Panduan Scanning Malware Menggunakan 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 system pendeteksi bagi aktivitas berbahaya yang terlewat oleh antivirus umum. Hasil dari pendeteksian menggunakan Thor Scanner dapat dieksport dalam bentuk HTML,TXT, JSON, CSV.

Requirement

Thor Scanner dapat berjalan pada sistem operasi Windows, Linux, macOS tanpa persyaratan khusus. Thor Scanner dapat memberikan hasil yang maksimal jika dijalankan dengan hak akses administrator/root. Berikut daftar sistem operasi yang dapat menggunakan Thor Scanner :

1. Windows 7 x86 /x64
2. Windows Server 2008 R2 x64
3. Windows 8.1, 10
4. Windows Server 2016, 2019, 2022
5. RHEL/CentOS 6, 7, 8
6. SuSE SLES 11, 12, 15
7. Ubuntu 16 LTS, 18 LTS, 20 LTS
8. Debian 9, 10, 11
9. macOS 10.15, 10.15, 11

Langkah – Langkah

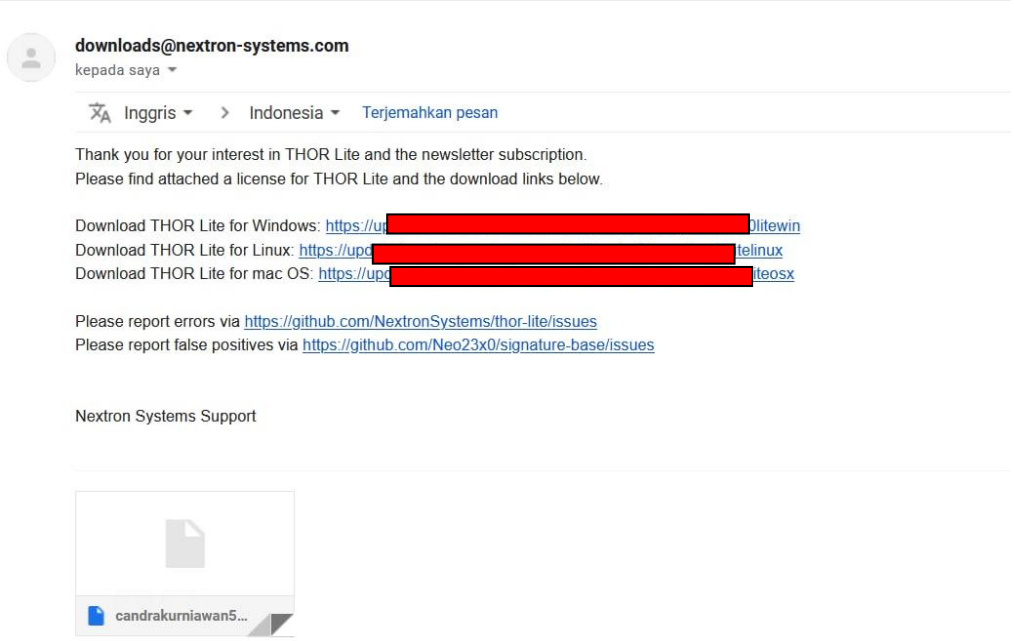
A. Menggunakan Windows

1. Tahap Instalasi Thor Scanner

   Unduh Thor Scanner pada laman berikut

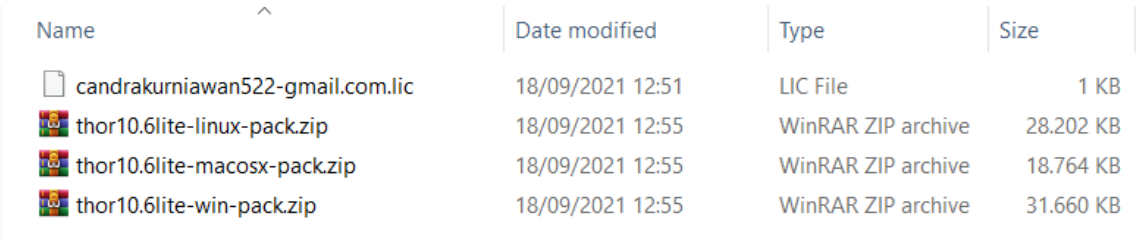
```
https://www.nextron-systems.com/thor-lite/download/
```

Laman diatas berisi perintah untuk melakukan subscribe dengan menggunakan akun email.



