

Finding Privilege Escalations with strace & SysInternals

@ OWASP Stammtisch Stuttgart 06.11.2017

- Diplom Mathematiker (FH)
- Administrator – Developer – Architect – Penetration-Tester
- Some 0days
- Certificates: OSCP, OSWP, OSCE, ISO27001 Foundation
- Founder of Ungeheuer IT UG (haftungsbeschränkt)

Ungeheuer IT

- Sitz in Rülzheim
(Between Karlsruhe and Mannheim)
- Any kind of Penetrationtests
- Kunden aus den Bereichen
 - Kommunen
 - Versicherungen
 - Banken
 - Industrie
 - Kritische Infrastrukturen



DAIMLER



Agenda

1. Some Basics
2. Sysinternals & Procmon
3. Strace

Basics

Basics

What is Privilege Escalation?

„**Privilege escalation** is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.“

Wikipedia

Basics



You Start Here



Your Target

SysInternals

the Windows part

Sysinternals

What is Sysinternals?

Windows Sysinternals is a part of the Microsoft TechNet website which offers technical resources and utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment.

- *Wikipedia*

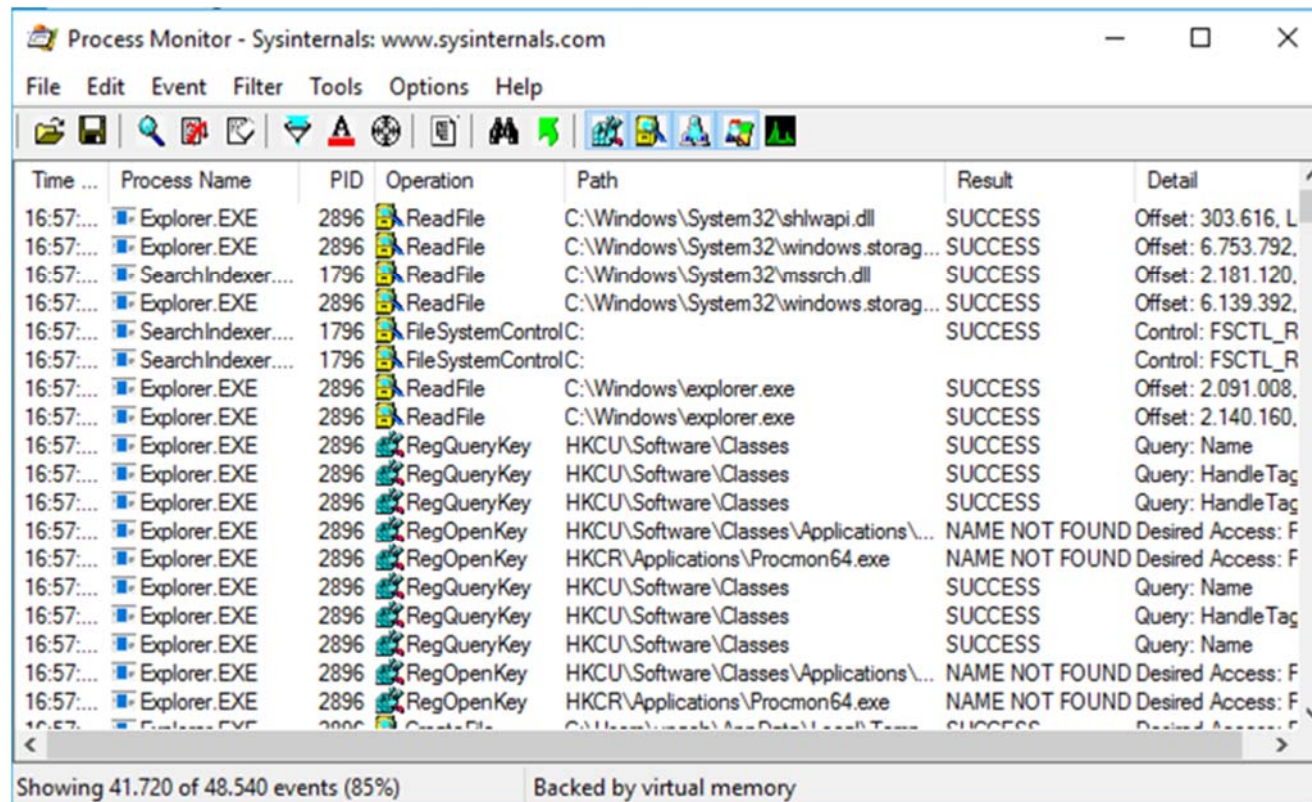
Lots of nice tools

AccessChk	AccessEnum	AdExplorer	AdInsight	AdRestore
Autologon	Autoruns	BgInfo	CacheSet	ClockRes
Contig	Coreinfo	Ctrl2Cap	DebugView	Desktops
Disk2vhd	DiskExt	DiskMon	DiskView	Disk Usage (DU)
EFSDump	FindLinks	Handle	Hex2dec	Junction
LDMDump	ListDLLs	LiveKd	LoadOrder	LogonSessions
MoveFile	NTFSInfo	PendMoves	PipeList	PortMon
ProcDump	Process Explorer	Process Monitor	PsExec	PsFile
PsGetSid	PsInfo	PsPing	PsKill	PsList
PsLoggedOn	PsLogList	PsPasswd	PsService	PsShutdown
