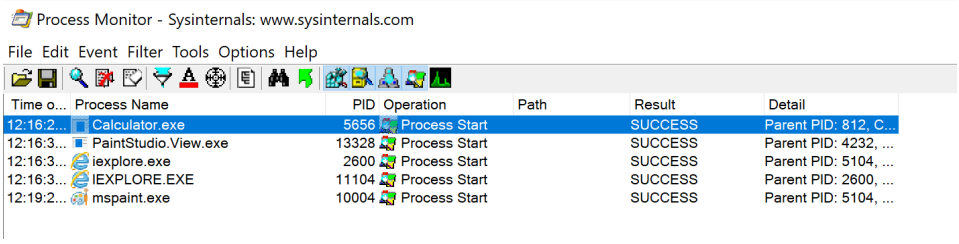
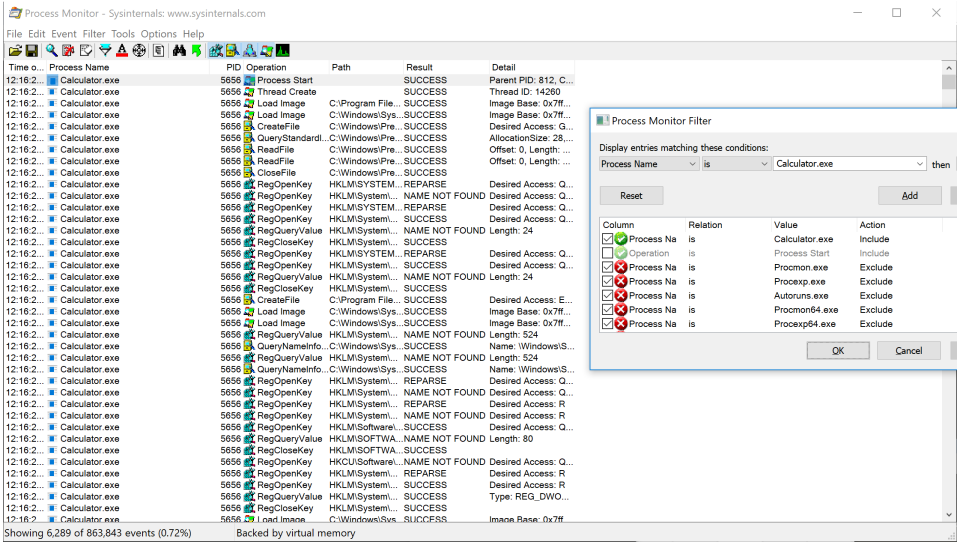
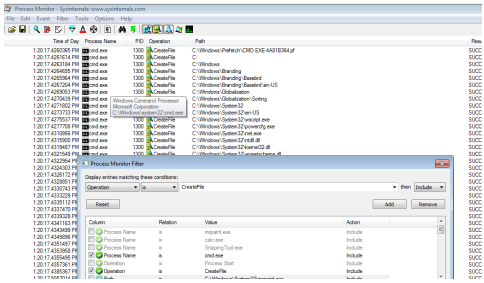
Exercise Task 2

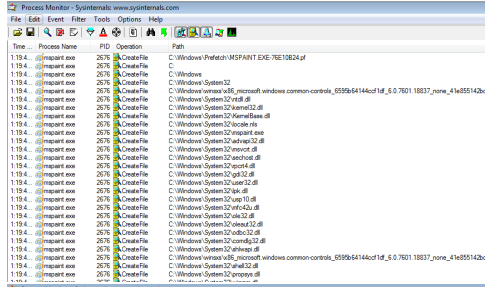
Part 1: Normal programs

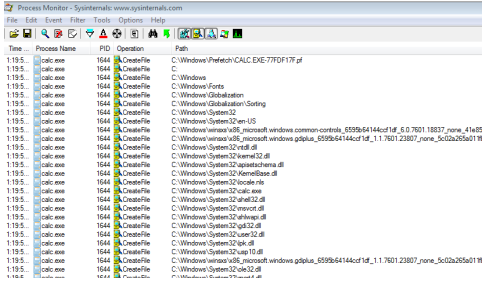
- Choose 5 different normal programs and use Process Monitor and Process Explorer to get an overview of the events that occur during a normal startup procedure.
- Use Paint and Notepad to create two new files and save them to disk. Find the corresponding events in Process Monitor. Do these actions trigger loading of additional DLLs than those loaded at startup?

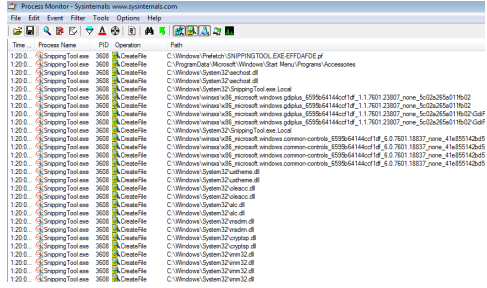

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
12:16:2... Calculator.exe 5656 Process Start SUCCESS Parent PID: 812, C...
12:16:3... PaintStudio.View.exe 13328 Process Start SUCCESS Parent PID: 4232, ...
12:16:3... iexplore.exe 2600 Process Start SUCCESS Parent PID: 5104, ...
12:16:3... IEXPLORE.EXE 11104 Process Start SUCCESS Parent PID: 2600, ...
12:19:2... mspaint.exe 10004 Process Start SUCCESS Parent PID: 5104, ...

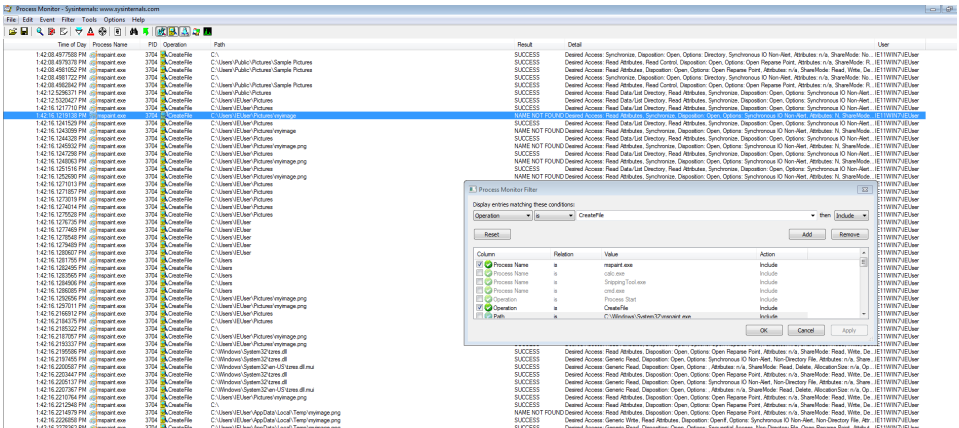

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
12:16:2... Calculator.exe 5656 Process Start SUCCESS Parent PID: 812, C...
12:16:2... Calculator.exe 5656 Thread Create SUCCESS Thread ID: 14260
12:16:2... Calculator.exe 5656 Load Image C:\Program File... SUCCESS Image Base: 0x7ff...
12:16:2... Calculator.exe 5656 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x7ff...
12:16:2... Calculator.exe 5656 CreateFile C:\Windows\Pre... SUCCESS Desired Access: G...
12:16:2... Calculator.exe 5656 QueryStandardI... C:\Windows\Pre... SUCCESS AllocationSize: 28,...
12:16:2... Calculator.exe 5656 ReadFile C:\Windows\Pre... SUCCESS Offset: 0, Length: ...
12:16:2... Calculator.exe 5656 ReadFile C:\Windows\Pre... SUCCESS Offset: 0, Length: ...
12:16:2... Calculator.exe 5656 CloseFile C:\Windows\Pre... SUCCESS
12:16:2... Calculator.exe 5656 RegOpenKey HKLM\SYSTEM... REPARSE Desired Access: Q...
12:16:2... Calculator.exe 5656 RegOpenKey HKLM\System\... NAME NOT FOUND Desired Access: Q...
12:16:2... Calculator.exe 5656 RegOpenKey HKLM\SYSTEM... REPARSE Desired Access: Q...
12:16:2... Calculator.exe 5656 RegOpenKey HKLM\System\... SUCCESS Desired Access: Q...
12:16:2... Calculator.exe 5656 RegQueryValue HKLM\System\... NAME NOT FOUND Length: 24
12:16:2... Calculator.exe 5656 RegCloseKey HKLM\System\... SUCCESS
12:16:2... Calculator.exe 5656 RegOpenKey HKLM\SYSTEM... REPARSE Desired Access: Q...
12:16:2... Calculator.exe 5656 RegOpenKey HKLM\System\... SUCCESS Desired Access: Q...
12:16:2... Calculator.exe 5656 RegQueryValue HKLM\System\... NAME NOT FOUND Length: 24
12:16:2... Calculator.exe 5656 RegCloseKey HKLM\System\... SUCCESS
12:16:2... Calculator.exe 5656 CreateFile C:\Program File... SUCCESS Desired Access: E...
12:16:2... Calculator.exe 5656 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x7ff...
12:16:2... Calculator.exe 5656 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x7ff...
12:16:2... Calculator.exe 5656 RegQueryValue HKLM\System\... NAME NOT FOUND Length: 524
12:16:2... Calculator.exe 5656 QueryNameInfo... C:\Windows\Sys... SUCCESS Name: \Windows\S...
12:16:2... Calculator.exe 5656 RegQueryValue HKLM\System\... NAME NOT FOUND Length: 524
12:16:2... Calculator.exe 5656 QueryNameInfo... C:\Windows\Sys... SUCCESS Name: \Windows\S...
12:16:2... Calculator.exe 5656 RegOpenKey HKLM\System\... REPARSE Desired Access: Q...
12:16:2... Calculator.exe 5656 RegOpenKey HKLM\System\... NAME NOT FOUND Desired Access: Q...
12:16:2... Calculator.exe 5656 RegOpenKey HKLM\System\... REPARSE Desired Access: R
12:16:2... Calculator.exe 5656 RegOpenKey HKLM\System\... NAME NOT FOUND Desired Access: R
12:16:2... Calculator.exe 5656 RegOpenKey HKLM\Software\... SUCCESS Desired Access: Q...
12:16:2... Calculator.exe 5656 RegQueryValue HKLM\SOFTWA... NAME NOT FOUND Length: 80
12:16:2... Calculator.exe 5656 RegCloseKey HKLM\SOFTWA... SUCCESS
12:16:2... Calculator.exe 5656 RegOpenKey HKCU\Software\... NAME NOT FOUND Desired Access: Q...
12:16:2... Calculator.exe 5656 RegOpenKey HKLM\System\... REPARSE Desired Access: R
12:16:2... Calculator.exe 5656 RegOpenKey HKLM\System\... SUCCESS Desired Access: R
12:16:2... Calculator.exe 5656 RegQueryValue HKLM\System\... SUCCESS Type: REG_DWO...
12:16:2... Calculator.exe 5656 RegCloseKey HKLM\System\... SUCCESS
12:16:2... Calculator.exe 5656 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x7ff...
Showing 6,289 of 863,843 events (0.72%)
Backed by virtual memory
Process Monitor Filter
Display entries matching these conditions:
Process Name is Calculator.exe then
Reset
Add
Column Relation Value Action
Process Na is Calculator.exe Include
Operation is Process Start Include
Process Na is Procmon.exe Exclude
Process Na is Procexp.exe Exclude
Process Na is Autoruns.exe Exclude
Process Na is Procmon64.exe Exclude
Process Na is Procexp64.exe Exclude
OK
Cancel


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Process Monitor Filter
Display entries matching these conditions:
Operation is CreateFile then Include
Reset Add Remove
Column Relation Value Action
Process Name is mspaint.exe Include
Process Name is calc.exe Include
Process Name is SnippingTool.exe Include
Process Name is cmd.exe Include
Operation is Process Start Include
Operation is CreateFile Include


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\Prefetch\MSPAINT.EXE-76E10B24.pf
1:19:4... mspaint.exe 2676 CreateFile C:
1:19:4... mspaint.exe 2676 CreateFile C:\Windows
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\Branding
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5de22
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\ntdll.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\kernel32.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\KernelBase.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\locale.nls
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\mspaint.exe
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\advapi32.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\msvcrt.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\sechost.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\rpcrt4.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\sspicli.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\user32.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\gdi32.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\usp10.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\ntdll.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\clbcatq.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\comdlg32.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\shlwapi.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5de22
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\shell32.dll
1:19:4... mspaint.exe 2676 CreateFile C:\Windows\System32\propsys.dll


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path
1:19:5... calc.exe 1644 CreateFile C:\Windows\Prefetch\CALC.EXE-77FDF17F.pf
1:19:5... calc.exe 1644 CreateFile C:
1:19:5... calc.exe 1644 CreateFile C:\Windows
1:19:5... calc.exe 1644 CreateFile C:\Windows\Fonts
1:19:5... calc.exe 1644 CreateFile C:\Windows\Globalization
1:19:5... calc.exe 1644 CreateFile C:\Windows\Globalization\Sorting
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\en-US
1:19:5... calc.exe 1644 CreateFile C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5de22
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\ntdll.dll
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\kernel32.dll
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\apisetschema.dll
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\KernelBase.dll
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\locale.nls
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\calc.exe
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\shell32.dll
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\msvcrt.dll
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\shlwapi.dll
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\gdi32.dll
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\user32.dll
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\lpk.dll
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\usp10.dll
1:19:5... calc.exe 1644 CreateFile C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.23807_none_5c02a265a011fb02.dll
1:19:5... calc.exe 1644 CreateFile C:\Windows\System32\ole32.dll


