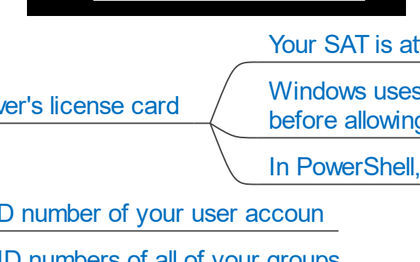
Muhammed Dardir

LinkedIn : https://www.linkedin.com/in/muhammed-dardir

401.5_windowsSecurity

Windows Security Infrastructure

- Windows operating system (OS)
  - Three classes of OS
    - Client
      - Client operating systems are intended for devices such as tablets, laptops, PC workstations, and gaming consoles
      - Users directly interact with these devices by touch, voice, gesture, keyboard, and mouse
      - personally own these hardware devices
      - use, graphical applications, and backward compatibility. Examples include Windows 7 and Windows 10.
      - Microsoft has many client operating systems
        - Windows XP , Vista , 7 , 8 , RT , 10
        - Editions
          - Editions that include words such as Starter or Home are intended for personal use, cannot be joined to an Active Directory (AD) domain, and cost less
          - Editions that include words such as Business, Professional, or Enterprise are intended for business use,can be joined to a domain, and cost more
          - The Ultimate editions are aimed at enthusiasts, have more features than the Home editions, can be joined to a domain, and often cost the most — Some operating system versions do not have an Ultimate edition at all.
        - Usage
          - Client Editions — Starter , Home , Ultimate
          - Work Editions — Business, Professional , Enterprise
        - Platforms
          - Some editions of Windows come in both 32-bit (x86) and 64-bit (x64) versions for platforms with Intel or AMD CPUs.
          - Microsoft wants to move away from the older 32-bit (x86) platform and support only 64-bit
          - AMD OR INTEL
          - (x86, x64, ARM)
          - ARM --> the obsolete Windows RT and Windows Phone products (which were replaced by the ARM version of Windows I 0).
        - Full Mode versus S Mode
          - is not an edition of Windows 10 anymore
          - but a special configuration of Windows in which users cannot install any applications except those installed from the Microsoft Store over the internet
          - The only browser permitted to run in S Mode is Microsoft Edge , not Chrome or Firefox
          - PowerShell cannot run in S Mode either
          - A local administrator can tum offS Mode, which makes the computer run normally in "Full Mode"
          - "S" really means in S Mode (discreetly ask your instructor).
        - Licensing
          - The Starter, Home, Business, Professional, and Ultimate editions are usually purchased and licensed one at a time
            - as either a retail license, which is not bound to a particular piece of hardware and is more expensive
            - or as an OEM license "which is bound to a particular computer and is less expensive"
          - The Enterprise edition is purchased and licensed as part of an organization-wide agreement between your company and Microsoft, which is sometimes called a 11site license11 or a "software assurance license
    - Server
      - Server operating systems are intended for devices such as rack-mounted computers that often have RAID storage, 128GB or more of memory, and multiple network interfaces,
      - Windows Server appliance might be no bigger than a paperback novel with a System On a Chip (SOC) architecture and flash memory for storage
      - also be virtual machines (VMs).
      - interact with these physical or virtual machines over the network, not directly by mouse or touch input.
      - designed for web servers, email gateways, VPN gateways, file and printer sharing, VM hosting, domain controllers, DNS, DHCP, and so on
      - The different editions have different scalability and fault-tolerance capabilities, such as for clustering and Network Load Balancing (NLB).
      - Server os
        - Windows NT 4.0 Server
        - Windows Server 2000 ,2003,2008,2012,2016,2019 — Note that starting with Server 2012, the Enterprise edition no longer exists , there's only Standard and Datacenter
        - Hyper-V Server (Free)
        - What is R2?
          - 1first release "R1" — release to manufacturing "RTM" — is a term used when a software product is ready to be delivered
          - Then, usually about two years after the first release, came the second release (or "R2" version) , of that same OS
          - It's best to consider the R2 versions as whole new operating systems for the sake of migration planning. This naming strategy has made it more confusing to manage Microsoft's server products. Recently, Microsoft has mostly dropped the whole 11Rl/R2" naming convention
        - Server Editions
          - Standard
          - Enterprise
          - DataCenter
          - There are also specialty editions, such as Small Business Server (SBS) and Windows Server Essentials — which are intended for small offices (less than 25 people), and Windows Storage Server ,which is intended for OEM appliances
      - Server Core and Server Nano
        - do not refer to editions of Windows Server
        - Server Core and Server Nano refer to installation options for Windows Server
        - Server Core and Nano are mostly managed with PowerShell or using graphical tools over the network from a management workstation
        - Server Core — remove the graphical desktop from the OS
        - Server Nano
      - Platforms
        - Windows Server 2008 was the last server OS to be available in a 32-bit (x86) version. Server 2008 R2 and later are only available as 64-bit (x64). "Itanium" CPUs are no longer supported.
      - Licensing
        - Window Server licensing is even more complex than the licensing of client devices.
        - Client Access Licenses (CALs) — that allows **client** computers to use server software services
        - OEM licensing for appliances, special deals for Azure hosting, and Office 365 versions of SharePoint and Exchange
      - Roles for Windows Server
        - Domain Controller
        - Web Server (IIS)
        - Hyper-V Virtualization (VMs and Containers)
        - Remote Desktop Services
        - DirectAccess and VPN
        - File and Print Services
        - DHCP Server
        - DNS Server
        - Network Policy Server (RADIUS)
    - Embedded
      - Windows for the Internet of Things (IoT) , "Windows IoT" is just another name for Windows Embedded
      - Embedded operating systems are intended for devices such as Point of Sale terminals, automobile dashboards, electronic signs, industrial control equipment, robotics, sonogram machines, handheld laser scanners, welding machines, and all the myriad "Internet ofThings11 devices.
      - usually customized by equipment manufacturers to suit just their hardware
      - Examples include Windows Embedded 8.1 and Windows IO IoT Core.
      - Intended for industry-specific hardware appliances, such as ICS/SCADA equipment, retail point-of-sale, MRI scanners, robotics, digital signs, drones, 3D printers, and more
      - Supports the ARM platform, as well as x86 and x64 CPUs
      - Runs on Raspberry Pi, MinnowBoard, and Arduino devices
- workgroup
  - Two or more Windows computers that share information in the absence of any domain controllers are called a workgroup — Even if all the computers are running Windows Server 2012 Enterprise
  - Characteristics of a workgroup
    - There are no domain controllers
    - Each computer has a local accounts database — Users and groups in that database are called local users and local groups
    - Permissions can be assigned to local users and groups only
    - Local groups cannot have users from other machines
    - Two computers may each have a local user account with the same name, but these are two different accounts. The accounts have different Security ID (SID) numbers
    - user of a computer in a workgroup is a member of the local Administrators
    - Workgroups tend to be small, usually less than 50 computers
    - You can have standalone computers in the midst of other machines that are members of a domain. They are not anathema to each other, and each has its benefits
  - Benefits of workgroups
    - Simple to understand
    - Each computer manages and protects itself
    - Lower initial deployment cost
    - Users are typically administrators of their own machines, allowing personal creative expression and joy
  - Drawbacks of workgroups
    - Users are insane
    - Workgroup =Chaos+ Anarchy
    - Difficult to manage large numbers
    - No centralized policy control or auditing
    - No single sign-on without great effort
    - No consistent permissions across machines
- local users and groups
  - Computer Management Tool
    - RClick PC - Manage
    - run "CompMgmt.msc" to launch
  - run CompMgmt.msc to launch
    - Get-Help LocalUser
    - net. exe help user
- Security ID (SID) number
  - Like a Windows Social Security number — Example: S-l-5-21-4272796178-4779766465-l 106779640-1000
  - Each user, computer, and group has its own unique SID — Well-known SID numbers exist for certain built-in users and groups that exist on all systems (for example, the Everyone group)
  - The username of an account might be renamed, but the SID number stays the same.
  - Windows actually cares only about SID numbers when it is enforcing privileges and permissions — This ID card is officially called your "Security Access Token " (SAT)
  - cmd : whoami .exe /all /fo list