PsSuspend	RAMMap	RegDelNull	Registry Usage (RU)	RegJump
SDelete	ShareEnum	ShellRunas	Sigcheck	Streams
Strings	Sync	Sysmon	TCPView	VMMMap
VolumelD	Whols	WinObj	ZoomIt	

Lots of nice tools

AccessChk	AccessEnum	AdExplorer	AdInsight	AdRestore
Autologon	Autoruns	BgInfo	CacheSet	ClockRes
Contig	Coreinfo	Ctrl2Cap	DebugView	Desktops
Disk2vhd	DiskExt	DiskMon	DiskView	Disk Usage (DU)
EFSDump	FindLinks	Handle	Hex2dec	Junction
LDMDump	ListDLLs	LiveKd	LoadOrder	LogonSessions
MoveFile	NTFSInfo	PendMoves	PipeList	PortMon
ProcDump	Process Explorer	Process Monitor	PsExec	PsFile
PsGetSid	PsInfo	PsPing	PsKill	PsList
PsLoggedOn	PsLogList	PsPasswd	PsService	PsShutdown
PsSuspend	RAMMap	RegDelNull	Registry Usage (RU)	RegJump
SDelete	ShareEnum	ShellRunas	Sigcheck	Streams
Strings	Sync	Sysmon	TCPView	VMMMap
VolumeID	Whols	WinObj	ZoomIt	

ProcMon - GUI



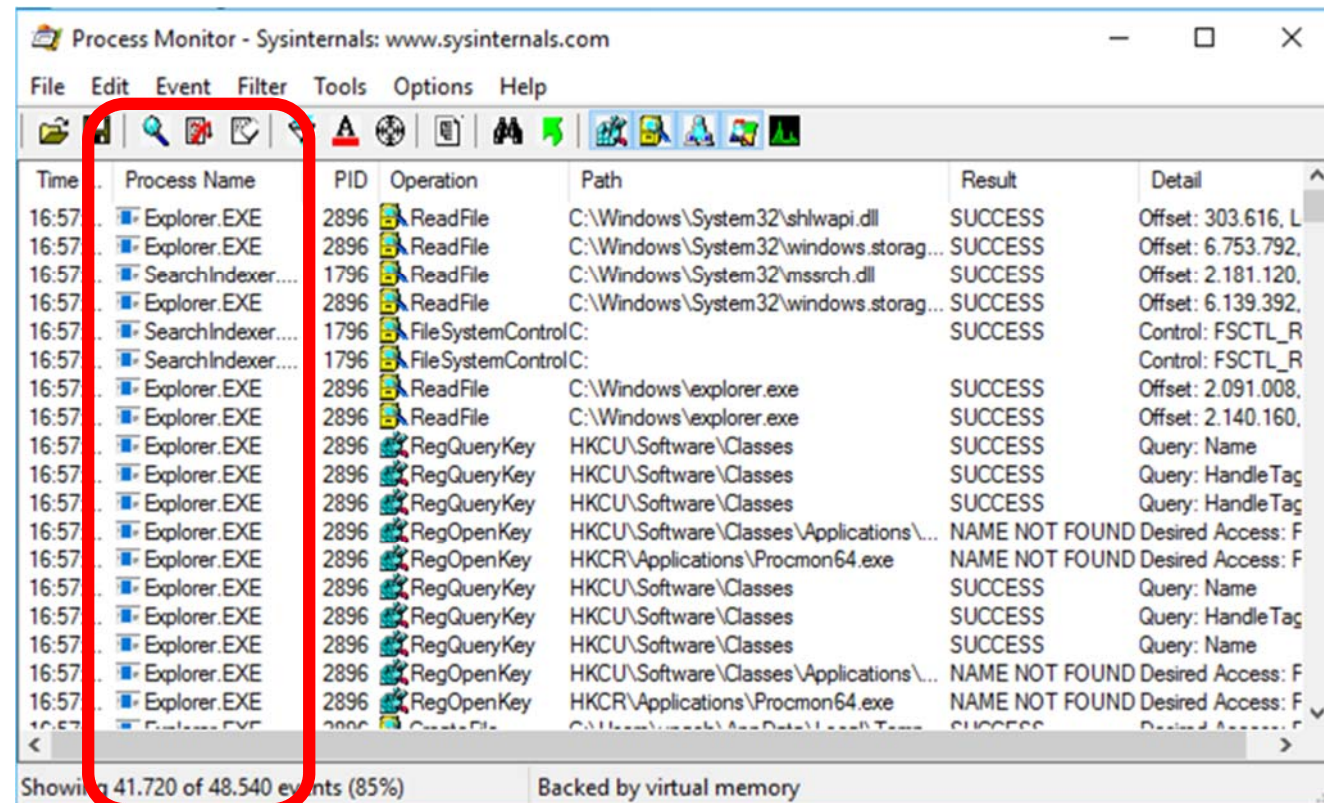
The screenshot shows the Process Monitor (ProcMon) application window. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes "File", "Edit", "Event", "Filter", "Tools", "Options", and "Help". The toolbar contains various icons for file operations, search, and process management. The main window displays a table of events with the following columns: Time, Process Name, PID, Operation, Path, Result, and Detail. The table shows a series of events from 16:57:00 to 16:57:10, primarily involving Explorer.EXE and SearchIndexer.exe. The events include file reads, file system controls, and registry queries. The status bar at the bottom indicates "Showing 41.720 of 48.540 events (85%)" and "Backed by virtual memory".

