Unit 4
Analisis Anatomy Malware

A. Tujuan

- Meneliti dan menganalisis malware

B. Latar Belakang

Malware, atau perangkat lunak berbahaya, mengacu pada berbagai program perangkat lunak berbahaya yang dapat digunakan untuk menyebabkan kerusakan pada sistem komputer, mencuri data, dan melewati tindakan keamanan. Malware juga dapat menyerang infrastruktur penting, menonaktifkan layanan darurat, menyebabkan jalur perakitan membuat produk yang cacat, menonaktifkan generator listrik, dan mengganggu layanan transportasi. Pakar keamanan memperkirakan bahwa lebih dari satu juta ancaman malware baru dirilis setiap hari. McAfee Labs Threats Report 2019 menunjukkan penemuan teknik ransomware baru, pengungkapan miliaran akun melalui dump data profil tinggi, eksploitasi web HTTP yang signifikan, kerusakan pada Windows, Microsoft Office, dan Apple iOS, dan serangan lanjutan pada perangkat pribadi IoT. Temukan versi terbaru dari laporan dengan melakukan pencarian web untuk McAfee Labs Threats Report.

C. Alat dan Bahan

- PC dengan akses internet

D. Instruksi Kerja

1. Menggunakan mesin pencari favorit Anda, lakukan pencarian untuk malware terbaru. Selama pencarian Anda, pilih empat contoh malware, masing-masing dari jenis malware yang berbeda, dan bersiaplah untuk membahas detail tentang apa yang dilakukan masing-masing, bagaimana masing-masing ditransmisikan, dan dampak masing-masing penyebabnya.

   Contoh jenis malware antara lain: Ransomware, Trojan, Hoax, Adware, Malware, PUP, Exploit, Exploit Kit dan Kerentanan. Cari malware dengan mengunjungi situs web berikut menggunakan istilah pencarian berikut:

   • Dasbor Lanskap Ancaman Pusat Ancaman McAfee

   • Pusat Ancaman Malwarebytes Labs (10 Malware Teratas)

   • Securityweek.com > ancaman virus > virus-malware

   • Technewsworld.com > keamanan > malware

2. Baca informasi tentang malware yang ditemukan dari pencarian Anda di langkah sebelumnya, pilih salah satu dan tulis ringkasan singkat yang menjelaskan apa yang dilakukan malware, cara penularannya, dan dampaknya.

Unit 5
Serangan Rekayasa Sosial

A. Tujuan

- Meneliti dan menganalisis Serangan Rekayasa Sosial

B. Latar Belakang

Rekayasa sosial adalah serangan dengan tujuan membuat korban memasukkan informasi pribadi atau sensitif, jenis serangan ini dapat dilakukan oleh penyerang dengan memanfaatkan keylogger, email phishing, atau metode tatap muka. Laboratorium ini membutuhkan penelitian rekayasa sosial dan identifikasi cara untuk mengenali dan mencegahnya.

C. Alat dan Bahan

PC dengan akses internet

D. Instruksi Kerja

Gunakanlah browser web, temukan artikel "Metode untuk Memahami dan Mengurangi Serangan Rekayasa Sosial" di situs web SANS Institute. Sebuah mesin pencari harus dengan mudah menemukan artikel.

SANS Institute adalah organisasi penelitian dan pendidikan kooperatif yang menawarkan pelatihan keamanan informasi dan sertifikasi keamanan. Ruang Baca SANS memiliki banyak artikel yang relevan dengan praktik analisis keamanan siber. Anda dapat bergabung dengan komunitas SANS dengan membuat akun pengguna gratis untuk mengakses artikel terbaru, atau Anda dapat mengakses artikel lama tanpa akun pengguna.

Bacalah artikel atau pilihlah artikel lain tentang rekayasa sosial, dan jawablah pertanyaan berikut:

Pertanyaan:

1. Apa tiga metode yang digunakan dalam rekayasa sosial untuk mendapatkan akses ke informasi?

2. Apa tiga contoh serangan rekayasa sosial dari dua metode pertama di langkah sebelumnya?

3. Mengapa jejaring sosial merupakan ancaman rekayasa sosial?

4. Bagaimana sebuah organisasi dapat mempertahankan diri dari serangan rekayasa sosial?

5. Apa itu SANS Institute?

6. Buatlah laporan tentang pengerjaan anda ini kemudian dikumpulkan melalui elok.

Unit 6
Pembacaan Log Server

A. Tujuan

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

B. 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.

C. Alat dan Bahan

- CyberOps Workstation virtual machine

D. Instruksi Kerja

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 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. 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.

   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.

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.

   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.

