PANDUAN TEKNIS

PROSES IDENTIFIKASI DAN ANALISIS

Dokumen ini menjelaskan secara teknis proses identifikasi dan analisis untuk memastikan bahwa insiden yang telah terjadi dapat diketahui sumber serangannya. Selain itu juga untuk mengumpulkan informasi yang cukup tentang insiden tersebut sehingga tim dapat memprioritaskan langkah selanjutnya dalam menangani insiden. Dalam melakukan proses identifikasi insiden, tim yang bertugas diharuskan melakukan proses dengan menggunakan akun administrator atau root. Rincian proses identifikasi dan analisis adalah sebagai berikut :

A. Identifikasi dan Analisis Kerentanan

Proses	Penjelasan	Tools
Identifikasi Kerentanan Sistem	Melakukan identifikasi kerentanan dengan menggunakan tools baik yang Open Source maupun Lisensi. Proses ini bertujuan untuk menemukan kerentanan dengan berdasarkan teknik scanning atau secara otomatis dengan tools. Analisis dilakukan dengan memeriksa tingkat kerentanan yang ditemukan oleh tools tersebut, High/Medium/Low. Dan lakukan verifikasi dengan melakukan akses pada halaman/aplikasi yang terdapat kerentanan.	Open Source (Kali Linux): • Nikto • Burp Suite Lisensi : • Accunetix • Nessus Online Scanning : • Virus Total (https://virustotal.com) • Sucuri (https://sitecheck. sucuri.net)
Identifikasi Kerentanan Sistem File atau Direktori	Melakukan identifikasi sistem File atau Direktori dengan menggunakan tools atau scanning secara otomatis. Proses ini bertujuan untuk menemukan File atau Direktori yang bersifat Publik dan terdapat kerentanan pada File atau Direktori tersebut.	Open Source (Kali Linux): • Uniscan Command : # uniscan -u <url> -qwed Contoh :

	Analisis dilakukan dengan memeriksa secara langsung File atau Direktori yang ditemukan dan melakukan verifikasi pada halaman yang terdapat kerentanan File atau Direktori.	# uniscan -u https://govcsirt.bssn.go.id -qwed
Identifikasi Kerentanan Content Management System (CMS)	Melakukan identifikasi sistem website yang menggunakan CMS secara otomatis dengan tools scanning. Tujuannya untuk menemukan kerentanan baik Versi/Plugins/Library yang telah usang (Old Version). Analisis dilakukan dengan memeriksa hasil scanning dan memverifikasi pada Website CVE Details dan Exploit-DB.	Open Source (Kali Linux): • CMS Wordpress # wpscan -u https://x123.com • CMS Joomla # joomscan -u https://x123.com • CMS Drupal # droopalscan -u https://x123.com
Identifikasi Kerentanan Listening Port (Port yang terbuka)	Melakukan identifikasi Listening Port dengan menggunakan tools untuk menemukan Layanan yang dibuka. Analisis dilakukan dengan memeriksa hasil scanning dan memverifikasi pada Website Exploit-DB atau via Google Dork dengan keyword Nama dan Versi Layanan yang ditemukan.	Open Source (Kali Linux): • Nmap Command : # nmap -A target # nmap -v -sU -sS -p- -A -T4 target Contoh : # nmap -A 192.168.8.120 # nmap -v -sU -sS -p- -A -T4 192.168.8.120

B. Identifikasi dan Analisis Environment System

Proses	Penjelasan	Command
Identifikasi Rute Jaringan (Network Routing)	Melakukan identifikasi jaring komunikasi yang terhubung dari Server menuju koneksi internet. Analisis dilakukan dengan memeriksa daftar perangkat atau IP address yang terkoneksi server menuju koneksi internet global	Untuk Debian Varian : # traceroute 8.8.8.8 Untuk RHEL/Centos : # tracepath 8.8.8.8 Untuk Windows : C:\> netstat -r

Identifikasi Versi Sistem Operasi	Melakukan identifikasi versi dan distribusi sistem operasi yang digunakan. Analisis dilakukan dengan memeriksa hasil yang ditemukan dan memverifikasi pada Website Exploit-DB atau via Google Dork dengan keyword Nama dan Versi Sistem Operasi yang ditemukan.	Mencetak versi kernel (Debian/RHEL/Centos) : # uname -a Mencetak distribusi Debian OS : # cat /etc/lsb-release Mencetak distribusi RHEL/CentOS : # cat /etc/redhat-release Untuk Windows : C:\> ver C:\> set

