**LAPORAN PRAKTIKUM**

**KEAMANAN INFORMASI 1**

**PERTEMUAN 3**

**Steganography & Pembacaan Log Server**



DISUSUN OLEH

Nama : Muhamad Alan Dharma Saputro S

NIM : 21/481348/SV/19761

Hari, Tanggal : Selasa, 7 Maret 2023

Dosen Pengampu : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

Kelas : RI4AA

**SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET**

**DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA**

**SEKOLAH VOKASI**

**UNIVERSITAS GADJAH MADA**

**YOGYAKARTA**

**2023**

1. Tujuan
2. Mengetahui penggunaan Steganography
3. Membaca File Log dengan *Cat, More, Less,* dan *Tail*
4. Memahami File Log dan Syslog
5. Memahami File Log dan Jurnalctl
6. Latar Belakang

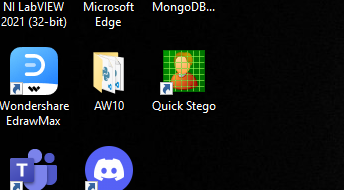
Steganografi adalah ilmu menulis pesan tersembunyi sedemikian rupa sehingga tidak ada seorang pun selain pengirim dan penerima yang dituju yang menyadari ada pesan tersembunyi. Dengan menggunakan QuickStego memungkinkan Anda menyembunyikan teks dalam gambar sehingga hanya pengguna QuickStego lain yang dapat mengambil dan membaca pesan rahasia yang tersembunyi. Setelah teks disembunyikan dalam gambar, gambar yang disimpan masih berupa 'gambar', itu akan dimuat seperti gambar lainnya dan muncul seperti sebelumnya. Gambar dapat disimpan, dikirim melalui email, diunggah ke web, satu-satunya perbedaan adalah berisi teks tersembunyi.

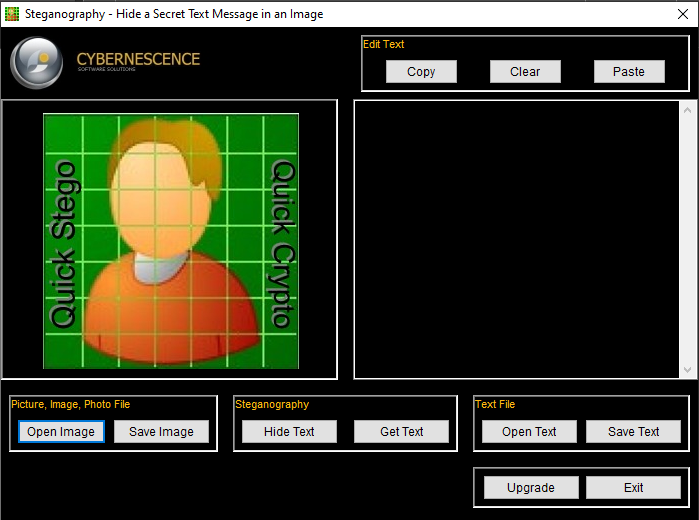
File Log adalah alat penting dalam pemecahan masalah dan pemantauan. Aplikasi yang berbeda menghasilkan file log yang berbeda, masing-masing berisi kumpulan bidang dan informasinya sendiri. Meskipun struktur bidang dapat berubah di antara file log, alat yang digunakan untuk membacanya sebagian besar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

1. Alat dan Bahan
2. PC dengan akses internet
3. Sofware QuickStego
4. CyberOps Workstation Virtual Machine
5. Intruksi Kerja

