

Reverse Engineering

AND

Malware Analysis

Introduction to Reverse Engineering

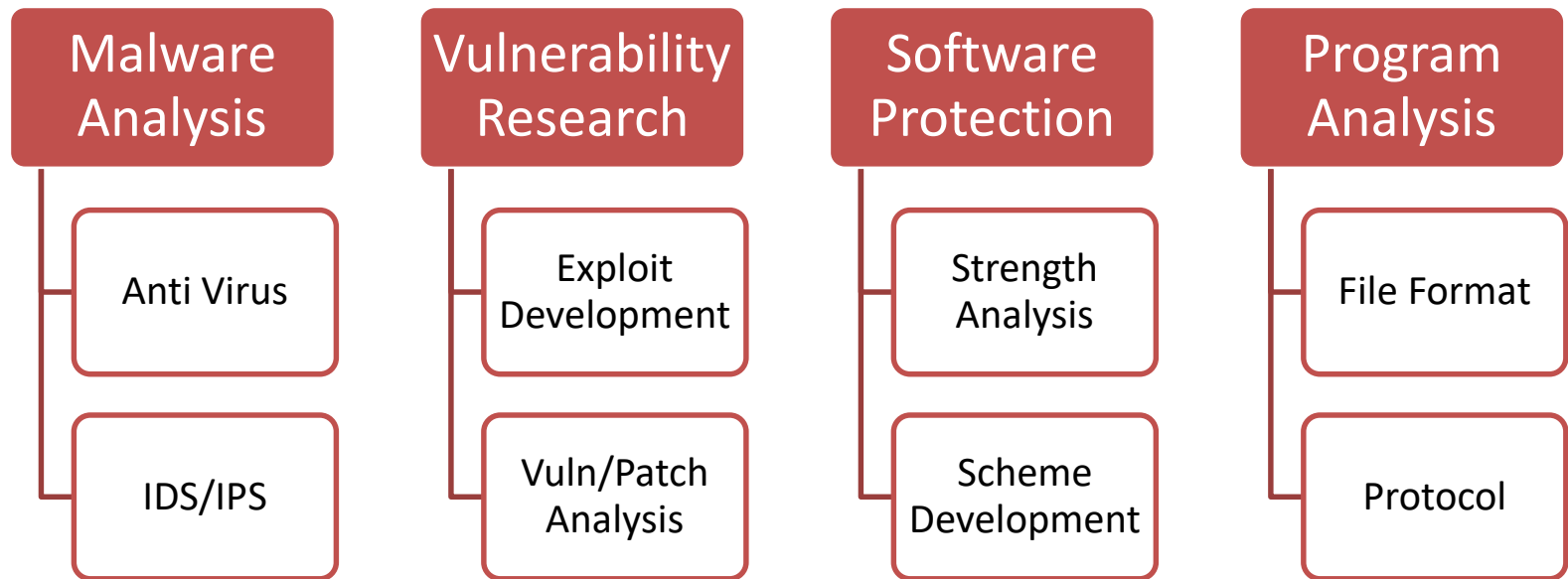
Reverse Engineering (RE): WHAT?

- In general – understanding the inner working of a system or deriving its blue prints from its functional sample can be called Reverse Engineering.

.. alternatively, quoting wikipedia:

- Reverse engineering is the process of discovering the technological principles of a device, object, or system through analysis of its structure, function, and operation.