C. Identifikasi dan Analisis Aplikasi / Layanan

Proses	Penjelasan	Command
Identifikasi Daftar Layanan/Proses yang Berjalan	Melakukan identifikasi layanan/proses yang berjalan dengan menggunakan tools yang telah ada pada sistem operasi. Hal ini bertujuan untuk mencari layanan/proses yang menggunakan resource sangat tinggi atau malicious service. Analisis dilakukan dengan memeriksa layanan/proses yang menggunakan resource yang tinggi, lalu memvalidasi user yang menggunakan serta ID Layanan tersebut.	Debian/RHEL/CentOS : # ps -aux Windows : C:\> net start C:\> sc query C:\> sc query <service> C:\> sc queryex state= all
Identifikasi Daftar Aplikasi yang Berjalan	Melakukan identifikasi daftar aplikasi yang berjalan dengan menggunakan tools yang telah ada pada sistem operasi. Hal ini bertujuan untuk mencari aplikasi yang menggunakan resource	Debian/RHEL/CentOS : # top # htop Windows : C:\> tasklist

	sangat tinggi atau malicious application. Analisis dilakukan dengan memeriksa aplikasi yang menggunakan resource yang tinggi, lalu memvalidasi user yang menggunakan serta ID Aplikasi tersebut.	
Identifikasi Riwayat/History Sistem Operasi	Melakukan identifikasi seluruh program/aplikasi/layanan yang telah dijalankan oleh user. Analisis dilakukan dengan memeriksa daftar program/aplikasi/layanan tersebut yang merupakan program/aplikasi/layanan bersifat maliciuos serta melakukan analisis kegiatan yang dilakukan dari User tersebut.	Debian/RHEL/CentOS : # history
Identifikasi Aplikasi Terjadwal	Melakukan identifikasi terhadap aplikasi yang berjalan secara terjadwal baik per menit, per jam, per hari. Analisis dilakukan dengan menemukan daftar tersebut dan memverifikasi terkait adanya malicious aplikasi terjadwal.	Debian/RHEL/CentOS : # ls /etc/cron* # crontab -l Untuk Windows : C:\> schtask C:\> wmic startup list full C:\> wmic startup get Caption, Command

D. Identifikasi dan Analisis Jaringan Komunikasi

Proses	Penjelasan	Command
Identifikasi Jaringan Komunikasi yang Dibuka	Melakukan identifikasi dengan menampilkan daftar layanan/aplikasi/port yang terbuka atau bersifat Listening	Debian/RHEL/CentOS : # netstat -tulnp Windows : C:\> netstat -nao C:\> netstat -nao 5

	Analisis dilakukan dengan memverifikasi layanan tersebut yang bersifat malicious application/port.	
Identifikasi Jaringan Komunikasi yang Dibuka	Melakukan identifikasi dengan menampilkan daftar layanan/aplikasi/port yang telah terbangun (Established). Analisis dilakukan dengan memverifikasi layanan tersebut yang bersifat malicious connection.	Debian/RHEL/CentOS : # netstat -antup | grep "ESTA" Windows : C:\> netstat -nao
Identifikasi Koneksi ke Server	Melakukan identifikasi dengan menampilkan daftar User dan IP yang sedang melakukan akses interface (TTY) seperti contoh akses SSH, akses onBoard ke OS Analisis dilakukan dengan memverifikasi layanan tersebut yang bersifat malicious application/port.	Debian/RHEL/CentOS : # w Windows : C:\> net session C:\> net share C:\> net use
Identifikasi DNS dan Hostname	Melakukan identifikasi terkait dengan konfigurasi DNS dan hostname yang ada pada sistem operasi. Analisis dilakukan dengan memeriksa setiap konten pada file konfigurasi DNS dan Hostname.	Debian/RHEL/CentOS : # cat /etc/resolv.conf # cat /etc/hostname # cat /etc/hosts Windows : C:\> ipconfig /displaydns

E. Identifikasi dan Analisis User

Proses	Penjelasan	Command
Identifikasi Daftar User	Melakukan identifikasi terkait dengan daftar user yang ada pada sistem operasi. Dan melakukan identifikasi user yang punya akses terminal atau bash system.	Debian/RHEL/CentOS : # cat /etc/passwd | grep "bash" Windows : C:\> net user

	Analisis dilakukan dengan memeriksa setiap user pada file daftar user tersebut.	C:\> net user nama_user C:\> net localgroup C:\> net localgroup administrators
Identifikasi Daftar User Logged In	Melakukan identifikasi terkait dengan user yang pernah melakukan Login serta waktu dilakukannya aktivitas login. Analisis dilakukan dengan memeriksa setiap user yang telah login dan waktu login.	Debian/RHEL/CentOS : # lastlog # last

F. Identifikasi dan Analisis Direktori

Proses	Penjelasan	Command
Identifikasi Direktori Web Server	Melakukan identifikasi direktori penyimpanan file aplikasi/website yang terkena insiden. Identifikasi dilakukan dengan time analysis yaitu memfilter berdasarkan waktu terakhir file/direktori dilakukan perubahan. Analisis dilakukan dengan memeriksa setiap file/folder pada direktori tersebut.	Debian/RHEL/CentOS : # ls -alrt /var/www/html Windows : C:\> tree /F /A <drive> C:\> wmic environment get Description, VariableValue
Identifikasi Direktori Konfigurasi Web Server	Melakukan identifikasi direktori penyimpanan file konfigurasi web server yang terkena insiden. Analisis dilakukan dengan memeriksa konfigurasi web pada direktori tersebut.	Debian : # cat /etc/apache2/apache2.conf # ls -alrt /etc/apache2/conf-available/ RHEL/CentOS : # cat /etc/httpd/conf/ httpd.conf # ls -alrt /etc/httpd/conf.d/

