**Week 2: Windows**

**Windows Security Architecture**

Name of the computer

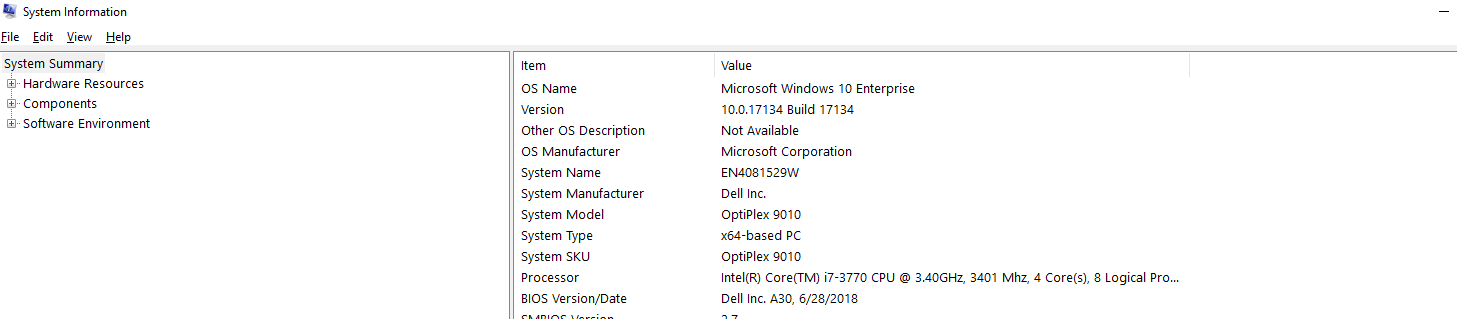
* hostname

Change the computer name

* netdomrenamecomputer <ComputerName> /NewName:<NewComputerName>

System Information

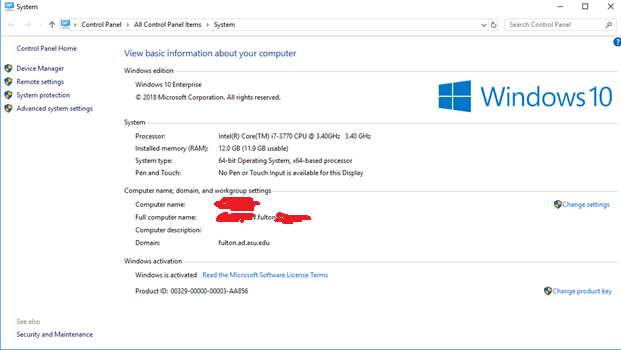
* msinfo32.exe



Local vs Domain Accounts

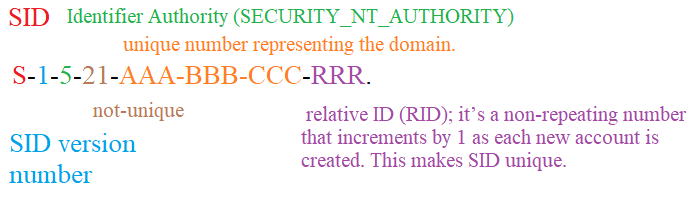
UNIX has users and groups. UNIX subjects are applied to one machine.

* Workgroup-collection of computers connected using one network. No domain controller in a workgroup, authentication performed at each computer.
* A networked Windows system can have two configurations – either domain joined or workgroup. In a domain joined computer, users can access accounts using centrally managed Active Directory.
* Users can also login using local account, but local accounts will not have access to domain resources - networked printers, Web servers, e-mail servers.
* In a workgroup – local accounts managed by SAM are used.
* Security policies can be centrally managed using AD.



