GPO Vs Applocker Restrictions

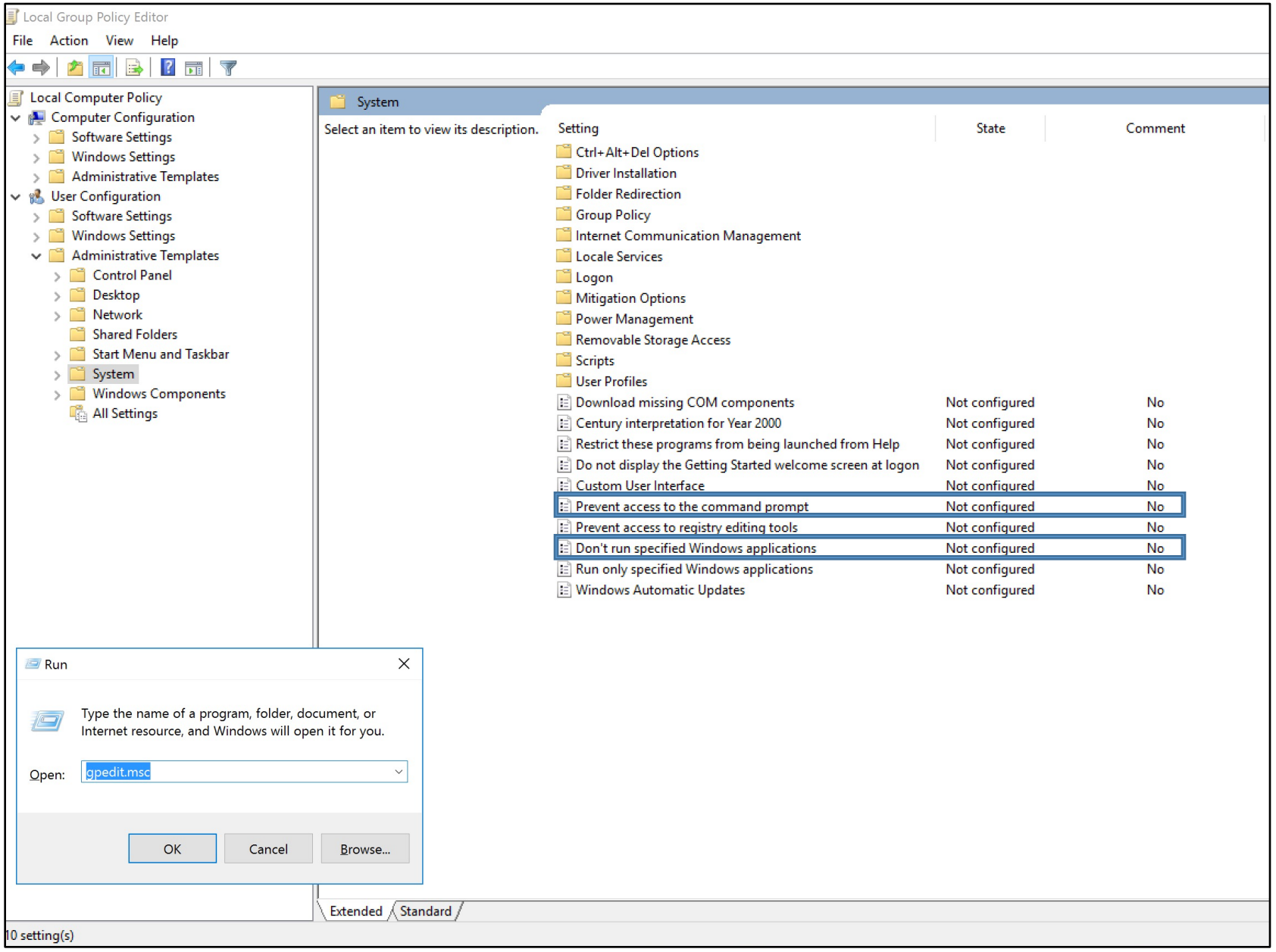
Pralhad Chaskar (@c0d3xpl0it)

What is GPO ?

- Group Policy, in part controls what users **can** and **cannot** do on a computer system: for example, to enforce a password complexity policy that prevents users from choosing an overly simple password, to allow or prevent unidentified users from remote computers to connect to a network share, to block access to the Windows Task Manager or to restrict access to certain folders.

- A set of such configurations is called a **Group Policy Object** (GPO).

