Pilih salah satu tools atau audit software yang digunakan dalam proses audit TI, kemudian jelaskan fungsi dari tools tersebut dalam mendukung proses audit (tugas presentasi kelompok)

Kelompok autopsy

Pamuji muhammad jakak

M apriliansyah

Singgih hananta

Edi supriyadi

AUTOPSY

- **APLIKASI AUTOPSY**
- Autopsy adalah sebuah antarmuka grafis untuk tool-tool didalam sleuth kit,yang memudahkan pengguna dalam melakukan investigasi. Mereka dapat menganalisis disk dan file system windows dan unix (NTFS, FAT, UFS1/2,EXT2/3). Autopsy menyediakan fungsi manajemen kasus, integritas gambar, pencarian kata kunci, dan operasi lainnya.
- Autopsy menggunakan perl untuk menjalankan program-program sleuth kit dan mengubah hasilnya ke HTML, olehkarena itu pengguna autopsy membutuhkan web client untuk mengakses fungsi-fungsinya

- Autopsy sebenarnya adalah sebuah mini web server dengan script CGI berbasis perl.
- Autopsy menggunakan perl untuk menjalankan pr ogram-program sleuth kit dan mengubah hasilnya ke HTML. Oleh karena itu pengguna autopsy membutuhkan web client untuk mengakses fungsi-fungsi autopsy. Selain sebagaiuser interface sleuthkit, autopsy menyediakan fungsi-fungsi administratif tambahan. Beberapa fungsi tersebut adalah logging (mencatat tindakan /perintah sleuth kit yang telah di jalankan), notes (mencatat keterangan tambahan yang di peroleh penyelidik), dan report (mencatat hasil analisa

CONTOH GAMBAR APLIKASI

Fitur Autopsy :

- Multi-User Cases: Berkolaborasi dengan sesama penguji dalam kasus besar.
- Timeline Analysis: Menampilkan kejadian sistem dalam antarmuka grafis untuk membantu mengidentifikasi aktivitas.
- Ekstraksi String Unicode: Ekstrak senar dari ruang yang tidak terisi dan jenis file yang tidak dikenal dalam banyak bahasa (Arab, Cina, Jepang, dll.)
- Tag: Tag file dengan nama tag yang sewenang-wenang, seperti 'bookmark' atau 'curiga', dan tambahkan komentar.
- Keyword Search: Teks ekstraksi dan indeks dicari modul memungkinkan Anda untuk menemukan file yang menyebutkan istilah tertentu dan menemukan pola ekspresi reguler.
- Web Artifacts: Ekstrak aktivitas web dari browser umum untuk membantu mengidentifikasi aktivitas pengguna.
- Registry Analysis: Kegunaan RegRipper Untuk mengidentifikasi dokumen dan perangkat USB yang baru diakses.
- Analisis File LNK: Mengidentifikasi jalan pintas dan dokumen yang mudah diakses
- Email Analysis: MBOX Format pesan, seperti Thunderbird.
- EXIF: Ekstrak lokasi geografis dan informasi kamera dari file JPEG.

Fitur Autopsy :

- Sortir Jenis File: Kelompokkan file menurut jenisnya untuk menemukan semua gambar atau dokumen.
- Pemutaran Media: Lihat video dan gambar dalam aplikasi dan tidak memerlukan penampil eksternal.
- Penampil Thumbnail: Menampilkan thumbnail gambar untuk membantu melihat gambar dengan cepat.
- Robust File System Analysis: Dukungan untuk sistem berkas yang umum, termasuk NTFS, FAT12/FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2, and UFS dari The Sleuth Kit
- Hash Set Filtering: Saring file yang diketahui dengan baik NSRL Dan flag file buruk yang diketahui menggunakan hashsets khusus dalam format HashKeeper, md5sum, dan EnCase.
- Deteksi Tipe File berdasarkan tanda tangan dan deteksi ketidakcocokan ekstensi.
- Modul File yang Menarik akan menandai file dan folder berdasarkan nama dan path.
- Dukungan Android: Ekstrak data dari SMS, log panggilan, kontak, Tango, Words with Friends, dan banyak lagi.

Penutup

- Kesimpulan

  Autopsy adalah sebuah antarmuka grafis untuk tool-tool didalam sleuth kit, yang memudahkan pengguna dalam melakukan investigasi. Tiap host harus menggunakan port terpisah. Autopsy menggunakan cookies untuk memvalidasi hal ini.

IT Audit Tools

NMAP (Network Mapper)

- Ilsa Palingga Ninditama
- Rahma Fitriyani
- Ricca Verana Sari
- Safta Hastini
- Uci Suryani

NMAP (Network Mapper)

Open source untuk melakukan eksplorasi jaringan dan audit keamanan. Nmap didesain untuk mampu menscan network yang besar, walau NMAP juga sangat handal untuk melakukan scan pada satu host tertentu.

Nmap mempergunakan IP paket raw untuk menentukan host yang aktif pada jaringan, service (nama aplikasi dan versi) yang disediakan oleh host, operating system (versi OS) yang sedang berjalan, tipe filter/firewall yang dipakai, dan karakteristik lainnya.

Nmap biasanya dipakai juga untuk audit keamanan, banyak sistem dan network admin menemukan kemudahan untuk pemakaiannya untuk pemakaian rutin, seperti network inventory,manajemen jadwal update service, monitoring host or service uptime.

Fungsi

NMAP

- Untuk mengeksplorasi jaringan seperti banyaknya administrator system dan jaringan yang menggunakan aplikasi
- Menemukan banyak fungsi dalam inventori jaringan
- Mengatur jadwal peningkatan service.
- Memonitor host atau waktu pelayanan.

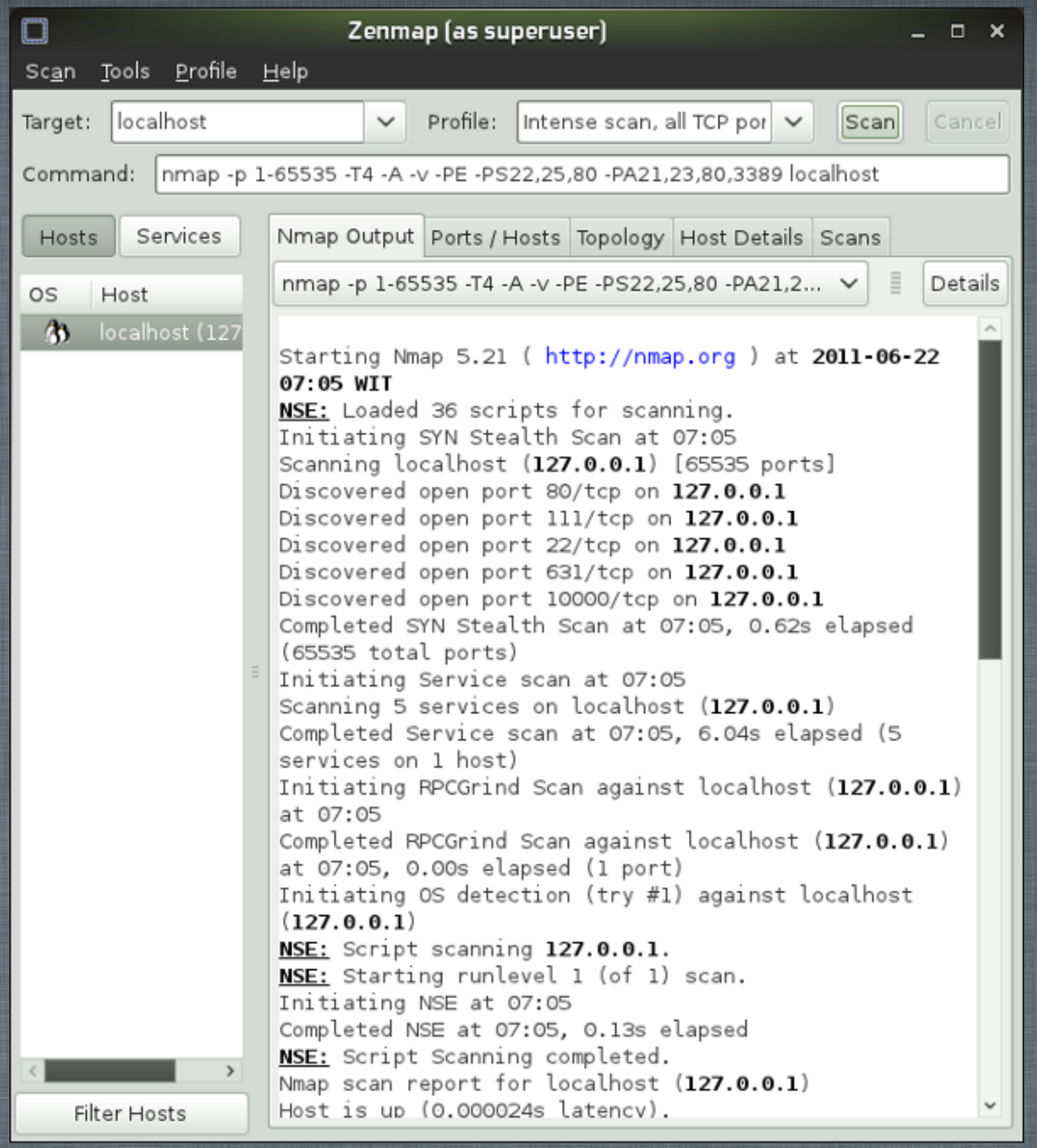
Contoh Penggunaan NMAP Dengan Menggunakan Command Line:

```
wdzgouch@server1:~> nmap localhost

Starting Nmap 5.21 ( http://nmap.org ) at 2011-06-22 10:28 WIT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00028s latency).
rDNS record for 127.0.0.1: linux-34ar.site
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
631/tcp   open  ipp
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Contoh Tampilan Penggunaan NMAP dengan menggunakan Aplikasi GUI: Zenmap.

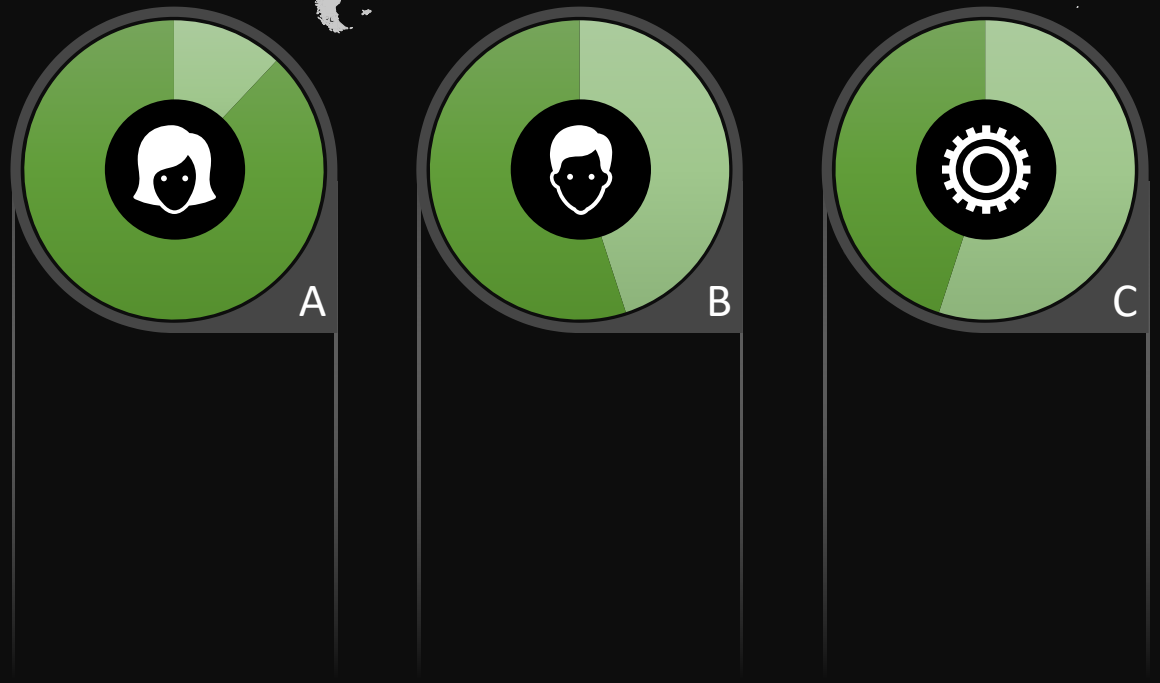


KESIMPULAN

NMAP adalah sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Output NMAP adalah sebuah daftar target host yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan.

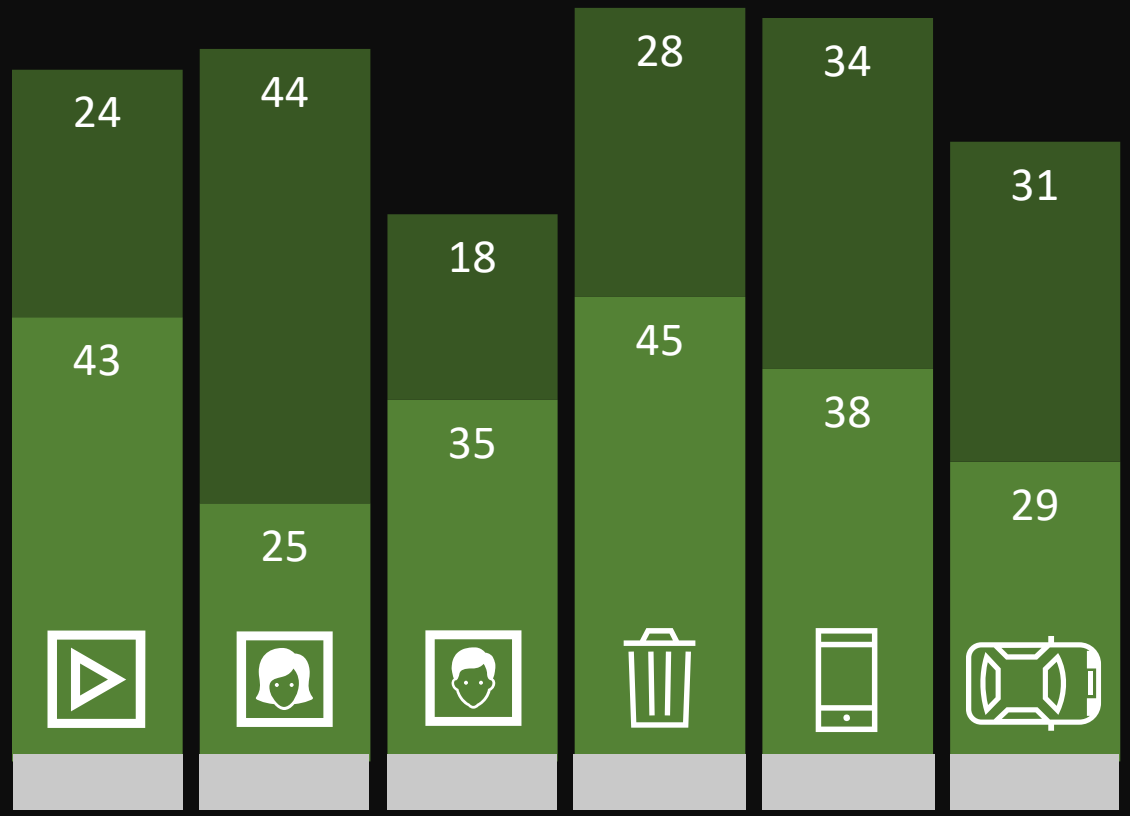
That’s all!

Thank you! ☺



RAJU SEPTA WIJAYA

182420094



Apa itu SEO..?

SEO adalah singkatan dari "search engine optimization" (pengoptimalan mesin telusur) atau "search engine optimizer". Penggunaan jasa SEO adalah keputusan besar yang dapat meningkatkan peringkat situs Anda dan menghemat waktu, tapi juga berisiko tinggi terhadap situs dan reputasi. Pastikan meneliti kemungkinan keuntungan serta kelemahan yang dapat ditimbulkan oleh SEO yang tidak bertanggung jawab terhadap situs Anda. Banyak SEO dan agen serta konsultan lain yang menyediakan layanan yang bermanfaat bagi pemilik situs web, meliputi:

Ulasan tentang konten atau struktur situs Anda

Saran teknis tentang pengembangan situs web: misalnya, hosting, pengalihan, halaman error, dan penggunaan JavaScript

Pengembangan konten

Manajemen kampanye pengembangan bisnis online

Penelitian kata kunci

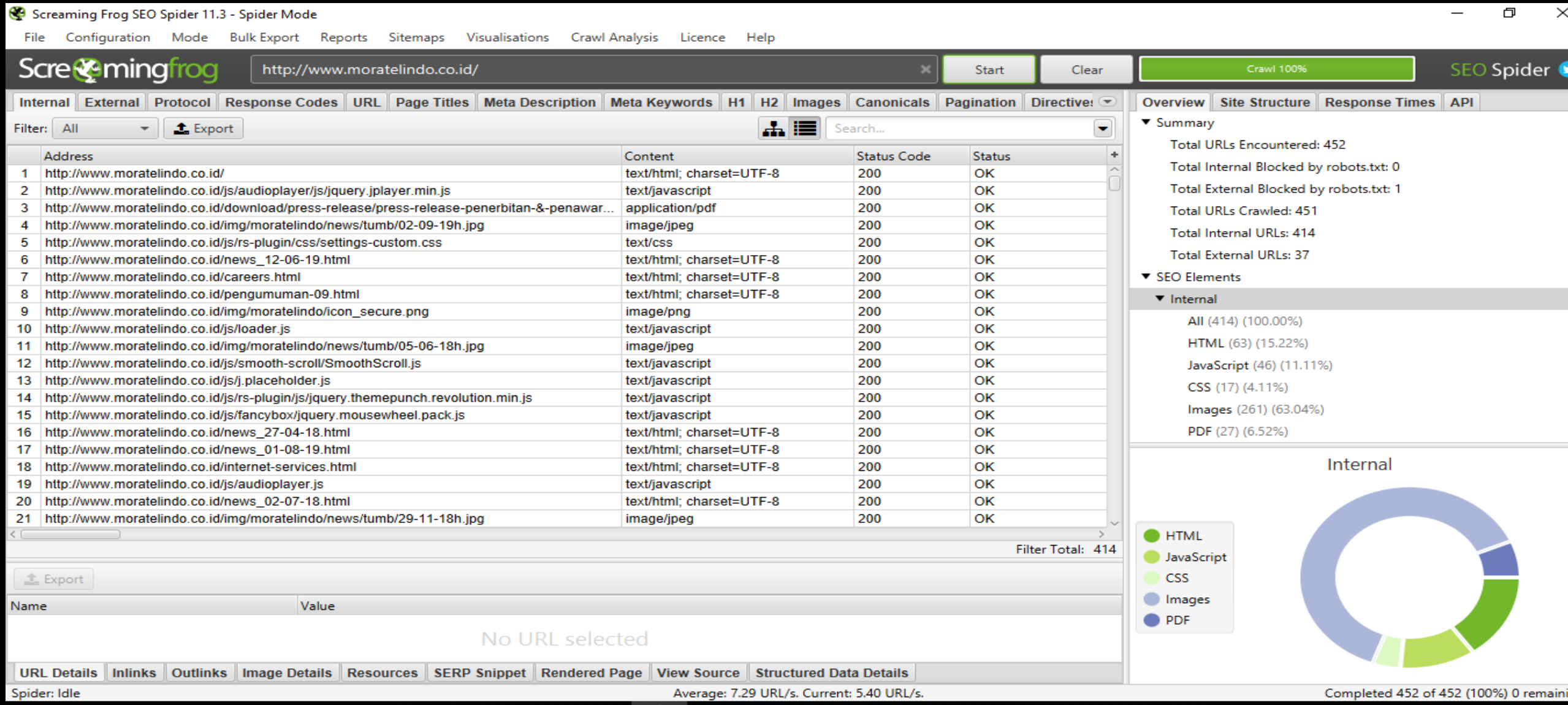
Pelatihan SEO

Keahlian dalam pasar dan geografis tertentu.

Apa itu Screaming Frog?

Screaming Frog SEO Spider adalah sebuah aplikasi desktop yang kecil, Anda dapat menginstal secara lokal di komputer PC, Mac, atau Linux. Dia menjelajahi link, gambar, CSS, dll situs web dari sudut pandang SEO. Yang pada dasarnya memberitahu Anda apa yang akan search spider lihat ketika dia menjelajahi situs web.
Informasi ini memungkinkan Anda untuk dengan cepat menganalisa, audit dan meninjau situs dari perspektif SEO onsite. Hal ini dapat menghemat satu ton pekerjaan, karena secara manual menganalisis setiap halaman website besar bisa sangat menantang.

Screaming Frog



Kesimpulan

Dengan Screaming Frog SEO Spider Anda dapat menganalisis beberapa elemen di tempat, seperti judul halaman, meta descriptions, struktur URL, kode respon, gambar, dll. Ini adalah alat yang hebat untuk membantu Anda mengoptimalkan sebuah situs web dan meningkatkan kinerja di halaman hasil pencarian. Selain itu; itu benar-benar gratis, sehingga seharusnya menjadi alat wajib dalam toolbox setiap desainer web!

SEO AUDIT TOOL

semrush


search...
WHAT IS
SEO?
Lorem ipsum

Why SEO is

IMPORTANT

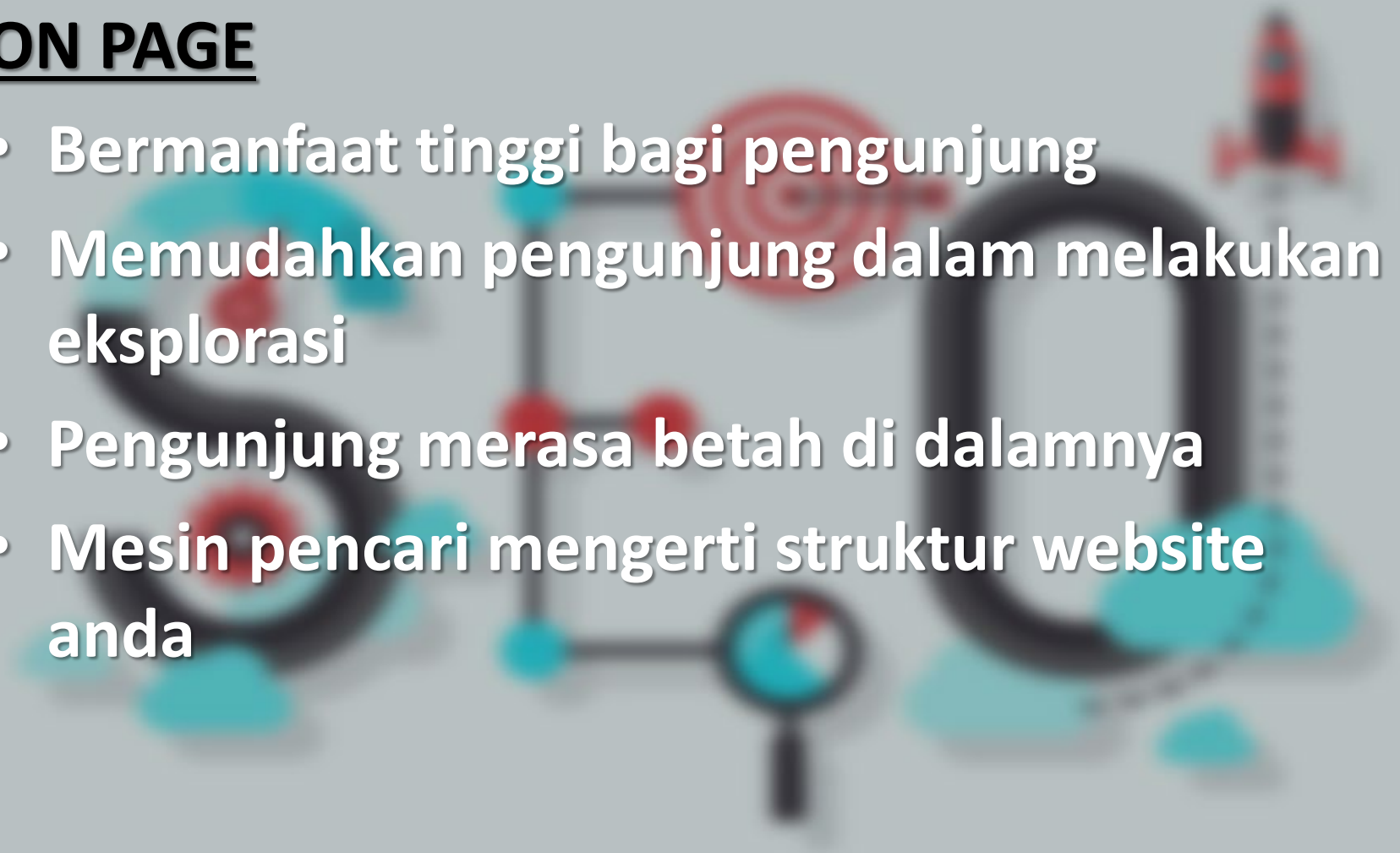
for website ???

BASIC CONCEPT OF SEO

- Content
- Navigation And Structure
- User Experience
- Popularity

ON PAGE AND OFF PAGE

ON PAGE – OFF PAGE



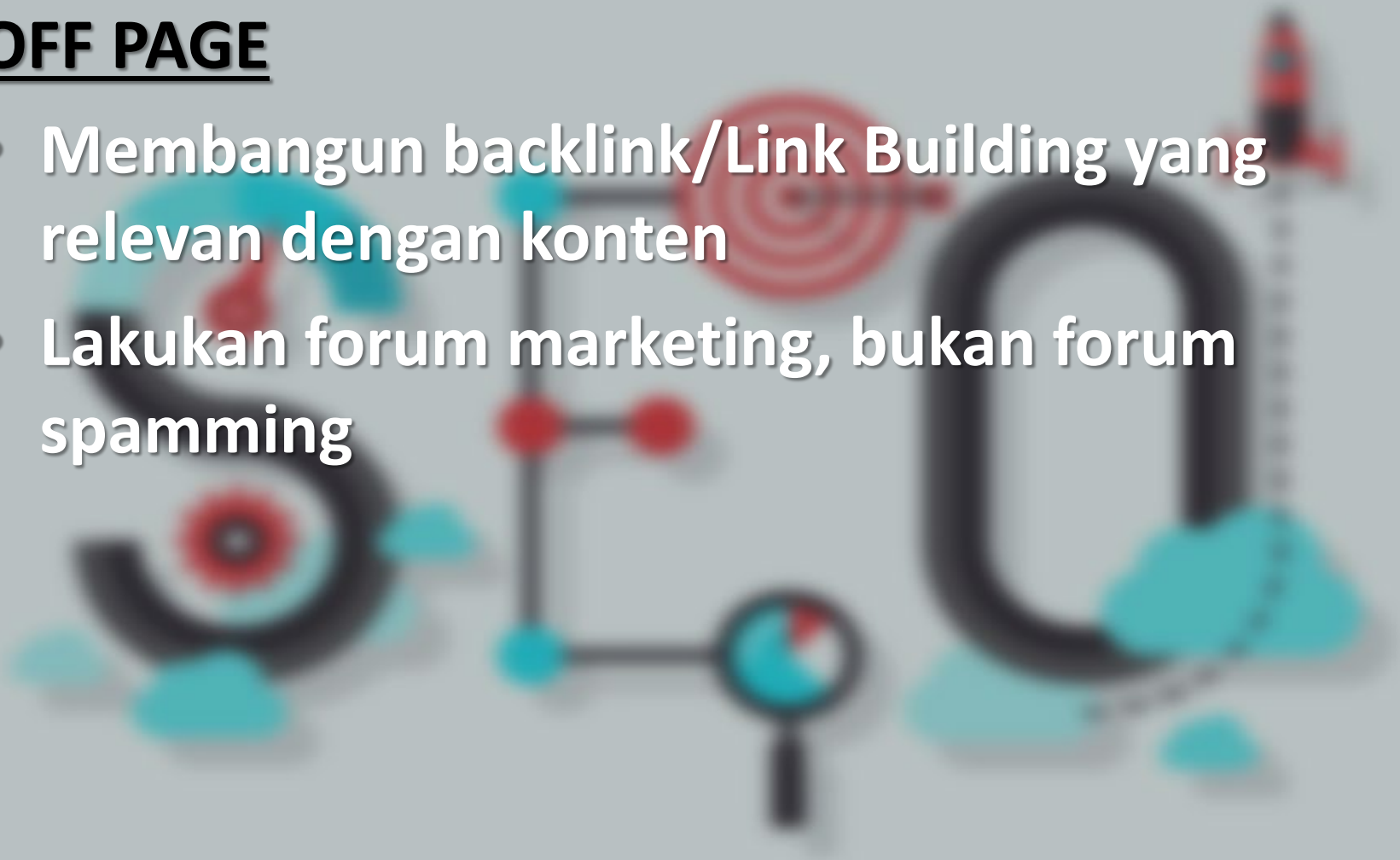
ON PAGE

- Bermanfaat tinggi bagi pengunjung
- Memudahkan pengunjung dalam melakukan eksplorasi
- Pengunjung merasa betah di dalamnya
- Mesin pencari mengerti struktur website anda

ON PAGE – OFF PAGE

OFF PAGE

- Membangun backlink/Link Building yang relevan dengan konten
- Lakukan forum marketing, bukan forum spamming




semrush

All-Inclusive Suite for Your Marketing Workflow

SEO

Advertising

Social Media

Content

Competitive Research

Reporting & Management

SEO

- Organic Research
- Organic Traffic Insights
- Keyword Research
- Backlink Building and Analytics
- Rank Tracking
- Site Audit
- On Page SEO Checker
- Search Engine Sensor

Advertising

- Advertising Research
- PPC Keyword Tool
- Display Advertising
- Ad Builder
- Product Listing Ads

Social Media

- Social Media Poster
- Social Media Tracker

Content

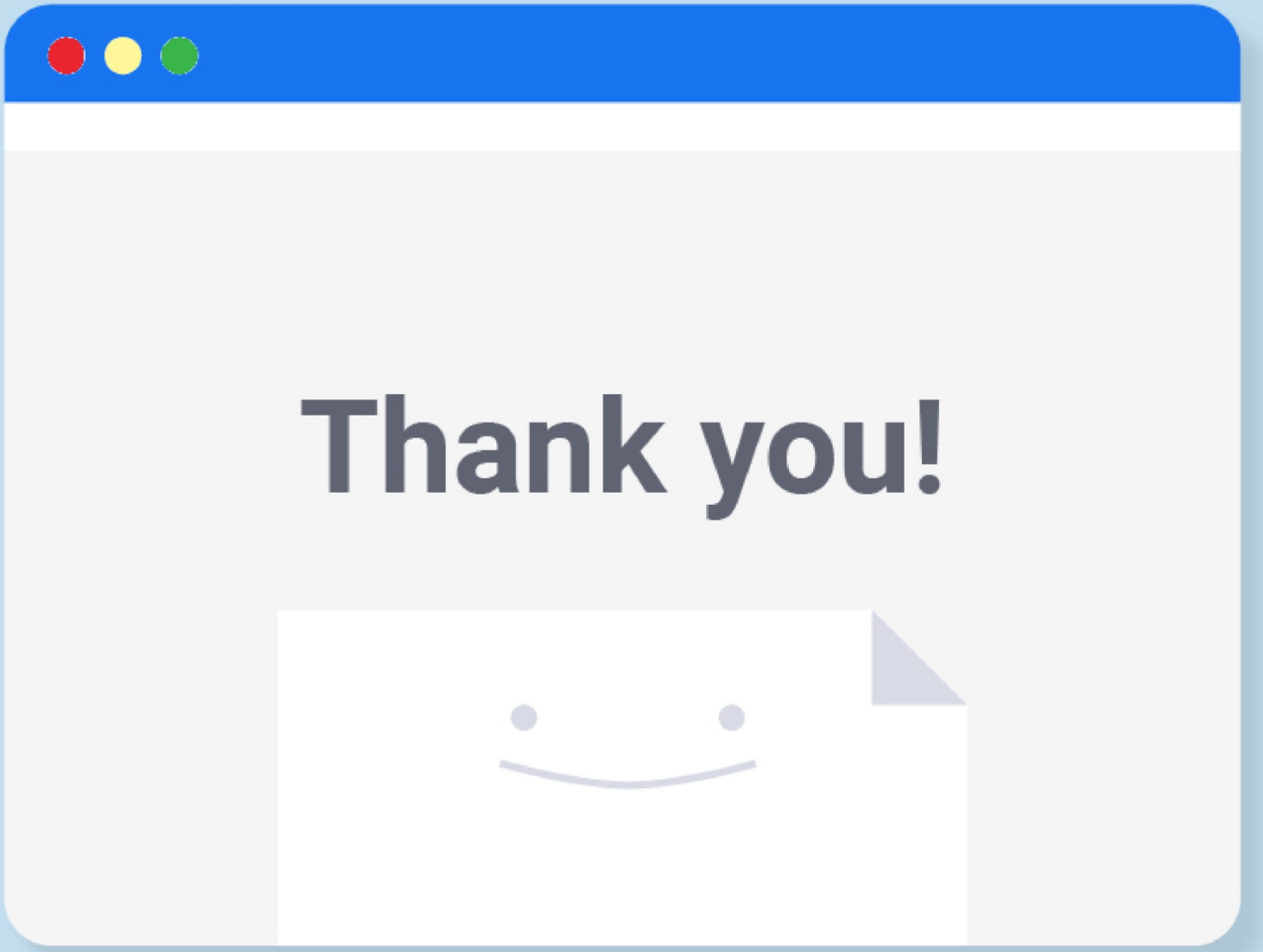
- Content Audit
- Topic Research
- SEO Content Template
- Post Tracking
- Keyword Research
- Related Keywords
- Brand Monitoring

Competitive Research

- Domain Overview
- Charts
- Keyword and Backlink gap Analysis
- Ranks
- Traffic Analytics

Reporting & Management

- Marketing Calendar
- My Reports
- Lead Generation Tool


Thank you!

IT Audit Tools

NMAP (Network Mapper)

- **Ilsa Palingga Ninditama**
- **Rahma Fitriyani**
- **Ricca Verana Sari**
- **Safta Hastini**
- **Uci Suryani**

NMAP (Network Mapper)

Open source untuk melakukan eksplorasi jaringan dan audit keamanan. Nmap didesain untuk mampu menscan network yang besar, walau NMAP juga sangat handal untuk melakukan scan pada satu host tertentu.

Nmap mempergunakan IP paket raw untuk menentukan host yang aktif pada jaringan, service (nama aplikasi dan versi) yang disediakan oleh host, operating system (versi OS) yang sedang berjalan, tipe filter/firewall yang dipakai, dan karakteristik lainnya.

Nmap biasanya dipakai juga untuk audit keamanan, banyak sistem dan network admin menemukan kemudahan untuk pemakaiannya untuk pemakaian rutin, seperti network inventory,manajemen jadwal update service, monitoring host or service uptime.

Fungsi

NMAP

- Untuk mengeksplorasi jaringan seperti banyaknya administrator system dan jaringan yang menggunakan aplikasi
- Menemukan banyak fungsi dalam inventori jaringan
- Mengatur jadwal peningkatan service.
- Memonitor host atau waktu pelayanan.

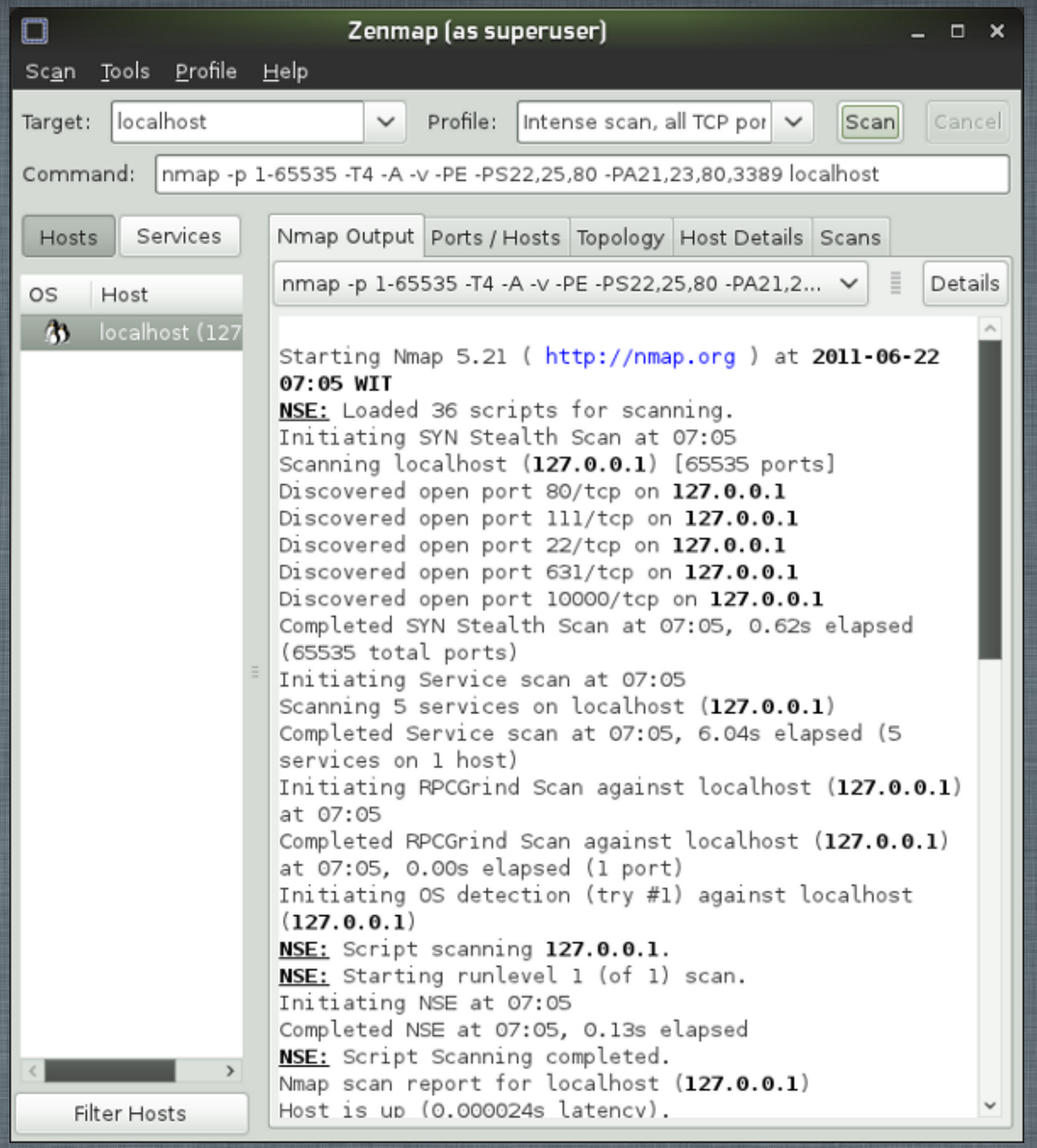
Contoh Penggunaan NMAP Dengan Menggunakan Command Line:

```
wdzgouch@server1:~> nmap localhost

Starting Nmap 5.21 ( http://nmap.org ) at 2011-06-22 10:28 WIT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00028s latency).
rDNS record for 127.0.0.1: linux-34ar.site
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
631/tcp   open  ipp
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Contoh Tampilan Penggunaan NMAP dengan menggunakan Aplikasi GUI: Zenmap.