G. Identifikasi dan Analisis Malicious File

Proses	Penjelasan	Command
Identifikasi Malicious File / Backdoor	Melakukan identifikasi file-file yang diasumsikan merupakan malicious file atau backdoor file. Identifikasi dilakukan dengan memfilter tiap file yang mempunyai konten string mengakses bash/shell, eksekusi file/aplikasi, membuka/menutup file, dll Analisis dilakukan dengan memeriksa setiap file yang ditampilkan.	Debian/RHEL/CentOS : # grep -RPn "(passthru|shell_exec|system|phpinfo|base64_decode|chmod|mkdir|fopen|fclose|fclose|readfile) *" nama_direktori # grep -Rinw nama_direktori -e "nama_string" Contoh : # grep -RPn "(passthru|shell_exec|system|phpinfo|base64_decode|chmod|mkdir|fopen|fclose|fclose|readfile) *" /var/ww/html # grep -Rinw /var/www/html -e "Hacked" Windows : C:\> find "nama_string_dicari"

H. Identifikasi dan Analisis Log

Proses	Penjelasan	Command
Identifikasi Direktori Access Log	Melakukan identifikasi direktori penyimpanan file log baik aplikasi, web server, ataupun error log. Analisis dilakukan dengan memeriksa secara detail mengenai konten dari setiap log tersebut. command tail -200 digunakan untuk menampilkan 200 baris terakhir dari file command tail -f digunakan untuk menampilkan baris-baris terakhir secara live pada file	Debian : # ls -alrt /var/log/apache2/ # tail -200 /var/log/apache2/access_log # tail -f /var/log/apache2/access_log # tail -200 /var/log/apache2/ssl_access_log RHEL/CentOS : # ls -alrt /var/log/httpd/

		# tail -200 /var/log/httpd/ access_log # tail -f /var/log/httpd/ access_log # tail -200 /var/log/httpd/ ssl_access_log Windows : C:\> eventvwr.msc (Security >> Special Logon (4672)) Export to *.evtx file
Identifikasi Log Berdasarkan Malicious File	Melakukan identifikasi malicious file yang ditemukan pada file Log. Analisis dilakukan dengan memeriksa identitas, timestamp, status code yang melakukan akses pada malicious file	Debian : # cat /var/log/apache2/ access_log | grep "nama_malicious_file" RHEL/CentOS : # cat /var/log/httpd/ access_log | grep "nama_malicious_file"
Identifikasi Log Berdasarkan IP Address	Melakukan identifikasi alamat IP yang melakukan malicious connection. Analisis dilakukan dengan memeriksa aktivitas yang dilakukan oleh alamat IP yang ditemukan.	Debian : # cat /var/log/apache2/ access_log | grep "ip_address" RHEL/CentOS : # cat /var/log/httpd/ access_log | grep "ip_address"

I. Identifikasi dan Analisis Database

Proses	Penjelasan	Command
Identifikasi Database	Melakukan identifikasi malicious string pada sistem database yang digunakan.	Debian/RHEL/CentOS : # mysqldump -u root -p nama_database > nama_file_export.sql

	Analisis dilakukan dengan memeriksa tabel dan string pada database.	Lalu masukan password root. Contoh : # mysqldump -u root -p csirt_db > export_db.sql

J. Identifikasi dan Analisis IP Address

Proses	Penjelasan	Tools
Identifikasi Alamat IP	Melakukan analisis sebuah alamat IP, baik pemilik IP, reputasi IP, IP report.	Whois IP : https://www.ultratools.com/tools/ipWhoisLookupResult IP Analyze : - https://www.ipalyzer.com/ - https://mxtoolbox.com/blacklists.aspx - https://www.abuseipdb.com/ IP Reputation : https://www.talosintelligence.com/reputation_center

PENGENALAN TOOLS PENANGANAN INSIDEN

A. Tools Log Analysis (GoAccess)

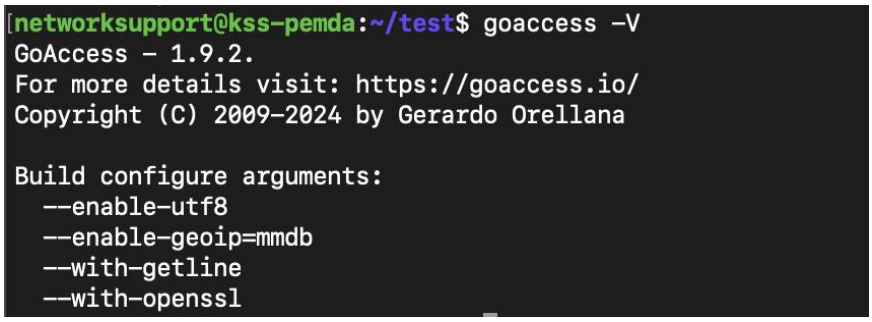
1) Definisi

GoAccess, merupakan sebuah aplikasi berbasis Open-Source yang digunakan untuk melakukan Visualisasi sebuah Log Web Aplikasi (access.log) secara realtime serta dapat ditampilkan menggunak interface Browser.