GPO Settings

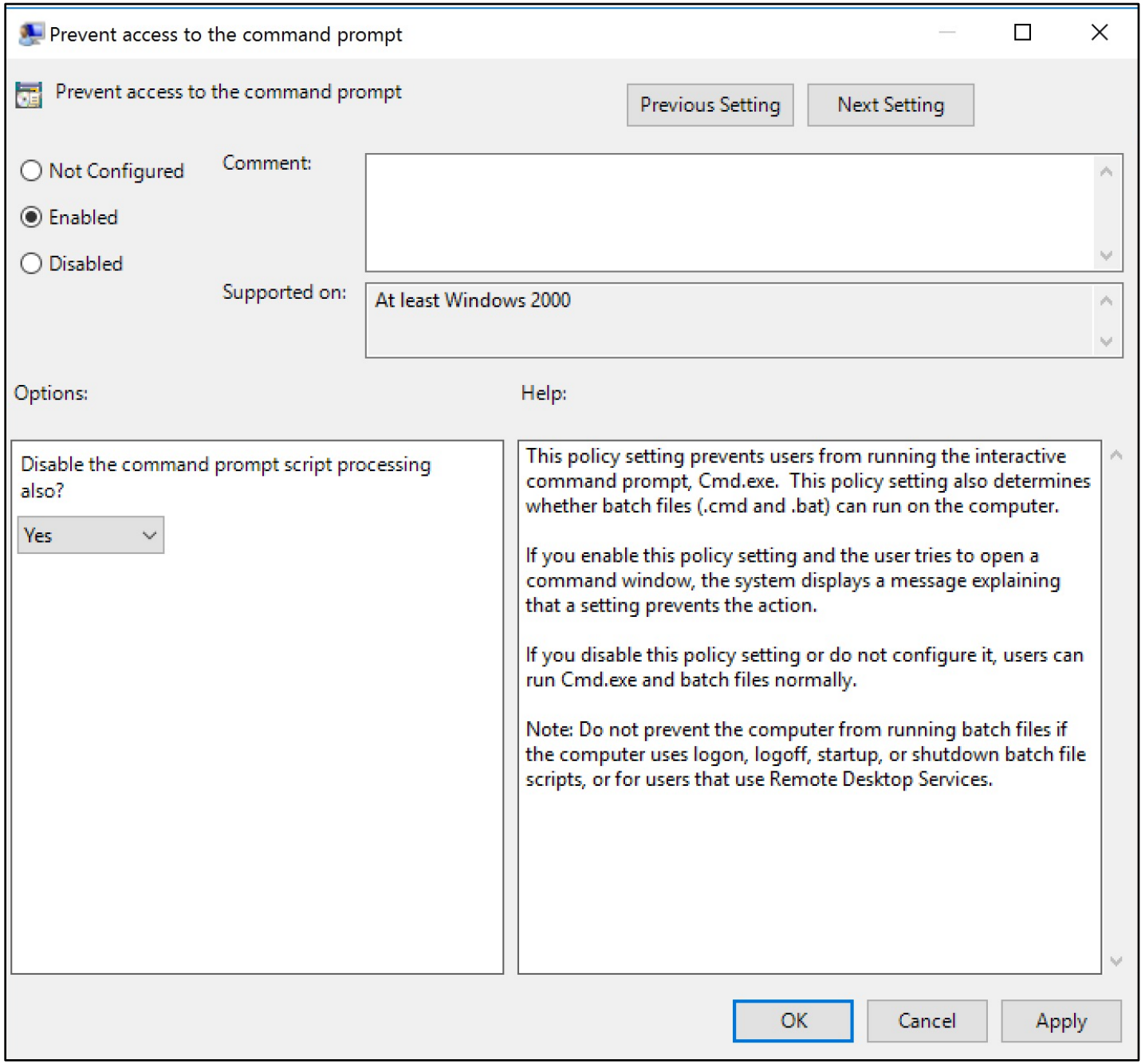


Today we cover below GPO Settings

- Prevent access to the command prompt
  - Blocking CMD.EXE

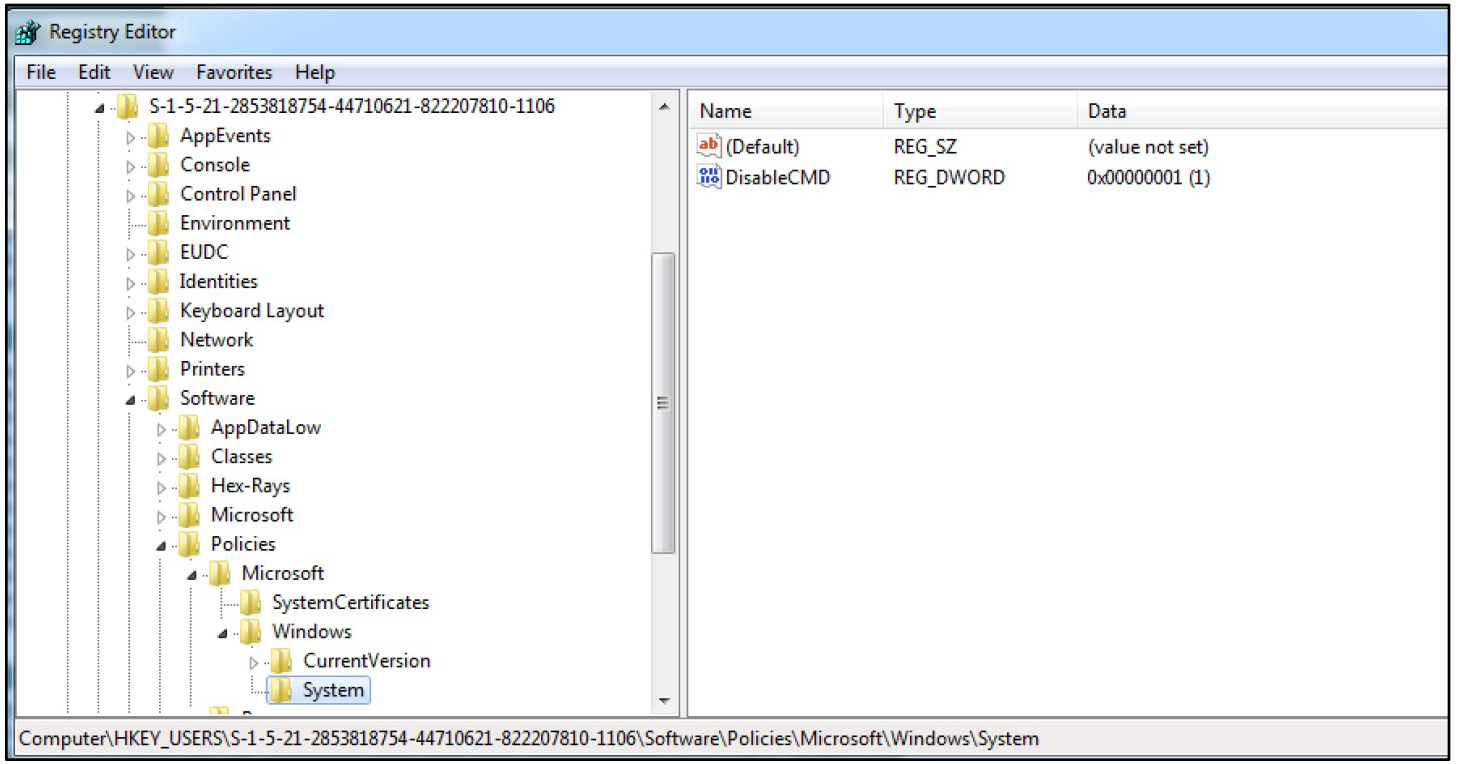
- Don’t run specified Windows applications
  - Blocking POWERSHELL.EXE, POWERSHELL_ISE.EXE, MSBUILD.EXE, RUNDLL32.EXE, BGINFO.EXE, MSIEXEC.EXE, ATBROKER.EXE, TRACKER.EXE, INSTALLUTIL.EXE, CDB.EXE, REGSVR32.EXE, REGASM.EXE, CSC.EXE, ETC.

