LAPORAN PRAKTIKUM
KEAMANAN INFORMASI 1
UNIT 5 & 6

DI SUSUN OLEH:

Nama	: Bintang Nur K
NIM	: 21/481453/SV/19790
Kelas	: RI4AA
Hari, tanggal	: Selasa, 07 Maret 2023
Dosen Pengampu	: Anni Karimatul Fauziyyah, S.Kom., M.Eng
Asisten Praktikum	: Gabriella Alvera Chaterine

PROGRAM SARJANA TERAPAN (DIV)
TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023

UNIT 5 & 6
TEKNIK STEGANOGRAFI DAN ANALISIS LOG SERVER

I. TUJUAN

- Memahami dan mempraktikan steganografi
- Membaca File Log dengan Cat, More, Less, dan Tail
- Memahami File Log dan Syslog
- Memahami File Log dan Jurnalctl

II. LATAR BELAKANG

File Log adalah alat penting dalam pemecahan masalah dan pemantauan. Aplikasi yang berbeda menghasilkan file log yang berbeda, masing-masing berisi kumpulan bidang dan informasinya sendiri. Meskipun struktur bidang dapat berubah di antara file log, alat yang digunakan untuk membacanya sebagian besar sama. Di lab ini, Anda akan mempelajari tentang alat umum yang digunakan untuk membaca file log dan berlatih menggunakannya.

Steganografi adalah ilmu, teknik atau seni menyembunyikan pesan rahasia "*hiding message*" atau tulisan rahasia "*covered writing*" sehingga keberadaan pesan tidak terdeteksi orang lain kecuali pengirim dan penerima pesan tersebut. Steganografi berasal dari bahasa Yunani yaitu steganos "tersembunyi/ menyembunyikan" dan graphy "tulisan", sehingga secara lengkap bermakna tulisan yang disembunyikan.

III. ALAT DAN BAHAN

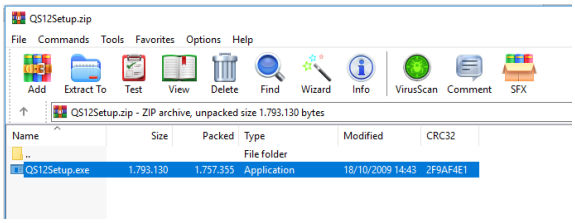
Alat dan Bahan yang dibutuhkan untuk melaksanakan praktikum adalah

