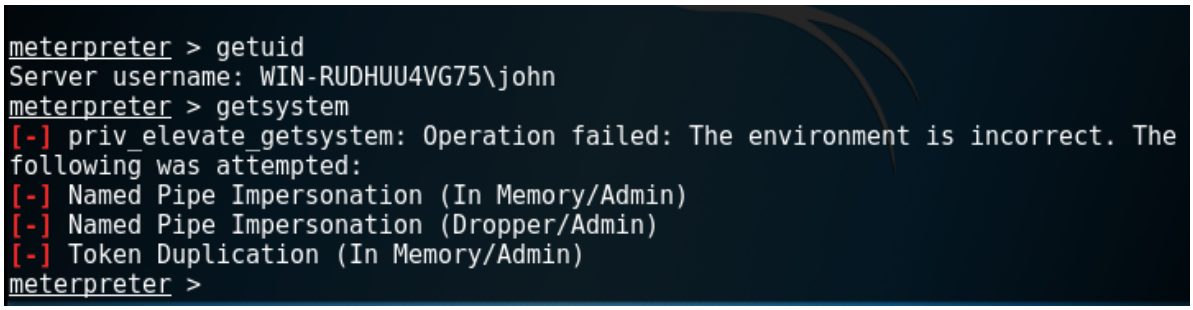
UAC Bypass – Event Viewer

pentestlab.blog/category/red-team/page/119

May 2, 2017

User account control was developed by Microsoft in order to restrict unauthorized applications to be executed with administrator level privileges unless the administrator supplies his password to allow elevation. In penetration testing this means that privilege escalation can be stopped through Meterpreter due to UAC.



UAC Prevents Privilege Escalation

Matt Nelson discovered and explained in his blog that it is possible to bypass UAC by abusing a native Windows service such as Event Viewer by hijacking a registry key. This can be achieved due to the fact that the process of Event Viewer (eventvwr.exe) is running as a high integrity level and because Event Viewer is loading through Microsoft Management Console via the registry.

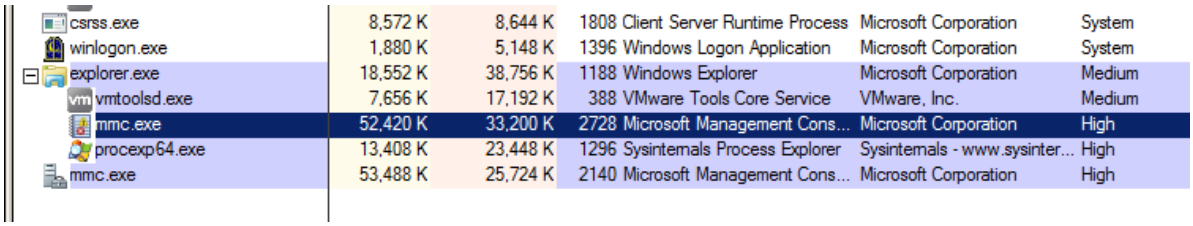
Manually

In newer versions of Windows (Vista and later) processes are running at three different levels of integrity. These three levels determine under which privileges a process is running:

- High // Administrator Rights
- Medium // Standard User Rights
- Low // Restricted

Process Explorer can be used to determine the integrity level of a process. Two things can be identified by checking the Windows processes while Event Viewer is running:

- Event Viewer is loading through Microsoft Management Console (mmc.exe)
- Event Viewer is running as a High Integrity Process

