bangga melayani bangsa

PENGENALAN DAN SIMULASI TOOLS INVESTIGASI JUDI ONLINE

Depok, 22 November 2024

Jabang Aru Saputro, S.Tr.Kom

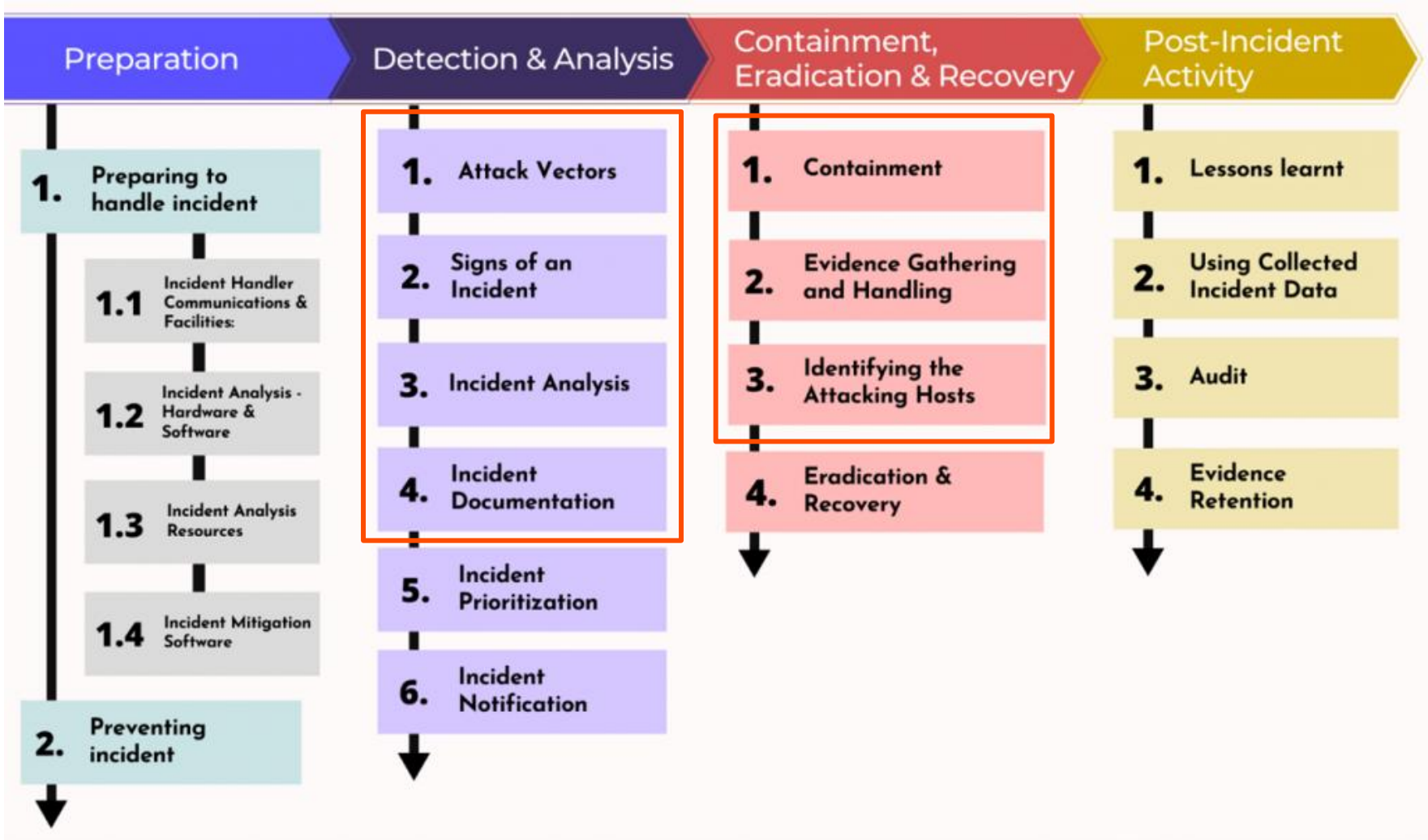
Direktorat Keamanan Siber dan Sandi Pemerintah Daerah

Jabang Aru Saputro, S.Tr.Kom.
Sandiman Ahli Pertama
pada Direktorat Keamanan Siber dan
Sandi Pemerintah Daerah