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset: 303.616, L
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6.753.792,
16:57:...	SearchIndexer....	1796	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2.181.120,
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6.139.392,
16:57:...	SearchIndexer....	1796	FileSystemControlC:		SUCCESS	Control: FSCTL_R
16:57:...	SearchIndexer....	1796	FileSystemControlC:			Control: FSCTL_R
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2.091.008,
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2.140.160,
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag
16:57:...	Explorer.EXE	2896	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
16:57:...	Explorer.EXE	2896	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	Create File	C:\Users\user\AppData\Local\Temp...	SUCCESS	Desired Access: F

Showing 41.720 of 48.540 events (85%) Backed by virtual memory

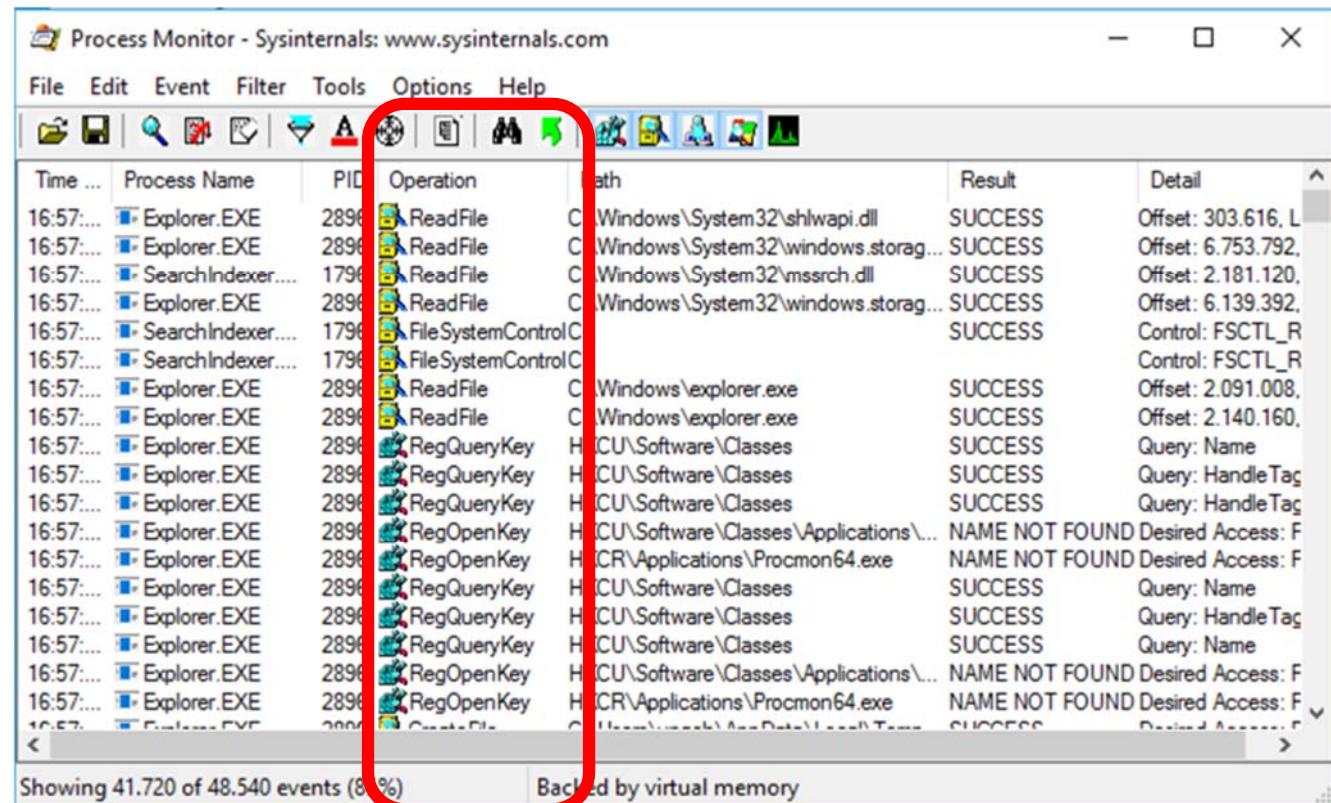
ProcMon - GUI

Name of the
Process
executing



ProcMon - GUI

Operation



Process Monitor - Sysinternals: www.sysinternals.com

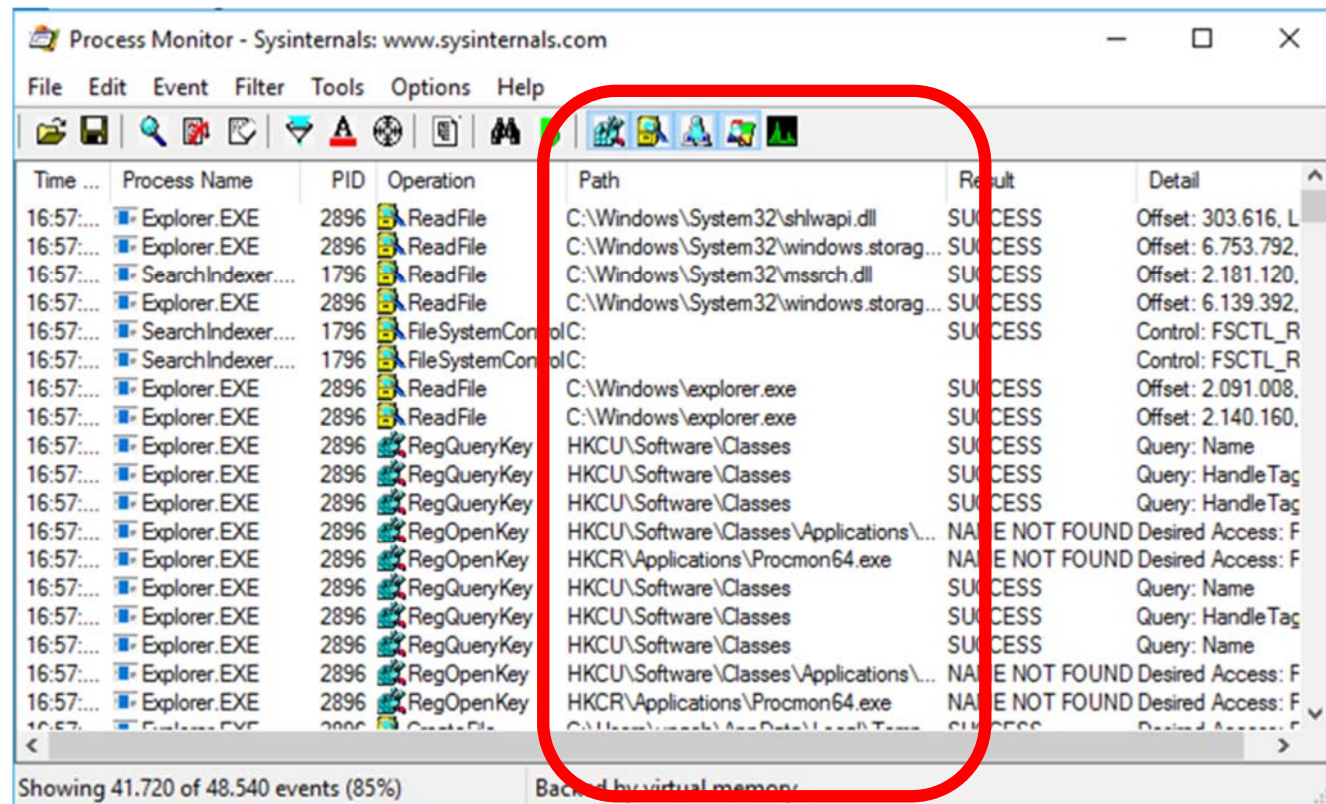
File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset: 303.616, L
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6.753.792,
