



VSGA Vocational School
Graduate Academy

Modul Pelatihan **JUNIOR CYBER SECURITY**

Vocational School Graduate Academy
Digital Talent Scholarship
Tahun 2023

KATA PENGANTAR

Dunia saat ini berada pada era industri 4.0 yang lebih banyak menggunakan teknologi digital dan Indonesia telah mempersiapkan diri untuk masuk ke dalam tahap industri 4.0 tersebut melalui agenda percepatan transformasi digital. Salah satu langkah yang dilakukan dalam percepatan transformasi digital adalah penyiapan talenta digital. Laporan Bank Dunia tahun 2019 menyatakan bahwa Indonesia memiliki kekurangan 9 juta pekerja berketerampilan teknologi informasi dan komunikasi, sehingga perlu dilakukan penyiapan talenta digital untuk memenuhi kebutuhan tersebut dengan alokasi 600.000 orang setiap tahun. Upaya penyiapan talenta digital dilakukan oleh berbagai unsur baik pemerintah, institusi pendidikan, industri, komunitas masyarakat, maupun media publik.

Sejak tahun 2018, Kementerian Komunikasi dan Informatika melalui Badan Penelitian dan Pengembangan Sumber Daya Manusia menginisiasi Program Beasiswa Pelatihan Digital bernama *Digital Talent Scholarship* (DTS) yang telah berhasil dianugerahkan kepada lebih dari 300.000 penerima pelatihan bidang teknologi informasi dan komunikasi. Program *Digital Talent Scholarship* ini ditujukan untuk memberikan pelatihan dan sertifikasi berbagai tema pada bidang informatika, komunikasi, dan telekomunikasi, serta diharapkan melengkapi pemenuhan kebutuhan talenta digital Indonesia.

Program DTS tahun 2023 secara garis besar dibagi menjadi delapan akademi, salah satunya Vocational School Graduate Academy (VSGA). VSGA merupakan program pelatihan berbasis kompetensi kerja nasional bagi lulusan pendidikan vokasi SMK/ sederajat dan diploma bidang *Science, Technology, Engineering, Mathematics* (STEM) yang belum mendapatkan pekerjaan atau sedang tidak bekerja. Tujuan Program VSGA adalah menyiapkan talenta digital dengan standar kompetensi sesuai Standar Kompetensi Kerja Nasional Indonesia (SKKNI). Oleh karena itu, penyusunan modul pelatihan untuk Program VSGA disusun dengan berbasis pada kompetensi (*Competency Based Training*). Kami berpesan agar modul pelatihan berbasis kompetensi yang telah disusun ini dapat menjadi referensi bagi peserta dan pengajar agar pelatihan berjalan efektif dan efisien.

Selamat mengikuti Pelatihan *Digital Talent Scholarship*, mari persiapkan diri kita menjadi talenta digital Indonesia yang kompeten.

Jakarta, April 2023
Kepala Badan Penelitian dan Pengembangan Sumber Daya Manusia
Kementerian Komunikasi dan Informatika Republik Indonesia

Dr. Hary Budiarto, M.Kom

Pendahuluan

Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam Mengelola Log untuk mengumpulkan, menganalisis, dan memonitor log aktivitas sistem untuk memperbaiki keamanan dan kinerja sistem.

A. Tujuan Umum

Setelah mempelajari modul ini peserta latih diharapkan mampu dalam Mengelola Log benar.

B. Tujuan Khusus

Adapun tujuan mempelajari unit kompetensi melalui buku modul alam mengumpulkan data ini guna memfasilitasi peserta latih sehingga pada akhir pelatihan diharapkan memiliki kemampuan sebagai berikut:

1. Pengetahuan tentang sistem operasi dan aplikasi: Dalam mengelola log, diperlukan pengetahuan tentang sistem operasi dan aplikasi yang digunakan untuk mengumpulkan log. Hal ini meliputi pemahaman tentang jenis log yang dihasilkan oleh sistem operasi dan aplikasi, di mana lokasi log disimpan, dan format log yang digunakan.
2. Keterampilan dalam analisis log: Analisis log adalah proses memeriksa dan mengevaluasi log untuk mencari tanda-tanda kegiatan tidak wajar atau aktivitas yang mencurigakan. Dalam mengelola log, diperlukan keterampilan dalam menganalisis log untuk mengidentifikasi masalah dan mengambil tindakan yang diperlukan.
3. Keterampilan dalam manajemen log: Manajemen log meliputi kemampuan untuk mengumpulkan, menyimpan, dan memonitor log. Dalam mengelola log, diperlukan keterampilan dalam mengelola siklus hidup log, termasuk pengaturan tingkat log, rotasi log, dan penghapusan log yang tidak diperlukan.
4. Pengetahuan tentang keamanan informasi: Karena log berisi informasi sensitif tentang kegiatan sistem, diperlukan pengetahuan tentang keamanan informasi untuk menjaga kerahasiaan, integritas, dan ketersediaan log. Hal ini meliputi pemahaman tentang regulasi dan kebijakan keamanan informasi, enkripsi log, dan manajemen akses log.
5. Sikap kerja yang teliti dan bertanggung jawab: Dalam mengelola log, diperlukan sikap kerja yang teliti dan bertanggung jawab untuk memastikan bahwa log diambil secara teratur, dianalisis secara cermat, dan dihapus sesuai dengan kebijakan yang ditetapkan.
6. Kemampuan komunikasi yang baik: Dalam mengelola log, diperlukan kemampuan komunikasi yang baik untuk berkomunikasi dengan tim keamanan informasi, administrator sistem, dan pengguna untuk mengidentifikasi masalah dan mengambil tindakan yang diperlukan.

Dalam keseluruhan, Mengelola Log memerlukan kombinasi pengetahuan teknis, keterampilan analitis, dan sikap kerja yang bertanggung jawab untuk memastikan bahwa log digunakan secara efektif untuk memperbaiki keamanan dan kinerja sistem.

Latar belakang

Unit kompetensi ini berhubungan dengan pengetahuan, keterampilan, dan sikap kerja yang dibutuhkan dalam mengumpulkan data untuk data science. Penilaian dilakukan dengan mengacu kepada Kriteria Unjuk Kerja (KUK) dan dilaksanakan di Tempat Uji Kompetensi (TUK), ruang simulasi atau workshop dengan cara:

- 1.1 Lisan
- 1.2 Wawancara
- 1.3 Tes tertulis
- 1.4 Demonstrasi
- 1.5 Metode lain yang relevan.

Deskripsi Pelatihan

Materi Pelatihan ini memfasilitasi pembentukan kompetensi dalam menentukan kebutuhan teknis Mengelola Log.

Tujuan Pembelajaran

Setelah mengikuti pelatihan ini, peserta mampu menentukan kebutuhan teknis Mengelola Log.

Kompetensi Dasar

Mampu menentukan kebutuhan teknis Mengelola Log.

Indikator Hasil Belajar

Ketepatan dalam melakukan proses pengambilan data sesuai dengan tools yang telah disiapkan

INFORMASI PELATIHAN

INFORMASI PELATIHAN	
Akademi	VSGA untuk Junior Cyber Security
Mitra Pelatihan	
Tema Pelatihan	<i>Junior Cyber Security</i>
Sertifikasi	Sertifikasi kompetensi BNSP <i>Junior Cyber Security</i>
Deskripsi Pelatihan	Pelatihan ini menyiapkan peserta agar kompeten dalam melaksanakan pekerjaan <i>junior cyber security</i> yang dapat membantu pekerjaan praktisi <i>cyber security</i> . Kualifikasi pada jabatan ini menuntut seseorang memiliki kompetensi dalam menerapkan prinsip perlindungan informasi, menerapkan prinsip keamanan informasi untuk penggunaan jaringan internet, menerapkan prinsip keamanan informasi pada transaksi elektronik, melaksanakan kebijakan keamanan informasi, mengaplikasikan ketentuan/persyaratan keamanan informasi, mengelola log, dan menerapkan kontrol akses berdasarkan konsep/metodologi yang telah ditetapkan
Output Pelatihan	Setelah mengikuti pelatihan peserta akan mampu menganalisis dan memvisualisasikan data sehingga dapat digunakan dalam pengambilan keputusan
Durasi Pelatihan	24 JP (3 hari)

INFORMASI PELATIHAN	
Jenis Pelatihan	Luring /Offline (40% Pengetahuan - 60% Praktek)
Persyaratan Peserta	<ul style="list-style-type: none"> • Warga Negara Indonesia • Usia Maksimal 29 Tahun pada saat mendaftar • Lulus Pendidikan D3 Bidang TIK/SMK Bidang (TKJ/TI/RPL) yang pernah bekerja minimal 3 tahun • Belum Mendapatkan Pekerjaan Tetap/Pernah Bekerja tapi sedang tidak bekerja • Lolos Seleksi Administrasi dan Tes Substansi
Persyaratan Sarana Peserta	Laptop/PC dengan spesifikasi: <ul style="list-style-type: none"> • RAM minimal 4 GB • 32/64-bit processor • Operating System Windows 7,8,10, Linux, atau MAC OSX • konektivitas WiFi • Akses Internet Dedicated 256 kbps per peserta per perangkat
Kriteria Pengajar/ <i>Trainer</i> /Instruktur:	<ol style="list-style-type: none"> 1. Minimal Lulusan S2 di bidang TIK; atau Memiliki kompetensi Okupasi Nasional "<i>Junior Cyber Security</i>". 2. Pengalaman Kerja diutamakan sebagai tenaga pengajar Pelatihan Bidang TIK minimal selama 2 tahun 3. Telah mengikuti pelatihan <i>training of trainner Junior Cyber Security</i>
Tim Penyusun:	<ol style="list-style-type: none"> 1. Yan Hadynoer (BSSN) 2. Yoyok Darmanto (BSSN)

INFORMASI PEMBELAJARAN

RENCANA PELATIHAN		
Pertemuan	Topik	Aktivitas
Hari 1	<ul style="list-style-type: none"> • Pembukaan dan Penjelasan Rencana Pembelajaran • Pre test 	Pemaparan materi, diskusi dan <i>hands-on lab live class 1 JP</i>
	Pengantar <i>Junior Cyber Security</i> (Posisi dan peran <i>junior cyber security</i>)	Pemaparan materi, diskusi dan <i>hands-on</i>