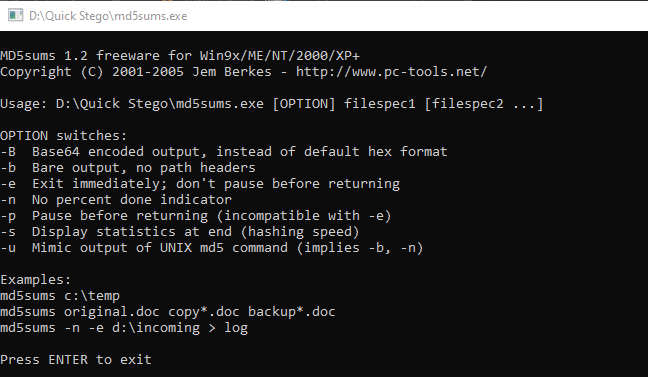
**Praktikum Staganografi**

1. Jalankan VM Windows OWASP
2. Install QuickStego

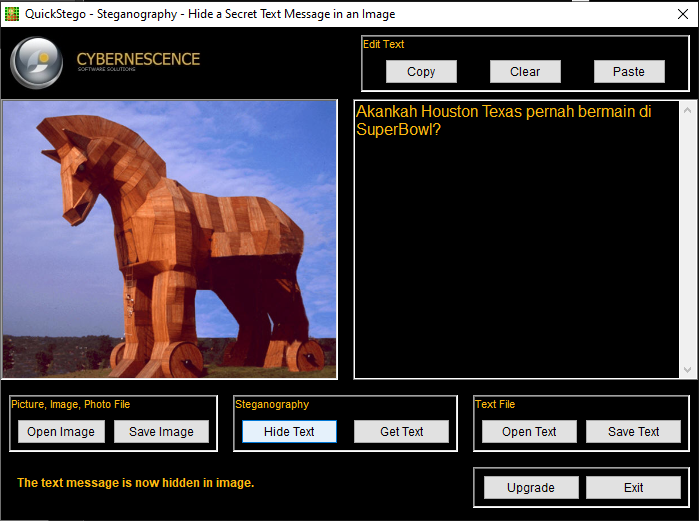




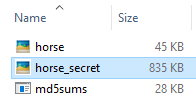
1. Install MD5SUMS



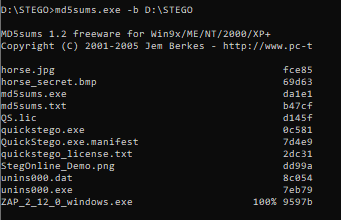
1. Sembunyikan pesan



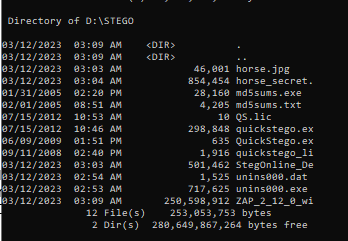
1. Melihat ukuran Byte files



1. Melihat MD5 checksum pada files



1. Hasil pembuktian dengan md5sum : buka command prompt , pastikan file md5sums.exe dalam satu folder dengan file gambar stego.



**Praktikum Analisis Log Server**

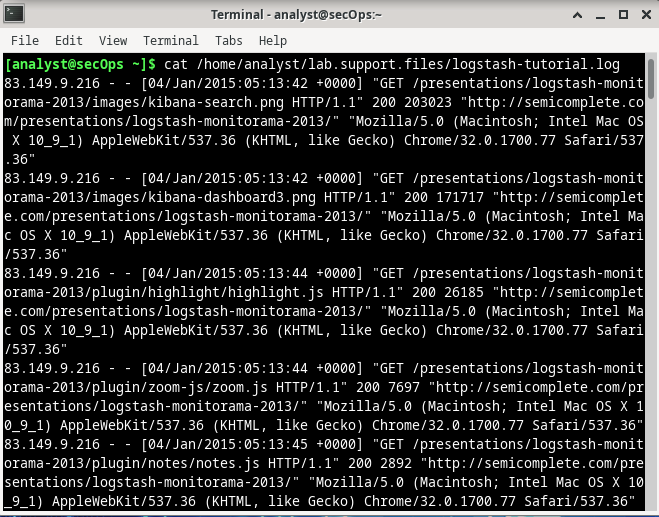
1. Membaca File Log dengan Cat, More, Less, dan Tail

File log adalah file yang digunakan untuk merekam peristiwa tertentu yang dihasilkan oleh aplikasi, layanan, atau sistem operasi itu sendiri. 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 untukmembaca dan menampilkan konten file di layar. Karena kemudahannya dan dapatmembuka file teks dan menampilkannya di terminal teks saja, cat banyak digunakan hingga hari ini. Bukalah VM CyberOps Worstation dan jendela terminal.

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

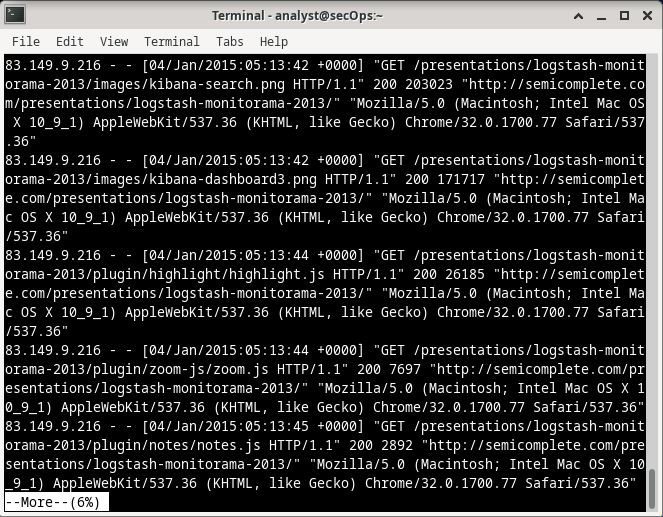


Pertanyaan:

Apa kelemahan menggunakan cat dengan file teks besar?