What happens when a user logs on to a Windows system – End to end domain Example

* Domain admin should add user’s account information to the system before he can log on (username, account name – domain specific, and password).
* Windows creates and account in domain controller running AD. Each account has unique Security ID (SID) – unique to domain. E.g. - S-1-5-21-AAA-BBB-CCC-RRR, S-1-5-21-123625317-425641126-188346712-2895.
* If you create account “Mike”, delete and re-create “Mike”, they are two totally different accounts because they will have different SID.
* Once user log’s in token SID is generated by OS and assigned to user.
* Token contains user’s SID, group membership information, and privileges.



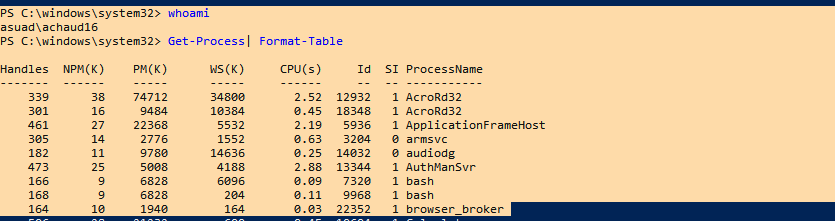
* On a domain-joined computer (we’ll use the ‘Marketing’ domain), it is possible for a user to logon to a local account by using the “.” domain.
* So rather than using “Marketing\Paige” or just “Paige” Paige can use “.\Paige” assuming there is a local Paige account on the computer. The “.” will substitute the machine name as the workgroup name.

Username Format

* SAM format - Domain\Username.
* User Principal Name (UPN) – [username@domain.company.com](mailto:username@domain.company.com).
* “Mike’s” PC in ASUAD domain, he can login using “ASUAD\Mike” or [Mike@asu.edu](mailto:Mike@asu.edu).

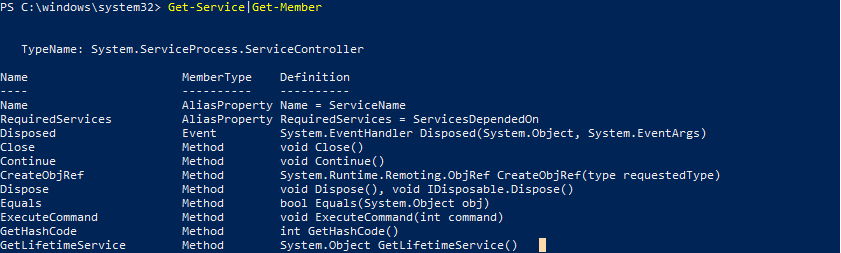
Powershell (PS)

* Flexible scripting language based on .NET framework.
* Rich access to Windows computers and security settings.
* Commands in PS are called cmdlets – consistent (verb-noun) syntax.
* PS supports command piping. PS pipes objects not text. Allows rich data processing, filtering, and analysis.
* whoami
* Get-Process | Format-Table



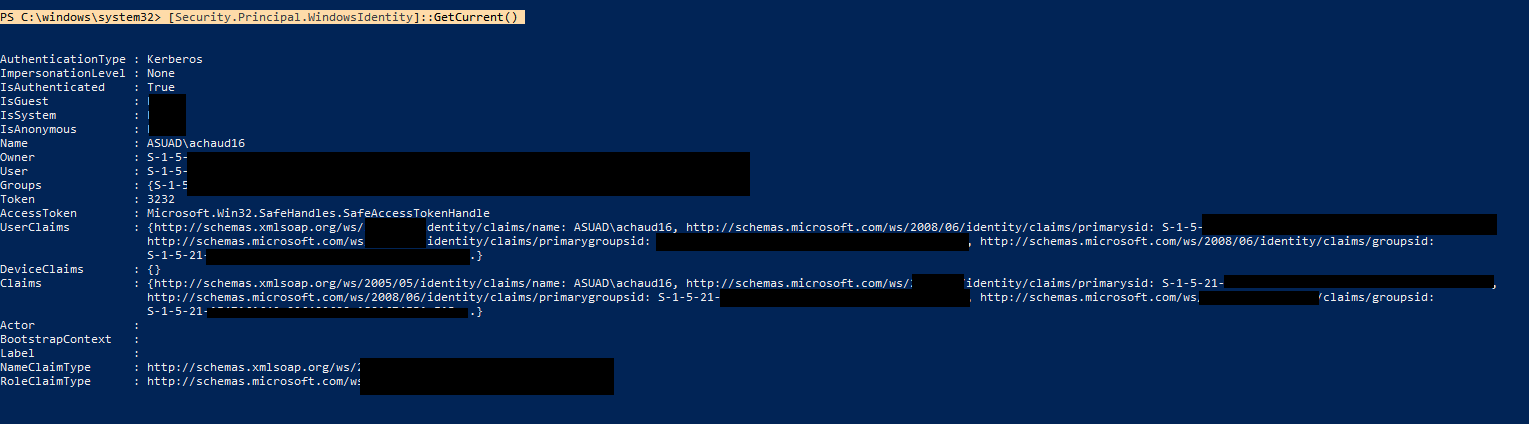
* Get-Process -name chrome | Stop-Process
* Get-Service | Get-Member