16:57:...	SearchIndexer....	1796	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2.181.120,
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6.139.392,
16:57:...	SearchIndexer....	1796	FileSystemControlC		SUCCESS	Control: FSCTL_R
16:57:...	SearchIndexer....	1796	FileSystemControlC		SUCCESS	Control: FSCTL_R
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2.091.008,
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2.140.160,
16:57:...	Explorer.EXE	2896	RegQueryKey	H:\CU\Software\Classes	SUCCESS	Query: Name
16:57:...	Explorer.EXE	2896	RegQueryKey	H:\CU\Software\Classes	SUCCESS	Query: HandleTag
16:57:...	Explorer.EXE	2896	RegQueryKey	H:\CU\Software\Classes	SUCCESS	Query: HandleTag
16:57:...	Explorer.EXE	2896	RegOpenKey	H:\CU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	RegOpenKey	H:\CR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	RegQueryKey	H:\CU\Software\Classes	SUCCESS	Query: Name
16:57:...	Explorer.EXE	2896	RegQueryKey	H:\CU\Software\Classes	SUCCESS	Query: HandleTag
16:57:...	Explorer.EXE	2896	RegQueryKey	H:\CU\Software\Classes	SUCCESS	Query: Name
16:57:...	Explorer.EXE	2896	RegOpenKey	H:\CU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	RegOpenKey	H:\CR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	RegOpenKey	H:\CU\Software\Classes	SUCCESS	Desired Access: F

