Malware Analysis Basics

1. Objective

The objective of this lab is to practice both static and dynamic analysis techniques on a benign Windows executable (calc.exe). The goal is to gain familiarity with analysis tools and reporting, not to detect malicious behavior.

2. Tools Used

- ***REMnux:*** Linux distribution for malware analysis.
- ***Hybrid Analysis (online sandbox)***: Dynamic analysis service.
- ***Utilities:*** strings, peframe.

3. Static Analysis

Step 1: Copy the binary (***calc.exe***) into REMnux VM.

Step 2: Run strings to extract readable text:

strings calc.exe > output.txt

```
.xdata
.idata$2
.idata$3
.idata$4
.idata$6
.data$brc
.data
.bss
.pdata
.rsrc$01
.rsrc$02
ShellExecuteW
SHELL32.dll
QueryPerformanceCounter
GetCurrentProcessId
GetCurrentThreadId
GetSystemTimeAsFileTime
GetTickCount
RtlCaptureContext
RtlLookupFunctionEntry
RtlVirtualUnwind
UnhandledExceptionFilter
SetUnhandledExceptionFilter
GetCurrentProcess
TerminateProcess
KERNEL32.dll
_XcptFilter
_amsg_exit
__wgetmainargs
__set_app_type
exit
_exit
_cexit
__setusermatherr
_initterm
__C_specific_handler
_wcmdln
_fmode
_commode
msvcrt.dll
?terminate@@YAXXZ
EventRegister
EventSetInformation
EventWriteTransfer
ADVAPI32.dll
Sleep
```

Step 3: Run peframe for PE header inspection:

peframe calc.exe

```
remnux@remnux:~$ peframe calc.exe
XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)


---------------------------------------------------------------------------
File Information (time: 0:00:01.185973)
---------------------------------------------------------------------------
filename          calc.exe
filetype          PE32+ executable (GUI) x86-64, for MS Windows
filesize          27648
hash sha256       58189cbd4e6dc0c7d8e66b6a6f75652fc9f4afc7ce0eba7d67d8c3feb0d5381f
virustotal        /
imagebase         0x140000000 *
entrypoint        0x1870
imphash           8eeaa9499666119d13b3f44ecd77a729
datetime          1971-09-24 16:02:24
dll               False
directories       import, debug, tls, resources, relocations
sections          .text, .rdata, .data, .pdata, .rsrc, .reloc
features          antidbg, packer


---------------------------------------------------------------------------
Yara Plugins
---------------------------------------------------------------------------
IsPE64
IsWindowsGUI
HasDebugData
HasRichSignature


---------------------------------------------------------------------------
Behavior
---------------------------------------------------------------------------
Xor
```

```
--------------------------------------------------------------------------------
Metadata
--------------------------------------------------------------------------------
CompanyName      Microsoft Corporation
FileDescription  Windows Calculator
FileVersion      10.0.19041.1 (WinBuild.160101.0800)
InternalName     CALC
LegalCopyright   © Microsoft Corporation. All rights reserved.
OriginalFilename CALC.EXE
ProductName      Microsoft® Windows® Operating System
ProductVersion   10.0.19041.1


--------------------------------------------------------------------------------
Import function
--------------------------------------------------------------------------------
SHELL32.dll      1
KERNEL32.dll     12
msvcrt.dll       14
ADVAPI32.dll     3
api-ms-win-core-synch-l1-2-0.dll 1
api-ms-win-core-processthreads-l1-1-0.dll 1
api-ms-win-core-libraryloader-l1-2-0.dll 1
```

Step 4: Observations

The file calc.exe was identified as a 64-bit Windows executable (27 KB). It imports common system DLLs (KERNEL32.dll, SHELL32.dll, msvcrt.dll, ADVAPI32.dll) and includes normal API calls such as ShellExecuteW, Sleep, and TerminateProcess. Metadata attributes confirm it is a signed Microsoft binary. A suspicious compilation timestamp (1971) was noted, but this is a known anomaly in Windows system files. No obfuscation, compression, or malicious indicators were observed.

4. Dynamic Analysis

Step 1: Upload calc.exe to https://www.hybrid-analysis.com.

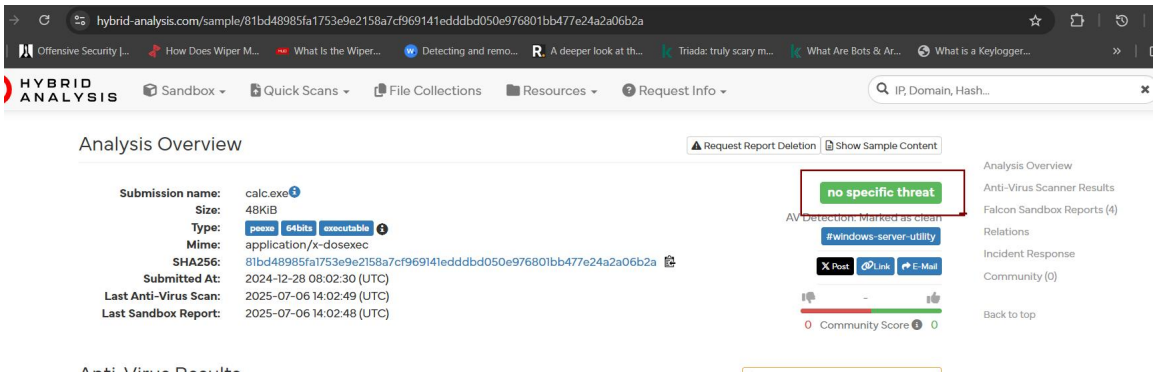
Step 2: Wait for the sandbox execution to complete.

Step 3: Review behavior summary:

Observed process creation: calc.exe spawns GUI window.

Registry activity: None suspicious.

Network activity: None (no outbound connections).



5. Comparison:

- Static analysis confirmed dependencies on Windows libraries (e.g., KERNEL32.dll).
- Dynamic analysis validated normal process behavior without anomalies.
- Both approaches confirmed the sample is benign.

6. Findings

Method	Observation	Notes
Strings	Found references to mscoree.dll, KERNEL32.dll, and "Microsoft Windows Calculator."	Confirms program is legitimate Windows binary.
PEframe	Imports standard Windows DLLs; no obfuscation or packing detected.	No indicators of malicious behavior.
Hybrid Analysis	Sandbox execution shows GUI launch only; no persistence, network, or file modifications.	Confirms benign behavior.

7. Conclusion

Through this exercise, the analyst practiced static and dynamic analysis techniques on a benign binary. The results confirmed that calc.exe is a legitimate Windows utility. This baseline exercise provided familiarity with analysis tools and reporting structures.