List of object methods and properties.



Admin Accounts and Blank Password

* Setting blank password applies to only local accounts, not to domain accounts,
* Remote access from one Windows computer to another using an account that is a member of the local Administrators group can only be performed if the account has a password.
* Access is denied when using a non-password admin account remotely.
* you can dump information about the current logged on user with this line:
* :[Security.Principal.WindowsIdentity]::GetCurrent()



Application, Service and Process

An **application** is a **program which you interact with on the desktop**. This is what you spend almost all of your time using on the computer. Internet explorer, Microsoft word, iTunes, skype - they are all applications.

A **process** is an **instance of a executable** (.exe program file) running. A given application may have several processes running simultaneously. For example, some modern browsers such as google chrome run several processes at once, with each tab actually being a separate instance/process of the same executable. In some cases, complicated applications may have multiple processes; for example, Visual Studio runs a separate process when it compiles code from when it displays the IDE. However, most often, a given application is running from a single process; for example, no matter how many microsoft word windows you have open, only a single instance of winword.exe is running.

A **service** is a **process which runs in the background** and does not interact with the desktop. In Windows, services almost always run as an instance of the svchost.exe process, the windows service host process; however, there are sometimes exceptions to this.

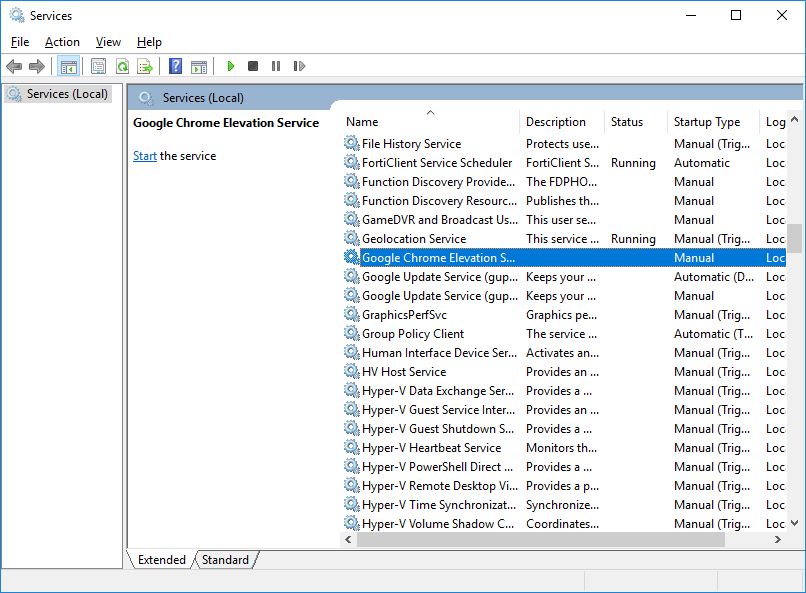
Sometimes, processes may run in the background without interacting with the desktop, but without being installed as a service. Many device drivers with enhanced features do this. For example, a touchpad driver will usually have a process which runs when a user logs in and handles the special features of the touchpad but isn't a service and doesn't show any windows to the user.