Prevent access to the command prompt

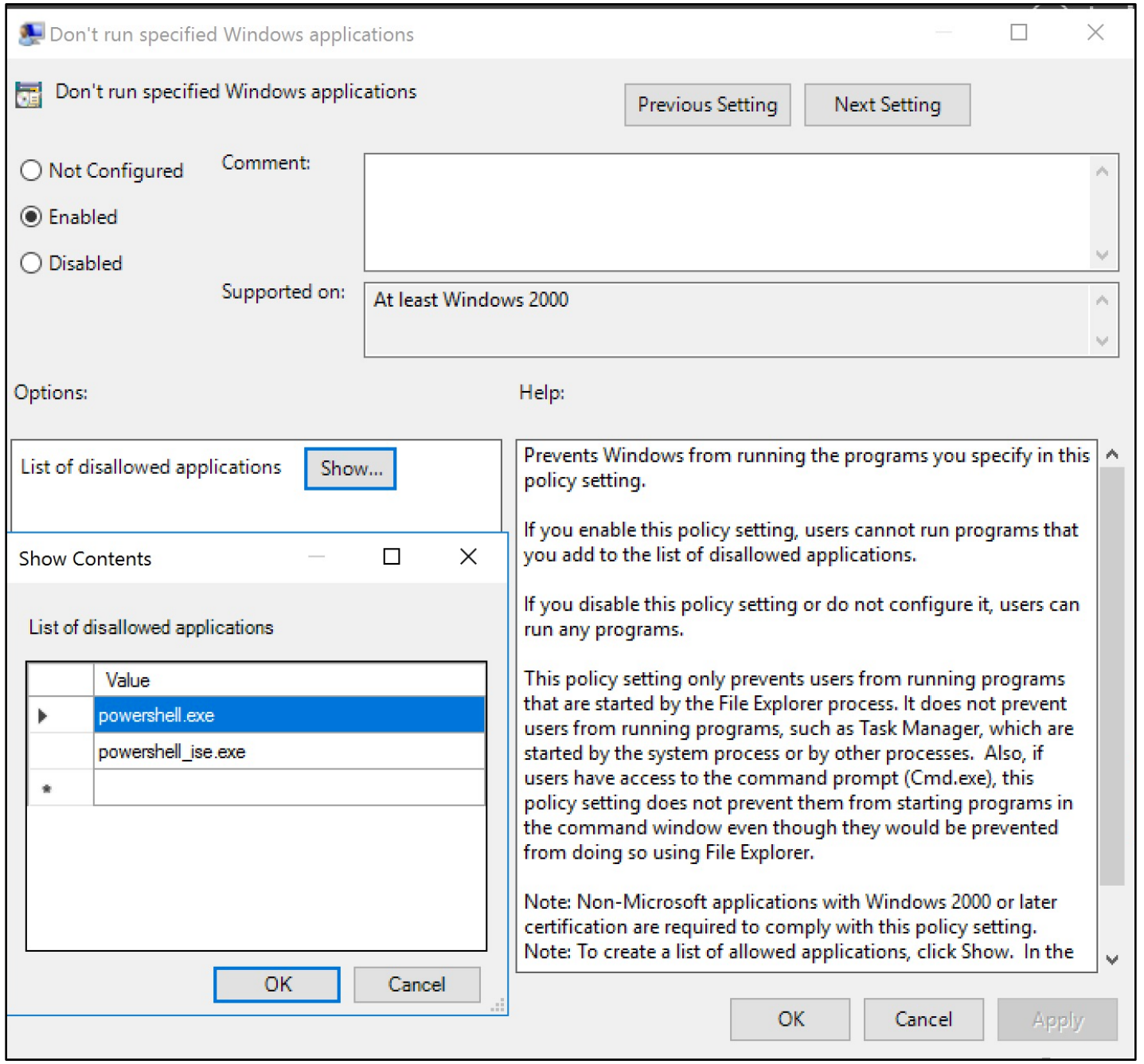


Registries added

- HKU\S-1-5-21-2853818754-44710621-822207810-1106\Software\Policies\Microsoft\Windows\System\DisableCMD: 0x00000001

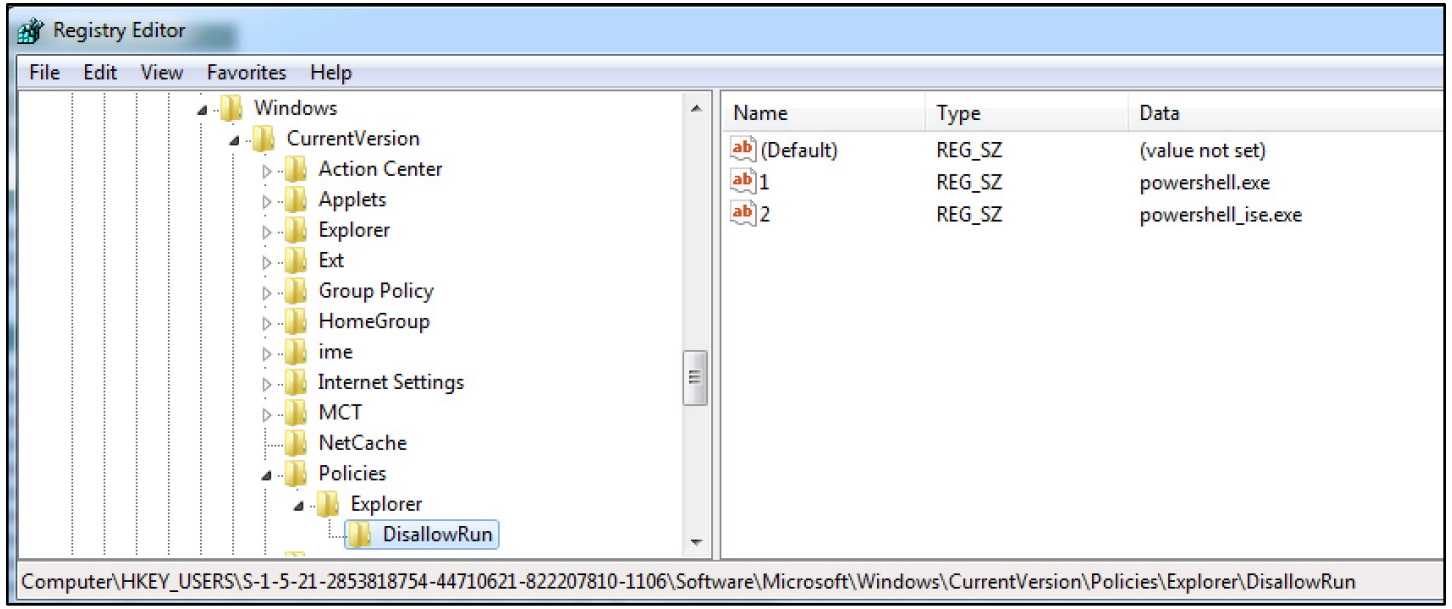


Don’t run specified Windows applications



Registries added

- HKU\S-1-5-21-2853818754-44710621-822207810-1106\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun: 0x00000001
- HKU\S-1-5-21-2853818754-44710621-822207810-1106\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun\1: "powershell.exe”
- HKU\S-1-5-21-2853818754-44710621-822207810-1106\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\DisallowRun\2: "powershell_ise.exe"



Demo time!

Can above settings be bypassed ?

