M T W T F S S

Date:

Yara Rules

Yara Tutorial Chap# 2

Tools

CFF Explorer

40 => m
5A => Z

Strings

Run in powershell
Commands => strings -n filename

Basic Yara Rule → rule Name

```
rule Suspicious {
    strings:
        $mz = { 4D5A }
        $s_str1 = "VS_VERSION_INFO"
        $s_str1 = "
    Condition:
        ($str_1 or $str_2 or $mz)
}
```

Powershell > yara32 -r rule1.yara .\file

* PE header starts from 000080
=> Important things in Optional Headers:-
- Image Base

Relative ~~Vadd~~ Virtual Address (RVA)

M T W T F S S

Date: 08/03/2022

Lecture 7/8

YARA

file name should be => name.yara

SYNTAX

rule Name

rule rule_identifier {

Strings:

$stringName = "value"

$stringName = {Hexadecimal values}

Condition:

(strings operators strings operators string ...)

}

To run:-

Yara32 -r name.yara ./file

Types of Strings in YARA :-

- Hexadecimal strings
- Text Strings
- Regular Expressions

Tool

awk Script

OR

awk Script

can YaraExtract ASCII and Unicode

e.g. MZ

(4)DSA

M T W T F S S

Date:

① Hexa decimal Strings

⇒ Syntax $stringName = { 4D5A }

Hexa decimal have three constraints

⇒ Wild Cards ? example ⇒ $string = { 4D5? }

⇒ Jump [a - b] (0<=a<=b) Example = $string = {F423[4-6]62}

⇒ alternatives : In this we need to write strings in regular expression $string = {F423(62B4|56)45}

In this example if rule math the the string would be F42362B445 OR F42356445

Note:- we can add multiple alternatives in one string

wildcards can also be use in alternative strings

$str = {F462(23|B4??)}

② Text Strings

⇒ it is case sensitive

⇒ Syntax $stringname = " testString "

⇒ modifiers :-

⇒ no case

Syntax $stringName = " Hello " nocase

This modifier string ki value ko lower case or uper case kar kay check kry ga without changing the places

Example :- Hello, hello, hEllo, HEllo, etc

⇒ wide

add extra bit bit

make it 16 bit "\x00h\x00e\x00l\x00l\x00o"

⇒ Base 64

M T W T F S S

Date:

=) Full word

Only compare the alphabet strings and did not scanning alphanumeric strings.

=) Private

make String private which will not effect the rule output. (we can say that private modifier is same as comments)

Strings Comand

strings -a -n 5 ./filename > testFileName.txt

BASIC YARARULE

```
rule malicious {

    strings:
        $ mz = { 4? 5A }          (wild card)
        $ string1 = "MACNINE" Inocase (modifier)
        $ string2 = { F4 23 [4-6] 62 }

    Condition:
        ( $ mz and $ string1 )
        $ mz and $ string1 , $ string2   (OR)

}
```

wild card =>?
jump [4-6]

We Can write multiple rules in one file

Comments in YARA

Syntax

/* comment */

wild card string ... different values ... kar checking ...

M T W T F S S

Date: 10/03/2022

Lecture - 9

Counting String Example

```
rule Counting
{
    strings:
        $s1 = "yoe"
        $s = "Lzzzzzzzzzzz"
    condition:
        #s==2 or #s1<5
}
```

Memoryat Example

if we have the exact location then use memoryat

```
rule Memoryat {
strings:
    $s1 = "p"
    $s2 = {45}

condition:-
    $s1 at 128 and $s2 at 129
}
```

offset location

128 = 0x80

Research it!

Q# Can we call file in the rules means if we have hundred of strings it is difficult to intilize them one by one.

If you define the string you have to use it otherwise it will through error

In counting if we want to count the occurances of string we need to use # instead of $ in the condition

M T W T F S S

Date:

Memoryin Example

```
rule    Memoryin
{
    Strings:
        $s1 = "P"
        $s2 = "B"
    Condition:-
        $s1 in (0..129) and $s2 in (129..filesize)
}
```

if we don't know the exact location then we give range of the location to check in use memoryin

Memorysize Example

```
rule Memorysize
{
    Strings:
        $s1 = "P"
        $s2 = "B"
    Condition:
        $s1 in (0..128) and $s2 in
        (128..filesize) and filesize>100KB
}
```

allofthem Example

```
rule    allofthem
{
    Strings:
        $s1 = "Yoe"
        $s2 = "AAA"
        $s3 = "BBB"

    Condition:
        all of them
}
```

M T W T F S S

Date:

Anonymous Strings in YARA :-

```
rule anonymousString
{
    Strings:
        $ = "dummydata 1"
        $ = "dummy data 2"

    Condition:
        1 of them
}
```

Iterating over string occurences :-

```
rule Occurances {
    Strings:
        $a = "dummy 1"
        $b = "dummy 2"
    Condition:
        for all i in (1,2,3): (@[i] + !a == @b[i])
}
```

(@ = address, !a = offset)

1,2,3 means string kay pehly 3 characters/bytes (tab) 1=d, 2=m, 3=m

characters mai 10 of sets ka difference hay

Calling rule in another rule :-

```
rule Rule 1
{
    Strings :
        $a = "dummy 1"
    Condition :
        $a
}

rule rule 2
{   Strings :
        $a = "dummy 2"
    Condition:
        $a and Rule 1
}
```

Global Rule :-

```
global rule SizeLimit
    {


        Condition :
            filesize < 2 MB

    }
```

We can define multiple global rule in one file.

M T W T F S S

Date:

Private Rule :-

This rule don't run

Syntax:

```
private rule privateRule {

    ......

}
```

MetaData :-

Syntax:

```
rule Metadata Example
    {
        meta :
                my_identifier 1 = " This rule is for ..... "
                    :
        Strings:
                $ s 1 = " dummy 1 "
                $ s2  = " dummy 2 "
        Condition :

    }               $ s1  or  $ s2
```

Note:-

Meta doesn't have any effect on output and they are not strings. In meta we can store information of rule in it.

M T W T F S S

Date:

Modules :-

```
import "pe"

rule Test
{
    strings:
        $a = "dummy1"

    Condition:
        $a and pe.entry_point == 0x1000
}
```

Include different rule file in rule :-

File 1

```
rule file1
    {
        strings:
            $a = "dummy1"

        Condition:
            $a
    }
```

File 2

```
include "file1"
rule file2
    { strings:
        $b = "dummy"
    Condition:
        $b
    }
```

→ Agar file same folder mai nai hay tu full path likhna hay

Exe	MZ => 4D5A
PE Exe	MZ..... PE => 4D5A 5045
PDF	%PDF =>
DOCX	PK =>
Excel ~~xls~~ xlsx	PK => 504B
ZIP	PK.. => 504B0304
7ZIP	
RAR	"Rar! ...." =>
JPEG	.....JFIF ffd8ffe0
PNG	.PNG => 8950 4e47
.bmp	BM => 424d
.gif	GIF8 => 4749 4638
.eps	%! => 2521
.flv	FLV => 464c56
.asf .wma .wmv	
.avi	
.wm	