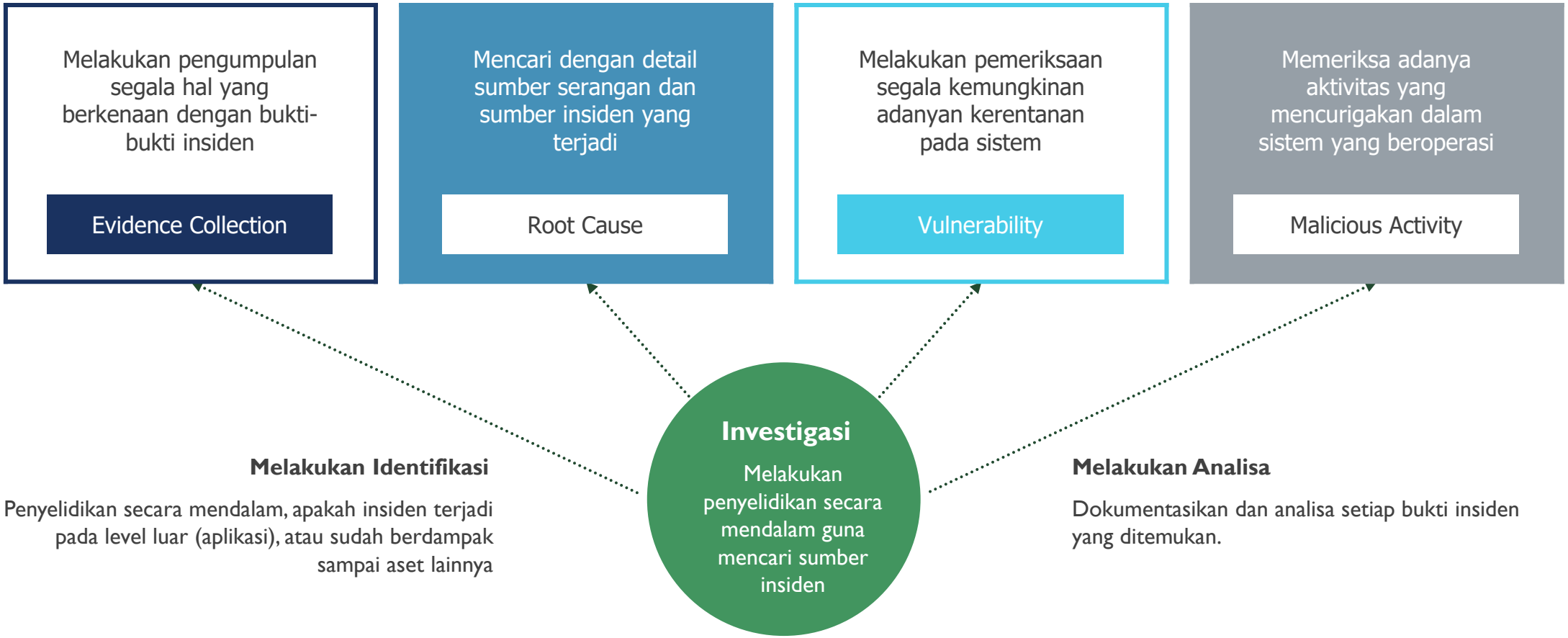
LinkedIn
Jabang Aru Saputro

DIREKTORAT KEAMANAN
SIBER DAN SANDI
PEMERINTAH DAERAH

TAHAPAN PENANGANAN INSIDEN



COMPROMISE ASSESSMENT

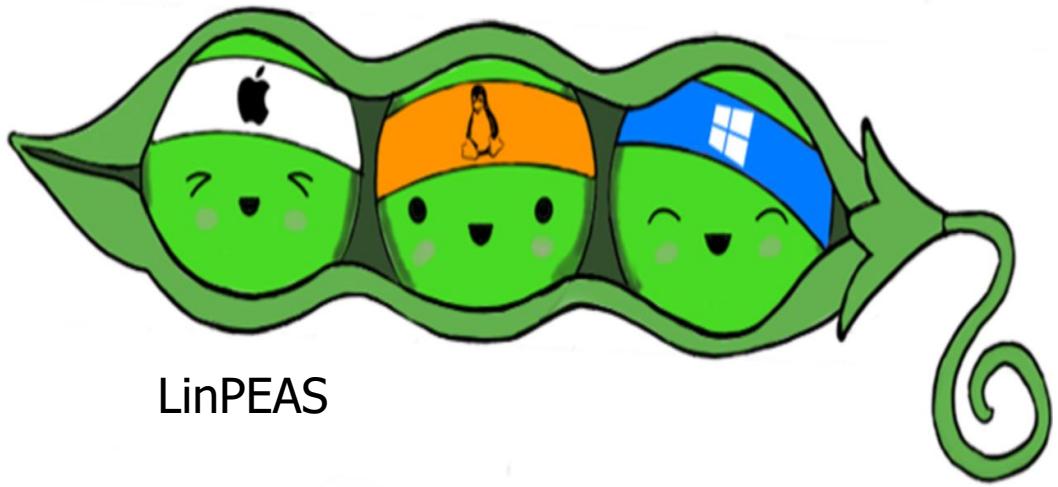


Sesi Pengenalan Tools

UbuntuIR

THOR Lite

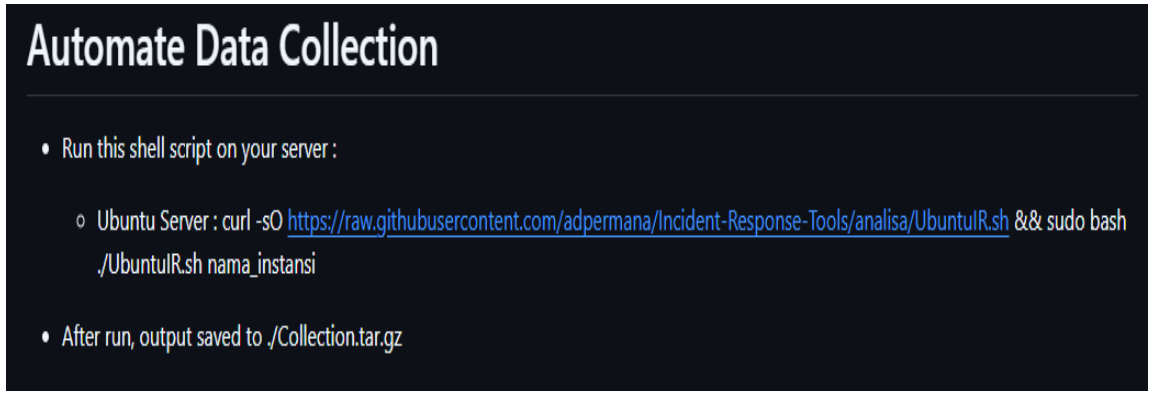
CISOFY
AUDITING-HARDENING-COMPLIANCE
Lynis

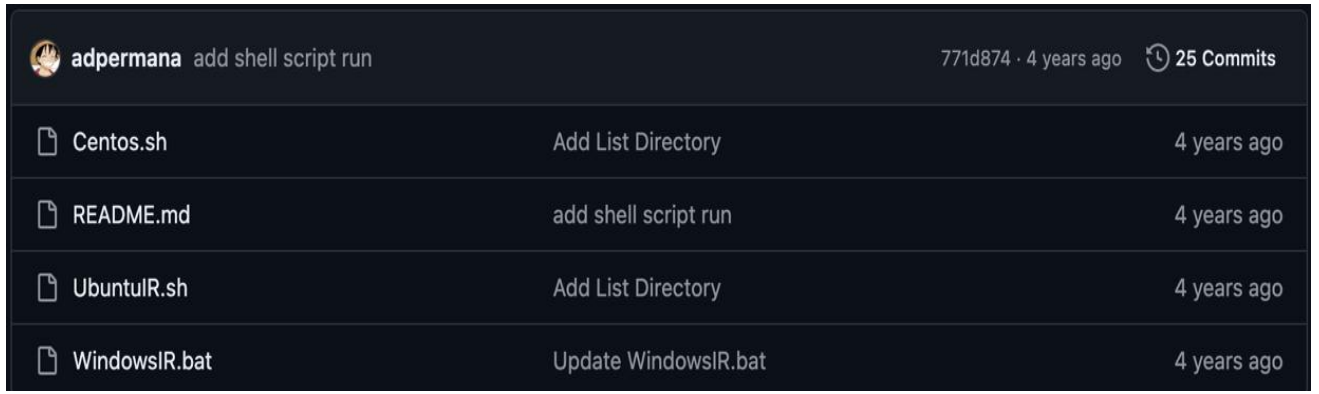


LinPEAS

Tools Log Analysis (UbuntuIR.sh)

Tools Log Analysis





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.

Script juga mencari potensi backdoor PHP di direktori tertentu, yang membantu dalam menganalisis keamanan sistem.

Silahkan akses https://raw.githubusercontent.com/adpermana/Incident-Response-Tools/analisa/UbuntuIR.sh

Evidence Collector

```bash
#! /bin/bash

echo "************************************************************"
echo "Automate Data Collection for Ubuntu Server Script v1.0"
echo "************************************************************"

# Read Current Directory
curr=${PWD}

# Create Directory :
mkdir $curr/UbuntuIR-$1

# Sesuaikan Directory
dir=$curr/UbuntuIR-$1

# Identifikasi Date :
date > $dir/0.DateTime-$1.txt

# Identifikasi Versi Environment System :
uname -a > $dir/1.Versi_Kernel-$1.txt
cat /etc/lsb-release > $dir/2.Versi_OS-$1.txt

# Identifikasi Aplikasi/Service
ps -aux > $dir/3.Daftar_Proses-$1.txt
top -b -n 1 > $dir/4.Daftar_Running_App-$1.txt
cat /root/.bash_history > $dir/5.History-$1.txt
ls -al /etc/cron* > $dir/6.Cron-$1.txt
crontab -l > $dir/7.Crontab-$1.txt
ls -al /var/spool/cron/crontabs/ > $dir/7-1.Crontab-$1.txt
bash -c 'for user in $(cut -f1 -d: /etc/passwd); do echo "Cron jobs for user: $user"; crontab -l -u $user; echo ""; done' > $dir/7-2.Crontab-$1.txt

# Identifikasi Jaring Komunikasi
netstat -tulnp > $dir/8.Inbound-$1.txt
netstat -antup > $dir/9.Outbound-$1.txt
netstat -antup | grep "ESTABLISHED" > $dir/10.Established_Conn-$1.txt
w > $dir/11.Connected_to_PC-$1.txt
cat /etc/resolv.conf > $dir/12.DNS-$1.txt
cat /etc/hostname > $dir/13.Hostname-$1.txt
cat /etc/hosts > $dir/14.Hosts-$1.txt
```

Isi dari UbuntuIR.sh

```bash
# Identifikasi User
cat /etc/passwd > $dir/15.Daftar_User-$1.txt
cat /etc/passwd | grep "bash"> $dir/16.Daftar_User_Bash-$1.txt
lastlog > $dir/17.Lastlog-$1.txt
last > $dir/18.Last-$1.txt

# List Directory
ls -alrt -R /home > $dir/19.Homedir-$1.txt
ls -alrt -R /var/www > $dir/20.VarWWWdir-$1.txt

# Searching Backdoor File
echo "Start Searching ..."
grep -RPn "(passthru|shell_exec|system|phpinfo|base64_decode|chmod|mkdir|fopen|fclose|fclose|readfile) *\(" /home/ > $dir/21.Backdoor-Homedir-$1.txt
grep -RPn "(passthru|shell_exec|system|phpinfo|base64_decode|chmod|mkdir|fopen|fclose|fclose|readfile) *\(" /var/www/ > $dir/22.Backdoor-VarWWWdir-$1.txt

# Searching others malicious activity
grep -Rinw /home -e "slot" -e "gacor" -e "maxwin" -e "thailand" -e "sigmaslot" -e "zeus" -e "cuan" > $dir/23.ListSlot-$1.txt
echo "Finish Searching.\n"

# Create Compressed File
tar -czf Collection-$1.tar.gz UbuntuIR-$1
rm -rf UbuntuIR-$1

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

Penjelasan Isi UbuntuIR.sh

```
#! /bin/bash

echo "************************************************************"
echo "Automate Data Collection for Ubuntu Server Script v1.0"
echo "************************************************************"

# Read Current Directory
curr=${PWD}

# Create Directory :
mkdir $curr/UbuntuIR-$1

# Sesuaikan Directory
dir=$curr/UbuntuIR-$1

# Identifikasi Date :
date > $dir/0.DateTime-$1.txt

# Identifikasi Versi Environment System :
uname -a > $dir/1.Versi_Kernel-$1.txt
cat /etc/lsb-release > $dir/2.Versi_OS-$1.txt