KESIMPULAN

NMAP adalah sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Output NMAP adalah sebuah daftar target host yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan.

That’s all!

Thank you! ☺

NESSUS

IT Audit Tool

Oleh:
Riduan Syahri
Dita Rahmawati
Rumondang Martha A

Pengertian

- Nessus dibuat oleh Renaud Deraison pada tahun 1998 yang berada di bawah perusahaan development Tenable yang berfokus pada Cybersecurity.
- Nessus merupakan software scanning yang dapat digunakan untuk mengaudit keamanan sebuah sistem, seperti vulnerability, misconfiguration, security patch yang belum diaplikasikan, default password, dan denial of service.

Pengertian

- Dikarenakan fungsi dari Nessus dapat digunakan untuk mendeteksi adanya kelemahan dari suatu sistem maka Nessus menjadi salah satu tool andalan ketika melakukan audit keamanan sistem.

Fitur-fitur NESSUS

- Database security Nessus diupdate setiap hari ketika terconnect dengan server Nessus.
- Nessus mampu mendeteksi tidak cuma port yang terbuka di setiap komputer yang terhubung kedalam jaringan, tetapi juga mengecek partch OS nya termasuk didalamnya patch untuk Windows, Unix, Linux, atau MacOS.
- Nessus bisa dibangun dalam skala kecil, satu atau dua komputer dengan sedikit resource prossesor sampai dengan prosessor dengan quad core lebih.

- Setiap security test dibentuk dalam modul plugin dan ditulis dalam NASL, artinya update nessus tidak akan melibatkan binaries yang tidak dipercaya dari internet.
- Setiap NASL plugin dapat dibaca, dimodifikasi agar report Nessus bisa dibaca dengan lebih mudah
- NASL (Nessus Attack Scripting Language) suatu bahasa yang dikembangkan khusus agar security test dapat dijalankan dengan mudah dan cepat

- NASL plugin di dalam suatu container yang bisa berdiri di atas virtual mesin sehingga membuat Nessus menjadi scanner yang benar benar secure
- Nessus memiliki kemampuan untuk mengetest SSL seperti https, smptps, imaps, dll dan dapat pulau diintegrasikan

3 tahap proses pada Nessus

- Scanning

Pada fase ini Nessus akan melakukan pengecekan untuk mengetahui mana host yang hidup (live), dengan cara mengirimkan ICMP Echo. Kemudian selanjutnya bisa host tersebut diketahui live akan deteruskan dengan port scanning

- Enumeration

Pada tahap ini Nessus akan melakukan pemeriksaan kepada host yang live dengan mencari banner grabbing yang bisa menunjukkan jenis dan versi OS yang digunakan host. Tergantung dari sistemnya di fase ini dimungkinkan untuk melakukan test penjebolan account dan password dengan metode Brute Force

- Deteksi Vulnerability

Setelah fase 2 selesai, maka Nessus akan melanjutkan dengan mencari vulnerability yang sesuai yang terdapat pada host target misalnya input validasi, buffer overflows, konfigurasi yang tidak tepat

REVIEW ACL (Audit Command Language)

Pengertian ACL

- ACL for Windows (sering disebut ACL) adalah sebuah program untuk membantu akuntan dalam melakukan pemeriksaan di lingkungan sistem informasi berbasis komputer atau Pemrosesan Data Elektronik. ACL secara khusus dirancang untuk menganalisa data, memanipulasi data dan mengekspor data sehingga membuatnya menjadi lebih berguna bagi auditor.
- ACL adalah sebuah software yang dirancang secara khusus untuk menganalisa data dan menghasilkan laporan audit baik untuk pengguna biasa (common/ nontechnical users) maupun pengguna ahli (expert users)
- ACL dapat mengerjakan berbagai tipe format data. Data yang dihasilkan oleh komputer, disimpan dalam karakter-karakter yang disebut byte. ACL dapat membaca data dari berbagai macam sistem yang terbentang mulai dari model sistem mainframe lama hingga ke relational database modern.
- ACL adalah aplikasi yang hanya 'read-only', ACL tidak pernah mengubah data sumber asli sehingga aman untuk menganalisis jenis live-data. Keanekaragaman sumber data dan teknologi akses data, cara mengakses data juga bervariasi dari satu sumber data ke lain. ACL membaca beberapa sumber data secara langsung dengan mengimport dan menyalin sumber data sehingga dapat dianalisis. Banyak jenis data modern saat ini berisi berisi informasi tentang layout record, seperti jumlah record, nama field, panjang field dan tipe data tiap field. Ketika semua informasi ini ada dalam sumber data, atau dalam suatu file definisi eksternal yang terkait, ACL memperoleh ini informasi secara otomatis. Jika informasi tidak menyajikan, maka harus mengacu pada suatu dokumen seperti layout record atau suatu kamus data dan mendefinisikan menggunakan ACL dengan manual.

Paling tidak ada 2 jenis yang utama dalam pengkodean dalam komputer, yaitu:

1. EBCDIC (Extended Binary Coded Decimal Interchang Code) – format ini seringkali ditemukan pada komputer jenis IBM Mainframe.
2. ASCII (American Standard Code for Information Interchange) – format ini hampir digunakan dibanyak komputer. ACL dapat membaca langsung baik jenis EBCDIC atau ASCII, sehingga tidak perlu untuk menngkonversi kedalam bentuk lain.

Perusahaan ACL

- ACL adalah salah satu jenis audit software yang termasuk dalam kategori Genaralized Audit Software (GAS). Seperti halnya aplikasi GAS yang lainnya, ACL hanya dapat digunakan untuk mengumpulkan dan mengevaluasi bukti yang dihasilkan dari pemrosesan transaksi perusahaan sehingga ACL lebih cenderung digunakan untuk menilai post transactions daripada current transaction. Setelah mengulang apa itu ACL sekarang kita belajar tentang bagaiana sejarah dari ACL ini.
- Prof Hart J. Will yang mengembangkan aplikasi ACL ini. Dikembangkannya ACL ini dimulai pada tahun 1970-an. Hart tidak sendiri mengembangkan aplikasi ini. Dia mengembangkan ACL ini melalui perusahaan yang bernama ACL Services Ltd yang ada di Kanada. Perusahaan ini sebenarnya khusus membuat aplikasi-aplikasi komputer. Sehingga kegiatan utamanya adalah membuat dan menjual aplikasi analisis data, aplikasi tata kelola, aplikasi manajemen resiko dan aplikasi kepatuhan.
- Harmut (Hart) J. Will. adalah seorang Profesor Emeritus Akuntansi, Auditing dan Sistem Informasi manajemen di Sekolah Administrasi Publik di Victoria. Penemuan dia bernama ACL ini disebut-sebut sebagai evolusi pendekatan audit audit.
- Awal mula Hart mengembangkan ACL dimulai pada tahun 1960 ketika dia berada di Berlin yang sedang menyelesaikan tesisnya. ACL yang dia kembangkan itu selesai pada tahun 1968 ketika dia berada di Illinois. Awal mula sistem yang dia buat adalah kerangka Manajemen Sistem Informasi yang isisnya adalah Bank Data dan Bank Model. Selanjutnya dikembangkan sedemikian rupa sehingga jadilah aplikasi audit yang bernama ACL.

Fungsi ACL

- Bidang Auditor

  Pengguna ahli ini memiliki latar belakang yang memungkinkan dia menjadi seorang auditor sehingga ACL yang digunakannya bisa ditafsirkan dan digunakan untuk mempermudah pekerjaannya sebagai auditor. Manfaat ACL yang dapat dirasakan oleh seorang auditor dalam penggunaan ACL ini adalah ACL bisa membantu auditor dalam melaksanakan tugasnya yaitu mengaudit laporan keuangan perusahaan secara fokus, cepat, efisien dan akurat. Karena teknologi pada intinya dibuat untuk mempermudah pekerjaan manusia, untuk mengurangi kesalahan yang bisa terjadi dan untuk mempercepat pekerjaan.

- Bidang Manajemen

  Dalam suatu peruahaan ada bagian keuangannya, bagian keuangan inilah yang dimaksudnya manajemen. Bagian keuangan bisa melakukan analisis suatu data perusahaan menggunakan ACL untuk tujuan tertentu seperti melakukan analisis terhadap penjualan, bagaimana trending penjualan dan lain sebagainya. Selain digunakan manajemen untuk melakukan analisis data ACL juga bisa dilakukan untuk pengujian pengendalian perusahaan. Kalau sudah masuk kedalam pengendalian internal ini menyangkut auditing. Pengendalian internal sangat diperlukan untuk mengetahui apakah kemungkinan perusahaan melakukan kecurangan tinggi atau tidak. Penjelasan lebih dalam tentang pengendalian internal akan dibahas dalam auditing. ACL juga bisa digunakan manajemen dalam pembuatan laporan yang diinginkan. Manajemen dapat menggunakan ACL untuk :

  1. Analisis data
  2. Pengujian pengendalian perusahaan
  3. Pembuatan laporan keuangan yang diinginkan

Fitur dan kemampuan ACL Software Tools :

1. ***Universal Data Access***, yaitu dapat mengakses data dari hampir semua jenis ***database*** yang ada (DBF, XLS, Text File, report file, Oracle, SQL, DB2, AS/400 FDF, COBOL, dsb) dan semua ***platform*** (PC, ***minicomputer***, dan ***mainframe***).
2. Jumlah Data Besar, yaitu kemampuan dalam mengakses dan memproses data dalam jumlah yang sangat besar (hingga ratusan juta ***record***).
3. Kecepatan Waktu Proses, kemampuannya untuk memproses dalam waktu yang singkat walaupun data yang diproses dalam jumlah yang besar.
4. Integritas Data, dengan kemampuan mengakses database 100% (tanpa metode ***sampling***) serta data yang bersifat ***Read Only*** yang dapat menjamin orisinalitas, keamanan dan integritas data untuk pengolahan menjadi informasi yang bermanfaat bagi ***user*** dan manajemen.
5. Automasi, pembuatan aplikasi audit yang sangat cepat dan mudah untuk melakukan automasi analisis data untuk efisiensi proses kerja.
6. ***Multi File Process***, dapat digunakan untuk menangani beberapa file sekaligus, tanpa mengganggu operasional teknologi informasi yang dijalankan oleh perusahaan.
7. ***Log File Navigation***, dilengkapi dengan ***log file*** untuk pencatatan proses analisis yang telah dilakukan sehingga menghasilkan suatu ***audit trail*** yang komprehensif.

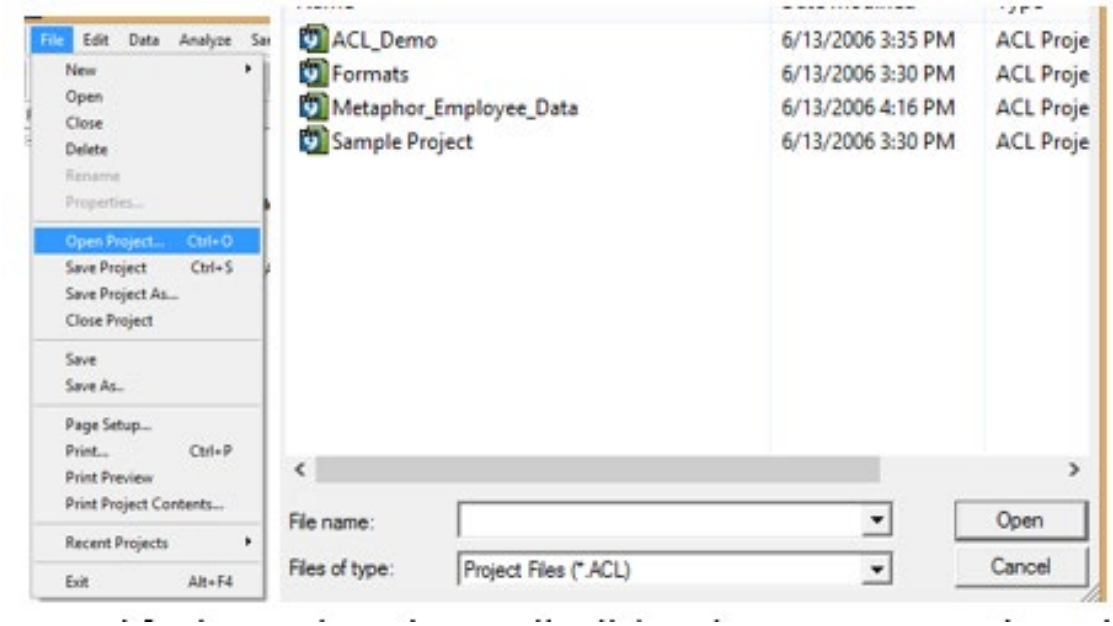
8. Fungsi Analisis yang Lengkap, dilengkapi fungsi-fungsi analisis yang sangat lengkap yang dapat dengan mudah dikombinasikan dalam menghasilkan temuan-temuan yang tidak pernah terkirakan sebelumnya.
9. Pelaporan yang Handal, kemudahan untuk merancang laporan yang handal sarat informasi yang bermanfaat serta dapat dikirimkan secara otomatis via email atau integrasi ke dalam ***software*** aplikasi Crystal Report.
10. IT Audit, kemudahan dalam menguji integritas data dan menganalisis data yang ada di dalam ***database*** ataupun menganalisis ***user-user*** yang telah masuk ke dalam suatu jaringan/***network***.

Manfaat menggunakan ACL Software Tools :

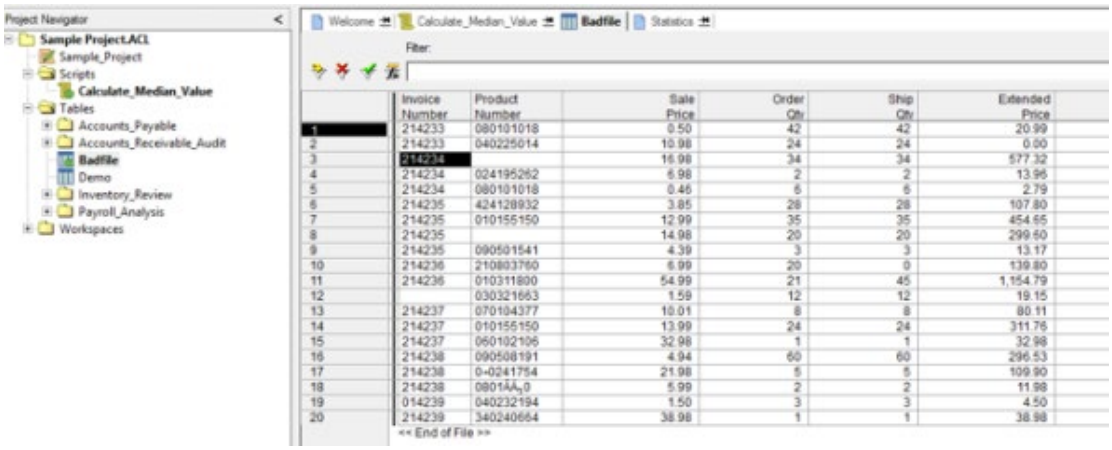
- Dapat membantu dalam mengAkses data baik langsung (***Direct***) kedalam system jaringan ataupun tidak langsung (***InDirec***t) melalui media lain seperti ***softcopy*** dalam bentuk ***teks file/report***.
- Menempatkan kesalahan dan potensial ***fraud*** sebagai pembanding dan menganalisa ***file-file*** menurut aturan-aturan yang ada.
- Mengidentifikasi kecenderungan/gejala-gejala, dapat juga menunjukan dengan tepat/sasaran pengecualian data dan menyoroti potensial area yang menjadi perhatian.
- Mengidentifikasi proses perhitungan kembali dan proses verifikasi yang benar.
- Mengidentifikasi persoalan sistem pengawasan dan memastikan terpenuhinya permohonan dengan aturan-aturan yang telah ditetapkan.
- ***Aging*** dan menganalisa ***Account Receivable/Payable*** atau beberapa transaksi lain dengan menggunakan basis waktu yang sensitif.
- Memulihkan biaya atau pendapatan yang hilang dengan pengujian data pada data-data duplikasi pembayaran, menguji data-data nomor ***Invoice***/Faktur yang hilang atau pelayanan yang tidak tertagih.
- Menguji terhadap hubungan antara authorisasi karyawan dengan ***supplier***.
- Melakukan proses ***Data Cleansing*** dan ***Data Matching*** atau pembersihan data dari data-data duplikasi terutama dari kesalahan pengetikan oleh ***End-User***.
- Dapat melaksanakan tugas pengawasan dan pemeriksaaan dengan lebih fokus, cepat, efisien, dan efektif dengan lingkup yang lebih luas dan analisa lebih mendalam. Mengidentifikasi penyimpangan (***Fraud Detection***) dapat dilakukan dengan cepat dan akurat sehingga memiliki waktu lebih banyak alam menganalisa data dan pembuktian.

- **Review Software ACL 9**

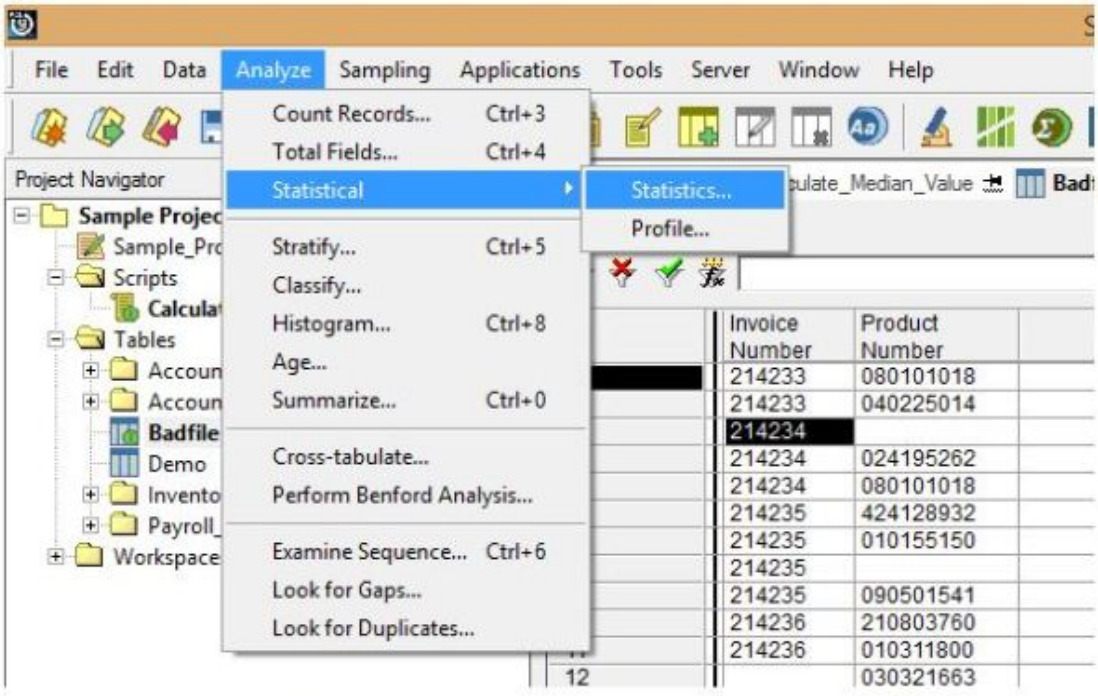
  Contoh menggunakan acl pada versi acl 9 untuk melihat data berupa statistika



Pada software acl 9 ada sample project yg disediakan, langsung open project saja dan pilih Sample Project.acl

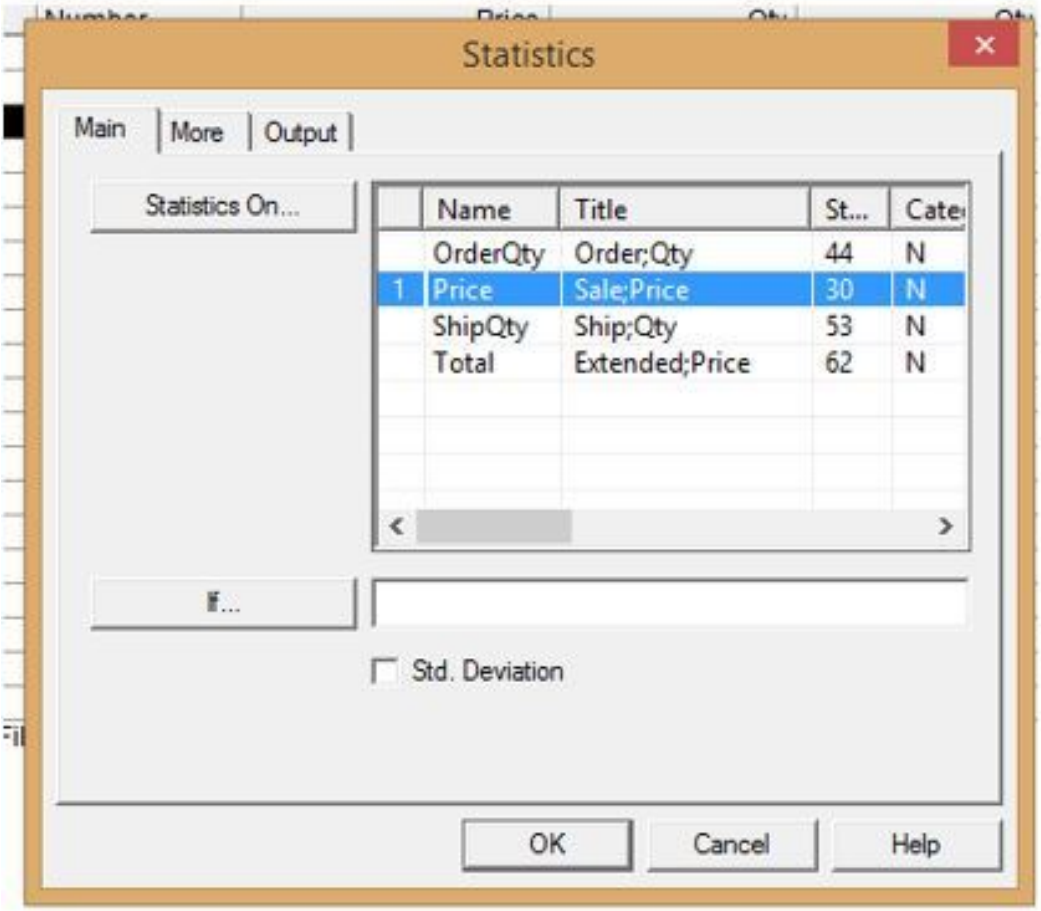


Pada software ACL setelah open sample project, akan menampilkan data berikut pada file BadFile

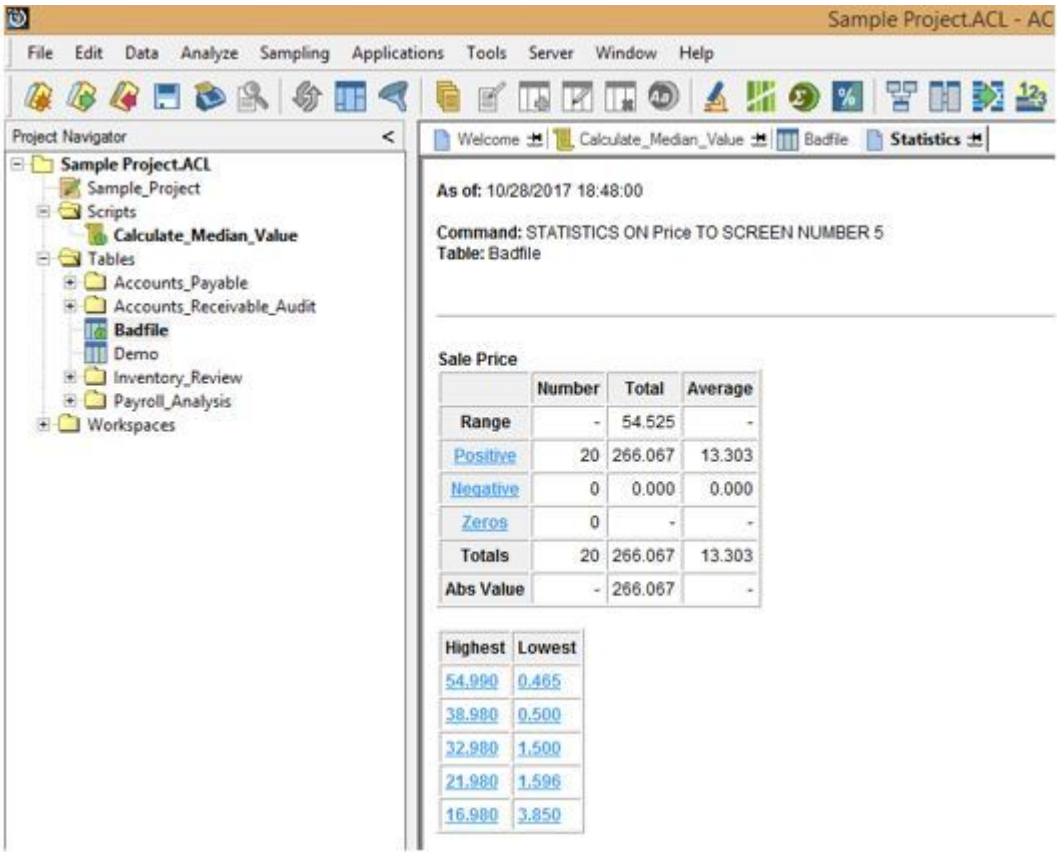


pilih menu Analyze dan pilih Statistical > Statistics...

pilih menu Analyze dan pilih Statistical > Statistics…



Pilih baris yang akan ditampilkan statistiknya, lalu klik OK



Hasil statistika bisa terlihat disini sehingga memudahkan untuk mengaudit dan menganalisa data.

NESSUS

IT Audit Tool

Oleh:
Riduan Syahri
Dita Rahmawati
Rumondang Martha A

Pengertian

- Nessus dibuat oleh Renaud Deraison pada tahun 1998 yang berada di bawah perusahaan development Tenable yang berfokus pada Cybersecurity.
- Nessus merupakan software scanning yang dapat digunakan untuk mengaudit keamanan sebuah sistem, seperti vulnerability, misconfiguration, security patch yang belum diaplikasikan, default password, dan denial of service.

Pengertian

- Dikarenakan fungsi dari Nessus dapat digunakan untuk mendeteksi adanya kelemahan dari suatu sistem maka Nessus menjadi salah satu tool andalan ketika melakukan audit keamanan sistem.

Fitur-fitur NESSUS

- Database security Nessus diupdate setiap hari ketika terconnect dengan server Nessus.
- Nessus mampu mendeteksi tidak cuma port yang terbuka di setiap komputer yang terhubung kedalam jaringan, tetapi juga mengecek partch OS nya termasuk didalamnya patch untuk Windows, Unix, Linux, atau MacOS.
- Nessus bisa dibangun dalam skala kecil, satu atau dua komputer dengan sedikit resource prossesor sampai dengan prosessor dengan quad core lebih.

- Setiap security test dibentuk dalam modul plugin dan ditulis dalam NASL, artinya update nessus tidak akan melibatkan binaries yang tidak dipercaya dari internet.
- Setiap NASL plugin dapat dibaca, dimodifikasi agar report Nessus bisa dibaca dengan lebih mudah
- NASL (Nessus Attack Scripting Language) suatu bahasa yang dikembangkan khusus agar security test dapat dijalankan dengan mudah dan cepat

- NASL plugin di dalam suatu container yang bisa berdiri di atas virtual mesin sehingga membuat Nessus menjadi scanner yang benar benar secure
- Nessus memiliki kemampuan untuk mengetest SSL seperti https, smptps, imaps, dll dan dapat pulau diintegrasikan

3 tahap proses pada Nessus

- Scanning

Pada fase ini Nessus akan melakukan pengecekan untuk mengetahui mana host yang hidup (live), dengan cara mengirimkan ICMP Echo. Kemudian selanjutnya bisa host tersebut diketahui live akan deteruskan dengan port scanning

- Enumeration

Pada tahap ini Nessus akan melakukan pemeriksaan kepada host yang live dengan mencari banner grabbing yang bisa menunjukkan jenis dan versi OS yang digunakan host. Tergantung dari sistemnya di fase ini dimungkinkan untuk melakukan test penjebolan account dan password dengan metode Brute Force

- Deteksi Vulnerability

Setelah fase 2 selesai, maka Nessus akan melanjutkan dengan mencari vulnerability yang sesuai yang terdapat pada host target misalnya input validasi, buffer overflows, konfigurasi yang tidak tepat

IT Audit Tools

NMAP (Network Mapper)

- **Ilsa Palingga Ninditama**
- **Rahma Fitriyani**
- **Ricca Verana Sari**
- **Safta Hastini**
- **Uci Suryani**

NMAP (Network Mapper)

Open source untuk melakukan eksplorasi jaringan dan audit keamanan. Nmap didesain untuk mampu menscan network yang besar, walau NMAP juga sangat handal untuk melakukan scan pada satu host tertentu.

Nmap mempergunakan IP paket raw untuk menentukan host yang aktif pada jaringan, service (nama aplikasi dan versi) yang disediakan oleh host, operating system (versi OS) yang sedang berjalan, tipe filter/firewall yang dipakai, dan karakteristik lainnya.

Nmap biasanya dipakai juga untuk audit keamanan, banyak sistem dan network admin menemukan kemudahan untuk pemakaiannya untuk pemakaian rutin, seperti network inventory,manajemen jadwal update service, monitoring host or service uptime.

Kelebihan Nmap :

- Mampu digunakan sebagai network inventory tools dan mapping IP, port, dan services.
- Mampu mendeteksi vulnerability di network.
- Port scanning.
- Relatif mudah digunakan.

Kekurangan Nmap :

Sulit menemukan issue tertentu terutama vulnerability dibagian aplikasi, nmap pada umumnya digunakan untuk menemukan celah vulnerability di bagian network.

Fungsi

NMAP

- Untuk mengeksplorasi jaringan seperti banyaknya administrator system dan jaringan yang menggunakan aplikasi
- Menemukan banyak fungsi dalam inventori jaringan
- Mengatur jadwal peningkatan service.
- Memonitor host atau waktu pelayanan.