- PC
- Koneksi internet
- *Software* Steganografi
- CyberOps Workstation VM

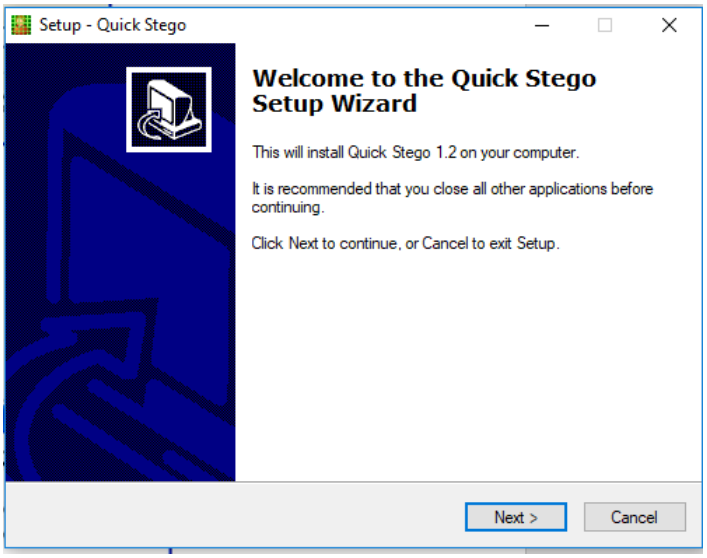
IV. LANGKAH KERJA DAN HASIL

Langkah kerja steganografi

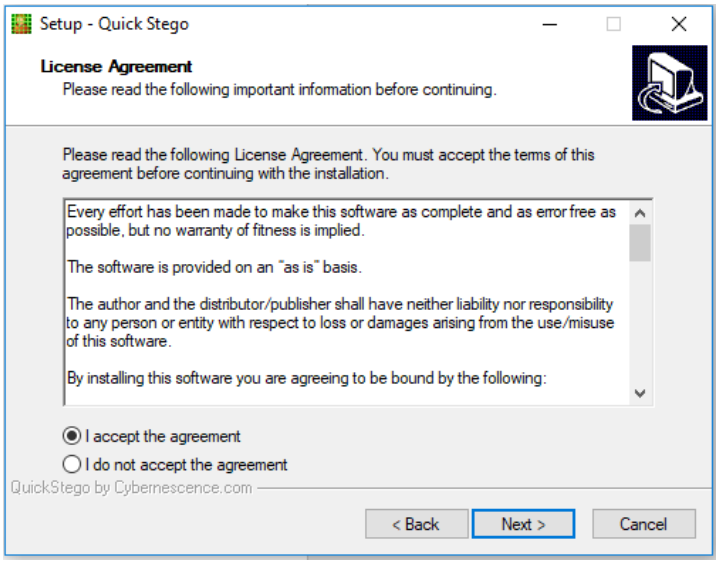
1. Buka windows



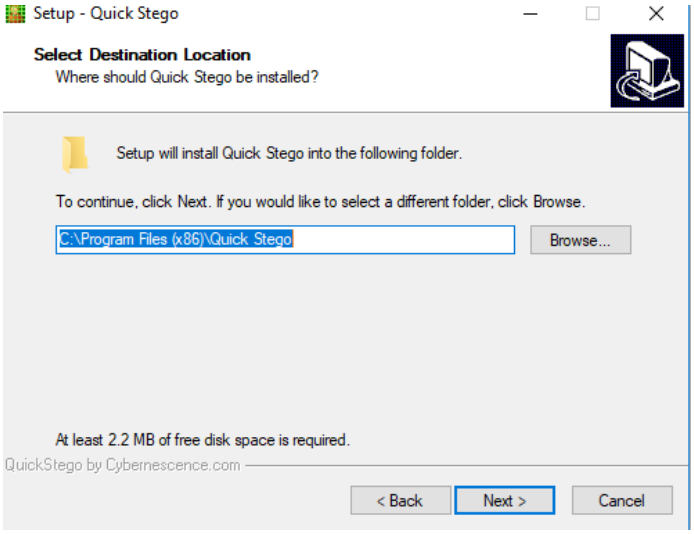
2. Instal quick stego



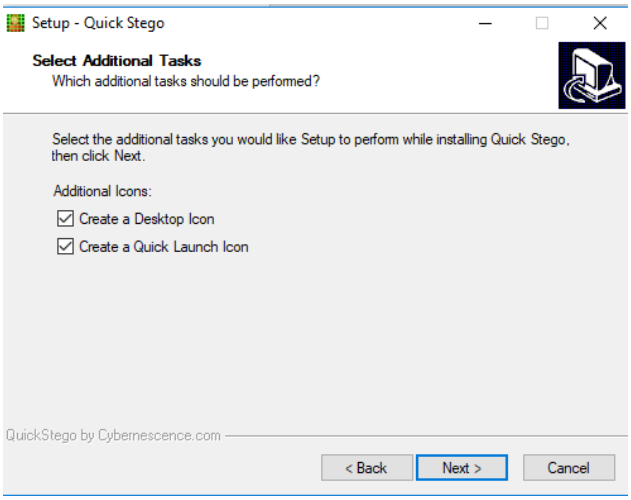
Pengaturan lisensi

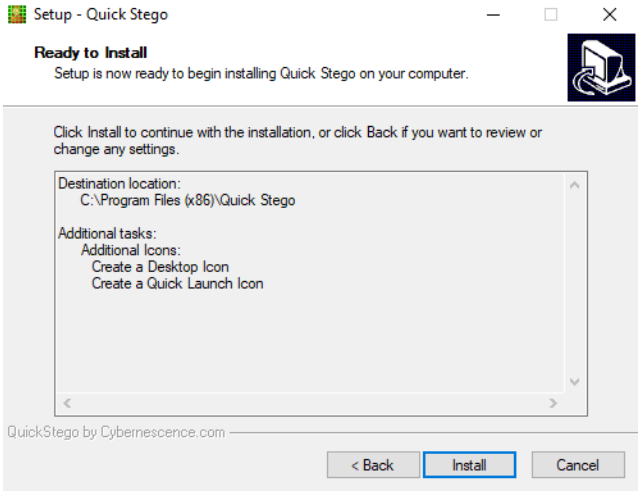


Pilih tujuan

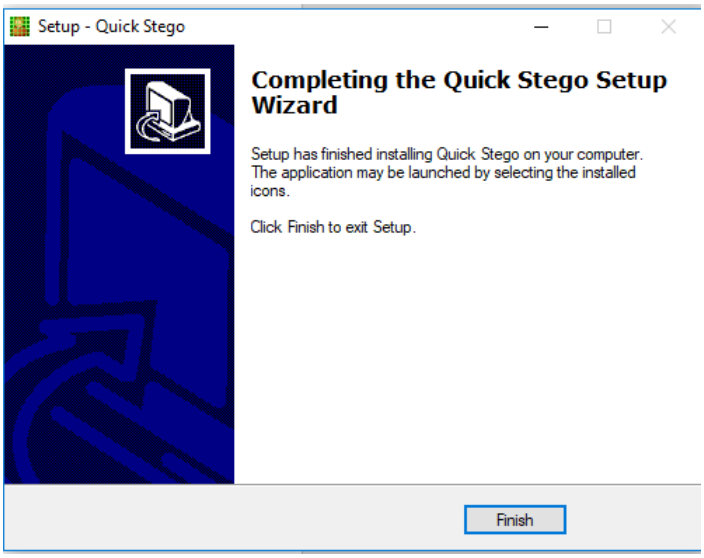


Pilih tugas tambahan, lalu klik siap instal





Maka penginstalan selesai dilakukan

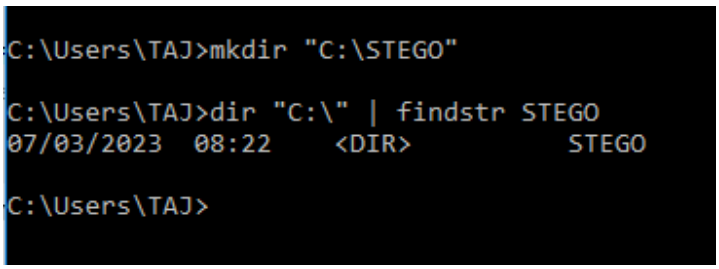


Buka Command Prompt

Buat Direktori STEGO

mkdir "C:\STEGO"

dir "C:\" | temukanstr STEGO

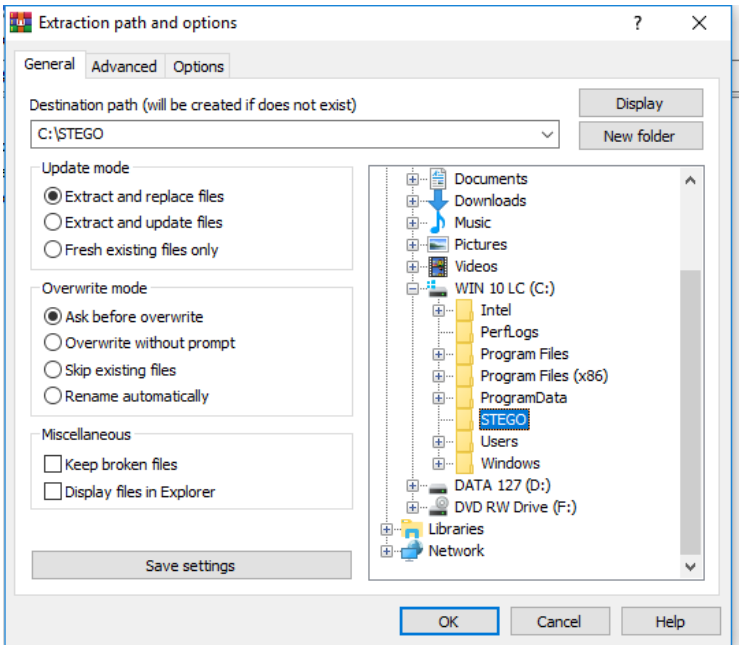


3. Install MD5SUMS

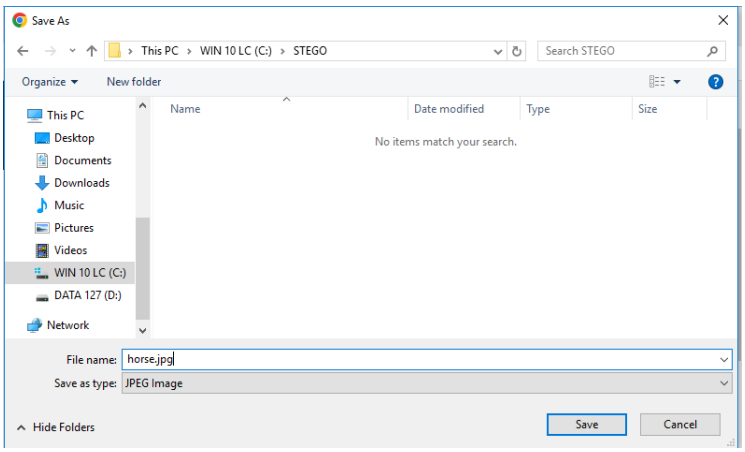
   Unduh md5sums-1.2, Arahkan ke URL berikut

   http://www.pc-tools.net/files/win32/freeware/md5sums-1.2.zip

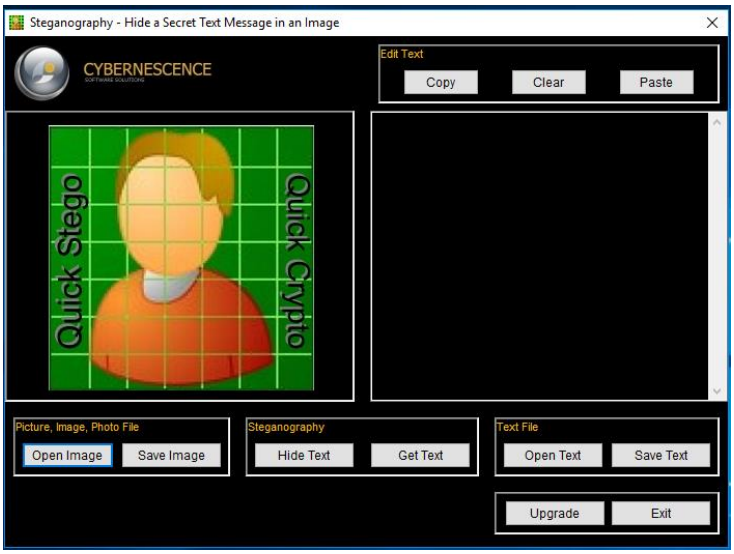
   Klik tombol Simpan File Radio dan klik OK