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\Prefetch\SNIPPINGTOOL.EXE-EFFDAFDE.pf
1:20:0... SnippingTool.exe 3608 CreateFile C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\sechost.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\sechost.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\SnippingTool.exe.Local
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.23807_none_5c02a265a011fb02
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.23807_none_5c02a265a011fb02.Local
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.23807_none_5c02a265a011fb02.Gdiplus
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.23807_none_5c02a265a011fb02.Gdiplus
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\SnippingTool.exe.Local
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5de22
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5de22.Local
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5de22.Manifest
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\uxtheme.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\uxtheme.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\oleacc.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\oleacc.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\calc.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\calc.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\msdrm.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\msdrm.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\cryptsp.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\cryptsp.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\rsaenh.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\rsaenh.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\cryptbase.dll
1:20:0... SnippingTool.exe 3608 CreateFile C:\Windows\System32\cryptbase.dll


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day Process Name PID Operation Path Result Detail User
1:42:08.4577588 PM rnsquirt.exe 3704 CreateFile C:\ SUCCESS Desired Access: Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: No... IE11WIN7\IEUser
1:42:08.4979378 PM rnsquirt.exe 3704 CreateFile C:\Users\Public\Pictures\Sample Pictures SUCCESS Desired Access: Read Attributes, Read Control, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: R... IE11WIN7\IEUser
1:42:08.4981052 PM rnsquirt.exe 3704 CreateFile C:\Users\Public\Pictures\Sample Pictures SUCCESS Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, De... IE11WIN7\IEUser
1:42:08.4981722 PM rnsquirt.exe 3704 CreateFile C:\ SUCCESS Desired Access: Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: No... IE11WIN7\IEUser
1:42:08.4982842 PM rnsquirt.exe 3704 CreateFile C:\Users\Public\Pictures\Sample Pictures SUCCESS Desired Access: Read Attributes, Read Control, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: R... IE11WIN7\IEUser
1:42:12.5296371 PM rnsquirt.exe 3704 CreateFile C:\Users\Public\Pictures SUCCESS Desired Access: Read Data/List Directory, Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert... IE11WIN7\IEUser
1:42:12.5320427 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures SUCCESS Desired Access: Read Data/List Directory, Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert... IE11WIN7\IEUser
1:42:16.1217710 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures SUCCESS Desired Access: Read Data/List Directory, Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert... IE11WIN7\IEUser
1:42:16.1219139 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures\myimage NAME NOT FOUND Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: N, ShareMode... IE11WIN7\IEUser
1:42:16.1241529 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures SUCCESS Desired Access: Read Data/List Directory, Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert... IE11WIN7\IEUser
1:42:16.1243099 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures\myimage NAME NOT FOUND Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: N, ShareMode... IE11WIN7\IEUser
1:42:16.1244328 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures SUCCESS Desired Access: Read Data/List Directory, Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert... IE11WIN7\IEUser
1:42:16.1245932 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures\myimage.png NAME NOT FOUND Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: N, ShareMode... IE11WIN7\IEUser
1:42:16.1247298 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures SUCCESS Desired Access: Read Data/List Directory, Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert... IE11WIN7\IEUser
1:42:16.1248063 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures\myimage.png NAME NOT FOUND Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: N, ShareMode... IE11WIN7\IEUser
1:42:16.1251516 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser SUCCESS Desired Access: Read Data/List Directory, Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert... IE11WIN7\IEUser
1:42:16.1252690 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures\myimage.png NAME NOT FOUND Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: N, ShareMode... IE11WIN7\IEUser
1:42:16.1271013 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures IE11WIN7\IEUser
1:42:16.1271857 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures IE11WIN7\IEUser
1:42:16.1273019 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures IE11WIN7\IEUser
1:42:16.1274014 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures IE11WIN7\IEUser
1:42:16.1275528 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures IE11WIN7\IEUser
1:42:16.1276735 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser IE11WIN7\IEUser
1:42:16.1277469 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser IE11WIN7\IEUser
1:42:16.1278548 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser IE11WIN7\IEUser
1:42:16.1279489 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser IE11WIN7\IEUser
1:42:16.1280827 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser IE11WIN7\IEUser
1:42:16.1281755 PM rnsquirt.exe 3704 CreateFile C:\Users IE11WIN7\IEUser
1:42:16.1282496 PM rnsquirt.exe 3704 CreateFile C:\Users IE11WIN7\IEUser
1:42:16.1283566 PM rnsquirt.exe 3704 CreateFile C:\Users IE11WIN7\IEUser
1:42:16.1284906 PM rnsquirt.exe 3704 CreateFile C:\Users IE11WIN7\IEUser
1:42:16.1285685 PM rnsquirt.exe 3704 CreateFile C:\Users IE11WIN7\IEUser
1:42:16.1292656 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures\myimage.png SUCCESS Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, De... IE11WIN7\IEUser
1:42:16.1297011 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures\myimage.png SUCCESS Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, Share... IE11WIN7\IEUser
1:42:16.2166912 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures SUCCESS Desired Access: Read Data/List Directory, Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert... IE11WIN7\IEUser
1:42:16.2184375 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures SUCCESS Desired Access: Read Data/List Directory, Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert... IE11WIN7\IEUser
1:42:16.2185322 PM rnsquirt.exe 3704 CreateFile C:\ SUCCESS Desired Access: Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: No... IE11WIN7\IEUser
1:42:16.2187057 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures\myimage.png SUCCESS Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, De... IE11WIN7\IEUser
1:42:16.2193337 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures\myimage.png SUCCESS Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, Share... IE11WIN7\IEUser
1:42:16.2195836 PM rnsquirt.exe 3704 CreateFile C:\Windows\System32\rpcss.dll SUCCESS Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, De... IE11WIN7\IEUser
1:42:16.2197455 PM rnsquirt.exe 3704 CreateFile C:\Windows\System32\rpcss.dll SUCCESS Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, Share... IE11WIN7\IEUser
1:42:16.2200587 PM rnsquirt.exe 3704 CreateFile C:\Windows\System32\en-US\rpcss.dll.mui SUCCESS Desired Access: Generic Read, Disposition: Open, Options: , Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, Op... IE11WIN7\IEUser
1:42:16.2203447 PM rnsquirt.exe 3704 CreateFile C:\Windows\System32\rpcss.dll SUCCESS Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, De... IE11WIN7\IEUser
1:42:16.2205137 PM rnsquirt.exe 3704 CreateFile C:\Windows\System32\rpcss.dll SUCCESS Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, Share... IE11WIN7\IEUser
1:42:16.2207367 PM rnsquirt.exe 3704 CreateFile C:\Windows\System32\en-US\rpcss.dll.mui SUCCESS Desired Access: Generic Read, Disposition: Open, Options: , Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, Op... IE11WIN7\IEUser
1:42:16.2210764 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\Pictures\myimage.png SUCCESS Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, De... IE11WIN7\IEUser
1:42:16.2212940 PM rnsquirt.exe 3704 CreateFile C:\ SUCCESS Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, De... IE11WIN7\IEUser
1:42:16.2214979 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\AppData\Local\Temp\myimage.png NAME NOT FOUND Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, De... IE11WIN7\IEUser
1:42:16.2226858 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\AppData\Local\Temp\myimage.png SUCCESS Desired Access: Generic Write, Read Attributes, Disposition: OpenIf, Options: Synchronous IO Non-Alert, Non-Directory File, Att... IE11WIN7\IEUser
1:42:16.2278362 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\AppData\Local\Temp\myimage.png SUCCESS Desired Access: Generic Read, Disposition: Open, Options: Sequential Access, Non-Directory File, Open Reparse Point, Attribut... IE11WIN7\IEUser
1:42:16.2279697 PM rnsquirt.exe 3704 CreateFile C:\Users\IEUser\AppData\Local\Temp\myimage.png SUCCESS Desired Access: Generic Read, Disposition: Open, Options: Sequential Access, Synchronous IO Non-Alert, Non-Directory File, ... IE11WIN7\IEUser
Process Monitor Filter
Display entries matching these conditions:
Operation is CreateFile then Include
Reset Add Remove
Column Relation Value Action
Process Name is rnsquirt.exe Include
Process Name is calc.exe Include
Process Name is Snipping Tool.exe Include
Process Name is cmd.exe Include
Operation is Process Start Include
Operation is CreateFile Include
Path is C:\Windows\System32\rnsquirt.exe Include
OK Cancel Apply

Part 1: What to learn?

- Be able to recognize common behavior at startup.
- Use filters to see events from only one process in Process Monitor.
- Find the startup of a process in Process Monitor.
- Find the dll files loaded by a process in Process Explorer.

Part 2: Malicious programs

- Turn off Windows Defender in your VM (and keep it off).
- Download the labs from the book's website:
  `https://practicalmalwareanalysis.com/labs/`
- Do the labs 3-1 and 3-3. Note that these two pieces of malware are written specifically for XP, so they will not work exactly as in the solutions described in the book.

Turn off Windows Defender

To turn it off in GUI only works for a while. Alternatives:

- Open regedit as admin
- Go to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsDefender`
- If there is a key named DisableAntiSpyware, set it to 1 and reboot. You're finished.
- If not, right click the Windows Defender folder in the folder hierarchy.
- New → DWORD (32-bit), set the name to DisableAntiSpyware and value to 1. Reboot

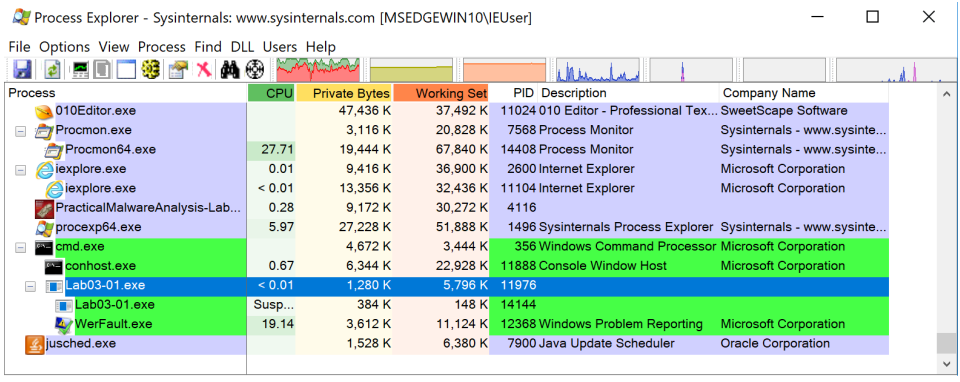
With group policy:

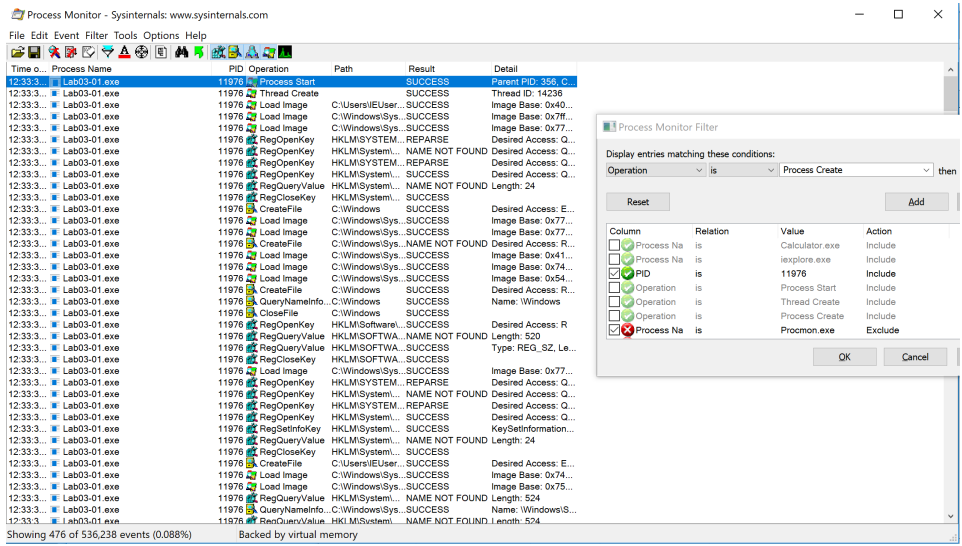
- Open gpedit.msc
- Computer configuration → Administrative templates → windows components → Windows Defender Antivirus
- Find the item "Turn off Windows Defender Antivirus" and set it to Enabled.

Or go to *Virus and threat protection settings* and add the Labs folder to Exclusions.

Lab 3-1

Examine the executable Lab03-01.exe using basic dynamic analysis.
Use Process Monitor, Process Explorer (and Regshot).


Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser]
File Options View Process Find DLL Users Help
Process CPU Private Bytes Working Set PID Description Company Name
010Editor.exe 47,436 K 37,492 K 11024 010 Editor - Professional Tex... SweetScape Software
Procmon.exe 3,116 K 20,828 K 7568 Process Monitor Sysinternals - www.sysinte...
Procmon64.exe 27.71 19,444 K 67,840 K 14408 Process Monitor Sysinternals - www.sysinte...
iexplore.exe 0.01 9,416 K 36,900 K 2600 Internet Explorer Microsoft Corporation
iexplore.exe < 0.01 13,356 K 32,436 K 11104 Internet Explorer Microsoft Corporation
PracticalMalwareAnalysis-Lab... 0.28 9,172 K 30,272 K 4116
procexp64.exe 5.97 27,228 K 51,888 K 1496 Sysinternals Process Explorer Sysinternals - www.sysinte...
cmd.exe 4,672 K 3,444 K 356 Windows Command Processor Microsoft Corporation
conhost.exe 0.67 6,344 K 22,928 K 11888 Console Window Host Microsoft Corporation
Lab03-01.exe < 0.01 1,280 K 5,796 K 11976
Lab03-01.exe Susp... 384 K 148 K 14144
WerFault.exe 19.14 3,612 K 11,124 K 12368 Windows Problem Reporting Microsoft Corporation
jusched.exe 1,528 K 6,380 K 7900 Java Update Scheduler Oracle Corporation

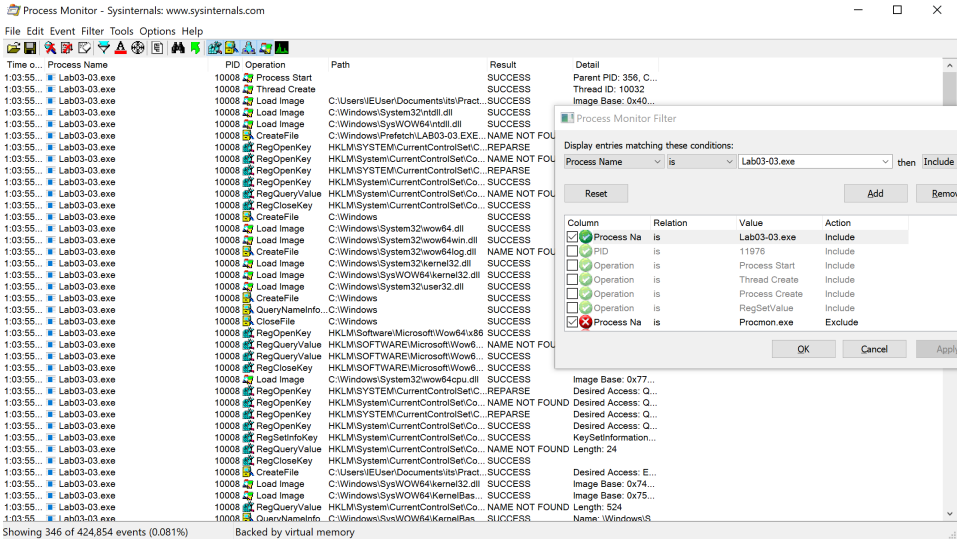

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
12:33:3... Lab03-01.exe 11976 Process Start SUCCESS Parent PID: 356, C...
12:33:3... Lab03-01.exe 11976 Thread Create SUCCESS Thread ID: 14236
12:33:3... Lab03-01.exe 11976 Load Image C:\Users\IEUser... SUCCESS Image Base: 0x40...
12:33:3... Lab03-01.exe 11976 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x7ff...
12:33:3... Lab03-01.exe 11976 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x777...
12:33:3... Lab03-01.exe 11976 RegOpenKey HKLM\SYSTEM... REPARSE Desired Access: Q...
12:33:3... Lab03-01.exe 11976 RegOpenKey HKLM\System\... NAME NOT FOUND Desired Access: Q...
12:33:3... Lab03-01.exe 11976 RegOpenKey HKLM\SYSTEM... REPARSE Desired Access: Q...
12:33:3... Lab03-01.exe 11976 RegOpenKey HKLM\System\... SUCCESS Desired Access: Q...
12:33:3... Lab03-01.exe 11976 RegQueryValue HKLM\System\... NAME NOT FOUND Length: 24
12:33:3... Lab03-01.exe 11976 RegCloseKey HKLM\System\... SUCCESS
12:33:3... Lab03-01.exe 11976 CreateFile C:\Windows SUCCESS Desired Access: E...
12:33:3... Lab03-01.exe 11976 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x777...
12:33:3... Lab03-01.exe 11976 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x777...
12:33:3... Lab03-01.exe 11976 CreateFile C:\Windows\Sys... NAME NOT FOUND Desired Access: R...
12:33:3... Lab03-01.exe 11976 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x41...
12:33:3... Lab03-01.exe 11976 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x74...
12:33:3... Lab03-01.exe 11976 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x54...
12:33:3... Lab03-01.exe 11976 CreateFile C:\Windows SUCCESS Desired Access: R...
12:33:3... Lab03-01.exe 11976 QueryNameInfo... C:\Windows SUCCESS Name: \Windows
12:33:3... Lab03-01.exe 11976 CloseFile C:\Windows SUCCESS
12:33:3... Lab03-01.exe 11976 RegOpenKey HKLM\Software\... SUCCESS Desired Access: R
12:33:3... Lab03-01.exe 11976 RegQueryValue HKLM\SOFTWA... NAME NOT FOUND Length: 520
12:33:3... Lab03-01.exe 11976 RegQueryValue HKLM\SOFTWA... SUCCESS Type: REG_SZ, Le...
12:33:3... Lab03-01.exe 11976 RegCloseKey HKLM\SOFTWA... SUCCESS
12:33:3... Lab03-01.exe 11976 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x777...
12:33:3... Lab03-01.exe 11976 RegOpenKey HKLM\SYSTEM... REPARSE Desired Access: Q...
12:33:3... Lab03-01.exe 11976 RegOpenKey HKLM\System\... NAME NOT FOUND Desired Access: Q...
12:33:3... Lab03-01.exe 11976 RegOpenKey HKLM\SYSTEM... REPARSE Desired Access: Q...
12:33:3... Lab03-01.exe 11976 RegOpenKey HKLM\System\... SUCCESS Desired Access: Q...
12:33:3... Lab03-01.exe 11976 RegSetInfoKey HKLM\System\... SUCCESS KeySetInformation...
12:33:3... Lab03-01.exe 11976 RegQueryValue HKLM\System\... NAME NOT FOUND Length: 24
12:33:3... Lab03-01.exe 11976 RegCloseKey HKLM\System\... SUCCESS
12:33:3... Lab03-01.exe 11976 CreateFile C:\Users\IEUser... SUCCESS Desired Access: E...
12:33:3... Lab03-01.exe 11976 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x74...
12:33:3... Lab03-01.exe 11976 Load Image C:\Windows\Sys... SUCCESS Image Base: 0x775...
12:33:3... Lab03-01.exe 11976 RegQueryValue HKLM\System\... NAME NOT FOUND Length: 524
12:33:3... Lab03-01.exe 11976 QueryNameInfo... C:\Windows\Sys... SUCCESS Name: \Windows\S...
12:33:3... Lab03-01.exe 11976 RegQueryValue HKLM\System\... NAME NOT FOUND Length: 524
Showing 476 of 536,238 events (0.088%)
Backed by virtual memory
Process Monitor Filter
Display entries matching these conditions:
Operation is Process Create then
Reset
Add
Column Relation Value Action
Process Na is Calculator.exe Include
Process Na is iexplore.exe Include
PID is 11976 Include
Operation is Process Start Include
Operation is Thread Create Include
Operation is Process Create Include
Process Na is Procmon.exe Exclude
OK
Cancel

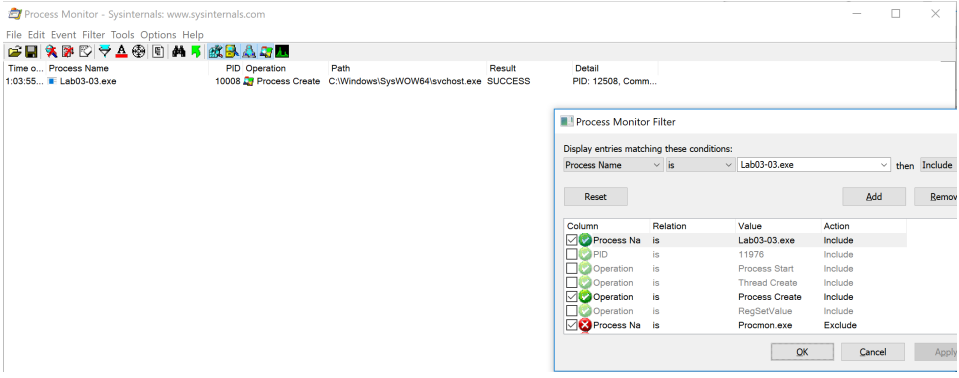
Lab 3-1: What to learn?

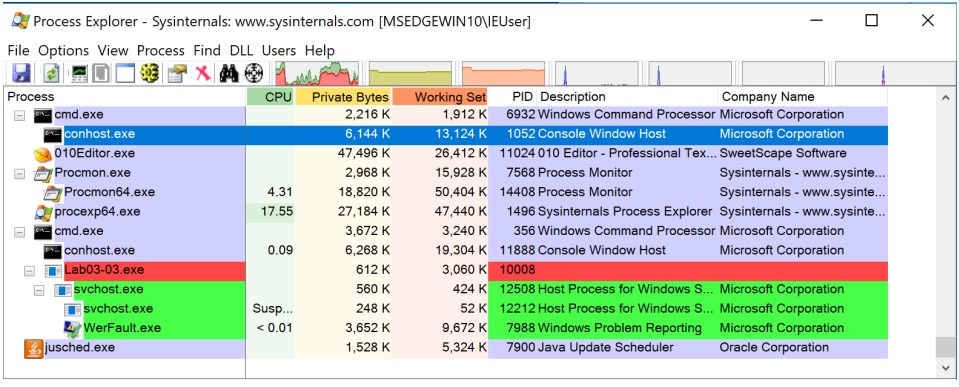
- Identify the processes started by an executable.
- Use filters in Process Monitor to analyze all relevant processes.
- WerFault is started because a problem is detected and may be reported.
- Identify files that are written to and changes in the registry using Regshot or filters in Process Monitor.

Lab 3-3

Examine the executable Lab03-03.exe using basic dynamic analysis.
Use Process Monitor, Process Explorer (and Regshot).


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
1:03:55... Lab03-03.exe 10008 Process Start SUCCESS Parent PID: 356, C...
1:03:55... Lab03-03.exe 10008 Thread Create SUCCESS Thread ID: 10032
1:03:55... Lab03-03.exe 10008 Load Image C:\Users\IEUser\Documents\its\Pract... SUCCESS Image Base: 0x40...
1:03:55... Lab03-03.exe 10008 Load Image C:\Windows\System32\ntdll.dll SUCCESS
1:03:55... Lab03-03.exe 10008 Load Image C:\Windows\SysWOW64\ntdll.dll SUCCESS
1:03:55... Lab03-03.exe 10008 CreateFile C:\Windows\Prefetch\LAB03-03.EXE... NAME NOT FOU
1:03:55... Lab03-03.exe 10008 RegOpenKey HKLM\SYSTEM\CurrentControlSet\C... REPARSE
1:03:55... Lab03-03.exe 10008 RegOpenKey HKLM\System\CurrentControlSet\Co... NAME NOT FOU
1:03:55... Lab03-03.exe 10008 RegOpenKey HKLM\SYSTEM\CurrentControlSet\C... REPARSE
1:03:55... Lab03-03.exe 10008 RegOpenKey HKLM\System\CurrentControlSet\Co... SUCCESS
1:03:55... Lab03-03.exe 10008 RegQueryValue HKLM\System\CurrentControlSet\Co... NAME NOT FOU
1:03:55... Lab03-03.exe 10008 RegCloseKey HKLM\System\CurrentControlSet\Co... SUCCESS
1:03:55... Lab03-03.exe 10008 CreateFile C:\Windows SUCCESS
1:03:55... Lab03-03.exe 10008 Load Image C:\Windows\System32\wow64.dll SUCCESS
1:03:55... Lab03-03.exe 10008 Load Image C:\Windows\System32\wow64win.dll SUCCESS
1:03:55... Lab03-03.exe 10008 CreateFile C:\Windows\System32\wow64log.dll NAME NOT FOU
1:03:55... Lab03-03.exe 10008 Load Image C:\Windows\System32\kernel32.dll SUCCESS
1:03:55... Lab03-03.exe 10008 Load Image C:\Windows\SysWOW64\kernel32.dll SUCCESS
1:03:55... Lab03-03.exe 10008 Load Image C:\Windows\System32\user32.dll SUCCESS
1:03:55... Lab03-03.exe 10008 CreateFile C:\Windows SUCCESS
1:03:55... Lab03-03.exe 10008 QueryNameInfo... C:\Windows SUCCESS
1:03:55... Lab03-03.exe 10008 CloseFile C:\Windows SUCCESS
1:03:55... Lab03-03.exe 10008 RegOpenKey HKLM\Software\Microsoft\Wow64\x86 SUCCESS
1:03:55... Lab03-03.exe 10008 RegQueryValue HKLM\SOFTWARE\Microsoft\Wow6... NAME NOT FOU
1:03:55... Lab03-03.exe 10008 RegQueryValue HKLM\SOFTWARE\Microsoft\Wow6... SUCCESS
1:03:55... Lab03-03.exe 10008 RegCloseKey HKLM\SOFTWARE\Microsoft\Wow6... SUCCESS
1:03:55... Lab03-03.exe 10008 Load Image C:\Windows\System32\wow64cpu.dll SUCCESS Image Base: 0x77...
1:03:55... Lab03-03.exe 10008 RegOpenKey HKLM\SYSTEM\CurrentControlSet\C... REPARSE Desired Access: Q...
1:03:55... Lab03-03.exe 10008 RegOpenKey HKLM\System\CurrentControlSet\Co... NAME NOT FOUND Desired Access: Q...
1:03:55... Lab03-03.exe 10008 RegOpenKey HKLM\SYSTEM\CurrentControlSet\C... REPARSE Desired Access: Q...
1:03:55... Lab03-03.exe 10008 RegOpenKey HKLM\System\CurrentControlSet\Co... SUCCESS Desired Access: Q...
1:03:55... Lab03-03.exe 10008 RegSetInfoKey HKLM\System\CurrentControlSet\Co... SUCCESS KeySetInformation...
1:03:55... Lab03-03.exe 10008 RegQueryValue HKLM\System\CurrentControlSet\Co... NAME NOT FOUND Length: 24
1:03:55... Lab03-03.exe 10008 RegCloseKey HKLM\System\CurrentControlSet\Co... SUCCESS
1:03:55... Lab03-03.exe 10008 CreateFile C:\Users\IEUser\Documents\its\Pract... SUCCESS Desired Access: E...
1:03:55... Lab03-03.exe 10008 Load Image C:\Windows\SysWOW64\kernel32.dll SUCCESS Image Base: 0x74...
1:03:55... Lab03-03.exe 10008 Load Image C:\Windows\SysWOW64\KernelBas... SUCCESS Image Base: 0x75...
1:03:55... Lab03-03.exe 10008 RegQueryValue HKLM\System\CurrentControlSet\Co... NAME NOT FOUND Length: 524
1:03:55... Lab03-03.exe 10008 QueryNameInfo... C:\Windows\SysWOW64\KernelBas... SUCCESS Name: \Windows\S...
Showing 346 of 424,854 events (0.081%)
Backed by virtual memory
Process Monitor Filter
Display entries matching these conditions:
Process Name is Lab03-03.exe then Include
Reset Add Remov
Column Relation Value Action
Process Na is Lab03-03.exe Include
PID is 11976 Include
Operation is Process Start Include
Operation is Thread Create Include
Operation is Process Create Include
Operation is RegSetValue Include
Process Na is Procmon.exe Exclude
OK Cancel Apply