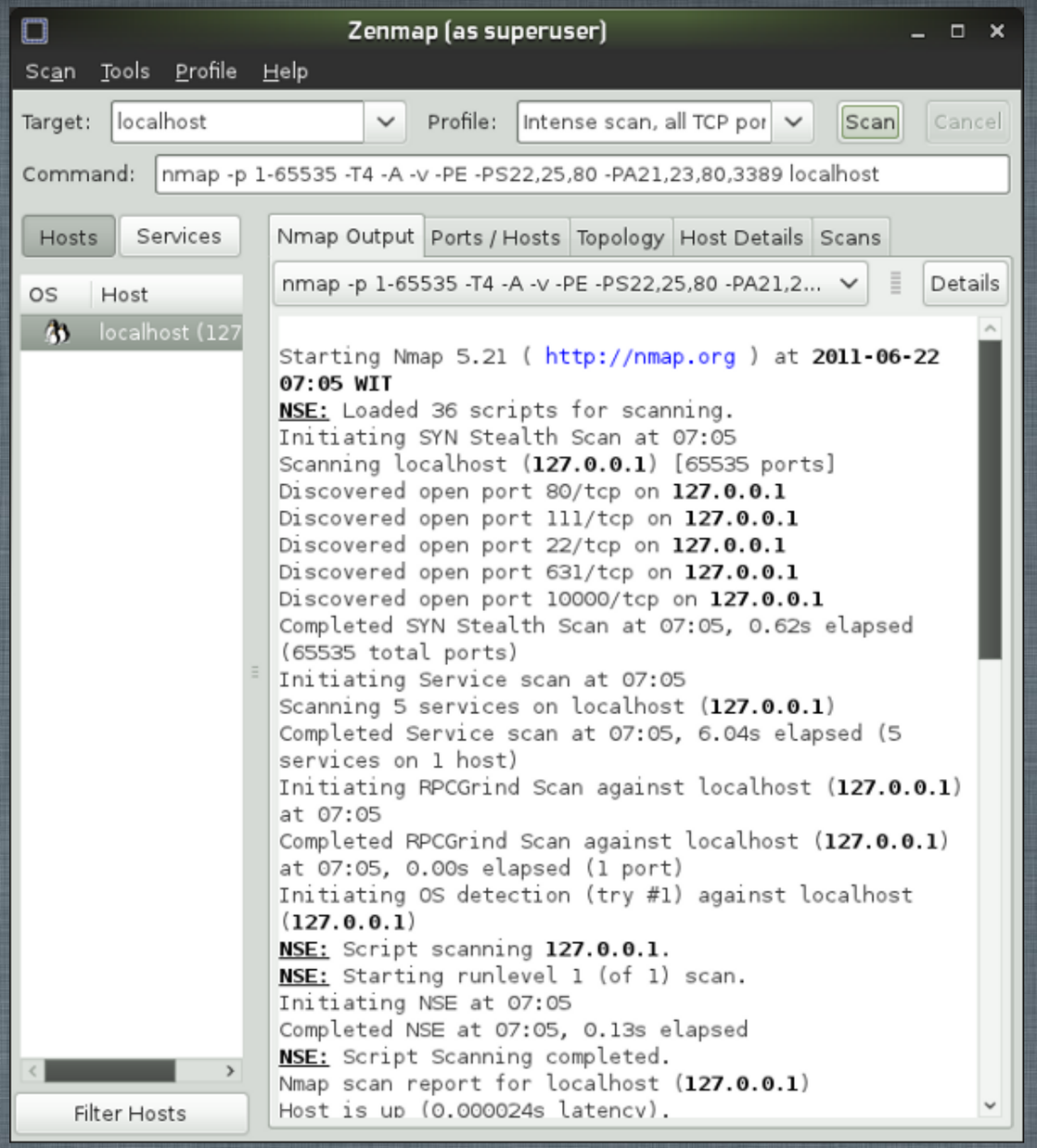
Contoh Penggunaan NMAP Dengan Menggunakan Command Line:

```
wdzgouch@server1:~> nmap localhost

Starting Nmap 5.21 ( http://nmap.org ) at 2011-06-22 10:28 WIT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00028s latency).
rDNS record for 127.0.0.1: linux-34ar.site
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
631/tcp   open  ipp
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Contoh Tampilan Penggunaan NMAP dengan menggunakan Aplikasi GUI: Zenmap.



KESIMPULAN

NMAP adalah sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Output NMAP adalah sebuah daftar target host yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan.

That’s all!

Thank you! ☺

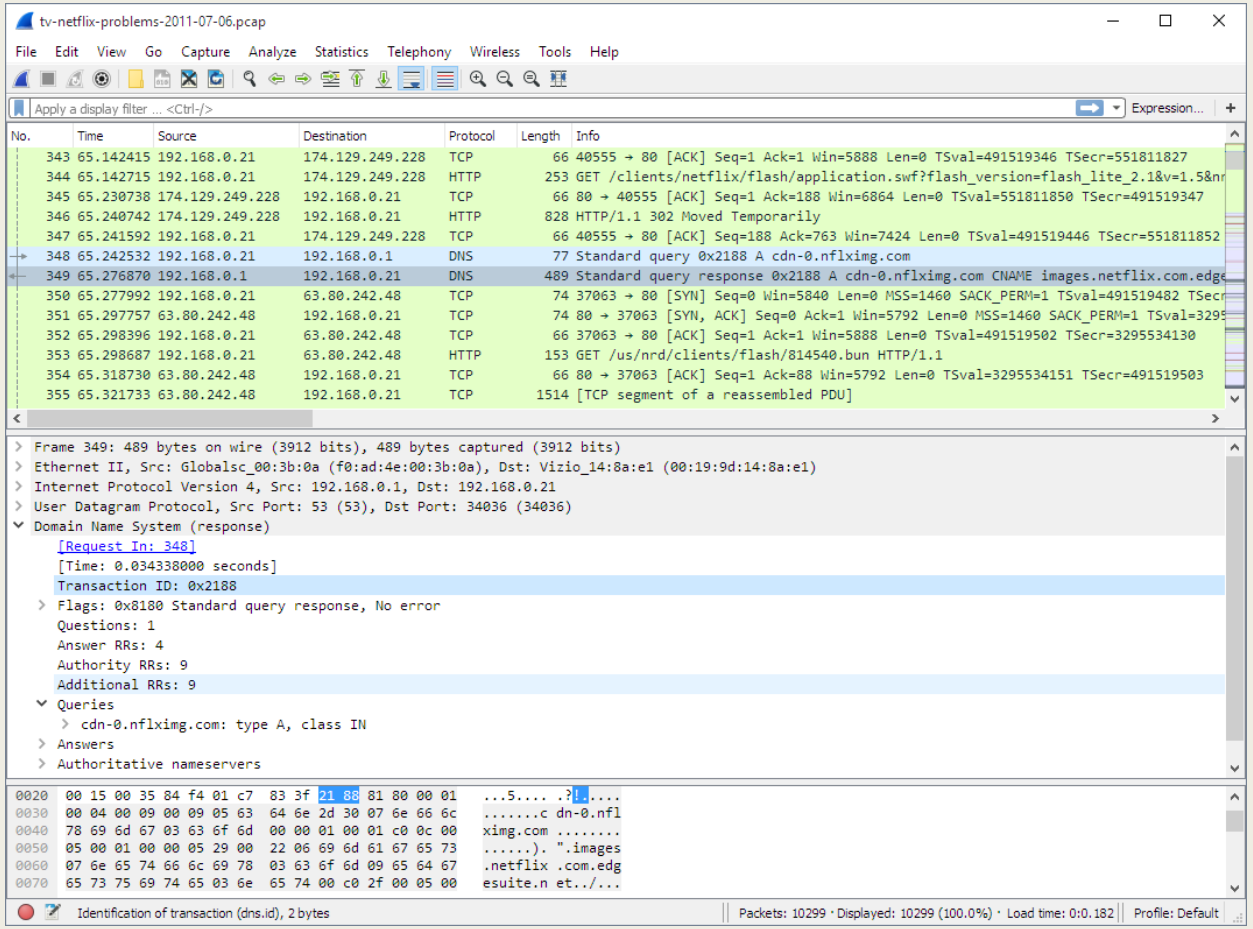
SOFTWARE IT AUDIT TOOLS

WIRESHARK

Disusun Oleh:

1. Muhammad Irvai
2. Muhammad Diah Maulidin
3. Nurhachita
4. Sahirillah

Pengertian Wireshark



- Wireshark adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis.

Pengertian Wireshark

- Wireshark adalah sebuah program analisa paket jaringan yang akan mencoba untuk menangkap paket jaringan dan mencoba untuk menampilkan data paket sedetail mungkin. Sehingga dapat melogikakan atau memikirkan sebuah packet analyzer jaringan sebagai alat ukur yang digunakan untuk memeriksa apa yang terjadi di dalam kabel jaringan
- Wireshark mampu menangkap dan paket-paket data/informasi yang ada di dalam jaringan, sehingga data tersebut dapat kita analisa untuk berbagai keperluan, diantaranya:
  - *Troubleshooting masalah di jaringan*
  - *Memeriksa keamanan jaringan*
  - *Sniffer data-data privasi di jaringan*

Tujuan Penggunaan Wireshark

- Beberapa tujuan penggunaan wireshark, yaitu:
  - *administrator jaringan menggunakannya untuk memecahkan masalah jaringan*
  - *insinyur keamanan jaringan menggunakannya untuk memeriksa masalah keamanan*
  - *pengembang menggunakannya untuk men-debug implementasi protocol*
  - *beberapa orang menggunakannya untuk mempelajari protokol jaringan internal*

Tujuan Penggunaan Wireshark

- Wireshark dapat membaca:

- Ethernet
- Token-Ring
- Serial(PPP dan SLIP)
- 802.11 wireless LAN
- Koneksi ATM
- Mengetahui IP chatter(seseorang)
- Proses transmisi dan
- Transmisi data antar komputer

Contoh Penggunaan Wireshark

- Contoh penggunaan WireShark:
  - *Admin sebuah jaringan menggunakannya untuk troubleshooting masalah-masalah di jaringan.*
  - *Teknisi keamanan jaringan menggunakan untuk memeriksa keamanan jaringan.*
  - *Pengembang software biasa menggunakan untuk men-debug implementasi protokol jaringan dalam software.*
  - *Banyak orang menggunakan Wireshark untuk mempelajari protokol jaringan secara lebih terperinci.*
  - *Selain itu digunakan sebagai sniffer atau pencari/pendeteksi data-data privasi jaringan.*

Fitur dan Kelebihan Penggunaan Wireshark

- Fitur dan kelebihan WireShark:
  - *Tersedia untuk Linux dan Windows.*
  - *Menangkap paket data secara langsung dari sebuah network interface.*
  - *Mampu menampilkan informasi yang sangat terperinci mengenai hasil tangkapan tersebut.*
  - *Dapat melakukan import dan export hasil tangkapan dari atau ke komputer lain.*
  - *Pencarian paket menggunakan berbagai macam kriteria filter/pemilahan.*
  - *Dapat membuat berbagai macam tampilan statistika*

Kesimpulan

Wireshark adalah tool open source terkemuka yang banyak di gunakan untuk melakukan analisis dan pemecah masalah jaringan, Memungkinkan untuk mengetahui masalah di jaringan. Pengembangan Wireshark berkembang berkat kontribusi relawan ahli jaringan di seluruh dunia. Wireshark di buat dengan bahasa C, C+.

Referensi Wireshark

- http://wireshark.org
- https://seruni.id/cara-menggunakan-wireshark/
- https://medium.com/@kitaadmin/wireshark-adalah-pengertian-dan-fungsi-256dc09c8292
- http://elektro.um.ac.id/wp-content/uploads/2016/05/Modul-Praktikum-3-Analisa-Jaringan-Menggunakan-WireShark.pdf

Mata Kuliah : IT Audit
Tugas 3 : Indri Endang Lestari & Sulistiyani

A. Menentukan thread/Ancaman :

1. Access to the network by unauthorized persons
2. Disclosure of passwords
3. Loss of electricity
4. Unauthorized access to the information system
5. Compromising confidential information

B. Menentukan Thread Source

1. Access to the network by unauthorized persons : Employee, Vendor
2. Disclosure of passwords : Employee
3. Loss of electricity : Employee , Contractor
4. Unauthorized access to the information system : Employee , Vendor
5. Compromising confidential information : Employee , Vendor

C. Menentukan Probability/Kemungkinan :

Probability of Occurrence	Score
Access to the network by unauthorized persons	4
Disclosure of passwords	2
Loss of electricity	4
Unauthorized access to the information system	4
Compromising confidential information	3

D. Menentukan Impact

Probability of Occurrence	Score
Access to the network by unauthorized persons	5
Disclosure of passwords	1
Loss of electricity	2
Unauthorized access to the information system	3
Compromising confidential information	5

E. Menentukan *Risk Acceptance*

	Risk Score		Risk Score	Risk Acceptance
	Probability	Impact		
Access to the network by unauthorized persons	4	5	20	High
Disclosure of passwords	2	1	2	Very Low
Loss of electricity	4	2	8	Low
Unauthorized access to the information system	4	3	12	Medium
Compromising confidential information	3	5	15	Medium

RESIKO INHERENT (RESIKO BAWAAN)

Contoh dari resiko inherent :

yaitu terjangkitnya pc/ kompter pada virus trojan yang bisa melalui flasdisk, hardisk, dan menginstal sebuah software yang akan menyebabkan komputer menjadi lambat dan juga virus ini bisa mencuri data- data yang penting. . Virus ini pun bisa merusak sistem operasi sebuah perangkat PC dan merupakan salah satu virus yang mampu mempengaruhi sistem koimputer.

CARA PENGENDALIAN NYA

1.Jangan pernah membuka lampiran pada email

2. Uninstal program yang mengerikan

3. Buka registri editor

4. Update anti virus dan antimalware

5.Scan dalam safe mode

RESIKO AUDIT IT

INHERENT YANG DAPAT TERJADI

1. Kejahatan yang dilakukan dengan menyusup kedalam sistem jaringan komputer tanpa sepengetahuan dari pemilik sistem jaringan komputer. Contohnya : seorang pelaku kejahatan atau hacker melakukan sabotase terhadap informasi yang sangat penting atau mencuri informasi yang sangat penting dan rahasia.
2. Kejahatan dengan memasukkan data atau berupa informasi ke jaringan internet tentang sesuatu yang tidak benar dan melanggar ketentuan hukum. Contohnya pemuatan berita atau informasi yang tidak benar seperti memuat video pornografi, memuat informasi yang sangat rahasia seperti rahasi negara, dll
3. Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan pada dokumen melalu internet.
4. Kejahatan dengan memanfaatkan jaringan internet untuk melakukan mata-mata terhadap pihak yang menjadi sasaran, dengan memasuki sistem jaringan komputer pihak yang menjadi sasarannya.
5. Kejahatan yang dilakukan dengan membuat gangguan, perusakan atau pengahncuran terhadap data atau sistem jaringan komputer. Misalnya menyusupkan virus komputer dimana data yang terkena virus tidak dapat digunakan lagi

CARA PENGENDALIAN NYA

1. Pengendalian secara umum (General control) yang merupakan pengendalian sistem tekonologi informasi yang paling luar dan harus dihadapi terlebih dahulu oleh pemakai sistem informasi. Beberapa pengendaliannya yaitu : Organisasi, dokumentasi, kontrol pencegah kerusakan perangkat, parameter keamanan data, dll.
2. Pengendalian aplikasi merupakan pengendalian yang dipasang pada pengelolaan aplikasinya yaitu berupa : pengendalian masukan, pengendalian pengolahan, dan pengendalian keluaran.

AUDIT IT

KELOMPOK 5

1. ZENA LUSI
2. TRI AKHYARI ROMADHON
3. ABI DAUD

RESIKO AUDIT IT

- Menurut Peltier dalam Gondodiyoto (2007 : 110), risiko adalah sesuatu yang dapat menciptakan atau menimbulkan bahaya.

- Menurut Peltier (2005: 325), “Risiko adalah kemungkinan adanya kelemehan infrastruktur yang kemudian dimanfaatkan oleh ancaman tertentu yang dipengaruhi eksploitasi tersebut.”

JENIS-JENIS RESIKO

1. Risiko Bawaan (*Inherent Risk*)

Risiko bawaan ialah potensi kesalahan atau penyalahgunaan yang melekat pada suatu kegiatan jika tidak ada pengendalian internal.

2. Risiko Pengendalian (*Control Risk*)

Dalam suatu organisasi yang baik seharusnya sudah ada *risk assessment*, dan dirancang pengendalian internal secara optimal terhadap setiap potensi risiko. Risiko pengendalian ialah masih adanya risiko meskipun sudah ada pengendalian

3. Risiko Deteksi (*Detection Risk*)

Risiko deteksi adalah risiko yang terjadi karena prosedur audit yang dilakukan mungkin tidak dapat mendeteksi adanya *error* yang cukup matrealitas atau adanya kemungkinan *fraud*.

CONTOH RESIKO AUDIT IT

PENCURIAN DANA DENGAN KARTU ATM PALSU

1. Pembobolan dana rekening tersebut kemungkinan besar dilakukan oleh orang dalam perusahaan atau orang dalam perbankan dan dilakukan lebih dari satu orang.
2. Karena tidak semua pemilik rekening memiliki hubungan dengan perusahaan tersebut, ada kemungkinan pembocoran informasi itu tidak dilakukan oleh satu perusahaan saja, mengingat jumlah dana yang dibobol sangat besar.
3. Modusnya mungkin penipuan berkedok program yang menawarkan keanggotaan. Korban, yang tergoda mendaftar menjadi anggota, secara tidak sadar mungkin telah mencantumkan informasi-informasi yang seharusnya bersifat rahasia.

4. Pelaku kemungkinan memanfaatkan kelemahan sistem keamanan kartu ATM yang hanya dilindungi oleh PIN.

5. Pelaku juga kemungkinan besar menguasai pengetahuan tentang sistem jaringan perbankan. Hal ini ditunjukkan dengan penggunaan teknik yang masih belum diketahui dan hampir bisa dapat dipastikan belum pernah digunakan sebelumnya.

6. Dari rangkuman berita diatas, disebutkan bahwa para pemilik yang uangnya hilang telah melakukan keluhan sebelumnya terhadap pihak bank. Hal ini dapat diartikan bahwa lamanya bank dalam merespon keluhan-keluhan tersebut juga dapat menjadi salah satu sebab mengapa kasus ini menjadi begitu besar.

PENGENDALIAN NYA

- Melakukan perbaikan atau perubahan sistem keamanan untuk kartu ATM. Dengan penggunaan kartu ATM berbasis chip misalnya, yang dirasa lebih aman dari skimming. Atau dengan penggunaan sistem keamanan lainnya yang tidak bersifat PIN, seperti pengamanan dengan sidik jari, scan retina, atau dengan penerapan tanda tangan digital misalnya.

- Karena pembobolan ini sebagiannya juga disebabkan oleh kelengahan pemilik rekening, ada baiknya jika setiap bank yang mengeluarkan kartu ATM memberikan edukasi kepada para nasabahnya tentang tata cara penggunaan kartu ATM dan bagaimana cara untuk menjaga keamanannya.

TOOLS

Metasploit merupakan sofware security yang sering digunakan untuk menguji coba ketahanan suatu sistem dengan cara mengeksploitasi kelemahan software suatu sistem. Metasploit biasanya digunakan untuk menyerang application layer dengan 1day attack yang merupakan metode penyerangan pada software yang belum di patch. Metasploit biasa dikaitkan dengan istilah remote exploitation! maksudnya penyerang berada pada jarak jangkauan yang jauh dapat mengendalikan komputer korban.Metasploit menyerang dengan cara mengirimkan extasploit pada komputer korban. Exploit ini berisi payload yang sudah ditentukan oleh penyerang.

exploit adalah software yang berfungsi untuk memanfaatkan kelemahan pada software korban(misal web browser)! setelah berhasil mengeksploitasinya exploit tersebut memasukkan payload ke dalam memori korban.payload merupakan sebuah executable milik penyerang yang akan di run pada komputer korban dengan tujuan dapat mengendalikan komputer tersebut secara remote atau memasang backdoor! trojan! "irus! worm! dan lain-lain. Terlepas dari penggunaan metasploit yang disalah gunakan untuk kejahatan! software ini juga membantu System Security untuk memperkuat pertahanan jaringannya dari ulah penyerang dari luar.

IT Audit Tools

NMAP (Network Mapper)

- **Ilsa Palingga Ninditama**
- **Rahma Fitriyani**
- **Ricca Verana Sari**
- **Safta Hastini**
- **Uci Suryani**

NMAP (Network Mapper)

Open source untuk melakukan eksplorasi jaringan dan audit keamanan. Nmap didesain untuk mampu menscan network yang besar, walau NMAP juga sangat handal untuk melakukan scan pada satu host tertentu.

Nmap mempergunakan IP paket raw untuk menentukan host yang aktif pada jaringan, service (nama aplikasi dan versi) yang disediakan oleh host, operating system (versi OS) yang sedang berjalan, tipe filter/firewall yang dipakai, dan karakteristik lainnya.

Nmap biasanya dipakai juga untuk audit keamanan, banyak sistem dan network admin menemukan kemudahan untuk pemakaiannya untuk pemakaian rutin, seperti network inventory,manajemen jadwal update service, monitoring host or service uptime.

Fungsi

NMAP

- Untuk mengeksplorasi jaringan seperti banyaknya administrator system dan jaringan yang menggunakan aplikasi
- Menemukan banyak fungsi dalam inventori jaringan
- Mengatur jadwal peningkatan service.
- Memonitor host atau waktu pelayanan.

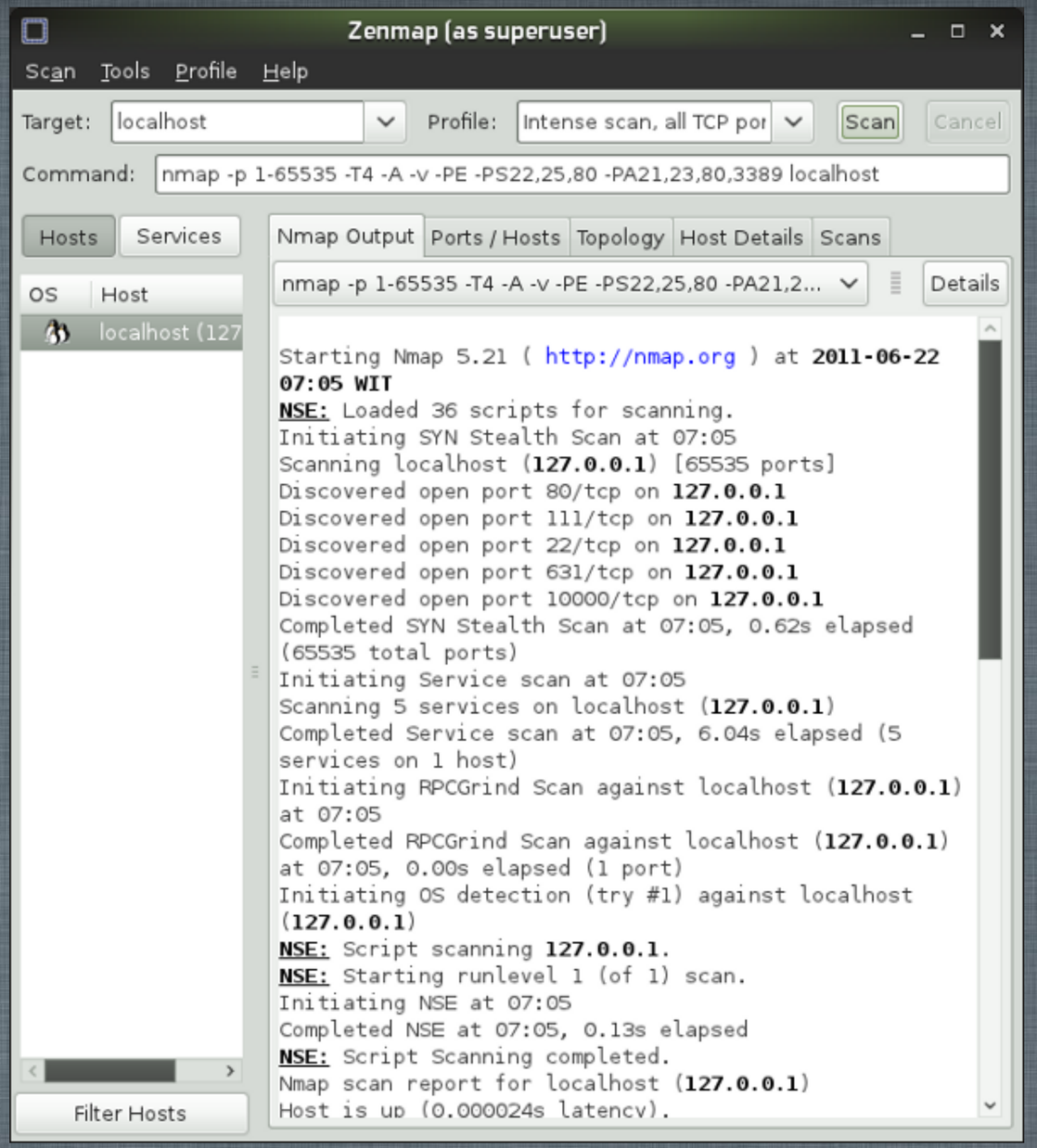
Contoh Penggunaan NMAP Dengan Menggunakan Command Line:

```
wdzgouch@server1:~> nmap localhost

Starting Nmap 5.21 ( http://nmap.org ) at 2011-06-22 10:28 WIT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00028s latency).
rDNS record for 127.0.0.1: linux-34ar.site
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
631/tcp   open  ipp
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Contoh Tampilan Penggunaan NMAP dengan menggunakan Aplikasi GUI: Zenmap.



KESIMPULAN

NMAP adalah sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Output NMAP adalah sebuah daftar target host yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan.

That’s all!

Thank you! ☺

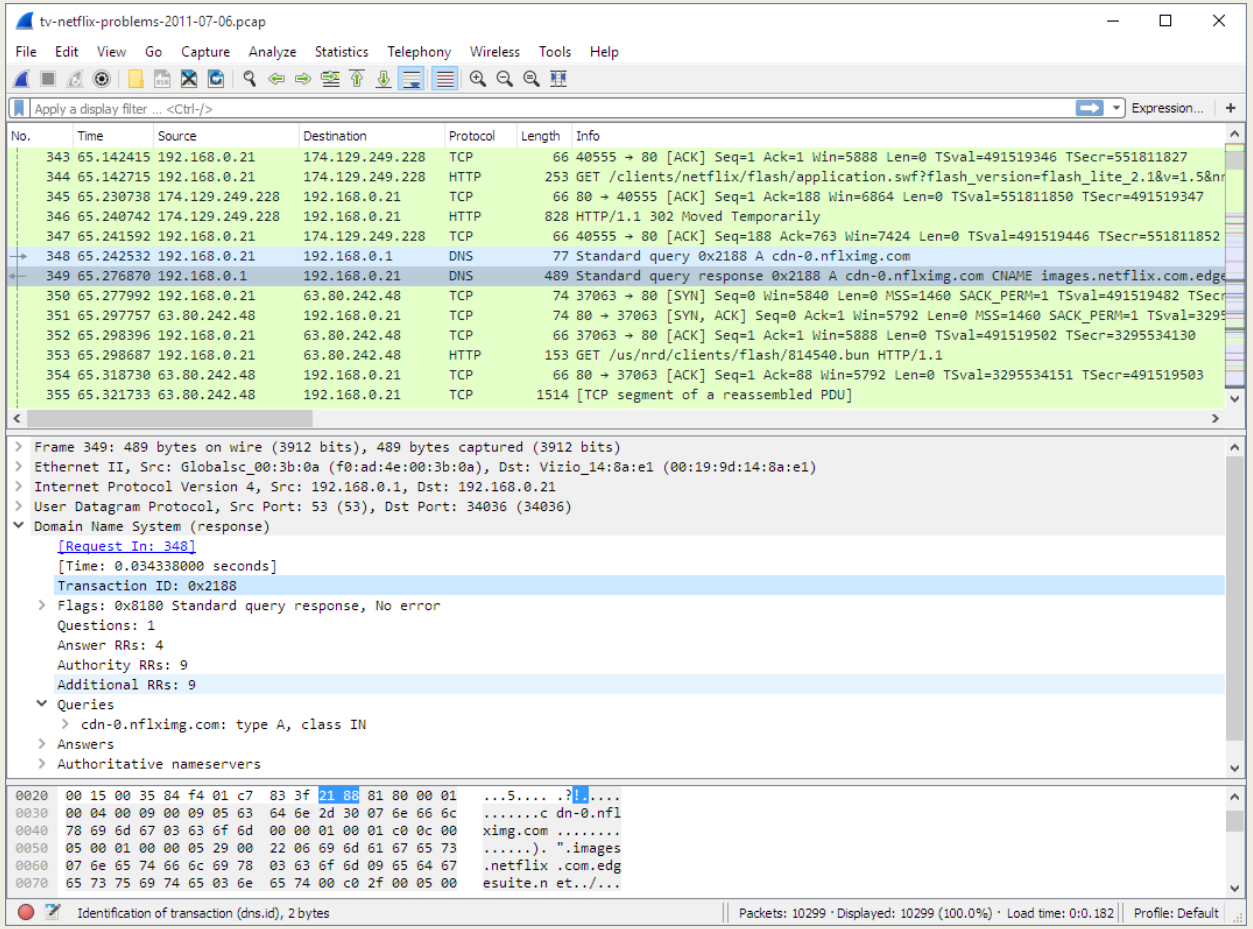
SOFTWARE IT AUDIT TOOLS

WIRESHARK

Disusun Oleh:

1. Muhammad Irvai
2. Muhammad Diah Maulidin
3. Nurhachita
4. Sahirillah
5. Winata Nugraha

Pengertian Wireshark



- Wireshark adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis.

Pengertian Wireshark

- Wireshark adalah sebuah program analisa paket jaringan yang akan mencoba untuk menangkap paket jaringan dan mencoba untuk menampilkan data paket sedetail mungkin. Sehingga dapat melogikakan atau memikirkan sebuah packet analyzer jaringan sebagai alat ukur yang digunakan untuk memeriksa apa yang terjadi di dalam kabel jaringan
- Wireshark mampu menangkap dan paket-paket data/informasi yang ada di dalam jaringan, sehingga data tersebut dapat kita analisa untuk berbagai keperluan, diantaranya:
  - *Troubleshooting masalah di jaringan*
  - *Memeriksa keamanan jaringan*
  - *Sniffer data-data privasi di jaringan*

Tujuan Penggunaan Wireshark

- Beberapa tujuan penggunaan wireshark, yaitu:
  - *administrator jaringan menggunakannya untuk memecahkan masalah jaringan*
  - *insinyur keamanan jaringan menggunakannya untuk memeriksa masalah keamanan*
  - *pengembang menggunakannya untuk men-debug implementasi protocol*
  - *beberapa orang menggunakannya untuk mempelajari protokol jaringan internal*

Tujuan Penggunaan Wireshark

- Wireshark dapat membaca:

- Ethernet
- Token-Ring
- Serial(PPP dan SLIP)
- 802.11 wireless LAN
- Koneksi ATM
- Mengetahui IP chatter(seseorang)
- Proses transmisi dan
- Transmisi data antar komputer

Contoh Penggunaan Wireshark

- Contoh penggunaan WireShark:
  - *Admin sebuah jaringan menggunakannya untuk troubleshooting masalah-masalah di jaringan.*
  - *Teknisi keamanan jaringan menggunakan untuk memeriksa keamanan jaringan.*
  - *Pengembang software biasa menggunakan untuk men-debug implementasi protokol jaringan dalam software.*
  - *Banyak orang menggunakan Wireshark untuk mempelajari protokol jaringan secara lebih terperinci.*
  - *Selain itu digunakan sebagai sniffer atau pencari/pendeteksi data-data privasi jaringan.*

Fitur dan Kelebihan Penggunaan Wireshark

- Fitur dan kelebihan WireShark:
  - *Tersedia untuk Linux dan Windows.*
  - *Menangkap paket data secara langsung dari sebuah network interface.*
  - *Mampu menampilkan informasi yang sangat terperinci mengenai hasil tangkapan tersebut.*
  - *Dapat melakukan import dan export hasil tangkapan dari atau ke komputer lain.*
  - *Pencarian paket menggunakan berbagai macam kriteria filter/pemilahan.*
  - *Dapat membuat berbagai macam tampilan statistika*

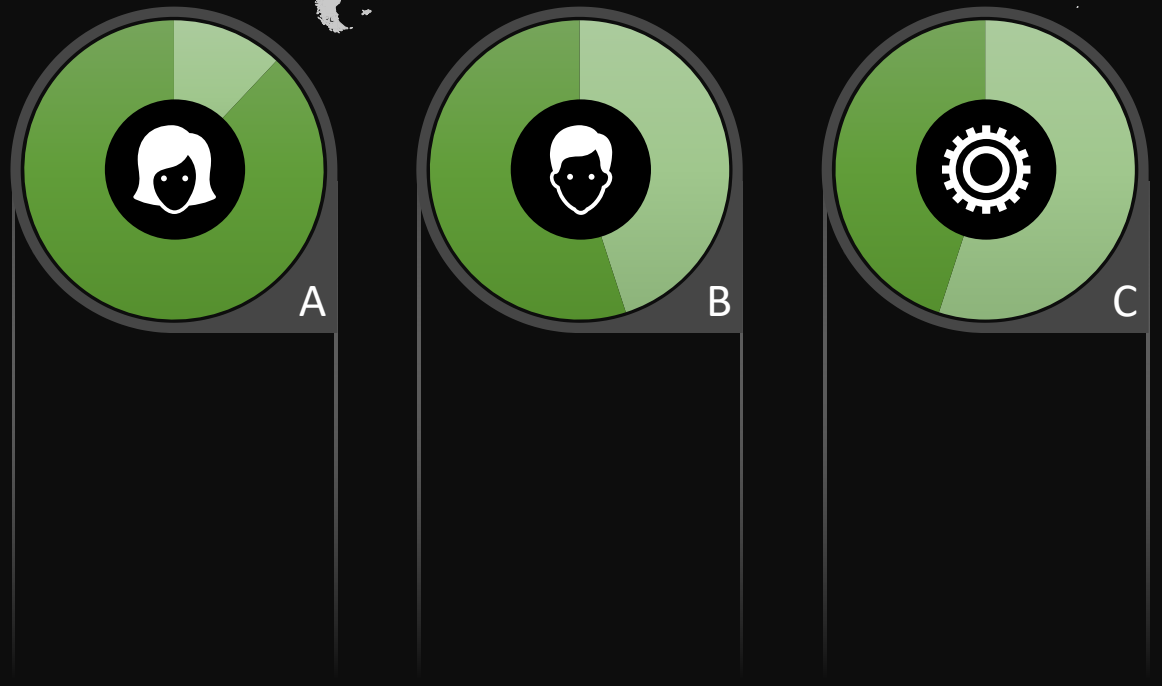
Kesimpulan

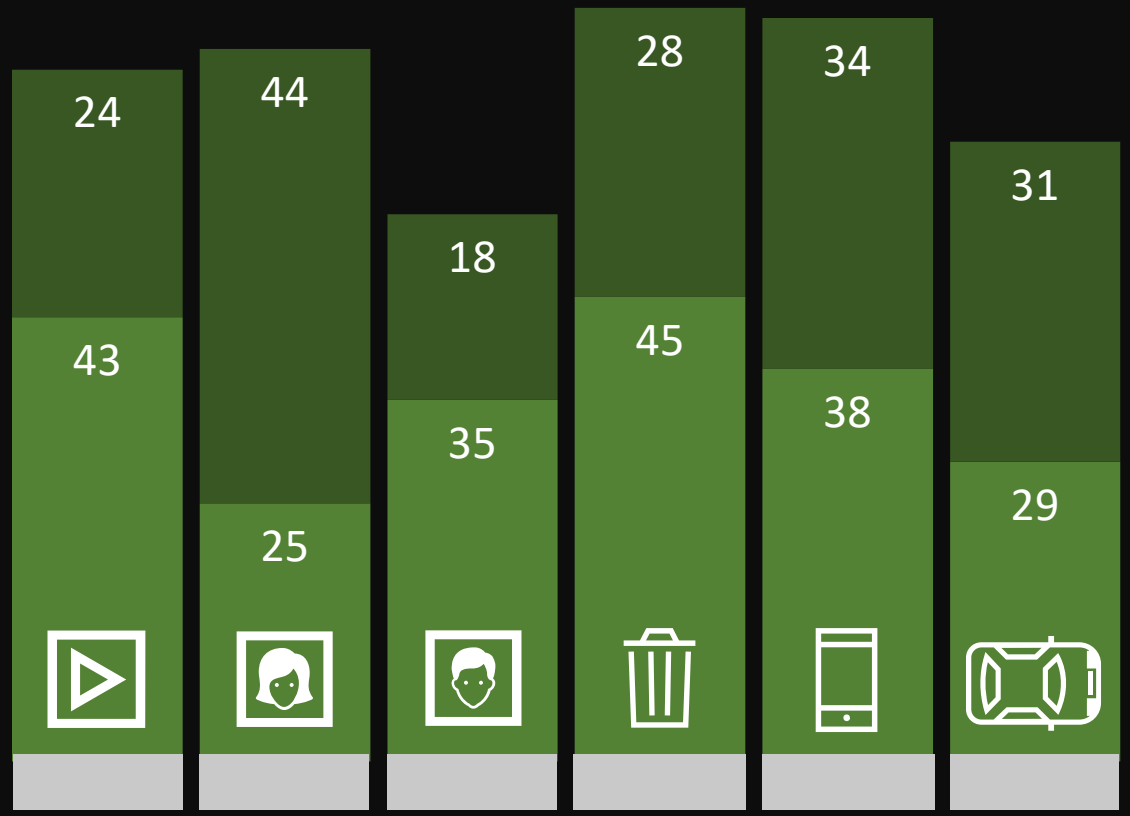
Wireshark adalah tool open source terkemuka yang banyak di gunakan untuk melakukan analisis dan pemecah masalah jaringan, Memungkinkan untuk mengetahui masalah di jaringan. Pengembangan Wireshark berkembang berkat kontribusi relawan ahli jaringan di seluruh dunia. Wireshark di buat dengan bahasa C, C+.

Referensi Wireshark

- http://wireshark.org
- https://seruni.id/cara-menggunakan-wireshark/
- https://medium.com/@kitaadmin/wireshark-adalah-pengertian-dan-fungsi-256dc09c8292
- http://elektro.um.ac.id/wp-content/uploads/2016/05/Modul-Praktikum-3-Analisa-Jaringan-Menggunakan-WireShark.pdf


Locations
Measured


A
B
C


24
43
44
25
18
35
28
45
34
38
31
29

Apa itu SEO..?

SEO adalah singkatan dari "search engine optimization" (pengoptimalan mesin telusur) atau "search engine optimizer". Penggunaan jasa SEO adalah keputusan besar yang dapat meningkatkan peringkat situs Anda dan menghemat waktu, tapi juga berisiko tinggi terhadap situs dan reputasi. Pastikan meneliti kemungkinan keuntungan serta kelemahan yang dapat ditimbulkan oleh SEO yang tidak bertanggung jawab terhadap situs Anda. Banyak SEO dan agen serta konsultan lain yang menyediakan layanan yang bermanfaat bagi pemilik situs web, meliputi:

Ulasan tentang konten atau struktur situs Anda

Saran teknis tentang pengembangan situs web: misalnya, hosting, pengalihan, halaman error, dan penggunaan JavaScript

Pengembangan konten

Manajemen kampanye pengembangan bisnis online

Penelitian kata kunci

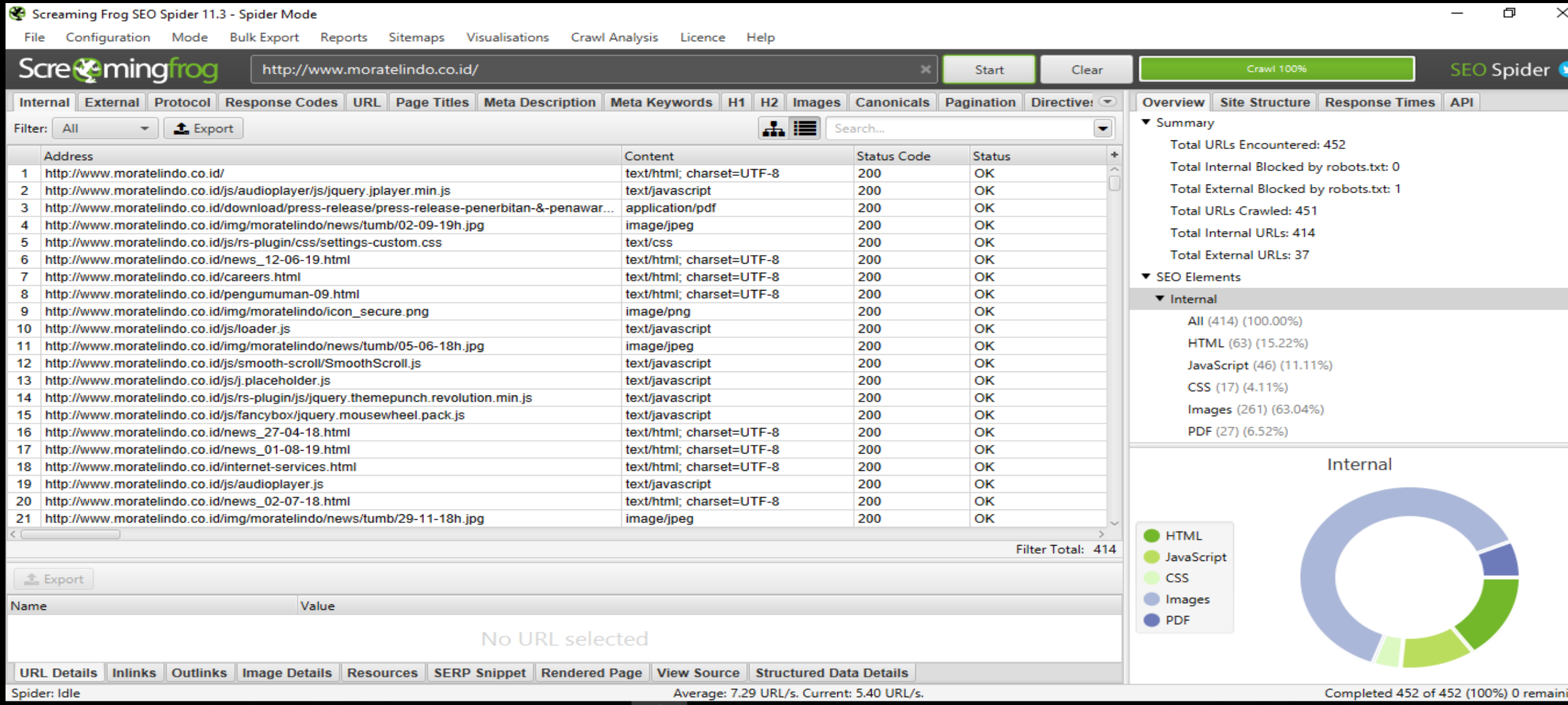
Pelatihan SEO

Keahlian dalam pasar dan geografis tertentu.

Apa itu Screaming Frog?

Screaming Frog SEO Spider adalah sebuah aplikasi desktop yang kecil, Anda dapat menginstal secara lokal di komputer PC, Mac, atau Linux. Dia menjelajahi link, gambar, CSS, dll situs web dari sudut pandang SEO. Yang pada dasarnya memberitahu Anda apa yang akan search spider lihat ketika dia menjelajahi situs web.
Informasi ini memungkinkan Anda untuk dengan cepat menganalisa, audit dan meninjau situs dari perspektif SEO onsite. Hal ini dapat menghemat satu ton pekerjaan, karena secara manual menganalisis setiap halaman website besar bisa sangat menantang.

Screaming Frog



Kesimpulan

Dengan Screaming Frog SEO Spider Anda dapat menganalisis beberapa elemen di tempat, seperti judul halaman, meta descriptions, struktur URL, kode respon, gambar, dll. Ini adalah alat yang hebat untuk membantu Anda mengoptimalkan sebuah situs web dan meningkatkan kinerja di halaman hasil pencarian. Selain itu; itu benar-benar gratis, sehingga seharusnya menjadi alat wajib dalam toolbox setiap desainer web!