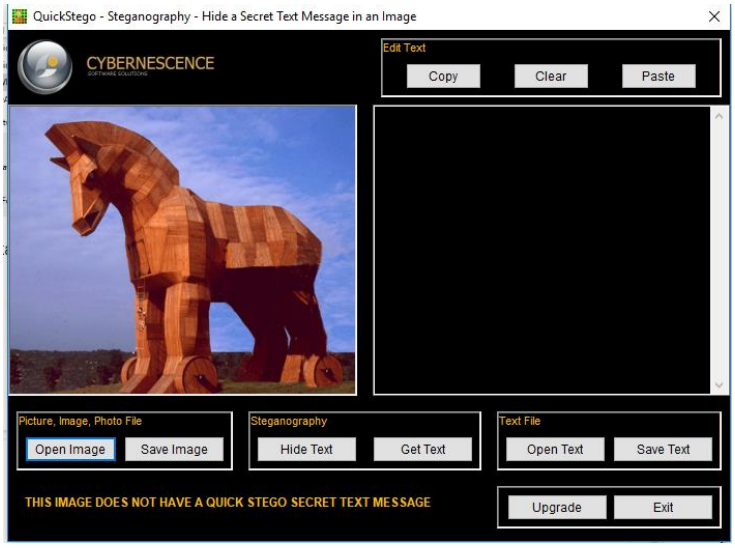
Beri nama dengan jenis file jpg



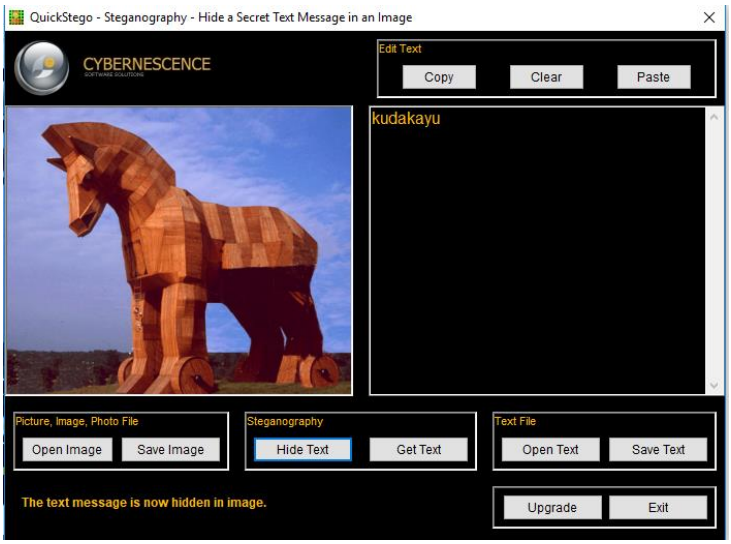
Jalankan Stego Cepat



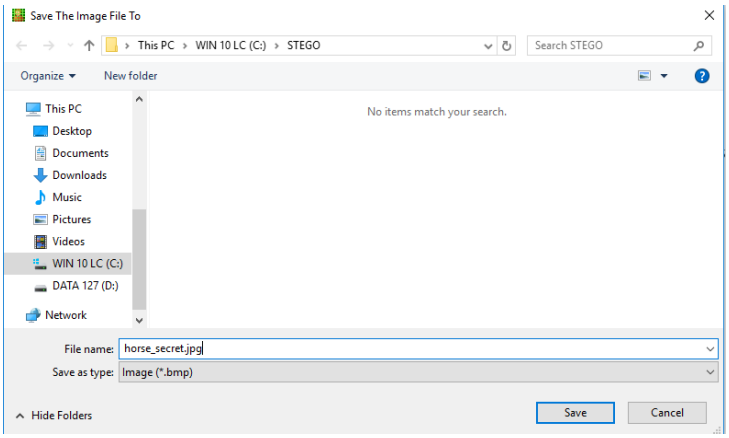
Masukkan gambar yang ingin diberi kata tersembunyi



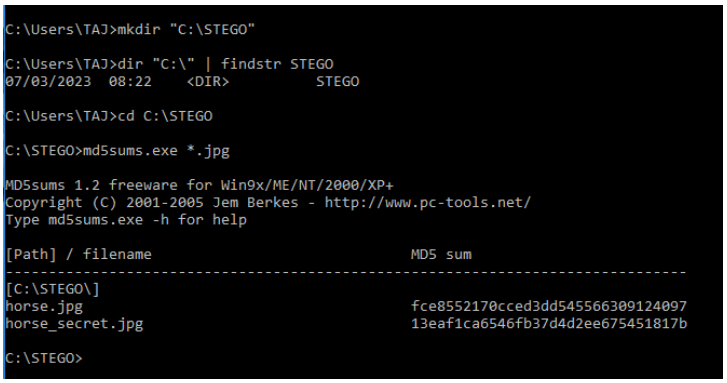
Sembunyikan Teks



Simpan gambar dengan nama file “horse_secret.jpg”



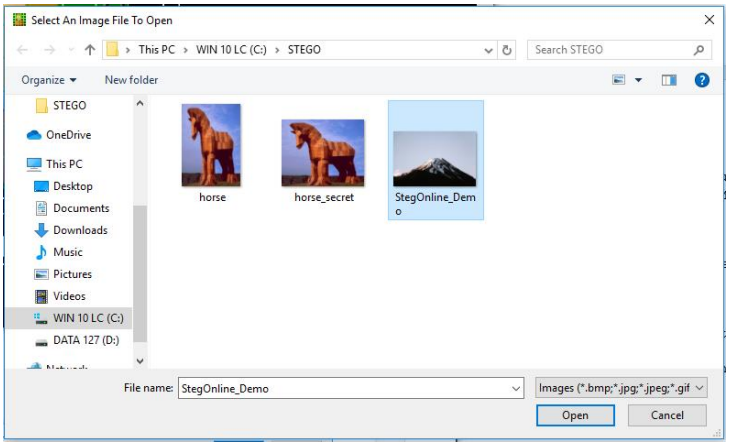
Buka Command Prompt



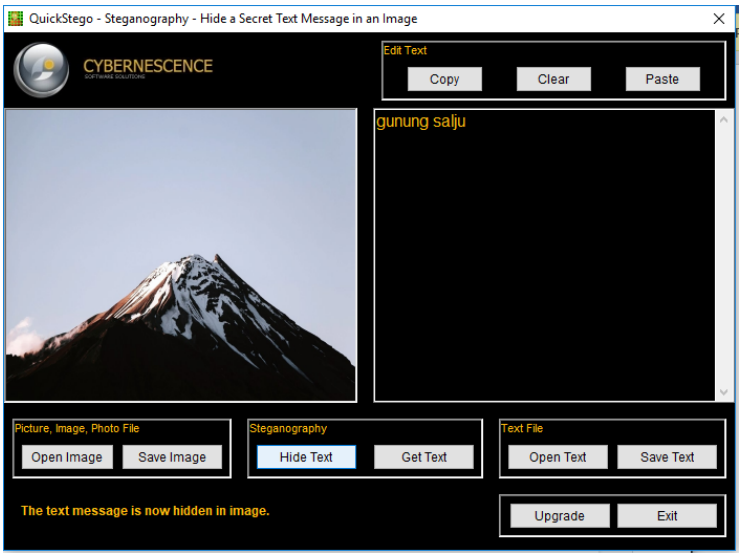
```
C:\Users\TAJ>mkdir "C:\STEGO"

C:\Users\TAJ>dir "C:\" | findstr STEGO
07/03/2023  08:22    <DIR>          STEGO

C:\Users\TAJ>cd C:\STEGO

C:\STEGO>md5sums.exe *.jpg

MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type md5sums.exe -h for help

[Path] / filename                                MD5 sum
-------------------------------------------------------------------------------
[C:\STEGO\]
horse.jpg                                        fce8552170cced3dd545566309124097
horse_secret.jpg                                 13eaf1ca6546fb37d4d2ee67545817b

C:\STEGO>
```

PADA GAMBAR 2

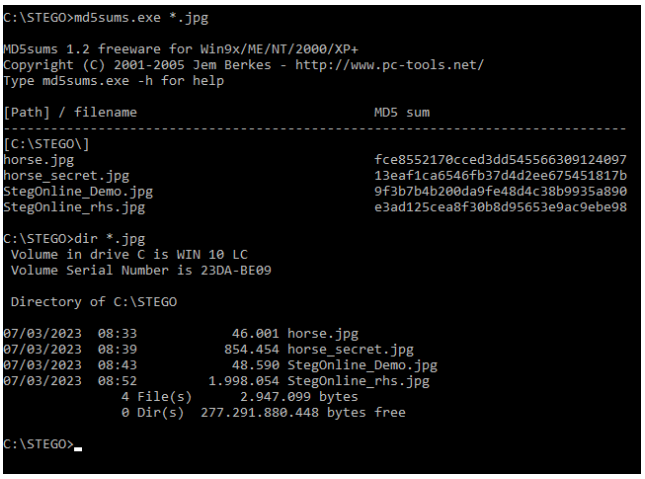
Ubah PNG to JPG terlebih dahulu, lalu pindahkan file ke STEGO