Sometimes an application may depend on a certain service. Printing from any program requires that the print spooler service be active. Installation packages (.msi installers) require that the windows installer service be running. Antivirus programs usually employ a service so they can continue running even when the user is not logged in.

Processes usually exit when an application is closed, however this is not always the case. Some programs, particularly download and backup programs, may continue to run in the background without displaying any windows. Antivirus is also an example of this - in addition to using a service, many antivirus applications run a process silently in the background which only displays an application to the user when action is required.

Services

Service is a program, routine, or process that performs a specific system function to support other programs or to provide a network service. A service runs in the system background without a user interface. Some examples include web serving, event logging, and file serving.



When you configure a service, you need to configure what account the service runs under. You can use the built-in accounts included with Windows or you can use a service account that you create locally or on the domain. Built-in accounts include:

Local System: – can access most resources on the local system.

NT Authority\LocalService: privileges of local Users group on the computer. When it accesses network resources, it uses no credentials and a null session.

NT Authority\NetworkService: Has same access level as Users group on the local computer. When it accesses network resources, it does so under the context of the local computer account.

Do not change the Allow service to interact with desktop settings, since this will allow the service to access any information displayed on interactive user’s desktop. Use account with minimum rights and permissions for the service to operate.

Read the description and properties of some of the services.

Registry

Central database in windows to store hardware, software configuration information, and system security policies. Components that use registry include Windows kernel, device drivers, setup programs, hardware profiles, and user profiles. Most of the times programs and applications make all necessary changes in the registry automatically. To make changes to the registry entries manually, use Registry Editor (regedit.exe). Registry keys are similar to folders, which contain values or subkeys.

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows refers to the subkey “Windows” of the subkey “Microsoft” of the subkey “Software” of the HKEY\_LOCAL\_MACHINE key.

Registry is split into several logical sections, referred as “hive”. Hives begin with HKEY, and are often abbreviated, e.g., HKCU is HKEY\_CURRENT\_USER and HKLM is HKEY\_LOCAL\_MACHINE.

HKEY\_CLASSES\_ROOT: stores information about registered applications, such as file associations – tells which default program opens file with certain extension.

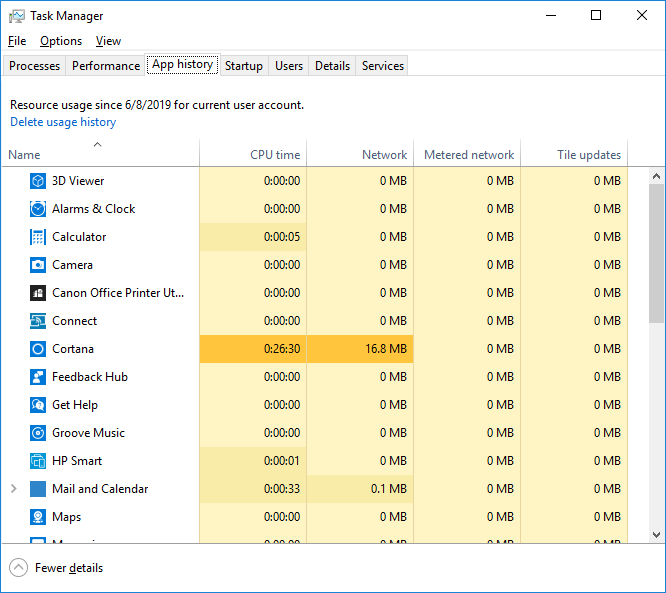
HKEY\_CURRENT\_USER: settings specific to currently logged in user. On the user log off, settings are saved to HKEY\_USERS.