Showing 41.720 of 48.540 events (86%) Backed by virtual memory

ProcMon - GUI

The related
Path



Process Monitor - Sysinternals: www.sysinternals.com

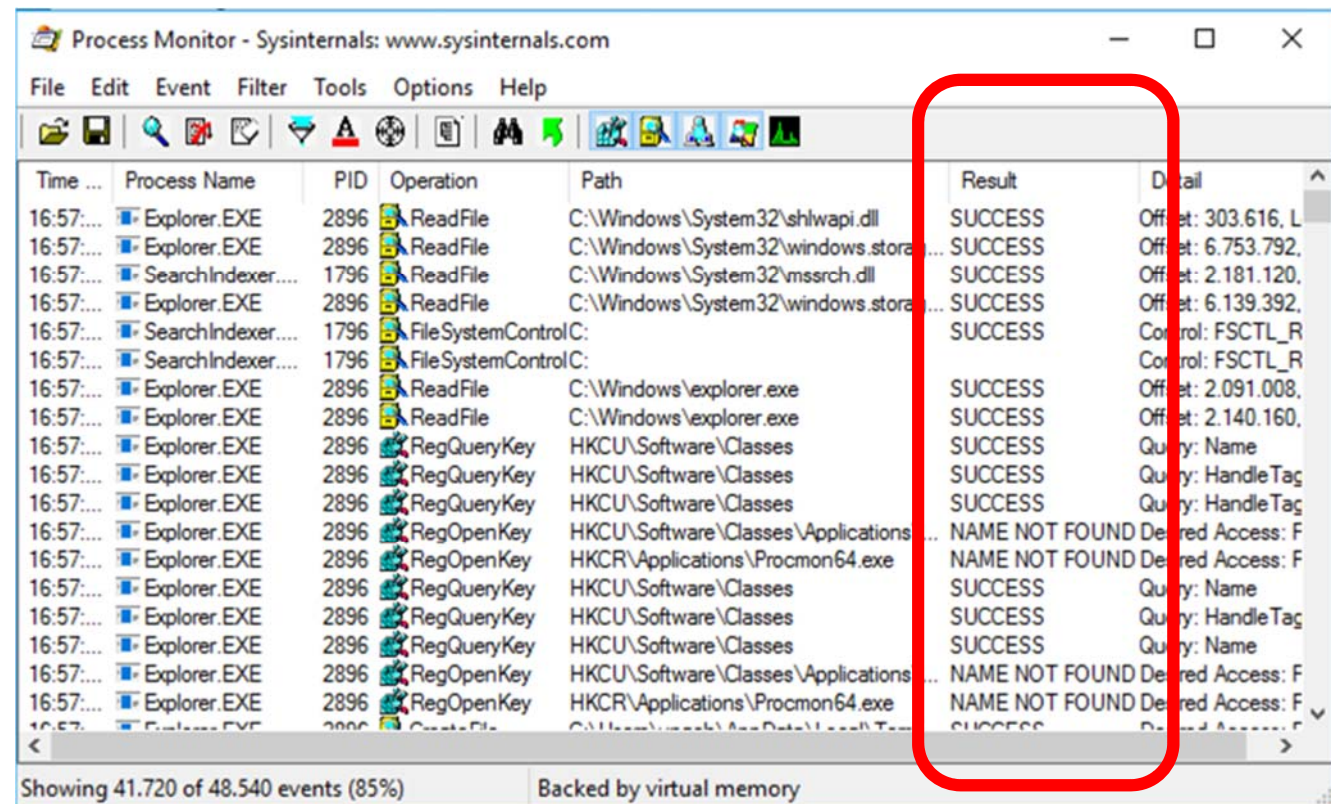
File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset: 303.616, L
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6.753.792,
16:57:...	SearchIndexer....	1796	ReadFile	C:\Windows\System32\mssrch.dll	SUCCESS	Offset: 2.181.120,
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6.139.392,
16:57:...	SearchIndexer....	1796	FileSystemControlC:		SUCCESS	Control: FSCTL_R
16:57:...	SearchIndexer....	1796	FileSystemControlC:		SUCCESS	Control: FSCTL_R
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2.091.008,
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2.140.160,
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag
16:57:...	Explorer.EXE	2896	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
16:57:...	Explorer.EXE	2896	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	Create File	C:\Users\... \AppData\Local\Temp...	SUCCESS	Desired Access: F