Masukkan hidden text



Buka command prompt

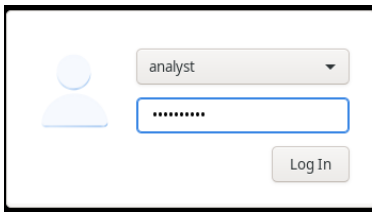


UNIT 6

Pembacaan Log Server

1. Membaca File Log dengan Cat, More, Less, dan Tail

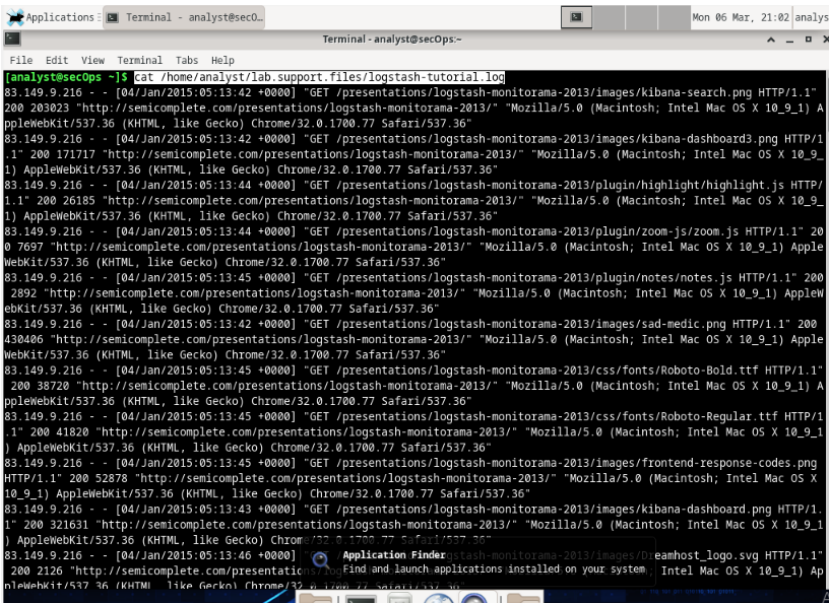
   Bukalah VM CyberOps Worstation dan jendela terminal



2. Dari jendela terminal, jalankan perintah di bawah ini untuk menampilkan konten file logstash-tutorial.log, yang terletak di folder /home/analyst/lab.support.files/:

   analis@secOps ~$ cat /home/analyst/lab.support.files/logstash-tutorial.log

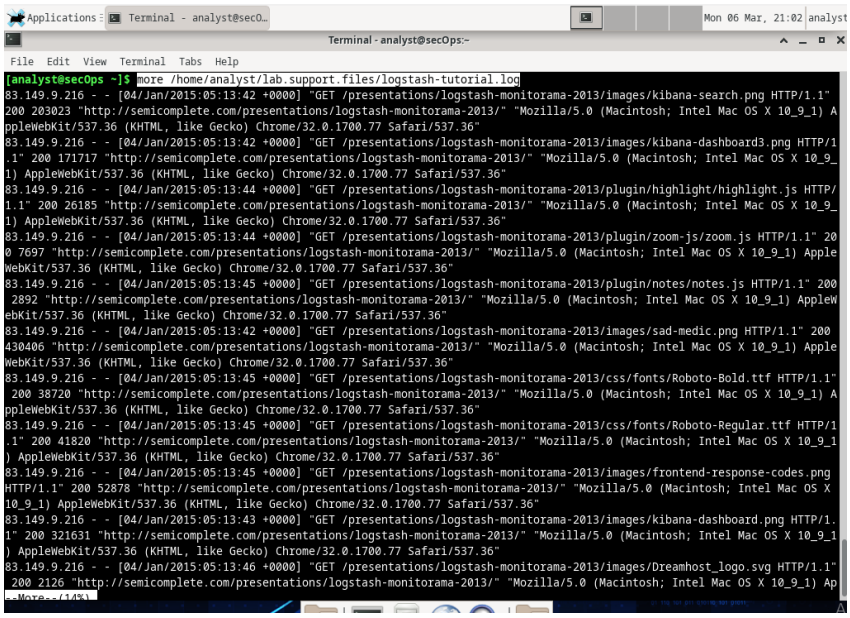
   Isi file harus ditampilkan melalui jendela terminal



3. Dari jendela terminal yang sama, gunakan perintah di bawah ini untuk menampilkan kembali isi file logstash-tutorial.log. Proses ini menggunakan more:

   analis@secOps ~$ more /home/analyst/lab.support.files/logstash-tutorial.log

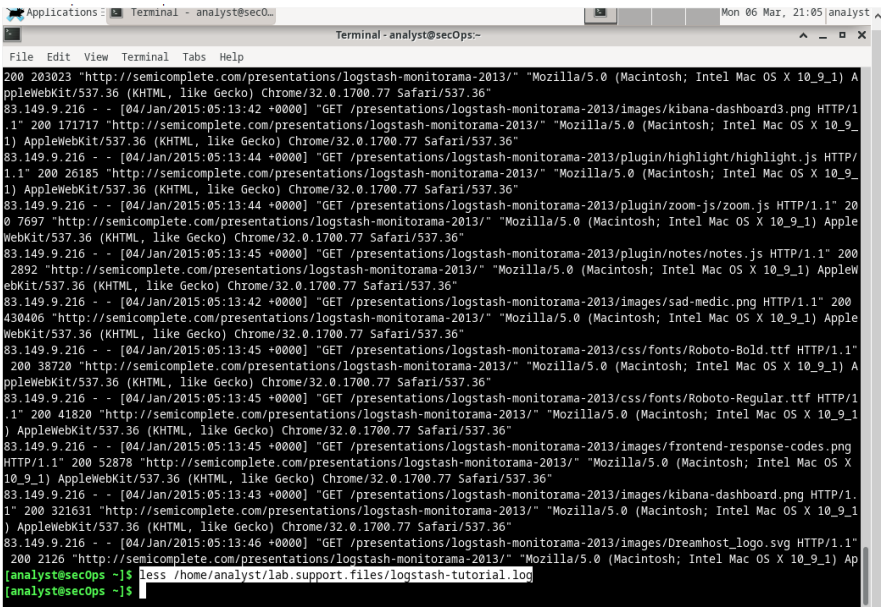
   Isi file harus ditampilkan melalui jendela terminal dan berhenti ketika satu halaman tersebut ditampilkan. Tekan spasi untuk berpindah ke halaman berikutnya. Tekan enter untuk menampilkan baris teks berikutnya

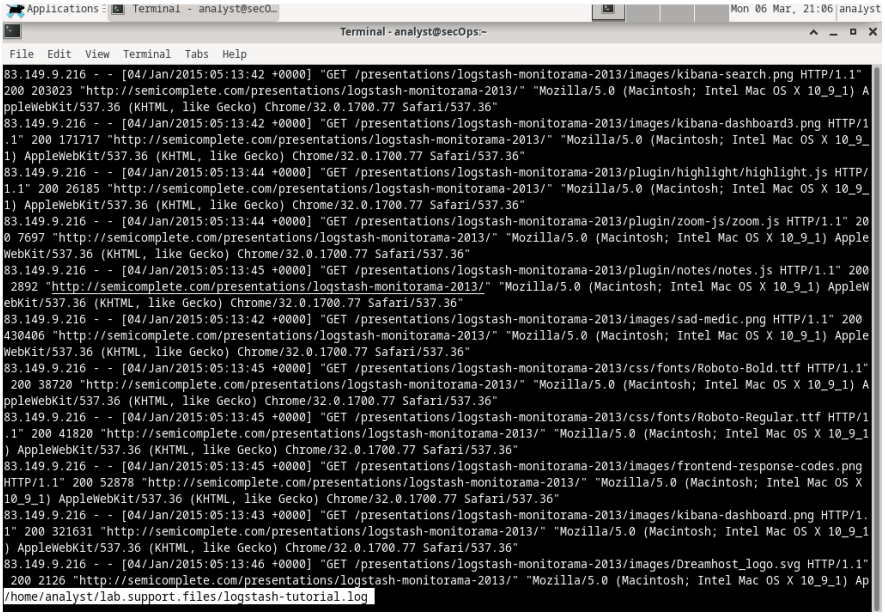


4. Dari tampilan terminal yang sama, gunakan less untuk menampilkan konten file logstashtutorial.log lagi:

   analis@secOps ~$ lebih sedikit /home/analyst/lab.support.files/logstash-tutorial.log

   Isi file harus menggulir melalui jendela terminal dan berhenti ketika satu halaman ditampilkan. Tekan spasi untuk maju ke halaman berikutnya. Tekan enter untuk menampilkan baris teks berikutnya. Gunakan tombol panah atas dan bawah untuk bergerak maju mundur melalui file teks. Gunakan tombol q pada keyboard untuk keluar.