4. Dari tampilan terminal yang sama, gunakan **less** untuk menampilkan konten file logstash-tutorial.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
   218.30.103.62 - - [04/Jan/2015:05:28:43 +0000] "DAPATKAN /blog/geekery/xvfb-firefox.html HTTP/1.1" 200 10975 "-" "Sogou web spider/4.0(+http ://www.sogou.com/docs/help/webmasters.htm#07)"

218.30.103.62 - - [04/Jan/2015:05:29:06 +0000] "GET /blog/geekery/puppet-facts-into-mcollective.html HTTP/1.1" 200 9872 "-" "Sogou web spider/ 4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "DAPATKAN /blog/geekery/disabling-battery-in-ubuntu-vms.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete%2Fmain+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 9316 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
198.46.149.143 - - [04/Jan/2015:05:29:13 +0000] "GET /blog/geekery/solving-good-or-bad-problems.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+semicomplete %2Fmain+%28semicomplete.com+-+Jordan+Sissel%29 HTTP/1.1" 200 10756 "-" "Tiny Tiny RSS/1.11 (http://tt-rss.org/)"
218.30.103.62 - - [04/Jan/2015:05:29:26 +0000] "GET /blog/geekery/jquery-interface-puffer.html%20target= HTTP/1.1" 200 202 "-" "Sogou web spider /4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
218.30.103.62 - - [04/Jan/2015:05:29:48 +0000] "GET /blog/geekery/ec2-reserved-vs-ondemand.html HTTP/1.1" 200 11834 "-" "Sogou web spider/ 4.0(+http://www.sogou.com/docs/help/webmasters.htm#07)"
66.249.73.135 - - [04/Jan/2015:05:30:06 +0000] "DAPATKAN /blog/web/firefox-scrolling-fix.html HTTP/1.1" 200 8956 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 seperti Mac OS X) AppleWebKit/536.26 (KHTML, seperti Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (kompatibel; Googlebot/2.1; +http://www.google.com/bot.html)"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "GET /projects/xdotool/ HTTP/1.1" 200 12292 "http://www.haskell.org/haskellwiki/Xmonad/Frequently_asked_questions" "Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "DAPATKAN /reset.css HTTP/1.1" 200 1015 "http://www.semicomplete.com/projects/xdotool/" "Mozilla /5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"
86.1.76.62 - - [04/Jan/2015:05:30:37 +0000] "DAPATKAN /style2.css HTTP/1.1" 200 4877 "http://www.semicomplete.com/projects/xdotool/" "Mozilla /5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140205 Firefox/24.0 Iceweasel/24.3.0"

Dalam beberapa situasi, diinginkan untuk memantau file log karena entri log ditulis ke file log. Untuk kasus tersebut, perintah tail -f sangat membantu.

sebuah. Gunakan tail -f untuk memantau konten file /var/log/syslog secara aktif:

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

Pertanyaan:

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

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
   Perintah di atas menambahkan pesan "ini adalah entri baru ke file log yang dipantau" ke file /home/analyst/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:
   7 Feb 13:23:15 secOps kernel: [5.458959] psmouse serio1: hgpk: ID: 10 00 64
   7 Februari 13:23:15 kernel secOps: [5.467285] masukan: ImExPS/2 BYD TouchPad sebagai /devices/platform/i8042/seri1/input/input6
   7 Feb 13:23:15 kernel secOps: [5.502469] RAPL PMU: Unit API adalah 2^-32 Joule, 4 penghitung tetap, timer ovfl 10737418240 ms
   Feb 7 13:23:15 secOps kernel: [5.502476] RAPL PMU: unit hw domain pp0-core 2^-0 Joule
   7 Feb 13:23:15 secOps kernel: [5.502478] RAPL PMU: unit hw paket domain 2^-0 Joule
   Feb 7 13:23:15 secOps kernel: [5.502479] RAPL PMU: hw unit domain dram 2^-0 Joule

Feb 7 13:23:15 secOps kernel: [5.502480] RAPL PMU: hw unit domain pp1-gpu 2^-0 Joule
7 Februari 13:23:15 kernel secOps: [5.672547] ppdev: driver port paralel ruang pengguna
7 Feb 13:23:15 secOps kernel: [5.709000] pcnet32 0000:00:03.0 enp0s3: diganti namanya dari eth0
7 Feb 13:23:16 secOps kernel: [6.166738] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
7 Februari 13:23:16 secOps kernel: [6.706058] acak: crng init selesai
7 Feb 13:23:18 secOps kernel: [8.318984] floppy0: tidak ditemukan pengontrol floppy
7 Februari 13:23:18 secOps kernel: [8.319028] pekerjaan masih tertunda
7 Februari 14:26:35 secOps kernel: [3806.118242] hrtimer: interupsi membutuhkan 4085149 ns
7 Feb 15:02:13 secOps kernel: [5943.582952] pcnet32 0000:00:03.0 enp0s3: link down
7 Feb 15:02:19 secOps kernel: [5949.556153] pcnet32 0000:00:03.0 enp0s3: link up, 100Mbps, full-duplex
Pertanyaan:
Mengapa perintah **cat** harus dijalankan sebagai **root**?

