

IOT Inclass Exercise Week10_2 YARA

Lakshminath Reddy Alamuru

SUID: 367982169

Task-1

Extracted the strings from malware sample file given in the task.
I showed the strings which are at least 30 characters.

```
laxshminath@laxshminathvm2004: ~/IOT$ ls
Malware.yara1.exe.malz  Malware.yara.7z  'Week 10-2 in-class exercise -
YARA Rules Fall 2025.pdf'  yara-4.5.4  yara-4.5.4.tar.gz  yara_templat
e.yara
laxshminath@laxshminathvm2004: ~/IOT$ strings -n 30 ~/malware/my_sample |
sort | uniq
strings: '/home/laxshminath/malware/my_sample': No such file
laxshminath@laxshminathvm2004: ~/IOT$ strings -n 30 Malware.yara1.exe.malz
| sort | uniq
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789- _ABCDEFGHI
JKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/data
_acceptEx__qL9a0i8PW0vBR8SHPxunTBw
@add__3D9a0yz4rDqPZKBlqn0xlg@16
@add__8FwY5enLGB0dFer06Ny9caw@8
@addChunkToMatrix__YSJZJgeUSU2aa8GNvs3WA@8
@addHeapLink__LIRFHBfc9aX3C5dmMlnpWA@12
@addInt__mftMOxbyu0h4yByfs3sqjA@12
@addQuoted__45fPtFhY4FavRaYwDhRfuA@8
Address %p has no image-section
_add_W9aRfhn7HvnQTPAb8aJo1uwsystem
_addZCT__Y66tOYfjgwJ0k4aLz4bc0Q
_addZCT__Y66tOYfjgwJ0k4aLz4bc0Q.constprop.0
@align__vzThvqZajaR9ct9cQ7S0y1tQ@8
@alloc0__9aB7LvPFb7RSPI8u51kYo2Q@8
@alloc0Impl__aMIFDISudztFhhVWVqortg
@alloc__9aB7LvPFb7RSPI8u51kYo2Q_2@8
@allocAvlNode__Du8pyfSf0Lyn9ao52IcBsHg@12
@allocImpl__aMIFDISudztFhhVWVqortg_2
Argument domain error (DOMAIN)
(bad format; library may be wrong architecture)
@buildCommandLine__UDw4GM1E9cGPJc4ElZzKCgg@12
@buildEnv__YMjuewsJgp315PbogSaL0w@4
./build/i686-w64-mingw32-i686-w64-mingw32-crt
_callSoonProc__9b9b4iUSd60R02UqC52lfJ6A
_cb64safe__q0GCLBVULDDeEKBmNHUGw
@cellSetEnlarge__9bhPFIGFYIneoHljx80XvqA@4
@cellSetGet__ld9aj9akVqWcVwRCEMEk1MnQ@20
@cellSetPut__6bB10A4vUXoRvva9bRmnnwSQ@8
@cellSetRawInsert__a1sVKTgcDTTmcnBQqk9bNdA@24
@cellsetReset__Y9c9C0hDHR5oYkHFKHc9Fls0_2@4
```

The total number of strings are 572 with length greater than 30 in this case.

```
<?XML version="1.0" encoding="UTF-8" standalone="yes"?><assembly xmlns="urn:schemas-microsoft-com:asm.v1"
.0.0" processorArchitecture="*" name="winim" type="win32"/><dependency><dependentAssembly><assemblyIdentit
ls" version="6.0.0.0" processorArchitecture="*" publicKeyToken="6595b64144ccf1df" language="*" /></dependen
laxshminath@laxshminathvm2004: ~/IOT$ strings -n 30 Malware.yara1.exe.malz | sort | uniq | wc -l
572
laxshminath@laxshminathvm2004: ~/IOT$
```