Showing 41.720 of 48.540 events (85%) Backed by virtual memory

ProcMon - GUI

Result



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

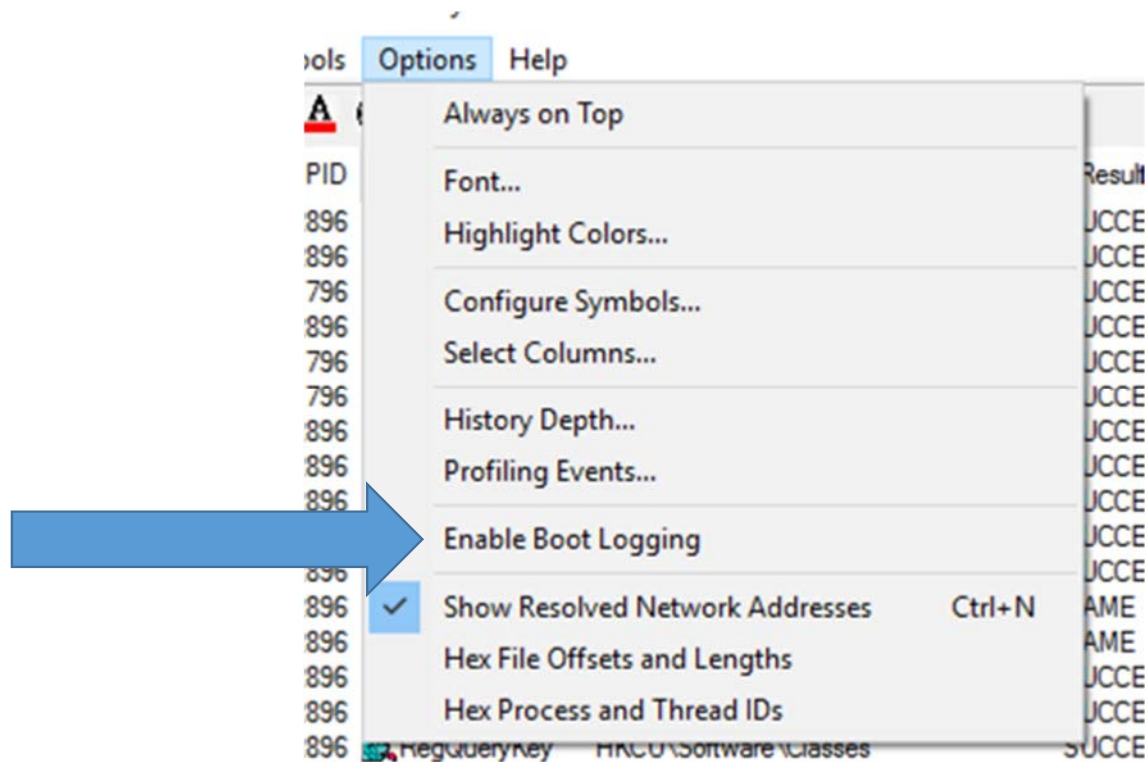
Time ...	Process Name	PID	Operation	Path	Result	Detail
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\System32\shlwapi.dll	SUCCESS	Offset: 303.616, L
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\System32\windows.stora...	SUCCESS	Offset: 6.753.792,
16:57:...	SearchIndexer....	1796	ReadFile	C:\Windows\System32\wmssrch.dll	SUCCESS	Offset: 2.181.120,
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\System32\windows.stora...	SUCCESS	Offset: 6.139.392,
16:57:...	SearchIndexer....	1796	FileSystemControlC:		SUCCESS	Control: FSCTL_R
16:57:...	SearchIndexer....	1796	FileSystemControlC:		SUCCESS	Control: FSCTL_R
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2.091.008,
16:57:...	Explorer.EXE	2896	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2.140.160,
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag
16:57:...	Explorer.EXE	2896	RegOpenKey	HKCU\Software\Classes\Applications...	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag
16:57:...	Explorer.EXE	2896	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
16:57:...	Explorer.EXE	2896	RegOpenKey	HKCU\Software\Classes\Applications...	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: F
16:57:...	Explorer.EXE	2896	CreateFile	C:\Users\user\AppData\Local\Temp...	SUCCESS	Desired Access: F