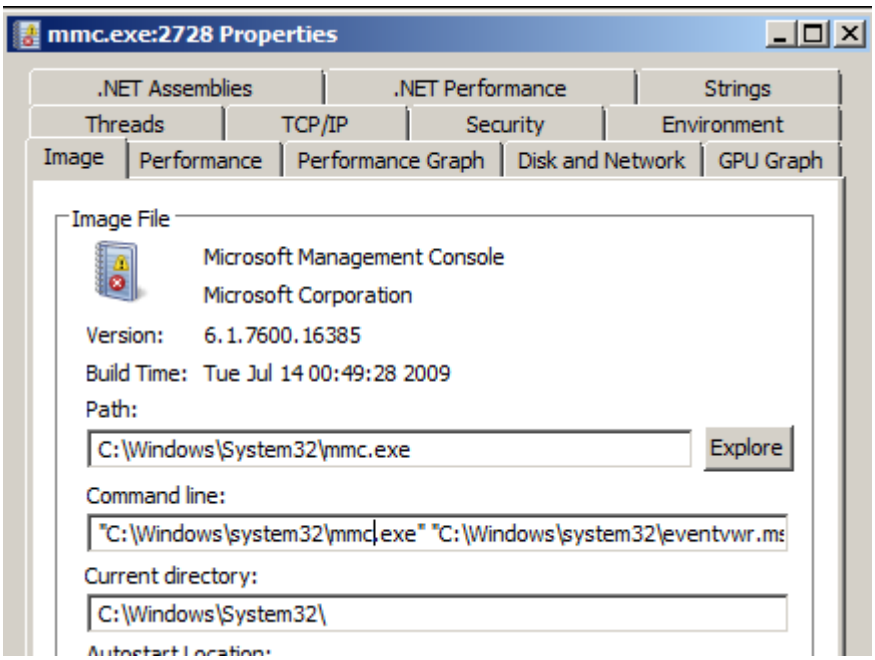


Event Viewer Process – High Integrity

Specifically what is really happens behind the scenes when eventvwr.exe is executed is that it tries to find mmc.exe in these two registry locations:

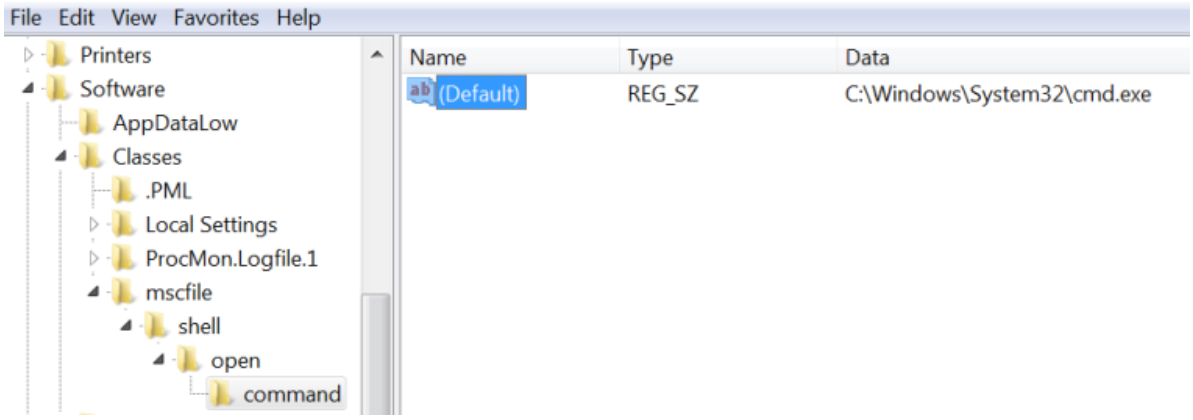
- **HKCU\Software\Classes\mscfile\shell\open\command**
- **HKCR\mscfile\shell\open\command**

The first registry location doesn't exist so mmc.exe is executed from the second location which then loads the eventvwr.msc file in order to display the information to the user.



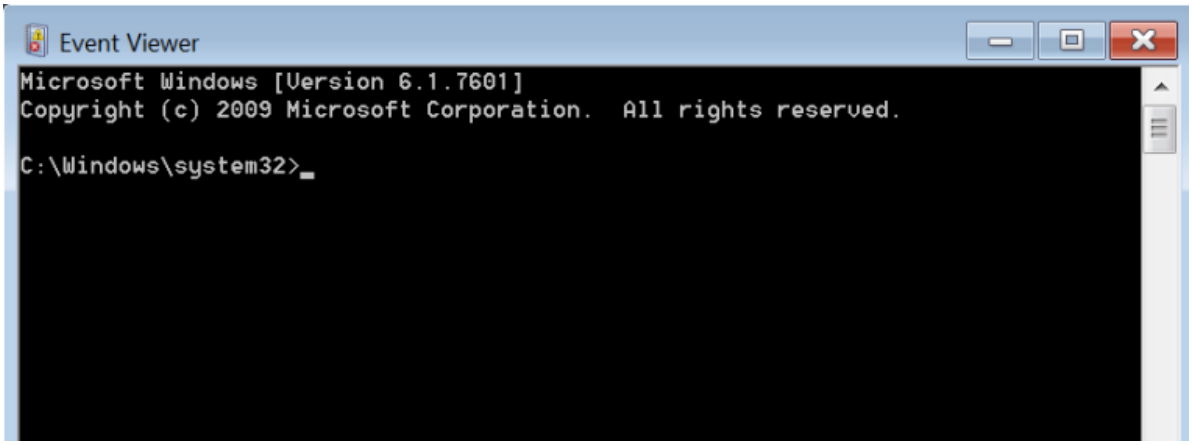
MMC and Event Viewer

Therefore it is possible for an attacker to create the registry location that doesn't exist in order to execute a process with High level integrity bypassing in that way the User Account Control (UAC).