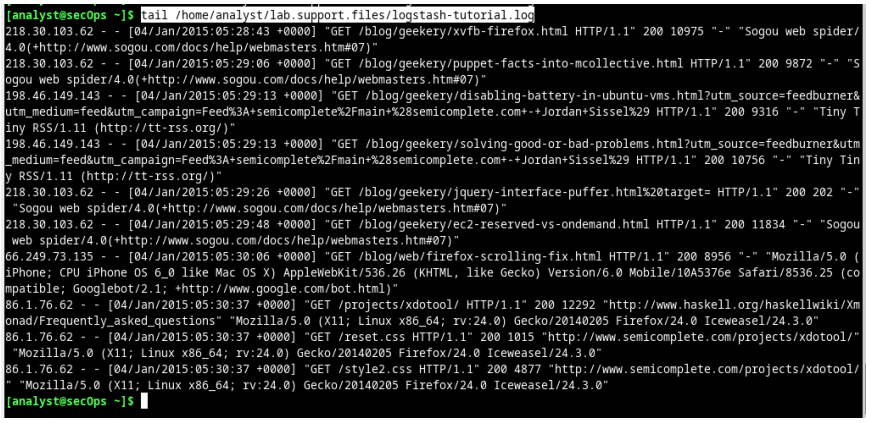




5. Perintah **tail** menampilkan akhir file teks. Secara default, tail menampilkan sepuluh baris terakhir file.

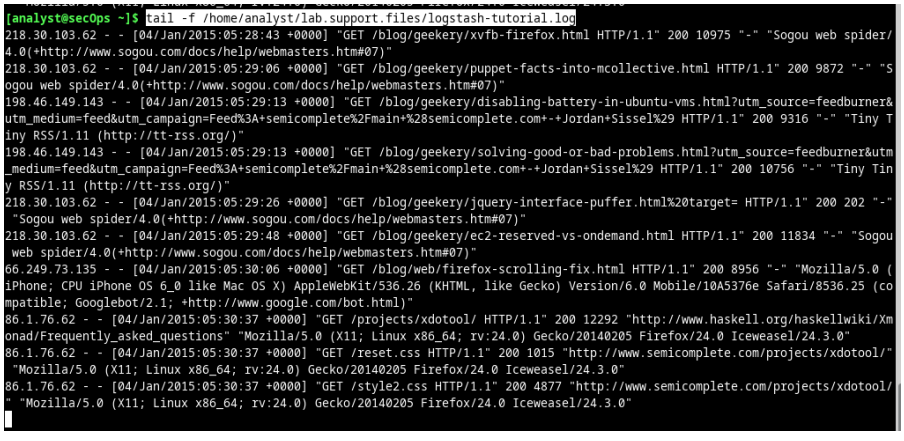
   Gunakan **tail** untuk menampilkan sepuluh baris terakhir dari file /home/analyst/lab.support.files/logstash-tutorial.log.

   analis@secOps ~$ tail /home/analyst/lab.support.files/logstash-tutorial.log



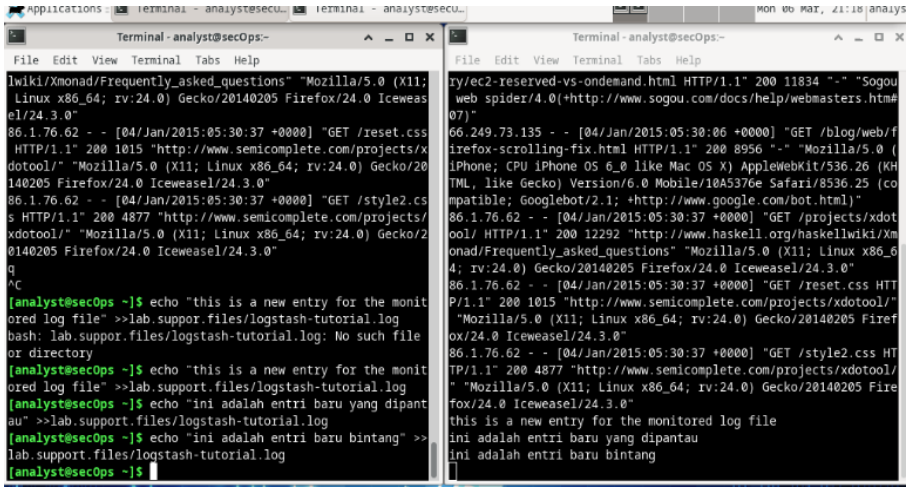
6. Atur tampilan Anda sehingga Anda dapat melihat kedua jendela terminal. Ubah ukuran jendela sehingga Anda dapat melihat keduanya secara bersamaan

   Pada jendela terminal tersebut, jalankanlah tail -f untuk melihat file /home/analyst/lab.support.files/logstash-tutorial.log. Gunakan jendela terminal di bagian bawah untuk menambahkan informasi ke file yang dipantau. Untuk memudahkan visualisasi, pilih jendela terminal atas (yang menjalankan tail -f) dan tekan enter beberapa kali. Ini akan menambahkan beberapa baris antara konten file saat ini dan informasi baru yang akan ditambahkan.



7. Pilihlah jendela terminal bawah dan masukkan perintah berikut: [analyst@secOps ~]$ echo "ini adalah entri baru untuk file log yang dipantau" >> lab.support.files/logstash-tutorial.log

Karena tail –f sedang memantau file pada saat sebuah baris ditambahkan ke file. Jendela atas akan menampilkan baris baru secara real-time. Tekan CTRL + C untuk menghentikan eksekusi tail -f dan kembali ke prompt shell. Tutup salah satu dari dua jendela terminal.