# Identifikasi Aplikasi/Service
ps -aux > $dir/3.Daftar_Proses-$1.txt
top -b -n 1 > $dir/4.Daftar_Running_App-$1.txt
cat /root/.bash_history > $dir/5.History-$1.txt
ls -al /etc/cron* > $dir/6.Cron-$1.txt
crontab -l > $dir/7.Crontab-$1.txt
ls -al /var/spool/cron/crontabs/ > $dir/7-1.Crontab-$1.txt
bash -c 'for user in $(cut -f1 -d: /etc/passwd); do echo "Cron jobs for user: $user"; crontab -l -u $user; echo ""; done' > $dir/7-2.Crontab-$1.txt
```

- **date > $dir/0.DateTime.txt :**
  Menyimpan tanggal dan waktu saat ini ke dalam file 0.DateTime.txt.
- **uname -a > $dir/1.Versi_Kernel.txt :**
  Menyimpan informasi kernel ke dalam file 1.Versi_Kernel.txt
- **cat /etc/lsb-release > $dir/2.Versi_OS.txt :**
  Menyimpan informasi versi OS ke dalam file 2.Versi_OS.txt
- **ps -aux > $dir/3.Daftar_Proses.txt :**
  Menyimpan daftar lengkap dari semua proses yang berjalan di sistem kedalam file 3.Daftar_Proses.txt
- **top -b -n 1 > $dir/4.Daftar_Running_App.txt :**
  Menyimpan daftar lengkap dari aplikasi yang berjalan di sistem kedalam file 4.Daftar_Running_App.txt
- **cat /root/.bash_history > $dir/5.History.txt :**
  Menyalin isi dari file /root/.bash_history (file yang berisi riwayat perintah-perintah bash yang pernah dieksekusi oleh pengguna root.) ke dalam file baru yang bernama 5.History.txt.
- **ls /etc/cron* > $dir/6.Cron.txt :**
  Script ini akan mencari dan menampilkan daftar file atau direktori yang dimulai dengan cron di dalam direktori /etc, dan menyimpan daftar tersebut dalam file 6.Cron.txt
- **crontab -l > $dir/7.Crontab.txt :**
  Berfungsi untuk menampilkan konten dari crontab (cron table) untuk pengguna saat ini kemudian disimpan di file crontab.txt
- **ls –al /var/spool/cron/crontabs/ > $dir/7-1.Crontab.txt**
  Mengambil informasi crontab dari semua pengguna yg ada di direktori /var/spool/cron/crontabs/. Direktori ini biasa digunakan oleh sistem untuk menyimpan file file crontab yg berisi tugas-tugas yg dijadwalkan menggunakan cron.
- **bash -c 'for user in $(cut -f1 -d: /etc/passwd); do echo "Cron jobs for user: $user"; crontab -l -u $user; echo ""; done' > $dir/7-2.Crontab.txt**
  Mengidentifikasi semua tugas cron (cron jobs) untuk setiap pengguna yang terdaftar di sistem.

Lanjutan Penjelasan Isi UbuntuIR.sh

```
# Identifikasi Jaring Komunikasi
netstat -tulnp > $dir/8.Inbound-$1.txt
netstat -antup > $dir/9.Outbound-$1.txt
netstat -antup | grep "ESTABLISHED" > $dir/10.Established_Conn-$1.txt
w > $dir/11.Connected_to_PC-$1.txt
cat /etc/resolv.conf > $dir/12.DNS-$1.txt
cat /etc/hostname > $dir/13.Hostname-$1.txt
cat /etc/hosts > $dir/14.Hosts-$1.txt
```

- **netstat -tulnp > $dir/8.Inbound.txt**
  Perintah netstat dengan opsi -tulnp akan menampilkan daftar semua koneksi yang sedang mendengarkan (listening) di dalam sistem, termasuk port dan program yang mendengarkan port tersebut. Output dari perintah ini akan disimpan dalam file 8.Inbound.txt
- **netstat -antup > $dir/9.Outbound.txt**
  Perintah netstat dengan opsi -antup akan menampilkan daftar semua koneksi yang sedang aktif, termasuk koneksi TCP dan UDP yang sedang aktif. Output dari perintah ini akan disimpan dalam file 9.Outbound.txt
- **netstat -antup | grep "ESTA" > $dir/10.Established_Conn.txt**
  Perintah ini akan menampilkan daftar semua koneksi yang sedang berstatus "ESTABLISHED" (terhubung) dan menyimpannya dalam file 10.Established_Conn.txt
- **w > $dir/11.Connected_to_PC.txt**
  Perintah w digunakan untuk menampilkan informasi tentang pengguna yang sedang login ke sistem, termasuk informasi tentang koneksi yang sedang aktif. Output dari perintah ini akan disimpan dalam file 11.Connected_to_PC.txt
- **cat /etc/resolv.conf > $dir/12.DNS.txt**
  Perintah cat digunakan untuk menampilkan isi dari file /etc/resolv.conf, yang berisi konfigurasi DNS untuk sistem. Output dari perintah ini akan disimpan dalam file 12.DNS.txt
- **cat /etc/hostname > $dir/13.Hostname.txt**
  Perintah cat digunakan untuk menampilkan isi dari file /etc/hostname, yang berisi nama host untuk sistem. Output dari perintah ini akan disimpan dalam file 13.Hostname.txt
- **cat /etc/hosts > $dir/14.Hosts.txt**
  Perintah cat digunakan untuk menampilkan isi dari file /etc/hosts, yang berisi daftar nama host dan alamat IP yang sesuai untuk sistem. Output dari perintah ini akan disimpan dalam file 14.Hosts.txt

Lanjutan Penjelasan Isi UbuntuIR.sh

```
# Identifikasi User
cat /etc/passwd > $dir/15.Daftar_User.txt
cat /etc/passwd | grep "bash"> $dir/16.Daftar_User_Bash.txt
lastlog > $dir/17.Lastlog.txt
last > $dir/18.Last.txt
```

- **cat /etc/passwd > $dir/15.Daftar_User.txt**
  Perintah cat digunakan untuk menampilkan isi dari file /etc/passwd, yang berisi informasi tentang semua pengguna yang terdaftar di sistem. Output dari perintah ini akan disimpan dalam file 15.Daftar_User.txt
- **cat /etc/passwd | grep "bash" > $dir/16.Daftar_User_Bash.txt**
  Perintah ini akan mencari baris-baris dalam file /etc/passwd yang mengandung kata "bash" (menandakan pengguna yang menggunakan shell bash sebagai shell default mereka). Output dari perintah ini akan disimpan dalam file 16.Daftar_User_Bash.txt
- **lastlog > $dir/17.Lastlog.txt**
  Perintah lastlog digunakan untuk menampilkan informasi terkait waktu terakhir pengguna melakukan login ke sistem. Output dari perintah ini akan disimpan dalam file 17.Lastlog.txt
- **last > $dir/18.Last.txt**
  Perintah last digunakan untuk menampilkan riwayat login pengguna ke sistem, termasuk informasi tentang waktu login dan logout terakhir, serta informasi terkait durasi sesi login. Output dari perintah ini akan disimpan dalam file 18.Last.txt

Lanjutan Penjelasan Isi UbuntuIR.sh

```
# List Directory
ls -alrt -R /home > $dir/19.Homedir.txt
ls -alrt -R /var/www > $dir/20.VarWWWdir.txt
```

- **ls -alrt -R /home**: Perintah ls dengan opsi -alrt -R /home digunakan untuk menampilkan semua file dan direktori secara rekursif dari direktori /home. **> $dir/19.Homedir.txt**: Operator > digunakan untuk mengarahkan output dari perintah ls ke dalam file teks yang bernama 19.Homedir.txt
- **ls -alrt -R /var/www**: Perintah ls dengan opsi yang sama digunakan untuk menampilkan semua file dan direktori secara rekursif dari direktori /var/www. **> $dir/20.VarWWWdir.txt**: Operator > digunakan untuk mengarahkan output dari perintah ls ke dalam file teks yang bernama 20.VarWWWdir.txt

Lanjutan Penjelasan Isi UbuntuIR.sh

```
# Searching Backdoor File
echo "Start Searching ..."
grep -RPn "(passthru|shell_exec|system|phpinfo|base64_decode|chmod|mkdir|fopen|fclose|fclose|readfile) *\(" /home/ > $dir/21.Backdoor-Homedir-$1.txt
grep -RPn "(passthru|shell_exec|system|phpinfo|base64_decode|chmod|mkdir|fopen|fclose|fclose|readfile) *\(" /var/www/ > $dir/22.Backdoor-VarWWWdir-$1.txt

# Searching others malicious activity
grep -Rinw /home -e "slot" -e "gacor" -e "maxwin" -e "thailand" -e "sigmaslot" -e "zeus" -e "cuan" > $dir/23.ListSlot-$1.txt
echo "Finish Searching.\n"