2) Instalasi dan Konfigurasi

Untuk melakukan instalasi, dapat mengunjungi situs https://goaccess.io/download yang berisi informasi mengenai detail download dan instalasi. Pada sesi ini, akan dilakukan instalasi dan konfigurasi pada Sistem Operasi Ubuntu, sebagai berikut :

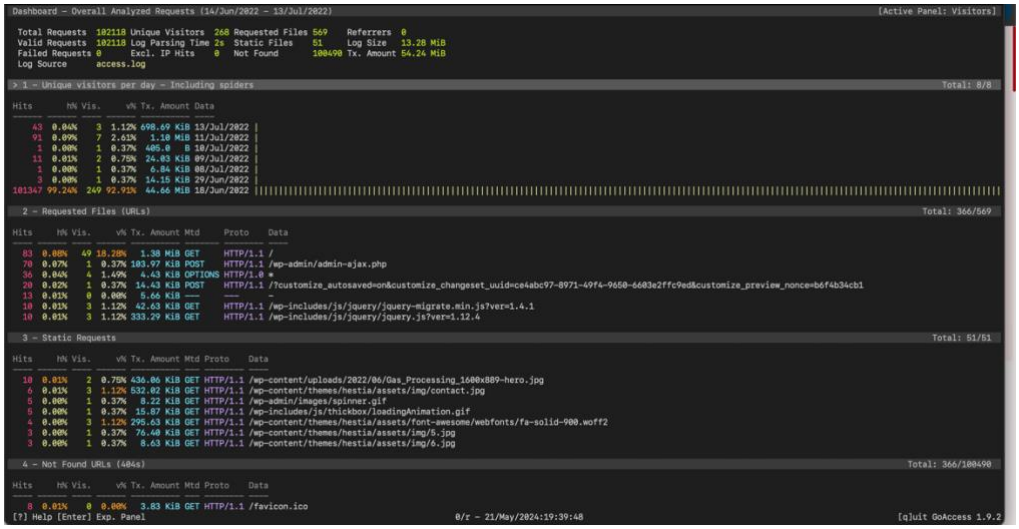
```
$ wget -O - https://deb.goaccess.io/gnugpg.key | gpg --dearmor | sudo tee /usr/share/keyrings/goaccess.gpg >/dev/null

$ echo "deb [signed-by=/usr/share/keyrings/goaccess.gpg arch=$(dpkg --print-architecture)] https://deb.goaccess.io/ $(lsb_release -cs) main" | sudo tee /etc/apt/sources.list.d/goaccess.list

$ sudo apt-get update
$ sudo apt-get install goaccess
$ goaccess -V
```



3) Implementasi dan Analisis

Jalankan perintah sebagai berikut :

```
$ goaccess access.log --log-format=COMBINED
```



Setelah dijalankan, akan mendapatkan visualisasi pada CLI yang menampilkan informasi dari file "access.log" tersebut. Informasi terdiri dari banyaknya akses yang diterima oleh Web Aplikasi, menampilkan path atau file mana saja yang banyak dilakukan akses oleh pengguna, hingga menampilkan Source IP yang melakukan akses kepada Web Aplikasi.

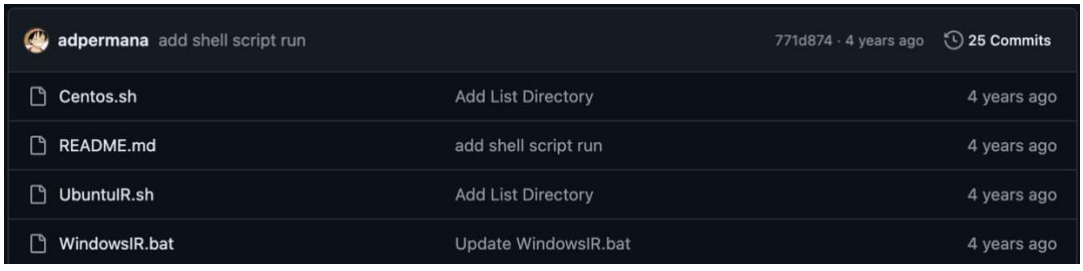
B. Tools Evidence Collector (UbuntuIR.sh)

1) Definisi

UbuntuIR.sh, merupakan sebuah script yang mengumpulkan beberapa evidence yang digunakan untuk melakukan analisa sebuah insiden keamanan siber. Script ini akan berjalan untuk mengumpulkan informasi mengenai Daftar Aplikasi Berjalan, Daftar User, Daftar Cronjob hingga informasi mengenai Malicious Software (Shell) yang seringkali ditemui saat terjadi insiden keamanan siber.

2) Instalasi dan Konfigurasi

Untuk melakukan instalasi, hanya perlu melakukan pengunduhan file script tersebut pada laman : https://github.com/adpermana/Incident-Response-Tools



3) Implementasi dan Analisis

Selanjutnya melakukan implementasi script tersebut dengan sintaks :

```
$ curl -sO https://raw.githubusercontent.com/adpermana/Incident-Response-Tools/analisa/UbuntuIR.sh && sudo bash ./UbuntuIR.sh nama_instansi
```

```
networksupport@kss-pemda:~$ curl https://raw.githubusercontent.com/adpermana/Incident-Response-Tools/master/UbuntuIR.sh | sudo sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1980  100  1980    0     0  26756      0 --:--:-- --:--:-- --:--:-- 26756
*******************************************************
Automate Data Collection for Ubuntu Server Script v1.0
*******************************************************
no crontab for root
Start Searching ...
grep: input file '/home/networksupport/UbuntuIR/21.Backdoor-Homedir.txt' is also the output
Finish Searching.

*******************************************************
Script Completed Succesfully, saved to ./Collection.tar.gz
*******************************************************
```