IT Audit Tools

NMAP (Network Mapper)

- NAMA : ZENA LUSI
- NIM : 182420016

NMAP (Network Mapper)

- Open source untuk melakukan eksplorasi jaringan dan audit keamanan. Nmap didesain untuk mampu menscan network yang besar, walau NMAP juga sangat handal untuk melakukan scan pada satu host tertentu.

- Nmap mempergunakan IP paket raw untuk menentukan host yang aktif pada jaringan, service (nama aplikasi dan versi) yang disediakan oleh host, operating system (versi OS) yang sedang berjalan, tipe filter/firewall yang dipakai, dan karakteristik lainnya.

- Nmap biasanya dipakai juga untuk audit keamanan, banyak sistem dan network admin menemukan kemudahan untuk pemakaiannya untuk pemakaian rutin, seperti network inventory,manajemen jadwal update service, monitoring host or service uptime.

Kelebihan Nmap :

- Mampu digunakan sebagai network inventory tools dan mapping IP, port, dan services.
- Mampu mendeteksi vulnerability di network.
- Port scanning.
- Relatif mudah digunakan.

Kekurangan Nmap :

- Sulit menemukan issue tertentu terutama vulnerability dibagian aplikasi, nmap pada umumnya digunakan untuk menemukan celah vulnerability di bagian network.

Fungsi NMAP

- Untuk mengeksplorasi jaringan seperti banyaknya administrator system dan jaringan yang menggunakan aplikasi
- Menemukan banyak fungsi dalam inventori jaringan
- Mengatur jadwal peningkatan service.
- Memonitor host atau waktu pelayanan.