HKEY\_LOCAL\_MACHINE: settings specific to local computer.

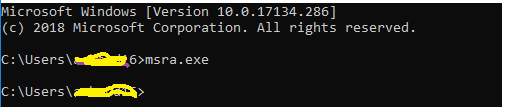
HKEY\_USERS: subkeys corresponding to HKEY\_CURRENT\_USER keys for each user profile actively loaded on the machine.

HKEY\_CURRENT\_CONFIG: information gathered at runtime. Generated at boot time, not stored permanently on the disk.

Task Manager

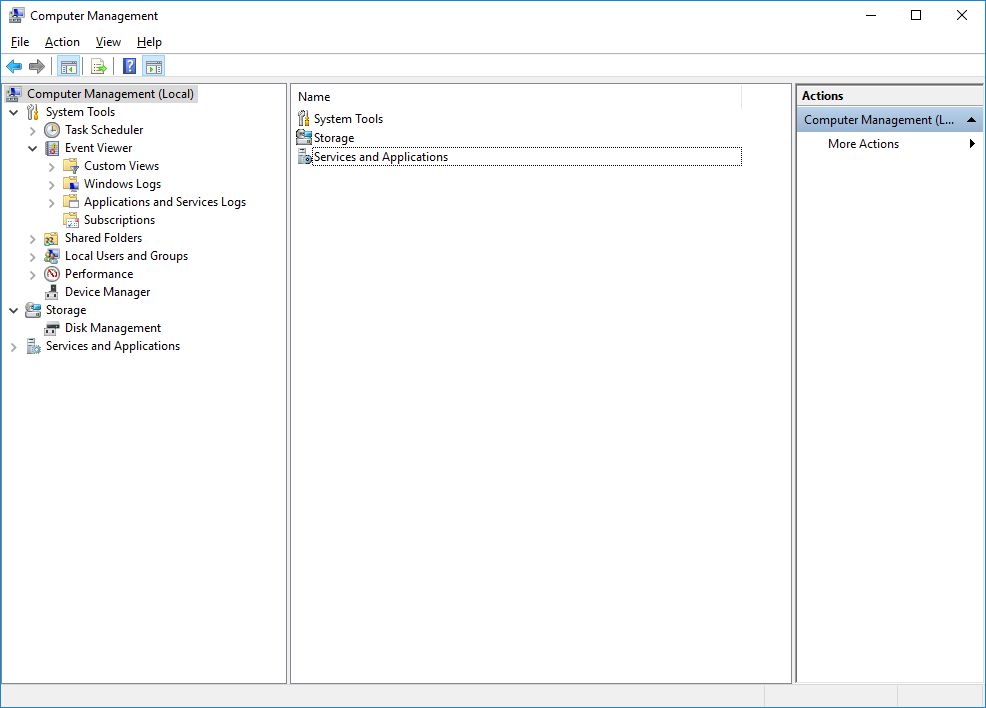


Windows Remote Assistance



Computer Management Console

Includes Task Scheduler, Event Viewer, Shared Folders, Local Users and Groups, Performance, Device Management, Routing and Remote Access, Services, and WMI Control. It can be opened through Administrative Tools or right-click MyComputer and clicking Manage. It is available in Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, and Windows 7