		<i>lab live class 1 JP</i>
	Persiapan alat bantu (tools) pelatihan <ul style="list-style-type: none"> - Python (Jupyter) kenalkan dengan yang online; numpy, pandas, matplotlib, seaborn, folium - MySql (XAMPP) 	Pemaparan materi, diskusi dan <i>hands-on lab live class 1 JP</i>
	Menerapkan prinsip perlindungan informasi <ol style="list-style-type: none"> 1. Mendefinisikan prosedur keamanan informasi yang tepat untuk tiap klasifikasi 2. Mengidentifikasi kelemahan dari informasi dalam sistem komunikasi bisnis 3. Menerapkan akses kontrol lingkungan Komputasi yang sesuai 4. Mematuhi dan melaksanakan petunjuk yang terdapat pada dokumen yang diterbitkan khusus oleh pemerintah atau badan-badan resmi terkait untuk mengelola sistem operasi 5. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem. 	Pemaparan materi, diskusi dan <i>hands-on lab live class 2 JP</i>
	Menerapkan prinsip keamanan informasi untuk penggunaan jaringan internet <ol style="list-style-type: none"> 1. Mematuhi dan menerapkan kebijakan dan prosedur keamanan informasi yang terkait dengan penggunaan jaringan internet 2. Mengidentifikasi tipe kelemahan dan jenis-jenis serangan dalam jaringan internet 3. Mengaplikasikan penggunaan jaringan internet secara aman 	Pemaparan materi, diskusi dan <i>hands-on lab live class 3 JP</i>

Hari 2	Menerapkan prinsip keamanan informasi pada transaksi elektronik <ol style="list-style-type: none"> 1. Mengidentifikasi dan memenuhi kebutuhan terkait kerahasiaan, integritas, bukti dari pengguna dokumen kunci dan kontrak yang diakui 2. Menetapkan aspek-aspek transaksi 3. Melaksanakan dan memantau perlindungan keamanan untuk sistem infrastruktur dan penggunaan teknologi informasi sesuai dengan rencana implementasi dan prosedur operasi standar 	Pemaparan materi, diskusi dan <i>hands-on lab live class 3 JP</i>
	Melaksanakan kebijakan keamanan informasi <ol style="list-style-type: none"> 1. Mengidentifikasi aset penting dalam organisasi 2. Memproteksi aset penting dalam organisasi 3. Melakukan pemantauan terhadap aktivitas yang rentan ancaman 	Pemaparan materi, diskusi dan <i>hands-on lab live class 2 JP</i>
	Mengaplikasikan ketentuan/persyaratan keamanan informasi <ol style="list-style-type: none"> 1. Mengaplikasikan persyaratan untuk program yang spesifik untuk keamanan lingkungan komputasi guna mengidentifikasi kelemahan/kerentanan 2. Menyediakan masukan tentang hal yang terkait dengan persyaratan keamanan untuk dimasukkan dalam laporan pekerjaan dan dokumen-dokumen pengadaan terkait 3. Mengumpulkan dan memelihara data yang diperlukan untuk memenuhi persyaratan pelaporan keamanan sistem 4. Mengidentifikasi persyaratan keamanan dalam prosedur operasi di lingkungan komputasi 5. Menyusun persyaratan keamanan untuk perangkat keras, piranti lunak, dan penggunaan layanan yang spesifik 	Pemaparan materi, diskusi dan <i>hands-on lab live class 3 JP</i>

	<p>untuk program keamanan jaringan</p> <p>6. Mengevaluasi dan/atau menyetujui persyaratan keamanan yang relevan terhadap kemampuan teknologi informasi yang baru</p>	
Hari 3	<p>Mengelola <i>log</i></p> <ol style="list-style-type: none"> 1. Menetapkan kebijakan pencatatan <i>log</i> untuk menyertakan peristiwa penting 2. Melakukan kontrol berkas <i>log</i> terhadap kemungkinan diubah atau dihapus 3. Melakukan kontrol tempat menyimpan media file pencatatan terhadap kemungkinan penuh sehingga terjadi kegagalan ketika mencatat kejadian yang terjadi 	Pemaparan materi, diskusi dan <i>hands-on lab live class</i> 4 JP
	<p>Menerapkan kontrol akses berdasarkan konsep/metodologi yang telah ditetapkan</p> <ol style="list-style-type: none"> 1. Menerapkan kontrol akses lingkungan komputasi yang sesuai 2. Melaksanakan kebijakan organisasi dan kebijakan <i>password</i> organisasi 3. Mengelola akun hak jaringan dan hak akses ke sistem jaringan dan infrastrukturnya 4. Mengimplementasikan peringatan secara online untuk menginformasikan para pengguna atas peraturan akses dari seluruh infrastruktur dan penggunaan sistem teknologi informasi 5. Menyusun prosedur untuk memastikan pengguna sistem menyadari tanggung jawab keamanan mereka sebelum memberikan akses ke sistem informasi organisasi 6. Melakukan kontrol dan pengawasan pada setiap pengguna yang memiliki akses khusus menjalankan fungsi keamanan agar menerima pelatihan keamanan dasar dan berkelanjutan serta mendapatkan sertifikasi yang sesuai untuk melaksanakan tugas keamanan 	Pemaparan materi, diskusi dan <i>hands-on lab live class</i> 4 JP

Materi Pokok

- 5.1 Menetapkan kebijakan pencatatan *log* untuk menyertakan peristiwa penting
- 5.2 Melakukan kontrol berkas *log* terhadap kemungkinan diubah atau dihapus
- 5.3 Melakukan kontrol tempat menyimpan media file pencatatan terhadap kemungkinan penuh sehingga terjadi kegagalan ketika mencatat kejadian yang terjadi

Sub Materi Pokok

- 1.1. Prosedur dan kebijakan *log* dan pengarsipannya
- 1.2. Pencatatan Log ketika terjadi peristiwa penting dan jalannya layanan
- 1.3. Arsip *Log* dibuat
- 2.1. Pengendalian akses
- 2.2. Penerapan Backup *log*.
- 3.1. Penyediaan media penyimpanan file pencatatan
- 3.2. Penyediaan kapasitas disediakan agar mencegah terjadinya kegagalan.

5.1 MENETAPKAN KEBIJAKAN PENCATATAN LOG UNTUK MENYERTAKAN PERISTIWA PENTING

Menetapkan kebijakan pencatatan log yang mencakup peristiwa penting sangat penting dalam mengelola log. Berikut adalah beberapa langkah yang dapat dilakukan untuk menetapkan kebijakan pencatatan log:

1. Identifikasi peristiwa penting: Tentukan peristiwa penting yang harus dicatat dalam log, seperti serangan keamanan, penggunaan sumber daya penting, atau perubahan pada konfigurasi sistem.
2. Tentukan level log: Tentukan level log yang akan digunakan untuk setiap peristiwa penting. Level log yang umum digunakan adalah DEBUG, INFO, WARNING, ERROR, dan CRITICAL.

Level log adalah cara untuk mengkategorikan dan mengorganisir pesan log berdasarkan tingkat kepentingannya. Level log dapat membantu pengguna dalam mengelola dan memahami pesan log yang dihasilkan oleh suatu sistem atau aplikasi.

Beberapa contoh level log yang umum digunakan adalah sebagai berikut:

- a) DEBUG: level log yang digunakan untuk pesan log yang bersifat debugging atau pencarian kesalahan dalam suatu sistem atau aplikasi.
- b) INFO: level log yang digunakan untuk pesan log yang memberikan informasi tentang kejadian yang terjadi pada sistem atau aplikasi.
- c) WARNING: level log yang digunakan untuk pesan log yang memberikan peringatan tentang kejadian yang tidak diinginkan, tetapi tidak merusak sistem atau aplikasi.
- d) ERROR: level log yang digunakan untuk pesan log yang memberikan informasi tentang kejadian yang menyebabkan kesalahan dalam sistem atau aplikasi.

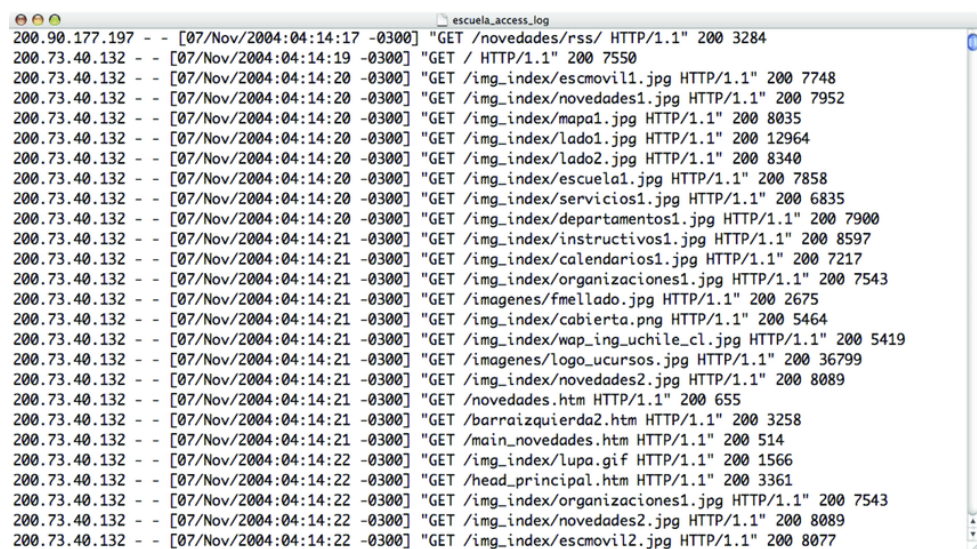
- e) **CRITICAL**: level log yang digunakan untuk pesan log yang memberikan informasi tentang kejadian yang sangat serius dan mengancam stabilitas sistem atau aplikasi. Setiap level log biasanya diidentifikasi dengan simbol atau kode tertentu, sehingga memudahkan pengguna dalam mengelola pesan log. Penting bagi pengguna untuk memahami level log yang digunakan oleh sistem atau aplikasi, sehingga dapat mengelola pesan log dengan lebih efektif dan efisien.
3. Tentukan format log: Tentukan format log yang akan digunakan untuk mencatat setiap peristiwa penting. Format log harus dapat mudah dibaca dan diproses oleh alat analisis log.
 4. Tentukan lokasi penyimpanan: Tentukan lokasi penyimpanan log. Pastikan bahwa lokasi penyimpanan aman dan dapat diakses oleh administrator jaringan.
 5. Tentukan kebijakan retensi: Tentukan kebijakan retensi untuk setiap jenis log. Pastikan bahwa log yang lebih penting disimpan untuk jangka waktu yang lebih lama.
 6. Pelajari aturan dan regulasi terkait: Pelajari aturan dan regulasi terkait yang mungkin berlaku untuk organisasi Anda. Pastikan kebijakan pencatatan log Anda memenuhi persyaratan tersebut.
 7. Implementasikan dan monitor kebijakan: Implementasikan kebijakan pencatatan log dan monitor secara teratur untuk memastikan bahwa semua peristiwa penting dicatat dan log aman dari peretasan atau manipulasi.