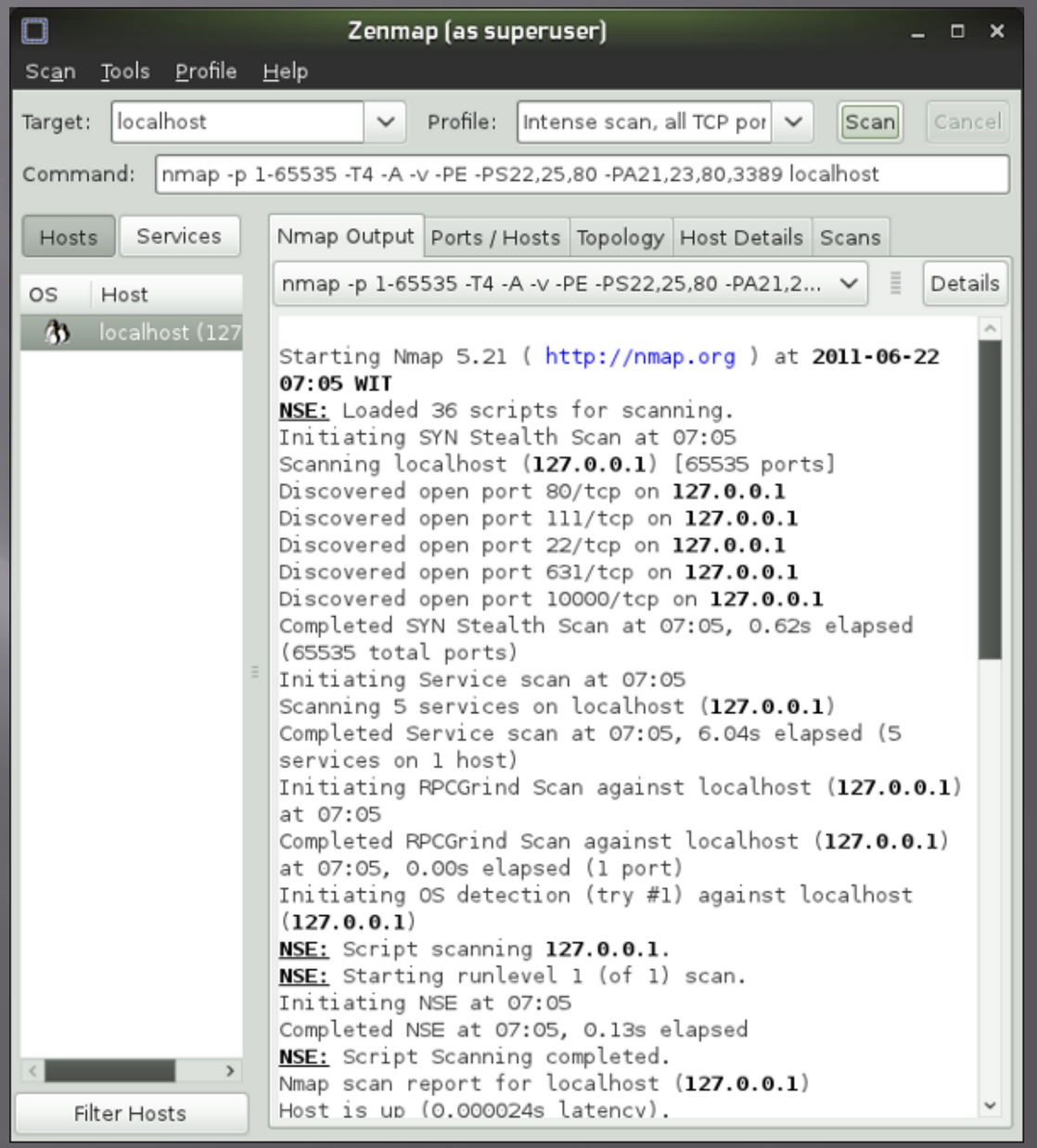
Contoh Penggunaan NMAP Dengan Menggunakan Command Line:

```
wdzgouch@server1:~> nmap localhost

Starting Nmap 5.21 ( http://nmap.org ) at 2011-06-22 10:28 WIT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00028s latency).
rDNS record for 127.0.0.1: linux-34ar.site
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
631/tcp   open  ipp
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Contoh Tampilan Penggunaan NMAP dengan menggunakan Aplikasi GUI: Zenmap.



KESIMPULAN

NMAP adalah sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Output NMAP adalah sebuah daftar target host yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan.

audit TI (Teknologi Informasi)

Audit teknologi informasi (Inggris: information technology (IT) audit atau information systems (IS) audit) adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit teknologi informasi ini dapat berjalan bersama-sama dengan audit finansial dan audit internal, atau dengan kegiatan pengawasan dan evaluasi lain yang sejenis. Pada mulanya istilah ini dikenal dengan audit pemrosesan data elektronik, dan sekarang audit teknologi informasisecara umum merupakan proses pengumpulan dan evaluasi dari semua kegiatan sistem informasi dalam perusahaan itu.

Istilah lain dari audit teknologi informasi adalah audit komputer yang banyak dipakai untuk menentukan apakah aset sistem informasi perusahaan itu telah bekerja secara efektif, dan integratif dalam mencapai target organisasinya. tujuannya untuk mendapatkan dan mengevaluasi fakta yang berkaitan dengan asersi mengenai kejadian dan tindakan ekonomi untuk memastikan kesesuaian antara asersi dengan kriteria yang ditetapkan dan mengkomunikasikan hasilnya kepada pemakai yang berkepentingan.

Secara umum Audit IT adalah suatu proses kontrol pengujian terhadap infrastruktur teknologi informasi dimana berhubungan dengan masalah audit finansial dan audit internal. Audit IT lebih dikenal dengan istilah EDP Auditing (Electronic Data Processing), biasanya digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer. Salah satu penggunaan istilah tersebut adalah untuk menjelaskan proses penelahan dan evaluasi pengendalian-pengendalian internal dalam EDP. Jenis aktivitas ini disebut sebagai auditing melalui komputer. Penggunaan istilah lainnya adalah untuk menjelaskan pemanfaatan komputer oleh auditor untuk melaksanakan

beberapa pekerjaan audit yang tidak dapat dilakukan secara manual. Jenis aktivitas ini disebut audit dengan komputer.

Internal auditing memiliki fungsi penilai independen yang dibentuk dalam organisasi untuk menguji dan mengevaluasi aktivitas-aktivitas dalam organisasi yaitu IIA (Institute of Internal Auditors), yang dilakukan:

- Pemeriksaan keuangan
- Evaluasi efisiensi operasi
- Review kepatuhan (Compliance)
- Mendeteksi kecurangan
- Pemeriksaan IT

Sertifikasinya yaitu CIA (Certified Internal Auditor). Standar, pedoman dan sertifikasi dikelola oleh: IIA.

Tugas Internal Auditor

- Bertanggung jawab kepada direktur
- Menjalankan fungsi internal control
- Membantu organisasi dalam pengukuran dan evaluasi:
- Efektivitas internal controls
- Pencapaian tujuan organisasi
- Ekonomis & efisiensi aktivitas
- Compliance with laws and regulations
- Operational audits

IT Audit Tools (Software)

Tool-tool yang dapat digunakan untuk membantu pelaksanaan Audit Teknologi Informasi. Tidak dapat dipungkiri, penggunaan tool-tool tersebut memang sangat membantu Auditor Teknologi Informasi dalam menjalankan profesinya, baik dari sisi kecepatan maupun akurasinya.

Berikut beberapa software yang dapat dijadikan alat bantu dalam pelaksanaan audit teknologi informasi

a. ACL

ACL dikembangkan sejak tahun 1970-an oleh **Prof. Hart J. Will** dari Canada dan kemudian dikelola oleh **ACL Services Ltd**, Vancouver, Canada, dan merupakan pemimpin pasar dalam teknologi pengambilan data, analisis data, serta pelaporan (hasil survey tahunan **The Institute of Internal Auditors**, USA, 2005).
ACL telah dikembangluaskan dengan fungsi untuk memenuhi kebutuhan analisis data seluruh aktivitas bisnis operasional di dalam perusahaan, di antaranya pada bidang audit untuk analisis data, pencocokan dan pembandingan data, laporan penyimpangan, dsb; pada bidang IT (*Information Technology*) untuk *data migration*, *data cleansing*, *data matching*, *data integrity testing*; selain itu juga untuk analisis, konsolidasi, rekonsiliasi data, dan pelaporan pada divisi lain seperti Keuangan, Pemasaran, Distribusi, Operasional, dan lain sebagainya.

ACL dapat membaca data dari berbagai macam sistem yang terbentang mulai dari model sistem *mainframe* lama hingga ke *relational database* modern. ACL adalah aplikasi yang hanya ‘read-only’, ACL tidak pernah mengubah data sumber asli sehingga aman untuk menganalisis jenis *live-data*. Keanekaragaman sumber data dan teknologi akses data, cara mengakses data juga bervariasi dari satu sumber data ke lain. ACL membaca beberapa sumber data secara langsung dengan mengimpor dan menyalin sumber data sehingga dapat dianalisis. ACL dirancang khusus untuk menganalisa data dan menghasilkan laporan audit baik untuk pengguna biasa (*common/nontechnical users*) maupun pengguna ahli (*expert users*). Dengan menggunakan ACL, pekerjaan auditing akan jauh lebih cepat daripada proses auditing secara manual yang memerlukan waktu sampai berjam-jam bahkan sampai berhari-hari.

Software ini dapat melakukan akses data langsung ke dalam *database* ataupun dalam bentuk teks *fil*e dalam waktu yang singkat tanpa menganggu sistem yang sedang berjalan, melakukan proses verifikasi hasil dari data yang diperoleh untuk menciptakan integrasi data yang dipercaya, dan hasil analisa data yang dapat diandalkan. Semua dapat dilakukan dengan cepat, tepat, aman, dan akurat.

Manfaat ACL antara lain:

- **Bagi auditor:** Penggunaan ACL akan membantu mereka dalam melaksanakan tugas audit secara lebih terfokus, cepat, efisien, efektif, dan murah dengan lingkup yang lebih luas dan analisis mendalam. Indikasi penyimpangan dapat dilakukan dengan cepat, akurat, dan dengan beraneka ragam analisis menggunakan ACL sehingga auditor dapat menemukan lebih banyak penyimpangandan memiliki lebih banyak waktu untuk melakukan pembuktian.
- **Untuk manajemen termasuk profesi akunting dan keuangan:**ACL dapat membantu mereka dalam menganalisis data dan informasi perusahaan, pengujian pengendalian yang telah ada, dan pembuatan laporan manajemen secara cepat dan fleksibel
- **Untuk Sumber Daya Manusia/Pemeriksa, IT, dan lainnya:**Dapat melakukan sistem pelaporan yang sesuai dengan keinginan atau laporan yang diinginkan (independensi) dengan akurasi dan kualitas data yang sangat bagus sehingga data pelaporan dapat dipercaya. Proses pembuatan rekapitulasi dengan sangat cepat.

Audit berbantuan komputer dengan menggunakan *software* **Audit Command Language** dimulai dari pendefinisian berbagai macam tipe data yang dapat dibaca oleh *software* ACL, analisa laporan keuangan perusahaan dimulai dari Neraca beserta Rugi Laba ditelusuri ke Buku Besar dengan menggunakan fungsi yang terdapat pada *software* ACL, yaitu: Verification, Count, Total, Age, Search, Sort, Index, Statistic, Profile, Summarize, Stratification, Sample, Export, Import, Extract, Relation, Joint, Merge, pembuatan laporan yang dihasilkan dari fungsi yang ada di*software* ACl, serta dilengkapi dengan pembuatan batch (meliputi tahapan pemeriksaan laporan keuangan yang dirangkum menjadi satu program.

Fitur dan kemampuan **ACL Software Tools**:

1. ***Universal Data Access***, yaitu dapat mengakses data dari hampir semua jenis *database* yang ada (DBF, XLS, Text File, report file, Oracle, SQL, DB2,

AS/400 FDF, COBOL, dsb) dan semua *platform* (PC, *minicomputer*, dan*mainframe*).

2. **Jumlah Data Besar**, yaitu kemampuan dalam mengakses dan memproses data dalam jumlah yang sangat besar (hingga ratusan juta *record*).
3. **Kecepatan Waktu Proses**, kemampuannya untuk memproses dalam waktu yang singkat walaupun data yang diproses dalam jumlah yang besar.
4. **Integritas Data**, dengan kemampuan mengakses database 100% (tanpa metode *sampling*) serta data yang bersifat *Read Only* yang dapat menjamin orisinalitas, keamanan dan integritas data untuk pengolahan menjadi informasi yang bermanfaat bagi *user* dan manajemen.
5. **Automasi**, pembuatan aplikasi audit yang sangat cepat dan mudah untuk melakukan automasi analisis data untuk efisiensi proses kerja.
6. ***Multi File Process***, dapat digunakan untuk menangani beberapa file sekaligus, tanpa mengganggu operasional teknologi informasi yang dijalankan oleh perusahaan.
7. ***Log File Navigation***, dilengkapi dengan *log file* untuk pencatatan proses analisis yang telah dilakukan sehingga menghasilkan suatu *audit trail* yang komprehensif.
8. **Fungsi Analisis yang Lengkap**, dilengkapi fungsi-fungsi analisis yang sangat lengkap yang dapat dengan mudah dikombinasikan dalam menghasilkan temuan-temuan yang tidak pernah terkirakan sebelumnya.
9. **Pelaporan yang Handal**, kemudahan untuk merancang laporan yang handal sarat informasi yang bermanfaat serta dapat dikirimkan secara otomatis via email atau integrasi ke dalam *software* aplikasi **Crystal Report**.
10. **IT Audit**, kemudahan dalam menguji integritas data dan menganalisis data yang ada di dalam *database* ataupun menganalisis *user-user* yang telah masuk ke dalam suatu jaringan/*network*.

Manfaat menggunakan **ACL Software Tools**:

- Dapat membantu dalam mengAkses data baik langsung (*Direct*) kedalam system jaringan ataupun tidak langsung (*InDirec*t) melalui media lain seperti *softcopy* dalam bentuk *teks file/report*.
- Menempatkan kesalahan dan potensial *fraud* sebagai pembanding dan menganalisa *file-file* menurut aturan-aturan yang ada.
- Mengidentifikasi kecenderungan/gejala-gejala, dapat juga menunjukan dengan tepat/sasaran pengecualian data dan menyoroti potensial area yang menjadi perhatian.
- Mengidentifikasi proses perhitungan kembali dan proses verifikasi yang benar.
- Mengidentifikasi persoalan sistem pengawasan dan memastikan terpenuhinya permohonan dengan aturan-aturan yang telah ditetapkan.
- *Aging* dan menganalisa *Account Receivable/Payable* atau beberapa transaksi lain dengan menggunakan basis waktu yang sensitif.
- Memulihkan biaya atau pendapatan yang hilang dengan pengujian data pada data-data duplikasi pembayaran, menguji data-data nomor*Invoice*/Faktur yang hilang atau pelayanan yang tidak tertagih.
- Menguji terhadap hubungan antara authorisasi karyawan dengan*supplier*.
- Melakukan proses *Data Cleansing* dan *Data Matching* atau pembersihan data dari data-data duplikasi terutama dari kesalahan pengetikan oleh *End-User*.
- Dapat melaksanakan tugas pengawasan dan pemeriksaaan dengan lebih fokus, cepat, efisien, dan efektif dengan lingkup yang lebih luas dan analisa lebih mendalam. Mengidentifikasi penyimpangan (*Fraud Detection*) dapat dilakukan dengan cepat dan akurat sehingga memiliki waktu lebih banyak alam menganalisa data dan pembuktian.

b. Picalo

Picalo merupakan sebuah software CAAT (Computer Assisted Audit Techniques) seperti halnya ACL yang dapat dipergunakan untuk menganalisa data dari berbagai macam sumber.Picalo bekerja dengan menggunakan GUI Front end, dan memiliki banyak fitur untuk ETL sebagai proses utama dalam mengekstrak dan membuka data,

kelebihan utamanya adalah fleksibilitas dan front end yang baik hingga Librari Python numerik.
Berikut ini beberapa kegunaannya :
· Menganalisis data keungan, data karyawan
· Mengimport file Excel, CSV dan TSV ke dalam databse
· Analisa event jaringan yang interaktif, log server situs, dan record sistem login
· Mengimport email kedalam relasional dan berbasis teks database
· Menanamkan kontrol dan test rutin penipuan ke dalam sistem produksi.

c. Powertech Compliance Assessment

Powertech Compliance Assessment merupakan automated audit tool yang dapat dipergunakan untuk mengaudit dan mem-benchmark user access to data, public authority to libraries, user security, system security, system auditing dan administrator rights (special authority) sebuah serverAS/400.

Penilaian Kepatuhan melihat level keamanan dan kerentanan sistem Anda, dan menyarankan langkah-langkah yang dapat Anda ambil untuk melindungi data penting Anda. Sebuah test sistem adalah:

Cepat - test berjalan hanya dalam 10 menit
Rahasia - Hanya Anda yang melihat hasil
Teliti - Penasehat Keamanan yang membantu Anda memahami kondisi keamanan IBM anda saat ini
Clear – kamu dapat mengetahui di mana area sistem anda yang aman dan area yang membutuhkan perbaikan

Software ini mengecek 6 area kritis :

- User Access
- Public Authority
- User Security

- System Security
- System Auditing
- Administrative Rights

d. Nipper

Nipper merupakan audit automation software yang dapat dipergunakan untuk mengaudit dan mem-benchmark konfigurasi sebuah router seperti cisco.
Nipper adalah alat berbasis open source untuk membantu profesional TI dalam mengaudit, konfigurasi dan mengelola jaringankomputer dan perangkat jaringan infrastruktur.

Nipper tidak hanya bisa mengaudit security cisco saja tapi bisa juga alat yang lain , dibawah ini adalah daftar yang bisa di audit oleh nipper :
* Cisco switches (IOS)
* Cisco routers (IOS)
* Cisco firewalls (PIX, ASA, FWSM)
* Cisco Catalyst switches (NMP, CatOS, IOS)
* Cisco Content Service Switches (CSS)
* Juniper NetScreen Firewalls (ScreenOS)

Cara gunakan Nipper
sebagai contoh saya menggunakan cisco router 2600, download nipper disourceforge.net
Kemudian ambil konfigurasi cisco router bisa dengan cara login ke router dengan telnet, kemudian melalui perintah **show running-configuration** copy dan paste output ke Notepad, dan save ke local PC misal di folder C:\nipper .
atau bisa juga menggunakan tftp.
melalui windows command promt ketikkan perintah berikut :
nipper –ios-router –input=testrouterconfig.txt –output=audit.html

Hasil dari perintah tersebut berupa file html, dalam hal ini nama file = audit.html
buka file tersebut dengan browser. File tersebut berisi :

* A software version that has vulnerabilities and the reference numbers for those vulnerabilities
* Recommendations to disable services that might cause others to be able to access the router
* Commands that you need to enable to secure the router
* Upgrade the router's IOS needs to prevent vulnerability to a Telnet remote DoS attack and a TCP listener DoS attack.
* Configure the service tcp-keepalives-in command to help prevent a DoS attack.
* Configure timeouts on consoles to prevent anyone from gaining access to the router from a Telnet or console session.
* Configure the HTTP service as secure with HTTPS, and enable authentication.
* Enable logging.

e. Nessus

Nessus adalah tool bagus yang didesain untuk mengotomatisasi pengujian dan penemuan masalah keamanan dikenal. Biasanya seseorang, sekelompok hacker, perusahaan keamanan, atau peneliti menemukan sebuah cara khusus untuk melanggar keamanan dari produk perangkat lunak. Penemuan ini mungkin disengaja atau melalui penelitian diarahkan; kerentanan, dalam berbagai tingkat detail, kemudian dilepaskan ke komunitas keamanan. Nessus dirancang untuk membantu mengidentifikasi dan memecahkan masalah ini diketahui, sebelum seorang hacker mengambil keuntungan dari mereka. Nessus adalah alat yang hebat dengan banyak kemampuan. Namun itu cukup kompleks dan ada beberapa artikel untuk mengarahkan pengguna baru melalui seluk-beluk cara menginstal dan menggunakannya. Dengan demikian, artikel ini akan berusaha untuk menutupi dasar-dasar setup dan konfigurasi Nessus. Fitur dari versi

terbaru Nessus (Nessus 2.0.8a dan NessusWX 1.4.4) akan dibahas. Tulisan berikutnya akan mencakup Nessus secara lebih mendalam.

Nessus adalah sebuah program bebas yang dirilis di bawah GPL.Secara historis, banyak di dunia usaha telah diejek perangkat lunak domain publik seperti sebagai buang-buang waktu, bukan memilih “didukung” produk yang dikembangkan oleh perusahaan mapan. Biasanya ini ratusan biaya paket atau ribuan dolar, dan sering dibeli menggunakan logika bahwa Anda mendapatkan apa yang Anda bayar. Beberapa orang mulai menyadari bahwa perangkat lunak domain publik, seperti Nessus, tidak selalu lebih rendah dan kadang-kadang benar-benar unggul. Dukungan teknis dibayar untuk Nessus bahkan tersedia darihttp://www.tenablesecurity.com. Nessus juga memiliki komunitas besar pengembang berlabuh oleh penulis utama, Renaud Deraison. Bila dibiarkan cukup bersaing dalam tinjauan terhadap kerentanan scanner lain, Nessus telah menyamai atau outshined produk seharga ribuan dolar. [Ref: Keamanan Informasi, Network Computing]

Nessus dapat digunakan untuk melakukan audit sebagai berikut:
* credentialed and un-credentialed port scanning
* network based vulnerability scanning
* credentialed based patch audits for Windows and most UNIX platforms
* credentialed configuration auditing of most Windows and UNIX platforms
* robust and comprehensive credentialed security testing of 3rd party applications
* custom and embedded web application vulnerability testing
* SQL database configuration auditing
* software enumeration on Unix and Windows
* testing anti-virus installs for out-of date signatures and configuration errors

Salah satu fitur yang sangat kuat dari Nessus adalah klien teknologi servernya. Server dapat ditempatkan pada titik-titik strategis di jaringan memungkinkan tes yang akan dilakukan dari berbagai titik pandang. Seorang klien pusat atau klien didistribusikan beberapa dapat mengontrol semua server. Bagian server akan berjalan pada hampir

semua rasa Unix. Bahkan berjalan pada MAC OS X dan IBM / AIX, tetapi Linux cenderung membuat instalasi sederhana.Fitur-fiturini memberikan banyak fleksibilitas untuk penguji penetrasi. Klien tersedia untuk Windows dan Unix. Server Nessus melakukan pengujian yang sebenarnya sementara klien menyediakan fungsi konfigurasi dan pelaporan.

f. Metasploit

Metasploit merupakan sofware security yang sering digunakan untuk menguji coba ketahanan suatu sistem dengan cara mengeksploitasi kelemahan software suatu sistem. Metasploit biasanya digunakan untuk menyerang application layer dengan 0 day attack yang merupakan metode penyerangan pada software yang belum di patch. Metasploit biasa dikaitkan dengan istilah remote exploitation, maksudnya penyerang berada pada jarak jangkauan yang jauh dapat mengendalikan komputer korban. Metasploit menyerang dengan cara mengirimkan exploit pada komputer korban. Exploit ini berisi payload yang sudah ditentukan oleh penyerang. Exploit adalah software yang berfungsi untuk

memanfaatkan kelemahan pada software korban(misal web browser), setelah berhasil mengeksploitasinya exploit tersebut memasukkan payload ke dalam memori korban. Payload merupakan sebuah executable milik penyerang yang akan di run pada komputer korban dengan tujuan dapat mengendalikan komputer tersebut secara remote atau memasang backdoor, trojan, virus, worm, dan lain-lain. Terlepas dari penggunaan metasploit yang disalah gunakan untuk kejahatan, software ini juga membantu System Security untuk memperkuat pertahanan jaringannya dari ulah penyerang dari luar.

g. NMAP

NMAP merupakan open source utility untuk melakukan security auditing. NMAP

atau Network Mapper, adalah software untuk mengeksplorasi jaringan, banyak administrator sistem dan jaringan yang menggunakan aplikasi ini menemukan banyak fungsi dalam inventori jaringan, mengatur jadwal peningkatan service, dan memonitor host atau waktu pelayanan. Secara klasik Nmap klasik menggunakan tampilan command-line, dan NMAP suite sudah termasuk tampilan GUI yang terbaik dan tampilan hasil (Zenmap), fleksibel data transfer, pengarahan ulang dan tools untuk debugging (NCAT) , sebuah peralatan untuk membandingan hasil scan (NDIFF) dan sebuah paket peralatan analisis untuk menggenerasikan dan merespon (NPING)

h. Wireshark

WIRESHARK adalah satu dari sekian banyak tool Network Analyzer yang dipakai oleh orang – orang yang bekerja di bidang jaringan yang ingin melihat atau menganalisa paket jaringan, pengembangan protokol jaringan serta edukasi bagi yang ingin memperdalam ilmu nya dalam jaringan komputer. Yang menjadi kelebihan bagi wireshark adalah lisensi nya yang free alias open source. Tentu hal ini sangat menarik minat orang untuk menggunakan aplikasi ini bagi pekerjaan di bidang jaringan. Selain itu Wireshark juga dibuat dengan berbasiskan GUI yang cukup baik dan bagus.
Aplikasi ini juga dapat menangkap paket-paket data/informasi yang ada dalam jaringan yang kita ingin liahat. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang *tool* ini juga dapat dipakai untuk *sniffing* (memperoleh informasi penting spt*password* email
atau *account* lain) dengan menangkap paket-paket yang berseliweran di dalam jaringan dan menganalisanya.

i.Backtrack

BackTrack adalah salah satu distro linux yang merupakan turunan dari slackware yang mana merupakan merger dari whax dan auditor security collection. Backtrack dua dirilis pada tanggal 6 maret 2007 yang memasukkan lebih dari 300 tool security sedangkan

versi beta 3 dari backtrack dirilis pada tanggal 14 desember 2007 yang pada rilis ketiga ini lebih difokuskan untuk support hardware. Sedangkan versi backtrack 3 dirilis pada tanggal 19 juni 2008 pada backtrack versi 3 ini
memasukkan saint dan maltego sedangkan nessus tidak dimasukkan serta tetap memakai kernel versi 2.6.21.5. pada BackTrack 4 Final sekarang ini menawarkan kernel linux terbaru yaitu kernel 2.6.30.4. Sekaligus pada Rilis BackTrack 4, dapat dikatakan berpindah basis yakni dari dahulu yang Slackware menjadi berbasis Ubuntu. Dilengkapi juga dengan patch untuk wireless driver untuk menanggulangi serangan wireless injection (wireless injection attacks).
BackTrack menyediakan akses mudah untuk tools komprehensif yang berhubungan dengan keamanan, mulai dari Port Scanner sampai Password Scanner. Dukungan fungsi Live CD dan Live USB mengijinkan pengguna untuk me-boot BackTrack secara langsung dari media penyimpan portabel tanpa harus melakukan penginstallan pada Hardisk secara permanen.

J.aircrack-ng

Aircrack-ng adalah sebuah cracking program untuk 802.11 WEP dan WPA wireless keys, kegunaan nya adalah untuk merecover password wireless yang di enkripsi dengan mengumpul kan sebanyak-banyaknya paket data yang berhasil di tangkap dan menggenerate password nya. inti nya adalah aircrack-ng merupakan satu set tool untuk mengaudit wireless password.

Aircrack-ng biasa nya bisa di operasi kan dari distro linux semacam Backtrack atau Gentoo, tapi pada dasar nya semua distro linux mampu menjalan kan nya, dan untuk windows walaupun bisa tapi sangat terbatas cara pengoperasian dan tutorial nya pun sangat jarang di bahas.

k.Snort

Snort adalah sebuah program yang memiliki tiga fungsi atau tiga modus operasi. Snort dapat dipakai dalam **packet sniffer mode** sehingga bekerja sebagai sniffer sama seperti Wireshark. Sama seperti Wireshark, Snort juga dapat menyimpan setiap packet yang di-capture ke dalam media penyimpan di modus **packet logger mode**. Akan tetapi berbeda dengan Wireshark, Snort dapat dipakai sebagai komponen NIDS dengan menjalankannya pada **Network Intrusion Detection System (NIDS) mode**. Pada modus yang terakhir ini, Snort akan menganalisa packet berdasarkan rule yang ada untuk mengenali adanya upaya serangan hacker.

I.Netcut

Netcut yaitu aplikasi pemotong koneksi yang dapat dibuktikan dapat bekerja untuk memotong jaringan wi-fi ataupun jaringan lainnya. Langkah kerjanya yaitu menciptakan ip baru kloningan dari ip tujuan kita hingga dapat mengakibatkan ip conflict pada koneksi korban. Netcut sudah merilis kembali versi netcut terbaru yakni netcut 3. Didalam versi barunya ini, netcut sudah memberikan beragam spesifikasi serta di antara spesifikasi baru yang saya sukai yaitu fitur change mac. Dengan spesifikasi change mac netcut, anda dapat menyembunyikan identitas pc atau laptop anda didalam sesuatu jaringan.
Pencurian bandwith memutuskan koneksi dengan teoritis amat manjur untuk menambah kecepatan akses internet, contohnya sesuatu jaringan memperoleh jarah 100 kb/s serta dapat dibagi pada 10 client maka tiap-tiap client dapat beroleh 10 kb/s. Dengan netcut, maka kita dapat mengambil keputusan koneksi 9 client yang lain serta jatah 100 kb/s dapat jadi milik kita.

Jenis Audit IT

1. Sistem dan aplikasi
2. Mengidentifikasikan resiko dan kendali

3. Mengevaluasi kendali dan mengumpulkan bukti-bukti
4. Mendokumentasikan
5. Menyusun laporan

Manfaat Audit IT

A. Manfaat pada saat Implementasi (Pre-Implementation Review)

- Institusi dapat mengetahui apakah sistem yang telah dibuat sesuai dengan kebutuhan ataupun memenuhi acceptance criteria.
- Mengetahui apakah pemakai telah siap menggunakan sistem tersebut.
- Mengetahui apakah outcome sesuai dengan harapan manajemen.

B. Manfaat setelah sistem live

- Institusi mendapat masukan atas risiko-risiko yang masih yang masih ada dan saran untuk penanganannya.
- Masukan-masukan tersebut dimasukkan dalam agenda penyempurnaan sistem, perencanaan strategis, dan anggaran pada periode berikutnya.
- Bahan untuk perencanaan strategis dan rencana anggaran di masa mendatang.
- Memberikan reasonable assurance bahwa sistem informasi telah sesuai dengan kebijakan atau prosedur yang telah ditetapkan.
- Membantu memastikan bahwa jejak pemeriksaan (audit trail) telah diaktifkan dan dapat digunakan oleh manajemen, auditor maupun pihak lain yang berwewenang melakukan pemeriksaan.