- Security Access Token (SAT)
  - SAT is like your Windows driver's license card
    - Your SAT is attached to every process you start
    - Windows uses your SAT to check your permissions and privileges before allowing attempted actions
    - In PowerShell, run: whoami. exe /all /fo list
  - Your SAT contains
    - SID number of your user accoun
    - SID numbers of all of your groups
    - Your list of privileges on the computer
  - To Form a More Perfect Workgroup — Standalone computers do not trust each other's SATs; that is whyworkgroups don't scale — In that case, what we need is
    - A central shared database of SID numbers that all standalone computers agree to use for single sign-on and authorization
    - A secure authentication protocol for distributing SID numbers from this database to computers making SATs
    - In other words, we need a domain controller! ^_^
- Active Directory (AD)
  - Active Directory (AD) is the name of the shared accounts database that gets installed on a Windows Server when it is promoted to become a domain controller
  - Analogy: Active Directory is like a shared registry for all users and computers on the network
  - Active Directory is a multi-master replicated database of network data
  - Domain Controllers
    - A domain controller is just a server that helps to manage the AD database on behalf of the other computers and users in the organization
    - The AD database contains, among other things, all the SID numbers of the users ,computers, and groups that have "outsourced"
    - their authentication and account management work to the domain controller
    - This list of permissions based on user and group SID numbers is called an access control list (ACL). — ACL that contains (Alice: read,write; Bob: read)
    - Multi-Master Replication and Read-Only Domain Controllers
      - Multi-Master Replication — You can make a **change** to the AD **database** on any domain controller in an AD ·domaih, and this change is then automatically replicated to all other domain controllers. This is called **multi-master** replication
      - Read-Only Domain Controllers
        - An important exception to multi-master replication is when a domain controller is running Windows Server 2008 or later and the administrator has decided to install that controller as a **Read-Only Domain Controller (RODC)**.
        - A running RODC can authenticate users and fulfill search requests, but any changes made to the AD database on the RODC will never be replicated to any other controllers.
        - RODC controllers cache only the credentials of the groups an administrator specifies, and the list of cached credentials is tracked
        - RODC controllers using BitLocker and a TPM cryptographic — **Trusted Platform Module** (**TPM**, also known as **ISO/IEC 11889**) is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys
        - RODC controllers may also be installed using the Server Core option to give it smaller disk and memory footprint to keep costs down
  - Being "In the Domain"
    - Being in the domain has nothing to do with one's physical location or bandwidth
    - Who or what can be in the domain? Anything with a SID number can be in a domain
    - What can have a SID number? All users, groups, and computers have SID numbers
  - Active Directory Database
    - Just as the registry "REGEDIT.EXE"on a computer stores the configuration settings that affect just that one computer, Active Directory can store the configuration settings that affect the entire domain
    - what can be stored in Active Directory
      - User account properties and passwords
      - Groups and their memberships
      - Computer properties and passwords
      - Domain names and trust relationships
      - Kerberos master keys
      - Digital certificates and Certificate Trust Lists
      - Organizational Units and their members
      - LANs and IP subnets in the organization
      - AD replication links and their settings
      - Shared printer locations (UNC paths)
      - Exchange Server directory information
      - Group Policy Objects
      - Any custom data you want to add
    - Active Directory is a general-purpose database and can be accessed through an industry standard protocol, LDAP.
    - Active Directory uses the same database engine as Microsoft Exchange Server and can store millions of objects. Its maximum size is 4,000 GB (4 TB)
  - Global Versus Local — Local users and groups still exist in the local accounts databases of computers that have joined the domain. But now) the users and groups from the AD database are also available to domain member computers.
- authenticate to the domain
  - Autlientication protocols
    - The SID numbers of domain accounts and groups in the Active Directory database are conveyed to domain-joined computers through authentication protocols
    - An SAT is constructed "on the fly" at the remote computer where the user requests access to a resource, such as a shared folder
    - Privileges, local account SID numbers, and local group SID numbers all come from the target computer's own local registry
    - Security Access Tokens Revisited
      - SA Ts are never sent over the network
      - SATs are constructed on the fly inside the memory of the server where the user is requesting access.
      - But important parts of the SAT are sent over the network through the authentication protocol being used.
    - SAT can be broken down into four parts
      - SID number for the user's domain account (AD)
      - SID numbers for the domain groups the user is a member of (AD)
      - SID numbers for the local groups on the server being accessed that the user is a member of (from the server's local accounts database)