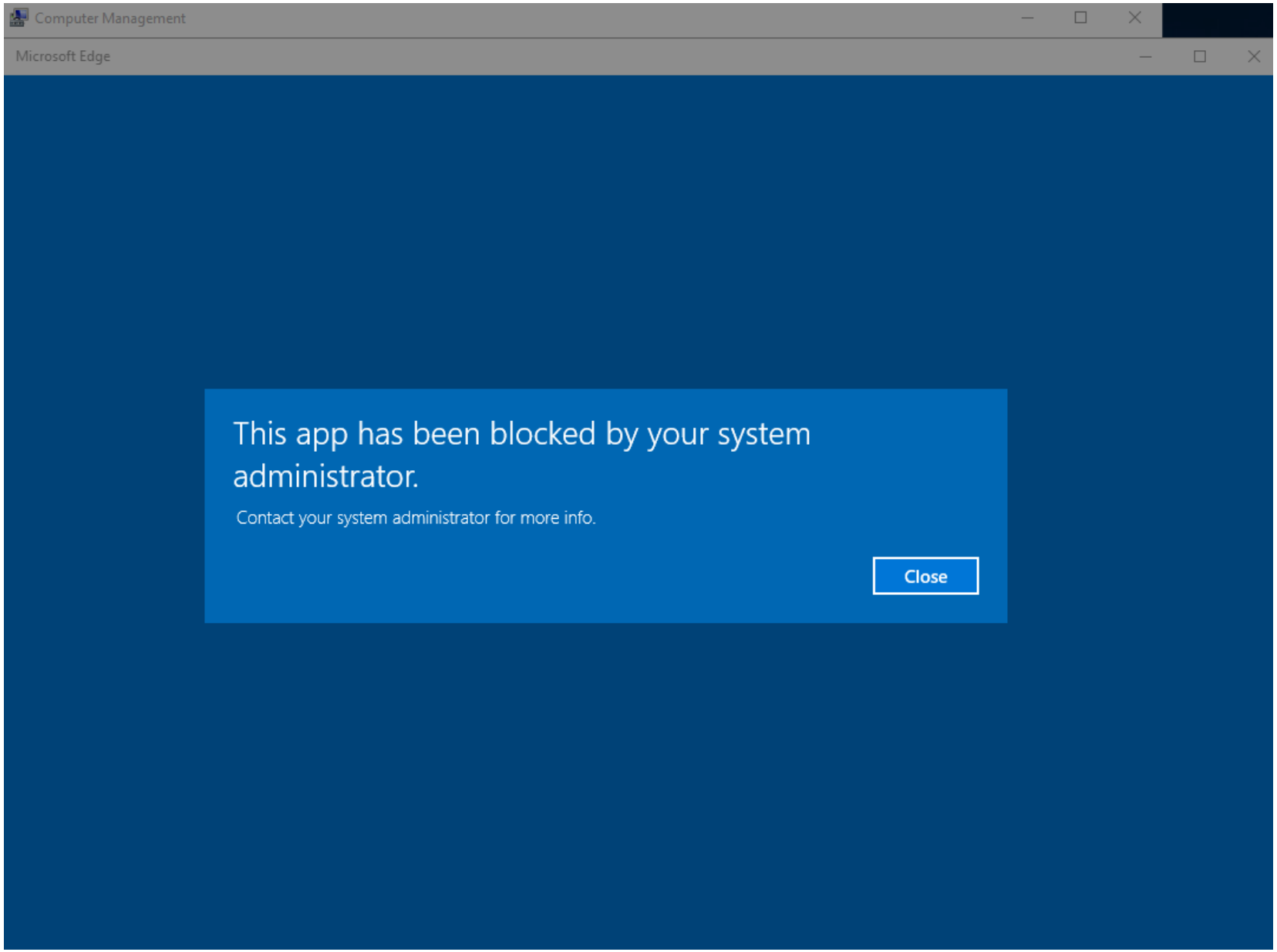
Demo time!

GPO Settings - Bypass

- Prevent access to the command prompt
  - Attacker can still access command prompt functions using ReactOS CMD.exe (Thank you Didier Stevens)

- Don’t run specified Windows applications
  - Attacker can still access powershell.exe by calling through cmd.exe
  - Renaming powershell.exe and running from desktop