Gambar 1 Laman Unduh Thor Scanner

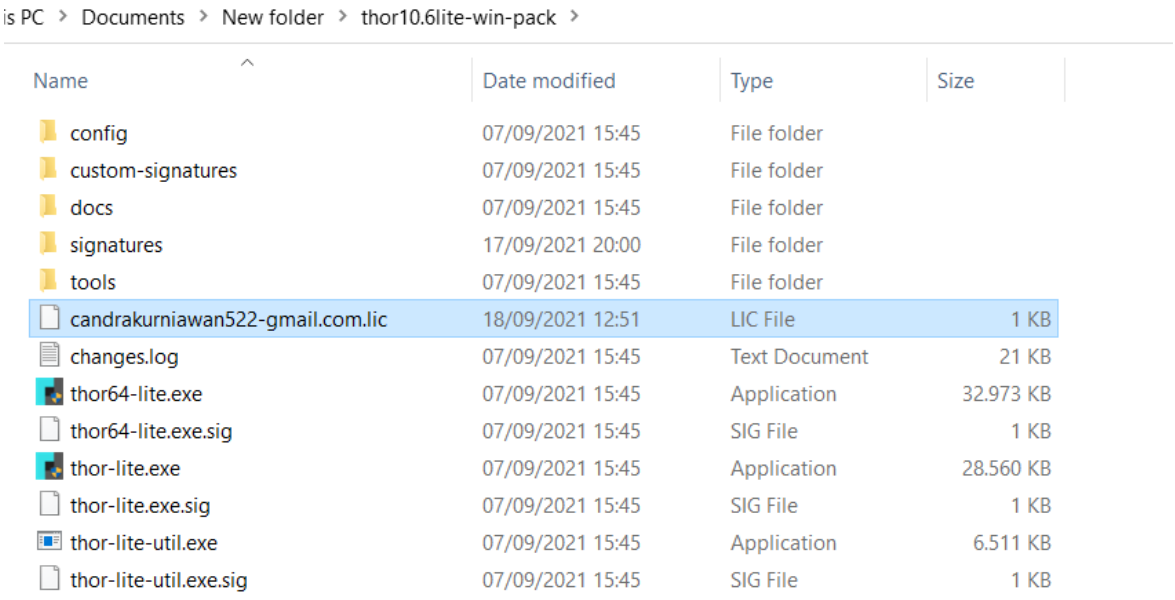
Setelah melakukan subscribe, laman untuk mengunduh akan dikirimkan melalui pesan email yang terdiri dari Thor Scanner untuk Windows, Linux, dan macOS, serta file lisensi.lic, kemudian unduh semua filenya.



Name	Date modified	Type	Size
candrakurniawan522-gmail.com.lic	18/09/2021 12:51	LIC File	1 KB
thor10.6lite-linux-pack.zip	18/09/2021 12:55	WinRAR ZIP archive	28.202 KB
thor10.6lite-macosx-pack.zip	18/09/2021 12:55	WinRAR ZIP archive	18.764 KB
thor10.6lite-win-pack.zip	18/09/2021 12:55	WinRAR ZIP archive	31.660 KB

Gambar 2. File Thor Scanner

Setelah keempat file terunduh seperti pada Gambar 2, lakukan ekstraksi masing-masing file zip dan salin lisensi.lic pada masing-masing folder dari ketiga file zip.