      - The list of privileges the user has on the server being accessed (from the server1s local registry)
    - authentication protocol convey the user's domain SID numbers to the server — TWO PROTOCOLS
      - Kerberos
      - NTLM
  - Kerberos
    - Kerberos (RFC 4120) : is the default authentication protocol in Active Directory environments
    - Kerberos uses tickets to convey the user's account SID and group SID numbers to the target server to which the user desires access
    - Tickets are encrypted with users' passwords and special keys shared only among the domain controllers
    - otherwise, the computer will fall back to using NTLM instead — On standalone computers, Kerberos cannot be used at all.
    - The most important requirement for making Kerberos available is the presence of an Active Directory domain controller. — AD domain controllers are all Kerberos Key Distribution Centers (KDC()), — because they hold eve1y user's and computer's Kerberos master key. Your Kerberos key is derived from your password.
    - Kerberos is available when any of the following protocols is used: SMB/CIFS, RPC, LDAP, HTTP, Dynamic DNS secure updates, IPsec IKE, and PowerShell Remoting (WSMAN).
    - Kerberos is faster than NTLM and scales better in large environments
    - Kerberos Risks
      - ifan attacker can capture the packets of the initial Kerberos exchange when the user first logs on, the attacker can mount a brute-force attack to discover the user's password
      - Another risk is inherent in the design ofKerberos itself and cannot be totally eliminated
      - With a Golden Ticket, the attacker can authenticate to any machine joined to the domain as a member of the Administrators local group on that machine
      - (Tickets do have time expiration limits, however.)
      - Why is the ticket encrypted? Because inside the ticket is the user's SID number and the SID numbers of the groups in Active Directory of which the user is a member
      - When the target server has the user's Kerbcros ticket, the server can construct a Security Access Token (SAT) to represent that remote user
    - prevent this
      - protect the integrity of the domain controllers
      - protect the backups of the domain controllers
      - protect the credentials of the network administrators
  - NTLM
    - NTLM authentication is supported by Windows NT and later
    - 1 - The client wants to access a server, so the client sends to the server the client's encrypted password information
    - 2 - The server passes this information through to a domain controller
    - 3 - If the password is good, the domain controller sends the server all the client1s domain SID numbers.
    - 4 - Now, the server can construct an SAT to represent the client.
    - When authenticating a local user account, such as in a workgroup, a domain controller is not required.
    - NTLMM protection of password data is dreadful, and the password data itself(the password hashes) are not well protected, either
    - Using a sniffing tool, such as Cain, a hacker can listen in on these NTLMM exchanges and extract password hashes
    - These are the same LanManager and NT/MD4 hashes that can be extracted from a stolen user accounts database,
    - Nonetheless, because ofNTLM1s performance, scalability, and security issues, we should stop usingNTLMjust like we should stop using LanManager
    - Starting with Windows 7 and Server 2008-RZ, you can use Group Policy to disable support for NTLM entirely, thus pem1itting only Kerberos and certificate-based authentication
- forest or trust
  - Domains can be linked with trusts to permit resource sharing and single sign-on across domains
  - AD forest
    - One or more domains
    - Inter-domain replication
    - Two-way transitive trusts
      - Nature of Trust
        - Without a trust link between two domains
        - No single sign-on across domain boundaries
        - Can't assign permissions to users in the other domain
        - Can't log on to your desktop in the local domain with an account created in the other domain
      - Cross-Forest Trusts
        - Entire forests can trust each other, too
        - These can be one-way or two-way, linked at the root domains
        - When two-way, every domain trusts every other domain
        - There is no replication of any AD data between the forests
    - The Global Catalog
    - Global Catalog Servers
- Group Policy
  - When you buy the licenses for your workstations , you get something called "Group Policy"
  - Group Policy is a set of Microsoft technologies and administrative tools for configuration management of all your domain-joined Windows computers
  - Group Policy can be used to configure virtually every security setting in Windows so that you do not have to touch each machine by hand
  - Group Policy is for Windows configuration management
    - Password policy
    - Lockout policy
    - NTFS permissions
    - Privileges
    - Eventlogs
    - Registry settings
    - IPsec settings
  - GPO
    - A term used throughout this manual is "Group Policy Object (GPO)." A GPO is like a cookie cutter that can be applied to domain-joined computers to reconfigure those computers to match the cutter
    - GPOs are replicated between your domain controllers and then periodically downloaded and applied by Windows machines joined to the domain.
  - How Group Policy Works
    - A GPO is like a configuration script that can change any setting when the script is run
    - GPOs are stored on and replicated between your domain controllers
    - Clients download and apply GPOs at boot up, user logon, and roughly every 90 to 12 0 minutes after that
    - double-click your forest> double-click your domain> right-click the Default Domain Policy icon> Edit
- Summary

