Panduan Update Rules Pada Thor Scanner

Pendahuluan

Thor Scanner merupakan alat pendeteksian *portable* untuk mendeteksi aktivitas mencurigakan pada sistem yang disusupi. Thor Scanner dapat mendeteki secara mendalam sampai *local event log*, *registry*, dan *file system*. Thor Scanner dapat menjadi sistem pendeteksi bagi aktivitas berbahaya yang terlewat oleh antivirus umum. Hasil dari pendeteksian menggunakan Thor Scanner dapat diekspor dalam bentuk HTML, TXT, JSON, CSV.

Langkah – Langkah

Thor Scanner memiliki fitur yang mengijinkan pengguna untuk melakukan *custom rules*. Thor Scanner memberikan template simple IoC *custom rules* yang berada pada direktori `thor10.6lite-win-pack\custom-signatures`. Selain berdasarkan template custom rules yang sudah ada, Thor Scanner juga mendukung penggunaan Yara Rules untuk pendeteksian malware atau virus. Berikut merupakan langkah custom rule pada Thor Scanner.

A. Custom Rules menggunakan Simple IoC Thor Scanner

Pada Sistem Operasi Windows, di dalam direktori *custom-signatures* terdapa 3 (tiga) direktori lagi yaitu direktori iocs, misc, dan yara.

Gambar 1. DIrektori Custom Rules

Sehingga setiap kali Thor Scanner dijalankan maka akan melakukan pengecekan pada direktori *custom-signatures*. Pada direktori tersebut terdapat beberapa format custom rules Simple IoC seperti :

a. Simple IoC Nilai Hash.

Simple IoC dengan nilai Hash dapat digunakan dengan MD5, SHA1, atau SHA256 dan dapat ditambahkan komen pada belakang nilai hash dengan dipisahkan karakter *semicolon* (;).

```
# FORMAT ------------------------------------------------------------
-----------
#
# MD5;COMMENT
# SHA1;COMMENT
# SHA256;COMMENT
#
# EXAMPLES ----------------------------------------------------------
-----------
#
0c2674c3a97c53082187d930efb645c2;DEEP PANDA Sakula Malware -
http://goo.gl/R3e6eG
000c907d39924de62b5891f8d0e03116;The Darkhotel APT
http://goo.gl/DuS7WS
c03318cb12b827c03d556c8747b1e323225df97bdc4258c2756b0d6a4fd52b47;Oper
ation SMN Hashes http://goo.gl/bfmF8B - Zxshell
```

b. Simple IoC Filename

Thor Scanner mengijinkan IoC berdasarkan nama file dan lokasi fila (*path*) dengan menggunakan regex serta dapat menambahkan nilai atas nama file yang di deteksi. Berikut merupakan format Simple IoC Filename.

```
# FORMAT ------------------------------------------------------------
-----------
# # COMMENT
# REGEX;SCORE to add;False Positive Regex
#
# EXAMPLES ----------------------------------------------------------
-----------
#
# # Various examples from APT case X
 \\svcsstat\.exe;75

\\(server|servisces|smrr|srrm|svchost|svhost|svshost|taskmgr)\.exe$;2
5
 ProgramData\\Mail\\MailAg\\;40
 (Anwendungsdaten|Application Data|APPDATA)\\sydmain\.dll;55
 (TEMP|Temp)\\[^\\]+\.(xmd|yls)$;45
 (LOCAL SETTINGS\\Temp|Local
Settings\\Temp|Local\\Temp)\\(word\.exe|winword\.exe);50
```

c. Simple IoC Keyword

Simple IoC keyword berupa string yang diindikasi merupakan string pada file berbahaya. Penggunaan keyword menerapkan *case sensitive* sehingga harus berhati-hati dalam menentukan strings. Berikut merupakan format Simple IoC Keyword.

```
# FORMAT ------------------------------------------------------------
-----------
#
# # COMMENT
# STRING
#
# EXAMPLES ----------------------------------------------------------
-----------
#
# # Evil strings from our case
sekurlsa::logonpasswords
failed to create Service 'GAMEOVER'
kiwi.eo.oe
```

d. Simple IoC Command and Control (C2)

Simple IoC C2 digunakan untuk menentukan domain, alamat IP yang menjadi server dari malware. Setiap IoC harus dalam satu bari. Berikut merupakan format Simple IoC C2.

```
# FORMAT ------------------------------------------------------------
-----------
#
# # Comment
# IP
# FQDN
#
# EXAMPLES ----------------------------------------------------------
-----------
#
## Case 44 C2 Server
mastermind.eu
googleaccountservices.com
89.22.123.12
```