RE: Common Motivation



RE: Methodology

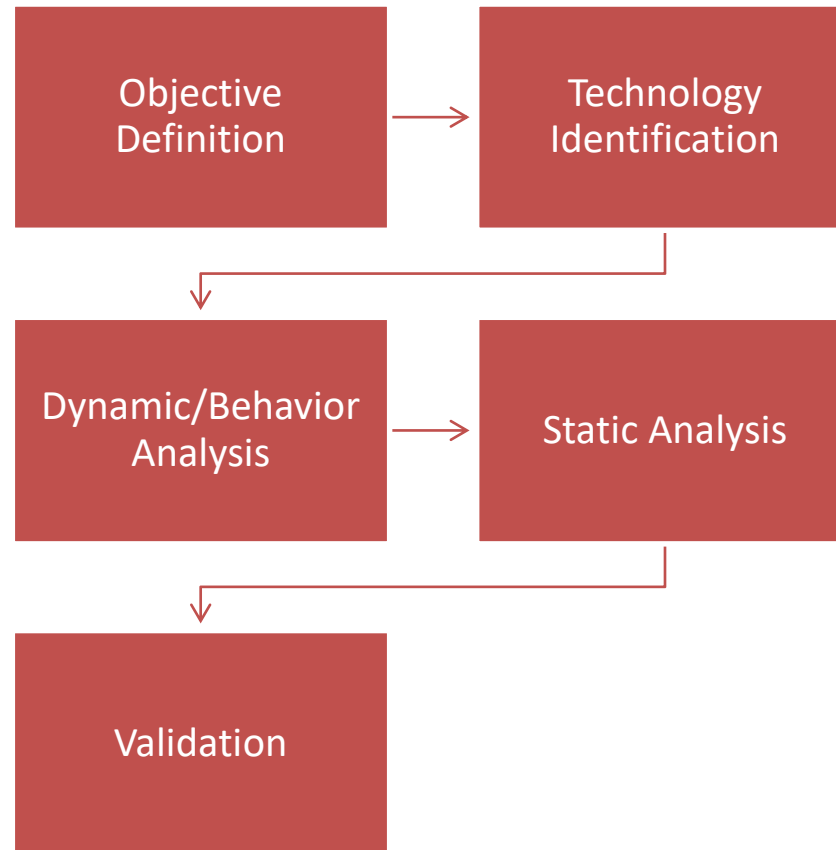


Static
Analysis



Dynamic
Analysis

RE: Basic Approach



Static Analysis

- The process of identifying the behavior and characteristics of a computer program statically i.e. **without actually executing it.**

This process is performed usually on the source code of the application or in case the source code is not available, it is subjected on the disassembled machine code of the application.

Static Analysis

Executable

- File Format Analysis
- Timestamp and Signature Analysis
- [...]

Code

- Disassembly / De-compilation (Logical)
- Program Logic Discovery
- Anti-Debug / Anti-RE bypass

Data

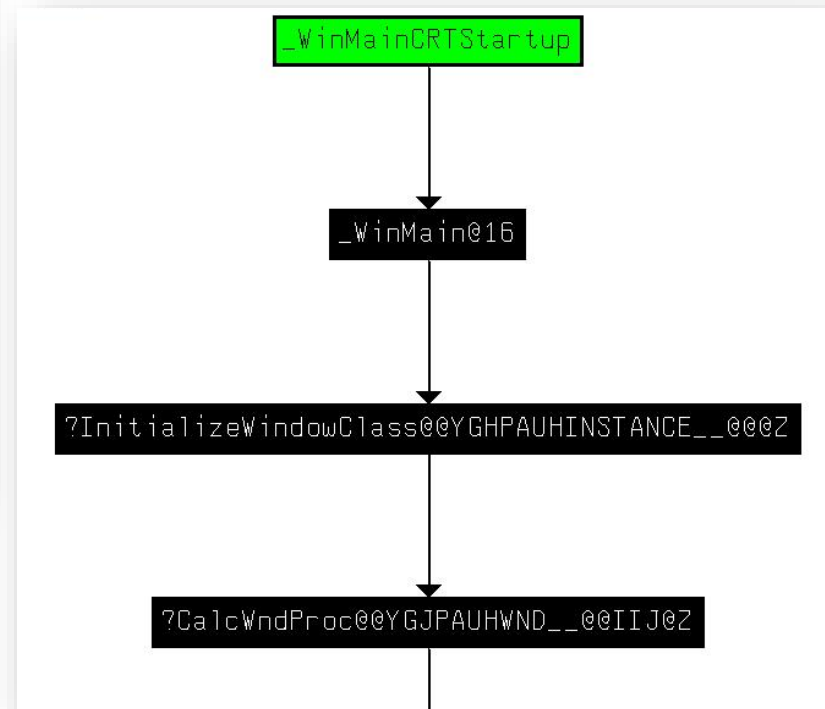
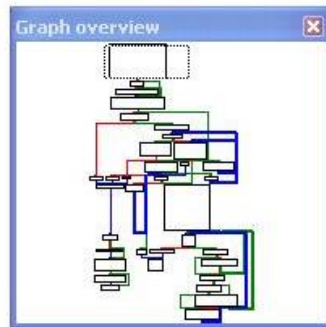
- Strings Analysis
- Configuration Analysis
- Hidden Code Discovery