Setelah dijalankan akan menghasilkan sebuah file yaitu "Collection.tar.gz" dan perlu dilakukan unzip dengan cara :

```
$ gunzip Collection.tar.gz
```

Di dalam file tersebut terdapat 22 file txt yang berisi informasi untuk dilakukan analisa lebih lanjut.

```
root@ubuntu:/home/adminsvr/UbuntuIR# ls -al
total 1416
drwxrwxr-x  2 adminsvr adminsvr   4096 Feb  5 19:43 .
drwxr-xr-x 18 adminsvr adminsvr   4096 Feb  5 19:43 ..
-rw-rw-r--  1 adminsvr adminsvr     32 Feb  5 19:41 0.DateTime.txt
-rw-rw-r--  1 adminsvr adminsvr    404 Feb  5 19:41 10.Established_Conn.txt
-rw-rw-r--  1 adminsvr adminsvr    287 Feb  5 19:41 11.Connected_to_PC.txt
-rw-rw-r--  1 adminsvr adminsvr    726 Feb  5 19:41 12.DNS.txt
-rw-rw-r--  1 adminsvr adminsvr      7 Feb  5 19:41 13.Hostname.txt
-rw-rw-r--  1 adminsvr adminsvr    221 Feb  5 19:41 14.Hosts.txt
-rw-rw-r--  1 adminsvr adminsvr   3044 Feb  5 19:41 15.Daftar_User.txt
-rw-rw-r--  1 adminsvr adminsvr    134 Feb  5 19:41 16.Daftar_User_Bash.txt
-rw-rw-r--  1 adminsvr adminsvr   3478 Feb  5 19:41 17.Lastlog.txt
-rw-rw-r--  1 adminsvr adminsvr   6402 Feb  5 19:41 18.Last.txt
-rw-rw-r--  1 adminsvr adminsvr 833243 Feb  5 19:41 19.Homedir.txt
-rw-rw-r--  1 adminsvr adminsvr    113 Feb  5 19:41 1.Versi_Kernel.txt
-rw-rw-r--  1 adminsvr adminsvr 340605 Feb  5 19:41 20.VarWWWdir.txt
-rw-rw-r--  1 adminsvr adminsvr  46443 Feb  5 19:43 21.Backdoor-Homedir.txt
-rw-r--r--  1 root     root      44596 Feb  5 19:43 22.Backdoor-VarWWWdir.txt
-rw-rw-r--  1 adminsvr adminsvr    104 Feb  5 19:41 2.Versi_OS.txt
-rw-rw-r--  1 adminsvr adminsvr  53198 Feb  5 19:41 3.Daftar_Proses.txt
-rw-rw-r--  1 adminsvr adminsvr  35087 Feb  5 19:41 4.Daftar_Running_App.txt
-rw-rw-r--  1 adminsvr adminsvr   3988 Feb  5 19:41 5.History.txt
-rw-rw-r--  1 adminsvr adminsvr    331 Feb  5 19:41 6.Cron.txt
-rw-rw-r--  1 adminsvr adminsvr    921 Feb  5 19:41 7.Crontab.txt
-rw-rw-r--  1 adminsvr adminsvr   1457 Feb  5 19:41 8.Inbound.txt
-rw-rw-r--  1 adminsvr adminsvr   6013 Feb  5 19:41 9.Outbound.txt
root@ubuntu:/home/adminsvr/UbuntuIR#
```

C. Tools Malware / Backdoor Scanner (Thor-Lite)

1) Definisi

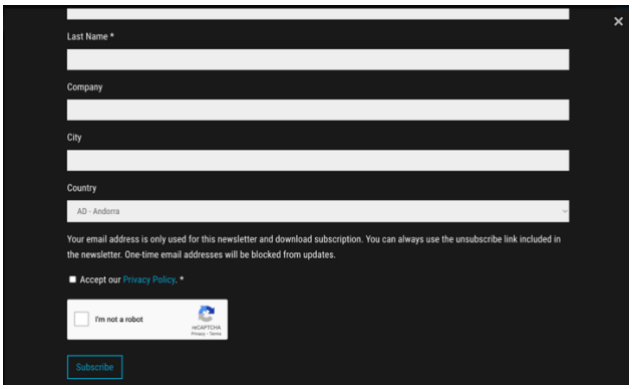
Thor-Lite, merupakan sebuah aplikasi pendeteksian portable untuk mendeteksi aktivitas mencurigakan pada sistem yang disusupi. Thor Scanner dapat mendeteki secara mendalam sampai local event log, registry, dan file system. Thor Scanner dapat menjadi system pendeteksi bagi aktivitas

berbahaya yang terlewat oleh antivirus umum. Hasil dari pendeteksian menggunakan Thor Scanner dapat dieksport dalam bentuk HTML,TXT, JSON, CSV.