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.

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



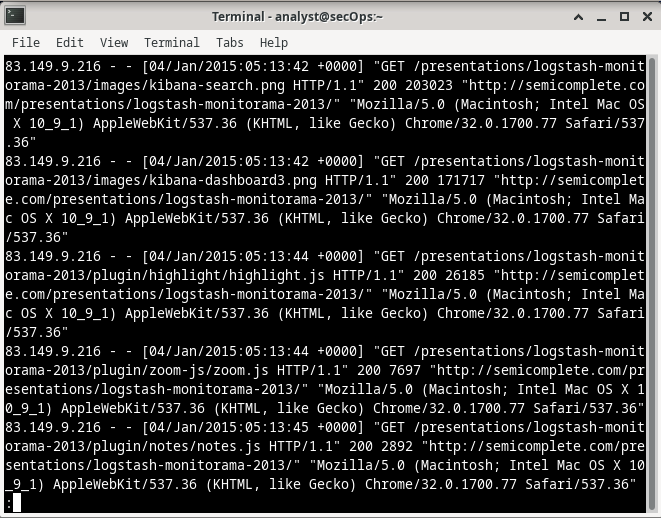
Pertanyaan:

Apa kelemahan menggunakan more?

Membangun fungsionalitas cat dan lebih banyak lagi, alat yang lebih sedikit memungkinkan konten file ditampilkan halaman demi halaman, sementara juga

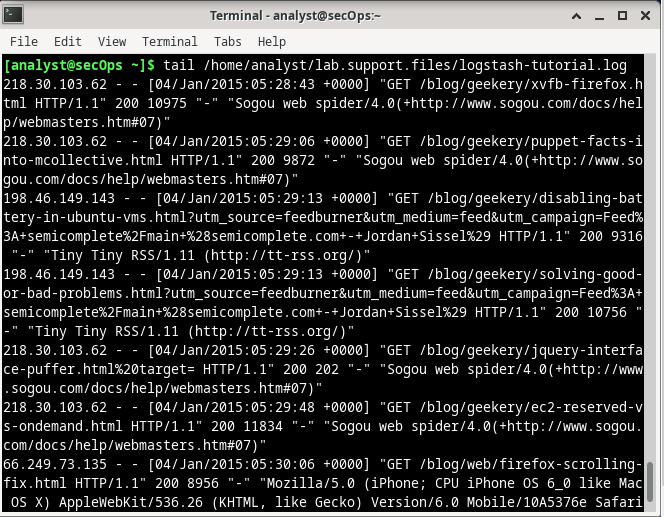
memungkinkan pengguna memilih untuk melihat halaman yang ditampilkan sebelumnya.

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

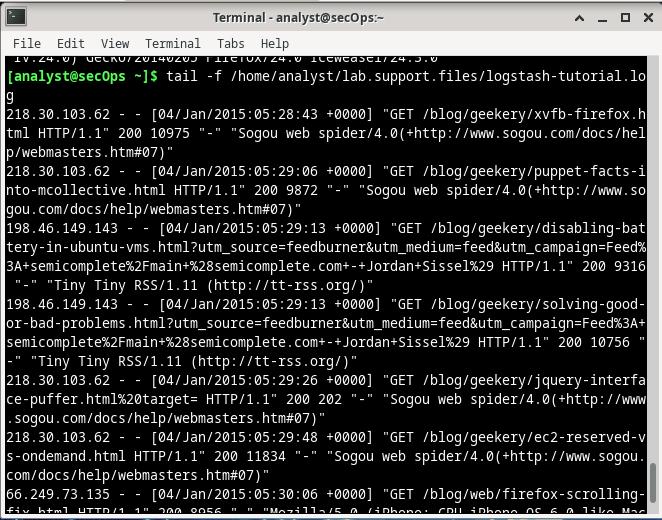


1. Perintah tail menampilkan akhir file teks. Secara default, tail menampilkan sepuluh baris terakhir file.

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

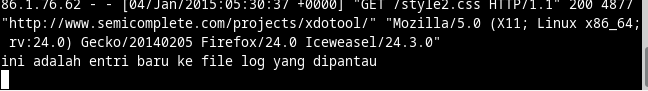


1. Atur tampilan Anda sehingga Anda dapat melihat kedua jendela terminal. Ubah ukuran jendela sehingga Anda dapat melihat keduanya secara bersamaan.



