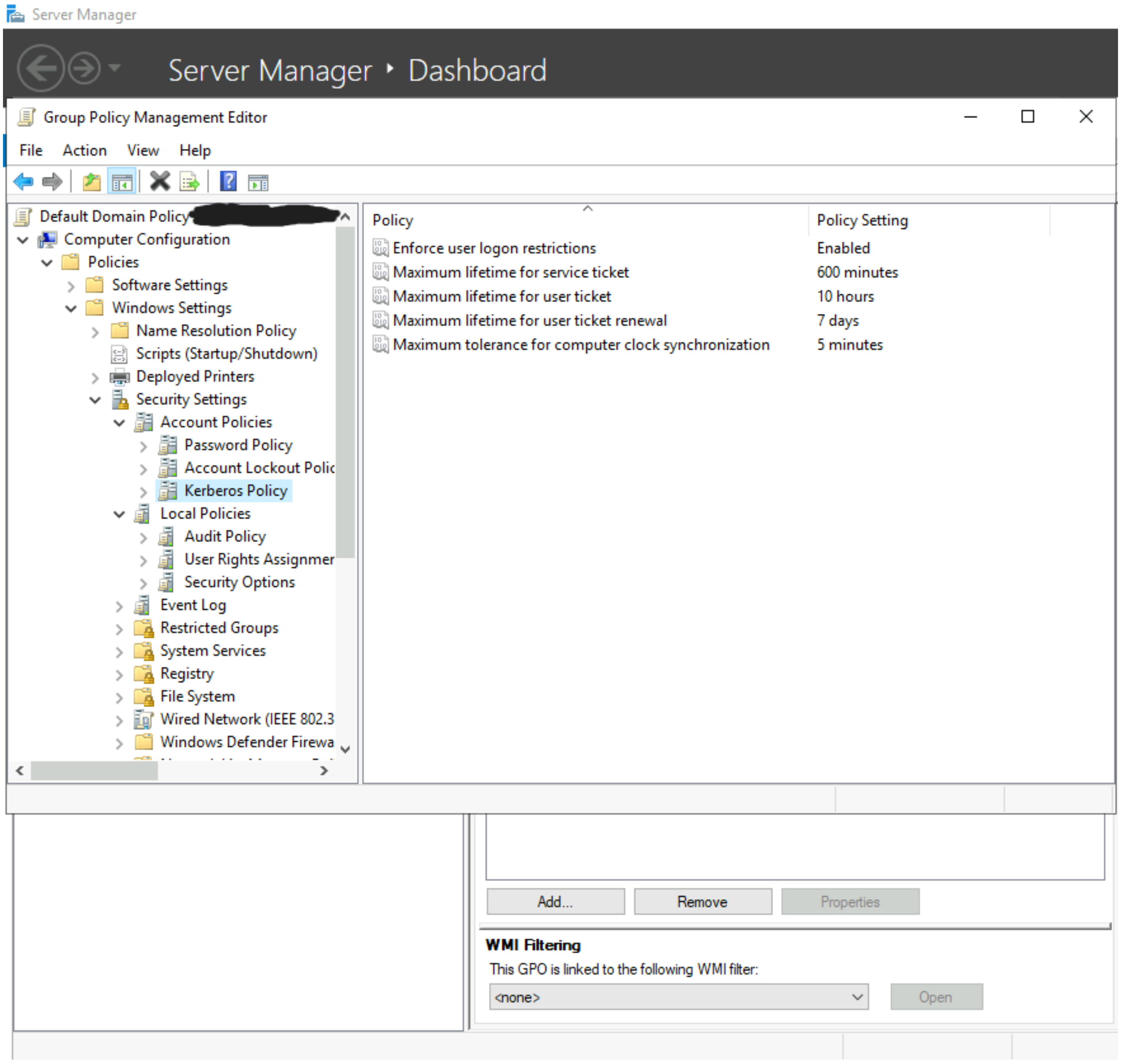
`Security Options > Domain controller: LDAP server signing requirements > select Require signing from the dropdown`

```
# Disable storing LM hash value on next password change
$lmHashPolicy = Get-WmiObject -Query "SELECT * FROM Win32_OperatingSystem" | ForEach-Object { $_.Version -eq '10.0.14393' }
if ($lmHashPolicy) {
    $lmHashPolicySetting = Get-WmiObject -Namespace root\cimv2 -Class Win32_AccountPolicy -Filter "Name='NewPassword'"
    $lmHashPolicySetting.SetPasswordHistory(0)
}

# Prompt user to press Enter before continuing
Read-Host "Press Enter to continue..."

# Enable SMB packet signing
$registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
$registryName = "RequireSecuritySignature"
$registryValue = 1
New-ItemProperty -Path $registryPath -Name $registryName -Value $registryValue -PropertyType DWORD -Force

# Prompt user to press Enter before continuing
Read-Host "Press Enter to continue..."

# Enable Microsoft network server: Digitally sign communication (always)
$digitallySignPolicy = Get-WmiObject -Query "SELECT * FROM Win32_OperatingSystem" | ForEach-Object { $_.Version -eq '10.0.14393' }
if ($digitallySignPolicy) {
    $digitallySignSetting = Get-WmiObject -Namespace root\cimv2 -Class Win32_NetworkLoginProfile
    $digitallySignSetting.DigitallySignServerCommunication = 1
    $digitallySignSetting.Put()
}

# Prompt user to press Enter before continuing
Read-Host "Press Enter to continue..."

# Enable LDAP server signing requirements
$ldapSigningPolicy = Get-WmiObject -Query "SELECT * FROM Win32_OperatingSystem" | ForEach-Object { $_.Version -eq '10.0.14393' }
if ($ldapSigningPolicy) {
    $ldapSigningSetting = Get-WmiObject -Namespace root\cimv2 -Class Win32_DirectorySpecification
    $ldapSigningSetting.DSHeuristics = 1
    $ldapSigningSetting.Put()
}

# Final message
Write-Host "Security configurations applied successfully."
```