9. 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.

   Gunakan perintah **cat** untuk membuat daftar file syslog yang lebih lama:
   analis@secOps ~$ sudo cat /var/log/syslog.2
   analis@secOps ~$ sudo cat /var/log/syslog.3
   analis@secOps ~$ sudo cat /var/log/syslog.4

   Pertanyaan:
   Jelaskan kenapa harus mensinkronkan waktu dan tanggal komputer dengan benar?

10. Memahami File Log dan Jurnalctl
    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.

    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
    -- Log dimulai pada Jum 26-09-2014 14:13:12 EDT, berakhir pada Selasa-02-07 13:23:29 ES

26 Sep 14:13:12 dataAnalyzer systemd[1087]: Memulai Jalur.
26 Sep 14:13:12 dataAnalyzer systemd[1087]: Mencapai Jalur target.
26 Sep 14:13:12 dataAnalyzer systemd[1087]: Memulai Timer.
26 Sep 14:13:12 dataAnalyzer systemd[1087]: Timer target tercapai.
26 Sep 14:13:12 dataAnalyzer systemd[1087]: Memulai Soket.
26 Sep 14:13:12 dataAnalyzer systemd[1087]: Mencapai soket target.
26 Sep 14:13:12 dataAnalyzer systemd[1087]: Memulai Sistem Dasar.
26 Sep 14:13:12 dataAnalyzer systemd[1087]: Mencapai target Sistem Dasar.
26 Sep 14:13:12 dataAnalyzer systemd[1087]: Mulai Default.
26 Sep 14:13:12 dataAnalyzer systemd[1087]: Mencapai target Default.
26 Sep 14:13:12 dataAnalyzer systemd[1087]: Startup selesai dalam 18ms.
26 Sep 14:14:24 dataAnalyzer systemd[1087]: Menghentikan Default.
26 Sep 14:14:24 dataAnalyzer systemd[1087]: Target yang dihentikan Default.
26 Sep 14:14:24 dataAnalyzer systemd[1087]: Menghentikan Sistem Dasar.
26 Sep 14:14:24 dataAnalyzer systemd[1087]: Menghentikan target Sistem Dasar.
26 Sep 14:14:24 dataAnalyzer systemd[1087]: Menghentikan Jalur.
26 Sep 14:14:24 dataAnalyzer systemd[1087]: Jalur target yang dihentikan.
26 Sep 14:14:24 dataAnalyzer systemd[1087]: Menghentikan Timer.
26 Sep 14:14:24 dataAnalyzer systemd[1087]: Pengatur waktu target yang dihentikan.
26 Sep 14:14:24 dataAnalyzer systemd[1087]: Stopping Sockets.
<keluaran dihilangkan>

Catatan:
Menjalankan journalctl sebagai root akan menampilkan informasi yang lebih detail.
Gunakan CTRL+C untuk keluar dari tampilan.

Kelebihan menggunakan journalctl terletak pada banyaknya pilihan. Gunakan journalctl --utc untuk menampilkan semua cap waktu dalam waktu UTC:

analis@secOps ~$ sudo journalctl --utc

Gunakan journalctl -b untuk menampilkan entri log yang direkam selama boot terakhir:

analis@secOps ~$ sudo journalctl –b
07 Feb 08:23:13 secOps systemd-journald[172]: Waktu yang dihabiskan untuk membilas ke /var adalah
Feb 07 08:23:13 secOps kernel: Linux versi 4.8.12-2-ARCH (builduser@andyrtr)
07 Feb 08:23:13 secOps kernel: x86/fpu: Mendukung fitur XSAVE 0x001: 'x87 fl
Feb 07 08:23:13 secOps kernel: x86/fpu: Mendukung fitur XSAVE 0x002: 'SSE re
07 Feb 08:23:13 secOps kernel: x86/fpu: Mendukung fitur XSAVE 0x004: 'AVX re
07 Februari 08:23:13 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]
07 Feb 08:23:13 secOps kernel: x86/fpu: Mengaktifkan fitur xstate 0x7, konteks si

07 Feb 08:23:13 secOps kernel: x86/fpu: Menggunakan sakelar konteks FPU 'bersemangat'.
07 Februari 08:23:13 kernel secOps: e820: Peta RAM fisik yang disediakan BIOS:

<keluaran dihilangkan>

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

14. Buatlah laporan tentang pengerjaan anda ini kemudian dikumpulkan melalui elok.