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
1:03:55... Lab03-03.exe 10008 Process Create C:\Windows\SysWOW64\svchost.exe SUCCESS PID: 12508, Comm...
Process Monitor Filter
Display entries matching these conditions:
Process Name is Lab03-03.exe then Include
Reset
Add
Remov
Column Relation Value Action
Process Na is Lab03-03.exe Include
PID is 11976 Include
Operation is Process Start Include
Operation is Thread Create Include
Operation is Process Create Include
Operation is RegSetValue Include
Process Na is Procmon.exe Exclude
OK
Cancel
Apply


Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser]
File Options View Process Find DLL Users Help
Process CPU Private Bytes Working Set PID Description Company Name
cmd.exe 2,216 K 1,912 K 6932 Windows Command Processor Microsoft Corporation
conhost.exe 6,144 K 13,124 K 1052 Console Window Host Microsoft Corporation
010Editor.exe 47,496 K 26,412 K 11024 010 Editor - Professional Tex... SweetScape Software
Procmon.exe 2,968 K 15,928 K 7568 Process Monitor Sysinternals - www.sysinte...
Procmon64.exe 4.31 18,820 K 50,404 K 14408 Process Monitor Sysinternals - www.sysinte...
procexp64.exe 17.55 27,184 K 47,440 K 1496 Sysinternals Process Explorer Sysinternals - www.sysinte...
cmd.exe 3,672 K 3,240 K 356 Windows Command Processor Microsoft Corporation
conhost.exe 0.09 6,268 K 19,304 K 11888 Console Window Host Microsoft Corporation
Lab03-03.exe 612 K 3,060 K 10008
svchost.exe 560 K 424 K 12508 Host Process for Windows S... Microsoft Corporation
svchost.exe Susp... 248 K 52 K 12212 Host Process for Windows S... Microsoft Corporation
WerFault.exe < 0.01 3,652 K 9,672 K 7988 Windows Problem Reporting Microsoft Corporation
jusched.exe 1,528 K 5,324 K 7900 Java Update Scheduler Oracle Corporation

Lab 3-3: What to learn?

- A familiar process name can be used to hide.
- When the parent process dies, the child process is orphaned, making it more difficult to see where it came from.
- Normal svchost processes are children of services.exe, not orphaned.
- Do not trust a process just because it has a familiar name. If its location in the process hierarchy, its filepath or anything else is unusual, check it out.

Part 3: Reversing with IDA

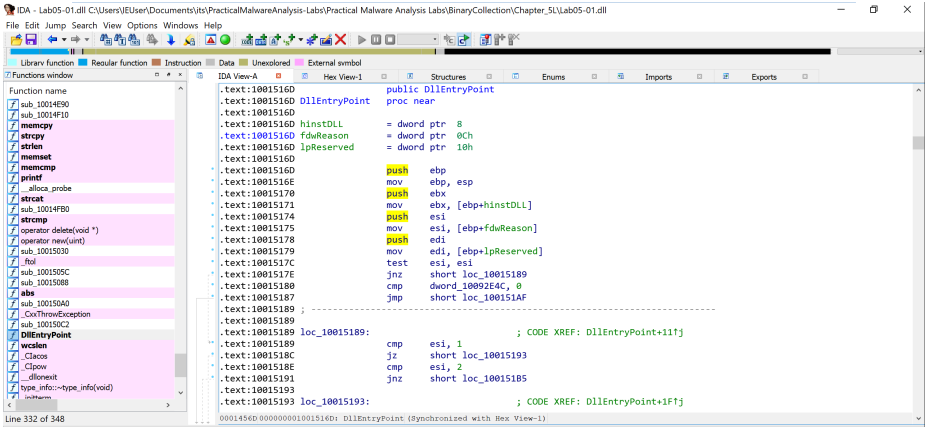
Do parts of Lab 5-1: Tasks 1-16

Part 3: What to learn

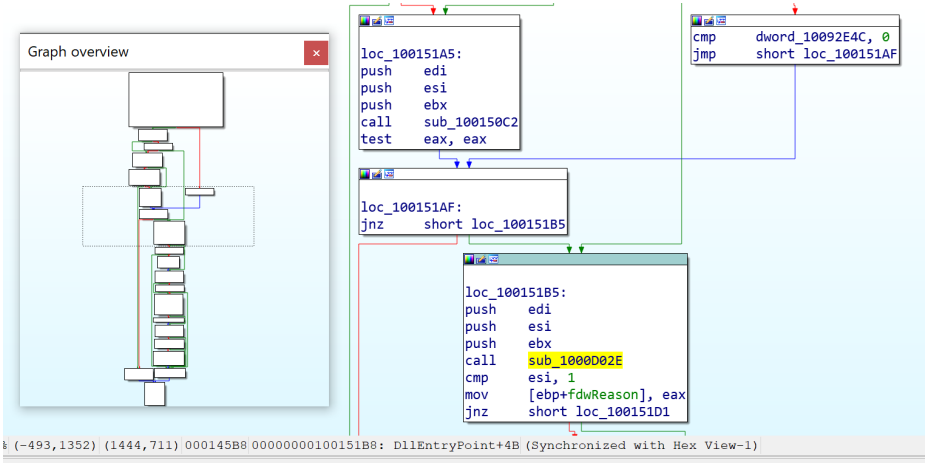
- Learn to navigate in IDA.
- Learn to find the types of information concerned in these tasks.
- Understand basic assembly. Example: How was the value put in eax? What are the parameters of the function?
- Be able to interpret IDA screenshots similar to the screenshots and relevant functions in this exercise.

1. What is the address of DllMain?

DllEntryPoint0x1001516D in the .text section

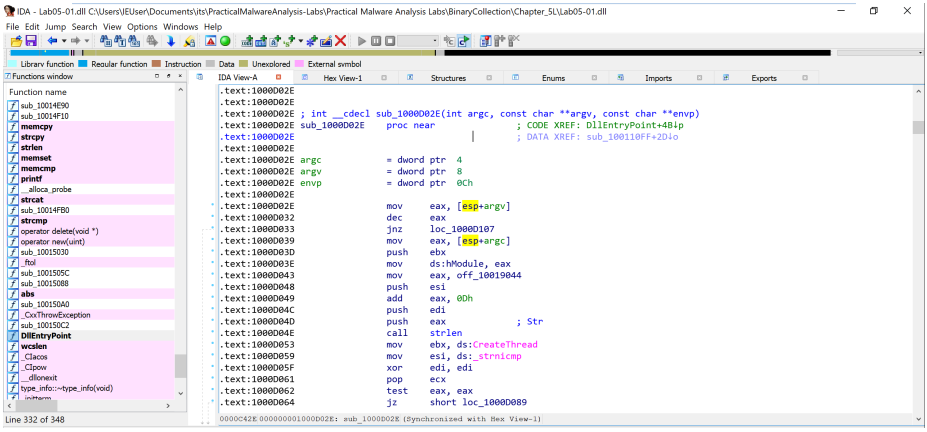


1. What is the address of DllMain?



1. What is the address of DllMain?

0x1000D02E in the .text section



2. Use the Imports window to browse to gethostbyname. Where is the import located?

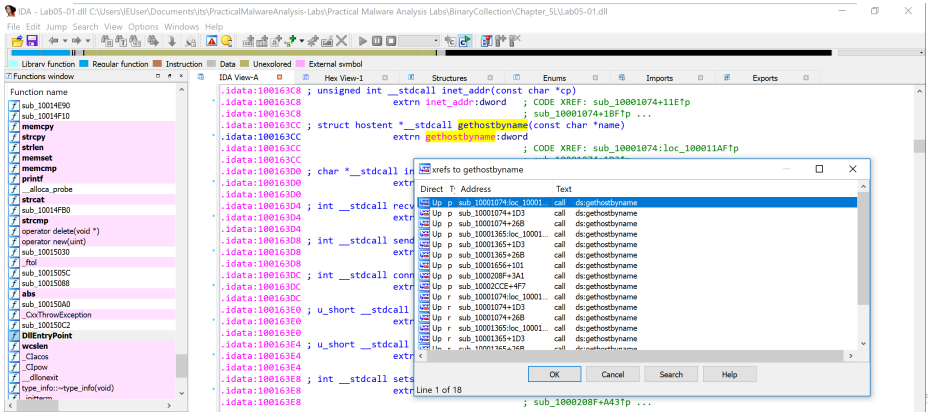
Start writing *gethostbyname* while in the Imports window.

0x100163CC in the .idata section

3. How many functions call gethostbyname?

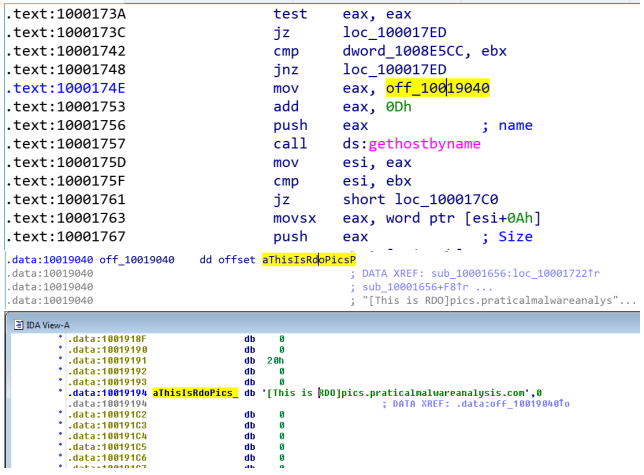
Double click in the Imports window. Press X while at the name.

It is called nine times, by five different functions.



4. Focusing on the call to gethostbyname at 0x10001757, which DNS request will be made?

pics.practicalmalwareanalysis.com



Consider the subroutine at 0x10001656

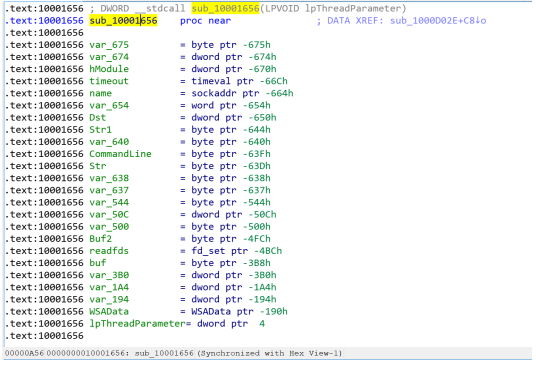
Press G and enter the address.

5. How many local variables has IDA recognized?

23, those with negative offsets. (Exact number may vary between versions.)

6. How many parameters has IDA recognized?

1, lpThreadParameter, which has positive offset



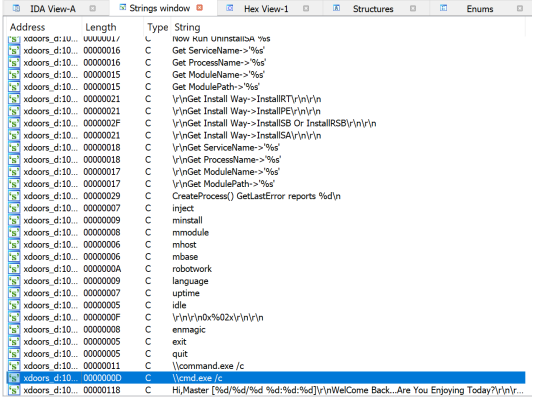
7. Use the Strings window to locate the string \cmd.exe /c in the disassembly. Where is it located?

View - Open subviews - Strings (Shift+F12)

Start writing the string to locate it. Note that the string is actually starting with \\.

Alternatively: Click the String column to sort alphabetically.

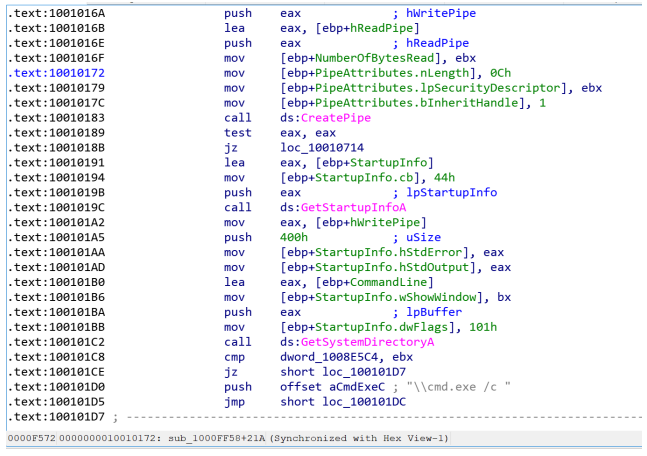
The string is located in the xdoors_d section.



8. What is happening in the area of code that references \cmd.exe /c?

Double click the string, press X to find cross references.

It appears to set up a remote shell connection. We see calls like *CreatePipe* and *recv*.