Contoh untuk mengetahui log web server, langkah-langkah yang perlu dilakukan tergantung pada jenis web server yang digunakan. Berikut adalah beberapa contoh langkah-langkah untuk mengetahui log web server pada beberapa jenis web server yang umum digunakan:

- a) **Apache**: Untuk mengetahui log di Apache, Anda dapat membuka file log yang dikonfigurasi di dalam file konfigurasi server Apache. Secara default, Apache menghasilkan dua jenis file log: `access.log` dan `error.log`. File `access.log` mencatat semua permintaan HTTP yang diterima oleh server Apache, sedangkan file `error.log` mencatat semua pesan kesalahan yang dihasilkan oleh server Apache. Lokasi file log biasanya ditemukan di direktori `/var/log/apache2/` pada sistem Linux atau `C:\xampp\apache\logs` pada sistem Windows jika menggunakan XAMPP. Apache adalah salah satu web server yang paling populer digunakan di seluruh dunia. Apache menyediakan dukungan untuk log file, yang memungkinkan server untuk mencatat semua aktivitas yang terjadi pada server web, seperti permintaan masuk, respons server, kesalahan, dan lain-lain. Berikut adalah cara membuat log di Apache:
 - i. Buka file konfigurasi Apache: Pertama-tama, buka file konfigurasi Apache di server Anda. File konfigurasi biasanya bernama `httpd.conf` atau `apache2.conf` dan dapat ditemukan di direktori instalasi Apache.
 - ii. Konfigurasi logging: Setelah membuka file konfigurasi Apache, cari bagian yang berkaitan dengan konfigurasi logging. Biasanya, bagian ini disebut dengan "Logging" atau "ErrorLog". Di sini, Anda dapat menentukan format logging, lokasi file log, dan tingkat logging yang diinginkan.
 - iii. Tentukan format logging: Apache mendukung banyak format logging, seperti Common Log Format (CLF), Combined Log Format, dan Extended Log Format.

Anda dapat memilih format logging yang paling sesuai dengan kebutuhan Anda.

- iv. Tentukan lokasi file log: Setelah menentukan format logging, tentukan lokasi file log. File log biasanya ditempatkan di direktori `/var/log/apache2/` pada sistem Linux atau di `C:\Program Files\Apache Group\Apache2\logs\` pada sistem Windows.
- v. Tentukan tingkat logging: Terakhir, tentukan tingkat logging yang diinginkan. Tingkat logging ini menentukan seberapa banyak informasi yang akan dicatat dalam file log. Beberapa tingkat logging yang umum digunakan antara lain "emerg" (darurat), "alert" (peringatan), "crit" (kritikal), "error" (kesalahan), "warn" (peringatan), "notice" (perhatian), "info" (informasi), dan "debug" (debugging).



```
200.90.177.197 - - [07/Nov/2004:04:14:17 -0300] "GET /novedades/rss/ HTTP/1.1" 200 3284
200.73.40.132 - - [07/Nov/2004:04:14:19 -0300] "GET / HTTP/1.1" 200 7550
200.73.40.132 - - [07/Nov/2004:04:14:20 -0300] "GET /img_index/escmovil1.jpg HTTP/1.1" 200 7748
200.73.40.132 - - [07/Nov/2004:04:14:20 -0300] "GET /img_index/novedades1.jpg HTTP/1.1" 200 7952
200.73.40.132 - - [07/Nov/2004:04:14:20 -0300] "GET /img_index/mapa1.jpg HTTP/1.1" 200 8035
200.73.40.132 - - [07/Nov/2004:04:14:20 -0300] "GET /img_index/lado1.jpg HTTP/1.1" 200 12964
200.73.40.132 - - [07/Nov/2004:04:14:20 -0300] "GET /img_index/lado2.jpg HTTP/1.1" 200 8340
200.73.40.132 - - [07/Nov/2004:04:14:20 -0300] "GET /img_index/escuela1.jpg HTTP/1.1" 200 7858
200.73.40.132 - - [07/Nov/2004:04:14:20 -0300] "GET /img_index/servicios1.jpg HTTP/1.1" 200 6835
200.73.40.132 - - [07/Nov/2004:04:14:20 -0300] "GET /img_index/departamentos1.jpg HTTP/1.1" 200 7900
200.73.40.132 - - [07/Nov/2004:04:14:21 -0300] "GET /img_index/instructivos1.jpg HTTP/1.1" 200 8597
200.73.40.132 - - [07/Nov/2004:04:14:21 -0300] "GET /img_index/calendarios1.jpg HTTP/1.1" 200 7217
200.73.40.132 - - [07/Nov/2004:04:14:21 -0300] "GET /img_index/organizaciones1.jpg HTTP/1.1" 200 7543
200.73.40.132 - - [07/Nov/2004:04:14:21 -0300] "GET /imagenes/fmellado.jpg HTTP/1.1" 200 2675
200.73.40.132 - - [07/Nov/2004:04:14:21 -0300] "GET /img_index/cabierta.png HTTP/1.1" 200 5464
200.73.40.132 - - [07/Nov/2004:04:14:21 -0300] "GET /img_index/wap_ing_uchile.cl.jpg HTTP/1.1" 200 5419
200.73.40.132 - - [07/Nov/2004:04:14:21 -0300] "GET /imagenes/logo_ucursos.jpg HTTP/1.1" 200 36799
200.73.40.132 - - [07/Nov/2004:04:14:21 -0300] "GET /img_index/novedades2.jpg HTTP/1.1" 200 8089
200.73.40.132 - - [07/Nov/2004:04:14:21 -0300] "GET /novedades.htm HTTP/1.1" 200 655
200.73.40.132 - - [07/Nov/2004:04:14:21 -0300] "GET /barraizquierda2.htm HTTP/1.1" 200 3258
200.73.40.132 - - [07/Nov/2004:04:14:21 -0300] "GET /main_novedades.htm HTTP/1.1" 200 514
200.73.40.132 - - [07/Nov/2004:04:14:22 -0300] "GET /img_index/lupa.gif HTTP/1.1" 200 1566
200.73.40.132 - - [07/Nov/2004:04:14:22 -0300] "GET /head_principal.htm HTTP/1.1" 200 3361
200.73.40.132 - - [07/Nov/2004:04:14:22 -0300] "GET /img_index/organizaciones1.jpg HTTP/1.1" 200 7543
200.73.40.132 - - [07/Nov/2004:04:14:22 -0300] "GET /img_index/novedades2.jpg HTTP/1.1" 200 8089
200.73.40.132 - - [07/Nov/2004:04:14:22 -0300] "GET /img_index/escmovil2.jpg HTTP/1.1" 200 8077
```

Setelah Anda melakukan konfigurasi logging, Apache akan mulai mencatat semua aktivitas pada server web dalam file log yang telah ditentukan. Anda dapat membuka file log tersebut dan menganalisisnya untuk mendapatkan informasi tentang permintaan masuk, respons server, kesalahan, dan lain-lain. Ini sangat berguna dalam mendiagnosis masalah pada server web dan meningkatkan kinerja server Anda

- b) Nginx: Untuk mengetahui log di Nginx, Anda dapat melihat file log yang telah dikonfigurasi di dalam file konfigurasi server Nginx. Secara default, Nginx menghasilkan dua jenis file log: `access.log` dan `error.log`. File `access.log` mencatat semua permintaan HTTP yang diterima oleh server Nginx, sedangkan file `error.log` mencatat semua pesan kesalahan yang dihasilkan oleh server Nginx. Lokasi file log biasanya ditemukan di direktori `/var/log/nginx/` pada sistem Linux.

Untuk mengetahui log di nginx, Anda dapat melihat file log yang telah dikonfigurasi di dalam konfigurasi server nginx. Secara default, nginx menghasilkan dua jenis file log: `access.log` dan `error.log`. File `access.log` mencatat semua permintaan HTTP yang diterima oleh server nginx, sedangkan file `error.log` mencatat semua pesan kesalahan yang dihasilkan oleh server nginx.

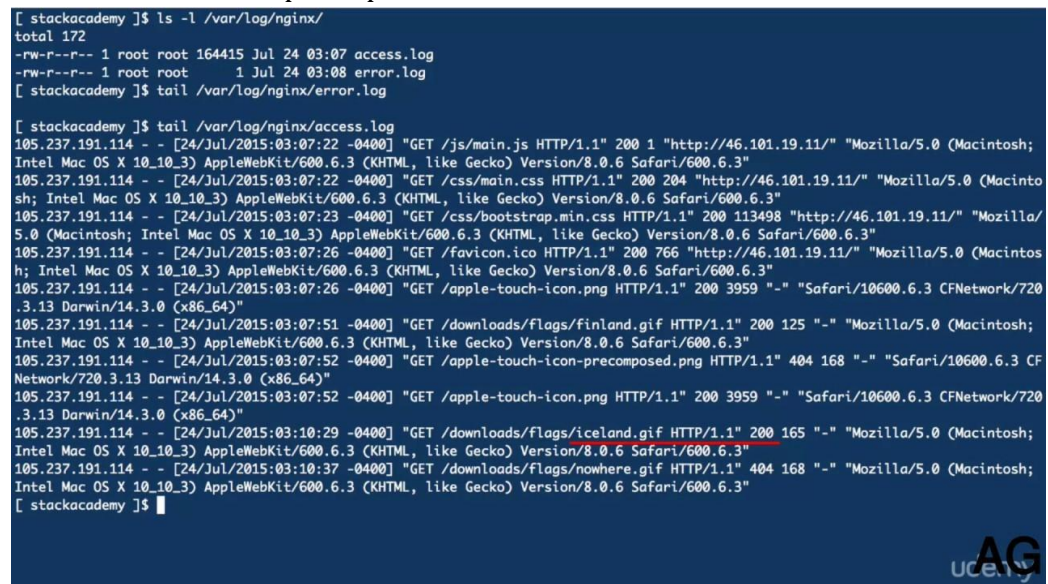
Untuk mengetahui lokasi file log nginx yang terkonfigurasi, Anda dapat membuka file konfigurasi nginx, biasanya ditemukan di direktori `/etc/nginx/`. Kemudian, cari blok `server {}` yang berisi konfigurasi server nginx, dan periksa bagian `access_log` dan `error_log`. Contoh konfigurasi log nginx seperti di bawah ini:

```
server {  
    listen 80;  
    server_name example.com;  
  
    access_log /var/log/nginx/access.log;  
    error_log /var/log/nginx/error.log;  
  
    # konfigurasi lainnya ...  
}
```

Dalam contoh ini, file `access log` dan `error log` dihasilkan di `/var/log/nginx/access.log` dan `/var/log/nginx/error.log`.