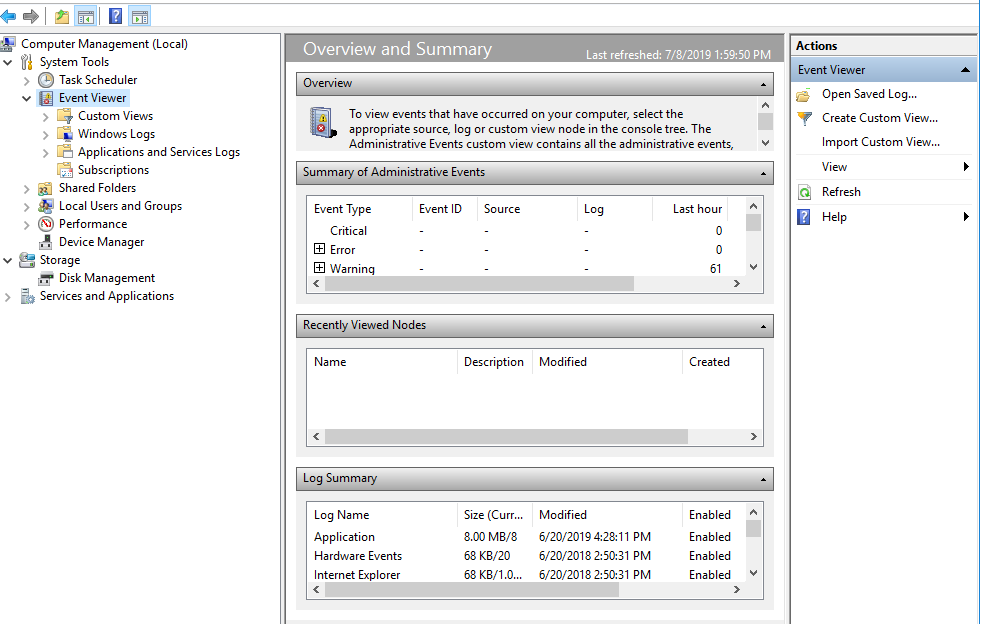


Server Manager Console

Remote Server Administration Tools pack is a feature available with Windows Server 2008R2 that enables remote management of Windows Server 2008 R2, Windows Server 2008, and, Windows Server 2003 from a computer running Windows Server 2008 R2, by allowing you to open and run management tools and snap-ins to manage roles, role services, or features on a remote computer. It includes AD Domain Services and AD Lightweight Directory Service (AD LDS), Hyper-V Tools, Web Server (IIS) Tools, DNS Server Tools, Network Policy and Access Service Tools

Monitoring and Troubleshooting

Event Viewer: Microsoft Management Console (MMC) tool that enables you to browse and manage event logs. It is included in the Computer Management and Server Manager MMC and is included in Administrative Tools as a stand-alone console. You can also execute the eventvwr.msc command. Event Viewer enables you to perform following tasks – view events from multiple event logs, save useful event filters as custom views, schedule task in response to event, create and manage event subscriptions.



Installing and Uninstalling Programs from Control Panel

**Windows Security Architecture**

Security Reference Monitor (SRM)

* access checks,
* generates audit log entries, and
* manipulates user rights, also called privileges.

Local Security Authority (LSA) – lsass.exe

* Issues security tokens to accounts
* Password policy, such as complexity rules and expiration times
* Auditing policy, or which operations on what objects to audit
* Privilege settings, or which accounts on a computer can perform privileged operations.

Security Account Manager (SAM)

* Account data and relevant security information about local principals and local groups
* User Login 🡪 SAM process (SamSrv) takes logon information and performs lookup in SAM DB in Windows System 32\config
* Passwords stored as MD4, PBKCS

Active Directory (AD)

* MS LDAP directory for security operations and account logon.
* All currently supported client versions of Windows, including Windows XP and Windows 7, can communicate with AD to perform security operations including account logon
* A windows client will authenticate using AD when user logs on to the computer using domain account.

Privileges in Windows

System wide permissions assigned to user accounts, e.g.,

* ability to backup computer (bypasses all access to perform complete backup),
* change time (can cause Kerberos authentication fail and lead to erroneous data being written to logging system).
* More than 45 privileges – some deemed dangerous.
* Act as part of OS privilege – account with this privilege can run code as part of trusted OS code. Granted only to Local system account – most dangerous privilege in Windows.
* Debug program privilege - allows debugging of processes running in Windows, user can run any code he wants in any process using this privilege.
* Backup files and directories privilege – process with this privilege can bypass Access Control List (ACL) checks and read all files for complete backup.
* Restore files and directory privilege is also able to bypass ACL.
* Bypass traverse checking – assigned to all user accounts by default – used as NTFS file system optimization. Deemed benign.