CHANGE ACCOUNT

Implementing the least privilege model requires limiting the user or application access to minimize security risks and attack surfaces.


Advantages of implementing least privilege model
Prevent malware spread
Minimize cyber attack chances
Improves productivity
Demonstrate compliance
Aid with data classification

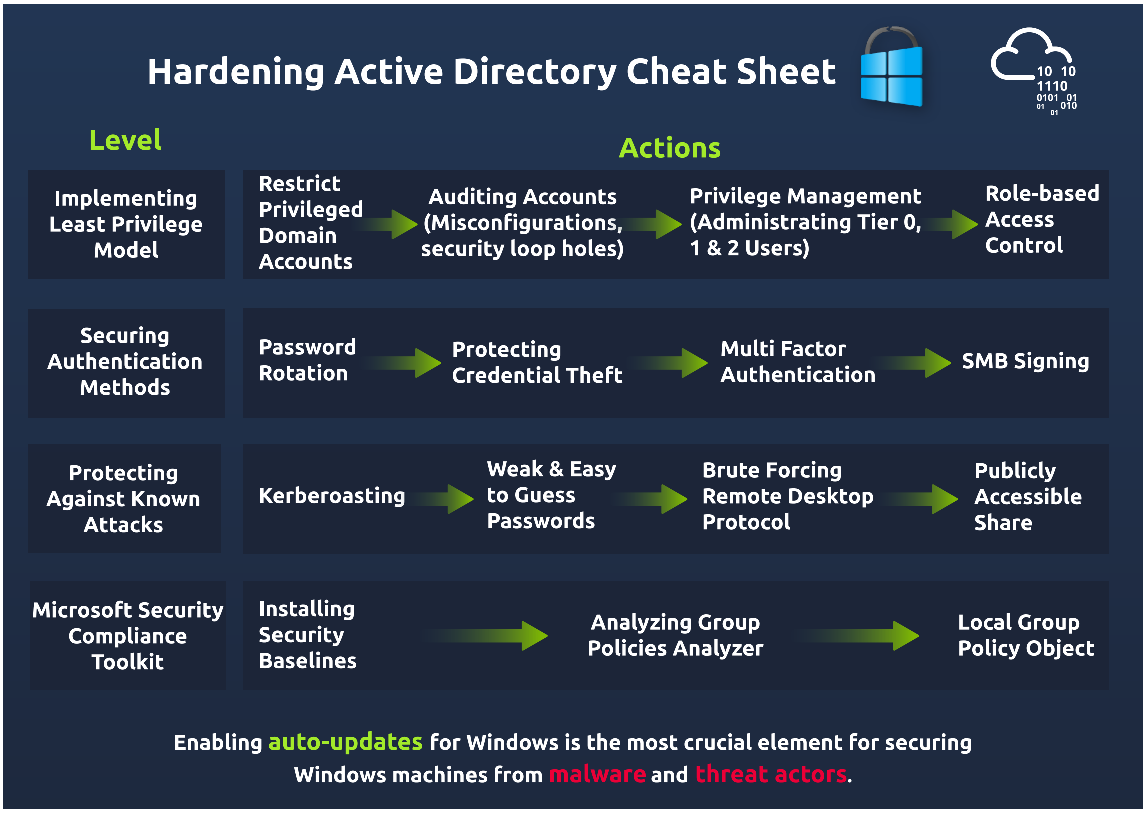


Policy	Policy Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Microsoft Baselines

https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-baselines-for-windows-8-1-windows-server-2012-r2-and/ba-p/701038

The attacker exploits Kerberos Ticket Granting Service (TGS) to request an encrypted password, and then the attacker cracks it offline through various brute force techniques.



Hardening Active Directory Cheat Sheet

Level	Actions			
Implementing Least Privilege Model	Restrict Privileged Domain Accounts	Auditing Accounts (Misconfigurations, security loop holes)	Privilege Management (Administrating Tier 0, 1 & 2 Users)	Role-based Access Control
Securing Authentication Methods	Password Rotation	Protecting Credential Theft	Multi Factor Authentication	SMB Signing
Protecting Against Known Attacks	Kerberoasting	Weak & Easy to Guess Passwords	Brute Forcing Remote Desktop Protocol	Publicly Accessible Share
Microsoft Security Compliance Toolkit	Installing Security Baselines	Analyzing Group Policies Analyzer	Local Group Policy Object	

Enabling **auto-updates** for Windows is the most crucial element for securing Windows machines from **malware** and **threat actors**.