Setelah mengetahui lokasi file log, Anda dapat membuka file log tersebut untuk melihat informasi yang tercatat. Anda dapat menggunakan editor teks atau perangkat lunak analisis log khusus untuk menganalisis aktivitas pada server nginx. Beberapa informasi yang biasanya tercatat dalam file log nginx antara lain alamat IP pengunjung, metode permintaan HTTP, kode status HTTP, ukuran file yang ditransfer, dan waktu akses.

Dengan menganalisis file log nginx, Anda dapat memperoleh informasi yang berguna untuk menganalisis kinerja server, mengidentifikasi serangan keamanan, atau menemukan masalah pada aplikasi web Anda.



The screenshot shows a terminal window with the following commands and output:

```
[ stackacademy ]$ ls -l /var/log/nginx/  
total 172  
-rw-r--r-- 1 root root 164415 Jul 24 03:07 access.log  
-rw-r--r-- 1 root root      1 Jul 24 03:08 error.log  
[ stackacademy ]$ tail /var/log/nginx/error.log  
  
[ stackacademy ]$ tail /var/log/nginx/access.log  
105.237.191.114 - - [24/Jul/2015:03:07:22 -0400] "GET /js/main.js HTTP/1.1" 200 1 "http://46.101.19.11/" "Mozilla/5.0 (Macintosh;  
Intel Mac OS X 10_10_3) AppleWebKit/600.6.3 (KHTML, like Gecko) Version/8.0.6 Safari/600.6.3"  
105.237.191.114 - - [24/Jul/2015:03:07:22 -0400] "GET /css/main.css HTTP/1.1" 200 204 "http://46.101.19.11/" "Mozilla/5.0 (Macintosh;  
Intel Mac OS X 10_10_3) AppleWebKit/600.6.3 (KHTML, like Gecko) Version/8.0.6 Safari/600.6.3"  
105.237.191.114 - - [24/Jul/2015:03:07:23 -0400] "GET /css/bootstrap.min.css HTTP/1.1" 200 113498 "http://46.101.19.11/" "Mozilla/  
5.0 (Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/600.6.3 (KHTML, like Gecko) Version/8.0.6 Safari/600.6.3"  
105.237.191.114 - - [24/Jul/2015:03:07:26 -0400] "GET /favicon.ico HTTP/1.1" 200 766 "http://46.101.19.11/" "Mozilla/5.0 (Macintosh  
h; Intel Mac OS X 10_10_3) AppleWebKit/600.6.3 (KHTML, like Gecko) Version/8.0.6 Safari/600.6.3"  
105.237.191.114 - - [24/Jul/2015:03:07:26 -0400] "GET /apple-touch-icon.png HTTP/1.1" 200 3959 "-" "Safari/10600.6.3 CFNetwork/720  
.3.13 Darwin/14.3.0 (x86_64)"  
105.237.191.114 - - [24/Jul/2015:03:07:51 -0400] "GET /downloads/flags/finland.gif HTTP/1.1" 200 125 "-" "Mozilla/5.0 (Macintosh;  
Intel Mac OS X 10_10_3) AppleWebKit/600.6.3 (KHTML, like Gecko) Version/8.0.6 Safari/600.6.3"  
105.237.191.114 - - [24/Jul/2015:03:07:52 -0400] "GET /apple-touch-icon-precomposed.png HTTP/1.1" 404 168 "-" "Safari/10600.6.3 CF  
Network/720.3.13 Darwin/14.3.0 (x86_64)"  
105.237.191.114 - - [24/Jul/2015:03:07:52 -0400] "GET /apple-touch-icon.png HTTP/1.1" 200 3959 "-" "Safari/10600.6.3 CFNetwork/720  
.3.13 Darwin/14.3.0 (x86_64)"  
105.237.191.114 - - [24/Jul/2015:03:10:29 -0400] "GET /downloads/flags/iceland.gif HTTP/1.1" 200 165 "-" "Mozilla/5.0 (Macintosh;  
Intel Mac OS X 10_10_3) AppleWebKit/600.6.3 (KHTML, like Gecko) Version/8.0.6 Safari/600.6.3"  
105.237.191.114 - - [24/Jul/2015:03:10:37 -0400] "GET /downloads/flags/nowhere.gif HTTP/1.1" 404 168 "-" "Mozilla/5.0 (Macintosh;  
Intel Mac OS X 10_10_3) AppleWebKit/600.6.3 (KHTML, like Gecko) Version/8.0.6 Safari/600.6.3"  
[ stackacademy ]$
```

- c) IIS: Untuk mengetahui log di IIS, Anda dapat membuka console IIS Manager dan memeriksa properti situs web. Pada tab Logging, Anda dapat melihat lokasi file log dan konfigurasi lainnya. Secara default, IIS menghasilkan satu jenis file log: W3C Extended Log File Format. File log ini mencatat semua permintaan HTTP yang diterima oleh server IIS. Lokasi file log biasanya ditemukan di direktori `C:\inetpub\logs\LogFiles` pada sistem Windows.

```

216.239.46.60 - - [04/Jan/2003:14:56:50 +0200] "GET
/~lpis/curriculum/C+Unix/Ergastiria/Week-7/filetype.c.txt HTTP/1.0"
304 -
216.239.46.100 - - [04/Jan/2003:14:57:33 +0200] "GET
/~oswinds/top.html HTTP/1.0" 200 869
64.68.82.70 - - [04/Jan/2003:14:58:25 +0200] "GET /~lpis/systems/r-
device/r_device_examples.html HTTP/1.0" 200 16792
216.239.46.133 - - [04/Jan/2003:14:58:27 +0200] "GET
/~lpis/publications/crc-chapter1.html HTTP/1.0" 304 -
209.237.238.161 - - [04/Jan/2003:14:59:11 +0200] "GET /robots.txt
HTTP/1.0" 404 276
209.237.238.161 - - [04/Jan/2003:14:59:12 +0200] "GET
/teachers/pitas1.html HTTP/1.0" 404 286
216.239.46.43 - - [04/Jan/2003:14:59:45 +0200] "GET
/~oswinds/publications.html HTTP/1.0" 200 48966

```

Setelah mengetahui lokasi file log, Anda dapat membuka file log tersebut untuk melihat informasi yang tercatat. Anda dapat menggunakan editor teks atau perangkat lunak analisis log khusus untuk menganalisis aktivitas pada server web. Beberapa informasi yang biasanya tercatat dalam file log web server antara lain alamat IP pengunjung, metode permintaan HTTP, kode status HTTP, ukuran file yang ditransfer, dan waktu akses.

Dengan menganalisis file log web server, Anda dapat memperoleh informasi yang berguna untuk menganalisis kinerja server, mengidentifikasi serangan keamanan, atau menemukan masalah pada aplikasi web Anda.

1.1 Prosedur dan kebijakan log dan pengarsipannya.

"Prosedur dan kebijakan log dan pengarsipannya ditetapkan" mengindikasikan bahwa dalam sebuah organisasi atau perusahaan, sudah ada prosedur dan kebijakan yang telah ditetapkan untuk mengelola log dan pengarsipannya.

Prosedur dan kebijakan log dapat mencakup aturan dan praktik yang berkaitan dengan:

1. Jenis data apa yang harus dicatat di dalam log, seperti peristiwa keamanan, aktivitas pengguna, atau data sistem.
2. Level log yang harus digunakan untuk setiap jenis data, misalnya DEBUG, INFO, WARNING, ERROR, atau CRITICAL.
3. Format log yang harus digunakan, seperti format tanggal dan waktu, format pesan, dan format metadata.
4. Lokasi penyimpanan log, seperti direktori di dalam sistem file atau basis data log.
5. Kebijakan retensi log, yaitu berapa lama log harus disimpan sebelum dihapus atau diarsipkan.
6. Kebijakan keamanan log, termasuk pengamanan akses ke log, kontrol integritas, dan deteksi manipulasi log.

Pengarsipan log dapat mencakup praktik-praktik seperti backup rutin, pemantauan ketersediaan log, dan pengarsipan log dalam format yang terstruktur dan mudah diakses. Prosedur dan kebijakan log yang jelas dan terstruktur adalah bagian penting dari upaya pengelolaan risiko dan keamanan informasi yang efektif dalam sebuah organisasi.

1.2 Pencatatan Log pada ketika terjadi peristiwa penting dan jalannya layanan

"Log pencatatan peristiwa penting, layanan, dan proxy dibuat" mengindikasikan bahwa dalam sebuah sistem atau jaringan, sudah ada proses pencatatan atau logging yang dilakukan untuk peristiwa penting, layanan, dan proxy.

Pencatatan atau logging ini bertujuan untuk mencatat dan merekam semua aktivitas dan peristiwa yang terjadi pada sistem atau jaringan, termasuk peristiwa penting, layanan, dan proxy. Logging yang dilakukan secara teratur dan terstruktur dapat membantu dalam mendeteksi dan menganalisis masalah, mengamati trend aktivitas, dan memberikan bukti audit dalam kasus keamanan dan kebijakan.

Beberapa jenis peristiwa penting yang umumnya dicatat dalam log meliputi:

1. Upaya masuk yang gagal ke sistem atau jaringan.
2. Pencarian atau pengambilan data sensitif seperti password dan informasi identitas.
3. Pembaruan dan perubahan pada konfigurasi sistem atau jaringan.
4. Serangan dan ancaman keamanan seperti serangan DDoS atau serangan malware.
5. Aktivitas pengguna yang tidak biasa seperti penggunaan terlalu banyak sumber daya atau akses ke area yang tidak diperlukan.

Sementara itu, pencatatan layanan dan proxy mencakup pencatatan aktivitas yang terkait dengan layanan atau proxy yang digunakan dalam sistem atau jaringan, seperti aktivitas email, web, atau protokol lainnya.