Showing 41.720 of 48.540 events (85%) Backed by virtual memory

ProcMon

- It is also able to log during boot!

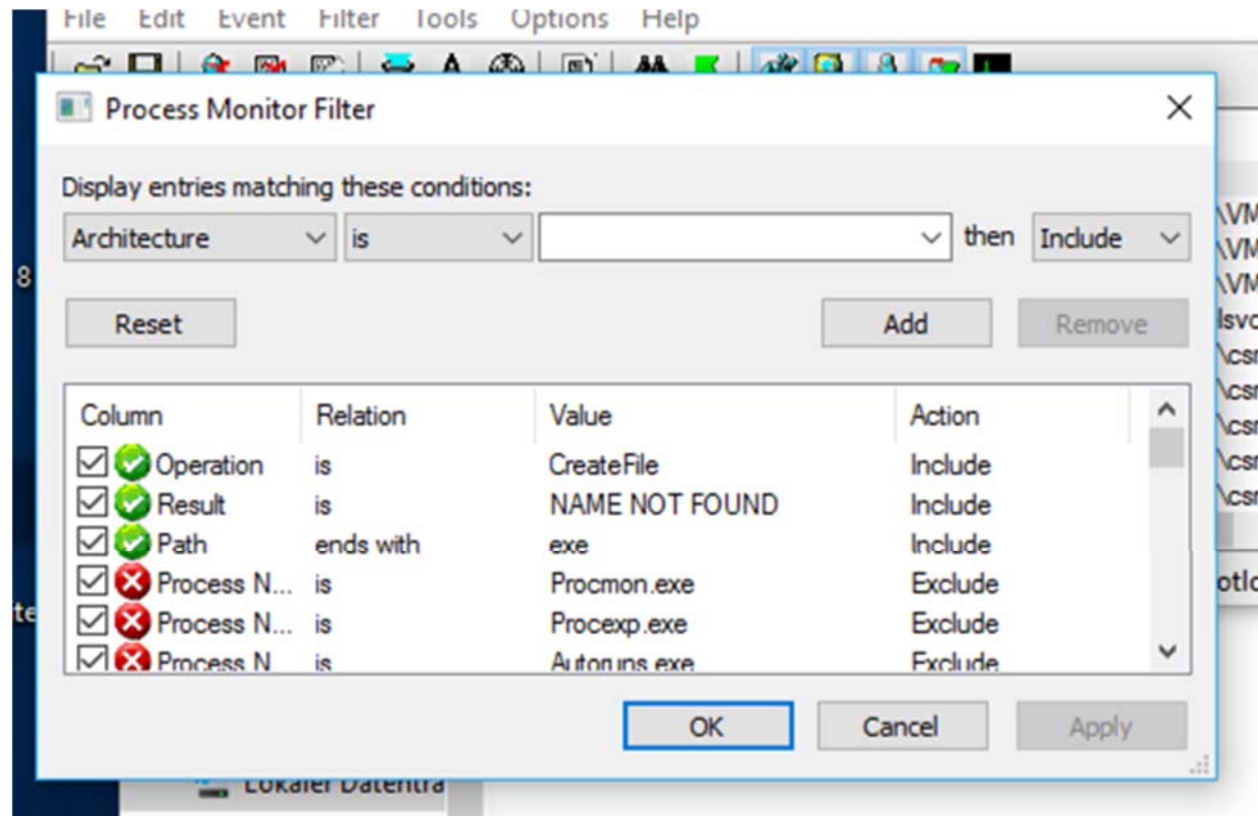
ProcMon - Boot



ProcMon

- But what can we do with it?
- We can find Privilege Escalations by combining
 - ... the %PATH% variable
 - ... errors in the ProcMon Log
 - ... a broken application

ProcMon – Filter for PrivEsc!