2) Instalasi dan Konfigurasi

a) Registrasi User

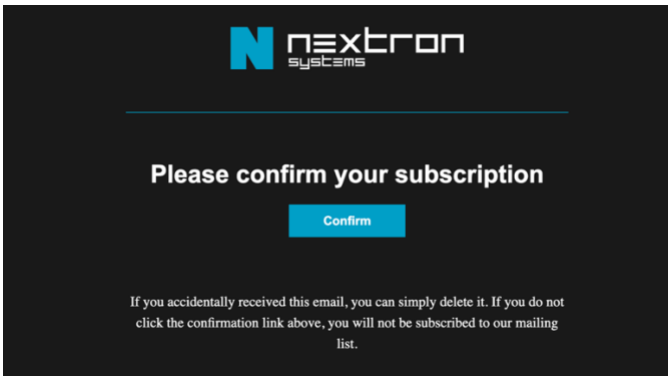
Lakukan registrasi user dengan melakukan akses ke alamat https://www.nextron-systems.com/thor-lite/#get-thor dan klik "Download THOR Lite" maka akan dilanjut ke page Registrasi seperti berikut :



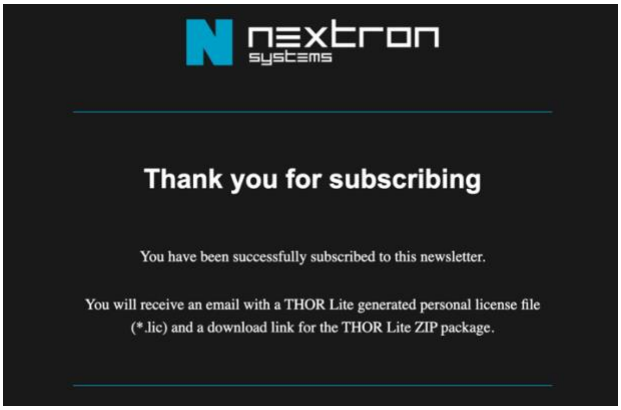
Lanjutkan dengan mengisi Email dan Nama (gunakan public mail) dan Klik "Subscribe"

b) Unduh lisensi dan aplikasi

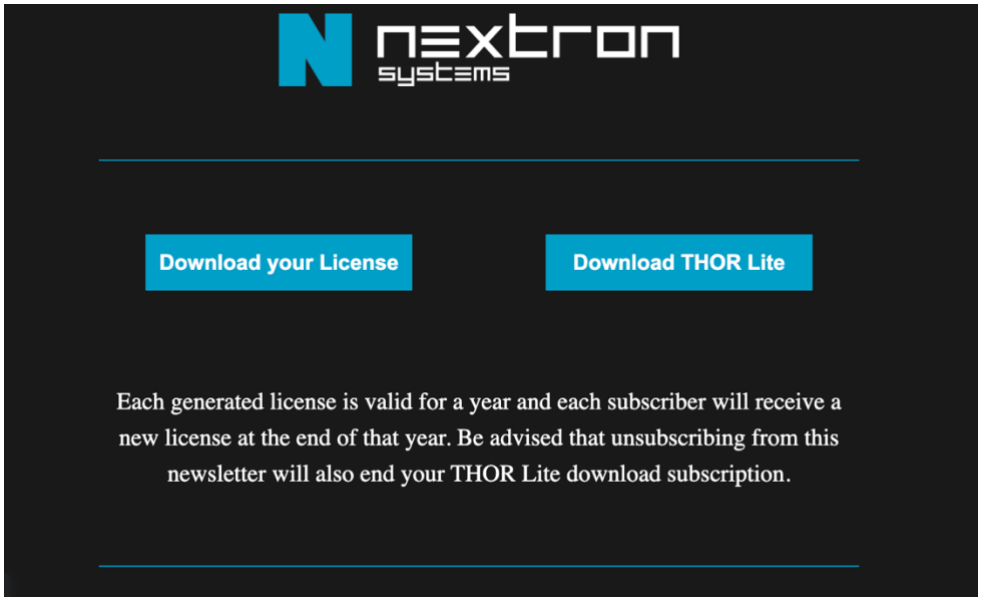
Setelah melakukan subscribe, tunggu beberapa saat dan akan muncul notifikasi pada email yang telah diregistrasi sebelumnya. Dan buka notifikasi tersebut akan muncul email sebagai berikut :



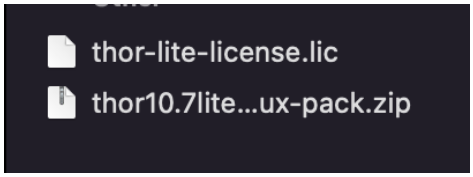
Lanjutkan dengan klik "Confirm" dan akan muncul kembali notifikasi email sebagai berikut :



Lanjutkan kembali dengan menunggu beberapa saat sampai muncul notifikasi kembali email untuk unduh lisensi dan aplikasi Thor, sebagai berikut :



Lakukan "Download your Licence" dan "Download THOR Lite" serta lakukan penyimpanan pada Direktori Komputer masing-masing sesuai berikut :