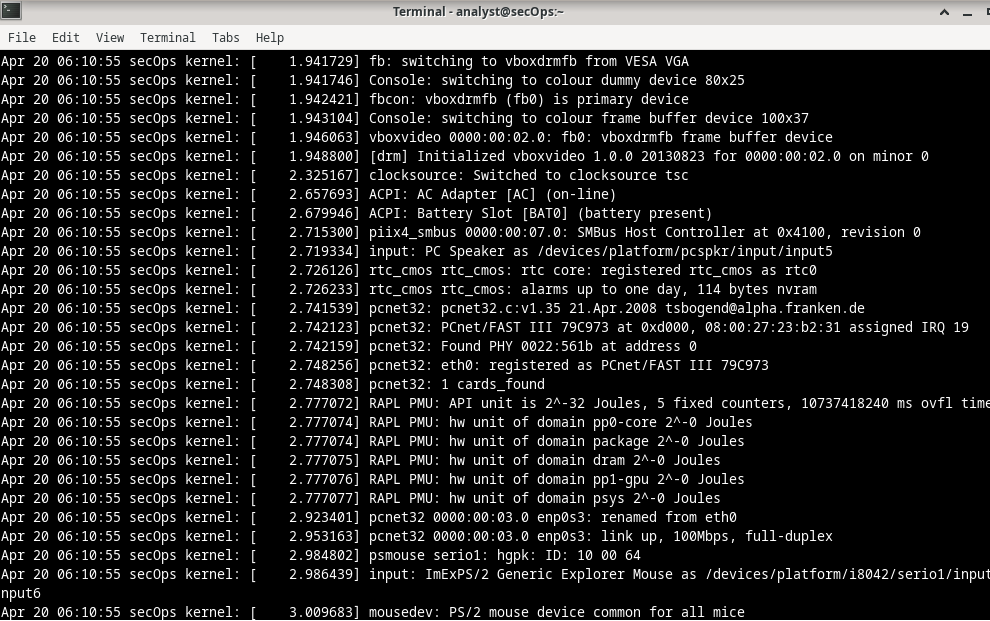
1. Pilihlah jendela terminal bawah dan masukkan perintah berikut



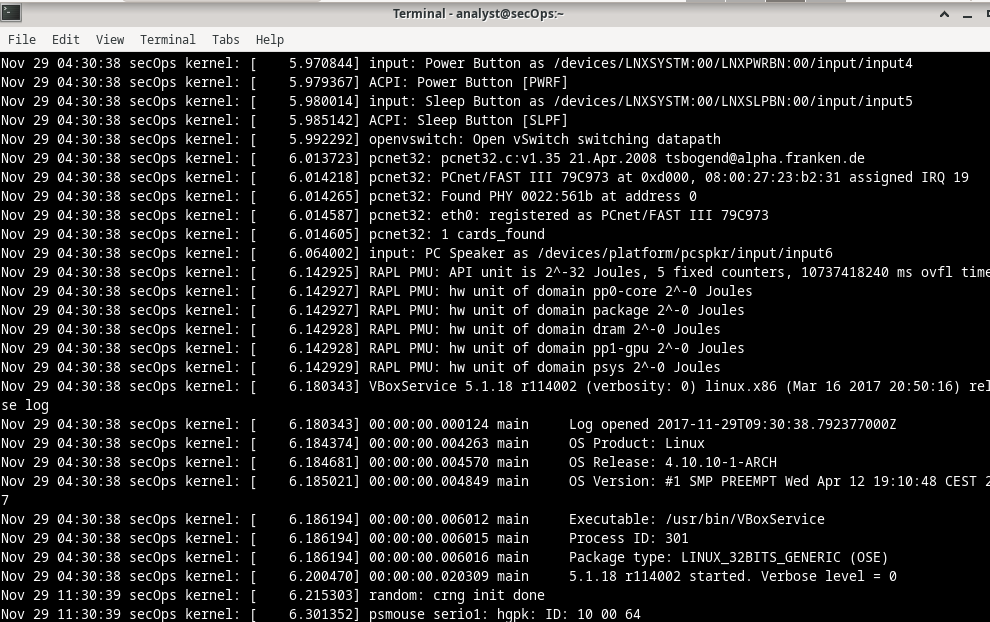


1. Memahami File Log dan Syslog

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.