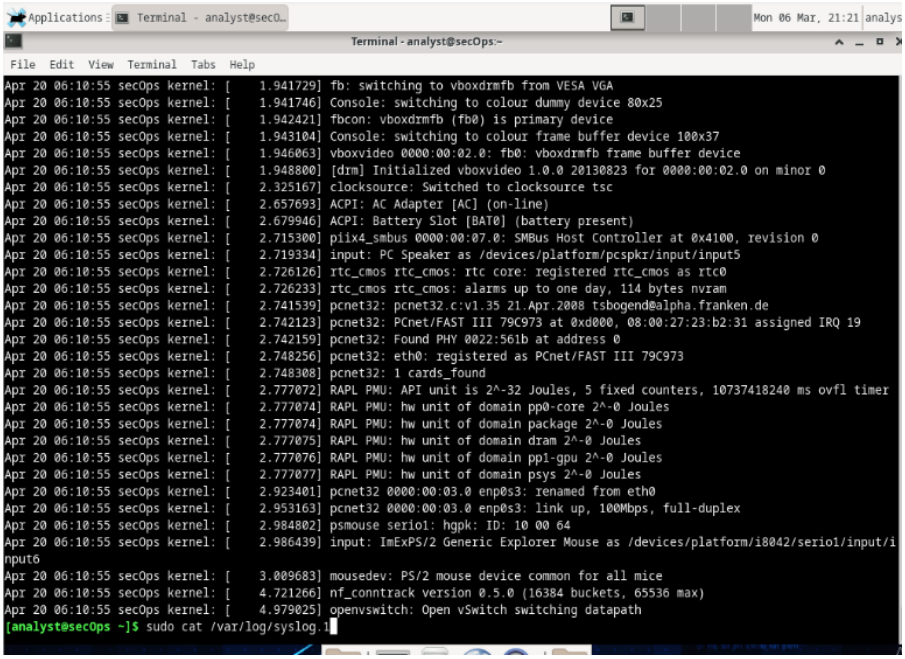


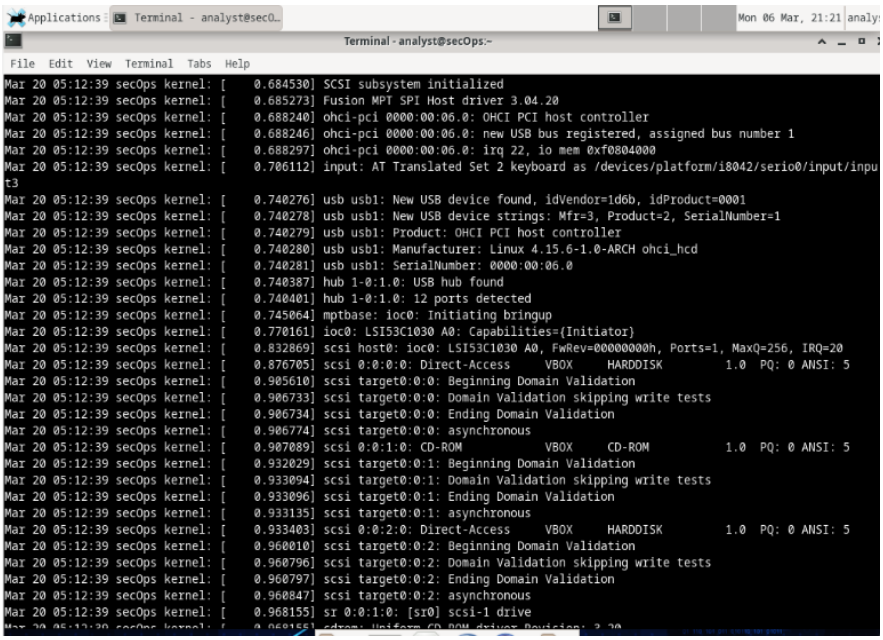
8. Memahami File Log dan Syslog

File log dapat dijadikan dalam satu server agar lebih mudah dalam pemantauannya. Syslog adalah sistem yang dirancang agar perangkat dapat mengirim file log ke server, yang dikenal sebagai server syslog. Klien berkomunikasi ke server syslog menggunakan protokol syslog. Syslog umumnya digunakan dan mendukung hampir semua platform komputer. VM CyberOps Workstation menghasilkan file log dan megirimkannya ke syslog. Gunakan perintah cat sebagai root untuk membuat daftar isi file /var/log/syslog.1. File ini menyimpan entri log yang dihasilkan oleh sistem operasi CyberOps Workstation VM dan dikirim ke layanan syslog.

analis@secOps ~$ sudo cat /var/log/syslog.1

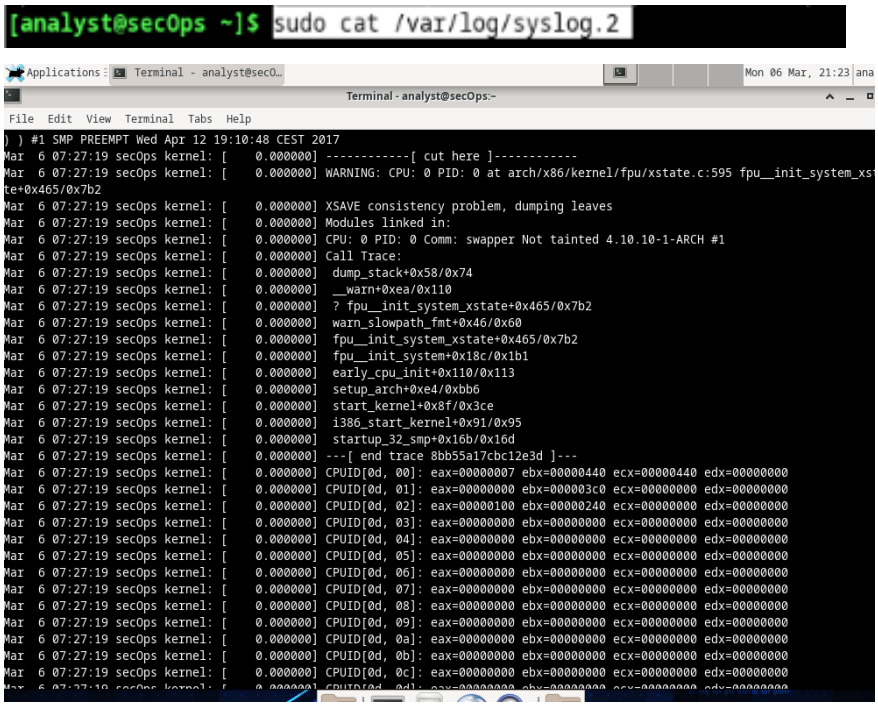
[Sudo] kata sandi untuk analis:



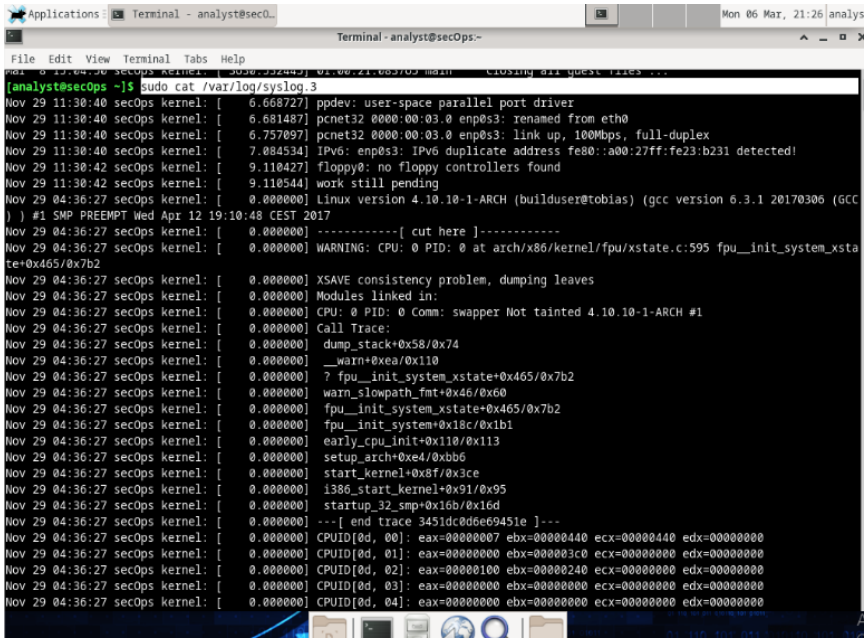


9. Untuk menjaga agar file syslog tetap kecil, sistem operasi secara berkala merotasi file log, mengganti nama file log lama menjadi syslog.1, syslog.2, dan seterusnya.

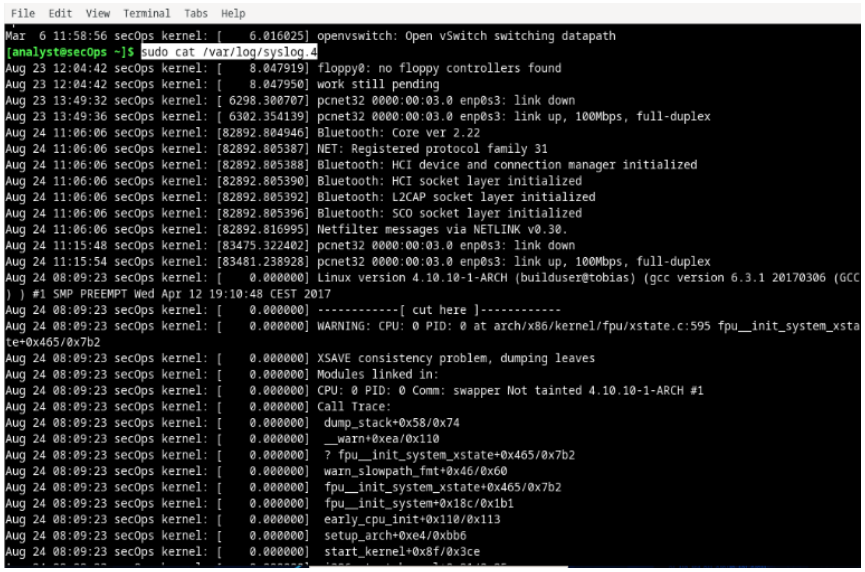
analis@secOps ~$ sudo cat /var/log/syslog.2