Windows as a Service

- techniques for managing updates
  - End of Support
    - End of Extended Support
      - When security updates and paid support can no longer be purchased, except in special cases with (expensive) Custom Support
      - Stuck with an Expired Client OS? — If a computer cannot be upgraded before it expires — In this situation, block all network connectivity to/from expired computers (or at least internet access),
    - End of Custom Support — When there will be no further update or support options whatsoever unless they are negotiated with Microsoft
    - Windows as a Service= Continuous Updates — An "update" replaces existing program files with newer ones
      - **Feature Updates:** Large new service or application changes that increment the Windows version (released roughly every 180 days)
      - **Quality Updates:** Smaller improvements to what currently exists, such as bug fixes and security patches (released every 30 days)
    - Most vulnerabilities are eliminated by applying updates
    - Microsoft Security Updates Guide
      - An update will roll up many changes into a single all-or-nothing package that fixes many bugs in one shot
      - These are called "cumulative" updates
      - Update and vulnerability information is provided in a searchable online database called the "Security Updates Guide": — https://portal.ms:rc.microso:ft.com
  - Servicing Channels
    - Applying an update immediately after Microsoft releases it can be dangerous to the stability of your computer
    - Servicing "channels" are just options for delaying the installation of new updates instead of applying the updates immediately after release
    - Updates for Channels
      - How long may quality updates be deferred?
        - Up to 30 days on the Semi-Annual channel
        - Home edition users may hit the pause button five times, each time pausing for a week (35 days maximum)
      - How long may feature updates be deferred?
        - Up to 365 days on the Semi-Annual channel
        - Home edition users have the pause button for these too
      - Channel Configuration
        - All Settings > Update & Security icon > Windows Update area > Advanced Options link
        - Centrally manage this feature through domain Group Policy
        - To manage these options through Group Policy, open the relevant GPO and navigate to Computer Configuration >Policies> Administrative Templates> Windows Components> Windows Update
      - Long-Term Channel and the Windows Insider Program
        - Long-Term Channel
          - Will never get feature updates (must upgrade entire OS)
          - Only monthly quality updates can be applied
          - Requires a Volume License Agreement with Microsoft
        - Windows Insider Program
          - Get access to upcoming feature updates while still in development
          - Important for early testing and feedback to Microsoft
  - Windows Update — Automatically download and install updates
    - Hands free
    - Scheduled
    - All Settings > Update & Security > Windows Update
  - Windows Server Update Services (WSUS)
    - WSUS is your own local Windows Update server
      - WSUS is free because it's built into Windows Server as an IIS web application.
      - WSUS clients can connect to a local WSUS Server and download their updates from there instead of connecting to Microsoft, but this is configurable
      - To use WSUS, users do not have to be members of the Administrators group on their computers
      - WSUS provides updates not just for Windows and Edge, but also for SQL Server, Exchange Server, Microsoft Office, and most other Microsoft products
      - WSUS permits the grouping of computers into custom sets that can be managed and updated separately
      - A single WSUS server can handle more than 10,000 client computers, and WSUS servers can be loadbalanced and chained together to form administrative arrays
      - WSUS logs to a local SQL Server database that can be queried to identify (for example, which machines have (not) successfully received a particular update
      - Generating reports of patches deployed to systems in the enterprise, which cannot be done when using Windows Update.
      - Like almost every Microsoft product, WSUS can be managed using PowerShell
    - How Does WSUS Work? — One or more local WSUS Servers can be installed on Windows Server 2003 or later as an IIS application
    - WSUS Administration
      - WSUS is installed with the Server Manager tool like any other role or feature
      - WSUS clients are configured through Group Policy or simple registry edits on standalones
      - WSUS clients are infonned of their local WSUS Server's HITPS path, the schedule for checking for new updates, and whether the updates should be installed automatically.
    - Third-Party Patch Management — Many excellent non-Microsoft products available
      - IBM Endpoint Manager: www.ibm.com
      - Altiris: www.symantec.com
      - Gravity Storm: www.securitybastion.com
      - Ivanti: www.ivanti.com
      - System Center Configuration Manager: www.microsoft.com
      - Many other companies not listed here