Dalam membangun pencatatan atau logging ini, organisasi harus memperhatikan kebijakan dan prosedur yang telah ditetapkan sebelumnya untuk menentukan jenis data apa yang harus dicatat dan level log yang harus digunakan untuk setiap jenis data. Hal ini akan membantu menghindari pencatatan yang tidak perlu dan memastikan log dapat diakses dan dianalisis dengan mudah. Selain itu, organisasi harus menentukan lokasi penyimpanan log dan kebijakan retensi untuk memastikan log tersedia dalam jangka waktu yang cukup lama dan dapat diakses dengan mudah ketika diperlukan.

1.3 Arsip log dibuat

Setelah log dicatat, selanjutnya log tersebut perlu diarsipkan agar dapat dimanfaatkan untuk kepentingan pengelolaan keamanan informasi di masa depan. Untuk itu, beberapa langkah yang dapat dilakukan dalam membuat arsip log antara lain:

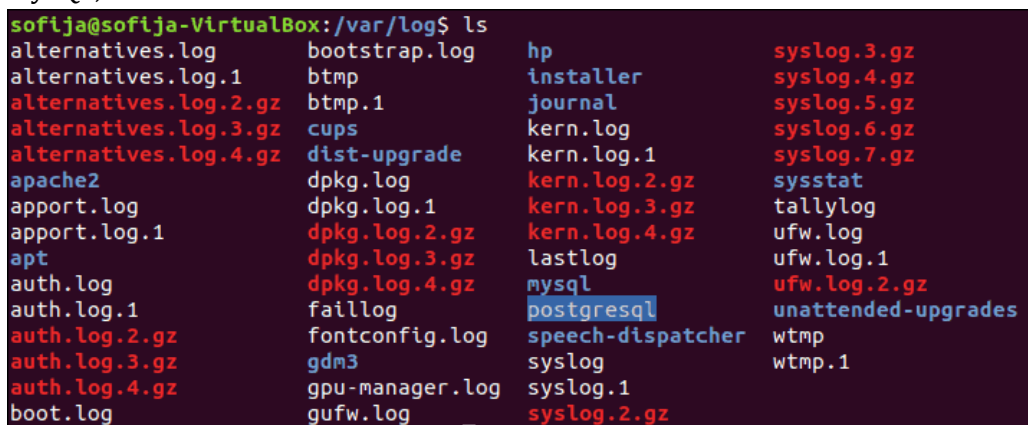
1. Menentukan rentang waktu arsip log: Untuk memastikan bahwa arsip log terbuat dengan benar, Anda perlu menentukan periode waktu yang akan diarsipkan. Waktu yang tepat tergantung pada kebutuhan organisasi, tetapi umumnya rentang waktu yang disarankan adalah minimal 1 tahun.
2. Memilih tempat penyimpanan yang tepat: Pilih tempat penyimpanan yang aman dan terlindungi untuk log arsip, seperti server jarak jauh, backup cloud, atau media penyimpanan fisik seperti hard disk atau flash drive yang disimpan di tempat yang aman.
3. Membuat format arsip yang terstruktur: Untuk memudahkan pengelolaan log arsip, Anda perlu membuat format yang terstruktur. Format ini dapat mencakup informasi seperti tanggal dan waktu, jenis peristiwa, lokasi, dan rincian lainnya yang terkait dengan peristiwa yang tercatat.
4. Membuat prosedur pemulihan log: Ketika terjadi insiden keamanan, log arsip dapat membantu dalam investigasi dan analisis. Pastikan bahwa prosedur yang jelas dan terstruktur tersedia untuk pemulihan log yang diperlukan.

5. Mengatur akses: Terakhir, pastikan bahwa hanya orang yang memenuhi syarat dan memiliki hak akses yang tepat yang dapat mengakses log arsip. Ini dapat membantu memastikan bahwa log terlindungi dari manipulasi atau penghapusan yang tidak sah.

- **Sistem Logging di Linux**

Linux memiliki sistem logging yang kuat yang memungkinkan pengguna untuk mencatat semua aktivitas pada sistem, termasuk pesan sistem, pesan kernel, dan aktivitas aplikasi. Berikut adalah beberapa cara untuk membuat log di Linux:

- a. Syslog: Syslog adalah sistem logging bawaan pada sistem Linux yang mencatat semua pesan sistem dan kernel ke dalam file log. File log biasanya disimpan di direktori `/var/log/` dan diberi nama sesuai dengan jenis pesan, misalnya `messages`, `kern.log`, atau `auth.log`. Anda dapat memeriksa file log ini untuk melacak masalah sistem, seperti kegagalan boot, kegagalan jaringan, dan lain-lain.
- b. Daemon logging: Banyak daemon atau aplikasi di Linux memiliki sistem logging mereka sendiri, yang memungkinkan pengguna untuk mencatat aktivitas aplikasi ke dalam file log. Beberapa daemon logging populer yang digunakan di Linux antara lain `syslog-ng`, `rsyslog`, dan `logrotate`. Anda dapat menggunakan daemon logging ini untuk mencatat aktivitas aplikasi, misalnya web server, database, atau aplikasi lainnya.
- c. Log file konfigurasi: Banyak aplikasi di Linux menyimpan konfigurasi mereka dalam file log khusus, yang mencatat aktivitas konfigurasi pada sistem. File log konfigurasi ini sering digunakan dalam debugging masalah konfigurasi atau untuk melacak aktivitas administrator pada sistem. Beberapa contoh file log konfigurasi di Linux antara lain `/var/log/auth.log` untuk logging autentikasi, `/var/log/syslog` untuk logging sistem, dan `/var/log/dmccg` untuk logging kernel.
- d. Aplikasi logging: Banyak aplikasi di Linux memungkinkan pengguna untuk mencatat aktivitas aplikasi ke dalam file log khusus. Anda dapat menggunakan aplikasi logging ini untuk menganalisis aktivitas aplikasi dan mendiagnosis masalah pada aplikasi. Beberapa aplikasi logging yang umum digunakan di Linux antara lain Apache, MySQL, dan Postfix.



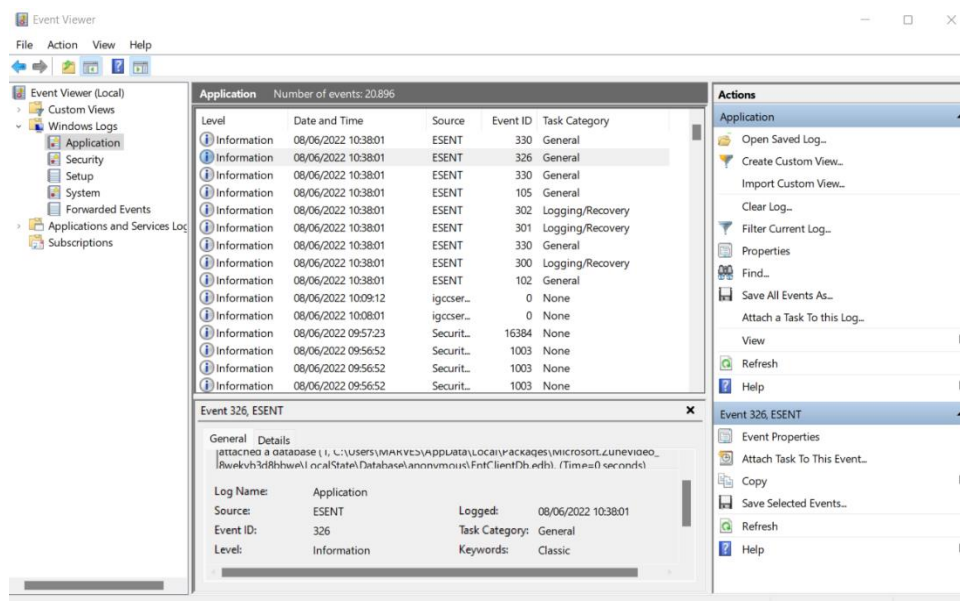
```
sofi@sofi-VirtualBox: /var/log$ ls
alternatives.log      bootstrap.log          hp                     syslog.3.gz
alternatives.log.1    btmp                  installer              syslog.4.gz
alternatives.log.2.gz btmp.1                journal                syslog.5.gz
alternatives.log.3.gz cups                   kern.log               syslog.6.gz
alternatives.log.4.gz dist-upgrade           kern.log.1             syslog.7.gz
apache2               dpkg.log              kern.log.2.gz          sysstat
apport.log            dpkg.log.1            kern.log.3.gz          tallylog
apport.log.1          dpkg.log.2.gz         kern.log.4.gz          ufw.log
apt                   dpkg.log.3.gz         lastlog                ufw.log.1
auth.log              dpkg.log.4.gz         mysql                  ufw.log.2.gz
auth.log.1            faillog               postgresql              unattended-upgrades
auth.log.2.gz         fontconfig.log        speech-dispatcher      wtmp
auth.log.3.gz         gdm3                  syslog                 wtmp.1
auth.log.4.gz         gpu-manager.log       syslog.1
boot.log              gufw.log              syslog.2.gz
```

Dalam semua kasus di atas, file log biasanya ditempatkan di direktori `/var/log/` pada sistem Linux. Anda dapat membuka file log ini dengan editor teks atau perangkat lunak analisis log khusus untuk menganalisis aktivitas sistem dan aplikasi pada sistem Linux Anda.

- **Sistem Login di Windows**

Untuk melakukan analisis log di Windows, Anda dapat menggunakan alat bawaan seperti Event Viewer dan PowerShell. Berikut adalah beberapa langkah yang dapat dilakukan untuk melakukan analisis log di Windows:

- Buka Event Viewer: Event Viewer adalah alat bawaan Windows yang digunakan untuk melihat log sistem, aplikasi, keamanan, dan banyak lagi. Anda dapat membuka Event Viewer dengan cara menekan tombol Windows + R pada keyboard, lalu ketik "eventvwr.msc" dan tekan Enter.
- Pilih log yang ingin dianalisis: Setelah membuka Event Viewer, pilih log yang ingin dianalisis. Misalnya, jika Anda ingin menganalisis log aplikasi, klik pada bagian "Windows Logs" dan pilih "Application".
- Analisis informasi log: Setelah memilih log, Anda dapat melihat informasi log seperti tanggal dan waktu kejadian, sumber, ID acara, dan deskripsi. Anda dapat menggunakan informasi ini untuk menganalisis masalah pada sistem atau aplikasi.
- Filter log: Anda dapat menggunakan fitur filter pada Event Viewer untuk mencari informasi log tertentu. Misalnya, jika Anda ingin mencari log yang berhubungan dengan suatu aplikasi tertentu, Anda dapat memfilter log dengan nama aplikasi tersebut.