analis@secOps ~$ sudo cat /var/log/syslog.3



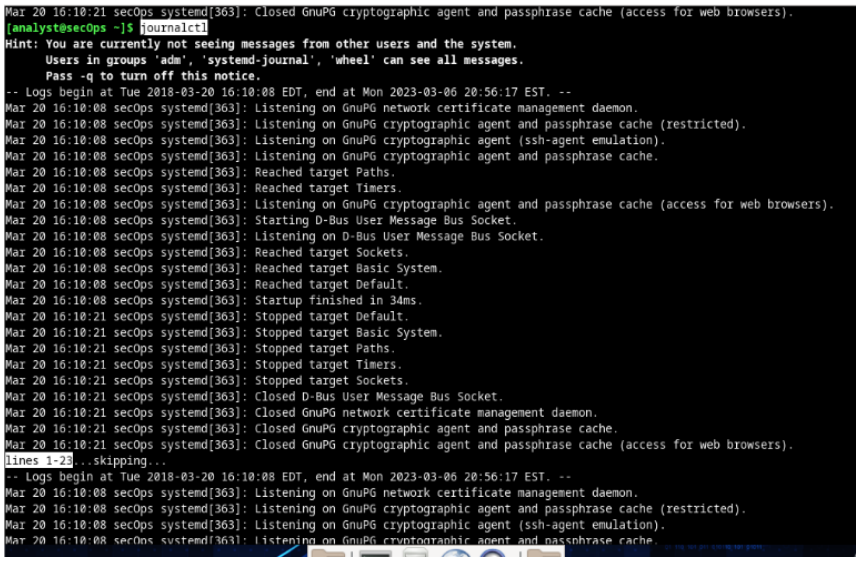
analis@secOps ~$ sudo cat /var/log/syslog.4



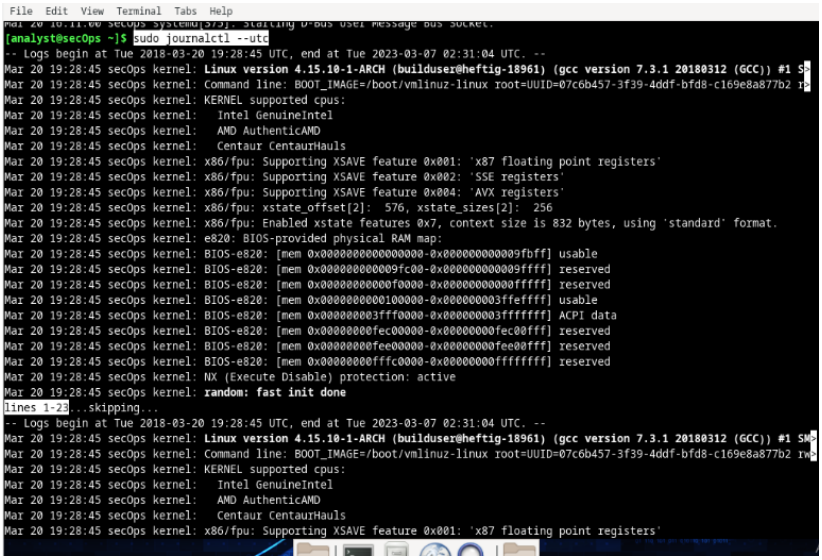
10. Memahami File Log dan Jurnalctl

Untuk melihat log journald, gunakan perintah journalctl. Alat journalctl menafsirkan dan menampilkan entri log yang sebelumnya disimpan dalam file log biner jurnal

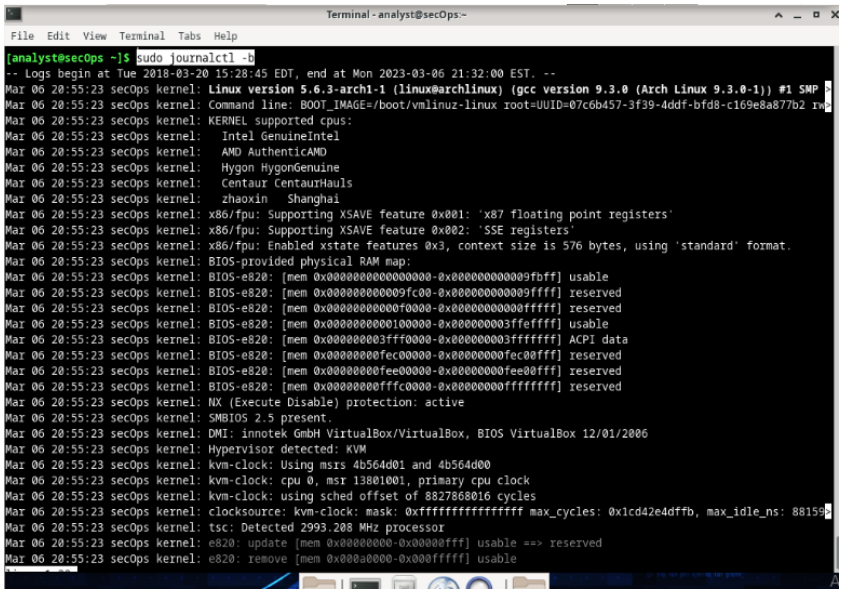
analis@secOps ~$ journalctl



analis@secOps ~$ sudo journalctl --utc

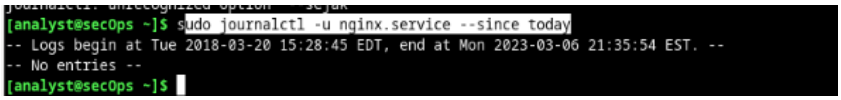


Gunakan journalctl -b untuk menampilkan entri log yang direkam selama boot terakhir: analis@secOps ~$ sudo journalctl –b



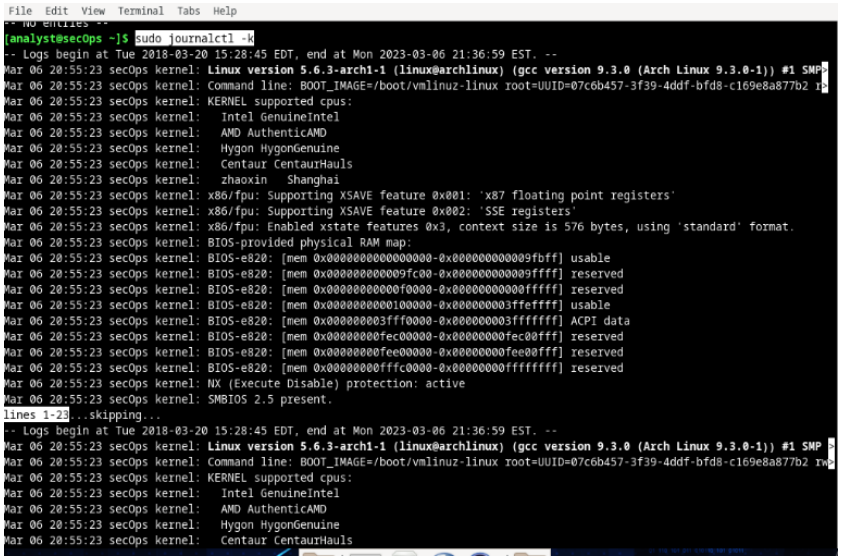
11. Gunakan journalctl untuk menentukan layanan dan kerangka waktu untuk entri log. Perintah di bawah ini menunjukkan semua log layanan nginx yang direkam hari ini

analis@secOps ~$ sudo journalctl -u nginx.service --sejak hari ini



12. Gunakan sakelar -k untuk hanya menampilkan pesan yang dihasilkan oleh kernel:

    analis@secOps ~$ sudo journalctl –k



13. Mirip dengan tail -f yang dijelaskan di atas, gunakan -f untuk secara aktif mengikuti log saat sedang ditulis:

    analis@secOps ~$ sudo journalctl –f

File yang tersimpan:

https://simpan.ugm.ac.id/apps/files/

V. ANALISIS

Pada praktikum kali ini melakukan praktik steganografi dan pembacaan log server/ file log.

Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya, kebanyakan pesan disembunyikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya.

Cara Kerja Steganografi antara lain dengan menyisipkan data yang ingin disembunyikan membutuhkan dua unsur. Unsur pertama ialah media penampung seperti citra, suara, video dan sebagainya yang terlihat tidak mencurigakan untuk menyimpan pesan rahasia. Unsur kedua adalah pesan yang ingin disembunyikan yaitu media penampungnya berupa citra yang disebut *cover-object* dan citra yang telah disisipi pesan disebut *stego-object*.