ProcMon

PATH=C:\Windows;C:\Python27;C:\SomeFolder;C:\BrokenTool\bin

Foo.exe

C:\Windows

C:\Python27

C:\SomeFolder

C:\BrokenTool\bin

ProcMon

PATH=C:\Windows;C:\Python27;C:\SomeFolder;C:\BrokenTool\bin

Foo.exe

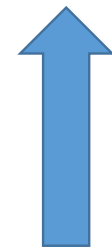
C:\Windows

C:\Python27

C:\SomeFolder

C:\BrokenTool\bin

Foo.exe (Malicious)



Powershell is nice to us!

- Before it calls its own functions and methods it first searches in PATH!

The screenshot illustrates the process of PowerShell resolving the path for the `Get-Date` command. On the left, the Process Monitor window shows a series of 'QueryDirectory' operations performed by `powershell.exe` (PID 8808) to search for `Get-Date.*` in various system paths. On the right, a PowerShell command prompt shows the execution of `Get-Date` after bypassing execution policy.

Time	Process Name	PID	Operation	Path	Result
17:45:27.6251694	powershell.exe	8808	QueryDirectory	C:\ProgramData\Oracle\Java\javapath\Get-Date.*	NO SUCH FILE
17:45:27.6251694	powershell.exe	8808	QueryDirectory	C:\Windows\System32\Get-Date.*	NO SUCH FILE
17:45:27.6251694	powershell.exe	8808	QueryDirectory	C:\Windows\Get-Date.*	NO SUCH FILE
17:45:27.6251694	powershell.exe	8808	QueryDirectory	C:\Windows\System32\wbem\Get-Date.*	NO SUCH FILE
17:45:27.6251694	powershell.exe	8808	QueryDirectory	C:\Windows\System32\WindowsPowerShell\v1.0\Get-Date.*	NO SUCH FILE
17:45:27.6251694	powershell.exe	8808	QueryDirectory	C:\Program Files\Microsoft\Web Platform Installer\Get-Date.*	NO SUCH FILE
17:45:27.6251694	powershell.exe	8808	QueryDirectory	C:\Program Files (x86)\Microsoft ASP.NET\ASP.NET\Get-Date.*	NO SUCH FILE
17:45:27.6251694	powershell.exe	8808	QueryDirectory	C:\Program Files (x86)\Windows Kits\8.0\Windows P\Get-Date.*	NO SUCH FILE
17:45:27.6251694	powershell.exe	8808	QueryDirectory	C:\Program Files\Microsoft SQL Server\110\Tools\Bi\Get-Date.*	NO SUCH FILE
17:45:27.6251694	powershell.exe	8808	QueryDirectory	C:\Program Files (x86)\Nmap\Get-Date.*	NO SUCH FILE
17:45:27.6251694	powershell.exe	8808	QueryDirectory	C:\Users\ungeh\AppData\Local\Microsoft\Windows\Get-Date.*	NO SUCH FILE
17:45:27.6251694	powershell.exe	8808	QueryDirectory	C:\Program Files\SDCC\bin\Get-Date.*	NO SUCH FILE

PowerShell Command Prompt Output:

```
C:\Users\ungeh>powershell -ExecutionPolicy bypass -nopprofile -f test.ps1
Montag, 29. Mai 2017 17:45:27
C:\Users\ungeh>
```

ProcMon - Demos

Strace

the Linux part

Strace

- Available on (almost) all Unix/Linux based systems (for AIX and Solaris there is **truss**)
- It traces system calls and signals
- It is possible to attach to running processes
- Can follow forked threads

Simple strace call

```

mmap(0, 1024000, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x00000000
fstat(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
brk(NULL)                               = 0x107c000
brk(0x109d000)                           = 0x109d000
write(1, "\n", 1)                         = 1
write(1, "\n", 1)                         = 1
write(1, "Hello World\n", 12Hello World) = 12
write(1, "\n", 1)                         = 1
exit_group(0)                            = ?
+++ exited with 0 +++
root@f198:~# █

```

How to use it?

- Put some placeholder into the parameters and grep for them

Strace - Demos

Only Local Priv Esc?

You can also check remote protocols for RCE!