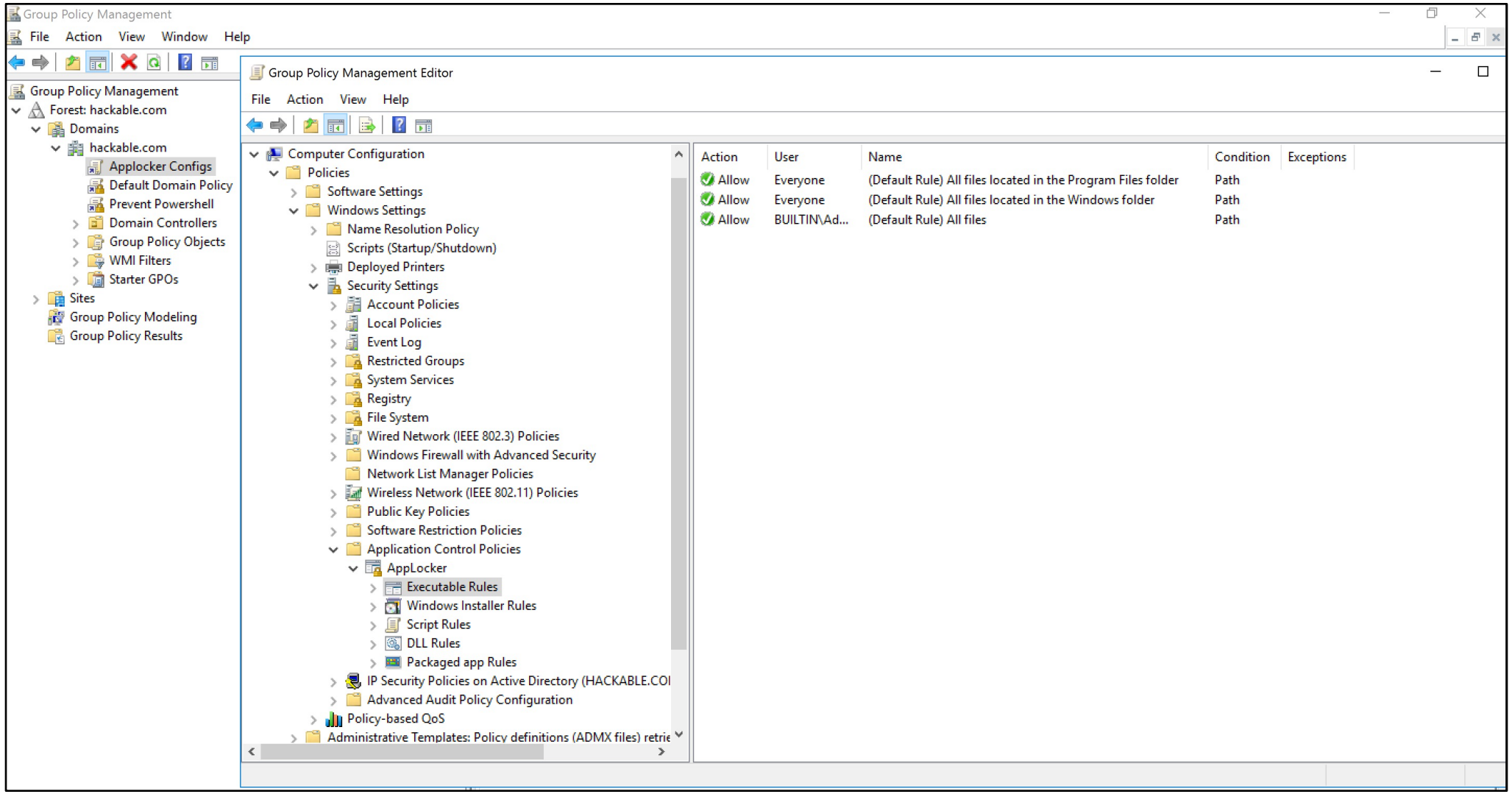
Applocker


Computer Management
Microsoft Edge
This app has been blocked by your system administrator.
Contact your system administrator for more info.
Close

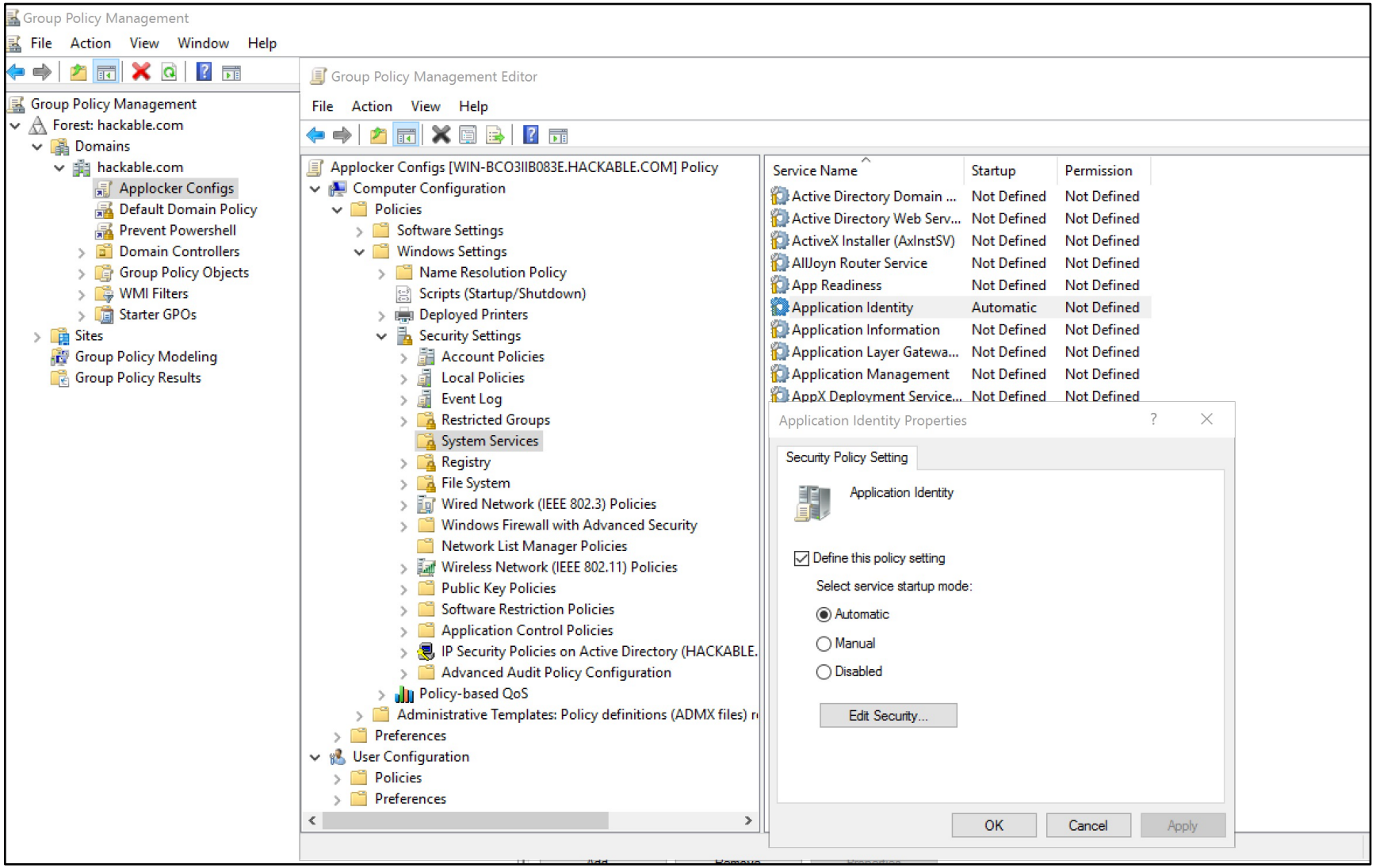
What is Applocker ?