Seluruh format *custom rules* disimpan dalam ekstensi .txt.template, untuk dapat menggunakan format tersebut harus dilakukan perubahan ekstensi menjadi txt. Berikut merupakan contoh *custom rules* simple IoC Nilai Hash.

a) Sistem Operasi Windows

1. Menggunakan CMD/PowerShell dengan hak akses Administrator (Klik kanan "Run as administrator"). Selanjutnya menuju direktori `thor10.6lite-win-pack/custom-signatures/iocs/templates`

```
C:\Windows\system32>
cd \Users\awan\Documents\ThorLite\thor10.6lite-win-
pack\custom-signatures\iocs\templates
```

2. Salin format dan ganti ekstensi menjadi .txt. Kemudian buka file .txt dengan Notepad dan sesuaikan file dengan nilai hash *custom rules.*

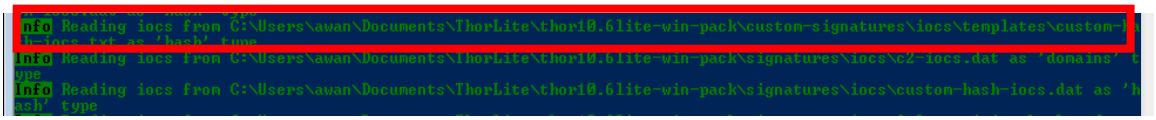
```
C:\..\custom-signatures\iocs\templates> copy .\custom-
hash-iocs.txt.template .\custom-hash-iocs.txt
```

Berikut isi file *custom rules* `custom-hash-iocs.txt`

```
#Format
#nilai hash; komentar

0c2674c3a97c53082187d930efb645c2;DEEP PANDA Sakula Malware
000c907d39924de62b5891f8d0e03116;The Darkhotel APT
```

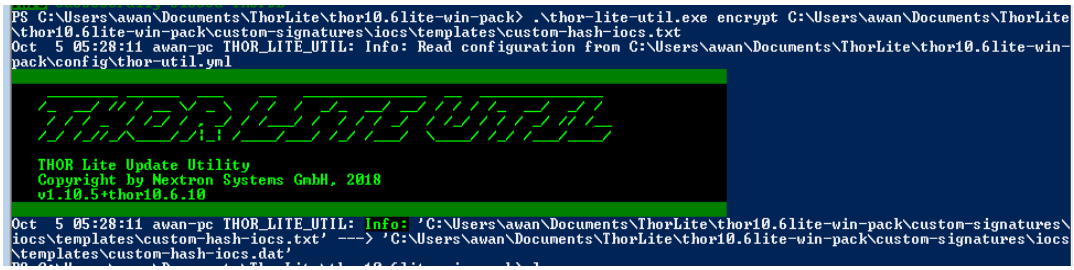
3. Setelah file dibuat, kemudian disimpan dalam ekstensi .txt. Ketika Thor Scanner dijalankan maka secara otomatis *rules* akan ditambahkan.



Gambar 2. Update Rules Nilai Hash

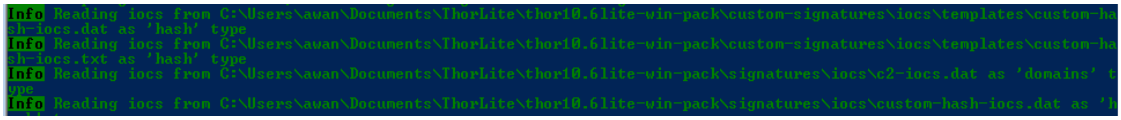
4. Thor Scanner memiliki fitur untuk enkripsi rules untuk tujuan supaya IoC atau rules tidak mudah dibaca atau diketahui oleh penyerang. Untuk melakukan enkripsi digunakan aplikasi `thor-lite-util.exe` yang sudah ada pada package Thor Scanner. Ketika sudah dilakukan enkripsi maka ekstensi file berubah menjadi .dat. Berikut perintah untuk melakukan enkripsi :

```
.\thor-lite-util.exe encrypt [lokasi file custom-hash-
iocs.txt]
```