# Create Compressed File
tar -czf Collection-$1.tar.gz UbuntuIR-$1
rm -rf UbuntuIR-$1

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

- Script ini secara berurutan melakukan pencarian pada direktori **/home** dan **/var/www** untuk mencari file yang mengandung fungsi PHP yang sering digunakan untuk eksekusi perintah shell atau operasi berbahaya lainnya, dan menyimpan hasilnya dalam file teks yang sesuai di direktori yang ditentukan.
- **grep -Rinw /home -e "slot" -e "gacor" -e "maxwin" -e "thailand" -e "sigmaslot" -e "zeus" -e "cuan" > $dir/23.ListSlot.txt**
  Mencari kata kunci terkait "slot", "gacor" dll di dalam semua file yg berada pada direktori /home.
- Jadi, secara keseluruhan, script ini membuat arsip dari direktori UbuntuIR dengan nama **Collection.tar.gz** menggunakan kompresi gzip, dan kemudian menghapus seluruh direktori UbuntuIR beserta isinya dari sistem setelah proses pengarsipan selesai

Implementasi

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

```
admin@ubuntu:~$ sudo su
[sudo] password for admin:
root@ubuntu:/home/admin# curl -sO https://raw.githubusercontent.com/adpermana/Incident-Response-Tools/
analisa/UbuntuIR.sh && sudo bash ./UbuntuIR.sh pemdaX
************************************************************
Automate Data Collection for Ubuntu Server Script v1.0
************************************************************
no crontab for root
no crontab for root
no crontab for daemon
no crontab for bin
no crontab for sys
no crontab for sync
no crontab for games
no crontab for man
no crontab for lp
no crontab for mail
no crontab for news
no crontab for uucp
no crontab for proxy
no crontab for www-data
no crontab for backup
no crontab for list
no crontab for irc
no crontab for gnats
no crontab for nobody
no crontab for systemd-timesync
no crontab for systemd-network
no crontab for systemd-resolve
no crontab for systemd-bus-proxy
no crontab for syslog
no crontab for _apt
no crontab for lxd
no crontab for messagebus
no crontab for uuidd
no crontab for dnsmasq
no crontab for sshd
no crontab for mysql
no crontab for postfix
no crontab for admin
no crontab for admiin
no crontab for ossec
Start Searching ...
grep: input file ‘/home/admin/UbuntuIR-pemdaX/21.Backdoor-Homedir-pemdaX.txt’ is also the output
grep: input file ‘/home/admin/UbuntuIR-pemdaX/23.ListSlot-pemdaX.txt’ is also the output
Finish Searching.\n
************************************************************
Script Completed Succesfully, saved to ./Collection.tar.gz
************************************************************
```

Implementasi

Setelah selesai akan muncul folder : Collection-nama_instansi.tar.gz

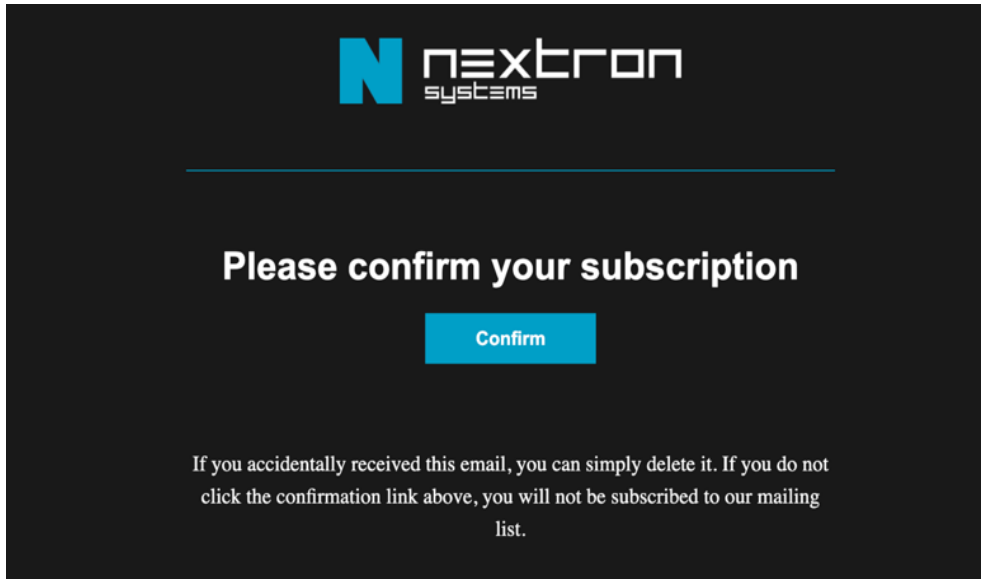
```
# tar –xvf Collection-nama_instansi.tar.gz
# cd UbuntuIR
# ls -al
```

```
root@ubuntu:/home/admin# cd UbuntuIR-pemdaX/
root@ubuntu:/home/admin/UbuntuIR-pemdaX# ls -al
total 552
drwxr-xr-x 2 root  root    4096 Nov 21 18:24 .
drwxr-xr-x 7 admin admin   4096 Nov 21 18:45 ..
-rw-r--r-- 1 root  root      29 Nov 21 18:24 0.DateTime-pemdaX.txt
-rw-r--r-- 1 root  root     100 Nov 21 18:24 10.Established_Conn-pemdaX.txt
-rw-r--r-- 1 root  root     285 Nov 21 18:24 11.Connected_to_PC-pemdaX.txt
-rw-r--r-- 1 root  root     220 Nov 21 18:24 12.DNS-pemdaX.txt
-rw-r--r-- 1 root  root       7 Nov 21 18:24 13.Hostname-pemdaX.txt
-rw-r--r-- 1 root  root     186 Nov 21 18:24 14.Hosts-pemdaX.txt
-rw-r--r-- 1 root  root    1793 Nov 21 18:24 15.Daftar_User-pemdaX.txt
-rw-r--r-- 1 root  root     165 Nov 21 18:24 16.Daftar_User_Bash-pemdaX.txt
-rw-r--r-- 1 root  root    2226 Nov 21 18:24 17.Lastlog-pemdaX.txt
-rw-r--r-- 1 root  root    5030 Nov 21 18:24 18.Last-pemdaX.txt
-rw-r--r-- 1 root  root  348266 Nov 21 18:24 19.Homedir-pemdaX.txt
-rw-r--r-- 1 root  root     107 Nov 21 18:24 1.Versi_Kernel-pemdaX.txt
-rw-r--r-- 1 root  root   89142 Nov 21 18:24 20.VarWWWdir-pemdaX.txt
-rw-r--r-- 1 root  root     500 Nov 21 18:24 21.Backdoor-Homedir-pemdaX.txt
-rw-r--r-- 1 root  root    3919 Nov 21 18:24 22.Backdoor-VarWWWdir-pemdaX.txt
-rw-r--r-- 1 root  root     598 Nov 21 18:24 23.ListSlot-pemdaX.txt
-rw-r--r-- 1 root  root     105 Nov 21 18:24 2.Versi_OS-pemdaX.txt
-rw-r--r-- 1 root  root    9885 Nov 21 18:24 3.Daftar_Proses-pemdaX.txt
-rw-r--r-- 1 root  root    9344 Nov 21 18:24 4.Daftar_Running_App-pemdaX.txt
-rw-r--r-- 1 root  root    1976 Nov 21 18:24 5.History-pemdaX.txt
-rw-r--r-- 1 root  root    1952 Nov 21 18:24 6.Cron-pemdaX.txt
-rw-r--r-- 1 root  root     101 Nov 21 18:24 7-1.Crontab-pemdaX.txt
-rw-r--r-- 1 root  root     957 Nov 21 18:24 7-2.Crontab-pemdaX.txt
-rw-r--r-- 1 root  root       0 Nov 21 18:24 7.Crontab-pemdaX.txt
-rw-r--r-- 1 root  root     819 Nov 21 18:24 8.Inbound-pemdaX.txt
-rw-r--r-- 1 root  root    1124 Nov 21 18:24 9.Outbound-pemdaX.txt
```

Tools Malware / Backdoor Scanner (Thor-Lite)

Definisi

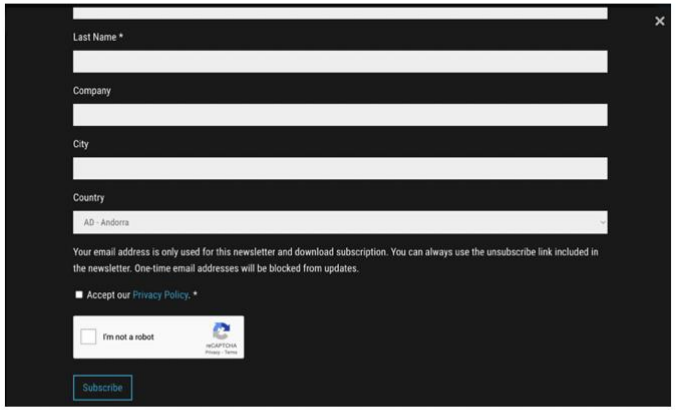
Thor-Lite, merupakan sebuah aplikasi pendeteksian portable untuk mendeteksi aktivitas mencurigakan pada sistem yang disusupi. Thor Scanner dapat mendeteki secara mendalam sampai local event log, registry, dan file system. Thor Scanner dapat menjadi system pendeteksi bagi aktivitas berbahaya yang terlewat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