- **AppLocker** is a new feature in Windows 7, Windows Server 2008 R2 and above that allows you to specify which users or groups can run particular applications in your organization based on unique identities of files. If you use AppLocker, you can create rules to **allow** or **deny** applications from running.

Configuring Applocker Default Rules



Service to be enabled



Lets see default rules block which binaries

- Below is sample list binaries that can be abused by attacker/adversary
  - Regsvr32.exe
  - Msbuild.exe
  - Rundll32.exe
  - Regsvcs.exe
  - Regasm.exe
  - Bginfo.exe
  - InstallUtil.exe
  - mshta.exe
  - IEExec.exe
  - cdb.exe
  - msiexec.exe
  - cmstp.exe
  - MavInject32.exe
  - odbcconf.exe
  - ….more other which we are unware ☹

Rundll32.exe

- **Rundll32** is a Microsoft binary that can execute code that is inside a DLL file. Since this utility is part of the Windows operating system it can be used as a method in order to bypass AppLocker rules or Software Restriction Policies.
- So if the environment is not properly lockdown and users are permitted to use this binary then they can write their own DLL's and bypass any restrictions or execute malicious JavaScript code.

MSBuild.exe

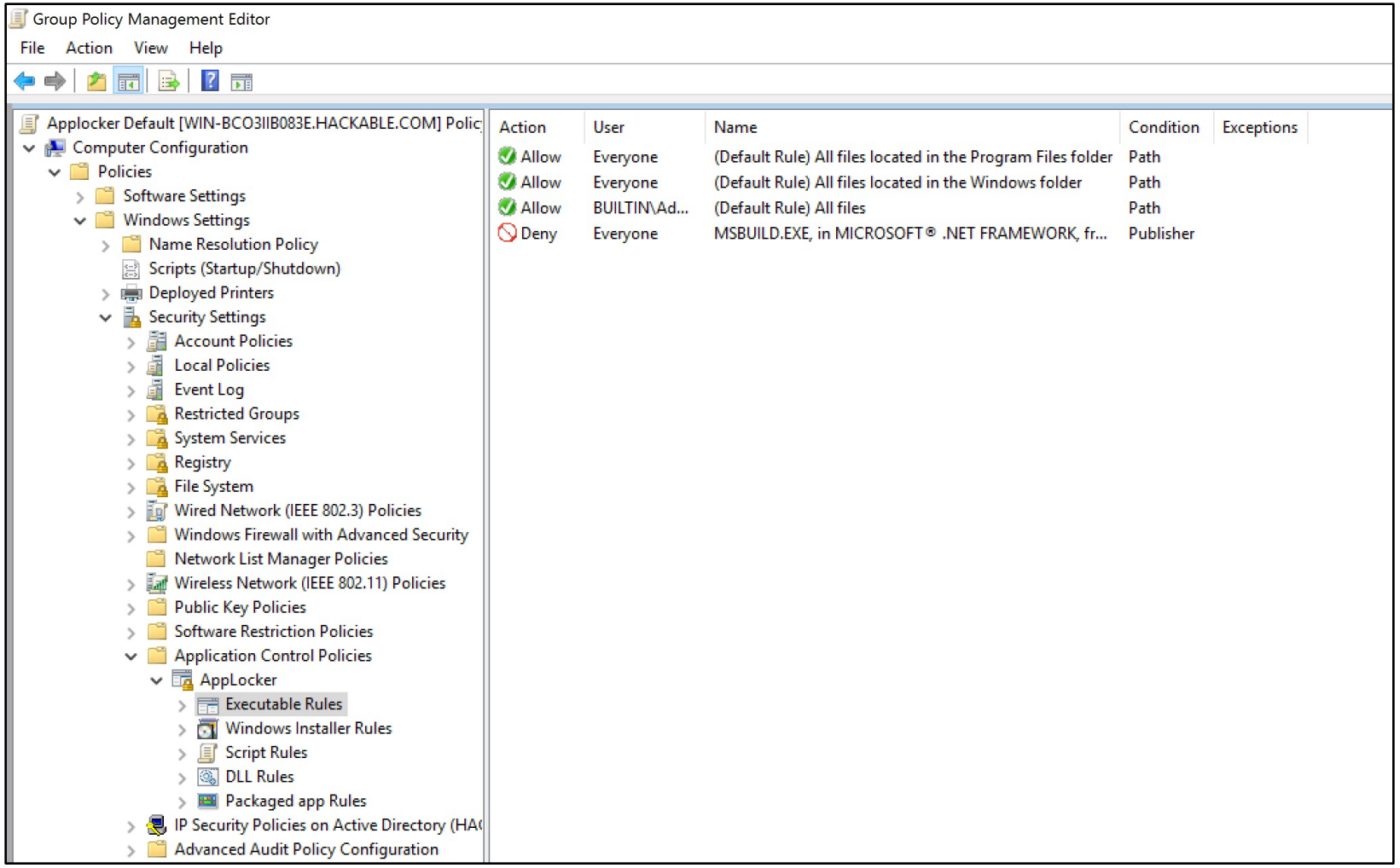
- **MSBuild.exe** (Microsoft Build Engine) is a software build platform used by Visual Studio. It takes XML formatted project files that define requirements for building various platforms and configurations.
- Adversaries can use MSBuild to proxy execution of code through a trusted Windows utility. The inline task capability of MSBuild that was introduced in .NET version 4 allows for C# code to be inserted into the XML project file. MSBuild will compile and execute the inline task. MSBuild.exe is a signed Microsoft binary, so when it is used this way it can execute arbitrary code and bypass application whitelisting defenses that are configured to allow MSBuild.exe execution.