Muhammed Dardir

LinkedIn - https://www.linkedin.com/in/muhammed-dardir/

alt:f4_windowsSecurity

Intro

I access control is encryption: if you can't decrypt a file, you can't read its contents.

Windows Vista and later includes BitLocker Drive Encryption at the volume level. It can be configured to use the Trusted Platform Module (TPM) chip in the motherboard.

Finally, Windows Vista introduced a new method of applying the principle of least privilege to Security Access Tokens (SA Ts) and is called User Account Control (UAC).

Windows Access Controls

NTFS Permissions

NTFS Overview

Windows File Systems

- CDFS
- FAT
- FAT32
- exFAT
- ReFS
- NTFS

NTFS characteristics

Use NTFS by default

- Permissions
- Auditing
- Encryption (EFS and BitLocker)
- Compression
- Transactions-oriented processing

Theoretical maximum volume size: 256 TB (terabytes)

Resilient File System (ReFS)

- Resilient File System (ReFS) is available on Windows Server 2012 and Windows Server 2012 R2.
- ReFS is also available on Windows 10 for Workstations version 1709 and later

NTFS and ReFS are similar. Both support permissions, BitLocker encryption, and large volumes.

Windows NT File System (NTFS)

But while NTFS supports a maximum volume size of only 256 TB, ReFS supports a theoretical maximum volume size of 35,000 TB (think 35 petabytes).

NTFS DACLs

A set of NTFS permissions on a folder or file is called a discretionary access control list (DACL).

Individual permissions in the DACL are called access control entries (ACEs)

Advanced Security Settings for ACEs

- Deny Overrides Allow
- A user can be a member of multiple groups
- On the Security tab, notice that some ACEs are represented by checkboxes that are somewhat gray and cannot be altered
- Explicit Versus Inherited Permissions

NTFS DACLs are always enforced, even with

- Local users
- IIS HTTP and FTP sites
- Remote Desktop Protocol
- SMB shared folders
- PowerShell remoting
- ICACLS.EXE OR PowerShell: Set-ACL

Apply Only: Scope ofInheritance

NTFS Owners

Every NTFS folder and file has an owner associated with it

right-clicking th Properties> Security tab > Advanced button> Permissions tab (or the Owners tab on Windows 7)

Principle of Least Privilege

Which NTFS permissions should I grant?

- Perform a "needs analysis" based on job roles.
- Grant the minimum permissions that still permit users to get their legitimate work done

A good default DACL, but edit this for least privilege

- System: Full Control
- Administrators: Full Control
- CREATOR OWNER: Full Control
- Authenticated Users: Read and Execute (or Modify)

AGLP

There is a formal model of how privileges and permissions should be applied

Active Directory Accounts and Groups

Domain Users

- right-click any OU> select New> User.
- Groups in Active Directory
- right-click any OU> New> Group.

Shared Folder Permissions

The Server service and the SMB protocol

Share Permissions

- Full Control
- Change
- Read

PowerShell

- New-SmbShare

Common Internet File System (CIFS) protocol

- CIFS is not a new protocol. It's just SMB plus a few enhancements.
- For example, NetBIOS no longer is mandatory for file and print sharing. SMB can run directly on a network.
- SMB and CIFS do the same thing. Most documents just refer to SMB now, not CIFS.

Shared folders can be accessed via the following methods

- Network Places (that is, Network Neighborhood or just Network)
- Mapped drive letters (New-PsDrive or NET USE command)
- Run line (enter \\ComputerName or \\IP Address)
- Shortcuts (right-click your desktop or in a folder> New> Shortcut> \\ComputerName\ShareName path to the shared folder)

Hidden and Administrative Share

- ShareName$ --> The $ makes it hidden.
- IPC$ for inter-process communications.
- C$ and E$ are drive roots.
- PowerShell
  - Get-SmbShare | Format-Table -AutoSize
- AutoShareServer (REG_DWORD) to zero under the following key and then rebooting
  - HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters

Combining NTFS and Share DACLs

NTFS Permissions

- Users: Read
- Sales: Deny,-M
- Amy: Modify

NTFS permissions are always enforced.