Instalasi dan Konfigurasi

a) Registrasi User

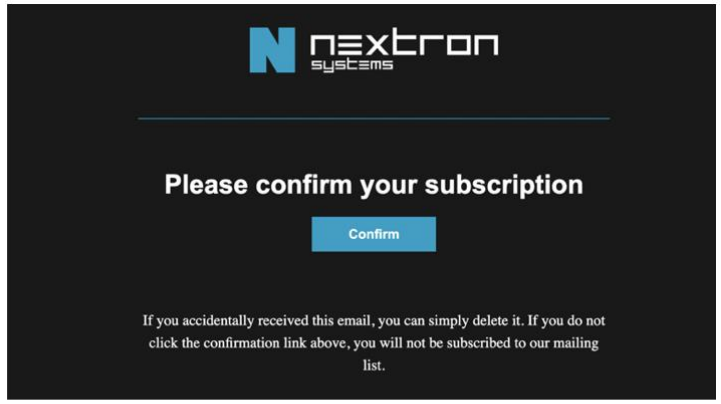
Lakukan registrasi user dengan melakukan akses ke alamat https://www.nextron-systems.com/thor-lite/#get-thor dan klik "Download THOR Lite" maka akan dilanjut ke page Registrasi seperti berikut :



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

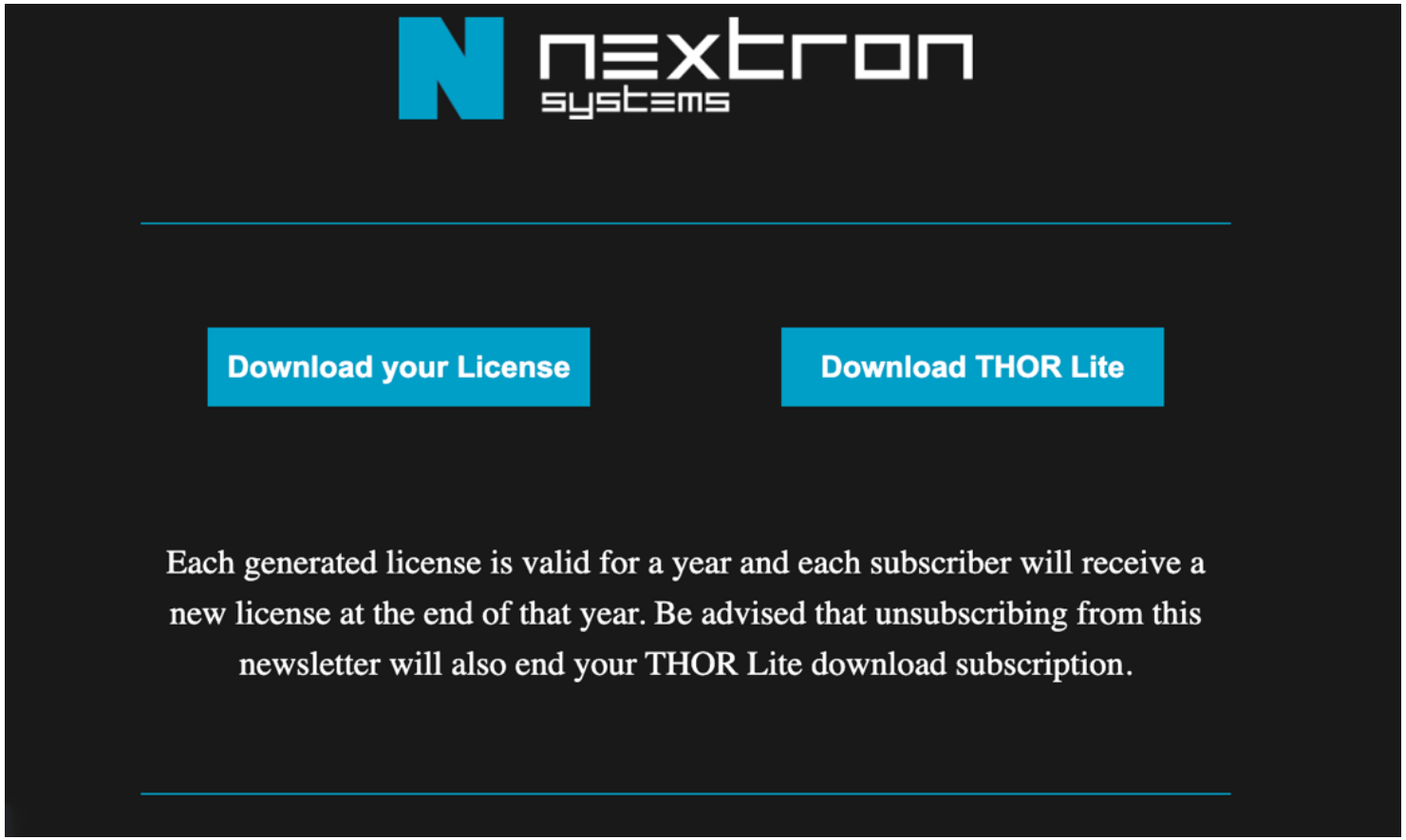
b) Unduh lisensi dan aplikasi

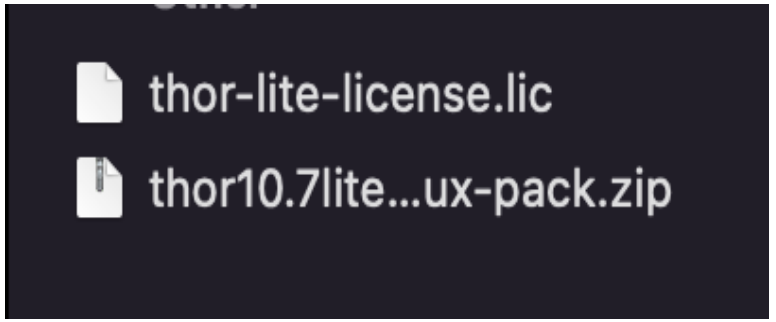
Setelah melakukan subscribe, tunggu beberapa saat dan akan muncul notifikasi pada email yang telah diregistrasi sebelumnya. Dan buka notifikasi tersebut akan muncul email sebagai berikut :



Lanjutkan dengan klik "Confirm" dan akan muncul kembali notifikasi email

Instalasi dan Konfigurasi





Implementasi

Unduh file Thor yang sudah teregistrasi BSSN :

$ sudo su

git clone https://github.com/adpermana/Thor-2

```
root@ubuntu:/home/admin# git clone https://github.com/adpermana/Thor-2
Cloning into 'Thor-2'...
remote: Enumerating objects: 13098, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 13098 (delta 0), reused 3 (delta 0), pack-reused 13095 (from 1)
Receiving objects: 100% (13098/13098), 92.37 MiB | 5.58 MiB/s, done.
Resolving deltas: 100% (6336/6336), done.
Checking connectivity... done.
```

Excutable pada command line Thor Lite

chmod +x thor-lite-linux

```
root@ubuntu:/home/admin/Thor-2# chmod +x thor-lite-linux
root@ubuntu:/home/admin/Thor-2# ls
changes.log       signatures                                  thor-lite-linux-64.sig
config            thor-lite270624.zip                         thor-lite-linux.sig
custom-signatures thor-lite-fcf1a639-d49c65a2-20240620-20241221.lic thor-lite-util
docs              thor-lite-linux                             thor-lite-util.sig
insidentil.sh     thor-lite-linux-64                          tools
```

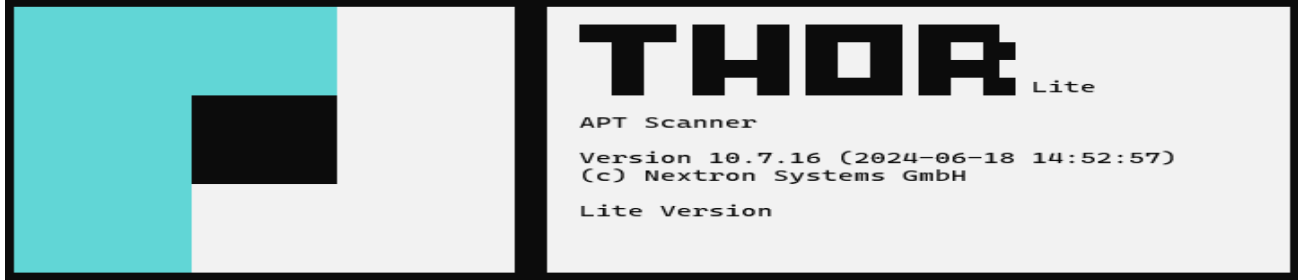
Terdapat penambahan YARA rules signature di dalam tools Thor Lite tersebut