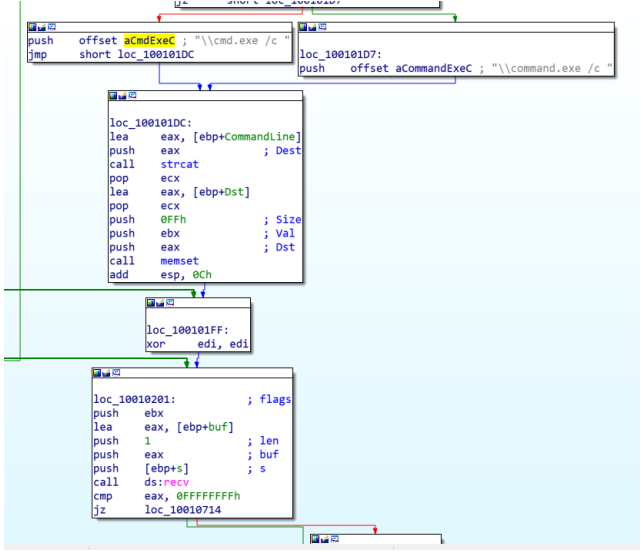


```
.text:1001016A                 push    eax             ; hWritePipe
.text:1001016B                 lea     eax, [ebp+hReadPipe]
.text:1001016E                 push    eax             ; hReadPipe
.text:1001016F                 mov     [ebp+NumberOfBytesRead], ebx
.text:10010172                 mov     [ebp+PipeAttributes.nLength], 0Ch
.text:10010179                 mov     [ebp+PipeAttributes.lpSecurityDescriptor], ebx
.text:1001017C                 mov     [ebp+PipeAttributes.bInheritHandle], 1
.text:10010183                 call    ds:CreatePipe
.text:10010189                 test    eax, eax
.text:1001018B                 jz      loc_10010714
.text:10010191                 lea     eax, [ebp+StartupInfo]
.text:10010194                 mov     [ebp+StartupInfo.cb], 44h
.text:1001019B                 push    eax             ; lpStartupInfo
.text:1001019C                 call    ds:GetStartupInfoA
.text:100101A2                 mov     eax, [ebp+hWritePipe]
.text:100101A5                 push    400h            ; uSize
.text:100101AA                 mov     [ebp+StartupInfo.hStdError], eax
.text:100101AD                 mov     [ebp+StartupInfo.hStdOutput], eax
.text:100101B0                 lea     eax, [ebp+CommandLine]
.text:100101B6                 mov     [ebp+StartupInfo.wShowWindow], bx
.text:100101BA                 push    eax             ; lpBuffer
.text:100101BB                 mov     [ebp+StartupInfo.dwFlags], 101h
.text:100101C2                 call    ds:GetSystemDirectoryA
.text:100101C8                 cmp     dword_1008E5C4, ebx
.text:100101CE                 jz      short loc_100101D7
.text:100101D0                 push    offset aCmdExeC ; "\\cmd.exe /c "
.text:100101D5                 jmp     short loc_100101DC
.text:100101D7 ; ---------------------------------------------------------------------------
0000F572 00000000010010172: sub_1000FF58+21A (Synchronized with Hex View-1)
```

8. What is happening in the area of code that references \cmd.exe /c?

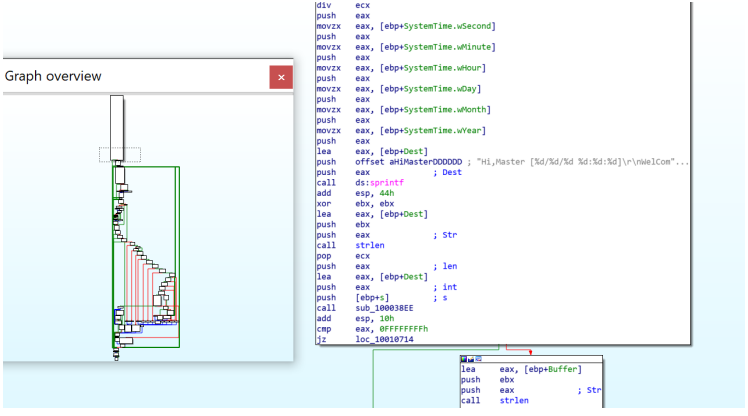
Double click the string, press X to find cross references.

It appears to set up a remote shell connection. We see calls like *CreatePipe* and *recv*.



8. What is happening in the area of code that references $\backslash cmd.exe\ /c$?

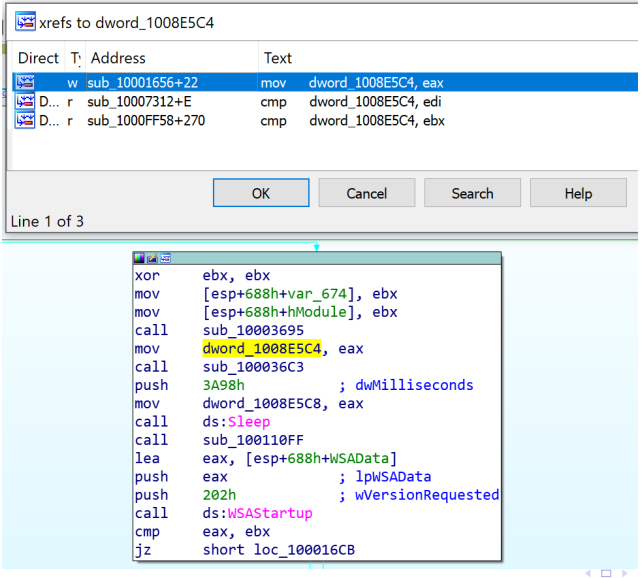
At the beginning of the same function, we see a string being used.




```
xdoors_d:10095B44 ; char aHiMasterDDDDDD[]
xdoors_d:10095B44 aHiMasterDDDDDD db 'Hi,Master [%d/%d/%d %d:%d:%d]',0Dh,0Ah
xdoors_d:10095B44                                       ; DATA XREF: sub_1000FF58+1451o
xdoors_d:10095B44                 db 'WelCome Back...Are You Enjoying Today?',0Dh,0Ah
xdoors_d:10095B44                 db 0Dh,0Ah
xdoors_d:10095B44                 db 'Machine UpTime  [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Secon'
xdoors_d:10095B44                 db 'ds]',0Dh,0Ah
xdoors_d:10095B44                 db 'Machine IdleTime [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Seco'
xdoors_d:10095B44                 db 'nds]',0Dh,0Ah
xdoors_d:10095B44                 db 0Dh,0Ah
xdoors_d:10095B44                 db 'Encrypt Magic Number For This Remote Shell Session [0x%02x]',0Dh,0Ah
xdoors_d:10095B44                 db 0Dh,0Ah,0
```

9. What is dword_1008E5C4?

Follow the cross reference for write, and the function call setting eax:



9. What is dword_1008E5C4?

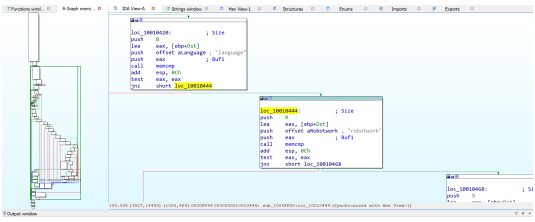
Follow the cross reference for write, and the function call setting eax to find the following function:

```
.text:10003695                                          ; sub_10003B75+74↓p ...
.text:10003695
.text:10003695 VersionInformation= _OSVERSIONINFOA ptr -94h
.text:10003695
.text:10003695                  push    ebp
.text:10003696                  mov     ebp, esp
.text:10003698                  sub     esp, 94h
.text:1000369E                  lea     eax, [ebp+VersionInformation]
.text:100036A4                  mov     [ebp+VersionInformation.dwOSVersionInfoSize], 94h
.text:100036AE                  push    eax             ; lpVersionInformation
.text:100036AF                  call    ds:GetVersionExA
.text:100036B5                  xor     eax, eax
.text:100036B7                  cmp     [ebp+VersionInformation.dwPlatformId], 2
.text:100036BE                  setz    al
.text:100036C1                  leave
.text:100036C2                  retn
.text:100036C2 sub_10003695     endp
.text:100036C2
```

It is the OS version.

10. In the subroutine at 0x1000FF58, what happens if the string comparison to robotwork is successful (when memcmp returns 0)?

The registry values at *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WorkTime* and WorkTimes are queried (and sent over the remote shell connection).

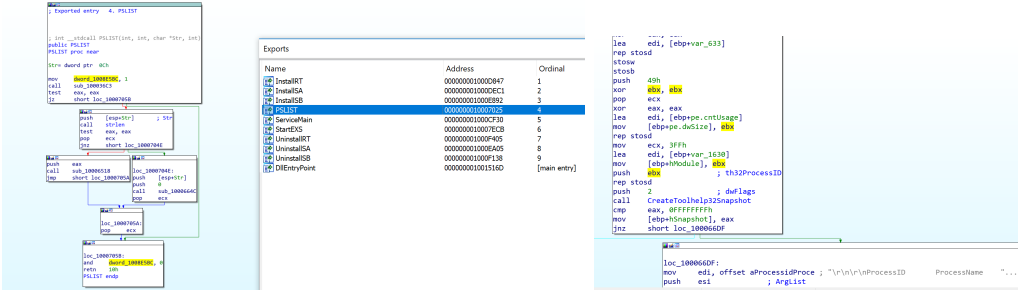


```
                                ; CODE XREF: su
push    9                       ; Size
lea     eax, [ebp+Dst]
push    offset aRobotwork ; "robotwork"
push    eax                     ; Buf1
call    memcmp
add     esp, 0Ch
test    eax, eax
jnz     short loc_10010468
push    [ebp+s]                 ; s
call    sub_100052A2
jmp     short loc_100103F6
```

```
.text:100052D9                 stosw
.text:100052DB                 stosb
.text:100052DC                 lea     eax, [ebp+phkResult]
.text:100052DF                 push    eax             ; phkResult
.text:100052E0                 push    0F003Fh         ; samDesired
.text:100052E5                 push    0               ; ulOptions
.text:100052E7                 push    offset aSoftwareMicros ; "SOFTWARE\\Microsoft\\Windows\\CurrentVe".
.text:100052EC                 push    80000002h       ; hKey
.text:100052F1                 call    ds:RegOpenKeyExA
.text:100052F7                 test    eax, eax
.text:100052F9                 jz      short loc_10005309
.text:100052FB                 push    [ebp+phkResult] ; hKey
.text:100052FE                 call    ds:RegCloseKey
.text:10005304                 jmp     loc_100053F6
.text:10005309 ; ---------------------------------------------------------------------------
.text:10005309
.text:10005309 loc_10005309:                           ; CODE XREF: sub_100052A2+57↑j
.text:10005309                 push    ebx
.text:1000530A                 lea     eax, [ebp+cbData]
.text:1000530D                 push    esi
.text:1000530E                 push    eax             ; lpcbData
.text:1000530F                 lea     eax, [ebp+Data]
.text:10005315                 mov     ebx, ds:RegQueryValueExA
.text:1000531B                 push    eax             ; lpData
.text:1000531C                 lea     eax, [ebp+Type]
.text:1000531F                 push    eax             ; lpType
.text:10005320                 push    0               ; lpReserved
.text:10005322                 push    offset aWorktime ; "WorkTime"
```

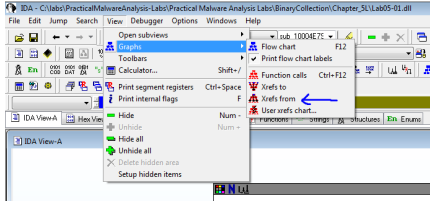
11. What does the export PSLIST do?

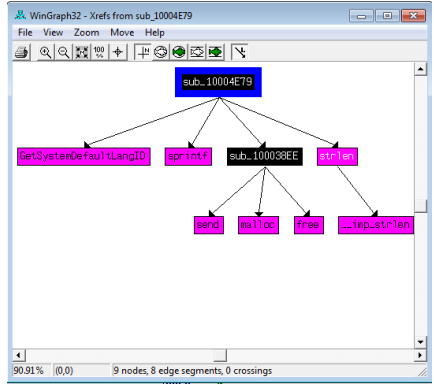
Find PSLIST in the Exports window. Double-click it to go to the function. It can take two code paths. Follow the calls in both paths. They use CreateToolhelp32Snapshot to help them grab a process listing and sending the result over the socket.



12. Graph the cross references from sub_10004E79. Which API functions could be called by entering this function? What could you rename this function?

Go to the function, and open the graph view while having the cursor at the function name. GetSystemDefaultLangID, send, and sprintf are called. It could be called GetSystemLanguage.

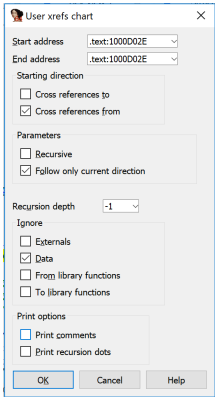


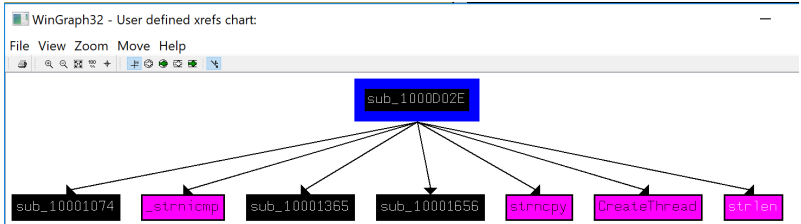


13. How many Windows API functions does DllMain call directly? How many at depth 2?

View→Graphs→User xrefs chart

Direct calls: strncpy, strnicmp, CreateThread, and strlen. Several at depth 2.





14. At 0x10001385 there is a call to Sleep. How long will the program sleep?

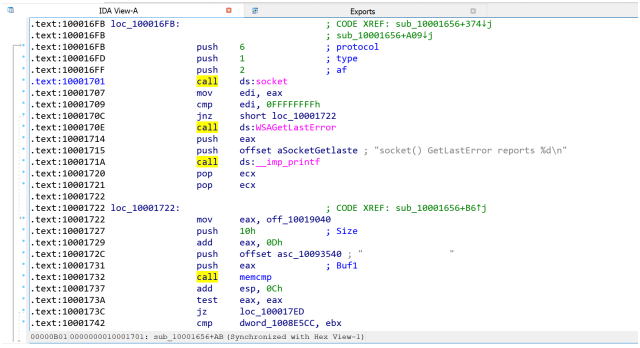
- off_10019020 leads us to the string **[This is CTI]30**
- eax is set to 30 ms using the value found from off_10019020+D.
- eax is multiplied by 1000, giving 30 seconds.