Selain Event Viewer, Anda juga dapat menggunakan PowerShell untuk melakukan analisis log di Windows. PowerShell adalah bahasa scripting yang kuat yang digunakan untuk mengotomatisasi tugas di Windows. Anda dapat menggunakan PowerShell untuk membaca dan menganalisis log Windows dengan lebih mudah.

Berikut adalah contoh cmdlet PowerShell untuk membaca log keamanan di Windows:

```
powershell
```

```
Get-EventLog -LogName Security | Select-Object EventID, TimeGenerated, Message
```

Cmdlet ini akan membaca log keamanan pada Windows dan menampilkan ID acara, waktu kejadian, dan pesan log. Anda dapat menggunakan cmdlet PowerShell ini untuk menganalisis log Windows dengan lebih mudah dan efisien.

5.2 MELAKUKAN KONTROL BERKAS LOG TERHADAP KEMUNGKINAN DIUBAH ATAU DIHAPUS

Untuk melaksanakan kontrol berkas log terhadap kemungkinan diubah atau dihapus, dapat dilakukan beberapa tindakan berikut:

1. Memastikan bahwa hak akses ke berkas log hanya diberikan pada orang-orang yang membutuhkannya. Hal ini dapat dilakukan dengan memberikan hak akses yang sesuai berdasarkan tingkat kebutuhan dan tanggung jawab masing-masing pengguna.
2. Memantau perubahan berkas log secara berkala dengan menggunakan perangkat lunak pemantauan log. Perangkat lunak tersebut dapat memberikan notifikasi jika terdapat perubahan pada berkas log.
3. Menetapkan kebijakan yang jelas terkait dengan penyimpanan dan penghapusan berkas log. Kebijakan tersebut harus mencakup kapan berkas log akan disimpan, bagaimana cara menyimpannya, dan siapa yang berwenang untuk menghapusnya.
4. Menggunakan teknologi keamanan yang dapat memastikan keaslian dan integritas berkas log. Contohnya, menggunakan hash atau tanda tangan digital untuk mengidentifikasi perubahan atau manipulasi berkas log.
5. Melakukan backup secara teratur untuk memastikan bahwa data log tetap tersedia dalam keadaan darurat dan untuk menghindari kehilangan data karena kegagalan perangkat keras atau bencana lainnya.

Dengan melakukan tindakan-tindakan tersebut, dapat membantu dalam mencegah perubahan atau penghapusan berkas log yang tidak sah dan memastikan data log tetap tersedia dan dapat dipercaya.

2.1 Pengendalian akses

Kendali akses adalah suatu mekanisme yang digunakan untuk membatasi akses ke sumber daya atau informasi tertentu, seperti file, folder, sistem, atau jaringan. Implementasi kendali akses dapat dilakukan dengan beberapa cara, di antaranya:

1. Sistem otentikasi: Sistem otentikasi adalah metode untuk memverifikasi identitas pengguna yang mencoba mengakses sumber daya atau informasi tertentu. Contohnya, pengguna dapat diminta untuk memasukkan nama pengguna dan kata sandi atau menggunakan otentikasi dua faktor seperti penggunaan token.
2. Izin akses: Izin akses menentukan jenis akses yang diizinkan atau tidak diizinkan oleh pengguna pada sumber daya atau informasi tertentu. Misalnya, pengguna hanya diizinkan untuk membaca, menulis, atau mengedit sumber daya tertentu, tergantung pada peran dan tanggung jawabnya.
3. Kelompok akses: Kelompok akses adalah kelompok pengguna atau peran yang memiliki hak akses yang sama terhadap sumber daya atau informasi tertentu. Kelompok ini memudahkan administrator untuk mengatur hak akses dan memastikan bahwa pengguna hanya memiliki akses sesuai dengan perannya.
4. Audit: Audit adalah proses memeriksa aktivitas pengguna yang telah mengakses sumber daya atau informasi tertentu. Ini membantu administrator untuk memastikan bahwa pengguna hanya melakukan aktivitas yang diizinkan dan mengidentifikasi pelanggaran kebijakan.

Implementasi kendali akses dapat dilakukan dengan menggunakan perangkat lunak khusus, seperti sistem manajemen hak akses atau sistem manajemen identitas dan akses. Selain itu, kebijakan keamanan yang jelas dan diterapkan dengan konsisten juga dapat membantu dalam implementasi kendali akses.

2.2 Penerapan backup log

Backup log adalah proses membuat salinan data log ke dalam media yang berbeda sebagai tindakan pencegahan terhadap hilangnya atau rusaknya log data. Implementasi backup log dapat dilakukan dengan beberapa langkah berikut:

1. Identifikasi jenis data log: Pertama-tama, identifikasi jenis data log yang perlu dicadangkan. Ini bisa meliputi log sistem operasi, log database, log jaringan, atau log aplikasi.
2. Pilih jenis media cadangan: Pilih jenis media cadangan yang cocok untuk jenis data log yang akan dicadangkan. Media cadangan yang umum digunakan antara lain kaset tape, hard disk eksternal, cloud storage, atau server cadangan.
3. Tentukan jadwal backup: Tentukan jadwal backup yang sesuai dengan kebutuhan bisnis dan tingkat risiko kehilangan data log. Backup dapat dilakukan setiap hari, setiap minggu, atau setiap bulan.
4. Tentukan metode backup: Pilih metode backup yang cocok untuk jenis data log yang akan dicadangkan. Metode backup yang umum digunakan meliputi backup lengkap, backup diferensial, dan backup inkremental.
5. Uji kembali proses backup: Uji kembali proses backup secara berkala untuk memastikan bahwa proses backup berjalan dengan baik dan data log dapat dipulihkan dengan benar jika diperlukan.
6. Simpan cadangan di tempat yang aman: Pastikan untuk menyimpan cadangan di tempat yang aman dan terlindungi dari kerusakan atau kehilangan, seperti brankas atau ruang server yang aman.

Dalam mengimplementasikan backup log, penting untuk memiliki kebijakan backup dan pemulihan data yang jelas, serta melakukan pelatihan kepada staf IT tentang proses backup dan pemulihan data. Selain itu, proses backup dan pemulihan data juga harus diuji secara berkala untuk memastikan bahwa data log dapat dipulihkan dengan cepat dan benar jika terjadi kehilangan data.

5.3 MELAKUKAN KONTROL TEMPAT MENYIMPAN MEDIA FILE PENCATATAN TERHADAP KEMUNGKINAN

Kontrol tempat penyimpanan media file pencatatan sangat penting untuk menjaga keamanan dan integritas data log. Beberapa langkah yang dapat dilakukan untuk mengontrol tempat penyimpanan media file pencatatan adalah sebagai berikut:

1. Identifikasi jenis media file pencatatan: Pertama-tama, identifikasi jenis media file pencatatan yang perlu disimpan, seperti hard disk, flash disk, CD/DVD, atau kaset tape.
2. Batasi akses ke tempat penyimpanan: Batasi akses ke tempat penyimpanan hanya kepada staf IT atau orang yang memiliki otorisasi akses yang sesuai. Hal ini dapat dilakukan dengan memberikan akses fisik yang terbatas atau dengan menggunakan teknologi akses yang lebih canggih seperti penggunaan kartu pintar atau biometrik.
3. Lakukan pengawasan secara berkala: Lakukan pengawasan secara berkala terhadap tempat penyimpanan media file pencatatan untuk memastikan keamanan dan integritas data log. Pastikan bahwa semua media file pencatatan masih ada, tidak ada media yang rusak atau hilang, dan tidak ada tanda-tanda manipulasi.

4. Simpan media file pencatatan di tempat yang aman: Pastikan untuk menyimpan media file pencatatan di tempat yang aman dan terlindungi dari kerusakan atau kehilangan, seperti brankas atau ruang server yang aman.
5. Lakukan backup media file pencatatan secara berkala: Lakukan backup media file pencatatan secara berkala untuk mengantisipasi kemungkinan kehilangan data log. Simpan backup di tempat yang berbeda dan terlindungi dari bencana alam atau kejadian yang tidak terduga.
6. Buat kebijakan penggunaan media file pencatatan: Buat kebijakan yang jelas tentang penggunaan media file pencatatan, termasuk jenis media yang diizinkan dan cara penggunaan yang benar. Selain itu, pastikan bahwa semua staf IT memahami dan mengikuti kebijakan ini.

Dengan melakukan kontrol tempat penyimpanan media file pencatatan yang tepat, perusahaan dapat memastikan keamanan dan integritas data log. Hal ini akan membantu menghindari kemungkinan kehilangan data log dan memastikan bahwa data log dapat dipulihkan dengan cepat dan benar jika terjadi masalah.

3.1 Penyediaan media penyimpanan file pencatatan

Sebelum memilih media penyimpanan untuk file pencatatan, perlu dilakukan analisis kebutuhan kapasitas untuk memastikan bahwa media yang dipilih dapat menampung data log dalam jangka waktu yang cukup lama dan dapat memenuhi kebutuhan bisnis. Berikut adalah beberapa langkah untuk melakukan analisis kebutuhan kapasitas media penyimpanan file pencatatan:

1. Identifikasi jenis file pencatatan: Identifikasi jenis file pencatatan yang akan disimpan, seperti log sistem operasi, log database, atau log aplikasi. Setiap jenis file pencatatan memiliki karakteristik dan pola penggunaan yang berbeda, sehingga mempengaruhi kebutuhan kapasitas.
2. Perkiraan volume data: Perkiraan volume data yang akan dihasilkan oleh file pencatatan dalam jangka waktu tertentu, seperti sehari, seminggu, atau sebulan. Perkiraan dengan mempertimbangkan aktivitas bisnis, volume transaksi, dan pola penggunaan sistem.
3. Hitung kebutuhan kapasitas: Hitung kebutuhan kapasitas media penyimpanan berdasarkan volume data yang diperkirakan dan waktu penyimpanan yang diinginkan. Pastikan untuk memperhitungkan juga cadangan dan retensi data yang mungkin diperlukan.
4. Pilih media penyimpanan yang sesuai: Pilih media penyimpanan yang sesuai dengan kebutuhan kapasitas yang telah dihitung. Ada banyak jenis media penyimpanan yang tersedia, seperti hard disk, solid-state drive, kaset tape, atau cloud storage. Pastikan untuk memilih media yang dapat menampung data log dalam jangka waktu yang cukup lama dan dapat memenuhi kebutuhan bisnis.
5. Pertimbangkan faktor lain: Selain kapasitas, pertimbangkan juga faktor lain seperti kecepatan transfer data, kehandalan, dan biaya. Pastikan bahwa media penyimpanan yang dipilih dapat memenuhi semua persyaratan bisnis dan memiliki nilai ekonomi yang sesuai.