- Membantu dalam penilaian apakah initial proposed values telah terealisasi dan saran tindak lanjutnya.

Alasan Melakukan Audit IT

Ron Webber, Dekan Fakultas Teknologi Informasi, monash University, dalam salah satu bukunya Information System Controls and Audit (Prentice-Hall, 2000) menyatakan beberapa alasan penting mengapa Audit IT perlu dilakukan, antara lain:

- Kerugian akibat kehilangan data.
- Kesalahan dalam pengambilan keputusan.
- Resiko kebocoran data.
- Penyalahgunaan komputer.
- Kerugian akibat kesalahan proses perhitungan.
- Tingginya nilai investasi perangkat keras dan perangkat lunak komputer.

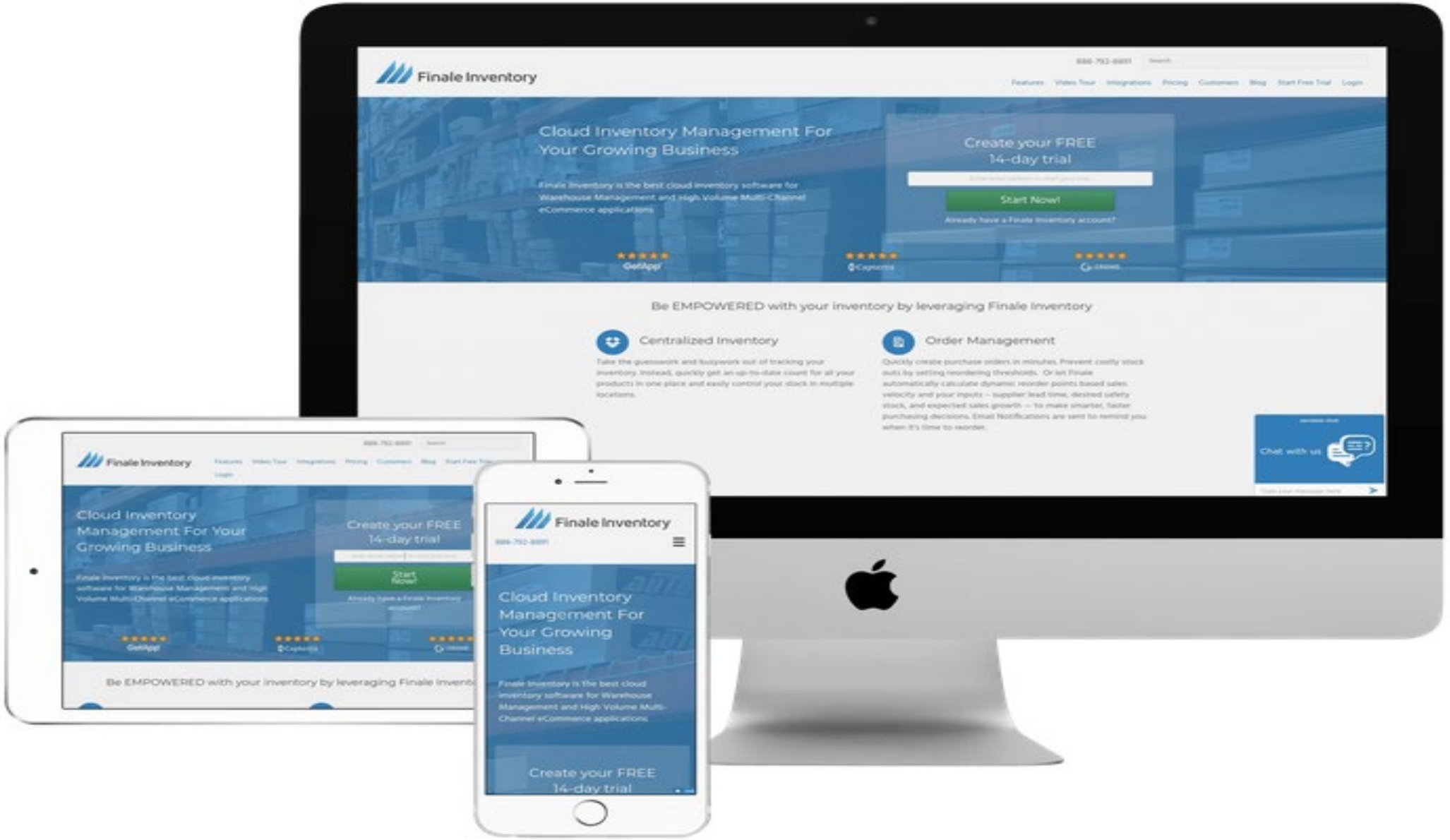
RESIKO AUDIT

OLEH
AHKMAD IPANDY
ANGGARI AYU P
ARVIAN AGUSAPUTRA
DEDI ZULKARNAIN

TOOL AUDIT INVENTORY

INVENTORY AUDIT SOFTWARE: FINALE INVENTORY

Mengelola persediaan dan pesanan adalah komponen penting untuk setiap bisnis berbasis inventaris. Ketidakmampuan untuk melacak barang-barang ini dapat menyebabkan pesanan tertunda, pesanan hilang, dan dalam skenario terburuk, kehilangan pelanggan. Melakukan audit inventaris secara teratur sangat penting untuk memastikan bahwa Anda menghindari sakit kepala operasional. Itu sebabnya bisnis beralih ke perangkat lunak audit inventaris untuk menghemat waktu, tenaga, dan uang.


Finale Inventory
Cloud Inventory Management For Your Growing Business
Create your FREE 14-day trial
Start Now!
Be EMPOWERED with your inventory by leveraging Finale Inventory
Centralized Inventory
Order Management
Chat with us
Finale Inventory
Cloud Inventory Management For Your Growing Business
Create your FREE 14-day trial
Start Now!
Finale Inventory
Cloud Inventory Management For Your Growing Business
Create your FREE 14-day trial

RESIKO AUDIT

risiko salah saji bersifat material dan/atau penggelapan (fraud) yang bisa lolos dari proses audit jika auditor tidak melakukan tugasnya secara cermat. Auditor menyadari bahwa risiko tersebut ada karena adanya hal-hal sebagai berikut, misalnya ketidakpastian mengenai kompetensi bukti, efektivitas struktur pengendalian intern klien, serta ketidakpastian apakah laporan memang telah disajikan secara wajar setelah audit selesai.

Jenis Resiko Audit

RESIKO BAWAAN

Risiko bawaan (Inherent risk) merupakan kerentanan asersi terhadap salah saji (misstatement) yang material, dengan mengasumsikan bahwa tidak ada pengendalian yang berhubungan

RESIKO PENGENDALIAN

risiko yang bisa timbul akibat kelemahan sistim pengendalian intern (SPI) auditee, entah karena desainnya yang lemah atau pelaksanaanya yang tidak sesuai desain

RESIKO DITEKSI

risiko yang bisa timbul akibat kegagalan auditor dalam menedeteksi adanya salahsaji bersifat material dan/atau penggelapan (fraud)

AUDITOR SALAH MENETAPKAN LANGKAH PENGUJIANNYA (PROSEDUR AUDIT)

prosedur pengeluaran barang menetapkan bahwa setiap pengeluaran barang harus didasarkan pada permintaan dari pihak yang akan menggunakan. Jadi dalam pelaksanaan pengeluaran barang akan terdapat dua populasi bukti yang saling terkait, bukti permintaan barang dan bukti pengeluaran barang.

prosedur audit “periksa apakah atas setiap bukti permintaan barang terdapat bukti pengeluaran barangnya!” Prosedur ini dipastikan tidak akan menemukan kesalahan seperti kecurangan pihak gudang yang mengeluarkan barang walaupun tidak ada permintaan dari pihak yang membutuhkan barang, karena jika ada permintaan barang dapat dipastikan bagian gudang akan menerbitkan bukti pengeluaran barang

prosedur audit yang ditetapkan adalah: “periksa apakah atas setiap bukti pengeluaran barang terdapat bukti permintaan barangnya!” maka prosedur ini mungkin akan dapat menemukan kecurangan bagian gudang atas pengeluaran barang yang tidak didasarkan pada permintaan barang. Dengan prosedur tersebut, jika seandainya bagian gudang melakukan kecurangan mengeluarkan barang tetapi bukan untuk kepentingan perusahaan, maka akan dapat ditemukan dari sampel pengeluaran barang yang tidak ditemukan bukti permintaan barangnya

CONTOH RESIKO DITEKSI

PENGENDALIAN

Aditor memahami prosedur dan dukumen yang akan di audit.

Menggunakan semua dokumen prosedur sebagai bukti untuk dilakukan audit

control

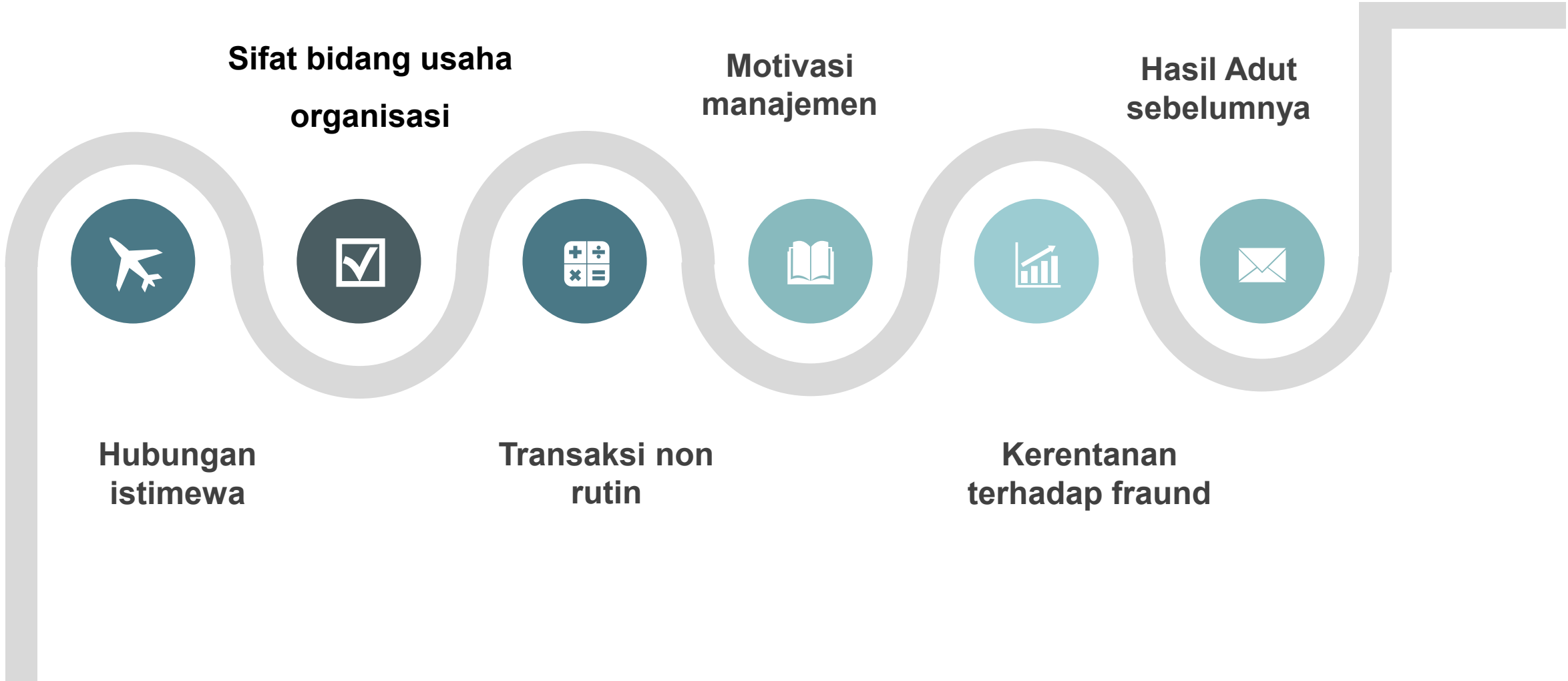
Dilakukan pelatihan bagi auditor, sehingga auditor paham mengenai model risiko audit

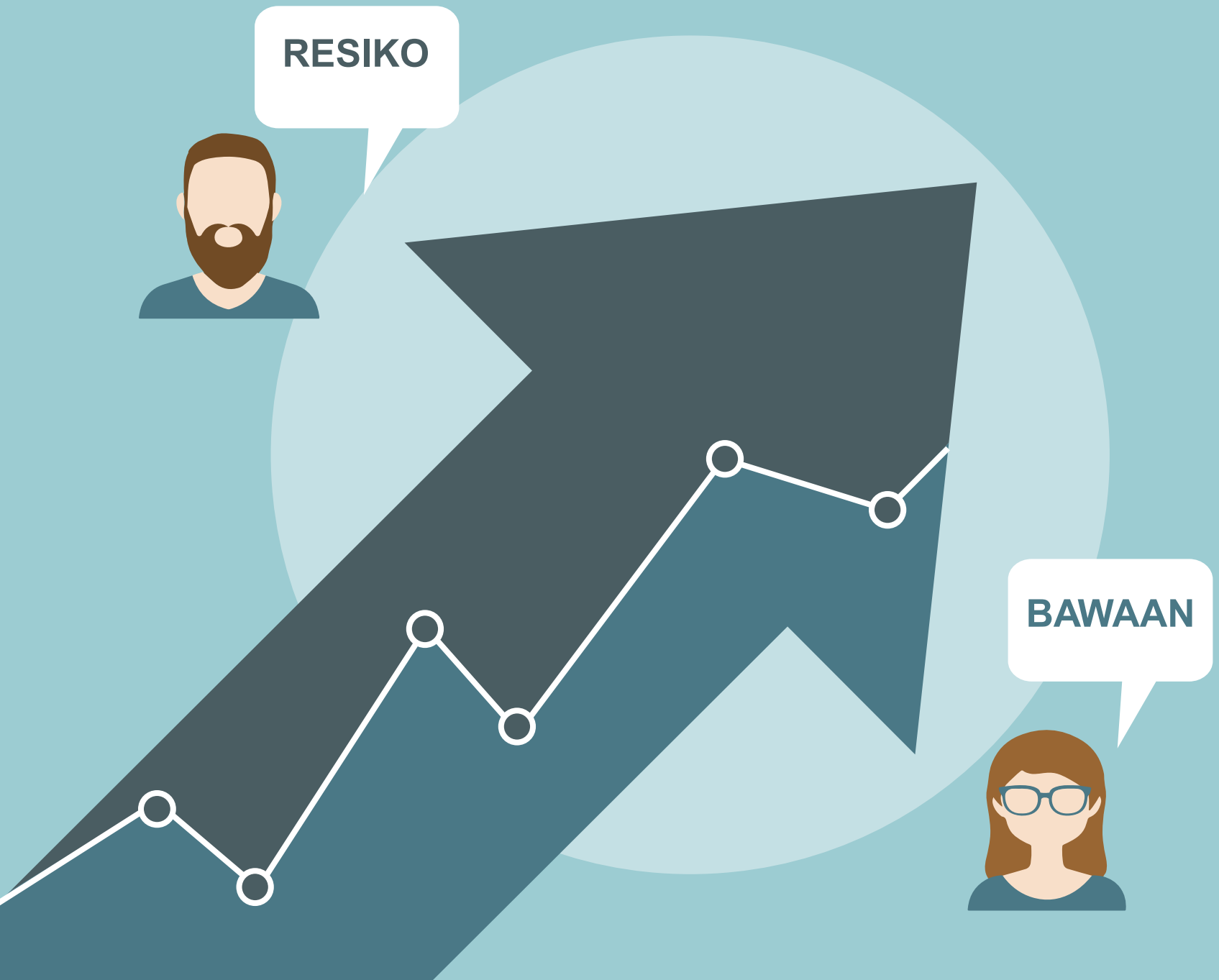
Merancang luasnya pengujian dan menggunakan metode audit yang baik sehingga agar auditor tidak mengalami risiko audit (dalam arti audit menjadi tidak efektif), serta agar audit dapat dilaksanakan secara efisien (dalam arti audit dapat menghindarkan diri, melakukan perluasan pengujian yang tidak perlu).

CONTOH RESIKO BAWAAN

Perhitungan yang rumit lebih mungkin disajikan salah jika dibandingkan dengan perhitungan yang sederhana. Akun yang terdiri dari jumlah yang berasal estimasi akuntansi cenderung mengandung risiko lebih besar dibandingkan dengan akun yang sifatnya rutin dan berisi data berupa fakta.

Faktor-faktor yang perlu ditelaah auditor dalam menetapkan risiko bawaan





Risiko bawaan selalu ada dan tidak pernah mencapai angka nol. Risiko bawaan tidak dapat diubah oleh penerapan prosedur audit yang paling baik sekalipun.

Contoh resiko pengendalian

Audit pada bagian Persediaan.
memeriksa apakah ada 2 pekerjaan terkait atau lebih dirangkap oleh satu orang petugas

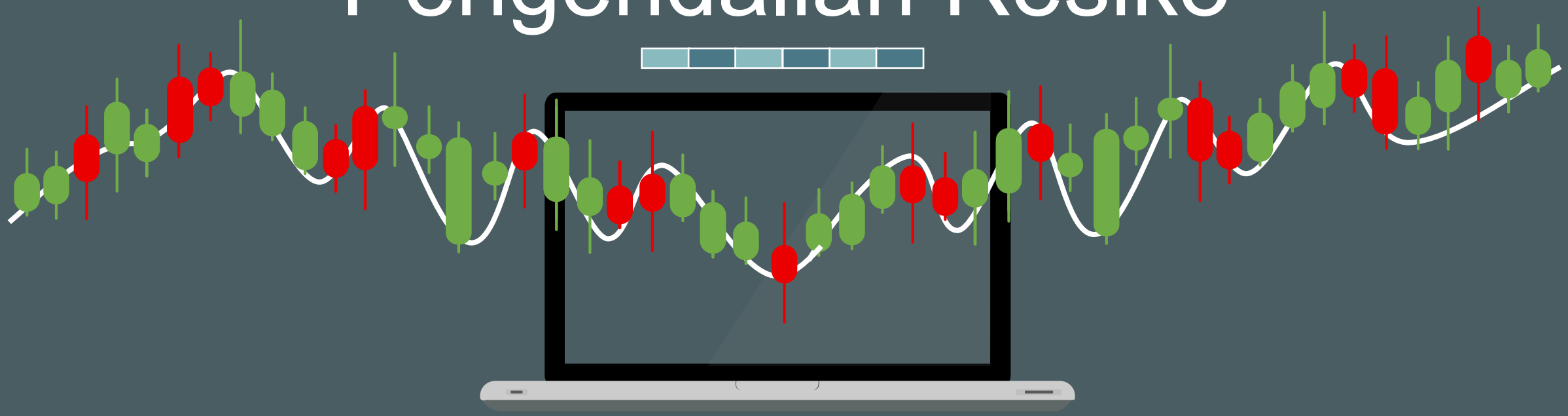
Pegawai Purchasing merangkap sebagai petugas yang penerima barang atau pekerjaan gudang persediaan lainnya (ini buruk); atau Pegawai Shipping merangkap sebagai petugas gudang yang mengurus persediaan barang jadi (ini juga buruk).

Foreman di bagian produksi (yang biasa request persediaan untuk keperluan produksi) diijinkan bebas keluar-masuk gudang persediaan bahan baku atau bahan penolong (ini buruk).

Pegawai admin yang input Receipt of Goods (ROG) memiliki kemampuan akses ke dalam data-data accounting terkait seperti Accounts Payable (Utang)

Pegawai admin yang input picking sheet di Shipping memiliki kemampuan akses ke dalam data-data accounting terkait seperti Accounts Receivable (Piutang).

Pengendalian Resiko



Resiko pengendalian ini tidak bisa dikendalikan oleh auditor akan tetapi bisa dikendalikan oleh auditee

Cara pengedalain resiko :

1. melakukan pembagian tugas yang jelas
2. Melakukan audit internal dan bila diperlukan memiliki bagian audit tersendiri
3. Memperkuat pengawasan manajemen terhadap pegawai


Thank You

Saya memilih IT Audit Tools ACL *(Audit Command Language).*

ACL dikembangkan sejak tahun 1970-an oleh **Prof. Hart J. Will** dari Canada dan kemudian dikelola oleh **ACL Services Ltd**, Vancouver, Canada, dan merupakan pemimpin pasar dalam teknologi pengambilan data, analisis data, serta pelaporan (hasil survey tahunan **The Institute of Internal Auditors**, USA, 2005).

ACL telah dikembangluaskan dengan fungsi untuk memenuhi kebutuhan analisis data seluruh aktivitas bisnis operasional di dalam perusahaan, di antaranya pada bidang audit untuk analisis data, pencocokan dan pembandingan data, laporan penyimpangan, dsb; pada bidang IT (*Information Technology*) untuk *data migration*, *data cleansing*, *data matching*, *data integrity testing*; selain itu juga untuk analisis, konsolidasi, rekonsiliasi data, dan pelaporan pada divisi lain seperti Keuangan, Pemasaran, Distribusi, Operasional, dan lain sebagainya.
ACL dapat membaca data dari berbagai macam sistem yang terbentang mulai dari model sistem *mainframe* lama hingga ke *relational database* modern. ACL adalah aplikasi yang hanya 'read-only', ACL tidak pernah mengubah data sumber asli sehingga aman untuk menganalisis jenis *live-data*. Keanekaragaman sumber data dan teknologi akses data, cara mengakses data juga bervariasi dari satu sumber data ke lain. ACL membaca beberapa sumber data secara langsung dengan mengimpor dan menyalin sumber data sehingga dapat dianalisis. ACL dirancang khusus untuk menganalisa data dan menghasilkan laporan audit baik untuk pengguna biasa (*common/nontechnical users*) maupun pengguna ahli (*expert users*). Dengan menggunakan ACL, pekerjaan auditing akan jauh lebih cepat daripada proses auditing secara manual yang memerlukan waktu sampai berjam-jam bahkan sampai berhari-hari.
Software ini dapat melakukan akses data langsung ke dalam *database* ataupun dalam bentuk teks *fil*e dalam waktu yang singkat tanpa menganggu sistem yang sedang berjalan, melakukan proses verifikasi hasil dari data yang diperoleh untuk menciptakan integrasi data yang dipercaya, dan hasil analisa data yang dapat diandalkan. Semua dapat dilakukan dengan cepat, tepat, aman, dan akurat.

Manfaat ACL antara lain:

- **Bagi auditor:** Penggunaan ACL akan membantu mereka dalam melaksanakan tugas audit secara lebih terfokus, cepat, efisien, efektif, dan murah dengan lingkup yang lebih luas dan analisis mendalam. Indikasi penyimpangan dapat dilakukan dengan cepat, akurat, dan dengan beraneka ragam analisis menggunakan ACL sehingga auditor dapat menemukan lebih banyak penyimpangandan memiliki lebih banyak waktu untuk melakukan pembuktian.

- **Untuk manajemen termasuk profesi akunting dan keuangan:** ACL dapat membantu mereka dalam menganalisis data dan informasi perusahaan, pengujian pengendalian yang telah ada, dan pembuatan laporan manajemen secara cepat dan fleksibel

- **Untuk Sumber Daya Manusia/Pemeriksa, IT, dan lainnya:** Dapat melakukan sistem pelaporan yang sesuai dengan keinginan atau laporan yang diinginkan (independensi) dengan akurasi dan kualitas data yang sangat bagus sehingga data pelaporan dapat dipercaya. Proses pembuatan rekapitulasi dengan sangat cepat.

  Audit berbantuan komputer dengan menggunakan *software* **Audit Command Language** dimulai dari pendefinisian berbagai macam tipe data yang dapat dibaca oleh *software* ACL, analisa laporan keuangan perusahaan dimulai dari Neraca beserta Rugi Laba ditelusuri ke Buku Besar dengan menggunakan fungsi yang terdapat pada *software* ACL, yaitu: Verification, Count, Total, Age, Search, Sort, Index, Statistic, Profile, Summarize, Stratification, Sample, Export, Import, Extract, Relation, Joint, Merge, pembuatan laporan yang dihasilkan dari fungsi yang ada di *software* ACl, serta dilengkapi dengan pembuatan batch (meliputi tahapan pemeriksaan laporan keuangan yang dirangkum menjadi satu program.

  Fitur dan kemampuan **ACL Software Tools**:

1. ***Universal Data Access***, yaitu dapat mengakses data dari hampir semua jenis *database* yang ada (DBF, XLS, Text File, report file, Oracle, SQL, DB2, AS/400 FDF, COBOL, dsb) dan semua *platform* (PC, *minicomputer*, dan *mainframe*).
2. **Jumlah Data Besar**, yaitu kemampuan dalam mengakses dan memproses data dalam jumlah yang sangat besar (hingga ratusan juta *record*).
3. **Kecepatan Waktu Proses**, kemampuannya untuk memproses dalam waktu yang singkat walaupun data yang diproses dalam jumlah yang besar.
4. **Integritas Data**, dengan kemampuan mengakses database 100% (tanpa metode *sampling*) serta data yang bersifat *Read Only* yang dapat menjamin orisinalitas, keamanan dan integritas data untuk pengolahan menjadi informasi yang bermanfaat bagi *user* dan manajemen.
5. **Automasi**, pembuatan aplikasi audit yang sangat cepat dan mudah untuk melakukan automasi analisis data untuk efisiensi proses kerja.
6. ***Multi File Process***, dapat digunakan untuk menangani beberapa file sekaligus, tanpa mengganggu operasional teknologi informasi yang dijalankan oleh perusahaan.
7. ***Log File Navigation***, dilengkapi dengan *log file* untuk pencatatan proses analisis yang telah dilakukan sehingga menghasilkan suatu *audit trail* yang komprehensif.
8. **Fungsi Analisis yang Lengkap**, dilengkapi fungsi-fungsi analisis yang sangat lengkap yang dapat dengan mudah dikombinasikan dalam menghasilkan temuan-temuan yang tidak pernah terkirakan sebelumnya.
9. **Pelaporan yang Handal**, kemudahan untuk merancang laporan yang handal sarat informasi yang bermanfaat serta dapat dikirimkan secara otomatis via email atau integrasi ke dalam *software* aplikasi **Crystal Report**.
10. **IT Audit**, kemudahan dalam menguji integritas data dan menganalisis data yang ada di dalam *database* ataupun menganalisis *user-user* yang telah masuk ke dalam suatu jaringan/*network*.

Manfaat menggunakan **ACL Software Tools**:

- Dapat membantu dalam mengAkses data baik langsung (*Direct*) kedalam system jaringan ataupun tidak langsung (*InDirec*t) melalui media lain seperti *softcopy* dalam bentuk *teks file/report*.
- Menempatkan kesalahan dan potensial *fraud* sebagai pembanding dan menganalisa *file-file* menurut aturan-aturan yang ada.
- Mengidentifikasi kecenderungan/gejala-gejala, dapat juga menunjukan dengan tepat/sasaran pengecualian data dan menyoroti potensial area yang menjadi perhatian.
- Mengidentifikasi proses perhitungan kembali dan proses verifikasi yang benar.
- Mengidentifikasi persoalan sistem pengawasan dan memastikan terpenuhinya permohonan dengan aturan-aturan yang telah ditetapkan.
- *Aging* dan menganalisa *Account Receivable/Payable* atau beberapa transaksi lain dengan menggunakan basis waktu yang sensitif.
- Memulihkan biaya atau pendapatan yang hilang dengan pengujian data pada data-data duplikasi pembayaran, menguji data-data nomor *Invoice*/Faktur yang hilang atau pelayanan yang tidak tertagih.
- Menguji terhadap hubungan antara authorisasi karyawan dengan *supplier*.
- Melakukan proses *Data Cleansing* dan *Data Matching* atau pembersihan data dari data-data duplikasi terutama dari kesalahan pengetikan oleh *End-User*.
- Dapat melaksanakan tugas pengawasan dan pemeriksaaan dengan lebih fokus, cepat, efisien, dan efektif dengan lingkup yang lebih luas dan analisa lebih mendalam. Mengidentifikasi penyimpangan (*Fraud Detection*) dapat dilakukan dengan cepat dan akurat sehingga memiliki waktu lebih banyak alam menganalisa data dan pembuktian.

IT AUDIT TOOLS

ANGGARI AYU P

ACL
(AUDIT COMMAND LANGUAGE)

- Sebuah software CAAT (Computer Assisted Audit Techniques) yang sudah sangat populer untuk melakukan analisa terhadap data dari berbagai macam sumber.
- ACL tidak pernah mengubah data sumber asli sehingga aman untuk menganalisis jenis live-data.
- ACL dirancang khusus untuk menganalisa data dan menghasilkan laporan audit baik untuk pengguna biasa (common/nontechnical users) maupun pengguna ahli (expert users). Dengan menggunakan ACL, pekerjaan auditing akan jauh lebih cepat daripada proses auditing secara manual yang memerlukan waktu sampai berjam-jam bahkan sampai berhari-hari.

ACL
(AUDIT COMMAND LANGUAGE)

Ada 2 jenis yang utama dalam pengkodean dalam komputer, yaitu:

- EBCDIC (Extended Binary Coded Decimal Interchang Code) – format ini seringkali ditemukan pada komputer jenis IBM Mainframe.
- ASCII (American Standard Code for Information Interchange) – format ini hampir digunakan dibanyak komputer. ACL dapat membaca langsung baik jenis EBCDIC atau ASCII, sehingga tidak perlu untuk menngkonversi kedalam bentuk lain.

FUNGSI ACL (AUDIT COMMAND LANGUAGE)

- Bidang Auditor

Pengguna ahli ini memiliki latar belakang yang memungkinkan dia menjadi seorang auditor sehingga ACL yang digunakannya bisa ditafsirkan dan digunakan untuk mempermudah pekerjaannya sebagai auditor. Manfaat ACL yang dapat dirasakan oleh seorang auditor dalam penggunaan ACL ini adalah ACL bisa membantu auditor dalam melaksanakan tugasnya yaitu mengaudit laporan keuangan perusahaan secara fokus, cepat, efisien dan akurat. Karena teknologi pada intinya dibuat untuk mempermudah pekerjaan manusia, untuk mengurangi kesalahan yang bisa terjadi dan untuk mempercepat pekerjaan.

FUNGSI ACL (AUDIT COMMAND LANGUAGE)

- Bidang Manajemen

Dalam suatu peruahaan ada bagian keuangannya, bagian keuangan inilah yang dimaksudnya manajemen. Bagian keuangan bisa melakukan analisis suatu data perusahaan menggunakan ACL untuk tujuan tertentu seperti melakukan analisis terhadap penjualan, bagaimana trending penjualan dan lain sebagainya. Selain digunakan manajemen untuk melakukan analisis data ACL juga bisa dilakukan untuk pengujian pengendalian perusahaan. Kalau sudah masuk kedalam pengendalian internal ini menyangkut auditing. Pengendalian internal sangat diperlukan untuk mengetahui apakah kemungkinan perusahaan melakukan kecurangan tinggi atau tidak. Penjelasan lebih dalam tentang pengendalian internal akan dibahas dalam auditing. ACL juga bisa digunakan manajemen dalam pembuatan laporan yang diinginkan. Manajemen dapat menggunakan ACL untuk :

- Analisis data
- Pengujian pengendalian perusahaan
- Pembuatan laporan keuangan yang diinginkan

KEMAMPUAN ACL

- ·Mudah dalam penggunaan. ACL for Windows sesuai dengan namanya adalanh softwere berbasis windows, dimana sistem operasi windows telah dikenal user Friendly (mudah dipengguna). Kemudahan ini ditunjukan dengan user hanya melakukan click pda gambar-gambar tertentu(icon) untuk melakukan suatu pekerjaan dan didukung pula fasilitas Wizard untuk mendefinisikan data yang akan dianalisis.
- Built-in audit dan analisis data secara fungsional. ACL for Windows didukung dengan kemampuan analisis untuk keperluan audit / pemeriksaan seperti : Analisis Statistik, menghitung total, stratifikasi, sortir, index dll
- Kemampuan menangani file yang tidak terbatas. ACL for Windows mampu menangi berbagai jenis file dengan ukuran file yang tidak terbatas.
- Kemampuan untuk membaca berbagai macam tipe data. ACL for Windows dapat membaca file yang berasal dari berbagai format antara lain : Flate Sequential dBase (DBS). Text (TXT), Delimited, Print, ODBC (Microsoft Acces database, Oracle).
- Kemampuan untuk mengeksport hasil audit ke berbagai macam format data antara lain: Plain Text (TXT), dBase III (DBF), Delimited (DEL), Excel (XLS),Lotus (WKS), Word (DOC) dan WordPerfect (WP).

TIPE-TIPE DATA YANG BISA DIBACA OLEH ACL

- Flate Sequential

  Flat Sequential file data berisi baris atas consecutive data yang diatur satu persatu setelah yang lainnya.

- Dbase

  ACL secara otomatis dapat mendeteksi, menganalisa dan kemudian membuat suatu format dBase file.

- TXT

  File data berupa text berisi hanya karakter yang bisa dicetak.semacam huruf dari a sampai z, angka 1 sampai 9 dan sebagian besar tombol pada keyboard).

- Delimited

  Kebanyakan file data berisi field yang tidak memiliki posisi tetap dalam sebuah record.

- Print Files

  Print Files adalah text dalam bentuk laporan tercetak.

- ODBC

  ODBS adalah singkatan dari “Open Database Conectivity”. Merupakan sebuah teknologi APL (Aplication Programing Laterface)standar yang memungkinkan aplikasi mengakses multiple database dari pihak ke tiga.

- Tape

  ACL dengna mudah mengakses dan membaca data root tape atau cartiges. Mengakses suatu file pada tape ha,pir sama dengan memproses file dengan disk based file.

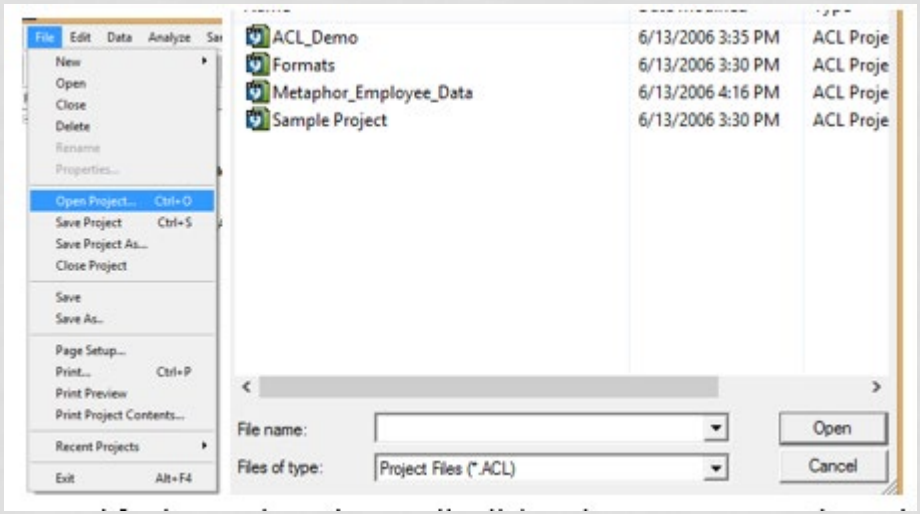
KEMAMPUAN ACL(AUDIT COMMAND LANGUAGE)

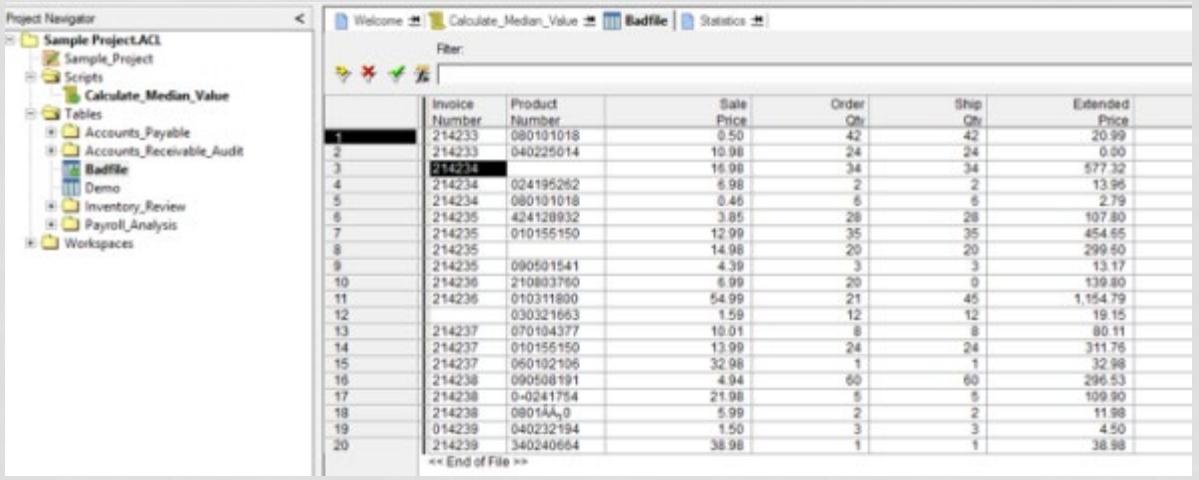
- Mudah dalam penggunaan (user friendly).
- Built-in audit dan analisis data secara fungsional.
- Kemampuan untuk mengeksport hasil audit ke berbagai macam format data.
- Kemampuan menangani ukuran file yang tidak terbatas.
- Pembuatan laporan yang berkualitas.

MANFAAT ACL(AUDIT COMMAND LANGUAGE)

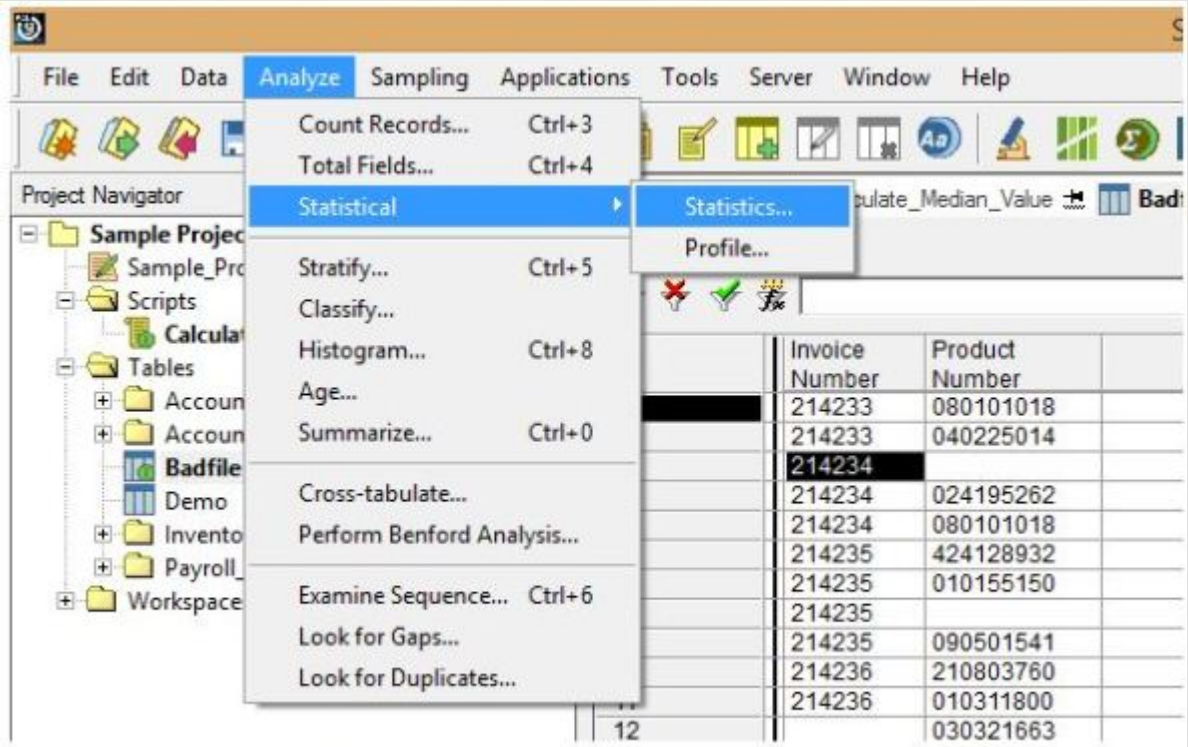
- Dapat membantu dalam mengakses data baik secara langsung (direct) ke dalam sistem jaringan ataupun tidak langsung (indirect) melalui media lain seperti softcopy dalam bentuk textfile/ report.
- Menempatkan kesalahan dan potensial “fraud” sebagai pembanding dan menganalisa file-file menurut aturan yang ada.
- Mengidentifikasi proses perhitungan kembali dan proses verifikasi yang benar
- Dapat melaksanakan tugas pengawasan dan pemeriksaaan dengan lebih fokus, cepat, efisien, dan efektif dengan lingkup yang lebih luas dan Analisa lebih mendalam. Mengidentifikasi penyimpangan (Fraud Detection) dapat dilakukan dengan cepat dan akurat sehingga memiliki waktu lebih banyak alam menganalisa data dan pembuktian.

CONTOH MENGGUNAKAN ACL PADA VERSI ACL 9 UNTUK MELIHAT DATA BERUPA STATISTIKA



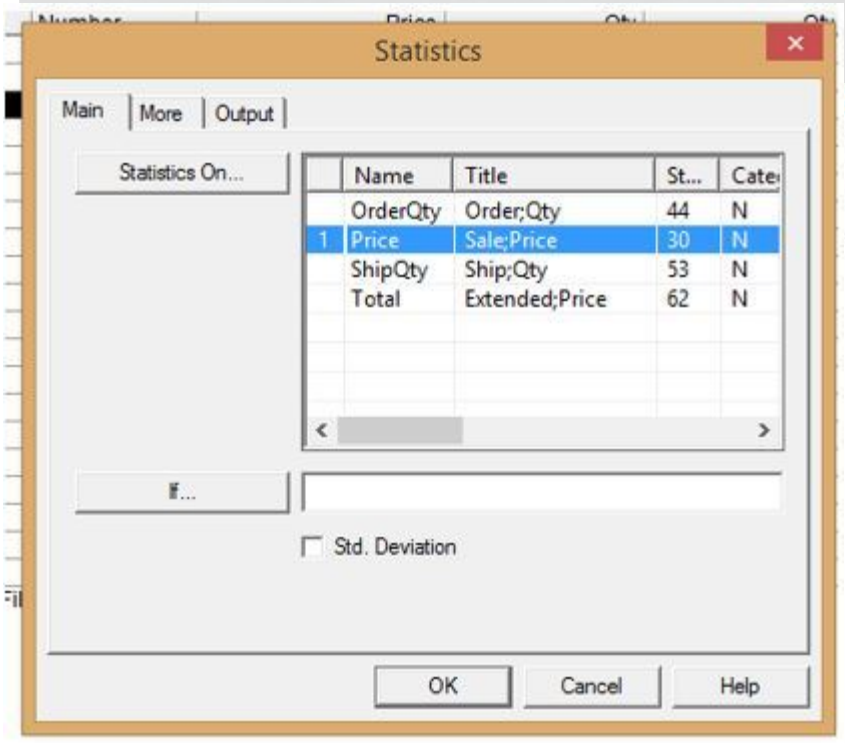


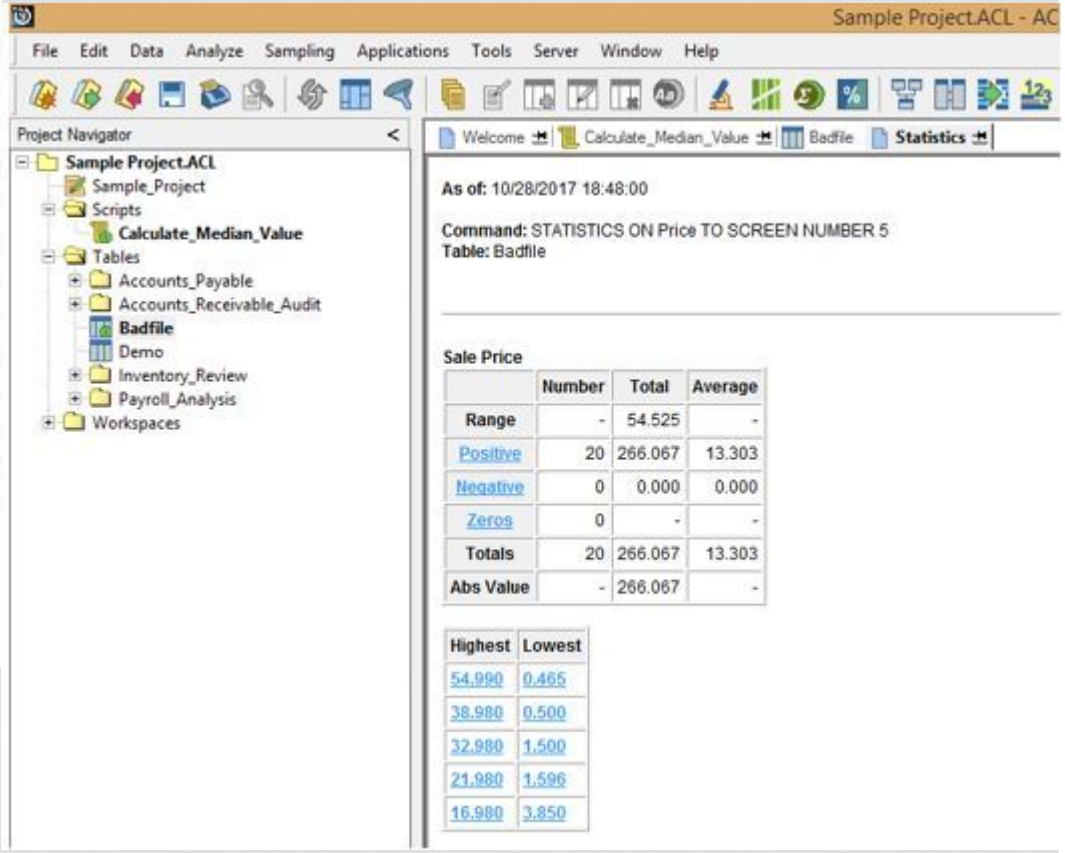
CONTOH MENGGUNAKAN ACL PADA VERSI ACL 9 UNTUK MELIHAT DATA BERUPA STATISTIKA



pilih menu Analyze dan pilih Statistical > Statistics...

CONTOH MENGGUNAKAN ACL PADA VERSI ACL 9 UNTUK MELIHAT DATA BERUPA STATISTIKA





Kelompok autopsy

M apriliansyah
Singgih hananta
Edi supriyadi
Pamuji muhammad jaka
Anshori

AUTOPSY

- **APLIKASI AUTOPSY**
- Autopsy adalah sebuah antarmuka grafis untuk tool-tool didalam sleuth kit,yang memudahkan pengguna dalam melakukan investigasi. Mereka dapat menganalisis disk dan file system windows dan unix (NTFS, FAT, UFS1/2,EXT2/3). Autopsy menyediakan fungsi manajemen kasus, integritas gambar, pencarian kata kunci, dan operasi lainnya.
- Autopsy menggunakan perl untuk menjalankan program-program sleuth kit dan mengubah hasilnya ke HTML, olehkarena itu pengguna autopsy membutuhkan web client untuk mengakses fungsi-fungsinya

- Autopsy sebenarnya adalah sebuah mini web server dengan script CGI berbasis perl.
- Autopsy menggunakan perl untuk menjalankan pr ogram-program sleuth kit dan mengubah hasilnya ke HTML. Oleh karena itu pengguna autopsy membutuhkan web client untuk mengakses fungsi-fungsi autopsy. Selain sebagaiuser interface sleuthkit, autopsy menyediakan fungsi-fungsi administratif tambahan. Beberapa fungsi tersebut adalah logging (mencatat tindakan /perintah sleuth kit yang telah di jalankan), notes (mencatat keterangan tambahan yang di peroleh penyelidik), dan report (mencatat hasil analisa

CONTOH GAMBAR APLIKASI

Fitur Autopsy :

- Multi-User Cases: Berkolaborasi dengan sesama penguji dalam kasus besar.
- Timeline Analysis: Menampilkan kejadian sistem dalam antarmuka grafis untuk membantu mengidentifikasi aktivitas.
- Ekstraksi String Unicode: Ekstrak senar dari ruang yang tidak terisi dan jenis file yang tidak dikenal dalam banyak bahasa (Arab, Cina, Jepang, dll.)
- Tag: Tag file dengan nama tag yang sewenang-wenang, seperti 'bookmark' atau 'curiga', dan tambahkan komentar.
- Keyword Search: Teks ekstraksi dan indeks dicari modul memungkinkan Anda untuk menemukan file yang menyebutkan istilah tertentu dan menemukan pola ekspresi reguler.
- Web Artifacts: Ekstrak aktivitas web dari browser umum untuk membantu mengidentifikasi aktivitas pengguna.
- Registry Analysis: Kegunaan RegRipper Untuk mengidentifikasi dokumen dan perangkat USB yang baru diakses.
- Analisis File LNK: Mengidentifikasi jalan pintas dan dokumen yang mudah diakses
- Email Analysis: MBOX Format pesan, seperti Thunderbird.
- EXIF: Ekstrak lokasi geografis dan informasi kamera dari file JPEG.

Fitur Autopsy :

- Sortir Jenis File: Kelompokkan file menurut jenisnya untuk menemukan semua gambar atau dokumen.
- Pemutaran Media: Lihat video dan gambar dalam aplikasi dan tidak memerlukan penampil eksternal.
- Penampil Thumbnail: Menampilkan thumbnail gambar untuk membantu melihat gambar dengan cepat.
- Robust File System Analysis: Dukungan untuk sistem berkas yang umum, termasuk NTFS, FAT12/FAT16/FAT32/ExFAT, HFS+, ISO9660 (CD-ROM), Ext2/Ext3/Ext4, Yaffs2, and UFS dari The Sleuth Kit
- Hash Set Filtering: Saring file yang diketahui dengan baik NSRL Dan flag file buruk yang diketahui menggunakan hashsets khusus dalam format HashKeeper, md5sum, dan EnCase.
- Deteksi Tipe File berdasarkan tanda tangan dan deteksi ketidakcocokan ekstensi.
- Modul File yang Menarik akan menandai file dan folder berdasarkan nama dan path.
- Dukungan Android: Ekstrak data dari SMS, log panggilan, kontak, Tango, Words with Friends, dan banyak lagi.

Penutup

- Kesimpulan

  Autopsy adalah sebuah antarmuka grafis untuk tool-tool didalam sleuth kit, yang memudahkan pengguna dalam melakukan investigasi. Tiap host harus menggunakan port terpisah. Autopsy menggunakan cookies untuk memvalidasi hal ini.

Evaluasi IT Governance Menggunakan Framework COBIT 5 (Studi Kasus : PT. XYZ)

Luzi Dwi Oktaviana[1], Prayoga Pribadi[2], Melly Sabrinawati[3]

[1,2,3] Sistem Informasi
STMIK Amikom Purwokerto
Email : oktaviana@amikompurwokerto.ac.id[1], yoga@amikompurwokerto.ac.id[2], mellysabrinaa@gmail.com[3]

ABSTRAK

PT. XYZ merupakan perusahaan yang bergerak dibidang distributor pelumas oli dan rem. Dalam menjalankan proses bisnisnya terdapat kendala yaitu apabila sistem mati ataupun error tidak dapat mengirimkan barang karena dalam pengiriman barang harus disertai dengan surat faktur. Tentunya hal ini tidak sesuai dengan visi misi perusahaan yang ingin memberikan kepuasan pelanggan salah satunya dalam hal ketepatan waktu dalam pengiriman. Penelitian ini membahas mengenai evaluasi tata kelola teknologi informasi dengan tujuan untuk mengukur tingkat kapabilitas tata kelola teknologi informasi. Peneliti menggunakan *framework* COBIT 5 dan menghasilkan domain teridentifikasi yaitu EDM02, APO04, APO09, DSS01, MEA01. Maka ditemukan hasil perhitungan *capability level* berada pada level 3 yaitu telah dikelola, dijalankan, dan diimplementasikan dalam cara yang lebih teratur.

Kata Kunci: Evaluasi Tata Kelola, Teknologi Informasi, COBIT 5, Capability level

ABSTRACT