Implementasi

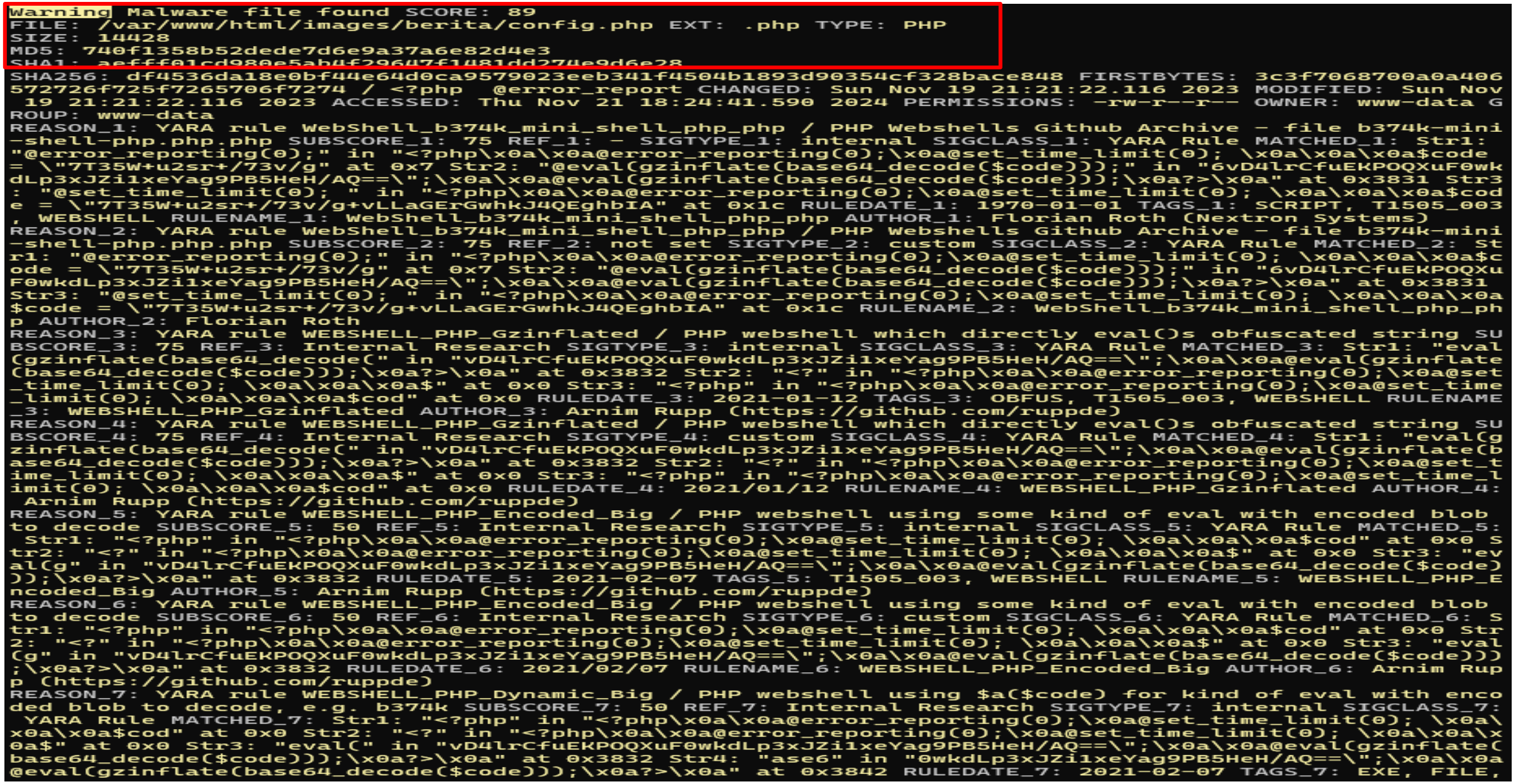
Jalankan perintah :

./thor-lite-linux -a Filescan --intense –norescontrol --cross-platform --alldrives -p /var/www/html/

```
root@ubuntu:/home/admin/Thor-2# ./thor-lite-linux -a Filescan --intense -norescontrol --cross-platform
 --alldrives -p /var/www/html/
Notice Some modules and features are not available in Lite version and will be disabled
Notice This THOR Lite license permits non-commercial use only. It is strictly prohibited to sell THOR
Lite or sell services that include the use of THOR Lite. For details, see the EULA in the ./docs folde
r. For a special license that covers these cases, allows Sigma scanning and suppresses this message, p
lease contact our sales via https://www.nextron-systems.com/get-started/
```




```
> Scan Information
Info Thor Version: 10.7.16
Info Thor Build: 0c84255d1499 (2024-06-18 14:52:57)
Info Run on system: ubuntu
Info Running as user: root
Info User has admin rights: yes
Info Working Directory: /home/admin/Thor-2
Warning 32 bit THOR was executed on 64 bit system. For improved results, use the 64 bit version of THO
R.
Info Thor Scan started START_TIME: Thu Nov 21 18:33:54 2024 HOSTNAME: ubuntu
Warning Fixed typical THOR flag error REPLACED: -norescontrol WITH: --norescontrol
Info Effective argument list: [--path /var/www/html/ --alldrives --cross-platform --intense --norescon
trol --module Filescan]
Info Platform: Ubuntu 16.04.4 LTS
Info Platform DeepEval NAME: Ubuntu 16.04.4 LTS KERNEL_NAME: Linux  KERNEL_VERSION: 4.4.0-116-generic
 PROC: x86_64  ARCH: x86_64
Info Language: en_US, Zone: WIB
Info System Uptime: 0.01 days
Info CPU Count: 1
Info Memory in Megabyte: 992
Info Signature Database: 2024/06/21-152349
Info Successfully compiled 0 false positive filters TYPE: log filter
Info Writing report file to: ubuntu_thor_2024-11-21_1833.txt
Info Writing csv report file to: ubuntu_files_md5s.csv
Info No json report file will be written
Info Writing html report file to: ubuntu_thor_2024-11-21_1833.html
Info Syslog Export: off
Info IP Address 1: 192.168.2.238
Info ScanID: S-BEJu6w3iH9M
Info System is not a domain controller
Info Intense Scan Mode
Info Max. file size to be scanned is 209.7 MB, use --max_file_size to increase the limit
Info Selected modules: Filescan
Info Deselected modules: Artifact-Collector, Autoruns, Cron, DeepDive, Dropzone, EnvCheck, Firewall, H
osts, Integritycheck, LoggedIn, ProcessCheck, Rootkit, ServiceCheck, Thunderstorm, Timestomp, UserDir,
 Users
```