To change the number 3E8h into decimal 1000, rightclick and choose decimal format.

```
.text:1000133B
.text:1000133B loc_1000133B:                           ; CODE XREF: sub_10001074+71↑j
.text:1000133B                 mov     dword_1008E5CC, ebp
.text:10001341
.text:10001341 loc_10001341:                           ; CODE XREF: sub_10001074+10F↑j
.text:10001341                                         ; sub_10001074+1B0↑j ...
.text:10001341                 mov     eax, off_10019020
.text:10001346                 add     eax, 0Dh
.text:10001349                 push    eax             ; Str
.text:1000134A                 call    ds:atoi
.text:10001350                 imul    eax, 3E8h
.text:10001356                 pop     ecx
.text:10001357                 push    eax             ; dwMilliseconds
.text:10001358                 call    ds:Sleep
.text:1000135E                 xor     ebp, ebp
.text:10001360                 jmp     loc_100010B4
.text:10001360 sub_10001074    endp
```

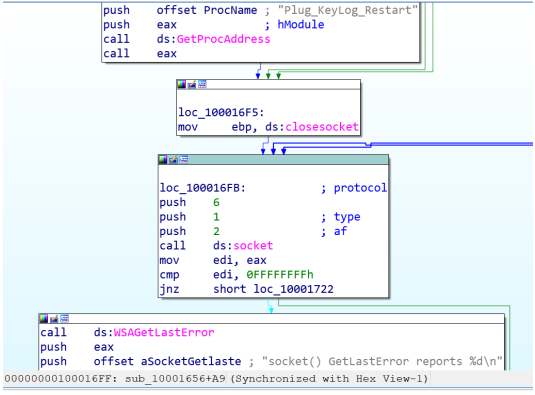
15. At 0x10001701 is a call to the function *socket*. What are the three parameters?

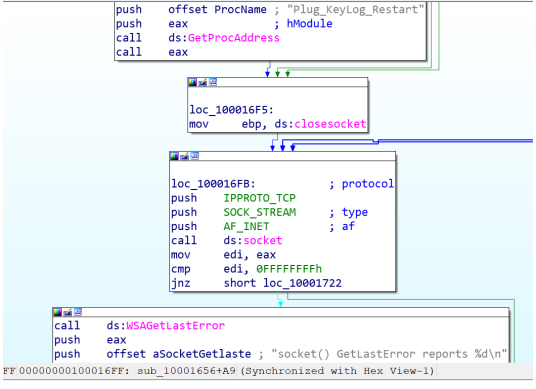
6, 1 and 2.



16. Use the MSDN page for socket and the named sumbolic constants functionality in IDA to make the parameters more meaningful.

Find the list of relevant named symbolic constants at: `https://docs.microsoft.com/en-us/windows/win32/api/winsock2/nf-winsock2-socket`





Part 4: Executable with known source

Use the source code to see what the executable does.
Find out the same using Process Monitor, Process Explorer, and IDA.

Part 4: What to learn

- Learn to navigate in IDA and understand what you see.
- Identify the command line parameters. Learn to recognize command line parameters in IDA.
- In dynamic analysis, what you see happening is not necessarily everything the executable can do.
- Run the executable with all variants of input to see all types of behavior. Find the related events in Process Monitor.
- When you want to learn how to reverse a specific behavior, you can write a related program, compile it and reverse it.

Exercise Task 3

Part 1: Integers

If your computer program uses unsigned 8-bit integers, what will the result of the following be?

- $255 + 2 = 1$
- $0 - 1 = 255$

If your computer program used signed 8-bit integers, what would the result of the following be:

- $0 - 1 =$ -1

Exercise Task 3

Part 2: Stack cookies

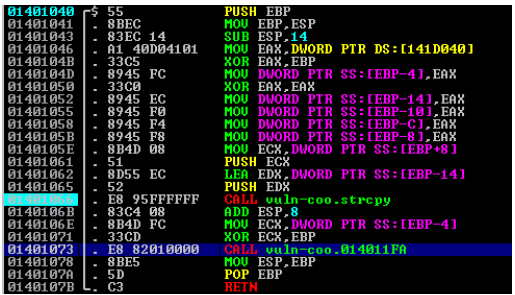
- Read the section 30.3.1 in *Low level Software Security by Example* (linked from Canvas).
- Go to the Files folder in Canvas and download and extract `lecture03.zip` .
- Make a text file containing at least 28 A's, and place it in the folder `vuln-cookie`.
- Open vuln-cookie.exe in Immunity Debugger, with the text file as an argument.
- Place a breakpoint (F2) at the address 0x01401066, and run (F9) until you hit the breakpoint.
- Step over (F8) the call to `strcpy`. Notice that `strcpy` overflows the return address of the current function.
- Continue running (F9), and notice that the program does not attempt to return into 41414141. Why is that?

Exercise Task 3

Part 2: Stack cookies

Viewing the disassembly of our function, we see that a cookie gets loaded into EAX (01401046), then XOR'ed with the frame pointer (0140104B) and placed on the stack as a canary (0140104D).

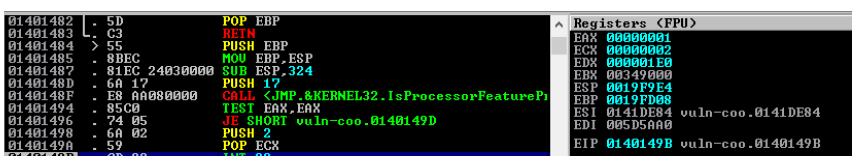
Before restoring the frame pointer and returning, the canary is fetched from the stack (0140106E), XOR'ed with the frame pointer (01401071) and then checked with a call to `vuln-coo.014011FA` (01401073)



Exercise Task 3

Part 2: Stack cookies

When we continue running after the call to `strcpy`, an interrupt (INT29)is issued by `vuln-coo.014011FA`. This is a Windows mechanism called *fast fail*, and is a way for a potentially corrupted process to request immediate process termination. The constant 2 which is loaded into ECX before issuing the interrupt, is the fast fail failure code for a stack cookie check failure.



Exercise Task 3

Part 3: Size checking

Give a fix to the flaw in the code below for concatenating two strings:

```
char buf[128];
combine(char *s1, size_t len1,
        char *s2, size_t len2)
{
  if (len1 + len2 + 1 <= sizeof(buf)) {
    strncpy(buf, s1, len1);
    strncat(buf, s2, len2);
  }
}
```

Exercise Task 3

Part 3: Size checking

```
char buf[128];
combine(char *s1, size_t len1,
        char *s2, size_t len2)
{
  if (len1 + len2 + 1 <= sizeof(buf) && len1 < len1 + len2) {
    strncpy(buf, s1, len1);
    strncat(buf, s2, len2);
  }
}
```

For an n bit unsigned integer, the maximal value for len2 is 2^n-1 , and len1 + $2^n - 1$ mod 2^n = len1 − 1; if there is an integer overflow, the result will be smaller than len1. (No claim that this is the optimal solution.)

Exercise Task 4

Part 1: Stack canaries

- Explain the principle of stack canaries, and how it protects specific pointers stored in a stack frame.

  A stack canary is a specific value placed inside the call stack frame, at the memory address just above (i.e. with lower address than) the saved EBP and the saved EIP to protect those values. The program verifies that the stack canary has not been modified before the program pops (fetches) the saved EIP and EBP to exit the call. If the stack canary has not been modified, then it is unlikely that the saved EIP and EBP have been modified by a buffer overflow, so the program continues normally. If the stack canary has been modified, then it is likely that the saved EIP and EBP have been modified, which is a sign of a buffer overflow attack, so the program is terminated.

Exercise Task 4

Part 1: Stack canaries

- What are the disadvantages of using stack canaries?

  Disadvantages are:

  - Slows down the computer, because it creates overhead code to be executed.
  - Only protects EIP and EBP values, not the rest of the stack frame.

Exercise Task 4

Part 1: Stack canaries

- Explain very roughly a scenario for attacking stack canaries so that buffer overflow attacks will not be detected.

  If the attacker can recompute/learn the valid stack canary value, then the attacker can keep the canary value unchanged when overflowing EBP and EIP.

  Also, if the attacker's code executes before returning from the function, the stack cookie will not stop the attack.

Exercise Task 4

Part 2: Data Execution Prevention (DEP)/Non-executable stack (NX)

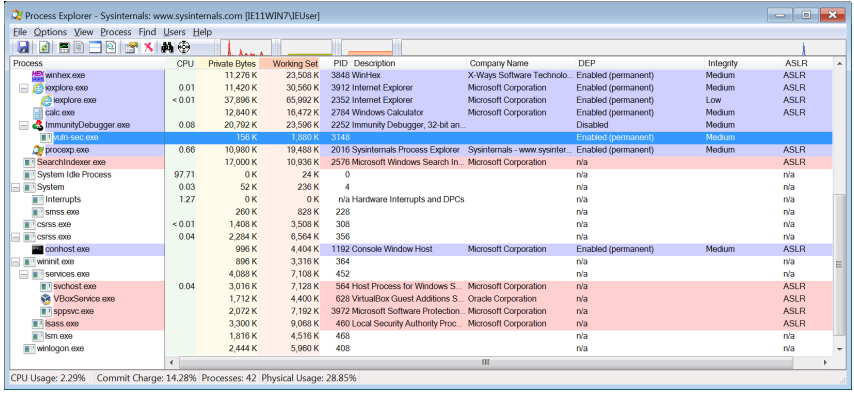
- Go to the Files folder in Canvas and download and extract `lecture04.zip` .
- Open `vuln-sec.exe` in Immunity Debugger, with the file `input.bin` as an argument.
- Open Process Explorer (procexp.exe) from Sysinternals, and check if `vuln-sec.exe` has ASLR and DEP enabled.
- Place a breakpoint (F2) at the address 0x00401027, and run (F9) until you hit the breakpoint.
- Step over (F8) the call to `strcpy`. Notice that `strcpy` overflows the return address of the current function.
- Single step (F7) until the function return, and we jump into the stack. What happens when we try to execute the NOPs?

Exercise Task 4

Part 2: Data Execution Prevention (DEP)/Non-executable stack (NX)

- Open Process Explorer (procexp.exe) from Sysinternals, and check if `vuln-sec.exe` has ASLR and DEP enabled.

We see that DEP has been enabled, but not ASLR.

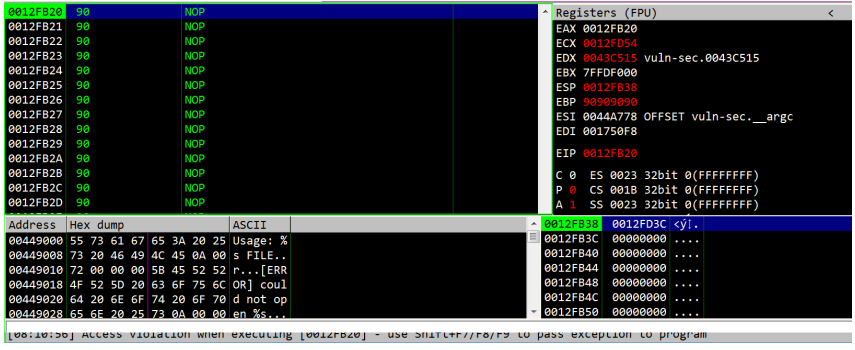


Exercise Task 4

Part 2: Data Execution Prevention (DEP)/Non-executable stack (NX)

- Single step (F7) until the function return, and we jump into the stack. What happens when we try to execute the NOPs?

We get an Access Violation when trying to execute the instruction on the stack, as it is marked non-executable.



Exercise Task 4

Part 3: Address space layout randomization (ASLR)

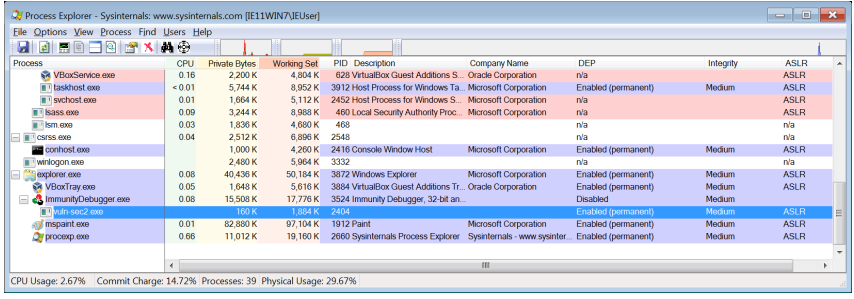
- Open `vuln-sec2.exe` in Immunity Debugger, with the file `input.bin` as an argument.
- Open Process Explorer (procexp.exe) from Sysinternals, and check if `vuln-sec2.exe` has ASLR and DEP enabled.
- Try to find the address of the call to `strcpy` (hint: offset 0x27 from the beginning of the file).
- Place a breakpoint (F2) at the address you found, and run (F9) until you hit the breakpoint.
- Step over (F8) the call to `strcpy`. Notice that `strcpy` overflows the return address of the current function.
- What happens when the function returns? In what way does it differ from what happened in Part 2?

Exercise Task 4

Part 3: Address space layout randomization (ASLR)

- Open Process Explorer (procexp.exe) from Sysinternals, and check if `vuln-sec2.exe` has ASLR and DEP enabled.

We see that both DEP and ASLR have been enabled.