Dengan melakukan analisis kebutuhan kapasitas media penyimpanan file pencatatan, perusahaan dapat memilih media yang tepat untuk menyimpan data log. Hal ini akan

membantu memastikan bahwa data log dapat disimpan dengan aman dan dapat dipulihkan dengan cepat dan benar jika terjadi masalah.

3.2 Penyediaan kapasitas disediakan agar mencegah terjadinya kegagalan.

Alokasi kapasitas yang tepat sangat penting untuk mencegah terjadinya kegagalan dalam penyimpanan file pencatatan. Dalam melakukan alokasi kapasitas, perlu memperhitungkan beberapa hal, di antaranya:

1. Kapasitas yang cukup: Pastikan bahwa kapasitas media penyimpanan yang dipilih memiliki kapasitas yang cukup untuk menampung semua file pencatatan yang dihasilkan dalam jangka waktu yang diinginkan. Alokasikan kapasitas yang lebih besar daripada perkiraan kebutuhan untuk memberikan ruang yang cukup untuk pertumbuhan data di masa depan.
2. Partisi dan drive terpisah: Pastikan bahwa file pencatatan disimpan pada partisi dan drive terpisah dari sistem operasi, program aplikasi, dan data bisnis lainnya. Ini akan mencegah kegagalan pada satu partisi atau drive mempengaruhi penyimpanan file pencatatan.
3. Redundansi: Pertimbangkan untuk menggunakan sistem redundansi seperti RAID (Redundant Array of Independent Disks) untuk memastikan keandalan penyimpanan data. RAID memungkinkan data disimpan di beberapa hard disk yang berbeda sehingga jika satu hard disk mengalami kerusakan, data masih dapat diakses dan dipulihkan.
4. Cadangan dan retensi: Pastikan bahwa cadangan dan retensi data telah dihitung dalam alokasi kapasitas. Pastikan bahwa ada ruang yang cukup di media penyimpanan untuk menyimpan cadangan dan retensi data.
5. Kebutuhan bisnis: Pertimbangkan kebutuhan bisnis saat melakukan alokasi kapasitas. Beberapa bisnis mungkin memerlukan penyimpanan file pencatatan yang lebih lama dan lebih banyak daripada yang diwajibkan oleh regulasi atau standar industri. Pastikan alokasi kapasitas memenuhi kebutuhan bisnis.

Dengan melakukan alokasi kapasitas yang tepat, perusahaan dapat mencegah terjadinya kegagalan dalam penyimpanan file pencatatan. Hal ini akan membantu memastikan keamanan dan integritas data log, dan memungkinkan perusahaan untuk mengakses dan memulihkan data log dengan cepat dan benar jika terjadi masalah.

Contoh perangkat lunak yang dapat digunakan untuk menganalisis file log :

Ada beberapa perangkat lunak analisis log yang dapat digunakan untuk menganalisis file log web server. Beberapa perangkat lunak tersebut gratis dan terbuka untuk umum, sementara yang lainnya berbayar dan memiliki fitur yang lebih lengkap. Berikut adalah beberapa perangkat lunak analisis log gratis yang dapat digunakan untuk analisis log web server dengan fitur yang dasar:

- a) Awstats: Awstats adalah perangkat lunak analisis log web server yang gratis dan terbuka untuk umum. Awstats dapat digunakan untuk menganalisis file log dari server web Apache, Nginx, dan IIS. Fitur yang ditawarkan oleh Awstats antara lain grafik dan tabel statistik tentang jumlah pengunjung, halaman yang paling banyak dilihat, kata kunci pencarian, dan informasi lainnya.
- b) Webalizer: Webalizer adalah perangkat lunak analisis log web server yang juga gratis dan terbuka untuk umum. Webalizer dapat digunakan untuk menganalisis file log dari server web Apache, Nginx, dan IIS. Fitur yang ditawarkan oleh Webalizer antara lain

grafik dan tabel statistik tentang jumlah pengunjung, halaman yang paling banyak dilihat, kata kunci pencarian, dan informasi lainnya.

- c) Analog: Analog adalah perangkat lunak analisis log web server yang juga gratis dan terbuka untuk umum. Analog dapat digunakan untuk menganalisis file log dari server web Apache, Nginx, dan IIS. Fitur yang ditawarkan oleh Analog antara lain grafik dan tabel statistik tentang jumlah pengunjung, halaman yang paling banyak dilihat, kata kunci pencarian, dan informasi lainnya.
- d) GoAccess: GoAccess adalah perangkat lunak analisis log web server yang gratis dan terbuka untuk umum. GoAccess dapat digunakan untuk menganalisis file log dari server web Apache, Nginx, dan IIS. Fitur yang ditawarkan oleh GoAccess antara lain tampilan real-time dan grafik interaktif yang memudahkan pengguna untuk memantau aktivitas pada server web.

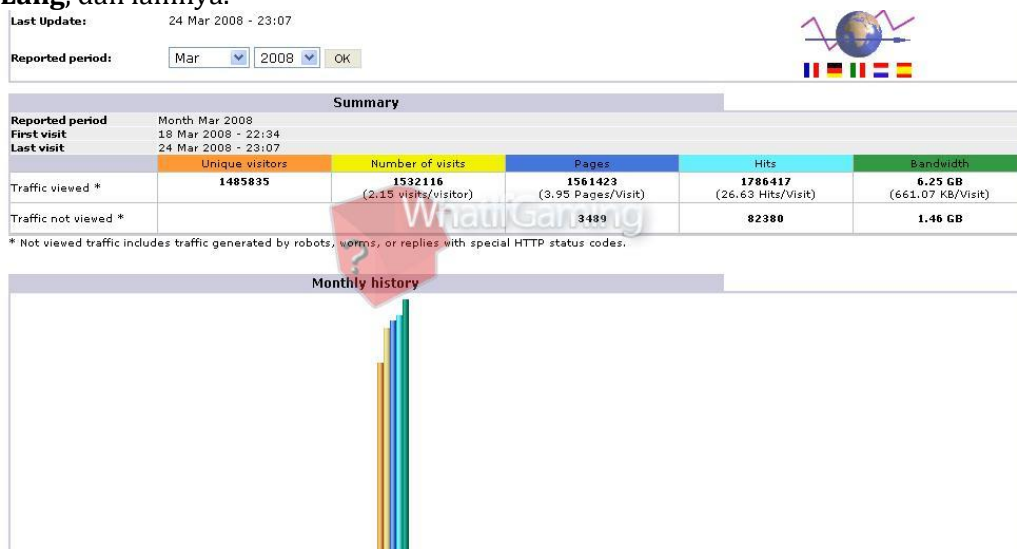
Dengan menggunakan perangkat lunak analisis log web server yang tepat, Anda dapat dengan mudah menganalisis file log web server dan mendapatkan wawasan yang lebih dalam tentang kinerja server, pengunjung, dan masalah keamanan.

Latihan Praktikum

Instalasi dan penggunaan menggunakan Perangkat Lunak Awstats :

Berikut adalah langkah-langkah cara menggunakan Awstats untuk menganalisis file log web server:

1. Pastikan Awstats sudah terpasang di server web. Jika belum terpasang, Anda dapat menginstalnya dengan perintah di terminal: **sudo apt-get install awstats** (untuk server web dengan OS Linux Debian atau Ubuntu).
2. Setelah Awstats terpasang, buka file konfigurasi awstats.conf dengan perintah **sudo nano /etc/awstats/awstats.conf** (untuk server web dengan OS Linux Debian atau Ubuntu). Pada file konfigurasi ini, pastikan sudah terdapat baris **LogFile="/var/log/apache2/access.log"** (atau alamat file log lainnya yang ingin Anda analisis).
3. Buka halaman web untuk Awstats dengan membuka browser dan memasukkan alamat URL **http://localhost/cgi-bin/awstats.pl**. Jika ingin mengakses dari jaringan lokal, ganti **localhost** dengan alamat IP server web.
4. Pilih situs web yang ingin Anda analisis dari daftar situs web yang ada di Awstats. Jika belum ada, tambahkan dengan menekan tombol **Add a new config file**.
5. Setelah memilih situs web, Anda akan melihat berbagai statistik tentang pengunjung dan aktivitas di situs web tersebut. Beberapa contoh statistik yang disediakan oleh Awstats antara lain jumlah pengunjung, halaman yang paling banyak dilihat, kata kunci pencarian, negara pengunjung, dan informasi lainnya.
6. Untuk mengubah tampilan statistik atau konfigurasi Awstats, Anda dapat mengedit file konfigurasi awstats.conf dengan perintah **sudo nano /etc/awstats/awstats.conf** dan mengubah nilai pada berbagai parameter seperti **ShowSummary**, **ShowLinksOnUrl**, **Lang**, dan lainnya.



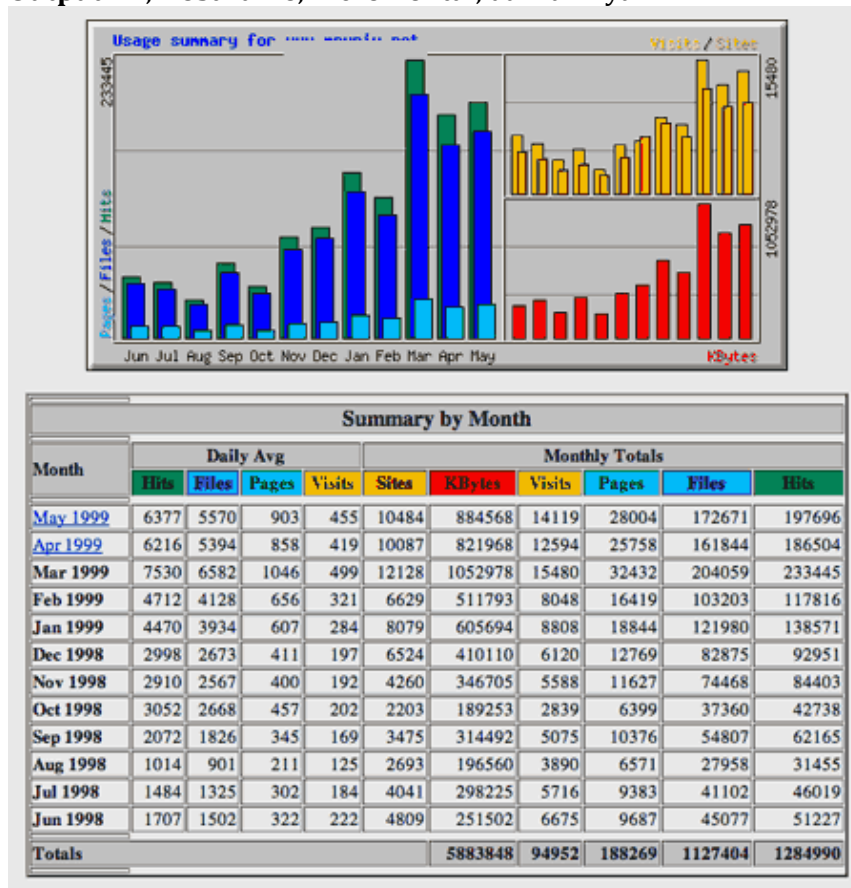
Dengan menggunakan Awstats, Anda dapat dengan mudah menganalisis file log web server dan mendapatkan wawasan yang lebih dalam tentang kinerja server, pengunjung, dan masalah keamanan.