Calculating a user's effective permissions to a file in a shared folder requires three steps:

- Assemble a list of all the share permissions the user has to the folder for that user's group memberships.
- Assemble a list of all the NTFS permissions the user has to the file. This includes both explicit and inherited NTFS permissions
- Examine both the final share and the final NTFS permissions.

Share Permissions

- Everyone:Change
- Administrators: Read
- Amy: Read,

Registry Key Permissions

Intro

Virtually all configuration settings for the computer's hardware, operating system, applications, and its users' preferences are stored in a special miniature database called the registry.

The registry can be modified directly using regedit, various command-line tools (REG.EXE, REGINI.EXE, and REGEDIT.EXE) and various cmdlets in PowerShell like Set-ItemProperty.

There are various types ofregistry values, including REG_DWORD, REG_BINARY, REG_SZ, REG_MULTI_SZ, and REG_EXPAND_SZ.

The type of the value determines what kind of data can be put in it and how that data must be formatted; for example, an REG_SZ type can hold a string.

You can create your own keys and values in REGEDIT using the Edit> New menu option.

Remote Registry Service

- REGEDIT.EXE > File menu > Connect Network Registry...
- Disable the Remote Registry service to prevent network access

Permissions on the WinReg key are interpreted as the share DACL if the service is enabled.

RemReg Registry Share Permissions

- Registry key permissions are always enforced against local or remote users
- HKLM\System\CurrentControlSet\Control\SecurePipeServers\winreg

The default permissions in Vista and later are Administrators Full Control, Local Service Read, and Backup Operators get a custom set of permissions, which more or less amount to Read.

Active Directory Users and Computers snap-in> right-click any OU> Delegate Control...> Add...> Select a user, computer, or group as the container in Active Directory Domain Services> Next> Next

Active Directory Permissions

- Consider an example of how property-level ACLs can be leveraged. A user account has many properties.
- Delegation of Authority in AD
- Name, phone, fax, email address, password, and so on. Each one of these properties can have its own separate DACL and SACL.

Privileges

1

privileges are listed in your SAC whereas rights control only local or over-the-network logon attempts.

the Take Ownership privilege permits one to take ownership of any object

Another privilege is Force Shutdown from a Remote System, which permits one to shut down a system but is a dangerous capability one certainly would want to restrict.

SAT also contains a list of all your privileges on that particular machine

On Windows Vista and later, you can see what privileges you have on your computer by opening a command-prompt window and running whoami /priv

2

Idden> Local Security Policy> Local Policies> User Rights Assignment

standalone system has its own local Group Policy Object (GPO).

You manage privileges through Group Policy.

- Allow Log On Locally
- Restrict who can log on interactively at the keyboard

3

- Allow Access to This Computer from the Network
- Restrict who can remotely authenticate to a computer.

4

- Allow Log On Through Remote Desktop Services
- Restrict who can use Remote Desktop Protocol (RDP).

Sometimes, the terms rights and privileges are used interchangeably. But when users and have a user can log , this privilege is called a "user right".

rights do not appear in a user's SAT after he or she has logged on. So, a logon privilege is called a ("right. 11

The deny-style rights are useful for defining exceptions to a general policy that otherwise allows access.

5

Take Ownership of Files and Objects

A powerful and dangerous privilege is Take Ownership of Files or Other Objects.

The owner of an object can change its permissions in any way verified

Objects include files, folders, printers, AD containers, registry keys, processes, and services.

Objects that have owners include NTFS files and folders

Only administrators have this by default.

6

The seemingly innocuous backup and restore privileges actually are quite dangerous.

Think of these as the "circumvent NTFS permissions" privileges.

- Backup Files and Directories
- Restore Files and Directories

Use Group Policy to delegate the Backup Files privilege, but reserve the Restore Files privilege for Domain Admins only.

7

Debug Programs

- Example of a debugger: DbgDsg (www.dbgdsg.de).
- Determines who can attach a debugger to any process

Used by developers for troubleshooting software and by security experts (and malware authors) for reverse engineering.

Windows "DLL Injection" Attack

- A new thread is injected into a running process that the attacker does not own (that is, that doesn't have her SAT).
- Can overcome to uses DLL injection to dump password hashes and the operating system's LSA Secrets data.

BitLocker Drive Encryption

Sectors encrypted with AES (128- or 256-bit).

BitLocker Whole Disk Encryption

Boot-up integrity checking with a TPM (TPM is optional)

- TPM is a chip in the motherboard.
- TPM performs encryption, hashing, random key generation, secure key storage, and other crypto tasks.
- A physical or virtual TPM can be used as a smart card or to encrypt domestic login data, so it's not just for BitLocker.