Lets run Rundll32.exe and MSBuild.exe against default Applocker rules

Demo time!

MSBuild.exe bypassed default rules

Configuring Applocker to block MSBuild.exe

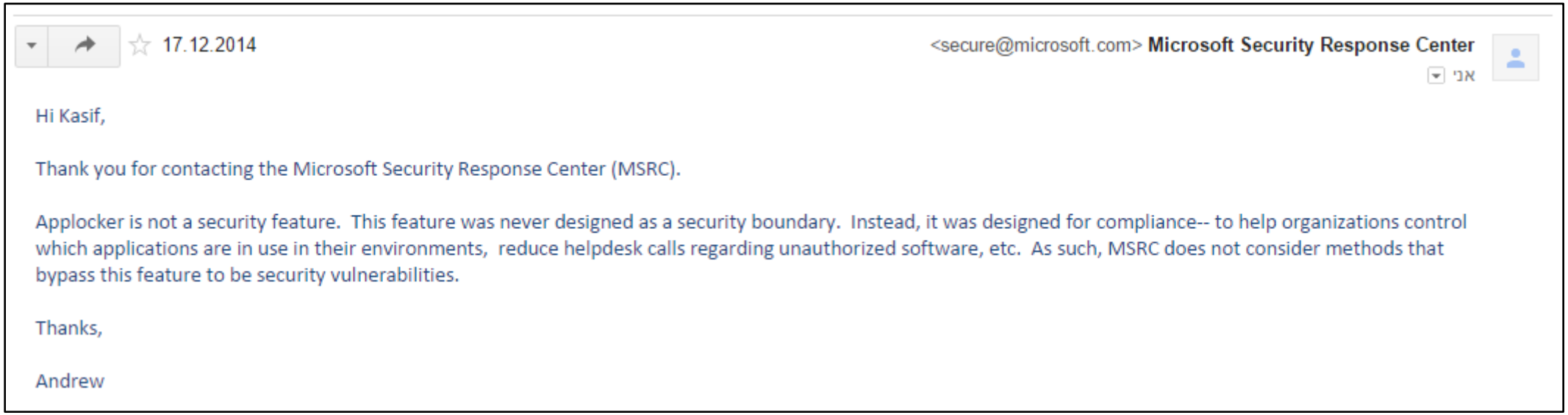


Demo time!

Summary

- Applocker is not a security feature
- Restrictions implemented by GPO are different from Applocker
- Review your defaults before implementing Applocker
- More research to follow this session....

Microsoft’s Response to Applocker Bypasses



17.12.2014

<secure@microsoft.com> **Microsoft Security Response Center**

אני

Hi Kasif,

Thank you for contacting the Microsoft Security Response Center (MSRC).

Applocker is not a security feature. This feature was never designed as a security boundary. Instead, it was designed for compliance-- to help organizations control which applications are in use in their environments, reduce helpdesk calls regarding unauthorized software, etc. As such, MSRC does not consider methods that bypass this feature to be security vulnerabilities.

Thanks,

Andrew

Reference :- https://github.com/kasif-dekel/Microsoft-Applocker-Bypass

Information security is always an arms race !!

References

- https://oddvar.moe/
- https://pentest.blog
- https://github.com/redcanaryco/atomic-red-team


THANK
YOU FOR
LISTENING
ANY
QUESTIONS?