

Table of Contents

Table of Contents.....	2
Introduction.....	5
Run Key Current User.....	5
Run Key Local Machine.....	8
To Test:.....	9
RunOnce Key.....	11
RunOnce Key (Current User).....	11
Explanation:.....	12
Proof of Concept.....	13
RunOnce Key (Local Machine).....	13
Explanation:.....	14
Summary:.....	15
Autostart Service.....	15
Startup Directory.....	18
Code.....	19
Explanation of the Code.....	20
Proof of Concept.....	20
WMI Task Scheduler.....	22
Key Advantages of WMI Persistence:.....	22
Creating a WMI Task.....	22
Code:.....	22
Code Breakdown.....	24
How It Works.....	25
Proof of Concept.....	25
Resurrector.....	26
Components.....	26
How to Store an EXE in the Registry.....	29
Retrieving the File from the Registry.....	33
Code.....	33
1. Function: runProcAsAdminFromUser.....	46
2. Function: persistenceViaRunKeys.....	46
3. Function: isProcessRunning.....	47
4. Function: existsFile.....	47
5. Function: existsRegistryKey.....	47
6. Function: WriteCallback.....	47
7. Function: DoesRegistryEntryExist.....	47
8. Main Function.....	48
Proof of Concept.....	48
DLL Proxying.....	50
Basic Concept:.....	50

How It Works:.....	50
Key Differences from DLL Hijacking:.....	51
Code Examples.....	51
Vulnerable Processes.....	53
Exercise -> Persistence Mechanism Targeting Specific Applications.....	53
Conclusions.....	54