Static Analysis

```
; int __stdcall WinMain(HINSTANCE hInstance,HINSTANCE hPrevInstance,LPSTR
_WinMain@16 proc near

hInstance= dword ptr  4
hPrevInstance= dword ptr  8
lpCmdLine= dword ptr  0Ch
nShowCmd= dword ptr  10h

mov     eax, offset sub_10128EE
call    __EH_prolog
sub     esp, 0F0h
push    ebx                ; wParamFilterMax
push    esi                ; wParamFilterMin
push    edi                ; hWnd
mov     [ebp-10h], esp
push    31h
pop     ecx
xor     eax, eax
xor     ebx, ebx
mov     [ebp-0FCh], bx
lea     edi, [ebp-0FAh]
rep stsd
stosw
lea     eax, [ebp-18h]
push    eax                ; lpMsg
call    ds:__imp_GetProcessDefaultLayout@4 ; GetProcessDefaultLayout(x)
test    eax, eax
jz      short loc_1001FA8
```



Dynamic Analysis

- The process of identifying the program logic and behavior of a given application by means of dynamic tracing and/or instrumentation **at runtime during its execution.**

The process usually involves hooking / intercepting various core platform APIs in order to understand its runtime characteristics.

Dynamic Analysis: Program Trace

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time...	Process Name	PID	Operation	Path	Result	Detail
4:34:3...	calc.exe	1920	Process Start		SUCCESS	Parent PID: 1604, ...
4:34:3...	calc.exe	1920	Thread Create		SUCCESS	Thread ID: 1808
4:34:3...	calc.exe	1920	QueryNameInfo...	C:\WINDOWS\system32\calc.exe	SUCCESS	Name: \WINDOW...
4:34:3...	calc.exe	1920	Load Image	C:\WINDOWS\system32\calc.exe	SUCCESS	Image Base: 0x100...
4:34:3...	calc.exe	1920	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
4:34:3...	calc.exe	1920	QueryNameInfo...	C:\WINDOWS\system32\calc.exe	SUCCESS	Name: \WINDOW...
4:34:3...	calc.exe	1920	CreateFile	C:\WINDOWS\Prefetch\CALC.EXE-02...	NAME NOT FOUND	Desired Access: G...
4:34:3...	calc.exe	1920	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: R...
4:34:3...	calc.exe	1920	CreateFile	C:\Documents and Settings\User1	SUCCESS	Desired Access: E...
4:34:3...	calc.exe	1920	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
4:34:3...	calc.exe	1920	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
4:34:3...	calc.exe	1920	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
4:34:3...	calc.exe	1920	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
4:34:3...	calc.exe	1920	Load Image	C:\WINDOWS\system32\shell32.dll	SUCCESS	Image Base: 0x7c9...
4:34:3...	calc.exe	1920	Load Image	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	Image Base: 0x77c...
4:34:3...	calc.exe	1920	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Image Base: 0x77f...
4:34:3...	calc.exe	1920	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x77d...
4:34:3...	calc.exe	1920	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d...
4:34:3...	calc.exe	1920	Load Image	C:\WINDOWS\system32\RPCRT4.dll	SUCCESS	Image Base: 0x77e...
4:34:3...	calc.exe	1920	Load Image	C:\WINDOWS\system32\SHLWAPI.dll	SUCCESS	Image Base: 0x77f...
4:34:3...	calc.exe	1920	ReadFile	C:\WINDOWS\system32\calc.exe	SUCCESS	Offset: 46,080, Len...
4:34:3...	calc.exe	1920	ReadFile	C:\WINDOWS\system32\calc.exe	SUCCESS	Offset: 1,024, Leng...
4:34:3...	calc.exe	1920	FileSystemControl	C:\Documents and Settings\User1	SUCCESS	Control: FSCTL_IS...
4:34:3...	calc.exe	1920	QueryOpen	C:\WINDOWS\system32\shimeng.dll	SUCCESS	CreationTime: 2/28...
4:34:3...	calc.exe	1920	CreateFile	C:\WINDOWS\system32\shimeng.dll	SUCCESS	Desired Access: E...
4:34:3...	calc.exe	1920	CreateFileMapp...	C:\WINDOWS\system32\shimeng.dll	SUCCESS	SyncType: SyncTy...
4:34:3...	calc.exe	1920	CreateFileMapp...	C:\WINDOWS\system32\shimeng.dll	SUCCESS	SyncType: SyncTy...
4:34:3...	calc.exe	1920	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
4:34:3...	calc.exe	1920	RegOpenKey	HKLM\Software\Policies\Microsoft\Win	SUCCESS	Desired Access: Q...