Gambar 3. Enkripsi Rules Custom

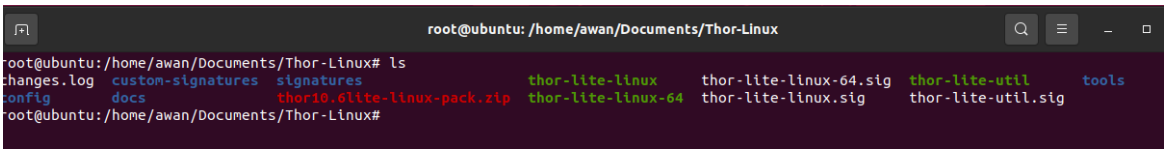
Berdasarkan Gambar 3, diketahui bahwa file telah menjadi custom-hash-iocs.dat. Ketika Thor Scanner dijalankan maka rules akan ditambahkan seperti Gambar 4.



Gambar 4. Rules Enkripsi Berhasil Ditambahkan

b. Sistem Operasi Linux

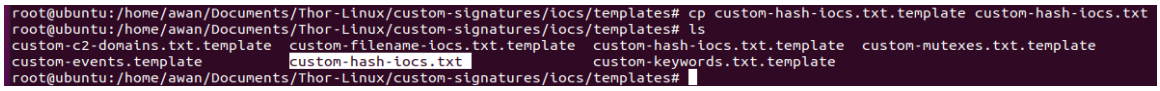
1. Buka terminal pada Linux kemudian masuk sebagai root dan menuju direktori tempat file Thor Scanner disimpan.



Gambar 5. Direktori Thor Scanner

2. Untuk melakukan *update* pada Linux dapat dilakukan seperti pada Sistem Operasi Windows yaitu dengan menyalin *file template* terdapat pada direktori `custom-signatures/iocs/templates/` dan melakukan pengeditan isi file sesuai strings serta mengubah ekstensi file dari .txt.template menjadi .txt dengan perintah sebagai berikut :

```
root@ubuntu#cp custom-hash-iocs.txt.template custom-hash-iocs.txt
```



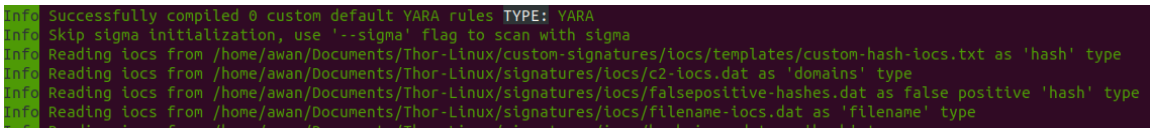
Gambar 6. Merubah ekstensi file

Berikut isi file *custom rules* `custom-hash-iocs.txt`

```
#Format
#nilai hash; komentar

0c2674c3a97c53082187d930efb645c2;DEEP PANDA Sakula Malware
000c907d39924de62b5891f8d0e03116;The Darkhotel APT
```

Ketika Thor Scanner dijalankan `sudo./thor-lite-linux-64` maka *custom rules* akan ditambahkan seperti pada gambar berikut.

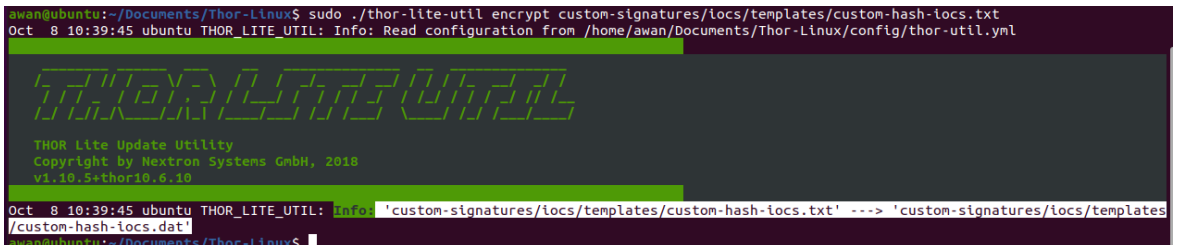


Gambar 7. Custom Rules Berhasil Ditambahkan

3. Custom rules pada Linux dapat dilakukan enkripsi seperti pada Windows. Berikut perintah untuk melakukan enkrpsi custom rules pada Linux.

```
sudo ./thor-lite-util encrypt custom-
signatures/iocs/templates/custom-hash-iocs.txt
```

Ketika proses enkripsi berhasil dilakukan maka akan menghasilkan dokumen dengan ekstensi .dat seperti pada gambar berikut.