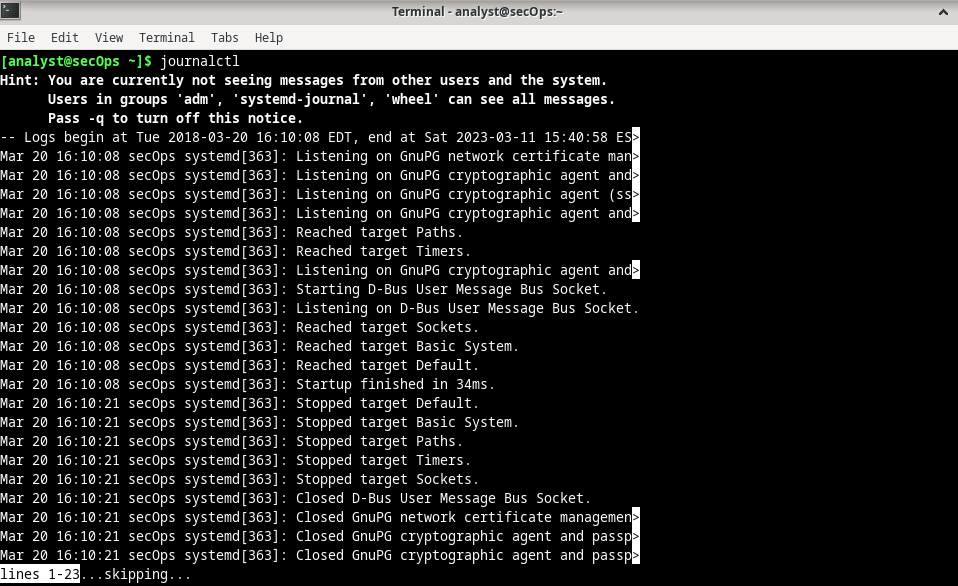


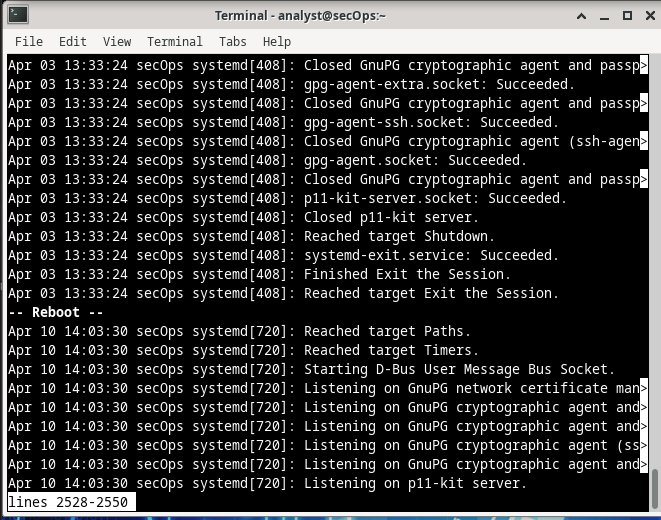
1. Perhatikan bahwa file /var/log/syslog hanya menyimpan entri log terbaru. Untuk menjaga agar file syslog tetap kecil, sistem operasi secara berkala merotasi file log, mengganti nama file log lama menjadi syslog.1, syslog.2, dan seterusnya.