Elevated CMD via Event Viewer

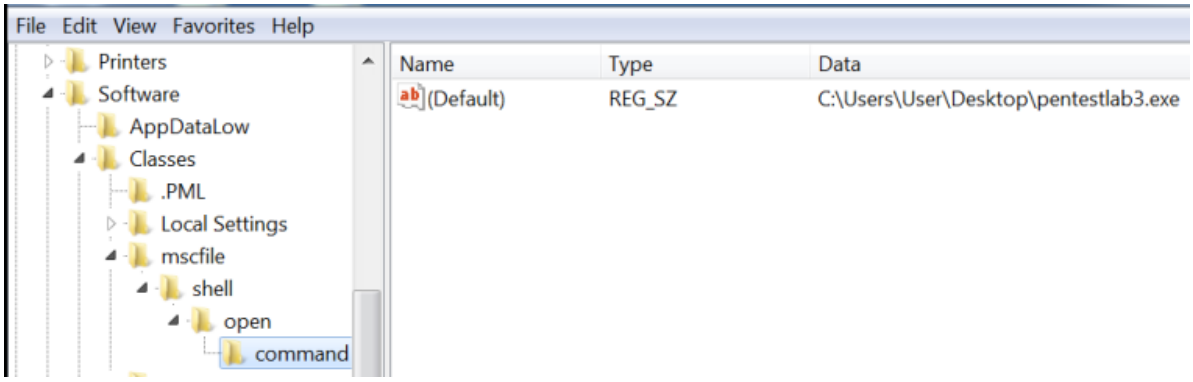
When the eventvwr.exe will be executed the command prompt will be opened directly without requiring any elevation from the UAC.



Bypass UAC via Event Viewer

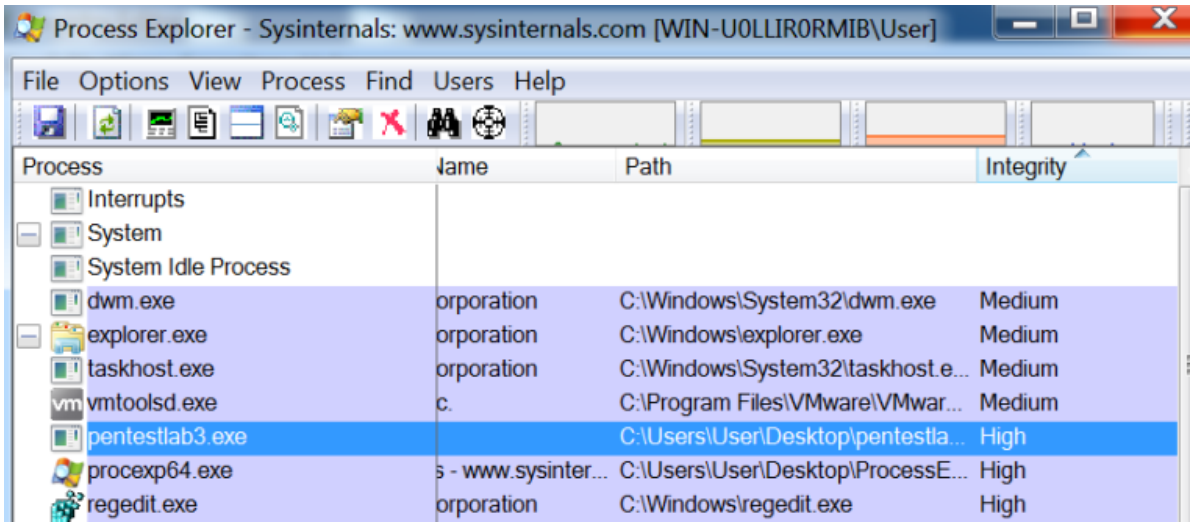
This technique is considered very stealthy since it doesn't touches the disk and it doesn't do any process injection avoiding the risk of being discovered by an antivirus or a security solution that monitors the behaviour of processes.

However a malicious and undetectable payload can be used as well instead of command prompt in order to get a proper Meterpreter session and escalate privileges with one of the techniques that Meterpreter is using via getsystem command.