PT. XYZ depot is a company engaged in the distributor of oil and brake lubricants. In carrying out the business process there are obstacles, namely if the system dies or errors cannot deliver goods because in the delivery of goods must be accompanied by an invoice. Of course this is not in accordance with the vision and mission of the company who wants to provide customer satisfaction, one of them in terms of the timeliness of delivery. This study discusses the evaluation of information technology governance with the aim of measuring the level of information technology governance capabilities. The researcher uses the COBIT 5 framework and produces identifiable domains namely EDM02, APO04, APO09, DSS01, MEA01. Then it is found that the calculation of capability level is at level 3, which has been managed, implemented, and implemented in a more regular way.

Keywords: Management Evaluation, Information Technology, COBIT 5, capability level

PENDAHULUAN

Kemajuan perkembangan teknologi informasi dan komunikasi telah berkembang dengan sangat pesat, hampir disetiap kehidupan manusia sudah terdapat teknologi di dalamnya, baik itu teknologi sederhana maupun yang sudah modern. Di dalam dunia bisnis juga mengalami perkembangan teknologi terutama pada teknologi informasi yang cukup pesat. Oleh karena itu, suatu perusahaan dituntut untuk harus melakukan pengembangan teknologi agar dapat bersaing dengan perusahaan lainnya. Bagi perusahaan, penerapan teknologi informasi dapat menimbulkan dampak dari penerapan teknologi informasi seperti meningkatnya alur informasi dan ketersediaan informasi bagi setiap stakeholder sehingga penerapan teknologi informasi dapat berjalan sesuai dengan tujuan perusahaan. Penerapan teknologi informasi dapat mendukung kesuksesan perusahaan karena mampu menciptakan peningkatan kompetitif dengan perusahaan lain. Selain itu, penerapan TI yang dikelola sesuai dengan *IT Governance* akan menunjang transformasi layanan dan proses kerja ke arah yang lebih baik guna mencapai kinerja perusahaan yang tinggi sehingga mampu meningkatkan aset perusahaan.

PT. XYZ merupakan perseroan terbatas (PT) yang bergerak dibidang distributor pelumas oli dan rem. PT. XYZ Depo Purwokerto beralamat di Jl. Kebocoran No. 06 RT 003 RW 004 Kebocoran Kedung Banteng kabupaten Banyumas Jawa Tengah. Berdiri pada 2001, PT. XYZ Depo Purwokerto yang merupakan distributor resmi yang memesan barang langsung dari gudang produksi pelumas oli dan rem yang berada di Tangerang. Proses bisnis yang ada pada PT. XYZ Depo Purwokerto yaitu kepala Depo Purwokerto memesan barang secara langsung ke gudang produksi, kemudian jika pesanan sudah tersedia maka admin gudang akan mengecek barang yang datang sesuai atau tidak dengan pesanan dan memeriksa surat jalan. PT. XYZ Depo Purwokerto melakukan mengiriman produk ke daerah Banyumas, Cilacap dan sekitarnya yang bertugas melakukan penawaran produk. Jika adanya pesanan maka admin piutang akan memasukkan data pesanan ke dalam sistem dan mencetak faktur, apabila sudah mencetak faktur, maka barang pesanan baru bisa dikirim ke pelanggan.

Sistem yang ada pada PT. XYZ adalah *Citrix Access Platform System* (CAP), terdapat seorang admin piutang yang bertugas dalam mengoperasikan sistem. Admin piutang bertugas memasukkan semua data ke dalam sistem seperti memasukkan orderan dari marketing, memasukkan data pemasukan kas, serta memasukkan referensi faktur pajak, yang berarti setiap pelanggan yang membeli produk dan memiliki NPWP maka secara otomatis diharuskan untuk membayar pajak. Pada PT. XYZ Depo Purwokerto terdapat admin kasir yang bertugas melakukan pembukuan dan masih dilakukan secara manual, yaitu menulis kas harian dan menerima setoran berupa *sales order* dari marketing. Berdasarkan hasil wawancara dengan kepala depo dan supervisor, permasalahan yang ada yaitu adanya komplain dari pelanggan mengenai keterlambatan pengiriman yang disebabkan oleh sistem yang *error* ataupun mati. Sistem yang ada pada PT. XYZ Depo Purwokerto tidak dapat mencetak surat faktur apabila sistem tidak terkoneksi, padahal salah satu syarat pengiriman produk harus menyertakan surat faktur. Dari permasalahan tersebut, terdapat ketidakselarasan antara proses bisnis dengan visi misi perusahaan, yang mana di dalam visi misi perusahaan ingin memberikan kepuasan kepada pelanggan. Oleh sebab itu diperlukan adanya evaluasi untuk menyelaraskan proses bisnis yang ada agar dapat selaras dengan tujuan perusahaan.

METODE PENELITIAN

1. **Wawancara**

   Suatu cara mendapatkan informasi penelitian dengan bertanya kepada narasumber dengan terlebih dahulu menyiapkan pedoman wawancara sehingga menjadi terarah (Rahmat, 2009).

2. **Observasi**

   Mengumpulkan data untuk penelitian dengan berusaha mengamati suatu peristiwa atau perilaku guna memahami sesuatu yang berkaitan dengan penelitian serta guna evaluasi terhadap aspek tertentu (Rahmat, 2009).

3. Dokumentasi

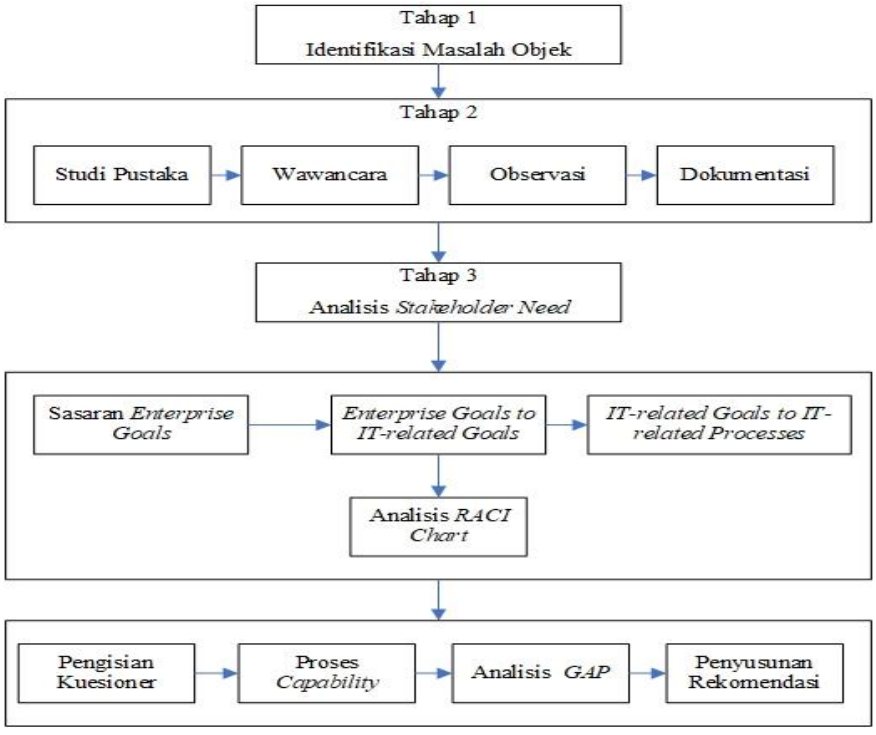
Mendapatkan data penelitian yang relevan dan didapatkan secara langsung dari lokasi penelitian berupa buku, laporan, foto, atau peraturan (Sunyoto, 2013).

4. Kuesioner

Mendapatkan data dengan menyebarkan angket atau kumpulan pernyataan bahkan pertanyaan tertulis kepada responden. Instrumen penelitian ini diperlukan guna melakukan pengukuran terhadap fenomena yang diamati (Sugiyono, 2010).

5. Diagram Penelitian

Penelitian ini menggunakan metode penelitian kuantitatif. Karena bersifat deskriptif, maka dari pengumpulan data, *mapping*, mengolah data, melakukan analisis hingga menyusun rekomendasi untuk mengetahui hasil pengukuran tingkat kapabilitas pada domain-domain yang diperoleh pada COBIT 5. Alur dalam pelaksanaan audit tata kelola teknologi informasi pada PT. XYZ Depo Purwokerto ditunjukan seperti Gambar 1.



Gambar 1. Diagram Penelitian

a. Tahap 1- Identifikasi Masalah Objek

Tahap awal ini dilakukan dengan menentukan identifikasi masalah objek pada PT. XYZ Depo Purwokerto. Identifikasi tersebut terpusat pada bagian sistem informasi yang mana masih belum selaras dengan visi misi perusahaan. Setelah identifikasi masalah objek diperoleh, dilakukan pengumpulan data untuk mengetahui lebih detail kondisi dan permasalahan yang terjadi saat ini pada PT. XYZ Depo Purwokerto.

b. Tahap 2- Pengumpulan Data

Pengumpulan data dilakukan melalui studi pustaka, wawancara, observasi dan dokumentasi. Studi pustaka dilakukan untuk mendapatkan referensi teori yang relevan terhadap permasalahan yang ada pada bidang teknologi informasi. Penelitian ini bertujuan untuk mengukur tingkat kapabilitas proses TI sehingga teori yang relevan dengan penelitian ini adalah panduan kerja *COBIT* 5. Wawancara dilakukan kepada Bapak Arief selaku kepala depo, Bapak Muchlicin selaku *supervisor*, Bu Rina Milasandi selaku bagian admin piutang, Bu Siska Purniasih selaku admin kasir dan Bapak Puji selaku admin gudang pada PT. XYZ Depo Purwokerto . Observasi dilakukan pengamatan langsung terhadap sistem *Citrix Access Platform System* (CAP) dan kondisi tata kelola perusahaan saat ini. Selain itu, dipelajari juga dokumen terkait PT. XYZ Depo Purwokerto dan penelitian-penelitian sebelumnya yang diperlukan sebagai referensi dalam penelitian ini.

c. Tahap 3- Analisis *Stakeholder Need*

Tahap analisis *stakeholder need* merupakan tahap untuk mengetahui kebutuhan-kebutuhan *stakeholder* sebuah organisasi atau perusahaan. Tahap ini dilakukan dengan menganalisis kebutuhan apa saja yang diperlukan oleh *stakeholder* di PT. XYZ Depo Purwokerto. *Stakeholder need* diketahui dari hasil tahap pengumpulan data yang sebelumnya sudah diperoleh dan selanjutnya *stakeholder need* tersebut digunakan untuk

mencari sasaran *Enterprise Goals* mulai dari *financial, customer, internal* dan *learning and growth*.

d. Tahap 4- *Scenario Mapping*

Persiapan untuk proses mengambil data menjadi bahan inputan tahap selanjutnya (tahap pengambilan dan penilaian data). Perencanaan penilaian dengan melakukan pemetaan atau *mapping Enterprise Goals* sesuai dengan visi, tujuan dan misi PT. XYZ Depo Purwokerto. Proses selanjutnya melakukan pemetaan *IT-related Goals.* Setelah *IT-related Goals* berlanjut melakukan *mapping to IT-related Processes*. Hasil yang didapatkan dalam pemetaan sebagai dasar penyusunan kuesioner audit (*form assessment).* Setelah *IT-related Goals to IT-related Processes* terpilih maka proses selanjutnya adalah analisis *RACI Chart*.

Analisis *RACI Chart* digunakan untuk membantu organisasi atau perusahaan dalam pengambilan keputusan. Menganalisis *RACI Chart* dapat dilihat dari struktur organisasi untuk menemukan siapa saja yang bertanggung jawab. Hasil dari *RACI Chart* tersebut kemudian digunakan untuk penyusunan kuesioner berdasarkan proses *COBIT* 5 yang didapat yaitu domain EDM, APO, DSS, dan MEA (diagram *RACI Chart* terlampir). Penyusunan kuesioner ini mengacu pada *form assessment* dalam *COBIT* 5.

e. Tahap 5- Pengolahan Data dan Laporan Penilaian

Tahap ini dilakukan dengan cara membagi kepada 4 responden terpilih dengan pertanyaan berdasarkan tiap-tiap domain yang telah terpilih. Kuesioner diberikan kepada bagian sumber daya manusia, bagian *IT* dan direktur. Hasil kuesioner yang telah didapat kemudian dilakukan proses *capability level* sebagai berikut:

$$Capability\ Level = \frac{(0*y_0) + (1*y_1) + \ldots + (5*y_5)}{z}$$

Keterangan:

$y_n(y_0 \ldots y_5)$ = jumlah proses yang berada dilevel n

z = jumlah proses yang dievaluasi

Langkah selanjutnya adalah menghitung GAP dengan cara membandingkan nilai *capability level* yang didapatkan terhadap level target yang telah ditentukan serta dilakukan pada setiap domain terpilih. Berdasarkan analisis GAP dapat disusun rekomendasi

HASIL DAN PEMBAHASAN

Proses bisnis yang berjalan pada PT. XYZ Depo Purwokerto yaitu kepala Depo Purwokerto memesan produk langsung ke pusat, produk yang tiba di Depo Purwokerto kemudian dicek oleh admin gudang berserta surat jalannya. Pendistribusian produk di area Banyumas, Cilacap, dan sekitarnya. *Staff* marketing bertugas datang langsung menawarkan produk-produk ke toko ataupun bengkel dengan membawa nota pemesanan. Nota pemesanan tersebut yang nantinya akan diberikan ke admin kasir yang selanjutnya akan dikroscek dan dimasukkan ke dalam sistem oleh admin piutang. Sistem yang ada pada PT. XYZ Depo Purwokerto bernama *Citrix Access Platform* (CAP).

1. Sasaran *Enterprise Goals*

Langkah awal yang dilakukan pada tahap ini adalah mengidentifikasikan COBIT *Enterprise Goals* kemudian memilih sesuai dengan visi PT. XYZ Depo Purwokerto, lalu menghasilkan pemetaan yang sesuai dengan ruang lingkup masalah di perusahaan.

Tabel 1. Hasil *Enterprise Goals*

Visi	Masalah	*Enterprise Goals*
Menjadi distributor pelumas dan rem yang handal, yang memberikan kepuasan baik dari segi harga, kualitas, serta ketepatan waktu dalam pengiriman.	Apabila sistem yang ada pada PT. XYZ Depo Purwokerto mati ataupun *error*, maka pengiriman barang tidak dapat dilakukan. Prosedur pengiriman barang harus disertai dengan surat faktur, yang mana jika sistem tersebut tidak dapat digunakan otomatis surat faktur juga tidak bisa dicetak, yang berdampak pada proses pengiriman produk.	*Optimisation of business process functionality*

2. *Mapping Enterprise Goal To It-Related Goals*

Jika pemetaan *Enterprise Goals* telah didapatkan maka melakukan identifikasi *IT-related Goals* dan menggabungkan hasilnya. Langkah tersebut dapat dilihat pada *Mapping Enterprise Goal to IT-related Goals* sebagai berikut .

Tabel 2. Hasil *Mapping Enterprise Goal*

No	*Enterprise Goals*	*Mapping Enterprise Goals to IT-related Goals*
1	*Optimisation of businessprocess functionality*	a. *Alignment of IT and business strategy (P) Primer Key*
		b. *Delivery of IT services in line with business requirements (P) Primer Key*
		c. *Adequate use of applications, information and technology solutions (P) Primer Key*
		d. *IT agility (P) Primer Key*
		e. *Enablement and support of business processes by integrating applications and tecnology into business processes (P) Primer Key*

3. *Mapping It-Related Goals To It-Related Processes*

Mapping IT-related Goals to Processes adalah proses memetakan *IT-related Goals* ke dalam proses COBIT 5.

Tabel 3. *Mapping IT-related Goals to IT-related Processes*

No	*IT-related Goals*	*Mapping IT-related Goals to Processes*
1	*Alignment of IT and business strategy*	EDM02
2	*Delivery of IT services in line with business requirements*	EDM02, APO09, DSS01,
3	*Adequate use of applications,*	MEA01
4	*Information and technology solutions*	APO04
5	*IT agility*	APO04

4. Pengolahan Data Dan Perhitungan *Capability Level*

4.1 Proses EDM02 *Ensure Benefit Delivery*

Hasil pada EDM02 (*Ensure Benefits Delivery*) mencapai level 3. Level 3 termasuk dalam kategori *Established Process* yang berarti di dalam perusahaan

sudah terdapat proses TI yang dibakukan dan diterapkan diseluruh lingkup organisasi. Dengan temuan masalah belum optimalnya manfaat dari TI bagi perusahaan, karena masih adanya kendala dari perusahaan yaitu tidak dapat mengirimkan barang apabila sistem *error* karena tidak adanya surat faktur dan belum pernah dilakukan evaluasi mengenai manfaat TI apakah benar dirasakan apa tidak.

4.2 Proses APO04 *Manage Innovation*

Penilaian APO04 *(Manage Innovation)* pada level 2 *Managed Process*. Proses TI telah dijalankan dengan baik guna mendukung tercapainya tujuan perusahaan. Fokus proses TI yang diperhatikan dari proses perencanaan sampai evaluasi agar berkembang ke arah yang lebih baik. Dengan temuan masalah belum adanya niatan perusahaan untuk mengganti sistem yang ada, padahal teknologi berkembang pesat dan seharusnya perusahaan mengikuti perkembangan karena perkembangan teknologi sekarang berjalan sangat pesat.

4.3 Proses APO09 *Manage Service Agreement*

Penilaian APO09 *(Manage Service Agreement)* mencapai level 4 *Predictable Process*. Level ini menandakan perusahaan menjalankan proses TI sesuai dengan batasan yang sudah ditentukan. Penentuan batasan berdasarkan pengukuran pada pelaksanaan proses TI sebelumnya. Dengan temuan masalah belum adanya perjanjian tertulis yang dibuat perusahaan dengan konsumen pada saat produk terlambat dikirim karena tidak tercetaknya surat faktur dan belum pernah dilakukan koordinasi untuk review apakah layanan yang ada pada perusahaan saat ini sudah baik atau belum.

4.4 Proses DSS01 *Manage Operations*

DSS01 (*Manage Operations*) mencapai pada level 4 *Predictable Process*. Proses TI yang dijalankan oleh perusahaan sesuai dengan batasan yang telah ditetapkan sesuai hasil perhitungan pada proses TI sebelumnya. Dengan temuan masalah tidak ada yang menggantikan peran apabila ada salah satu staff berhalangan hadir dan masih adanya penggunaan laptop pribadi dikarenakan penggunaan komputer perusahaan kurang efektif.

4.5 Proses MEA01 *Monitor, Evaluate, and Assess Performance and Confornance*

Penilaian MEA01 (*Manage Organizational Change Enablement*) mencapai pada level 4 *Predictable Process*. Penerapan dan proses menjalankan TI sudah memiliki batasan yang disesuaikan dengan pengukuran pelaksanaan TI yang lalu. Dengan temuan masalah belum pernah adanya monitoring mengenai manajemen kinerja perusahaan saat ini untuk kontribusi tujuan perusahaan.

5. ANALISIS GAP

Kondisi teknologi informasi yang ada di PT. XYZ Depo Purwokerto dapat dilihat berdasarkan hasil perhitungan *capability level* dengan 7 proses domain COBIT. Maka perolehan *capability level* yang telah dicapai dan kemudian ditentukan targetnya untuk mengetahui analisis GAP bahwa target level kapabilitas yang diharapkan adalah pada level 3 untuk sub domain APO04, level 4 untuk EDM02, dan level 5 untuk sub domain APO09, DSS01, MEA01. Pada level 3 artinya perusahaan menginginkan adanya pengukuran proses bisnis yang sudah dikelola, didefinisikan dan diimplementasikan secara teratur serta dijalankan untuk pencapaian hasil dari tujuan proses bisnis tersebut. Pada level 4 bagaimana perusahaan menjalankan proses TI dalam batasan yang sudah pasti, serta pada level 5 bagaimana perusahaan dapat melakukan inovasi melakukan perbaikan yang berkelanjutan sehingga proses bisnis dapat berjalan dengan tetap dan stabil untuk kedepannya pada PT. XYZ Depo Purwokerto.

Tabel 4. Hasil Analisis GAP

No	*IT Process*	Keterangan	Level	Target	GAP
1	EDM02	Memastikan Penyampaian Manfaat	3	4	1
2	APO04	Mengelola Mengelola Inovasi	2	3	1
3	APO09	Mengelola Perjanjian Layanan	4	5	1
4	DSS01	Mengelola operasi	4	5	1
5	MEA01	Memantau, mengevaluasi, Menilai kinerja dan penyesuaian	4	5	1

Capability level yang didapatkan pada masing-masing proses akan dicari rata-rata *capability level* untuk PT. XYZ Depo Purwokerto sebagai berikut:

$$Capability\ Level = \frac{(0 * y_0) + (1 * y_1) + \cdots + (5 * y_5)}{z} \quad (1)$$

Keterangan:

$y_n (y_{0\ldots}\ y_{5})$ = seluruh proses yang berada dilevel n

z = jumlah proses yang dievaluasi

$$Capability\ Level = \frac{(0 * 0) + (1 * 0) + (2 * 1) + (3 * 1) + (4 * 3)}{5} \quad (2)$$

$$Capability\ Level = \frac{(0) + (0) + (2) + (3) + (12)}{5}$$

$$\text{Capability Level} = \frac{17}{5}$$

$$\text{Capability Level} = 3{,}4$$

Capability level yang dihasilkan pada PT. XYZ Depo Purwokerto sebesar 3,4, yang artinya berada dalam level 3 yaitu *(Established Process).*

KESIMPULAN DAN SARAN

Hasil penelitian PT. XYZ Depo Purwokerto menggunakan COBIT 5 menghasilkan 5 proses sub domain yang teridentifikasi berada pada level 3 (*Established Process*) yaitu pada sub domain penyampaian manfaat (EDM02),

pengelolaan inovasi (APO04), pengelolaan perjanjian layanan (APO09), pengelolaan operasi (DSS01) dan mengevaluasi kinerja (MEA01).

Hasil perhitungan tingkat kapabilitas tata kelola teknologi informasi pada *capability level* di PT. XYZ Depo Purwokerto keseluruhan yang diperoleh berdasarkan rata-rata adalah 3,4. Proses TI telah dijalankan oleh perusahaan untuk mencapai tujuan bisnis dengan memperhatikan perencanaan dan penyesuaian untuk meningkatkan kinerja perusahaan. Penyesuaian yang dilakukan oleh perusahaan sudah dalam jangka panjang, yang mana perusahaan memikirkan bagaimana mencapai tujuan bisnisnya dengan lebih terkelola dengan baik. Rekomendasi yang dihasilkan disesuaikan dengan temuan-temuan yang ada dilapangan dan diselaraskan dengan hasil kuesioner yang diisi oleh karyawan PT. XYZ Depo Purwokerto. Rekomendasi-rekomendasi yang ada diantaranya yaitu:

1. Perusahaan membuat perjanjian secara tertulis dengan pelanggan mengenai kebijakan dalam prosedur keterlambatan dalam pengiriman barang.
2. Melakukan penerimaan karyawan baru yang sesuai dan memiliki kompetensi dan keahlian sehingga apabila ada karyawan yang tidak hadir, maka ada yang dapat menggantikan peran tersebut.
3. Dibuatnya sebuah prosedur pengawasan (SOP) yang nantinya dilakukan oleh staff ahli terhadap pengelolaan TI di perusahaan untuk melakukan pemantauan dari kinerja TI itu sendiri sehingga kinerja proses bisnis di PT. XYZ Depo Purwokerto dapat terpantau dengan baik.
4. Dibuatnya manajemen strategi untuk layanan TI supaya kinerja TI dalam perusahaan dapat dirasakan bagi perusahaan itu sendiri.

DAFTAR PUSTAKA

Adi, Nelvia. (2018). "Pelaksanaan Evaluasi Hasil Belajar Mahasiswa." *Jurnal Pendidikan dan Kebudayaan* 16(9): 321.

Adikara, Fransiskus. (2013). "Implementasi Tata Kelola Teknologi Informasi Perguruan Tinggi Berdasarkan Cobit 5 Pada Laboratorium Rekayasa Perangkat Lunak Universitas Esa Unggul." *Seminar Nasional Sistem Informasi Indonesia*: 2–4.

Adikara, Fransiskus & Pambudi, Ari. (2012). "Mengembangkan Model Tata Kelola Teknologi Informasi Dengan Kerangka Kerja Cobit 5 Pada Perguruan Tinggi Dengan Studi Kasus Di Universitas Esa Unggul." : 175–82.

Kurnianingtyas, Lorentya Yulianti, and Mahendra Adhi Nugroho. (2012). "Implementasi Strategi Pembelajaran Kooperatif Teknik Jigsaw Untuk Meningkatkan Keaktifan Belajar Akuntansi Pada Siswa Kelas X Akuntansi 3 Smk Negeri 7 Yogyakarta." *Jurnal Pendidikan Akuntansi Indonesia Lorentya Yulianti Kurnianingtyas & Mahendra Adhi Nugroho Halaman* X(1): 66–77.

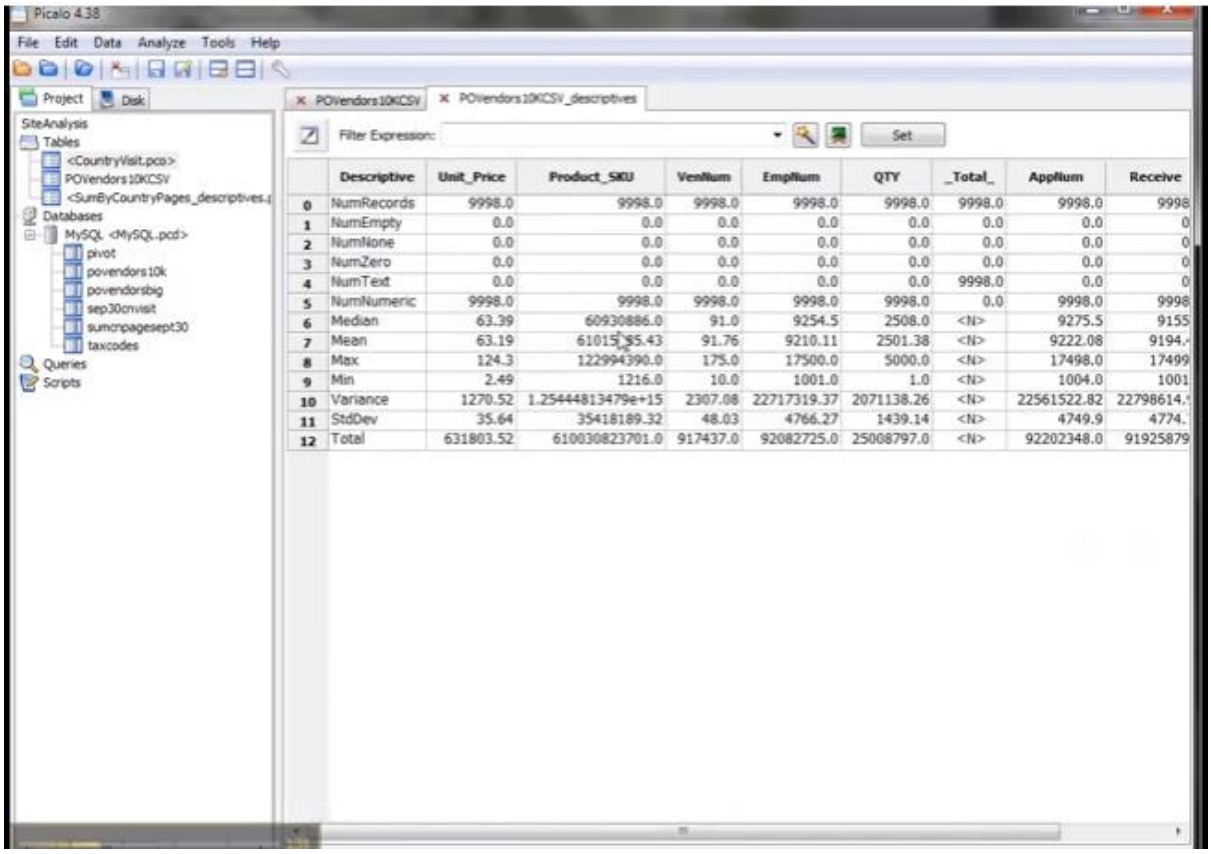
Mufti, Raja Gantino, and Yusi Tyroni Mursityo. (2017). "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses APO13 Dan DSS05 (Studi Pada PT Martina Berto Tbk)." *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* 1(12): 1622–31.

Rahmat, Saeful Pupu. (2009). "Penelitian Kualitatif." *Penelitian Kualitatif* 5 No. 9: 1–8.

Sunyoto, (2013). "Jenis Data," pp. 43–51, 2013.

Sugiyono. (2010). *Metode Penelitian Pendidikan Pendekatan Kuantitatif, kualitatif, dan R&D.* Bandung: Alfabeta

PICALO



	Descriptive	Unit_Price	Product_SKU	VenNum	EmpNum	QTY	_Total_	AppNum	Receive
0	NumRecords	9998.0	9998.0	9998.0	9998.0	9998.0	9998.0	9998.0	9998
1	NumEmpty	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0
2	NumNone	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0
3	NumZero	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0
4	NumText	0.0	0.0	0.0	0.0	0.0	9998.0	0.0	0
5	NumNumeric	9998.0	9998.0	9998.0	9998.0	9998.0	0.0	9998.0	9998
6	Median	63.39	60930886.0	91.0	9254.5	2508.0	<N>	9275.5	9155
7	Mean	63.19	61015155.43	91.76	9210.11	2501.38	<N>	9222.08	9194.
8	Max	124.3	122994390.0	175.0	17500.0	5000.0	<N>	17498.0	17499
9	Min	2.49	1216.0	10.0	1001.0	1.0	<N>	1004.0	1001
10	Variance	1270.52	1.25444813479e+15	2307.08	22717319.37	2071138.26	<N>	22561522.82	22798614.
11	StdDev	35.64	35418189.32	48.03	4766.27	1439.14	<N>	4749.9	4774.
12	Total	631803.52	610030823701.0	917437.0	92082725.0	25008797.0	<N>	92202348.0	91925879

Picalo adalah sebuah aplikasi data analisis yang cocok untuk auditor, pemeriksa fraud, data miner, dan data analisis lainnya. Fokus aplikasi Picalo pada pendeteksian terhadap fraud, korupsi dan untuk mendapatkan data dari database perusahaan. Picalo juga merupakan dasar untuk sebuah sistem otomasi pendeteksi fraud.

Picalo bekerja dengan menggunakan GUI Front end, dan memiliki banyak fitur untuk ETL sebagai proses utama dalam mengekstrak dan membuka data, kelebihan utamanya adalah fleksibilitas dan front end yang baik hingga Library Python numerik.

Picalo dapat dijalankan di system operasi linux, mac atau windows. Dalam IT audit picalo dapat digunakan untuk Analisa jaringan, Analisa log web server dan data login system serta import email kedalam database relational dalam picalo.

PICALO

1. Dedi Setiadi
2. Febriansyah
3. Fido Rizki
4. Tri Susanti
5. David Agustian

PICALO

- Picalo adalah sebuah aplikasi data analisis yang cocok untuk auditor, pemeriksa fraud, data miner, dan data analisis lainnya. Fokus aplikasi Picalo pada pendeteksian terhadap fraud, korupsi dan untuk mendapatkan data dari database perusahaan. Picalo juga merupakan dasar untuk sebuah sistem otomasi pendeteksi fraud.

FUNGSI DARI APLIKASI :

- Untuk menganalisa data finansial, data pegawai dan sistem purchasing dari adanya error dan fraud.
- Untuk mengimport file Excel, XML, EBCDIC, CSV dan TSV kedalam database.
- Secara interaktif menganalisa kejadian-kejadian dalam jaringan, log web server, dan data login suatu sistem.
- Mengimport email kedalam database relational atau text-based.
- Embedding control dan testing fraud secara rutin pada mesin produksi.

CONTOH PENGGUNAAN PICALO

Untuk menganalisa data finansial, data pegawai dan sistem purchasing dari adanya error dan fraoud

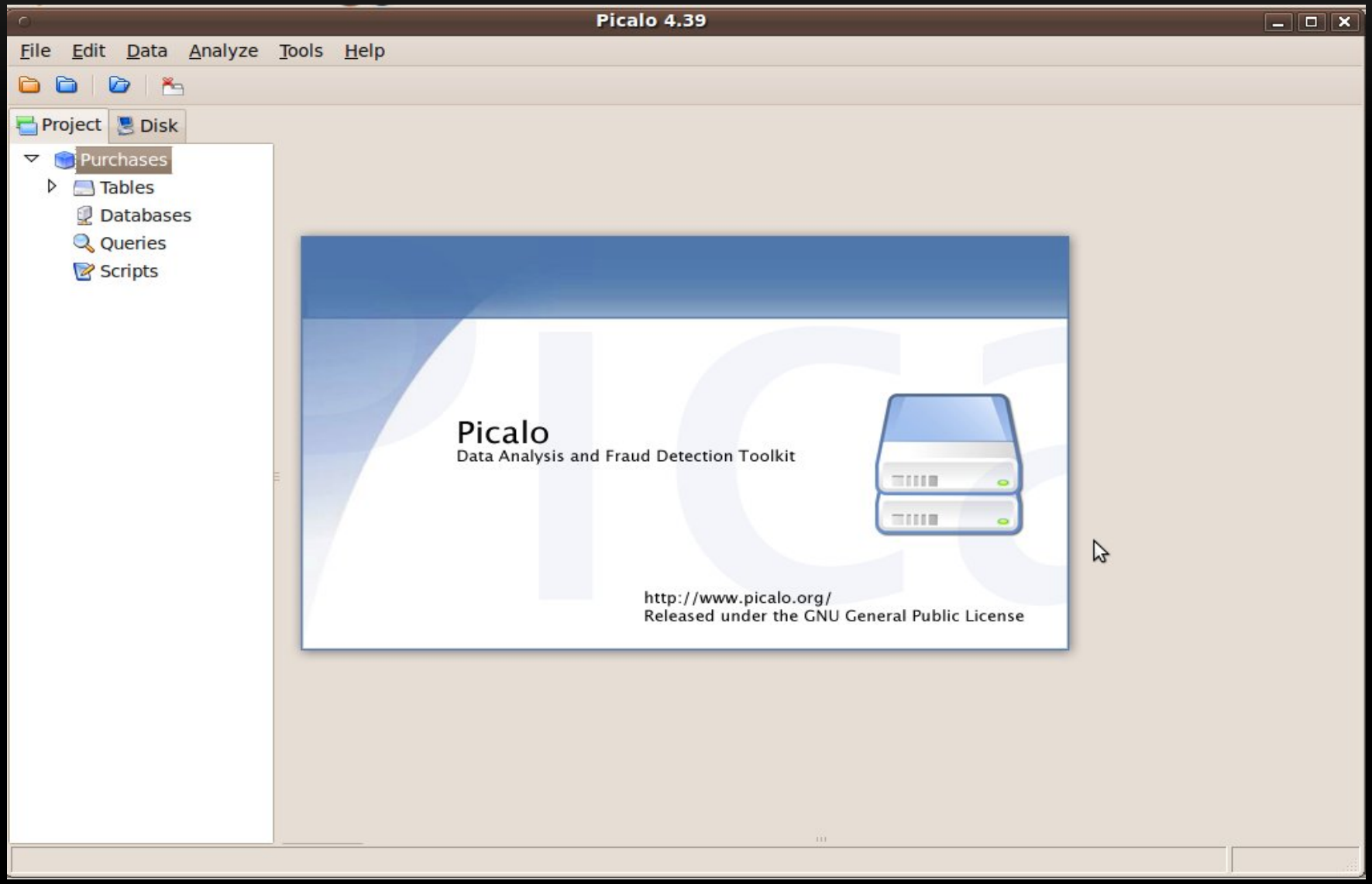
Untuk mengimport file Excel Excel, XML, EBCDIC, CSV dan TSV kedalam database

JENIS DOKUMEN YANG DAPAT DIGUNAKAN

Jenis dokumen yang dapat dianalisi pada picalo adalah sebagai berikut :

- CSV/TSV files,
- EBCDIC files,
- MS Excel files,
- log files,
- text files,

CONTOH


Picalo 4.39
File Edit Data Analyze Tools Help
Project Disk
Purchases
Tables
Databases
Queries
Scripts
Picalo
Data Analysis and Fraud Detection Toolkit
http://www.picalo.org/
Released under the GNU General Public License

KESIMPULAN

Picalo adalah sebuah aplikasi yang dapat digunakan untuk memeriksa fraud, data miner, dan data analisis lainnya.

REFERENCE :

https://aisyahoctav.weebly.com/softskill/review-software-audit-teknologi-informasi

https://www.slideshare.net/triyulianto182/picalo-tool-audit

https://pypi.org/project/picalo/

SEO AUDIT TOOL

semrush


search...
WHAT IS
SEO?
Lorem ipsum

Why SEO is

IMPORTANT

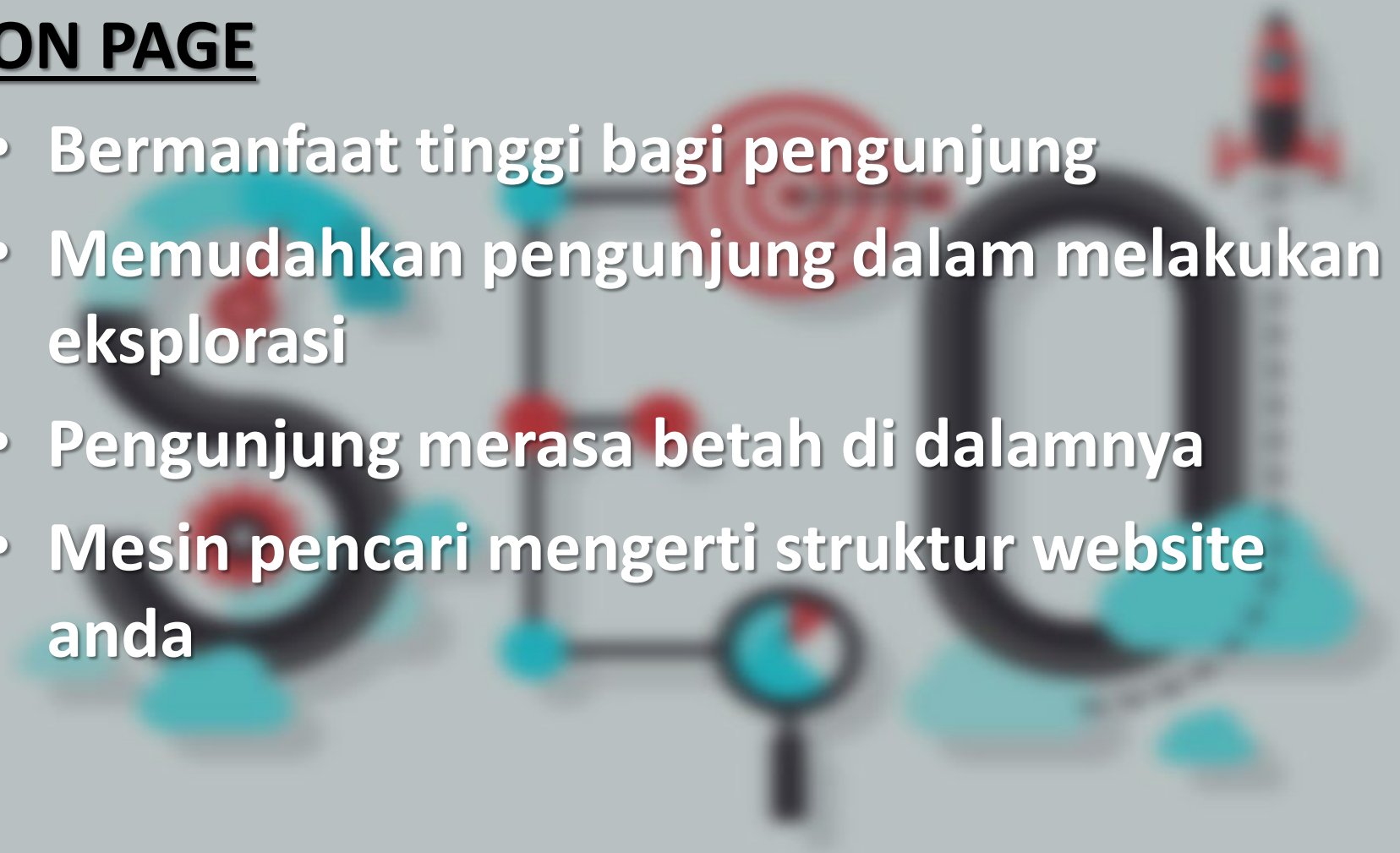
for website ???

BASIC CONCEPT OF SEO

- Content
- Navigation And Structure
- User Experience
- Popularity

ON PAGE AND OFF PAGE

ON PAGE – OFF PAGE



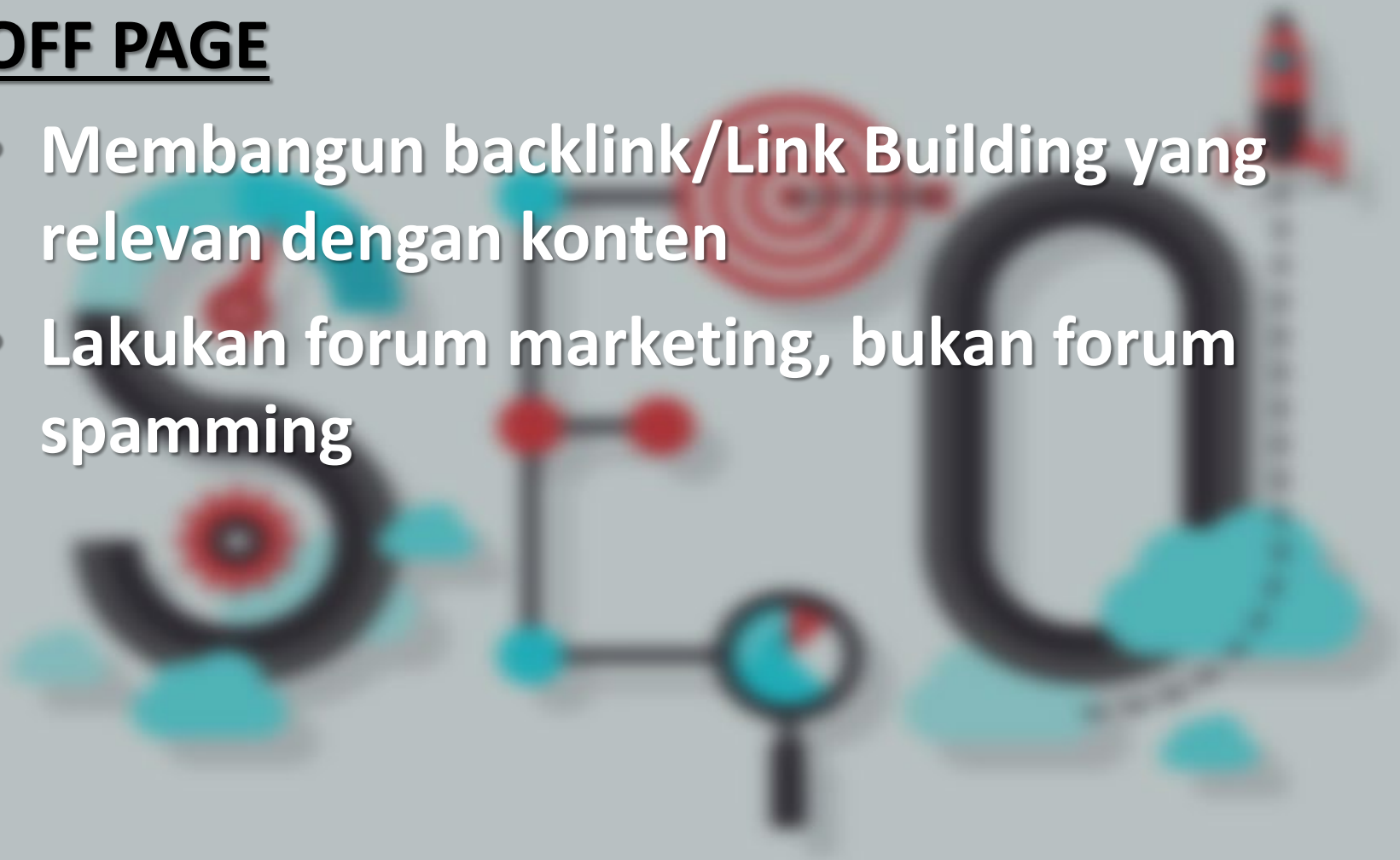
ON PAGE

- Bermanfaat tinggi bagi pengunjung
- Memudahkan pengunjung dalam melakukan eksplorasi
- Pengunjung merasa betah di dalamnya
- Mesin pencari mengerti struktur website anda

ON PAGE – OFF PAGE

OFF PAGE

- Membangun backlink/Link Building yang relevan dengan konten
- Lakukan forum marketing, bukan forum spamming




semrush

All-Inclusive Suite for Your Marketing Workflow

SEO

Advertising

Social Media

Content

Competitive Research

Reporting & Management

SEO

- Organic Research
- Organic Traffic Insights
- Keyword Research
- Backlink Building and Analytics
- Rank Tracking
- Site Audit
- On Page SEO Checker
- Search Engine Sensor

Advertising

- Advertising Research
- PPC Keyword Tool
- Display Advertising
- Ad Builder
- Product Listing Ads

Social Media

- Social Media Poster
- Social Media Tracker

Content

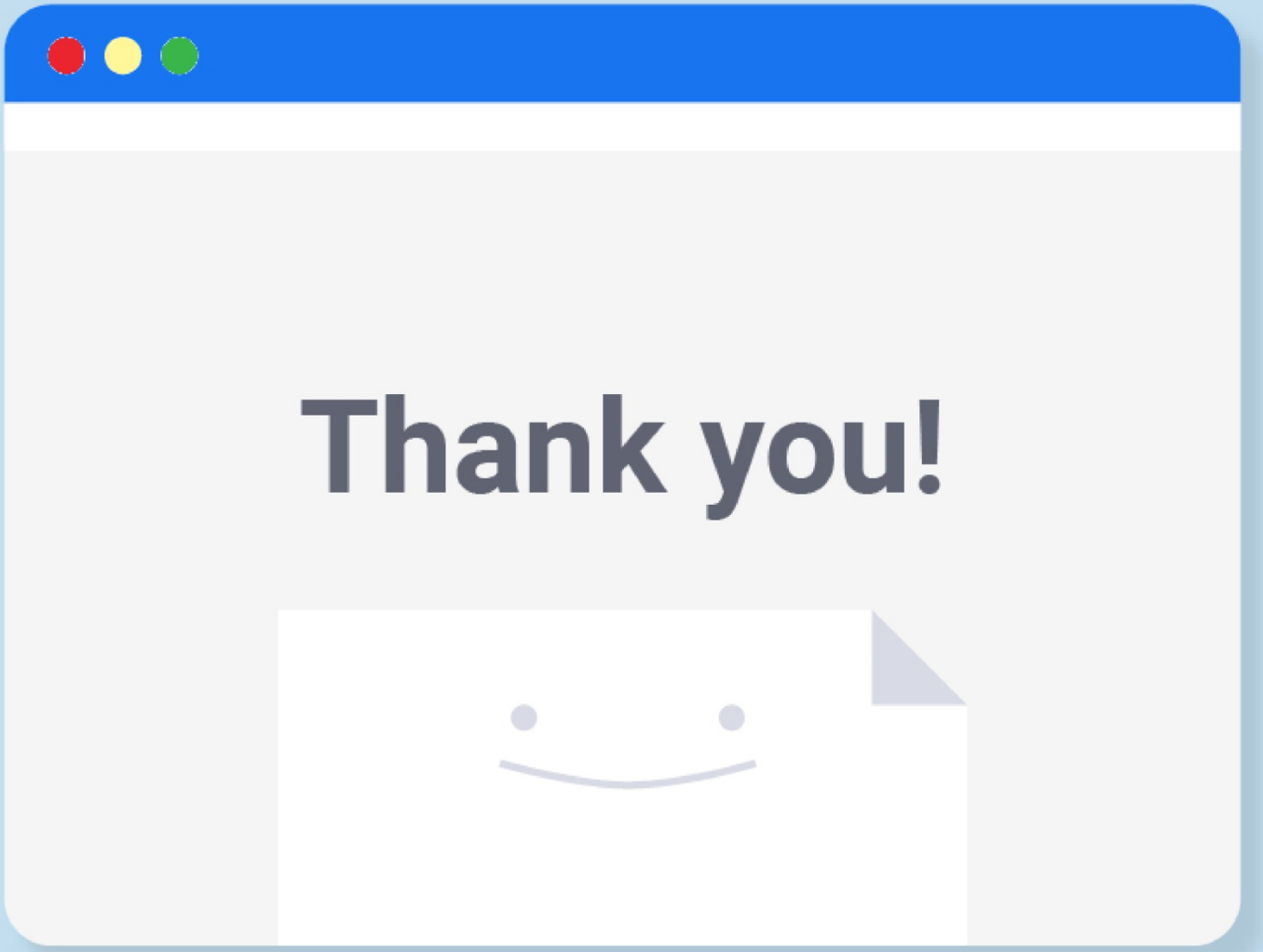
- Content Audit
- Topic Research
- SEO Content Template
- Post Tracking
- Keyword Research
- Related Keywords
- Brand Monitoring

Competitive Research

- Domain Overview
- Charts
- Keyword and Backlink gap Analysis
- Ranks
- Traffic Analytics

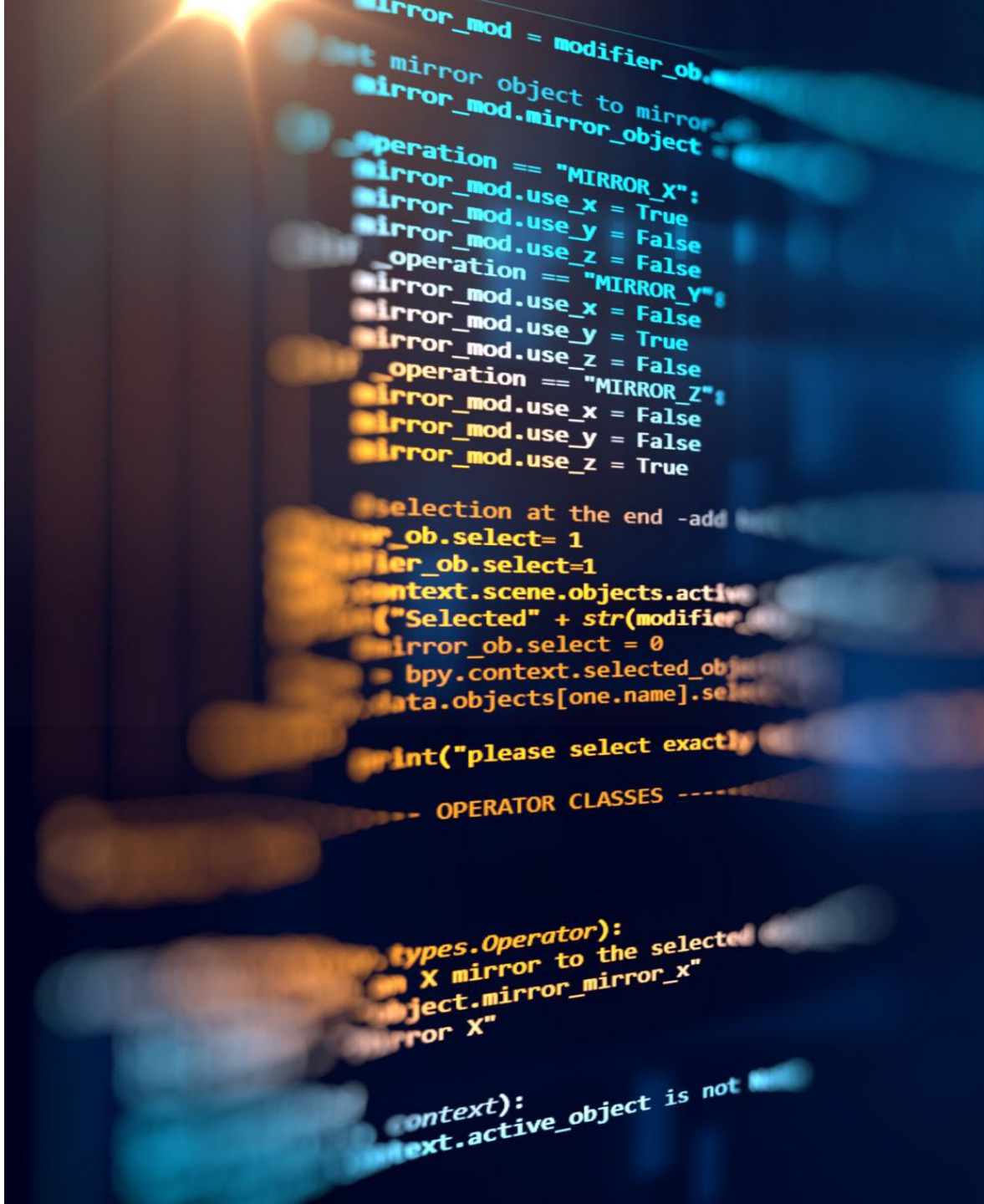
Reporting & Management

- Marketing Calendar
- My Reports
- Lead Generation Tool


Thank you!

SOFTWARE IT AUDIT

Manage Engine AD Audit Plus



SALAH SATU RESIKO YANG MUNCUL DI BIDANG IT

Data Breach