Warning Malware file found SCORE: 89
FILE: /var/www/html/images/berita/config.php EXT: .php TYPE: PHP
SIZE: 14428
MD5: 740f1358b52dede7d6e9a37a6e82d4e3
SHA1: aefff01cd980e5ab4f29647f1481dd274e9d6e28
SHA256: df4536da18e0bf44e64d0ca9579023eeb341f4504b1893d90354cf328bace848 FIRSTBYTES: 3c3f7068700a0a406
572726f725f7265706f7274 / <?php @error_report CHANGED: Sun Nov 19 21:21:22.116 2023 MODIFIED: Sun Nov
19 21:21:22.116 2023 ACCESSED: Thu Nov 21 18:24:41.590 2024 PERMISSIONS: -rw-r--r-- OWNER: www-data G
ROUP: www-data
REASON_1: YARA rule WebShell_b374k_mini_shell_php_php / PHP Webshells Github Archive - file b374k-mini
-shell-php.php.php SUBSCORE_1: 75 REF_1: - SIGTYPE_1: internal SIGCLASS_1: YARA Rule MATCHED_1: Str1:
"@error_reporting(0);" in "<?php\x0a\x0a@error_reporting(0);\x0a@set_time_limit(0); \x0a\x0a\x0a$code
= \"7T35W+u2sr+/73v/g" at 0x7 Str2: "@eval(gzinflate(base64_decode($code)));" in "6vD4lrCfuEKPOQXuF0wk
dLp3xJZi1xeYag9PB5HeH/AQ==\";\x0a\x0a@eval(gzinflate(base64_decode($code)));\x0a?>\x0a" at 0x3831 Str3
: "@set_time_limit(0); " in "<?php\x0a\x0a@error_reporting(0);\x0a@set_time_limit(0); \x0a\x0a\x0a$cod
e = \"7T35W+u2sr+/73v/g+vLLaGErGwhkJ4QEghbIA" at 0x1c RULEDATE_1: 1970-01-01 TAGS_1: SCRIPT, T1505_003
, WEBSHELL RULENAME_1: WebShell_b374k_mini_shell_php_php AUTHOR_1: Florian Roth (Nextron Systems)
REASON_2: YARA rule WebShell_b374k_mini_shell_php_php / PHP Webshells Github Archive - file b374k-mini
-shell-php.php.php SUBSCORE_2: 75 REF_2: not set SIGTYPE_2: custom SIGCLASS_2: YARA Rule MATCHED_2: St
r1: "@error_reporting(0);" in "<?php\x0a\x0a@error_reporting(0);\x0a@set_time_limit(0); \x0a\x0a\x0a$c
ode = \"7T35W+u2sr+/73v/g" at 0x7 Str2: "@eval(gzinflate(base64_decode($code)));" in "6vD4lrCfuEKPOQXu
F0wkdLp3xJZi1xeYag9PB5HeH/AQ==\";\x0a\x0a@eval(gzinflate(base64_decode($code)));\x0a?>\x0a" at 0x3831
Str3: "@set_time_limit(0); " in "<?php\x0a\x0a@error_reporting(0);\x0a@set_time_limit(0); \x0a\x0a\x0a
$code = \"7T35W+u2sr+/73v/g+vLLaGErGwhkJ4QEghbIA" at 0x1c RULENAME_2: WebShell_b374k_mini_shell_php_ph
p AUTHOR_2: Florian Roth
REASON_3: YARA rule WEBSHELL_PHP_Gzinflated / PHP webshell which directly eval()s obfuscated string SU
BSCORE_3: 75 REF_3: Internal Research SIGTYPE_3: internal SIGCLASS_3: YARA Rule MATCHED_3: Str1: "eval
(gzinflate(base64_decode(" in "vD4lrCfuEKPOQXuF0wkdLp3xJZi1xeYag9PB5HeH/AQ==\";\x0a\x0a@eval(gzinflate
(base64_decode($code)));\x0a?>\x0a" at 0x3832 Str2: "<?" in "<?php\x0a\x0a@error_reporting(0);\x0a@set
_time_limit(0); \x0a\x0a\x0a$" at 0x0 Str3: "<?php" in "<?php\x0a\x0a@error_reporting(0);\x0a@set_time
_limit(0); \x0a\x0a\x0a$cod" at 0x0 RULEDATE_3: 2021-01-12 TAGS_3: OBFUS, T1505_003, WEBSHELL RULENAME
_3: WEBSHELL_PHP_Gzinflated AUTHOR_3: Arnim Rupp (https://github.com/ruppde)
REASON_4: YARA rule WEBSHELL_PHP_Gzinflated / PHP webshell which directly eval()s obfuscated string SU
BSCORE_4: 75 REF_4: Internal Research SIGTYPE_4: custom SIGCLASS_4: YARA Rule MATCHED_4: Str1: "eval(g
zinflate(base64_decode(" in "vD4lrCfuEKPOQXuF0wkdLp3xJZi1xeYag9PB5HeH/AQ==\";\x0a\x0a@eval(gzinflate(b
ase64_decode($code)));\x0a?>\x0a" at 0x3832 Str2: "<?" in "<?php\x0a\x0a@error_reporting(0);\x0a@set_t
ime_limit(0); \x0a\x0a\x0a$" at 0x0 Str3: "<?php" in "<?php\x0a\x0a@error_reporting(0);\x0a@set_time_l
imit(0); \x0a\x0a\x0a$cod" at 0x0 RULEDATE_4: 2021/01/12 RULENAME_4: WEBSHELL_PHP_Gzinflated AUTHOR_4:
Arnim Rupp (https://github.com/ruppde)
REASON_5: YARA rule WEBSHELL_PHP_Encoded_Big / PHP webshell using some kind of eval with encoded blob
to decode SUBSCORE_5: 50 REF_5: Internal Research SIGTYPE_5: internal SIGCLASS_5: YARA Rule MATCHED_5:
Str1: "<?php" in "<?php\x0a\x0a@error_reporting(0);\x0a@set_time_limit(0); \x0a\x0a\x0a$cod" at 0x0 S
tr2: "<?" in "<?php\x0a\x0a@error_reporting(0);\x0a@set_time_limit(0); \x0a\x0a\x0a$" at 0x0 Str3: "ev
al(g" in "vD4lrCfuEKPOQXuF0wkdLp3xJZi1xeYag9PB5HeH/AQ==\";\x0a\x0a@eval(gzinflate(base64_decode($code)
));\x0a?>\x0a" at 0x3832 RULEDATE_5: 2021-02-07 TAGS_5: T1505_003, WEBSHELL RULENAME_5: WEBSHELL_PHP_E
ncoded_Big AUTHOR_5: Arnim Rupp (https://github.com/ruppde)
REASON_6: YARA rule WEBSHELL_PHP_Encoded_Big / PHP webshell using some kind of eval with encoded blob
to decode SUBSCORE_6: 50 REF_6: Internal Research SIGTYPE_6: custom SIGCLASS_6: YARA Rule MATCHED_6: S
tr1: "<?php" in "<?php\x0a\x0a@error_reporting(0);\x0a@set_time_limit(0); \x0a\x0a\x0a$cod" at 0x0 Str
2: "<?" in "<?php\x0a\x0a@error_reporting(0);\x0a@set_time_limit(0); \x0a\x0a\x0a$" at 0x0 Str3: "eval
(g" in "vD4lrCfuEKPOQXuF0wkdLp3xJZi1xeYag9PB5HeH/AQ==\";\x0a\x0a@eval(gzinflate(base64_decode($code)))
;\x0a?>\x0a" at 0x3832 RULEDATE_6: 2021/02/07 RULENAME_6: WEBSHELL_PHP_Encoded_Big AUTHOR_6: Arnim Rup
p (https://github.com/ruppde)
REASON_7: YARA rule WEBSHELL_PHP_Dynamic_Big / PHP webshell using $a($code) for kind of eval with enco
ded blob to decode, e.g. b374k SUBSCORE_7: 50 REF_7: Internal Research SIGTYPE_7: internal SIGCLASS_7:
YARA Rule MATCHED_7: Str1: "<?php" in "<?php\x0a\x0a@error_reporting(0);\x0a@set_time_limit(0); \x0a\
x0a\x0a$cod" at 0x0 Str2: "<?" in "<?php\x0a\x0a@error_reporting(0);\x0a@set_time_limit(0); \x0a\x0a\x
0a$" at 0x0 Str3: "eval(" in "vD4lrCfuEKPOQXuF0wkdLp3xJZi1xeYag9PB5HeH/AQ==\";\x0a\x0a@eval(gzinflate(
base64_decode($code)));\x0a?>\x0a" at 0x3832 Str4: "ase6" in "0wkdLp3xJZi1xeYag9PB5HeH/AQ==\";\x0a\x0a
@eval(gzinflate(base64_decode($code)));\x0a?>\x0a" at 0x3842 RULEDATE_7: 2021-02-07 TAGS_7: EXE, FILE,

Output .html

THOR Scan Report

This THOR Lite license permits non-commercial use only. It is strictly prohibited to sell THOR Lite or sell services that include the use of THOR Lite. For details, see the EULA in the ./docs folder. For a special license that covers these cases, allows Sigma scanning and suppresses this message, please contact our sales via https://www.nextron-systems.com/get-started/

Scan Information	
Scanner	Thor
Version	10.7.16
Run on System	ubuntu
Argument list	--path /var/www/html/ --alldrives --cross-platform --intense --norescontrol --module Filescan
Signature Database	2024/06/21-152349
Start Time	Thu Nov 21 14:44:57 2024
End Time	Thu Nov 21 14:45:06 2024
IP Addresses	192.168.17.140
Run as user	root
Admin rights	yes
Platform	Ubuntu 16.04.4 LTS
Log File Name	ubuntu_thor_2024-11-21_1444.txt
False Positive Filters Applied	0
Scan ID	S-J5jCLi1B0cU

Modules	
Filescan	1

Statistics	
Alerts	0
Warnings	3
Notice	3
Info	483
Errors	0

Help	
Shortcuts	Use Ctrl+↑ (Windows/Linux) or ⌘+↑ (macOS) to return to the top of the page
Filters	You can provide a file (--filter file) with regular expressions to suppress false positives
Hint 1	Select text and use the context menu to filter / select / lookup strings
Hint 2	Click on a module to filter for all events from that module.

