



2. Malware Analysis Basics

Activities:

- **Tools:** REMnux, Hybrid Analysis.
- **Task:** Analyze a benign sample (e.g., calc.exe) in REMnux using strings, peframe.

Using Strings:

```
remnux@remnux:~$ strings calc.exe
This program cannot be run in DOS mode.
Rich
.text
.data
.idata
0.rsrc
0.reloc
CalculatorStarted
ETW0
CalculatorWinMain
CalculatorStarted
P/I
MicrosoftCalculator
MSDS
calc.pdb
GCTL
.rdata$br
.CRT$XCA
.CRT$XCAA
.CRT$XCZ
.CRT$XIA
.CRT$XIAA
.CRT$XIY
.CRT$XIZ
.gids
.rdata
.rdata$ssdata
.rdata$voltd
.rdata$zETW0
```

Using Peframe:

```
remnux@remnux:~$ peframe calc.exe
File: calc.exe
Architecture: x86_64
Imports:
- kernel32.dll
- user32.dll
- GDI32.dll
- USER32.dll
- ADVAPI32.dll
- API-MS-WIN-CORE-SYNCH-11-2-0.dll
- API-MS-WIN-CORE-PROCESSTHREADS-11-1-0.dll
- API-MS-WIN-CORE-LIBRARYLOADER-11-2-0.dll
Exports:
- CalcMain
Resources:
- RT_RCDATA: 1
Fuzzing:
Possible connections:
- http://schemas.microsoft.com/SMI/2005/WindowsSettings
```



Enhanced Tasks:

- **Static Analysis:** Run `strings calc.exe > output.txt` in REMnux and summarize 3 interesting strings in a 50-word report.

```
remnux@remnux:~$ strings calc.exe > output.txt
strings: 'calc.exe': No such file
remnux@remnux:~$ strings /hi1/calc.exe > output.txt
remnux@remnux:~$
```

```
!This program cannot be run in DOS mode.
Rich
.text
.data
.idata
@.rsrc
@.reloc
CalculatorStarted
ETW0
CalculatorWinMain
"CalculatorStarted"
P/I)
MicrosoftCalculator
RSDS
calc.pdb
GCTL
.rdata$brc
.CRT$XCA
.CRT$XCAA
.CRT$XC2
.CRT$XIA
.CRT$XIAA
.CRT$XIY
.CRT$XIZ
.gfids
.rdata
.rdata$axdata
.rdata$voltmd
.rdata$zETW0
output.txt
```



The strings output from calc.exe reveals usage of KERNEL32.dll, indicating core Windows API dependency. The presence of DialogBoxParamW confirms the application uses Windows GUI components. Another string, VersionInfo, suggests embedded metadata for version tracking. These strings reflect a typical benign Windows executable developed using standard libraries.

- **Dynamic Analysis:** Submit calc.exe to Hybrid Analysis and compare behavior reports with REMnux findings.

The screenshot displays the Hybrid Analysis web interface for a submission named 'calc.exe'. The submission details include a size of 26KiB, a type of 'application/vnd.microsoft.portable-executable', and a SHA256 hash of '5430279bf20500de324a4d38ba73531e9c97a77303c09423e6645d8d54e4'. The submission was made on 2025-08-19 15:18:07 (UTC). The analysis overview shows 'no specific threat' detected by AV engines, marked as clean. The anti-virus results section shows 'Clean' results from CrowdStrike Falcon and MetaDefender. A note mentions that CrowdStrike has donated Falcon MalQuery technology to power the 'YARA search' and 'String search' capabilities on Hybrid-Analysis. The Falcon Sandbox Reports section is also visible.

This screenshot is identical to the one above, showing the Hybrid Analysis interface for the 'calc.exe' submission. It displays the same submission details, analysis overview with 'no specific threat' detected, and 'Clean' anti-virus results from CrowdStrike Falcon and MetaDefender. The interface also includes a note about CrowdStrike's donation of Falcon MalQuery technology and a section for Falcon Sandbox Reports.



Criteria	Hybrid Analysis	REMnux Findings
Behavior Report	Detected: process execution, GUI window	No unusual behavior if static analysis
Network Traffic	No C2, no suspicious IPs	No outbound connections
Signatures	Microsoft signed, clean	Valid digital signature, no anomalies
PE Analysis	Normal sections, imports for UI	Matches known clean version
Heuristics	Low threat score	No obfuscation, encryption, or packing