is PC › Documents › New folder › thor10.6lite-win-pack ›

Name	Date modified	Type	Size
config	07/09/2021 15:45	File folder	
custom-signatures	07/09/2021 15:45	File folder	
docs	07/09/2021 15:45	File folder	
signatures	17/09/2021 20:00	File folder	
tools	07/09/2021 15:45	File folder	
candrakurniawan522-gmail.com.lic	18/09/2021 12:51	LIC File	1 KB
changes.log	07/09/2021 15:45	Text Document	21 KB
thor64-lite.exe	07/09/2021 15:45	Application	32.973 KB
thor64-lite.exe.sig	07/09/2021 15:45	SIG File	1 KB
thor-lite.exe	07/09/2021 15:45	Application	28.560 KB
thor-lite.exe.sig	07/09/2021 15:45	SIG File	1 KB
thor-lite-util.exe	07/09/2021 15:45	Application	6.511 KB
thor-lite-util.exe.sig	07/09/2021 15:45	SIG File	1 KB

Gambar 3. Ekstrak File Zip dan Salin Lisensi

Ketika Thor Scanner dijalankan, pertama akan mencari lisensi yang valid terlebih dahulu, sehingga lisensi harus disalin pada masing-masing folder. Pada Gambar 3 menunjukkan hasil ekstraksi file thor10.6lite-win-pack.zip yang sudah ditambah file lisensi. Hasil ekstraksi file thor10.6lite-win-pack.zip berisi beberapa paket sebagai berikut:

a. Thor Binaries – thor-lite.exe untuk system 32-bit dan thor64-lite.exe untuk system 64-bit,
b. Thor Utility (thor-util.exe) digunakan untuk update aplikasi, enkripsi, generate report,

signature verification,

c. Konfigurasi file terdapat pada folder `config`,

d. Database signature Thor Scanner terdapat pada folder `signatures`,

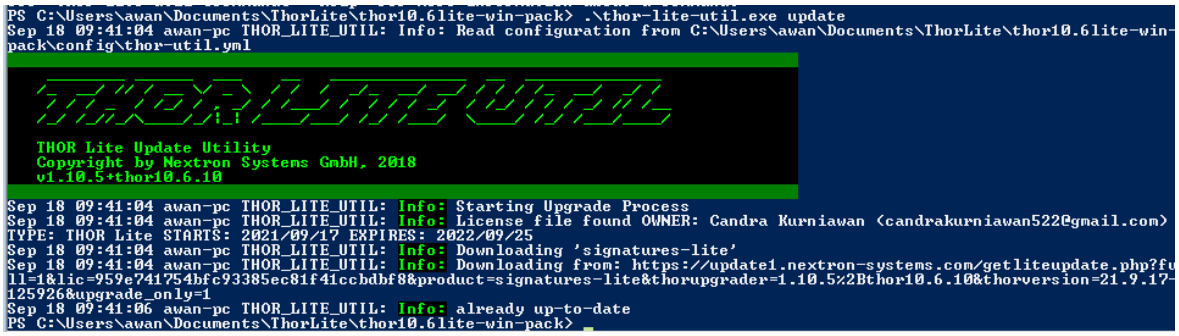
e. Custom signature dan hasil Threat Intel IoC terdapat pada folder `custom-signature`,

f. Terdapat tambahan file untuk packer EXE yang terdapat pada folder `tools`.