Gambar 8. Enkripsi Rules

B. Custom Rules Menggunakan YARA Rules

Thor Scanner mendukung *rules* berdasarkan format YARA. Rules Yara memiliki ekstensi .yar atau .yara. Custom rules Yara pada Thor Scanner disimpan pada direktori `/custom-signatures/yara/`.

1. Format YARA rules

```
rule CheckFileSize
{
        strings:
                $abc = "abc"
        condition:
                ($abc or not $abc) and filesize < 200KB
}
```

Baris pertama merupakan pengidentifikasi *rules*, pengidentifikasi *rules* dapat berisi karakter alfanumerik dan karakter garis bawah, namun karakter pertama tidak boleh angka. Format Yara rules terdiri dari 2 bagian yaitu *strings* dan *condition*. *Strings* merupakan bagian yang akan digunakan untuk mengidentifikasi file berdasarkan kesamaan text atau heksadesimal. Setiap *strings* akan diawali dengan karakter $. Sedangkan bagian *conditions* merupakan ekspresi logika.

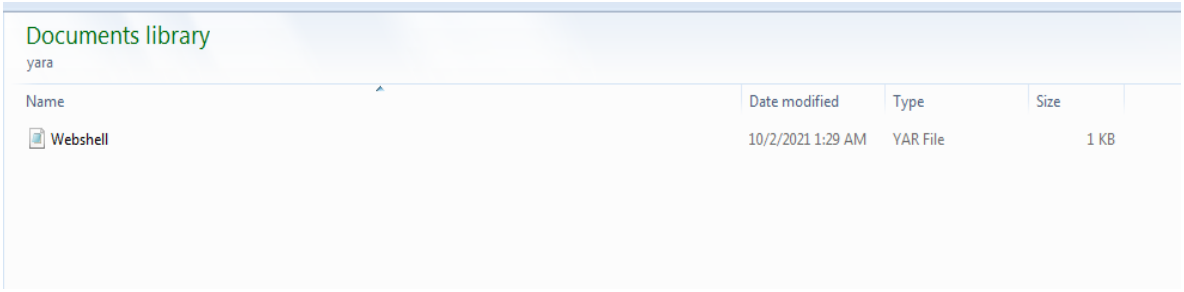
2. Menentukan file yang akan dibuat *custom rules*

Setelah memahami format penulisan pada Yara rules, selanjutnya menentukan file yang akan dilakukan pendeteksian dengan file yang dibuat. Dalam panduan ini diambil contoh file Web Shell IndoXpolit dengan ekstensi php. Pada webshell tersebut diketahui bahwa terdapat beberapa *strings* yang unik seperti “IndoXploit”, “idx_config”, “etc/passwd”, “Hacked by IndoXploit”. Dari keempat strings yang unik tersebut kemudian dibuat Yara rules sebagai berikut :

```
rule Shell_IndoXploit
{
        strings:
                $strings1 = “IndoXploit"
                $strings2 = “idx_config”
                $strings3 = “etc/passwd”
                $strings4 = “Hacked by IndoXploit” nocase
        condition:
                3 of ($strings*)
}
```

Pada $strings4 terdapat teks nocase bermaksud bahwa strings ke empat tidak *case sensitive*. Kemudian pada *condition* digunakan ekspresi 3 of ($strings*), ekspresi tersebut bermaksud bahwa jika terdapat 3 strings yang sama antara strings 1 - 4 pada suatu file,

maka akan terdeteksi sebagai Shell_IndoXploit. Setelah rules dibuat kemudian disimpan dalam ekstensi .yar atau .yara dan disimpan pada direktori `custom-signatures/yara`.

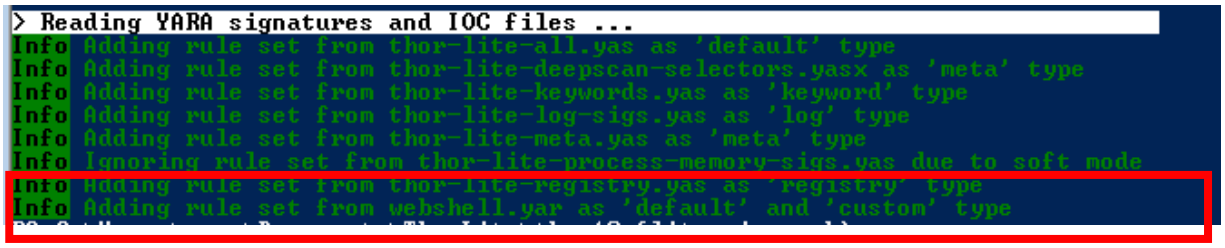


Gambar 9. Menyimpan Custom Rules Pada Direktori custom-signatures

3. Setelah *custom rules* dibuat maka selanjutnya mencoba menjalankan Thor Scanner melalui CMD atau PowerShell dengan perintah

```
.\thor-lite.exe
```