Errors

Alerts

Warnings

Warning 1	*Nov 21 07:44:46 ubuntu/192.168.17.140* **MODULE:** Startup **MESSAGE:** 32 bit THOR was executed on 64 bit system. For improved results, use the 64 bit version of THOR.
Warning 2	*Nov 21 07:44:46 ubuntu/192.168.17.140* **MODULE:** Startup **MESSAGE:** Fixed typical THOR flag error **REPLACED:** -norescontrol **WITH:** --norescontrol

No filters applied

Tools Audit TI (Lynis dan LinPEAS)

AUDIT TI

Dalam melakukan Audit, perlu memetakan seluruh kemungkinan celah kerawanan yang dapat diexploitasi. Untuk memetakannya, ada beberapa tools yang dapat digunakan. Salah satu tool yaitu "Lynis" dan "LinPEAS"

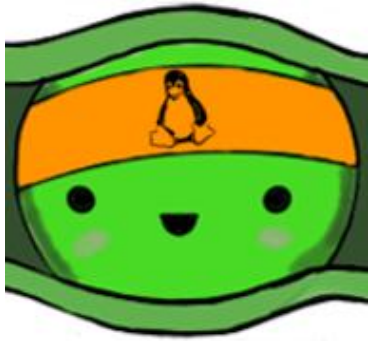
Lynis merupakan sebuah tool (open-source) yang dapat digunakan untuk melakukan audit dan hardening pada sebuah Sistem Operasi Unix (Linux)

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

CISOFY
AUDITING-HARDENING-COMPLIANCE

Lynis

Ref : https://cisofy.com/lynis/



LinPEAS

Ref : https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS

Implementasi

Untuk melakukan instalasi dan konfigurasi jalankan perintah berikut :

$ sudo su

git clone https://github.com/CISOfy/lynis

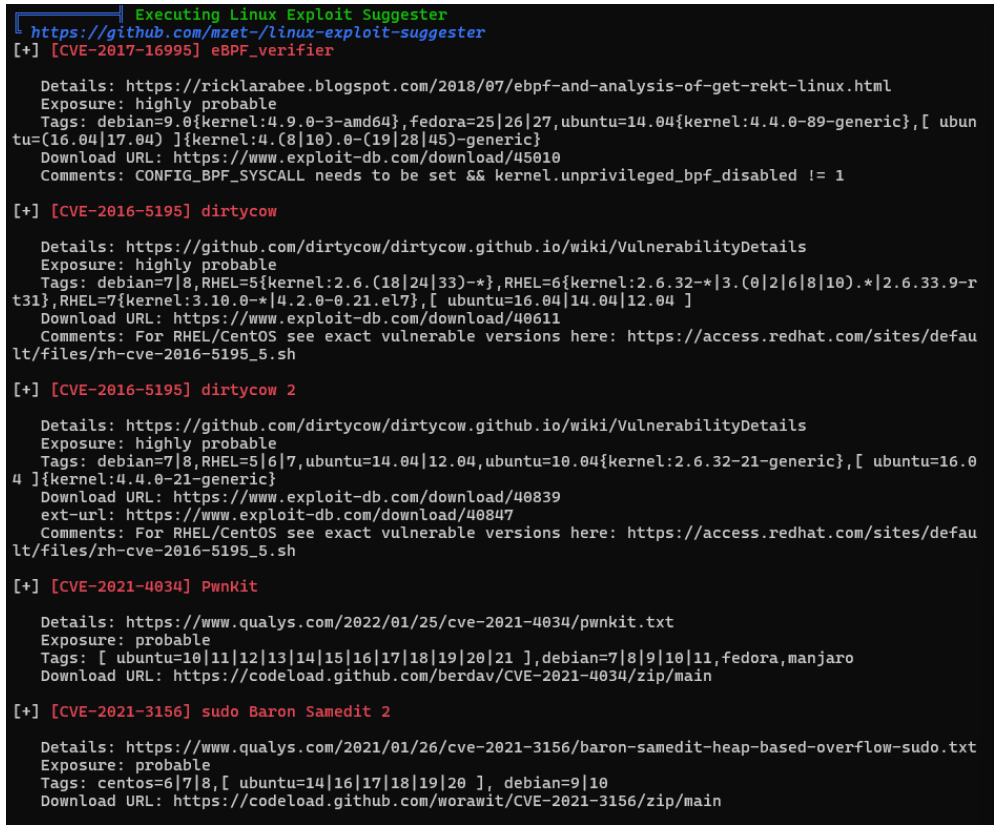
cd lynis

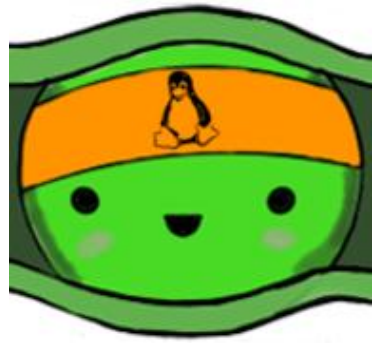
./lynis audit system

Implementasi

Untuk melakukan instalasi dan konfigurasi jalankan perintah berikut (tanpa masuk sudo su) :

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

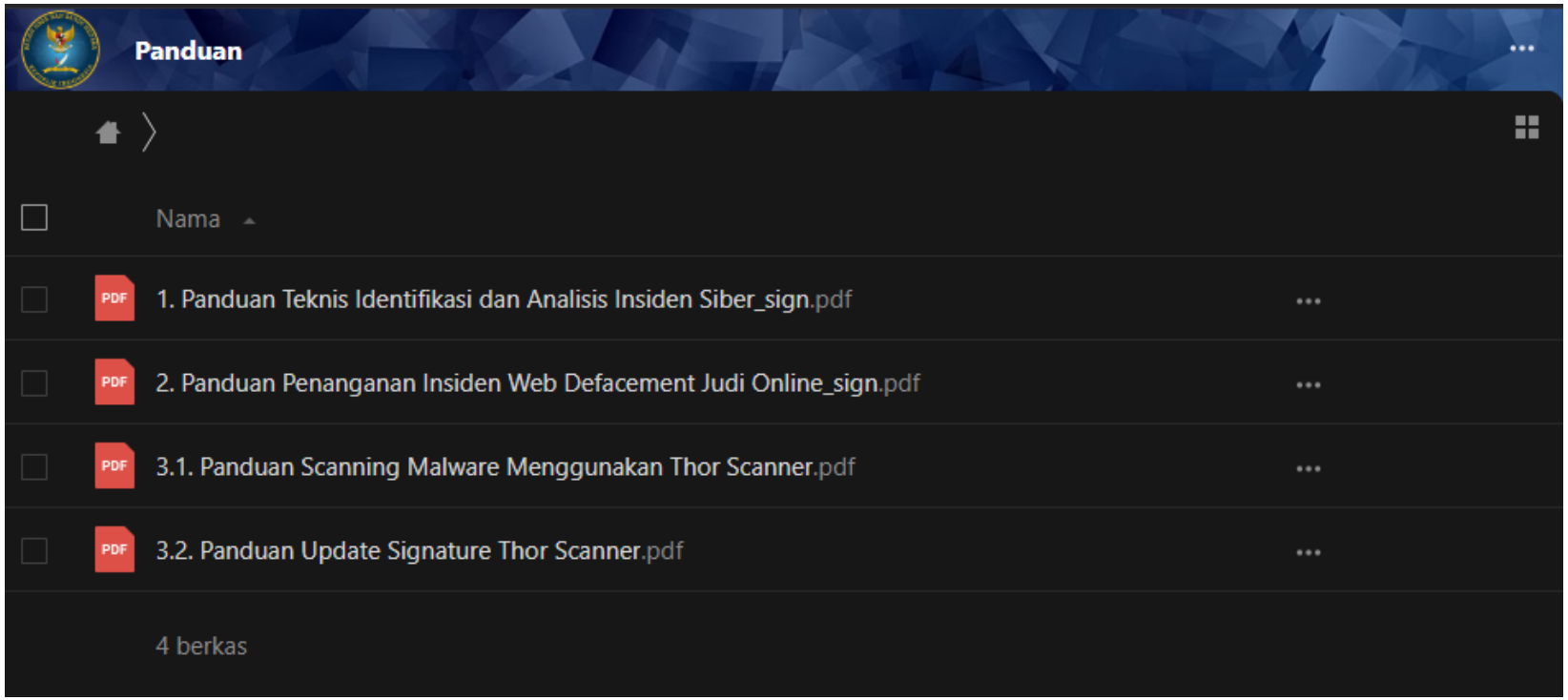




Panduan Teknis

Berikut link untuk mengakses panduan teknis

https://drive.bssn.go.id/index.php/s/2emmH7EKCSJqaJ4
pass : Panduan2024!.



SELESAI

BADAN SIBER DAN SANDI NEGARA
Jl. Harsono RM 70 Ragunan,
Pasar Minggu, Jakarta Selatan, 12550
Tel: +62217805814 Fax: +622178844104