2. Penggunaan Thor Scanner pada Windows

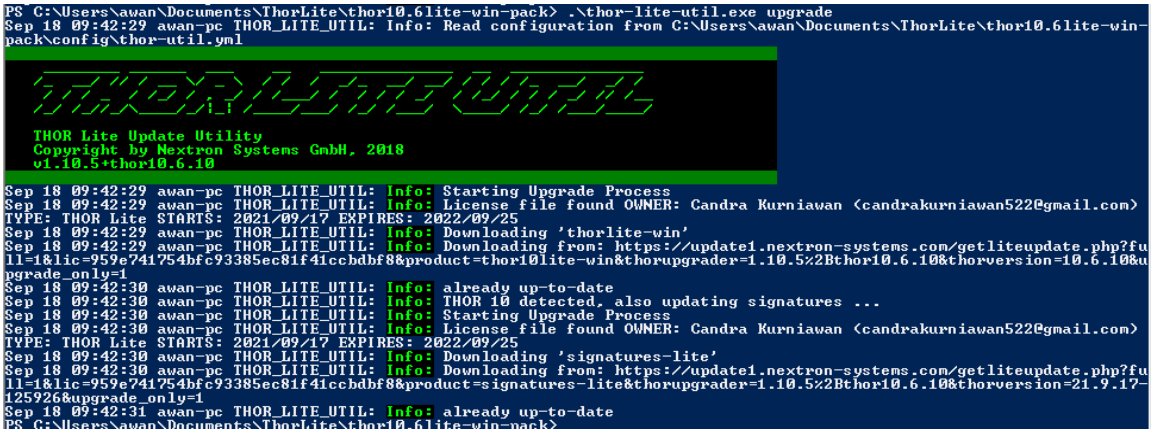
Sebelum menggunakan Thor Scanner lakukan *update* dan *upgrade signature* terlebih dengan masuk pada direktori Thor Scanner dan melakukan update dan upgrade dengan perintah seperti dibawah ini. Untuk menjalankan gunakan PowerShell atau CMD dengan hak akses administrator (klik kanan "Run as administrator"). Ketika melakukan *update* dan *upgrade* harus terhubung ke jaringan internet.

```
.\thor-lite-util.exe update
.\thor-lite-util.exe upgrade
```



Gambar 4.Update Signature File

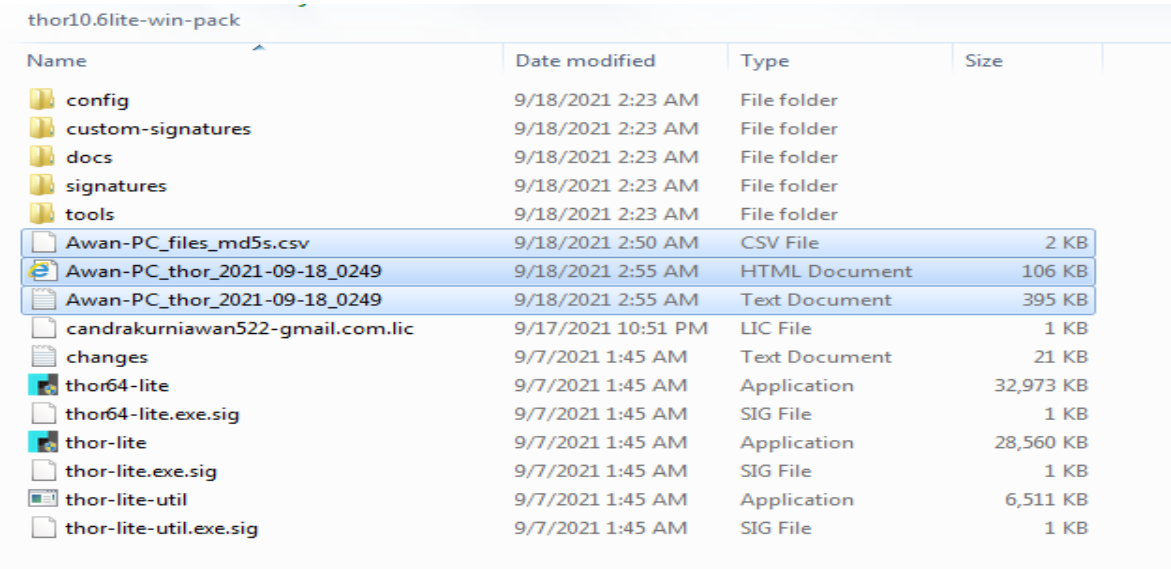
Pada Gambar diatas diketahui bahwa ketika dijalankan maka pertama akan mencari file lisensi terlebih dahulu.