Instalasi dan penggunaan menggunakan Perangkat Lunak Webalizer :

Berikut adalah langkah-langkah cara menggunakan Webalizer untuk menganalisis file log web server:

1. Pastikan Webalizer sudah terpasang di server web. Jika belum terpasang, Anda dapat menginstalnya dengan perintah di terminal: **sudo apt-get install webalizer** (untuk server web dengan OS Linux Debian atau Ubuntu).

- Setelah Webalizer terpasang, buka file konfigurasi webalizer.conf dengan perintah **sudo nano /etc/webalizer/webalizer.conf** (untuk server web dengan OS Linux Debian atau Ubuntu). Pada file konfigurasi ini, pastikan sudah terdapat baris **LogFile="/var/log/apache2/access.log"** (atau alamat file log lainnya yang ingin Anda analisis).
- Buka halaman web untuk Webalizer dengan membuka browser dan memasukkan alamat URL **http://localhost/webalizer** atau **http://localhost/cgi-bin/webalizer** (tergantung konfigurasi server web Anda). Jika ingin mengakses dari jaringan lokal, ganti **localhost** dengan alamat IP server web.
- Pilih situs web yang ingin Anda analisis dari daftar situs web yang ada di Webalizer. Jika belum ada, tambahkan dengan menekan tombol **Add new webalizer page**.
- Setelah memilih situs web, Anda akan melihat berbagai statistik tentang pengunjung dan aktivitas di situs web tersebut. Beberapa contoh statistik yang disediakan oleh Webalizer antara lain jumlah pengunjung, halaman yang paling banyak dilihat, kata kunci pencarian, negara pengunjung, dan informasi lainnya.
- Untuk mengubah tampilan statistik atau konfigurasi Webalizer, Anda dapat mengedit file konfigurasi webalizer.conf dengan perintah **sudo nano /etc/webalizer/webalizer.conf** dan mengubah nilai pada berbagai parameter seperti **OutputDir**, **HostName**, **Incremental**, dan lainnya.



Dengan menggunakan Webalizer, Anda dapat dengan mudah menganalisis file log web server dan mendapatkan wawasan yang lebih dalam tentang kinerja server, pengunjung, dan masalah keamanan.

Instalasi dan penggunaan menggunakan Perangkat Lunak Analog :

Berikut adalah langkah-langkah cara menggunakan Analog untuk menganalisis file log web server:

1. Pastikan Analog sudah terpasang di server web. Jika belum terpasang, Anda dapat menginstalnya dengan perintah di terminal: **sudo apt-get install analog** (untuk server web dengan OS Linux Debian atau Ubuntu).
2. Setelah Analog terpasang, buka file konfigurasi **analog.cfg** dengan perintah **sudo nano /etc/analog.cfg** (untuk server web dengan OS Linux Debian atau Ubuntu). Pada file konfigurasi ini, pastikan sudah terdapat baris **Logfile /var/log/apache2/access.log** (atau alamat file log lainnya yang ingin Anda analisis).
3. Jalankan Analog dengan perintah **analog** di terminal. Analog akan memproses file log web server dan menghasilkan file laporan dengan nama **analog_report.html** di direktori kerja saat ini.
4. Buka file laporan **analog_report.html** dengan browser web. Laporan ini akan menampilkan berbagai statistik tentang pengunjung dan aktivitas di situs web yang telah Anda analisis.
5. Beberapa statistik yang disediakan oleh Analog antara lain jumlah pengunjung, halaman yang paling banyak dilihat, kata kunci pencarian, negara pengunjung, dan informasi lainnya. Anda dapat mengubah tampilan statistik dengan mengedit file konfigurasi **analog.cfg** dan mengubah nilai pada berbagai parameter seperti **HOSTNAME, LOGFILE, LANGUAGE**, dan lainnya.

Dengan menggunakan Analog, Anda dapat dengan mudah menganalisis file log web server dan mendapatkan wawasan yang lebih dalam tentang kinerja server, pengunjung, dan masalah keamanan.

A. Pengetahuan yang diperlukan untuk dapat mengelola log

1. Jenis log: Anda perlu memahami jenis log yang ingin Anda kelola, seperti log sistem, log keamanan, log jaringan, atau log aplikasi.
2. Format log: Anda harus memahami format log dan cara membacanya, seperti tanda waktu (timestamp), level log, pesan log, dan metadata lainnya.
3. Alat dan teknologi: Anda perlu memahami alat dan teknologi yang digunakan untuk menghasilkan dan mengelola log, seperti server log, perangkat keras jaringan, aplikasi log, dan layanan cloud.
4. Pengumpulan dan penyimpanan: Anda perlu memahami cara mengumpulkan dan menyimpan log secara efisien, terutama jika Anda mengelola banyak log dari banyak sumber. Anda juga perlu memahami kebijakan penyimpanan data yang berlaku di perusahaan Anda dan peraturan privasi.
5. Analisis dan pelaporan: Anda perlu memahami cara menganalisis log untuk mendapatkan wawasan yang bermanfaat dan cara melaporkannya kepada tim IT atau manajemen.
6. Keamanan: Anda perlu memahami praktik keamanan yang tepat untuk melindungi log Anda dari ancaman seperti peretasan atau malware.
7. Compliance: Anda perlu memahami regulasi dan kepatuhan yang berlaku dalam bisnis Anda dan memastikan bahwa log Anda memenuhi persyaratan tersebut.

8. Manajemen dan pemeliharaan: Anda perlu memahami cara menjaga log Anda tetap up-to-date dan mengelola log secara teratur, seperti membersihkan log yang tidak perlu dan melakukan rotasi log.

B. Keterampilan yang diperlukan untuk dapat mengelola log

1. Analisis data: Keterampilan analisis data diperlukan untuk memahami dan mengambil informasi yang bermanfaat dari log yang dihasilkan oleh sistem atau aplikasi.
2. Pemrograman: Keterampilan pemrograman akan membantu Anda dalam mengotomatisasi proses pengumpulan, penyimpanan, analisis, dan pelaporan log.
3. Keamanan: Keterampilan keamanan sangat penting dalam mengelola log, terutama dalam mengidentifikasi ancaman keamanan dan memastikan bahwa log tidak mudah diretas atau diakses oleh pihak yang tidak berwenang.
4. Penyelesaian masalah: Keterampilan penyelesaian masalah sangat penting dalam mengelola log karena seringkali Anda akan dihadapkan pada situasi yang memerlukan analisis cepat dan penyelesaian masalah yang efektif.
5. Komunikasi: Keterampilan komunikasi yang baik diperlukan dalam melaporkan hasil analisis log kepada tim IT atau manajemen.
6. Pengelolaan waktu: Mengelola log memerlukan keterampilan manajemen waktu yang baik karena seringkali terdapat banyak log yang perlu dianalisis dan dipantau secara bersamaan.
7. Pemahaman sistem dan jaringan: Anda perlu memiliki pemahaman yang baik tentang sistem dan jaringan untuk dapat memahami log yang dihasilkan oleh sistem atau aplikasi, serta mengetahui apabila terjadi masalah dan melakukan perbaikan.
8. Kerja tim: Keterampilan kerja tim sangat penting karena Anda harus bekerja dengan tim IT, manajemen, dan departemen lain untuk memastikan bahwa log dikelola dengan benar dan kebijakan keamanan yang tepat diimplementasikan.

C. Sikap Kerja yang diperlukan untuk dapat mengelola log

1. Kepedulian terhadap keamanan: Kepedulian terhadap keamanan sangat penting dalam mengelola log karena log mengandung informasi sensitif tentang sistem dan jaringan.
2. Ketekunan dan teliti: Anda perlu memiliki ketekunan dan teliti dalam mengelola log karena terkadang informasi penting tersembunyi di dalam log yang tidak mudah ditemukan.
3. Kemampuan bekerja di bawah tekanan: Keterampilan ini diperlukan karena seringkali Anda akan dihadapkan pada situasi kritis yang memerlukan respons cepat dan tindakan yang tepat.

4. Kemampuan belajar mandiri: Kemampuan untuk belajar mandiri sangat penting dalam mengelola log karena teknologi dan alat yang digunakan untuk menghasilkan dan mengelola log terus berkembang.
5. Kemampuan berkomunikasi yang baik: Kemampuan berkomunikasi yang baik sangat penting dalam melaporkan hasil analisis log kepada tim IT atau manajemen, serta untuk meminta bantuan atau dukungan ketika dibutuhkan.
6. Kemampuan beradaptasi: Anda perlu dapat beradaptasi dengan cepat dengan perubahan teknologi atau perubahan dalam lingkungan kerja.
7. Tanggung jawab dan akuntabilitas: Anda perlu bertanggung jawab dan akuntabel atas tindakan Anda dalam mengelola log

Tugas Dan Proyek Pelatihan

1. Instalasi 3 Perangkat lunak yang berfungsi untuk menganalisa log

Link Referensi Modul Ketiga

1. Video Pembelajaran
2. E-book
3. Link Youtube/Website rujukan

Link Pertanyaan Modul Ketiga

<https://app.sli.do/> (bisa menggunakan aplikasi ini)

Bahan Tayang

Bisa berupa Link/ Screen Capture Slide pelatihan

Link room Pelatihan dan Jadwal live sesi bersama instruktur

Zoom, Meets

Penilaian

Komposisi penilaian Kuis 1 Mengumpulkan data: Nilai 10 (Range 0 -10)

Target Penyelesaian Modul Ketiga

1hari/sampai 6 JP

VSGA

Vocational School
Graduate Academy

2023