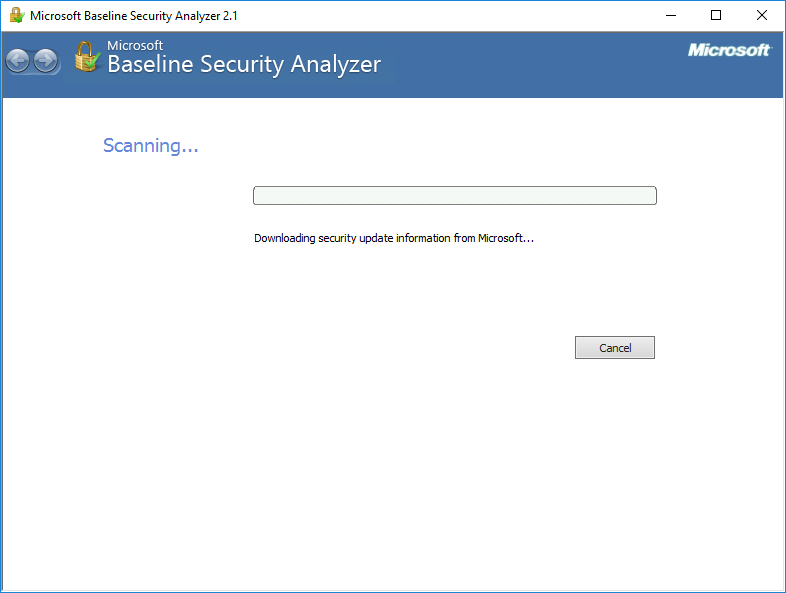
Access Control List

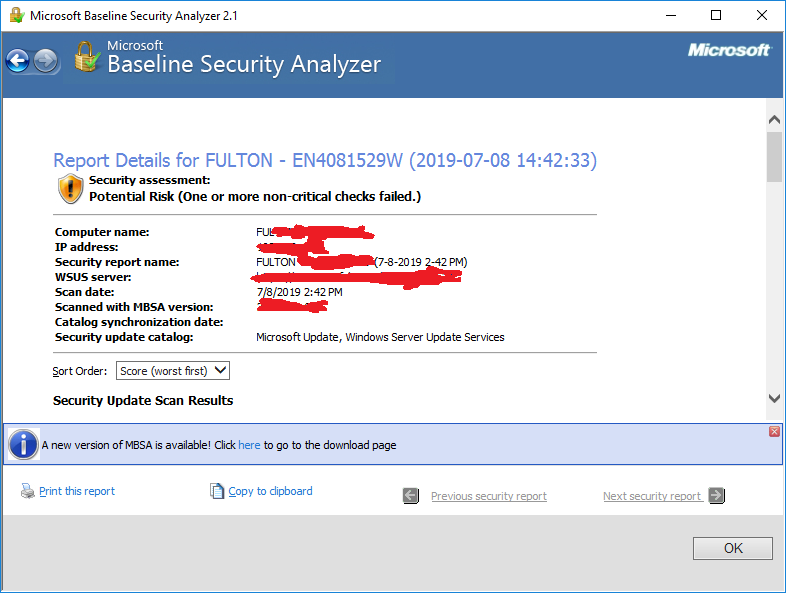
* Discretionary ACL (DACL) – grants or denies access to protected resources in Windows such as files, shared memory, named pipes.
* System ACL (SACL) – used for auditing and in enforcing mandatory integrity policy in some versions of Windows.

Microsoft Baseline Security Analyzer (MBSA)

Download the tools <https://www.microsoft.com/en-us/download/details.aspx?id=19892>

Install the .msi file





Microsoft Security Essentials

<https://www.microsoft.com/en-us/download/confirmation.aspx?id=5201>