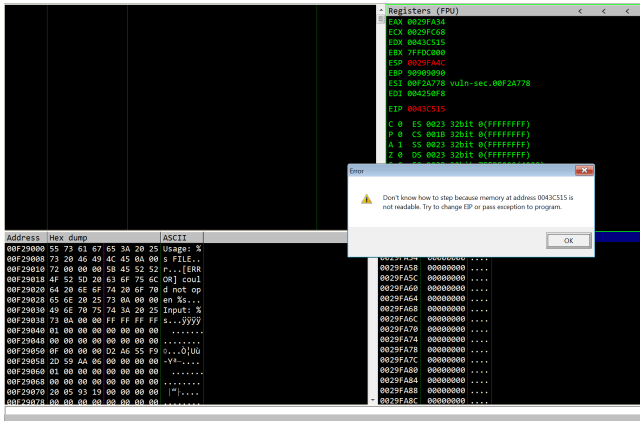


Exercise Task 4

Part 3: Address space layout randomization (ASLR)

- What happens when the function returns? In what way does it differ from what happened in Part 2?

The address we return into is not mapped, and the program crashes.



Exercise Task 4

Part 4: DEP/NX and ASLR questions

- Explain the principle of DEP/NX.

  DEP/NX is a mechanism that allows ranges of memory locations to be marked as non-executable. The stack does not normally contain executable code, so the stack memory can be marked as non-executable. Even if an attacker is able to inject malicious code into the stack, the malicious code will not be executed even if the instruction pointer is set to point to it, instead the program or computer will simply crash.

Exercise Task 4

Part 4: DEP/NX and ASLR questions

- Describe a type of buffer overflow attack that cannot be prevented by DEP/NX.

  DEP/NX does not protect against attacks where the attacker redirects the control flow to existing, executable code in the program's memory.

  This class of attacks are typically referred to as *return-to-libc*, where the attacker modifies the saved EIP so that the program execution returns to specific program library functions that by definition is executable.

  ROP (return-oriented programming) is a variant, where the attacker chain together numerous small pieces of code (called *gadgets*), all ending in the return instruction, each doing a small amount of useful work for the attacker. We will talk more about ROP in the last lecture of the course.

Exercise Task 4

Part 4: DEP/NX and ASLR questions

- Explain the principle of ASLR.

  ASLR hinders buffer overflow attacks by making it more difficult for an attacker to predict target memory addresses.

  For example, attackers trying to execute code using *return-to-libc* must first locate the code to be executed, and if that is difficult then the attack will most likely fail.

  With ASLR the memory addresses have to be guessed or leaked, and a mistaken guess will usually lead to the application crashing.

Exercise Task 4

Part 4: DEP/NX and ASLR questions

- Is enabling ASLR for just the main executable sufficient, or should it be enabled for all the dynamically linked libraries as well?

  For ASLR to be efficient, all the dynamically linked libraries must have ASLR enabled. Almost all libraries will have enough reusable code fragments the attacker can use to eventually gain arbitrary code execution.

Exercise Task 5

Part 1: Password length

Assume that a password can only contain the 26 characters from the alphabet.

- How many different passwords are possible if a password is at most n, n = 4,6,8, characters long and there is no distinction between upper case and lower case characters?

4 characters:	$26^4 + 26^3 + 26^2 + 26$	$= 4.75 * 10^5$
6 characters:	$26^6 + 26^5 + 26^4 + 26^3 + 26^2 + 26$	$= 3.21 * 10^8$
8 characters:	$26^8 + 26^7 + 26^6 + 26^5 + 26^4 + 26^3 + 26^2 + 26$	$= 2.17 * 10^{11}$

Exercise Task 5

Part 1: Password length

Assume that a password can only contain the 26 characters from the alphabet.

- How many different passwords are possible if a password is at most n, n = 4,6,8, characters long and passwords are case sensitive?

$$
\begin{array}{lll}
\text{4 characters:} & 52^4 + 52^3 + 52^2 + 52 & = 1.52 * 10^7 \\
\text{6 characters:} & 52^6 + 52^5 + 52^4 + 52^3 + 52^2 + 52 & = 4.11 * 10^{10} \\
\text{8 characters:} & 52^8 + 52^7 + 52^6 + 52^5 + 52^4 + 52^3 + 52^2 + 52 & = 1.11 * 10^{14}
\end{array}
$$

Exercise Task 5

Part 2: Brute force

Assume that passwords have length six and all alphanumerical characters, upper and lower case, can be used in their construction. How long will a brute force attack take on average if:

- it takes one tenth of a second to check a password?
- it takes a microsecond to check a password?

There are 62 symbols, so overall there are 62^6 possible passwords. In the first case, the search takes about 91 years, in the second case about 8 hours. The purpose of the exercise is to demonstrate that speed-ups in password checking are not relevant to individual end users but help an attacker.

Exercise Task 5

Part 3: Hashes and salts

1. What is the advantage of storing password databases as hash values instead of in plaintext?

Should an attacker obtain a copy of the passwords database, then the attacker does not get passwords directly if they are stored as hash values. The one-way property of hash functions makes it computationally infeasible to find a password from the hash value.

Exercise Task 5

Part 3: Hashes and salts

1. What is the advantage of storing passwords as salted hash values instead of just as hash values?

Should an attacker obtain a copy of a database of hashed passwords, then the attacker could use a precomputed hash table of all possible or likely passwords up to a certain length. The computing and storage capacity in modern devices makes it possible to prepare such hash tables. Then the attacker could just look up each password hash value in the hash table to find the plaintext password. In order to prevent this attack, hashing passwords with a salt (random value) would force the attacker to compute a separate hash table for every salt value, which isn't feasible, making precomputed hash/rainbow tables useless. Hence, salting makes it much more difficult to crack hashed passwords.

In addition, salting the password before hashing ensures that equal passwords get different hash values. In case one password has been cracked, this prevents attack against multiple users with the same password.

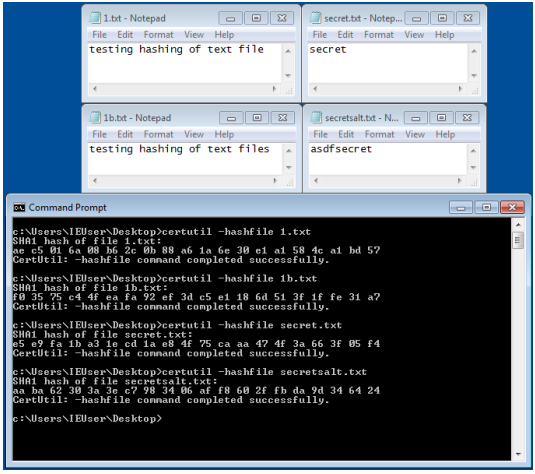
Exercise Task 5

Part 4: More hashes and salts

- Create a text file (`c:\pw.txt`) on your Windows 10 VM, and write a random string (without any linebreaks).
- Open a command prompt and use the command `certutil` to hash the file: `certutil -hashfile c:\pw.txt SHA1`.
- Make note of the hash value.
- Add a single character to the text file.
- Hash the file again, and note the hash value. Is it similar to the previous hash?
- Substitute the string with the word *secret*, and rehash the file. Do you get the same result as in the lecture slides?
- Try rehashing after appending the salt used in the slides.

Exercise Task 5

Part 4: More hashes and salts



Exercise Task 5

Part 5: Decryption

You have found the following data in binary format: d=000011110000111100000001
Reversing of the malware told you that you first need to xor the data with the string *key*, and thereafter reverse a Caesar cipher with a shift of 5. Decrypt it and write it as an ASCII string:

1. Write *key* in binary format using an ASCII table (e.g. a = 01100001) and xor the result with the data d.
2. Convert the result from binary format to ASCII.
3. Replace each letter with the letter five positions earlier in the alphabet (A-Z). Wrap around if neccessary.

Perform the steps by hand to master the techniques.
Resource: `http://sticksandstones.kstrom.com/appen.html`

Exercise Task 5

Part 5: Decryption

1. Write *key* in binary format using an ASCII table (e.g. a = 01100001):

key = 011010110110010101111001

Xor the result with the data *d*=000011110000111100000001:

011010110110010101111001
000011110000111100000001
011001000110101001111000

2. Convert the result from binary format to ASCII:

011001000110101001111000 = djx

3. Replace each letter with the letter five positions earlier in the alphabet (A-Z). Wrap around if neccessary.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U

d = y, j = e, x= s

The data *d* decodes to *yes*.

Resource: `http://sticksandstones.kstrom.com/appen.html`

Exercise Task 6

Part 1: Questions

1. In Linux, access rights are defined for users and groups. To facilitate better security management, users are placed into groups. How does Linux decide on an access request when an individual user has fewer privileges than its group?

   In Linux there are only positive access rights, and permission bits are examined in the order of priority: owner $>$ group $>$ others. When the user in question is the owner, and the owner does not have a required right that has been given to the group, access will be denied. When the user is not the owner, access will be granted.

Exercise Task 6

Part 1: Questions

2. How can access rights given to a group be withheld from individual members of that group?

   In standard Linux there is no mechanism to withhold rights from individual group members. A workaround might be to create a new group without that particular member, and let this new group own the resource.

Exercise Task 6

Part 1: Questions

3. In Linux systems users have a UID and username. Explain the relationship between usernames and UIDs. Which identifier is used for authentication, and which identifier is used to make access control decisions? Where are passwords stored in Linux systems, and who has access to them?

   In Linux systems each user has a username which is mapped to a UID (User Identity). Multiple users can be mapped to the same UID, but a single username can only have a single UID. The username is the key to find the hashed password which is used for user authentication. The UID is used when the system approves access to resources.

Exercise Task 6

Part 1: Questions

4. How are passwords protected in Linux systems?

Passwords are normally stored in a salted and hashed form to make brute force cracking as difficult as possible. Systems administrators can reduce the likelihood of brute force attacks by making the list of hashed passwords unreadable by unprivileged users. A simple way to do this would be to make the passwd file itself readable only by the root user. However, this would restrict access to other data in that file such as username-to-UID mappings, which would break many existing utilities and provisions. The typical solution is to let a "shadow" password file hold the password hashes separate from the other data in the world-readable passwd file. For local files, this is usually /etc/shadow on Linux and Unix systems, which readable only by root. In networked environments the password hashes are typically located in an LDAP directory and accessible by root processes through the LDAP protocol.

Exercise Task 6

Part 2: Users and Groups

This practical exercise will introduce user and group management in Linux.

Part 2a: Download Xubuntu

- Download the Linux virtual machine (Xubuntu) from `http://unik4270.project.ifi.uio.no/xubuntu.zip`.
- Extract the zip-file and open the VM in VirtualBox.
- Log in with the username student and the password tek5510.

Exercise Task 6

Part 2b: User creation

First we need to create some users at our system. Do this by opening the Xubuntu menu in the top left corner, and start writing Settings Manager in the search field. Open it when it shows in the result pane. Start writing Users and Groups in the search field of the Settings window. Open it when it shows in the result pane.

You have now opened the User Settings window. Click the Add button. Provide the Student user password when asked to authenticate.

1. Create the user Ole and give him a password.
2. Create the user Dole, and give him the same password as Ole.
3. Create the user Doffen with a different password than the others.

Exercise Task 6

Part 2c: The /etc/shadow file

Take a look at the /etc/shadow file that stores the passwords. Detailed information about this file can be found at [1] or by issuing the command `man shadow` in a terminal.

Note that you need to have root privileges to access the file (`sudo cat /etc/shadow`).

```
student:$6$kQyS1yss$9eZnAMZXAz7Tyt45yPzHizh6Z/rnisHtQ5Bn2Nr0WQ/dB2horbL0ge8eARfg022de1Mol9Uxk9nrTrqDC7A3X0:16674:0:99999:7:::
vboxadd:!:16674::::::
ole:$6$9Roat28Y$qNKVHOPDuumeE9bkKdz.QUFaT56JvCuPOCHs9S13alryM/FgxLL6QGh5DL7JclgnaqKAU1dv7mB1mnhk4zJSy1:17448:0:99999:7:::
dole:$6$nSsUX5.Y$BTh8HlIImaPZAE5MP0kWVs.oNXa3KFY76ePuXlQpSFJK8Jwlv4Auue7UNSdktASRvfxMi6gay4fqhuNFrEfie0:17448:0:99999:7:::
doffen:$6$ZFQ0FFV7$o3ZmK1D8cHV/AvmS84xJ.58OrKR4WY5OJGLyni/GI8FtPZnPxgk39MvmrfKDqWrC3lmRdDBkZAqXTxaYDOXaN/:17448:0:99999:7:::
student@student-vm:~$
```

[1] `http://www.cyberciti.biz/faq/understanding-etcshadow-file/`

Exercise Task 6

Part 2c: The /etc/shadow file

- What could happen if any users could read this file?

  They would get the password hashes, and could start cracking the passwords.

- What could happen if they could write?

  They could change the password hash (and salt) of any user to what they want, in effect setting the password.

Exercise Task 6

Part 2c: The /etc/shadow file

At the end of this file you should find your new users, and after the colon there is a prefix for the password between $ that indicates which hashing algorithm being used, and the hashed password is written from this and until the next colon.

- Are the hashed passwords for Ole and Dole the same?

  No, they are not.

- What does this mean? (Hint: `man crypt` in a terminal, and read the NOTES section.)

  From `man crypt`:

  ```
  So $5$salt$encrypted is an SHA-256 encoded password
  and $6$salt$encrypted is an SHA-512 encoded one.
  ```

  As Ole and Dole have different salts, their password hashes will be different.

Exercise Task 6

Part 2c: The /etc/shadow file

We have created (changed) the passwords today, so the "last password change field" should show (calculate to) today. Check if this is correct.