3) Implementasi dan Analisis

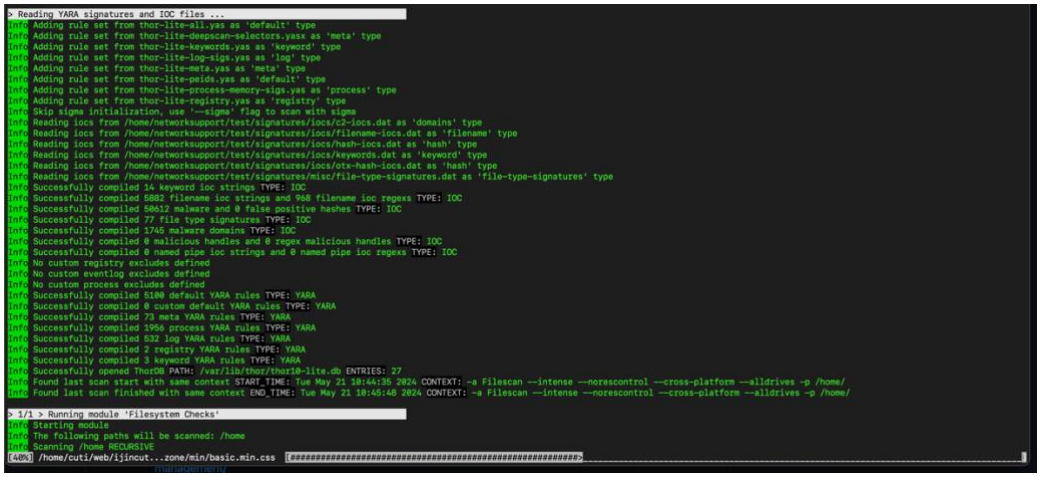
Selanjutnya copy-kan kedua file tersebut diatas ke Environment yang akan dilakukan analisa (File Lisensi dan File Aplikasi Thor harus 1 folder yang sama).

```
[networksupport@kss-pemda:~/test$ ls
 thor-lite-license.lic   thor10.7lite-linux-pack.zip
[networksupport@kss-pemda:~/test$ unzip thor10.7lite-linux-pack.zip
 Archive:  thor10.7lite-linux-pack.zip
    creating: signatures/
    creating: signatures/sigma/
   inflating: signatures/sigma/thor.yms
    creating: signatures/sigma/category/
```

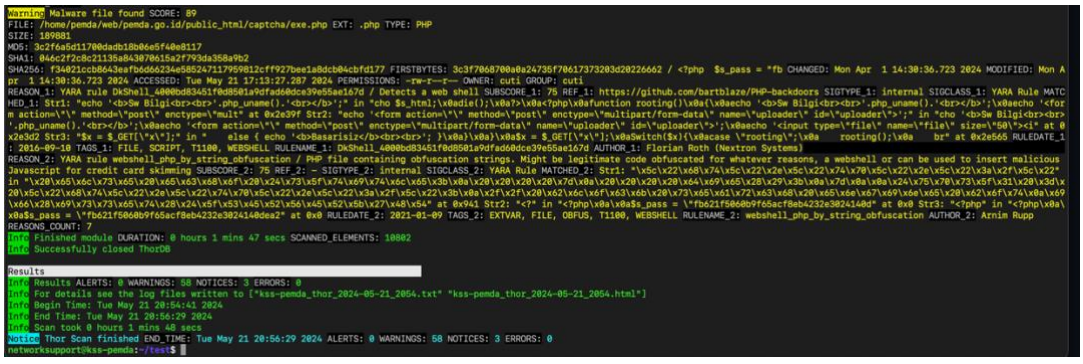
Setelah dipastikan smua file sudah siap, lanjutkan dengan :

```
$ sudo ./thor-lite-linux -a Filescan --intense -norescontrol -cross-platform -alldrives -p /home/
```

dengan /home merupakan folder yang akan dilakukan scan. Hasilnya sebagai berikut :



dan jika ditemukan adanya file berbahaya akan dimunculkan notifikasinya sebagai berikut :



D. Tools Security Audit (Lynis)

1) Definisi

Lynis, merupakan sebuah tool (open-source) yang dapat digunakan untuk melakukan audit dan hardening pada sebuah Sistem Operasi Unix (Linux)

2) Instalasi dan Konfigurasi

Untuk melakukan instalasi dan konfigurasi, lakukan sebagai berikut :

```
$ sudo apt-get update
$ sudo apt-get install lynis
$ sudo lynis show version
```

```
networksupport@kss-pemda:~/test$ sudo lynis show version
2.6.2
networksupport@kss-pemda:~/test$
```