Turning On and Initializing the TPM

- Enabled in the computer's firmware
- Turned on in Windows.
- Initialized in Windows with an owner's password

Supports USB and Thunderbolt drives.

Emergency recovery PIN

Supports some self-encrypting hard drives (eDrive spec)

The two main benefits ofBitLocker Drive Encryption

Verification of the integrity of boot-up files and other startup data structures to help prevent rootkits and other malwares from secretly taking control of the computer.

Encryption of the contents of the entire hard drive volumes, including the paging and hibernation files on those volumes, to prevent exposure of confidential data on stolen or lost hard drives.

Requirements

BitLocker is only available on Windows Vista or later, Ultimate and Enterprise editions, and on Windows Server 2008 or later. Note that it is not included in the Home, Business, or Professional editions.

BitLocker TPM Options

With a TPM in the Motherboard

- TPM+PIN
- TPM+USB Drive
- TPM Only (vulnerable to cold boot attack)

Pre-boot passphrase (Windows 8 or later)

BitLocker with No TPM

- USB drive with the key inserted at boot-up
- No boot-up integrity protection to detect malware though.

Group Policy can be used to control almost every aspect of how BitLocker may be used (GPO: Computer Configuration> Policies> Windows Settings> Security Settings> BitLocker Drive Encryption). BitLocker can also be managed through Windows Management Instrumentation (WMI) scripting of the Win32_ Encryptable Volume class for scalable deployment.

Emergency Recovery

Back up your BitLocker recovery password

- Recovery password is actually a 48-digit number.
- Recovery password can decrypt a volume even if the TPM is damaged, the user PIN is forgotten, or the USB token is lost

Use Group Policy to force backup of the recovery password to Active Directory for scalable mass deployments.

UEFI Secure Boot

Unified Extensible Firmware Interface (UEFI) replaces the older BIOS interface to the computer's firmware.

A computer must be purchased with UEFI.

Secure Boot requires UEFI, Windows 8, or later and a GUID Partition Table (GPT) bootable hard drive partition.

Applying security templates

A security template is a plaintext configuration file that can store hundreds of security settings.

Security templates are kept by default in %SystemRoot%\Security\Templates and have %SystemRoot%\inf, and they end with the .INF filename extension.

Security Configuration and Analysis "SCA" Tool

- Applies a template to a computer (reconfigures the computer).
- Compares a template to a computer's actual settings (audit only)

Templates can be edited with Notepad, but a much easier method is to use a Microsoft Management Console (MMC) snap-in named Security Templates.

- We cannot apply a template to a computer across the network with this tool, but that's why we have Group Policy and PowerShell.
- Warning: There is no undo feature!
- Install the SCA snap-in in the same console as the Security Templates snap-in using the same procedures described previously (File menu> Add/Remove Snap-in).
- SECEDIT.EXE is a command-line version of the SCA snap-in
- Imagine creating a USB drive with SECEDIT.EXE

template can store the following security settings

- Password policies
- Account lockout policies
- Kerberos policies
- Audit policies
- Custom privileges assignments
- Various security options
- Event log sizes and wrapping options
- Custom memberships in important groups
- Service startup options
- Registry key permissions
- Microsoft's security baseline guides

Several sources of security guidance for Windows

- Guides from the United States Government (DoD, NIST, NSA)
- Center for Internet Security (CIS)

Understanding Local Group Policy Objects

Group Policy Object (GPO) is a set of configuration changes.

- Every Windows computer has a local GPO.
- Add the "Group Policy Object Editor" snap-in to an MMC window

GPO = Computer Configuration

- Applies even when no one is logged on.

GPO = User Configuration

- Applies to current user's desktop

Local GPO Administrative Templates

- Registry controls almost everything
- Hundreds if settings are available.
- You can import more ADM templates.
- You can edit these ADM templates to configure any registry value.

Understanding Domain Group Policy Objects

Domain GPOs are stored in Active Directory

- Downloaded automatically at startup, shutdown, logon, and logoff.
- Refreshed on clients roughly every 90-12 0 minutes
- Only downloaded by domain-joined computers, not standalones

Domain GPOs can be applied to thousands of computers joined to the domain without touching each machine.

The Default Domain Policy GPO

There is a GPO named "l:\Default Domain Policy" stored on domain controllers.

Group Policy Management Console (GPMC)

- Importing Templates into GPOs
- is built into Windows Server by default and can be installed on client computers via RSAT. It's your primary tool for creating, editing, and managing domain GPOs.
- To import an INF security template into a domain GPO,

right-click the desired GPO> Edit> Computer Configuration> Policies> Windows Settings> right-click on Security Settings> Import Policy> locate and select your desired INF template > Open

Now that we know how to make security configuration changes through INF templates, local GPOs, and domain GPOs,

Checklist of GPO Settings

GPO> Computer Configuration> Policies> Windows Settings> Security Settings> Local Policies> Security Options

Password Policy

Account Lockout Policy

Anonymous Access Control

- A "null user session" is an SMB session with a blank username and password, like this:
- net use \\pentbtest\IPC$ * /u:""
- Security Settings > Security Options > Network Access

Kerberos and NTLMv2

- Kerberos support is built into the drivers for SMB, LDAP, RPC, HTTP, and other protocols.
- NTLMv2 authentication traffic can be sniffed with tools like Cain to reveal the user's password hashes.
- NTLMv2 Session Security is also required to make NTLMv2 traffic encrypted and thus unsniffable.