Task-2

For the task-2, I have created a myrule1.yar file with two extracted string from the task-1

```
1 rule myrule1 {
2   meta:
3     description = "Detect malware strings from sample Malware.yara1.exe.malz"
4     author      = "Lakshminath Alamuru"
5     date        = "10-30-2025"
6     hash1       = "e128283461b14224459e966abf317c070d50aae7a531d64"
7
8   strings:
9     // Example unique strings extracted from your malware sample
10    $s1 = "_acceptEx__qL9a0i8PW0vbR8SHPxunTBw" ascii
11    $s2 = "@add__3D9a0yz4rDquPZKBlqn0xig@16" ascii
12    $mz = {4D 5A} // MZ magic number for PE files
13
14   condition:
15     // Check if at least 2 of the defined strings are present
16     (uint16(0) == 0x5A4D) and // MZ at offset 0 (little-endian)
17     (#s1 + #s2 >= 2) // at least 2 of the defined strings
18
19 }
```

Task-3

Test the yara rule against the malware file that has given in exercise

```
rule myrule1 {
  meta:
    description = "Detect malware strings from sample Malware.yara1.exe.malz"
    author      = "Lakshminath Alamuru"
    date        = "10-30-2025"
    hash1       = "e128283461b14224459e966abf317c070d50aae7a531d64"

  strings:
    // Example unique strings extracted from your malware sample
    $s1 = "_acceptEx__qL9a0i8PW0vbR8SHPxunTBw" ascii
    $s2 = "@add__3D9a0yz4rDquPZKBlqn0xig@16" ascii
    $mz = {4D 5A} // MZ magic number for PE files

  condition:
    $mz at 0 and (#s1 + #s2 >= 2) // at least 2 of the defined strings and $mz at 0
}
```

```
lakshminath@lakshminathvm2004:~/IOT$ yara myrule1.yar ~/IOT/Malware.yara1.exe.malz
error: rule "myrule1" in myrule1.yar(18): unreferenced string "$mz"
lakshminath@lakshminathvm2004:~/IOT$ yara myrule1.yar ~/IOT/Malware.yara1.exe.malz
myrule1 /home/lakshminath/IOT/Malware.yara1.exe.malz
lakshminath@lakshminathvm2004:~/IOT$
```

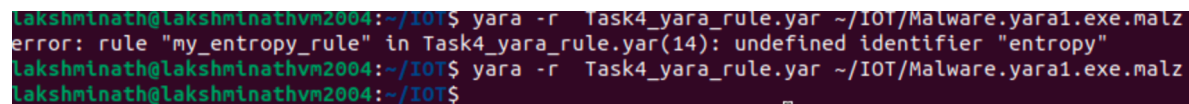
myrule1.yar file is has run against malware file successfully here. It seems no condition strings are found here.

Task-4



```
1 rule my_entropy_rule {
2   meta:
3     description = "Detect malware sample based on string, header, size"
4     author      = "Lakshminath Alanuru"
5     date        = "10-30-2025"
6
7   strings:
8     $md = "ExampleStringFromMalware" ascii
9
10  condition:
11    $md and
12    uint16(0) == 0x457f and // string must exist
13    filesize <= 20000 * 1024 // first 2 bytes in little-endian = 0x457f
14  }
15 }
```

Run the Task4_yara_rule.yar file again malware file didn't get any output. Seems the conditions are not met.



```
lakshminath@lakshminathvm2004:~/IOT$ yara -r Task4_yara_rule.yar ~/IOT/Malware.yara1.exe.malz
error: rule "my_entropy_rule" in Task4_yara_rule.yar(14): undefined identifier "entropy"
lakshminath@lakshminathvm2004:~/IOT$ yara -r Task4_yara_rule.yar ~/IOT/Malware.yara1.exe.malz
lakshminath@lakshminathvm2004:~/IOT$
```

Observations:

I got to know how to write war file and can check for the conditions met for string matching and file size checking as well. At least in the conditions that I have taken, those are not met. But it is successful learning for me about yara rules in detail.