Gambar 5. Update Program File & Signature File

Ketika sudah dilakukan *update* dan *upgrade* maka Thor Scanner siap untuk digunakan. Dalam menjalankan Thor Scanner tidak diperlukan perintah tambahan lagi, cukup menjalankan Thor Scanner melalui PowerShell/CMD dengan perintah `.\thor-lite.exe` maka akan melakukan pendeteksian secara menyeluruh. Hal ini akan memakan waktu cukup lama karena mendeteksi pada seluruh sistem.

Ketika proses pendeteksian sudah selesai maka pada folder thor10.6lite-win-pack akan terdapat output pendeteksian sebagai berikut



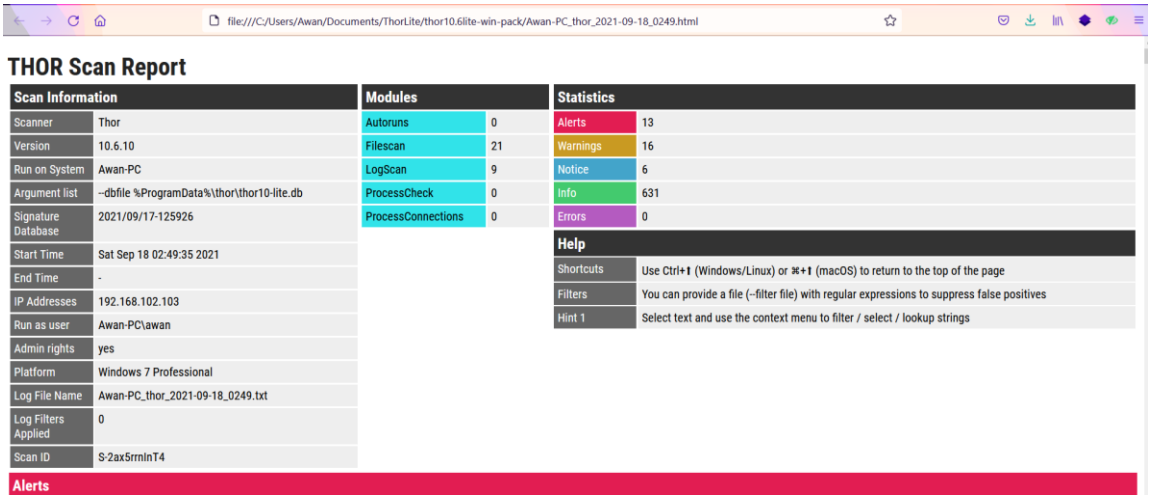
Gambar 6. Hasil Pendeteksian Pada Sistem

Hasil pendeteksian akan tersimpan dengan nama sesuai nama PC. File Awan-PC_files-md5s.csv berisi nilai hash MD5 dari file-file yang terdeteksi berbahaya. Gambar 7 menunjukkan nilai MD5, lokasi file, dan skor pendeteksian.