Credential Guard

Credential Guard protects credentials and other secrets in memory from malwares and tools like Mimikatz.

- Credential Guard relies on hardware, firmware and hypervisor features to secure these secrets
- Requirements
- UEFI firmware
- UEFI secure boot enabled.
- Windows 10 or later.
- Server 2016 or later.
- Hyper-V enabled.
- Must have Enterprise or Education edition, not Pro.

Guest Account

- Create a honeypot "Administrator" account as an IDS canary.
- Assign a random passphrase

Controlled Folder Access

- Blocks changes to protected folders from untrusted apps.
- Helps to thwart ransomware and other malware from altering files.
- Add additional folders and apps to the default list, including shared folders and mapped drive letters.
- To enable CF A, go to All Settings > Update & Security applet> Windows Security > Virus & Threat Protection > Virus & Threat Protection category> Manage Ransomware Protection link> turn on the Controlled Folder Access button. (CF A can also be managed through Group Policy and PowerShell.)

Checklist

Install and run apps inside a container (not a VM).

Windows Sandbox for Malware Isolation

- Locks like a VM with its own start menu, taskbar and desktop in a window on your real desktop, but all changes are discarded when the Windows Sandbox is closed.
- Requires Windows 10 version 1903+, Pro or Enterprise, with virtualization enabled
- All Settings> Apps > Apps & features> Programs and Features> Turn Windows Features On or Off>

Edge

The Group Policy settings for Edge are found in the GPO under User Configuration> Policies> Administrative Templates > Windows Components> Edge.

- Windows Defender Application Guard
- Firefox is free, open source, and cross-platform.
- Manageable through JSON policy file and Group Policy
- Extended Support Release (ESR) for enterprises.
- Many security-related extensions (next slide).

Firefox

Edge, Firefox, and Chrome

Many Firefox and Chrome Extensions Available

- Password Managers
- HTTPS Everywhere (enforcement and PDF)
- OpenPGP and S/MIME Email Encryption
- HTTP Encrusted
- Ad Blockers (uBlock Origin, etc.)
- Firefox Multi-Account Containers
- Antitracker Extensions
- Ad Blockers (Live Block more than ads)

Chrome

- Chrome can be deployed as an MSI package
- Auto-updates do not require user admin rights.
- Manageable through Group Policy.
- Phishing and malware site URL blocking
- Extensions for Azure and Office 365 single-sign-on

Adobe Reader

- Manageable through Group Policy and custom MSI files
- Disable internet access by PDF files
- Define exceptions by hostname or FQDN.
- Disables opening file attachments
- Define exceptions by file name extensions.
- Disable JavaScript entirely (if you can).
- This will break many PDF forms.

recommended minimum security options

- Page 141 , 141 in book

Enforcing Security Policy

Administrative Users

Enforce a strong passphrase policy .

Require smart card authentication (if you have a PKI).

Enable Credential Guard.

Require Kerberos and NTLMv2 (forbid LanManager and NTLMv 1).

One each admin at least two user accounts

- Regular account (regular activities).
- Administrative account (only as needed).

Admins should have two workstations (or a jump server).

Limit local account use of blank passwords to console logons only.

Audit all access to administrative users and groups in AD.

Rename the built-in Administrator account.

Create a honeypot "Administrator" account as an IDS canary.

AppLocker

AppLocker permits administrators to define exactly which applications users are and cannot be run on Windows 7, Server 2008 R2 and later systems.

Rules defined by

- SHA256 hash of program
- Local path to program
- Network path to program
- Code signing certificate
- User's group membership

Rules apply to

- Executables (EXE and DLL)
- MSI software packages
- APPX software packages
- Scripts (many types)

GPO > Computer Configuration> Policies > Windows Settings> Security Settings> Application Control Policies> right-click AppLocker> click either Executable Rules, Windows Installer Rules, or Script Rules> Create New Rule.

User Account Control

Right-click> Run As Administrator

- Administrative user process
- Standard User Approval Modes: Prompting Options
- Standard User Approval Modes: Fail or Prompt for Credentials

Standard SAT for a member of the Administrators local group.

- Standard user process (the default)
- Right-click> Run As Administrator
- SAT stripped of dangerous privileges

Checking Recommended GPO settings, including

- Password Policy
- Account Lockout Policy
- Security Options
- Internet Explorer Security
- Miscellaneous Administrative Templates
- Other Settings

Summary

- Security templates
- Local Security Policy
- Microsoft GPO
- Microsoft SCA
- Microsoft SCE
- Third-party tools
- Your security vendor
- Microsoft
- Other vendors

- Recommendations for
- Local workstations
- Local servers
- Domain workstations
- Domain servers
- Domain controllers