3) Implementasi dan Analisis

Untuk implementasinya, lakukan :

```
$ sudo lynis audit system
```

```
[+] System Tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...

[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to complete

  - Plugin: debian
    [
[+] Debian Tests
------------------------------------
  - Checking for system binaries that are required by Debian Tests...
    - Checking /bin...                                  [ FOUND ]
    - Checking /sbin...                                 [ FOUND ]
    - Checking /usr/bin...                              [ FOUND ]
    - Checking /usr/sbin...                             [ FOUND ]
    - Checking /usr/local/bin...                        [ FOUND ]
    - Checking /usr/local/sbin...                       [ FOUND ]
  - Authentication:
    - PAM (Pluggable Authentication Modules):
      - libpam-tmpdir                                   [ Not Installed ]
      - libpam-usb                                      [ Not Installed ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
      - Checking / on /dev/sda3                         [ NOT ENCRYPTED ]
      - Checking /snap/core20/2264 on /var/lib/snapd/snaps/core20_2264.snap  [ NOT ENCRYPTED ]
      - Checking /snap/core20/2318 on /var/lib/snapd/snaps/core20_2318.snap  [ NOT ENCRYPTED ]
      - Checking /snap/lxd/22753 on /var/lib/snapd/snaps/lxd_22753.snap  [ NOT ENCRYPTED ]
      - Checking /snap/snapd/21184 on /var/lib/snapd/snaps/snapd_21184.snap  [ NOT ENCRYPTED ]
      - Checking /snap/lxd/24061 on /var/lib/snapd/snaps/lxd_24061.snap  [ NOT ENCRYPTED ]
      - Checking /snap/snapd/21465 on /var/lib/snapd/snaps/snapd_21465.snap  [ NOT ENCRYPTED ]
      - Checking /boot on /dev/sda2                     [ NOT ENCRYPTED ]
  - Software:
    - apt-listbugs                                      [ Not Installed ]
    - apt-listchanges                                   [ Not Installed ]
    - checkrestart                                      [ Not Installed ]
    - needrestart                                       [ Not Installed ]
    - debsecan                                          [ Not Installed ]
    - debsums                                           [ Not Installed ]
    - fail2ban                                          [ Installed with jail.local ]
]
```

Setelah lynis dijalankan untuk melakukan audit sistem, maka akan muncul hasil aplikasi keamanan mana saja yang telah dilakukan instalasi dan yang belum dilakukan instalasi dan konfigurasi. Hal ini penting untuk dapat melakukan identifikasi dalam peningkatan keamanan pada Sistem Operasi yang menjalankan layanan aplikasi.

E. Tools Vulnerability Analysis (LinPEAS)

1) Definisi

LinPEAS, merupakan sebuah script yang memetakan kemungkinan path/aplikasi yang dapat dilakukan Privilege Escalation pada Sistem Operasi Unix (Linux/MacOS).

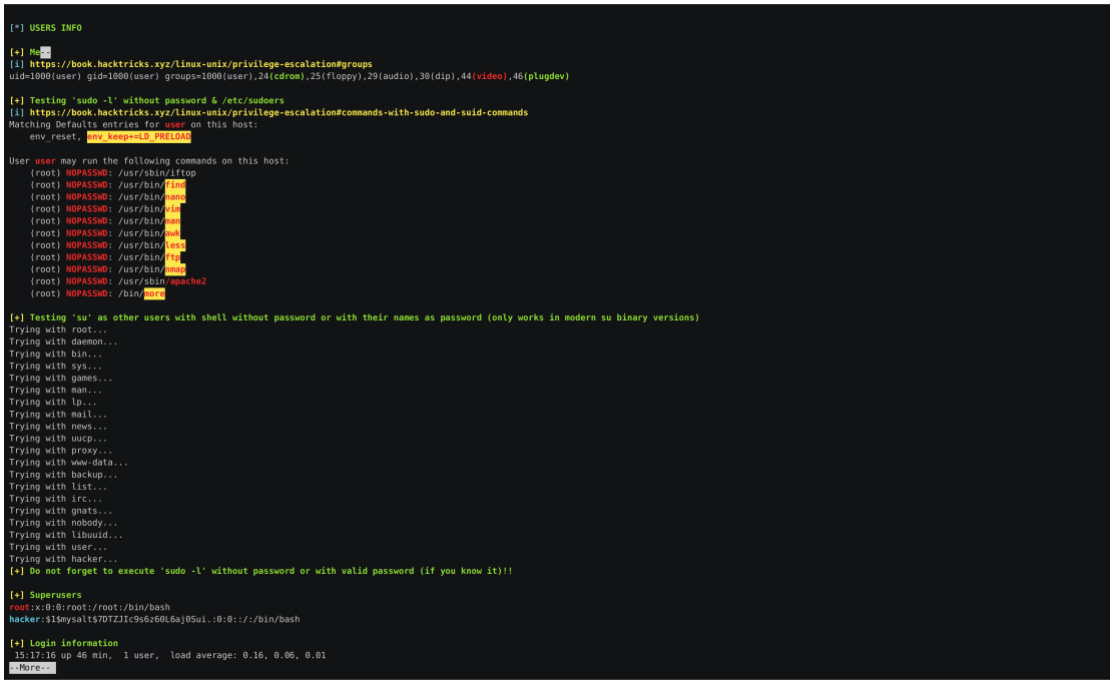
2) Instalasi dan Konfigurasi

Untuk menjalankan aplikasi ini, sebagai berikut :

```
$ curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh
```

3) Implementasi dan Analisis

Setelah dijalankan akan menghasilkan informasi mengenai aplikasi mana saja yang mempunyai kerawanan dan kemungkinan besar dapat diesploitasi guna esakalasi dari User biasa menjadi User tertinggi (root).



Jika informasi diberikan Legenda Bold Merah, maka 95% aplikasi tersebut dapat dilakukan Eksploitasi.