d3ebfad9ef5e0652f4c9bfaac7685b36	C:\Program Files (x86)\ossec-agent\shared\system_audit_rcl.txt	75
c73e71825adbfb9821b9fa6e8672903c	C:\Users\awan\AppData\Local\Temp\Rar$EXa2444.3634\Win32\mimidrv.sys	190
6c9ad4e67032301a61a9897377d9cff8	C:\Users\awan\AppData\Local\Temp\Rar$EXa2444.3634\Win32\mimikatz.exe	405
d0a1828f64842dde399244d604ceea24	C:\Users\awan\AppData\Local\Temp\Rar$EXa2444.3634\Win32\mimilib.dll	115
825e6e194a9d5e12cbf109b7de07a244	C:\Users\awan\AppData\Local\Temp\Rar$EXa2444.3634\Win32\mimilove.exe	110
64321f9e601651cb623e63d67de6c984	C:\Users\awan\AppData\Local\Temp\Rar$EXa2444.3634\Win32\mimispool.dll	135
c94de9019767a79573b25c870936d9a8	C:\Users\awan\AppData\Local\Temp\Rar$EXa2444.3634\x64\mimidrv.sys	190
bb8bdb3e8c92e97e2f63626bc3b254c4	C:\Users\awan\AppData\Local\Temp\Rar$EXa2444.3634\x64\mimikatz.exe	480
ddfad0d55be70acdfea36acf28d418b3	C:\Users\awan\AppData\Local\Temp\Rar$EXa2444.3634\x64\mimilib.dll	115
a03b57cc0103316e974bbb0f159f78f6	C:\Users\awan\AppData\Local\Temp\Rar$EXa2444.3634\x64\mimispool.dll	135
50af46128e147d85ef04ea91985986a3	C:\Users\awan\Downloads\c268156fdb9d27a85c1296b821b76551651583032f55620618c5c9a6facfb7c5	1035
c73e71825adbfb9821b9fa6e8672903c	C:\Users\awan\Downloads\Win32\mimidrv.sys	190
6c9ad4e67032301a61a9897377d9cff8	C:\Users\awan\Downloads\Win32\mimikatz.exe	405
d0a1828f64842dde399244d604ceea24	C:\Users\awan\Downloads\Win32\mimilib.dll	115
825e6e194a9d5e12cbf109b7de07a244	C:\Users\awan\Downloads\Win32\mimilove.exe	110
64321f9e601651cb623e63d67de6c984	C:\Users\awan\Downloads\Win32\mimispool.dll	135
c94de9019767a79573b25c870936d9a8	C:\Users\awan\Downloads\x64\mimidrv.sys	190
bb8bdb3e8c92e97e2f63626bc3b254c4	C:\Users\awan\Downloads\x64\mimikatz.exe	480
ddfad0d55be70acdfea36acf28d418b3	C:\Users\awan\Downloads\x64\mimilib.dll	115
a03b57cc0103316e974bbb0f159f78f6	C:\Users\awan\Downloads\x64\mimispool.dll	135
15e38bbae4b67894c1104145cc307081	C:\Users\awan\Favorites\Links\Suggested Sites.url	50

Gambar 7. Nilai Hash Hasil Pendeteksian

Selanjutnya pada file Awan-PC_thor_2021-09-18_0249.html dan .txt berisi hasil keseluruhan atas pendeteksian yang dilakukan. Berikut merupakan hasil dalam bentuk html.



Gambar 8. Hasil Pendeteksian dengan Format HTML

Hasil pendeteksian tercatat semua pada file Awan-PC_thor_2021-09-18_0249.html dan mudah dipahami.

B. Menggunakan Linux

Thor Scanner dapat berjalan juga pada perangkat Linux. Aplikasi Thor Scanner pada Linux sebelummya sudah diunduh pada tahap diatas, sehingga pada bagian ini akan dijelaskan cara penggunaannya yang tidak jauh beda seperti pada Windows.

1. Instalasi Thor Scanner Pada Linux

Thor Scanner pada Linux sebelumnya sudah diunduh dengan nama file thor10.6lite-linux-pack.zip. Selanjutnya dilakukan ekstraksi file zip dan menyalin file lisensi.lic dalam folder thor10.6lite-linux-pack. Lokasi file saat ini berada pada `awan@awan:~/Documents/ThorLite/`, sehingga dilakukan perintah berikut :

```
mkdir thor10.6lite-linux-pack
mv thor10.6lite-linux-pack.zip
/home/awan/Documents/ThorLite/thor10.6lite-linux-pack

unzip thor10.6lite-linux-pack.zip
cp candrakurniawan522-gmail.com.lic
/home/awan/Documents/ThorLite/thor10.6lite-linux-pack
```