Ketika *custom rules* benar maka akan menampilkan hasil pendeteksian seperti Gambar berikut



Gambar 10. Custom Rules Berhasil Ditambahkan

4. Pada Yara versi sebelum 4.1.0 menerima teks strings untuk digunakan pendeteksian seperti pada contoh *custom rules* yang dibuat diatas. Namun pada Yara versi setelah 4.1.0 hanya menerima strings dalam bentuk ASCII. Terdapat beberapa kata kunci strings yang dapat digunakan pada Yara versi 4.1.0 yaitu : nocase, wide, ascii, xor, base64, fullword.
   a. strings nocase

      Secara default teks strings Yara bersifat *case-sensitive*, dengan menambahkan kata kunci “nocase” setelah strings, bertujuan untuk menonaktifkan *case-sensitive*.

```
rule Shell_IndoXploit
{
        strings:
                $strings4 = "Hacked by IndoXploit" nocase
        condition:
                $strings4
}
```

Contoh rules diatas akan mendeteksi secara tidak *case-sensitive.*

b. Strings wide

Strings wide digunakan untuk mendeteksi teks strings yang diencode dengan 2 byte per karakter. Contohnya ketika terdapat script encode "H\x00a\x00c\x00k\x00e\x00d" pada rules Yara dapat ditulis sebagai berikut :

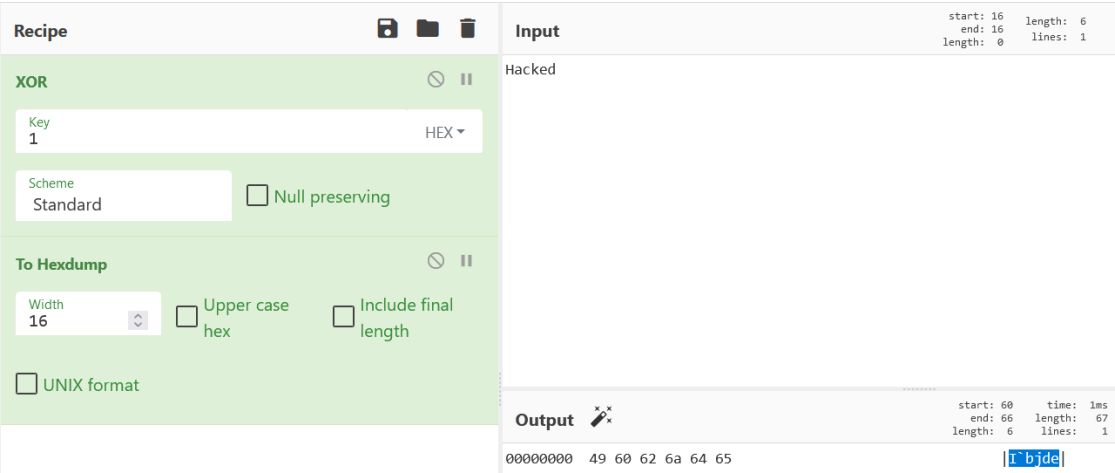
```
rule Shell_IndoXploit
{
        strings:
                $strings4 = "Hacked" wide
        condition:
                $strings4
}
```

c. Strings XOR

Strings xor digunakan untuk mendeteksi strings yang di encode menggunakan operasi xor. Contohnya ketika akan mendeteksi kemungkinan adanya strings Hacked yang di encode xor dengan suatu kunci. Rules pada Yara dapat ditulis sebagai berikut :

```
rule Shell_IndoXploit
{
        strings:
                $strings4 = "Hacked" xor
        condition:
                $strings4
}
```

Rules diatas akan mendeteksi jika ada strings Hacked yang di xor dengan 1 byte kunci dari 0 – F (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, A, B, C, D, E, F) seperti "I`bjde" dan lainnya.