Secara umum, terdapat dua proses didalam steganografi yaitu proses embedding untuk menyisipkan pesan kedalam cover-object dan proses decoding untuk ekstraksi pesan dari stego-object. Kedua proses ini mungkin memerlukan kunci rahasia yang dinamakan stego-key agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan.

Pada lab stegano ini mengunduh gambar yang sudah diberikan di modul elok lalu disimpan pada folder yang Bernama “STEGO” kemudian buka cmd dan ketik perintah dir *.jpg untuk menampilkan informasi file berupa gambar yang ada pada folder STEGO. Terlihat sebelum dan sesudah gambar tersebut disispi pesan hiden text dimana terjadi perbedaan ukuran file. Untuk dari segi visual hamper tidak terjadi perbedaan dan hanya bisa diketahui melalui perintah pada CMD. Ditampilkan juga total ukuran 4 files gambar yang ada. Lanjut untuk mengecek keaslian/integritas pda gambar yang ada pada folder STEGO menggunakan MD5SUMS.

Pesan yang ditampilkan berupa pesan acak untuk menjaga keamanan dan bernilai 32 karakter.

File-file log adalah file yang berada di sebuah sistem yang merupakan file-file penting yang senantiasa mencatat semua kejadian-kejadian(kegiatan) yang berlangsung pada system. File -file log kebanyakan ditulis dalam bentuk file text yang ditulis perbaris (istilah untuk namanya adalah record) oleh program-program sistem bawaan saat kita menginstall sebuah program ataupun sebuah SO (sistem operasi).

Biasanya file log ini disimpan sebagai teks biasa. File log merupakan sumber yang sangat diperlukan untuk pemecahan masalah. File log biasanya berisi informasi teks biasa yang dapat dilihat oleh hampir semua program yang dapat menangani teks (editor teks, misalnya). Namun, karena kemudahan, kegunaan, dan kecepatan, beberapa alat lebih umum digunakan daripada yang lain. Bagian ini berfokus pada empat program berbasis baris perintah: cat, more, less, dan tail. Fitur cat, berasal dari kata 'concatenate', alat berbasis baris perintah yang digunakan untuk membaca dan menampilkan konten file di layar. Karena kemudahannya dan dapat membuka file teks dan menampilkannya di terminal teks saja, cat banyak digunakan hingga hari ini.

Catatan

- mkdir, buat direktori. Dalam hal ini, buat direktori STEGO langsung di bawah Drive C.
- dir "C:\", daftar semua direktori dan file langsung di bawah Drive C. Kemudian gunakan findstr untuk mencantumkan hanya file dan/atau direktori yang berisi string STEGO.

Pada praktikum ini dilakukan di CyberOps Workstation virtual machine.

Alat populer lainnya untuk memvisualisasikan file log adalah lebih banyak. Mirip dengan cat, more juga merupakan alat berbasis perintah UNIX yang dapat membuka file berbasis teks dan menampilkan konten file di layar. Perbedaan utama antara cat dan more adalah lebih mendukung page break,

memungkinkan pengguna untuk melihat konten file, satu halaman dalam satu waktu. Ini dapat dilakukan dengan menggunakan tombol spasi untuk menampilkan halaman berikutnya.

Sistem manajemen log populer lainnya dikenal sebagai jurnal. Dikelola oleh daemon journald, sistem ini dirancang untuk memusatkan pengelolaan log terlepas dari mana pesan berasal. Dalam konteks lab ini, fitur yang paling jelas dari daemon sistem jurnal adalah penggunaan file biner khusus tambahan yang berfungsi sebagai file lognya.

Versi-versi Unix menyimpan file-file log-nya pada direktory berbeda-beda. Umumnya file ini berada pada:

- /usr/adm ---> Digunakan oleh Unix Versi lama
- /var/adm ---> Digunakan oleh kebanyakan Versi Unix/Linux terbaru. dimana partisi /usr di-mount read only
- /var/log ---> Digunakan oleh beberapa versi Solaris, Linux, BSD

Perintah echo untuk menambahkan data baru berupa tulisan yang terdapat pada baris akhir. Setelah perintah echo dijalankan lalu membuka text menggunakan tail -f, maka akan muncul text yang kita tulis tadi pada baris akhir. Perintah syslog untuk mengirim/mengekspor pesan log ke dalam satu server. Untuk pembuatan syslog yang lain berguna agar ukuran file yang dihasilkan tidak terlalu besar dan membebani satu server. Perintah journalctl untuk membaca dan berkomunikasi dengan jurnal log, serta menampilkan pesan log oleh jurnal log. Perintah –utc pada journalctl berfungsi untuk menampilkan waktu log in UTC dengan menampilkan waktu yang sesungguhnya. Perintah -b pada journalctl berfungsi untuk menampilkan rekaman log terakhir selama boot berakhir. Perintah sudo journalctl -u nginx.service—day untuk menampilkan catatan seluruh log.

Gunakan journalctl - -utc untuk menampilkan semua cap waktu dalam waktu UTC.

Pertanyaan:

Apa kelemahan menggunakan cat dengan file teks besar?

- Tidak efisien untuk file besar
- Tidak dapat mengedit isi file
- Output terlalu banyak dan Tidak fleksibel

Apa kelemahan menggunakan more?

- Tidak efisien untuk navigasi mundur,
- Tidak dapat mengedit isi file
- Tidak fleksibel, dan output terlalu banyak.

Apa yang berbeda dalam output tail dan tail -f? Jelaskan

Pada output tail digunakan untuk menampilkan beberapa baris terakhir dari sebuah file teks. Ketika menjalankan perintah tail, kita akan melihat isi file yang terakhir dibaca pada saat itu.

Sedangkan output tail -f memiliki arti “follow” atau “mengikuti” digunakan untuk menampilkan isi file teks secara real-time. Ketika menjalankan perintah tail -f, akan melihat isi file yang sedang terus bertambah seiring dengan penambahan isi file tersebut.

Mengapa perintah cat harus dijalankan sebagai root?

Perintah cat tidak harus dijalankan sebagai root karena perintah ini biasanya hanya digunakan untuk membaca isi file teks dan tidak memerlukan akses ke hak istimewa root. Tetapi dalam beberapa kasus cat harus dijalankan sebagai root contohnya Ketika membaca file dengan hak akses terbatas.

Jelaskan kenapa harus mensinkronkan waktu dan tanggal komputer dengan benar?

Karena untuk memudahkan manajemen jaringan, mencegah kegagalan sertifikat, mencegah kerentanan keamanan dan menjaga akurasi waktu.

VI. KESIMPULAN

Setelah melaksanakan praktikum yang saya dapatkan adalah

- File log adalah file yang digunakan untuk merekam peristiwa tertentu yang dihasilkan oleh aplikasi, layanan, atau sistem operasi itu sendiri.
- Rotasi file log, dilakukan berdasarkan ukuran file
- File log akan di-rotasi setelah mencapai ukuran tertentu
- Steganografi adalah tulisan atau pesan yang disembunyikan
- Kelebihan menggunakan journalctl terletak pada banyaknya pilihan.

VII. DAFTAR PUSTAKA

Priyambodo, D. (2022, December 29). *Apa itu Log dan Setting Rotasi Log di VPS cPanel*. Rumahweb Journal – News, Article, and Tutorial of Web Dev. https://www.rumahweb.com/journal/apa-itu-log-adalah/

Knowledge, S. S.-. S. I. A. (n.d.). *Mengenal berbagai jenis file log di server linux | Explore your Mind*. https://suryadisyamsu.blogspot.com/2009/05/mengenal-berbagai-jenis-file-log-di.html

Komputer, U. S. &. T. (n.d.). *Seni dan Ilmu Menulis Pesan Tersembunyi (Steganografi)|S1 Teknik Informatika S.Kom*. http://teknik-informatika-s1.stekom.ac.id/informasi/baca/Seni-dan-Ilmu-Menulis-Pesan-Tersembunyi-Steganografi/ff7dc125afd07f6dd43da9fa8a09809e96d41789