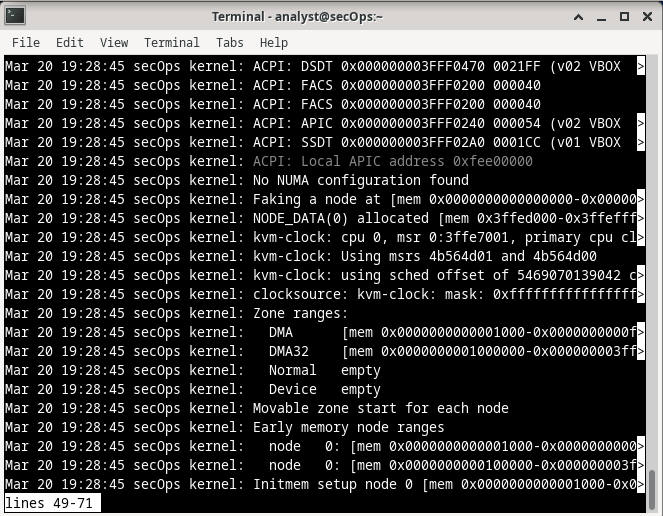
1. Memahami File Log dan Jurnalctl

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

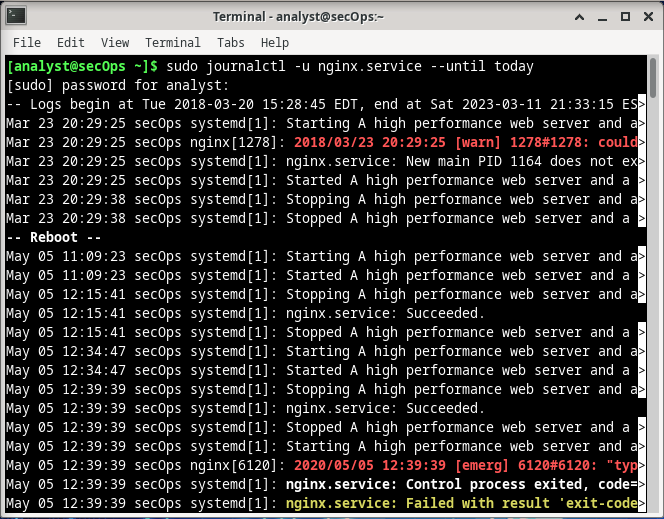




sudo journalctl –utc

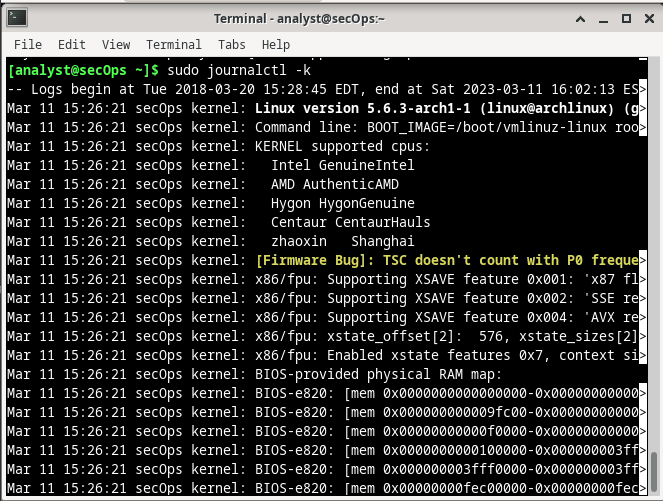


1. Gunakan journalctl untuk menentukan layanan dan kerangka waktu untuk entri log. Perintah di bawah ini menunjukkan semua log layanan nginx yang direkam hari ini:



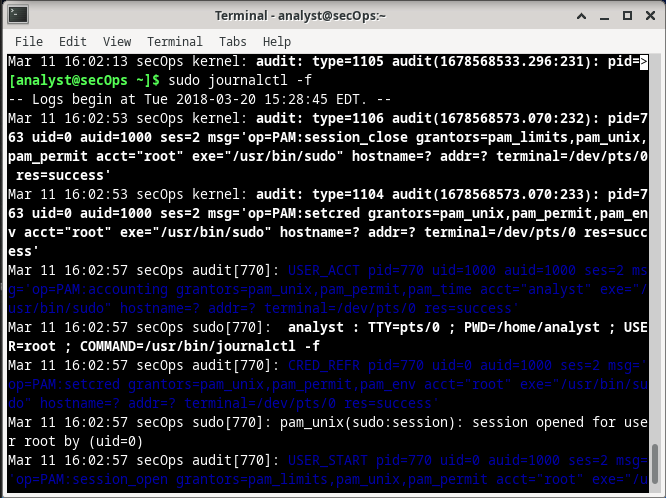


1. Gunakan sakelar -k untuk hanya menampilkan pesan yang dihasilkan oleh kernel: analis@secOps ~$ sudo journalctl –k



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

analis@secOps ~$ sudo journalctl –f



1. Buatlah laporan tentang pengerjaan anda ini kemudian dikumpulkan melalui elok.
2. Pembahasan
3. Kesimpulan

Kesimpulan yang didapatkan dari praktikum kali ini yaitu:

1. Daftar Pustaka