Gambar 11. Encode Xor String

d. Strings base64

Strings base64 dapat digunakan untuk mendeteksi strings yang di *encode* menggunakan base64. Contohnya jika terdapat *encode* base64 pada *strings* Hacked, maka rules Yara sebagai berikut

```
rule Shell_IndoXploit
{
        strings:
                $strings4 = "Hacked" base64
        condition:
                $strings4
}
```

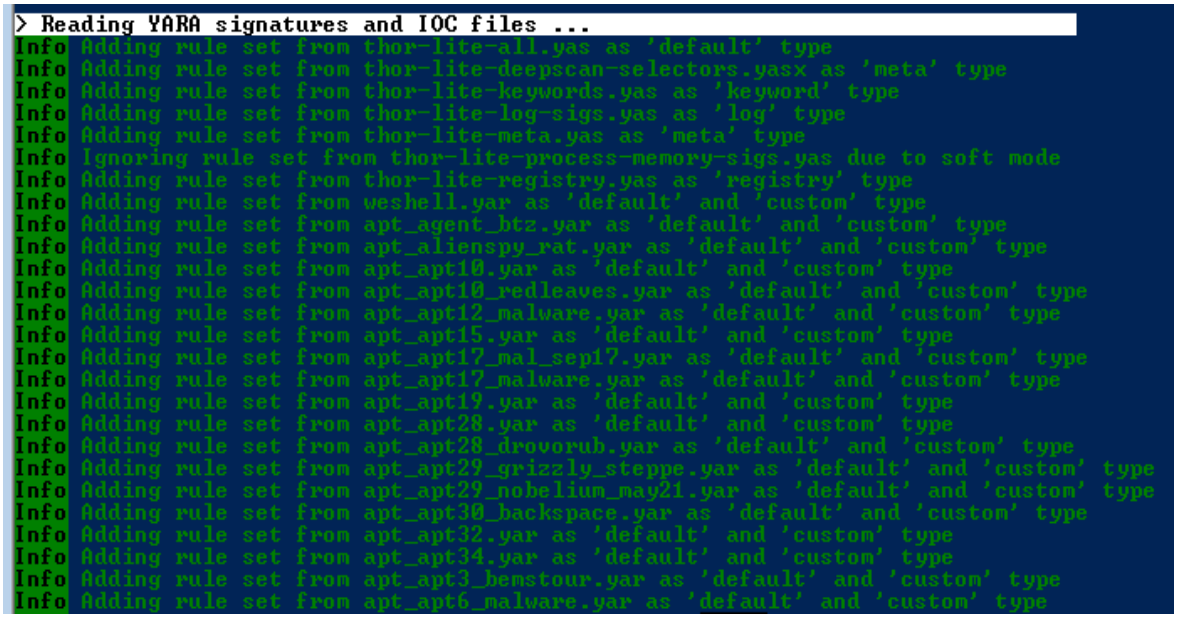
e. Strings fullword

Strings fullword digunakan untuk mendeteksi strings yang dibatasi oleh karakter non alfanumerik (selain A-Z, dan 0-9). Contoh jika terdapat strings "Hacked" maka pada rules dapat dibuat sebagai berikut :

```
rule Shell_IndoXploit
{
        strings:
                $strings4 = "Hacked" fullword
        condition:
                $strings4
}
```

Maka *rules* tersebut akan mendeteksi strings www.Hacked.com, www.my-Hacked.com, dan tidak mendeteksi www.myHacked.com.

5. *Custom rules* Yara pada Thor Scanner pada Linux dan Windows dapat disimpan pada direktori `/custom-signatures/yara/`
6. *Custom rules* YARA dapat diunduh pada link berikut : https://github.com/candk-cyber/Custom-Rules-ClamAV



Gambar 12. Yara Rules Berhasil Ditambahkan Pada Windows

Gambar 12 menunjukkan jika terdapat beberapa *rules* Yara yang ditambahkan dengan keterangan *custom type*.

Jakarta, 20 Oktober 2021

Mengetahui

Ditandatangani Secara Elektronik oleh :
PENGOLAH DATA KEAMANAN SIBER DAN SANDI

Renaltha Puja Bagaskara, S.Tr.TP.
Penata Muda (III/a)

Penyusun

PENGOLAH DATA KEAMANAN SIBER DAN SANDI

Candra Kurniawan, S.Tr.Kom

Disetujui Oleh

Ditandatangani secara elektronik oleh:
SANDIMAN AHLI MUDA

NOVIAN NUR CAHYA, S.ST, M.Kom.
Penata (III/c)