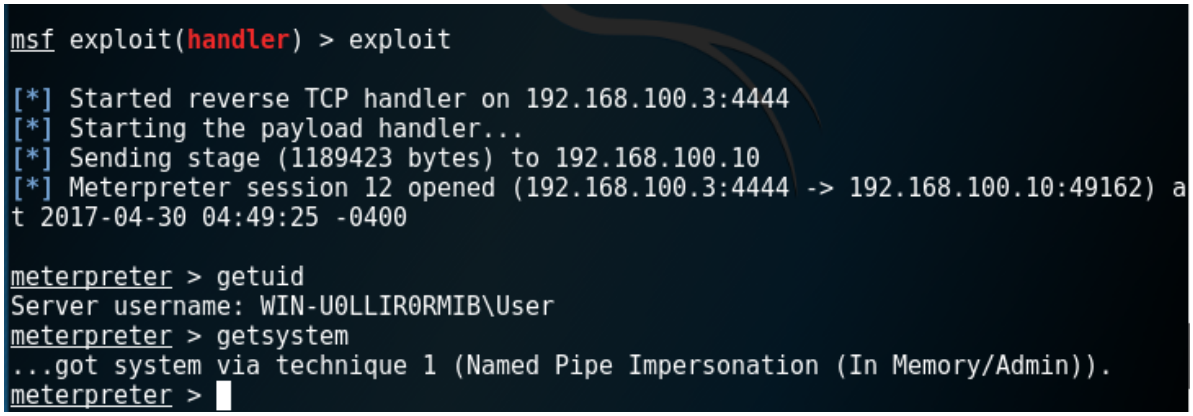
Custom Payload – Registry

Process Explorer can verify the integrity level of pentestlab3.exe process which again runs as high:



pentestlab3 – Running as High Integrity Process

Metasploit module **handler** will capture the elevated Meterpreter session which from then privilege escalation is possible since user account control is already bypassed.

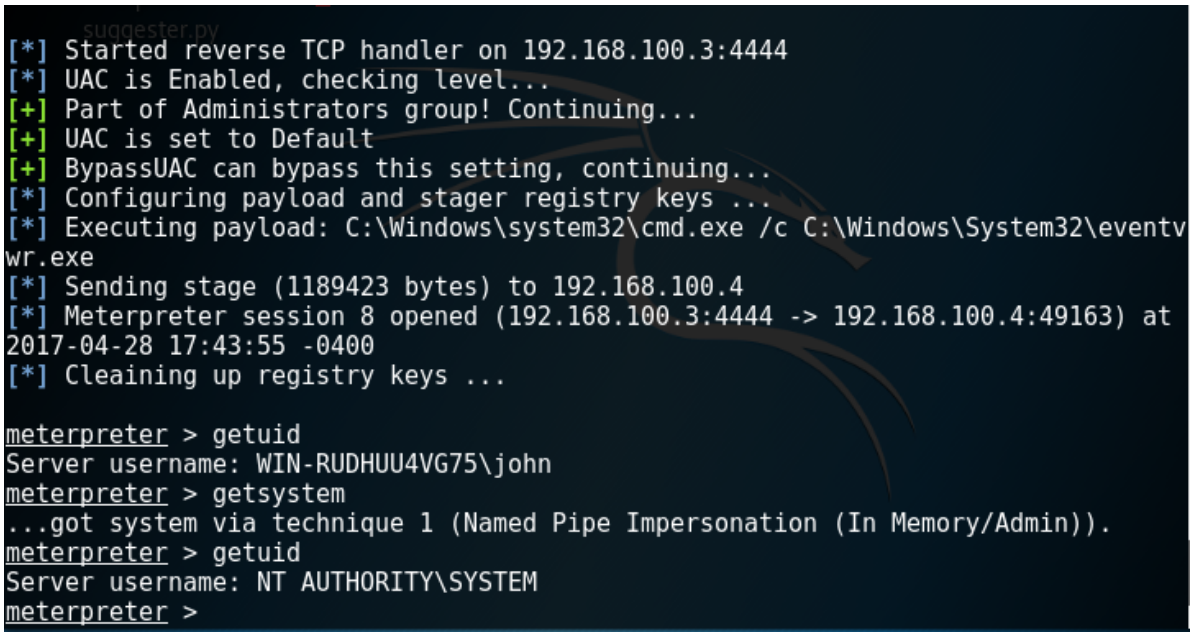


Pentestlab3 – Elevated Meterpreter

Metasploit

Alternatively there is a Metasploit module which automates this process above returns an elevated Meterpreter session.

```
exploit/windows/local/bypassuac_eventvwr
```



Metasploit – UAC Bypass via Event Viewer

Resources

"Fileless" UAC Bypass Using eventvwr.exe and Registry Hijacking

https://github.com/enigma0x3/Misc-PowerShell-Stuff/blob/master/Invoke-EventVwrBypass.ps1

https://www.rapid7.com/db/modules/exploit/windows/local/bypassuac_eventvwr

https://github.com/mdsecresearch/Publications/blob/master/tools/redteam/cna/eventvwr.cna