Sama seperti pada Windows, sebelum Thor Scanner dijalankan maka dilakukan update dan upgrade terlebih dahulu dengan perintah:

```
sudo ./thor-lite-util update
sudo ./thor-lite-util upgrade
```

2. Menjalankan Thor Scanner

Setelah Thor Scanner dilakukan update dan upgrade maka selanjutnya menjalankan Thor Scanner dapat digunakan dengan perintah :

```
sudo ./thor-lite-linux
```

Pendeteksian akan menghasilkan 3 files yaitu awan_files_md5s.csv, awan_thor_2021-09-18_1950.html, dan awan_thor_2021-09-18_1950.txt seperti Pada Gambar 9. Hasil ini seperti pada Windows yang telah dijelaskan diatas.

```
awan@awan:~/Documents/ThorLite/thor10.6lite-linux-pack$ ls -la
total 86648
drwxrwxr-x 7 awan awan     4096 Sep 18 20:20 .
drwxrwxr-x 3 awan awan     4096 Sep 18 19:43 ..
-rw------- 1 root root       49 Sep 18 20:19 awan_files_md5s.csv
-rw-r--r-- 1 root root   611269 Sep 18 20:15 awan_thor_2021-09-18_1950.html
-rw------- 1 root root   528235 Sep 18 20:15 awan_thor_2021-09-18_1950.txt
-rw-rw-r-- 1 awan awan      516 Sep 18 19:49 candrakurniawan522-gmail.com.lic
-rw-r--r-- 1 awan awan    21153 Sep  7 15:44 changes.log
drwxr-xr-x 2 awan awan     4096 Sep  7 15:44 config
drwxr-xr-x 5 awan awan     4096 Sep  7 15:44 custom-signatures
drwxr-xr-x 2 awan awan     4096 Sep  7 15:44 docs
drwxr-xr-x 5 awan awan     4096 Sep 17 20:00 signatures
-rw-rw-r-- 1 awan awan 28878108 Sep 18 12:55 thor10.6lite-linux-pack.zip
-rwxr-xr-x 1 awan awan 24380144 Sep  7 15:44 thor-lite-linux
-rwxr-xr-x 1 awan awan 27737880 Sep  7 15:44 thor-lite-linux-64
-rw-r--r-- 1 awan awan      256 Sep  7 15:44 thor-lite-linux-64.sig
-rw-r--r-- 1 awan awan      256 Sep  7 15:44 thor-lite-linux.sig
-rwxr-xr-x 1 awan awan  6503852 Sep  7 15:44 thor-lite-util
-rw-r--r-- 1 awan awan      256 Sep  7 15:44 thor-lite-util.sig
drwxr-xr-x 2 awan awan     4096 Sep  7 15:44 tools
```

Gambar 9. Hasil Pendeteksian Pada Sistem Linux

C. Hasil Scanning Menggunakan Thor Scanner Pada Windows dan Linux

Hasil pendeteksian menggunakan Thor Scanner akan disimpan dalam 2 (dua) bentuk *file* yaitu .txt dan .html. Kedua *file* tersebut akan secara otomatis akan terbentuk ketika proses pendeteksian telah selesai seperti pada Gambar 10.

Gambar 10. Hasil Pendeteksian

Dari hasil tersebut maka selanjutnya dapat dilakukan penghapusan pada *file-file* yang terdeteksi sebagai *malware* atau *malicious*. Selain itu pada hasil Thor Scanner juga memberikan nilai hash dari file yang dideteksi, sehingga memungkinkan untuk dapat mencari teknik, taknik, dan prosedur dari *malware* tersebut pada laman virustotal atau pada Mittre Attack.

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
CPNS (III/a)

Disetujui Oleh

Ditandatangani secara elektronik oleh:
SANDIMAN AHLI MUDA
NOVIAN NUR CAHYA, S.ST, M.Kom.
Penata (III/c)