Tip: the command `date +%s` gives you seconds since 00:00:00, Jan 1, 1970 (a GNU extension).

```
ole:$6$9Roat28Y$qNKVHOPDuumeE9bkKdz.QUFaT56JvCuPOCHs9S13alryM/FgxLL6QGh5DL7JclgnaqKAU1dv7mB1mnhk4zJSy1:17448:0:99999:7:::
dole:$6$nSsUX5.Y$BTh8HlIImaPZAE5MP0kWVs.oNXa3KFY76ePuXlQpSFJK8Jwlv4Auue7UNSdktASRvfxMi6gay4fqhuNFrEfie0:17448:0:99999:7:::
doffen:$6$ZFQ0FFV7$o3ZmK1D8cHV/AvmS84xJ.58OrKR4WY5OJGLyni/GI8FtPZnPxgk39MvmrfKDqWrC3lmRdDBkZAqXTxaYDOXaN/:17448:0:99999:7:::
student@student-vm:~$ date +%s
1507567261
student@student-vm:~$ echo "1507567261 / (60*60*24)" | bc
17448
student@student-vm:~$
```

Exercise Task 6

Part 2d: The /etc/passwd file

Try to open the /etc/passwd file. Detailed information about this file can be found at [1] or by issuing the command `man 5 passwd` in a terminal (note the 5).

- What access do you have in user mode?

  Read access.

- What could go wrong if users could write to this file?

  They could alter the UID and GUID for their username, in effect giving themselves elevated privileges.

Hint: What would happen if you change your group access field into someone else's number for group access?

[1] `http://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/`

Exercise Task 6

Part 2d: The /etc/passwd file

Open /etc/passwd with root privileges (`pkexec mousepad /etc/passwd`) and change the line for Doffen such that it contains Ole's number for identity and group. Change the path to home directory to /home/Ole. Your change should look something like this (the number may vary):

```
Ole:x:1001:1001::/home/Ole:/bin/bash
Doffen:x:1001:1001::/home/Ole:/bin/bash
```

Log in as Doffen (you can do a logout/login from the menu, or you can use the command `su -l doffen`).

- Do you get access to Oles home directory? Yes.
- Do a `whoami`. What was the result? The result was ole.
- Can you think of a way to change the etc/passwd file to prevent another user from getting access to his files? Change his UID/GUID to another user.

Undo the changes made to /etc/passwd before proceeding to the next section.

Exercise Task 6

Part 2e: Groups

Go back to the User Settings window and press the Manage Groups button. Add two groups called woodpeckers and scrimshanker. Put Ole and Dole in the group woodpeckers. Put Dole and Doffen in the group scrimshanker.

Login as Ole using `su -l ole`. Make a file called tent.make using the touch command:

```
touch tent.make
```

Look at the permissions of tent.make by using ls:

```
ls -l tent.make   -rw-rw-r-- 1 ole ole 0 okt.  9 18:58 tent.make
```

Login as Dole and try to access the file.

- Did it work? Yes.
- Can you both read from and write to the file? No, only read.
- Why/why not? dole is not the owner, nor part of the ole group, so the permission for others apply.

Exercise Task 6

Part 2e: Groups

We need to change the group ownership of the file. Log on as Ole again and type:

```
chown :woodpeckers tent.make
```

Check that Dole has full access to the file now. Yes, Dole has full access.
Check that group access is working by switching to Doffen and check that he has not write access to the file. No, Doffen does not have write access.

Exercise Task 6

Part 2f: Multi-group membership

Log in as Doffen and create the file dirty.trick in the home directory. Now, change the ownership and perfmissions so that anyone in the scrimshanker group have full access to this file. Now, switch to Dole and check that you can write to the file. Check Doles group identity with the command id.

- How are memberships in several groups handled in this system?

  A user has one primary group, but can be member of several other groups. Any resource, however, belongs to one group only.

Exercise Task 7

Exercise Task 7

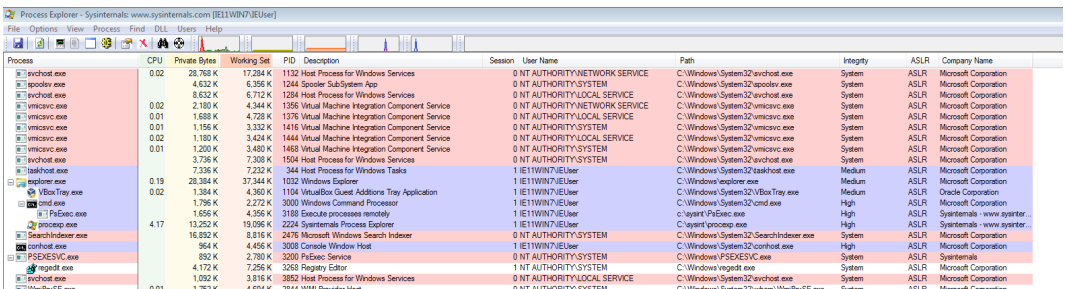
Part 1: Security related registry hives

1. Start Regedit as System: Psexec.exe –s –i regedit.exe
2. Use Process Explorer to confirm that it runs as System
3. Locate the SAM hive
4. Locate the System hive

Exercise Task 7

Part 1: Security related registry hives

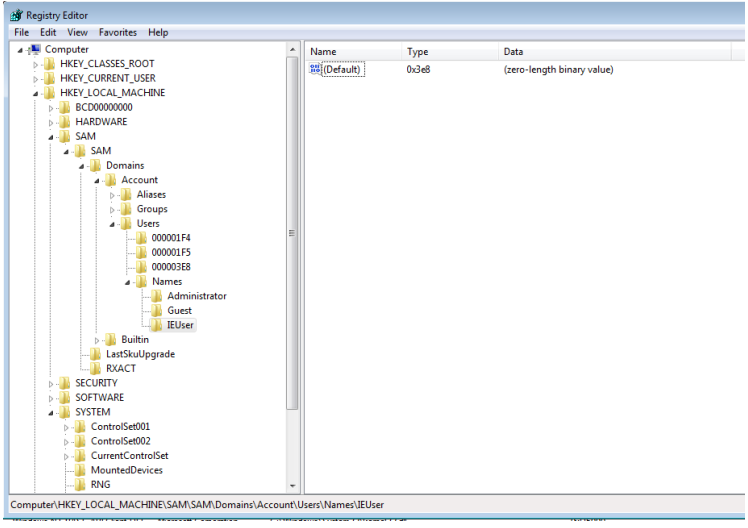
1. Start Regedit as System: Psexec.exe –s –i regedit.exe
2. Use Process Explorer to confirm that it runs as System



Exercise Task 7

Part 1: Security related registry hives

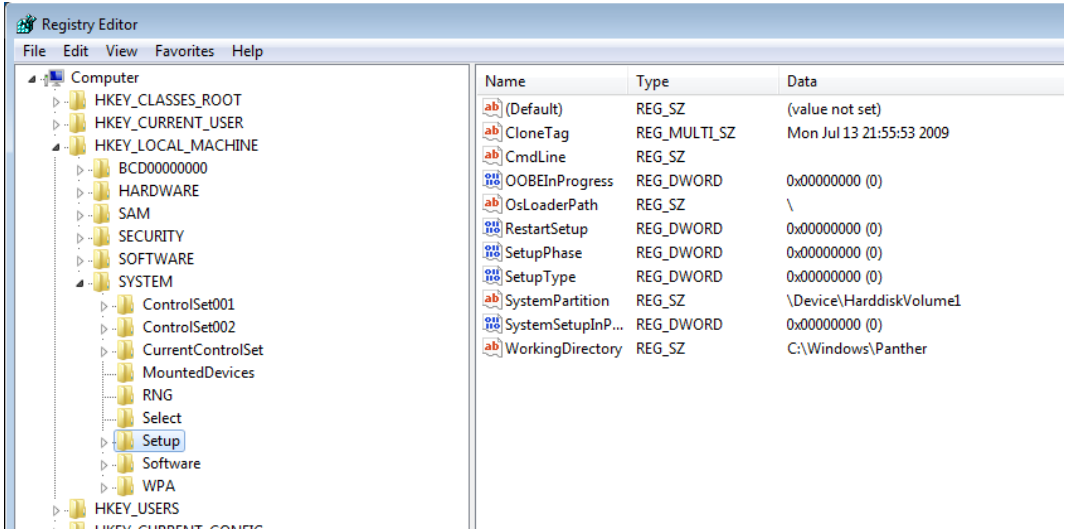
3 Locate the SAM hive



Exercise Task 7

Part 1: Security related registry hives

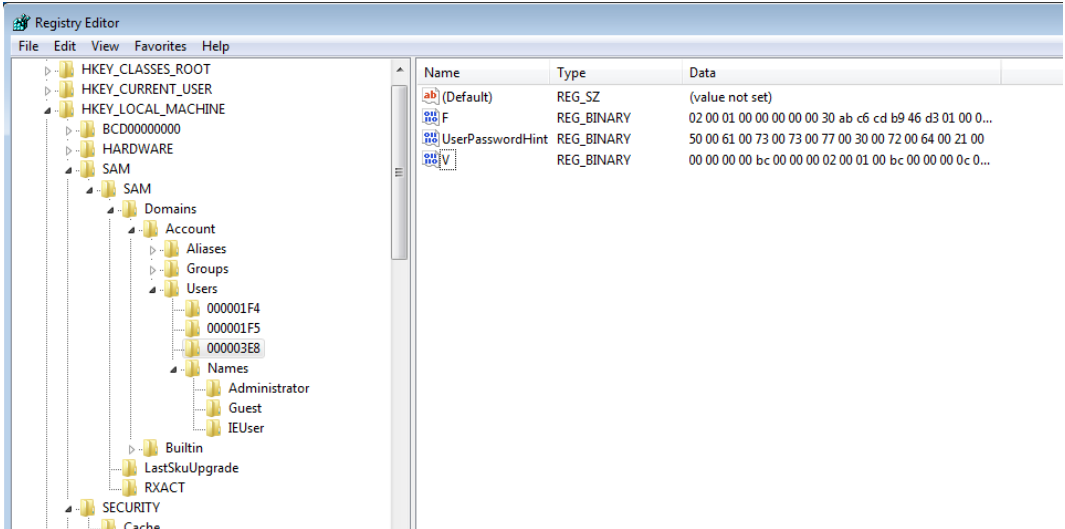
4 Locate the System hive



Exercise Task 7

Part 1: Security related registry hives

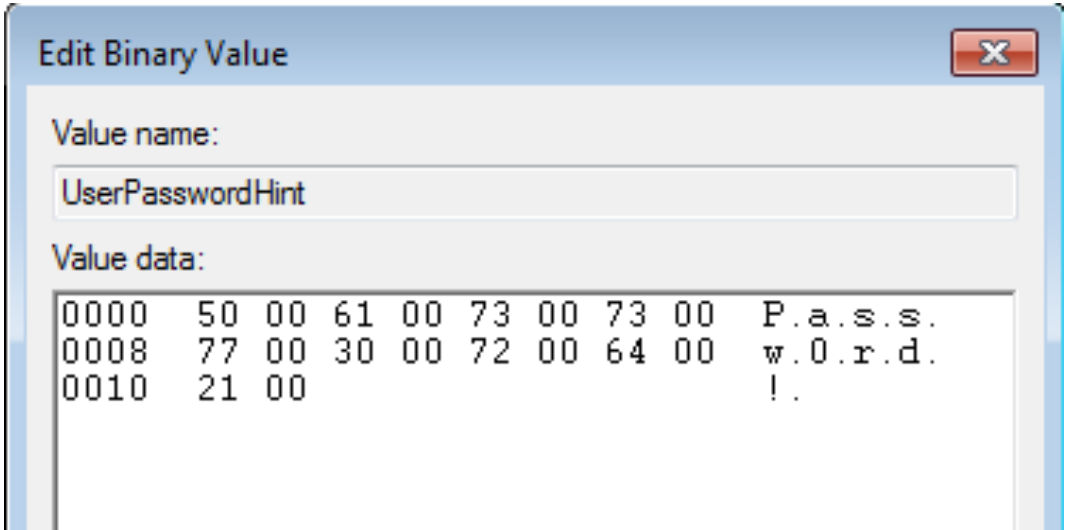
5 Find your stored user password



Exercise Task 7

Part 1: Security related registry hives

5 Find your stored user password



Exercise Task 7

Part 2: Tokens

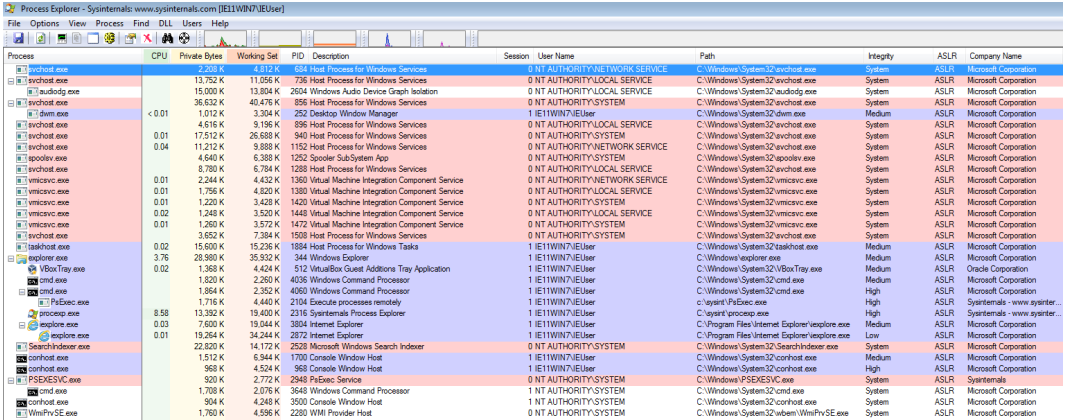
1. Start cmd.exe as normal user, Administrator and as System. (cmd as System: Psexec.exe –s –i cmd.exe)
2. Use Process Explorer to confirm that they run with Low, Medium and High integrity, respectively.
3. Use Process Hacker to investigate the tokens of the three processes.
4. Compare the tokens. What do you see?

Process Hacker: https://wj32.org/processhacker/nightly.php

Exercise Task 7

Part 2: Tokens

1. Start cmd.exe as normal user, Administrator and as System. (cmd as System: Psexec.exe –s –i cmd.exe)
2. Use Process Explorer to confirm that they run with Low, Medium and High integrity, respectively.



Exercise Task 7

Part 2: Tokens

3. Use Process Hacker to investigate the tokens of the three processes.
4. Compare the tokens. What do you see?