merupakan salah satu jenis serangan cyber yang dapat mengancam organisasi. Data breach atau pelanggaran data merupakan suatu kondisi di mana hacker mampu menyusup masuk ke dalam sistem dan mengekstraksi data-data penting di dalamnya.

Hal ini mampu membawa berbagai dampak negatif untuk bisnis, mulai dari tercurinya data-data sensitif sampai hilangnya kepercayaan pelanggan.

APA SAJA YANG DAPAT MENYEBABKAN DATA BREACH DAPAT TERJADI.

1. **Kredensial yang lemah**

Kredensial atau kata sandi yang lemah menjadi salah satu penyebab data breach dapat terjadi. Kata sandi dibuat dengan tujuan untuk mengamankan sistem. Namun sayangnya masih banyak yang menggunakan kata sandi dengan frasa sederhana seperti Password1 atau 123456. Jika hacker dapat menemukan kata sandi yang Anda gunakan, mereka dapat dengan mudah masuk ke dalam sistem dan mengakses data-data sensitif di dalamnya. Oleh karena itu, penting bagi perusahaan untuk selalu menggunakan kata sandi yang kuat dan secara regular memperbaruinya.

2. **Adanya kerentanan di dalam aplikasi**

Sebagian besar hacker akan melakukan sejumlah serangan ketika mereka menemukan kerentanan dalam sebuah sistem. Itulah sebabnya, penting bagi perusahaan untuk melakukan penetration testing secara rutin. Penetration testing dapat membantu perusahaan untuk menemukan celah keamanan agar bisa segera ditambal atau diperbaiki.

3. Malware

Malware (malicious software) merupakan suatu program atau file berbahaya yang dibuat dengan tujuan jahat. Peretas dapat menyebarluaskan malware ketika sistem memiliki kerentanan keamanan. Mereka juga dapat menanamkan malware ketika karyawan Anda secara tidak sadar mengklik tautan berbahaya yang dikirim melalui email. Berbagai serangan malware ini biasanya digunakan oleh peretas untuk menghilangkan langkah otentikasi yang digunakan untuk melindungi sistem.

4. **Orang dalam yang berbahaya**

Selain karena faktor kesalahan teknis, data breach juga dapat terjadi karena faktor kesengajaan. Beberapa karyawan Anda mungkin memiliki akses untuk melihat data sensitif perusahaan. Terkadang karena iming-iming imbalan berupa uang, karyawan dapat menyalahgunakannya dan memberikan akses tersebut kepada peretas. Jika peretas berhasil membujuk karyawan Anda, mereka dapat mengakses data dengan mudah tanpa harus mengekploitasi sistem untuk menemukan celah keamanan.

Sumber Infografis : https://hostingtribunal.com/blog/biggest-data-breach-statistics/

SOFTWARE IT AUDIT

Penggunaan software IT audit untuk melakukan pemantauan dan pengujian terhadap aktivitas yang dilakukan user terhadap devices di organisasi

Melakukan pengujian untuk mengetahui apakah sistem yang digunakan memiliki celah keamanan yang dapat diretas oleh pihak yang tidak bertanggung jawab

Mengontrol setiap perubahan yang terjadi pada sistem.

ManageEngine
ADAudit Plus

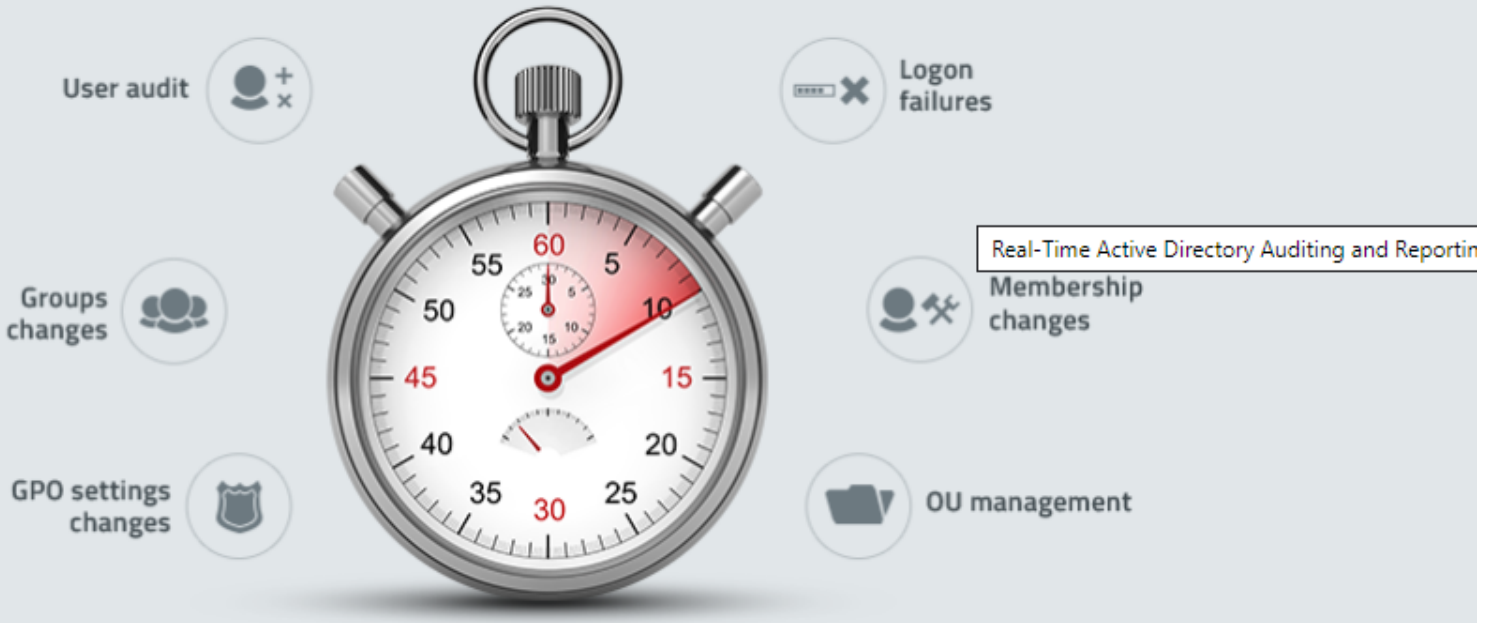
Products Store Partners Support |

Overview Features Demo Resources Get Quote Support Download

Real-Time Auditing for Active Directory

with 200+ audit reports & e-mail alerts

Download



ACTIVE DIRECTORY AUDITING

LOGON/LOGOFF AUDITING

FILE SERVER AUDITING

WINDOWS SERVERS AUDITING

REAL-TIME WINDOWS ACTIVE DIRECTORY AUDITING

In real-time, ensure critical resources in the network like the Domain Controllers are audited, monitored and reported with the entire information on AD objects - Users, Groups, GPO, Computer, OU, DNS, AD Schema and Configuration changes with 200+ detailed event specific GUI reports and email alerts.

Insider Threats

User Logon

Compliance

Reports & Alerts

Data Archiving

GPO Settings

WINDOWS LOGON/LOGOFF AUDITING

Audit the critical user workstation logon & logoff time to monitor the logon duration, logon failures, logon history and terminal services activity. View & Schedule graphical reports with Email alerts for periodic analysis & quick response during security threats.

Logon / Logoff

Compliance

Data Archiving

Reports & Alerts

All Workstation Reports

WINDOWS FILE SERVER AUDITING

Securely track the file creation, modification & deletion from an authorized / unauthorized access, with detailed forensics of security and permission changes to the documents in their files / folder structure and shares.

File Servers

Access Permissions

Failover Clusters

NetApp Filers

EMC Servers

All File Server Reports

WINDOWS SERVERS AUDITING

Track the Logon/Logoff, Schedule to track events like RADIUS Logon, Terminal Services Activity, Logon Duration and Logon History. Audit related processes can be kept tab by Tracking Windows Schedule jobs.

Windows Servers

Printer Auditing

File integrity Monitoring

Compliance

Reports & Alerts

All Windows Servers Reports

EX: HTTPS://WWW.YOUTUBE.COM/WATCH?V=X6SJRLSDQQU

NESSUS

IT Audit Tool

Oleh:
Riduan Syahri
Dita Rahmawati
Rumondang Martha A

Pengertian

- Nessus dibuat oleh Renaud Deraison pada tahun 1998 yang berada di bawah perusahaan development Tenable yang berfokus pada Cybersecurity.
- Nessus merupakan software scanning yang dapat digunakan untuk mengaudit keamanan sebuah sistem, seperti vulnerability, misconfiguration, security patch yang belum diaplikasikan, default password, dan denial of service.

Pengertian

- Dikarenakan fungsi dari Nessus dapat digunakan untuk mendeteksi adanya kelemahan dari suatu sistem maka Nessus menjadi salah satu tool andalan ketika melakukan audit keamanan sistem.

Fitur-fitur NESSUS

- Database security Nessus diupdate setiap hari ketika terconnect dengan server Nessus.
- Nessus mampu mendeteksi tidak cuma port yang terbuka di setiap komputer yang terhubung kedalam jaringan, tetapi juga mengecek partch OS nya termasuk didalamnya patch untuk Windows, Unix, Linux, atau MacOS.
- Nessus bisa dibangun dalam skala kecil, satu atau dua komputer dengan sedikit resource prossesor sampai dengan prosessor dengan quad core lebih.

- Setiap security test dibentuk dalam modul plugin dan ditulis dalam NASL, artinya update nessus tidak akan melibatkan binaries yang tidak dipercaya dari internet.
- Setiap NASL plugin dapat dibaca, dimodifikasi agar report Nessus bisa dibaca dengan lebih mudah
- NASL (Nessus Attack Scripting Language) suatu bahasa yang dikembangkan khusus agar security test dapat dijalankan dengan mudah dan cepat

- NASL plugin di dalam suatu container yang bisa berdiri di atas virtual mesin sehingga membuat Nessus menjadi scanner yang benar benar secure
- Nessus memiliki kemampuan untuk mengetest SSL seperti https, smptps, imaps, dll dan dapat pulau diintegrasikan

3 tahap proses pada Nessus

- Scanning

Pada fase ini Nessus akan melakukan pengecekan untuk mengetahui mana host yang hidup (live), dengan cara mengirimkan ICMP Echo. Kemudian selanjutnya bisa host tersebut diketahui live akan deteruskan dengan port scanning

- Enumeration

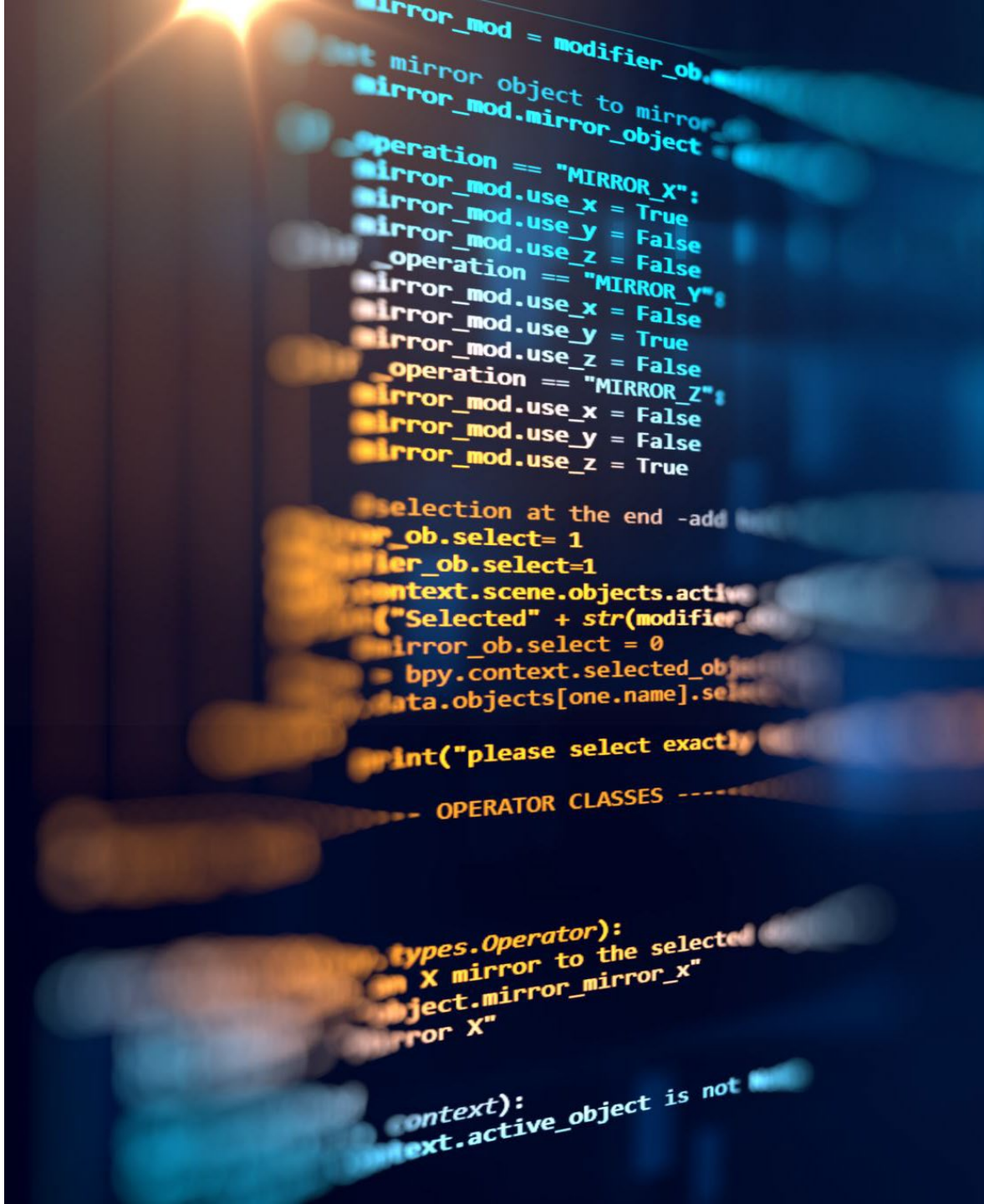
Pada tahap ini Nessus akan melakukan pemeriksaan kepada host yang live dengan mencari banner grabbing yang bisa menunjukkan jenis dan versi OS yang digunakan host. Tergantung dari sistemnya di fase ini dimungkinkan untuk melakukan test penjebolan account dan password dengan metode Brute Force

- Deteksi Vulnerability

Setelah fase 2 selesai, maka Nessus akan melanjutkan dengan mencari vulnerability yang sesuai yang terdapat pada host target misalnya input validasi, buffer overflows, konfigurasi yang tidak tepat

SOFTWARE IT AUDIT

Manage Engine AD Audit Plus



SALAH SATU RESIKO YANG MUNCUL DI BIDANG IT

Data Breach

merupakan salah satu jenis serangan cyber yang dapat mengancam organisasi. Data breach atau pelanggaran data merupakan suatu kondisi di mana hacker mampu menyusup masuk ke dalam sistem dan mengekstraksi data-data penting di dalamnya.

Hal ini mampu membawa berbagai dampak negatif untuk bisnis, mulai dari tercurinya data-data sensitif sampai hilangnya kepercayaan pelanggan.

APA SAJA YANG DAPAT MENYEBABKAN DATA BREACH DAPAT TERJADI.

1. **Kredensial yang lemah**

Kredensial atau kata sandi yang lemah menjadi salah satu penyebab data breach dapat terjadi. Kata sandi dibuat dengan tujuan untuk mengamankan sistem. Namun sayangnya masih banyak yang menggunakan kata sandi dengan frasa sederhana seperti Password1 atau 123456. Jika hacker dapat menemukan kata sandi yang Anda gunakan, mereka dapat dengan mudah masuk ke dalam sistem dan mengakses data-data sensitif di dalamnya. Oleh karena itu, penting bagi perusahaan untuk selalu menggunakan kata sandi yang kuat dan secara regular memperbaruinya.

2. **Adanya kerentanan di dalam aplikasi**

Sebagian besar hacker akan melakukan sejumlah serangan ketika mereka menemukan kerentanan dalam sebuah sistem. Itulah sebabnya, penting bagi perusahaan untuk melakukan penetration testing secara rutin. Penetration testing dapat membantu perusahaan untuk menemukan celah keamanan agar bisa segera ditambal atau diperbaiki.

3. Malware

Malware (malicious software) merupakan suatu program atau file berbahaya yang dibuat dengan tujuan jahat. Peretas dapat menyebarluaskan malware ketika sistem memiliki kerentanan keamanan. Mereka juga dapat menanamkan malware ketika karyawan Anda secara tidak sadar mengklik tautan berbahaya yang dikirim melalui email. Berbagai serangan malware ini biasanya digunakan oleh peretas untuk menghilangkan langkah otentikasi yang digunakan untuk melindungi sistem.

4. **Orang dalam yang berbahaya**

Selain karena faktor kesalahan teknis, data breach juga dapat terjadi karena faktor kesengajaan. Beberapa karyawan Anda mungkin memiliki akses untuk melihat data sensitif perusahaan. Terkadang karena iming-iming imbalan berupa uang, karyawan dapat menyalahgunakannya dan memberikan akses tersebut kepada peretas. Jika peretas berhasil membujuk karyawan Anda, mereka dapat mengakses data dengan mudah tanpa harus mengekploitasi sistem untuk menemukan celah keamanan.

Sumber Infografis : https://hostingtribunal.com/blog/biggest-data-breach-statistics/

SOFTWARE IT AUDIT

Penggunaan software IT audit untuk melakukan pemantauan dan pengujian terhadap aktivitas yang dilakukan user terhadap devices di organisasi

Melakukan pengujian untuk mengetahui apakah sistem yang digunakan memiliki celah keamanan yang dapat diretas oleh pihak yang tidak bertanggung jawab

Mengontrol setiap perubahan yang terjadi pada sistem.

ManageEngine
ADAudit Plus

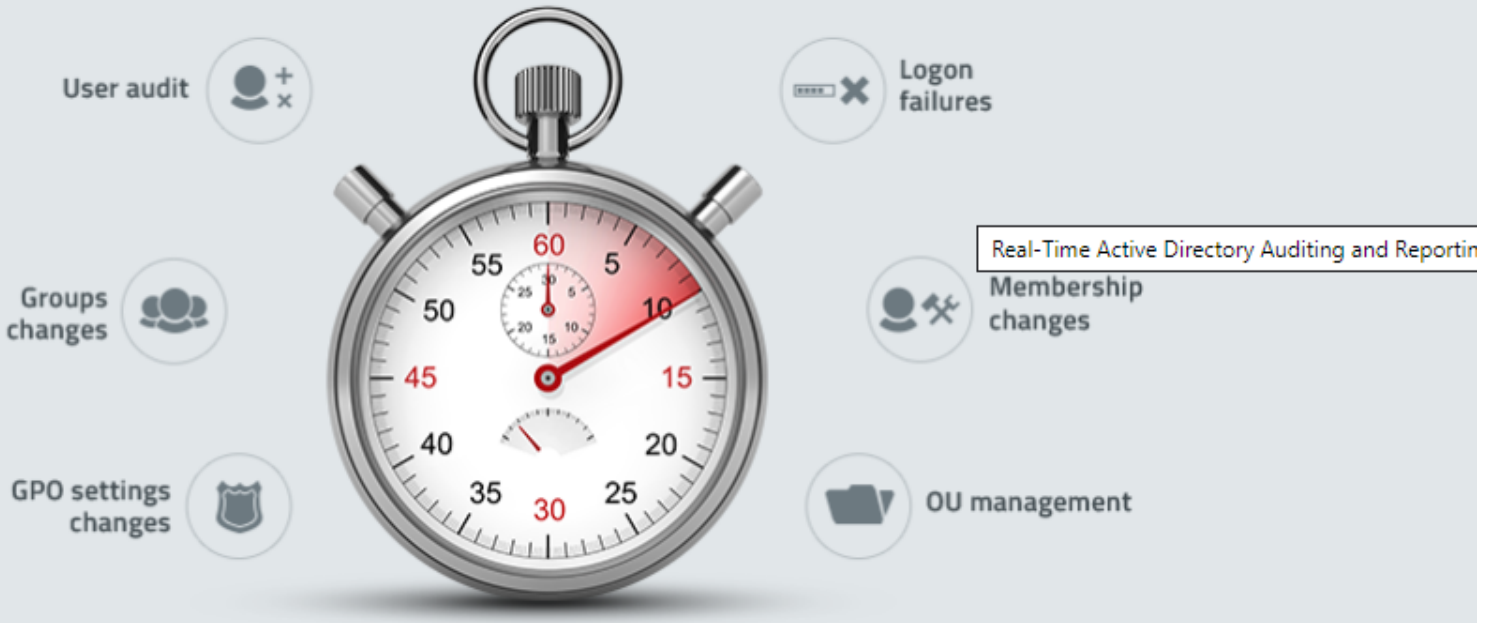
Products Store Partners Support |

Overview Features Demo Resources Get Quote Support Download

Real-Time Auditing for Active Directory

with 200+ audit reports & e-mail alerts

Download



ACTIVE DIRECTORY AUDITING

LOGON/LOGOFF AUDITING

FILE SERVER AUDITING

WINDOWS SERVERS AUDITING

REAL-TIME WINDOWS ACTIVE DIRECTORY AUDITING

In real-time, ensure critical resources in the network like the Domain Controllers are audited, monitored and reported with the entire information on AD objects - Users, Groups, GPO, Computer, OU, DNS, AD Schema and Configuration changes with 200+ detailed event specific GUI reports and email alerts.

Insider Threats

User Logon

Compliance

Reports & Alerts

Data Archiving

GPO Settings

WINDOWS LOGON/LOGOFF AUDITING

Audit the critical user workstation logon & logoff time to monitor the logon duration, logon failures, logon history and terminal services activity. View & Schedule graphical reports with Email alerts for periodic analysis & quick response during security threats.

Logon / Logoff

Compliance

Data Archiving

Reports & Alerts

All Workstation Reports

WINDOWS FILE SERVER AUDITING

Securely track the file creation, modification & deletion from an authorized / unauthorized access, with detailed forensics of security and permission changes to the documents in their files / folder structure and shares.

File Servers

Access Permissions

Failover Clusters

NetApp Filers

EMC Servers

All File Server Reports

WINDOWS SERVERS AUDITING

Track the Logon/Logoff, Schedule to track events like RADIUS Logon, Terminal Services Activity, Logon Duration and Logon History. Audit related processes can be kept tab by Tracking Windows Schedule jobs.

Windows Servers

Printer Auditing

File integrity Monitoring

Compliance

Reports & Alerts

All Windows Servers Reports

EX: HTTPS://WWW.YOUTUBE.COM/WATCH?V=X6SJRLSDQQU

NAMA : EVAN APRIADI DILATAMA

NIM :182420081

MATERI : TUGAS IT AUDIT IT audit Tools/ SEO Audit Tools

MTI 19 B

Pilih salah satu tools atau audit software yang digunakan dalam proses audit TI, kemudian jelaskan fungsi dari tools tersebut dalam mendukung proses audit ?

Picalo

Picalo merupakan sebuah software CAAT (Computer Assisted Audit Techniques) seperti halnya ACL yang dapat dipergunakan untuk menganalisa data dari berbagai macam sumber. Picalo bekerja dengan menggunakan GUI Front end, dan memiliki banyak fitur untuk ETL sebagai proses utama dalam mengekstrak dan membuka data, kelebihan utamanya adalah fleksibilitas dan front end yang baik hingga Librari Python numerik. Berikut ini beberapa kegunaannya : · Menganalisis data keungan, data karyawan · Mengimport file Excel, CSV dan TSV ke dalam databse · Analisa event jaringan yang interaktif, log server situs, dan record sistem login · Mengimport email kedalam relasional dan berbasis teks database · Menanamkan kontrol dan test rutin penipuan ke dalam sistem produksi.

PICALO

1. Dedi Setiadi
2. Febriansyah
3. Fido Rizki
4. Tri Susanti
5. David Agustian

PICALO

- Picalo adalah sebuah aplikasi data analisis yang cocok untuk auditor, pemeriksa fraud, data miner, dan data analisis lainnya. Fokus aplikasi Picalo pada pendeteksian terhadap fraud, korupsi dan untuk mendapatkan data dari database perusahaan. Picalo juga merupakan dasar untuk sebuah sistem otomasi pendeteksi fraud.

FUNGSI DARI APLIKASI :

- Untuk menganalisa data finansial, data pegawai dan sistem purchasing dari adanya error dan fraud.
- Untuk mengimport file Excel, XML, EBCDIC, CSV dan TSV kedalam database.
- Secara interaktif menganalisa kejadian-kejadian dalam jaringan, log web server, dan data login suatu sistem.
- Mengimport email kedalam database relational atau text-based.
- Embedding control dan testing fraud secara rutin pada mesin produksi.

CONTOH PENGGUNAAN PICALO

Untuk menganalisa data finansial, data pegawai dan sistem purchasing dari adanya error dan fraoud

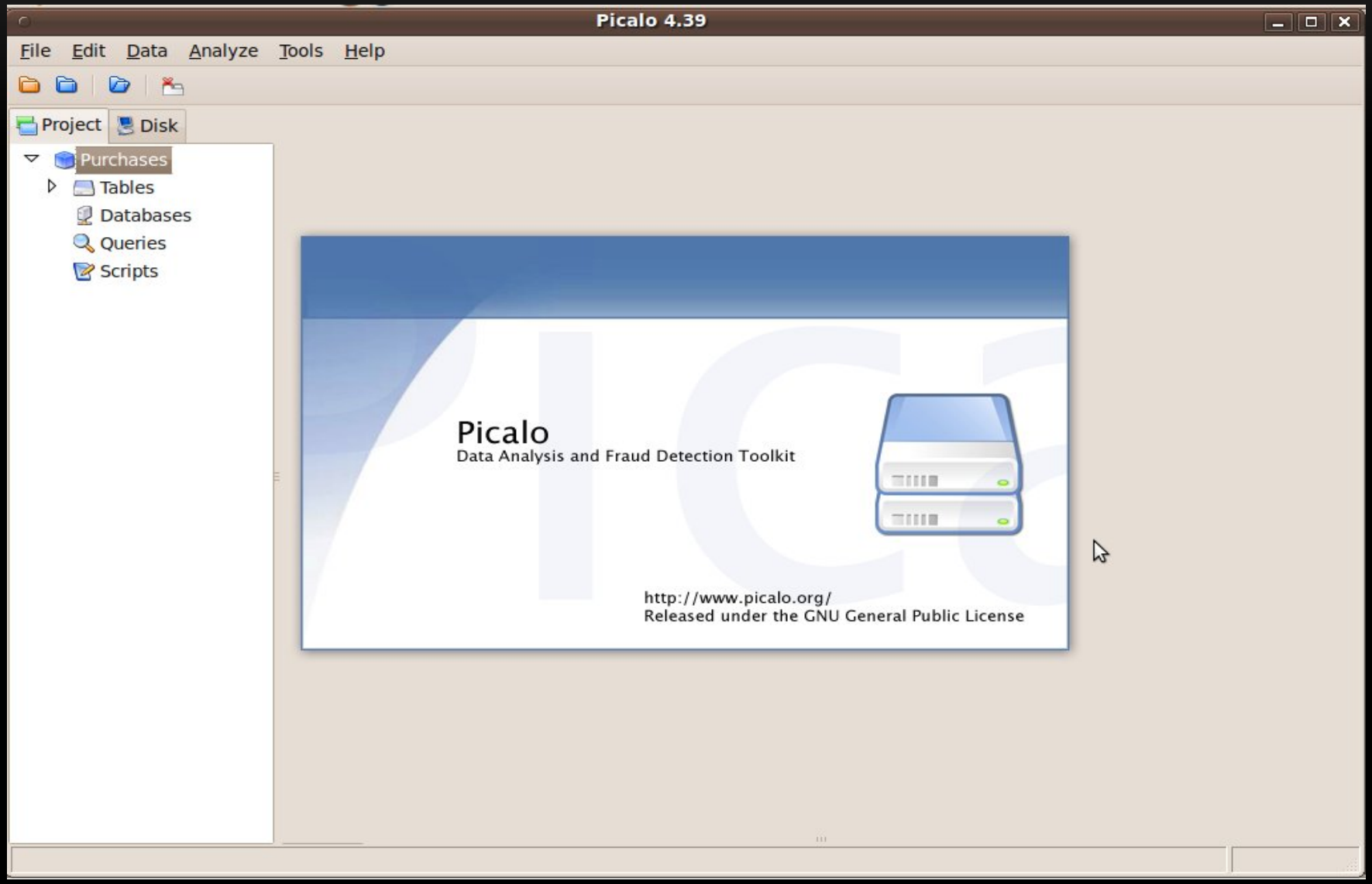
Untuk mengimport file Excel Excel, XML, EBCDIC, CSV dan TSV kedalam database

JENIS DOKUMEN YANG DAPAT DIGUNAKAN

Jenis dokumen yang dapat dianalisi pada picalo adalah sebagai berikut :

- CSV/TSV files,
- EBCDIC files,
- MS Excel files,
- log files,
- text files,

CONTOH


Picalo 4.39
File Edit Data Analyze Tools Help
Project Disk
Purchases
Tables
Databases
Queries
Scripts
Picalo
Data Analysis and Fraud Detection Toolkit
http://www.picalo.org/
Released under the GNU General Public License

KESIMPULAN

Picalo adalah sebuah aplikasi yang dapat digunakan untuk memeriksa fraud, data miner, dan data analisis lainnya.

REFERENCE :

https://aisyahoctav.weebly.com/softskill/review-software-audit-teknologi-informasi

https://www.slideshare.net/triyulianto182/picalo-tool-audit

https://pypi.org/project/picalo/

Nama : Fero Triando
NIM : 182420093
Kelas : MTI 19B

IT Audit Tools

REVIEW ACL (Audit Command Language)

ACL for Windows (sering disebut ACL) adalah sebuah program untuk membantu akuntan dalam melakukan pemeriksaan di lingkungan sistem informasi berbasis komputer atau Pemrosesan Data Elektronik. ACL secara khusus dirancang untuk menganalisa data, memanipulasi data dan mengekspor data sehingga membuatnya menjadi lebih berguna bagi auditor.

ACL dapat mengerjakan berbagai tipe format data. Data yang dihasilkan oleh komputer, disimpan dalam karakter-karakter yang disebut byte. ACL dapat membaca data dari berbagai macam sistem yang terbentang mulai dari model sistem mainframe lama hingga ke relational database modern.

ACL adalah aplikasi yang hanya 'read-only', ACL tidak pernah mengubah data sumber asli sehingga aman untuk menganalisis jenis live-data. Keanekaragaman sumber data dan teknologi akses data, cara mengakses data juga bervariasi dari satu sumber data ke lain. ACL membaca beberapa sumber data secara langsung dengan mengimport dan menyalin sumber data sehingga dapat dianalisis. Banyak jenis data modern saat ini berisi berisi informasi tentang layout record, seperti jumlah record, nama field, panjang field dan tipe data tiap field. Ketika semua informasi ini ada dalam sumber data, atau dalam suatu file definisi eksternal yang terkait, ACL memperoleh ini informasi secara otomatis. Jika informasi tidak menyajikan, maka harus mengacu pada suatu dokumen seperti layout record atau suatu kamus data dan mendefinisikan menggunakan ACL dengan manual.

Paling tidak ada 2 jenis yang utama dalam pengkodean dalam komputer, yaitu:

1. EBCDIC (Extended Binary Coded Decimal Interchang Code) – format ini seringkali ditemukan pada komputer jenis IBM Mainframe.
2. ASCII (American Standard Code for Information Interchange) – format ini hampir digunakan dibanyak komputer. ACL dapat membaca langsung baik jenis EBCDIC atau ASCII, sehingga tidak perlu untuk menngkonversi kedalam bentuk lain.

Perusahaan ACL

ACL adalah salah satu jenis audit software yang termasuk dalam kategori Genaralized Audit Software (GAS). Seperti halnya aplikasi GAS yang lainnya, ACL hanya dapat digunakan untuk mengumpulkan dan mengevaluasi bukti yang dihasilkan dari pemrosesan transaksi perusahaan sehingga ACL lebih cenderung digunakan untuk menilai post transactions daripada current transaction. Setelah mengulang apa itu ACL sekarang kita belajar tentang bagaiana sejarah dari ACL ini.

Prof Hart J. Will yang mengembangkan aplikasi ACL ini. Dikembangkannya ACL ini dimulai pada tahun 1970-an. Hart tidak sendiri mengembangkan aplikasi ini. Dia mengembangkan ACL ini melalui perusahaan yang bernama ACL Services Ltd yang ada di Kanada. Perusahaan ini sebenarnya khusus membuat aplikasi-aplikasi komputer. Sehingga kegiatan utamanya adalah membuat dan menjual aplikasi analisis data, aplikasi tata kelola, aplikasi manajemen resiko dan aplikasi kepatuhan.

Harmut (Hart) J. Will. adalah seorang Profesor Emeritus Akuntansi, Auditing dan Sistem Informasi manajemen di Sekolah Administrasi Publik di Victoria. Penemuan dia bernama ACL ini disebut-sebut sebagai evolusi pendekatan audit audit.

Awal mula Hart mengembangkan ACL dimulai pada tahun 1960 ketika dia berada di Berlin yang sedang menyelesaikan tesisnya. ACL yang dia kembangkan itu selesai pada tahun 1968 ketika dia berada di Illinois. Awal mula sistem yang dia buat adalah kerangka Manajemen Sistem Informasi yang isisnya adalah Bank Data dan Bank Model. Selanjutnya dikembangkan sedemikian rupa sehingga jadilah aplikasi audit yang bernama ACL.

Fungsi ACL

- Bidang Auditor

Pengguna ahli ini memiliki latar belakang yang memungkinkan dia menjadi seorang auditor sehingga ACL yang digunakannya bisa ditafsirkan dan digunakan untuk mempermudah pekerjaannya sebagai auditor. Manfaat ACL yang dapat dirasakan oleh seorang auditor dalam penggunaan ACL ini adalah ACL bisa membantu auditor dalam melaksanakan tugasnya yaitu mengaudit laporan keuangan perusahaan secara fokus, cepat, efisien dan akurat. Karena teknologi pada intinya dibuat untuk mempermudah pekerjaan manusia, untuk mengurangi kesalahan yang bisa terjadi dan untuk mempercepat pekerjaan.

- Bidang Manajemen

Dalam suatu peruahaan ada bagian keuangannya, bagian keuangan inilah yang dimaksudnya manajemen. Bagian keuangan bisa melakukan analisis suatu data perusahaan menggunakan ACL untuk tujuan tertentu seperti melakukan analisis terhadap penjualan, bagaimana trending penjualan dan lain sebagainya. Selain digunakan manajemen untuk melakukan analisis data ACL juga bisa dilakukan untuk pengujian pengendalian perusahaan. Kalau sudah masuk kedalam pengendalian internal ini menyangkut auditing. Pengendalian internal sangat diperlukan untuk mengetahui apakah kemungkinan perusahaan melakukan kecurangan tinggi atau tidak. Penjelasan lebih dalam tentang pengendalian internal akan dibahas dalam auditing. ACL juga bisa digunakan manajemen dalam pembuatan laporan yang diinginkan. Manajemen dapat menggunakan ACL untuk :

1. Analisis data
2. Pengujian pengendalian perusahaan
3. Pembuatan laporan keuangan yang diinginkan

Fitur dan kemampuan ACL Software Tools:

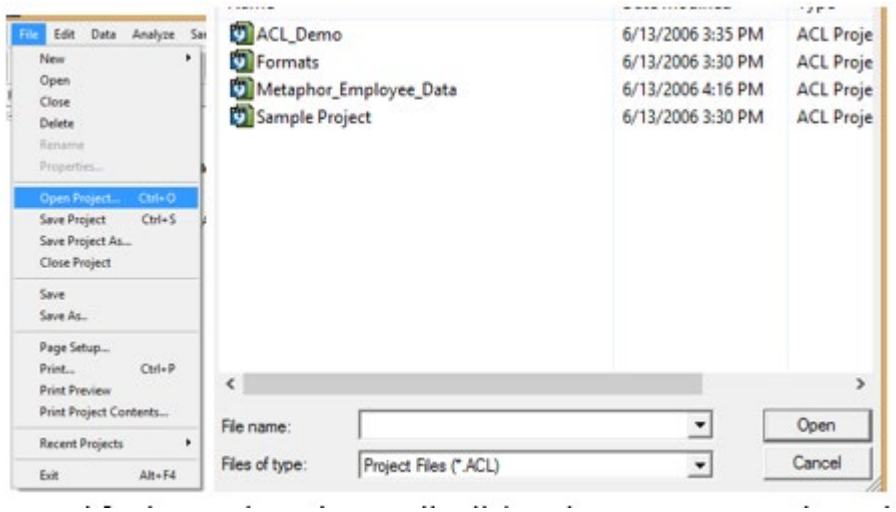
1. *Universal Data Access*, yaitu dapat mengakses data dari hampir semua jenis *database* yang ada (DBF, XLS, Text File, report file, Oracle, SQL, DB2, AS/400 FDF, COBOL, dsb) dan semua *platform*(PC, *minicomputer*, dan *mainframe*).
2. Jumlah Data Besar, yaitu kemampuan dalam mengakses dan memproses data dalam jumlah yang sangat besar (hingga ratusan juta *record*).
3. Kecepatan Waktu Proses, kemampuannya untuk memproses dalam waktu yang singkat walaupun data yang diproses dalam jumlah yang besar.
4. Integritas Data, dengan kemampuan mengakses database 100% (tanpa metode *sampling*) serta data yang bersifat *Read Only* yang dapat menjamin orisinalitas, keamanan dan integritas data untuk pengolahan menjadi informasi yang bermanfaat bagi *user* dan manajemen.
5. Automasi, pembuatan aplikasi audit yang sangat cepat dan mudah untuk melakukan automasi analisis data untuk efisiensi proses kerja.
6. *Multi File Process*, dapat digunakan untuk menangani beberapa file sekaligus, tanpa mengganggu operasional teknologi informasi yang dijalankan oleh perusahaan.
7. *Log File Navigation*, dilengkapi dengan *log file* untuk pencatatan proses analisis yang telah dilakukan sehingga menghasilkan suatu *audit trail* yang komprehensif.
8. Fungsi Analisis yang Lengkap, dilengkapi fungsi-fungsi analisis yang sangat lengkap yang dapat dengan mudah dikombinasikan dalam menghasilkan temuan-temuan yang tidak pernah terkirakan sebelumnya.
9. Pelaporan yang Handal, kemudahan untuk merancang laporan yang handal sarat informasi yang bermanfaat serta dapat dikirimkan secara otomatis via email atau integrasi ke dalam *software* aplikasi Crystal Report.
10. IT Audit, kemudahan dalam menguji integritas data dan menganalisis data yang ada di dalam *database* ataupun menganalisis *user-user* yang telah masuk ke dalam suatu jaringan/*network*.

Manfaat menggunakan ACL Software Tools:

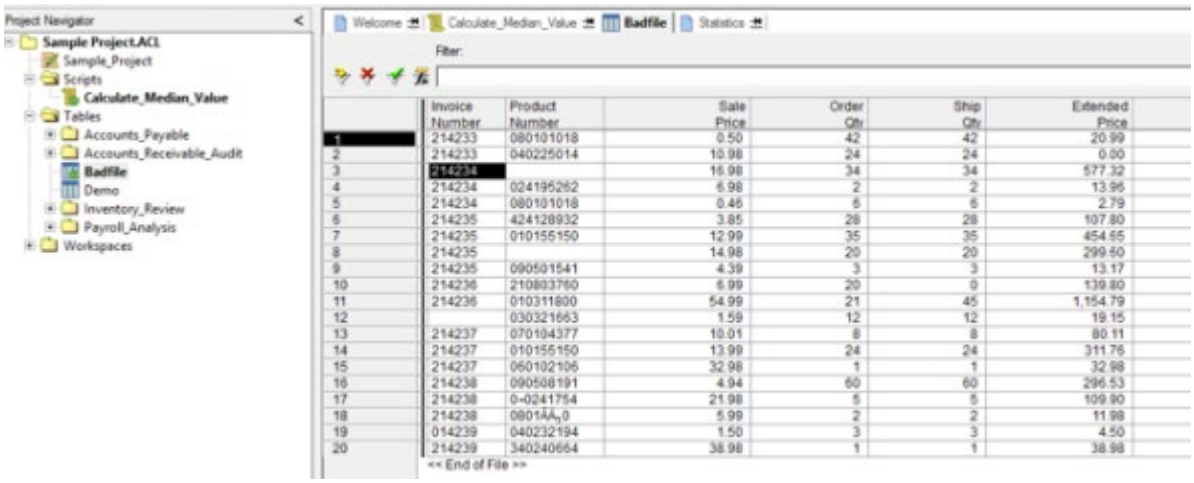
- Dapat membantu dalam mengAkses data baik langsung (*Direct*) kedalam system jaringan ataupun tidak langsung (*InDirec*t) melalui media lain seperti *softcopy* dalam bentuk *teks file/report*.
- Menempatkan kesalahan dan potensial *fraud* sebagai pembanding dan menganalisa *file-file* menurut aturan-aturan yang ada.
- Mengidentifikasi kecenderungan/gejala-gejala, dapat juga menunjukan dengan tepat/sasaran pengecualian data dan menyoroti potensial area yang menjadi perhatian.
- Mengidentifikasi proses perhitungan kembali dan proses verifikasi yang benar.
- Mengidentifikasi persoalan sistem pengawasan dan memastikan terpenuhinya permohonan dengan aturan-aturan yang telah ditetapkan.

- *Aging* dan menganalisa *Account Receivable/Payable* atau beberapa transaksi lain dengan menggunakan basis waktu yang sensitif.
- Memulihkan biaya atau pendapatan yang hilang dengan pengujian data pada data-data duplikasi pembayaran, menguji data-data nomor *Invoice*/Faktur yang hilang atau pelayanan yang tidak tertagih.
- Menguji terhadap hubungan antara authorisasi karyawan dengan *supplier*.
- Melakukan proses *Data Cleansing* dan *Data Matching* atau pembersihan data dari data-data duplikasi terutama dari kesalahan pengetikan oleh *End-User*.
- Dapat melaksanakan tugas pengawasan dan pemeriksaaan dengan lebih fokus, cepat, efisien, dan efektif dengan lingkup yang lebih luas dan analisa lebih mendalam. Mengidentifikasi penyimpangan (*Fraud Detection*) dapat dilakukan dengan cepat dan akurat sehingga memiliki waktu lebih banyak alam menganalisa data dan pembuktian.
- **Review Software ACL 9**

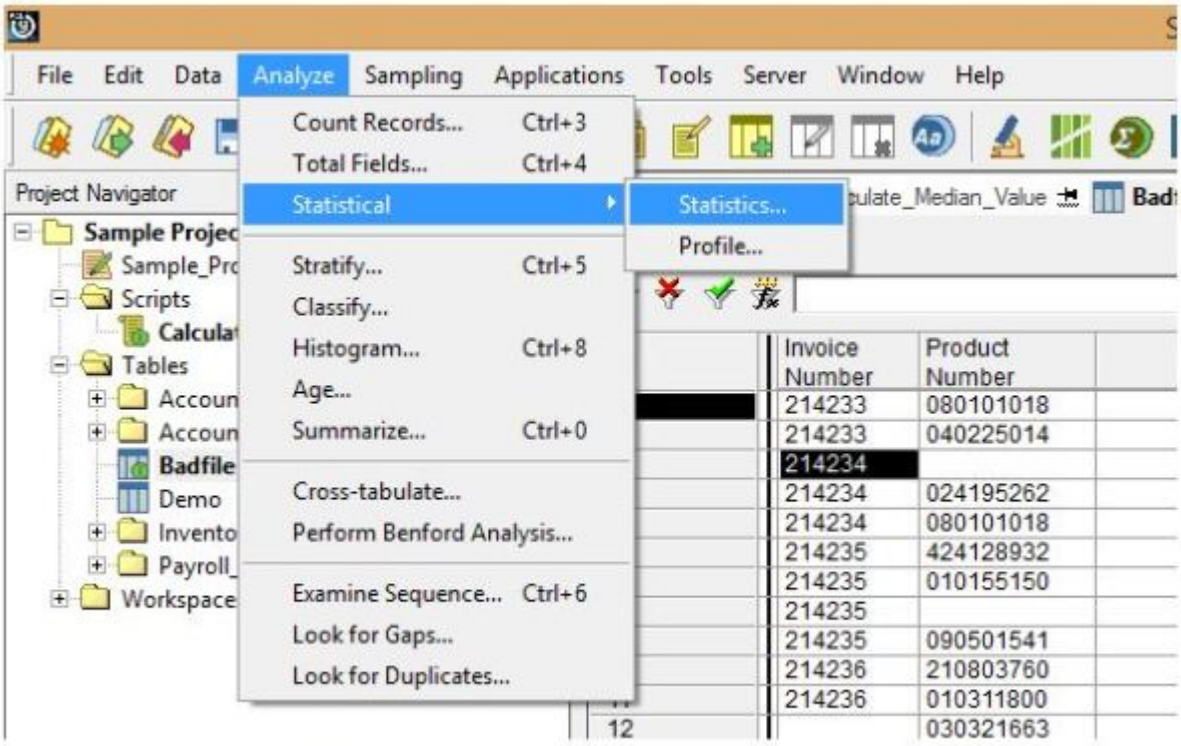
  Contoh menggunakan acl pada versi acl 9 untuk melihat data berupa statistika



Pada software acl 9 ada sample project yg disediakan, langsung open project saja dan pilih Sample Project.acl

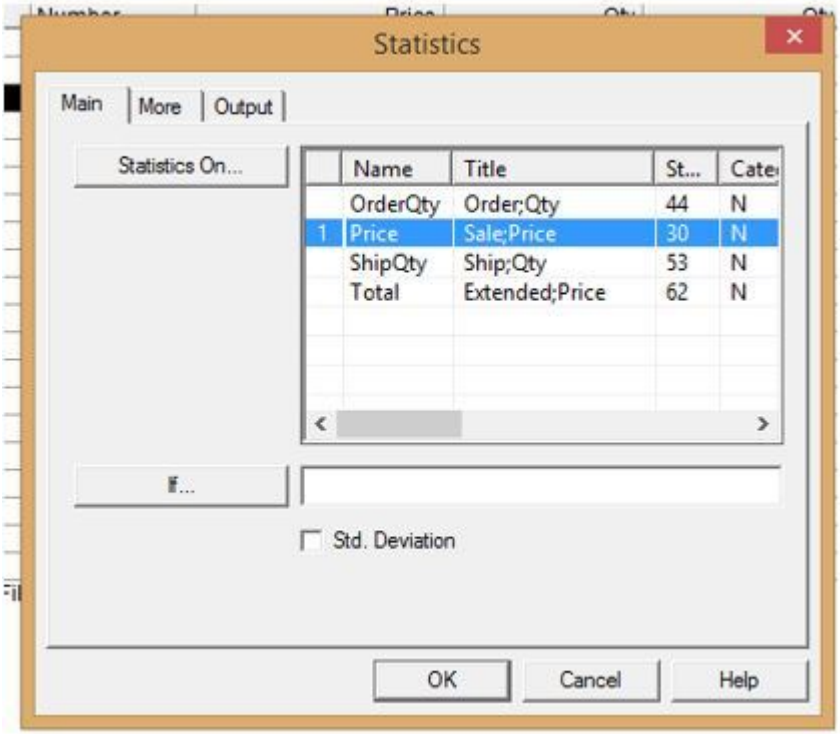


Pada software acl setelah open sample project, akan menampilkan data berikut pada file BadFile

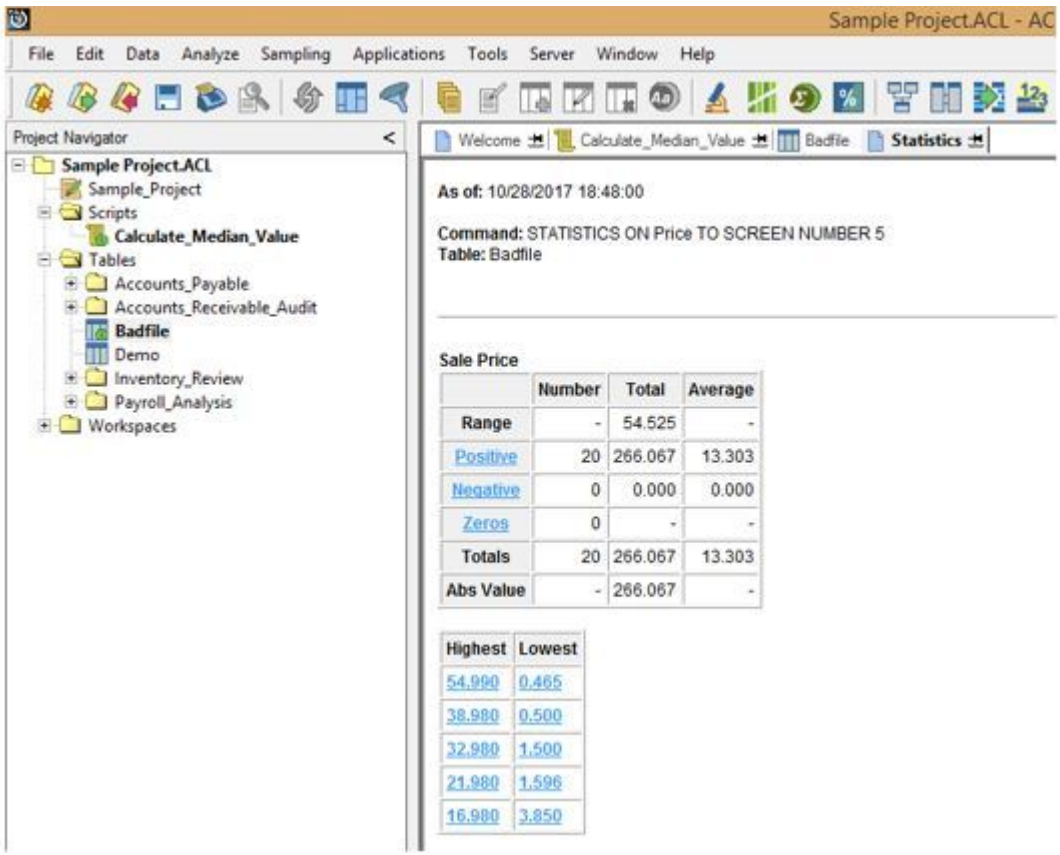


pilih menu Analyze dan pilih Statistical > Statistics...

pilih menu Analyze dan pilih Statistical > Statistics…



Pilih baris yang akan ditampilkan statistiknya, lalu klik OK



Hasil statistika bisa terlihat disini sehingga memudahkan untuk mengaudit dan menganalisa data

PICALO

1. Dedi Setiadi
2. Febriansyah
3. Fido Rizki
4. Tri Susanti
5. David Agustian

PICALO

- Picalo adalah sebuah aplikasi data analisis yang cocok untuk auditor, pemeriksa fraud, data miner, dan data analisis lainnya. Fokus aplikasi Picalo pada pendeteksian terhadap fraud, korupsi dan untuk mendapatkan data dari database perusahaan. Picalo juga merupakan dasar untuk sebuah sistem otomasi pendeteksi fraud.

FUNGSI DARI APLIKASI :

- Untuk menganalisa data finansial, data pegawai dan sistem purchasing dari adanya error dan fraud.
- Untuk mengimport file Excel, XML, EBCDIC, CSV dan TSV kedalam database.
- Secara interaktif menganalisa kejadian-kejadian dalam jaringan, log web server, dan data login suatu sistem.
- Mengimport email kedalam database relational atau text-based.
- Embedding control dan testing fraud secara rutin pada mesin produksi.

CONTOH PENGGUNAAN PICALO

Untuk menganalisa data finansial, data pegawai dan sistem purchasing dari adanya error dan fraoud

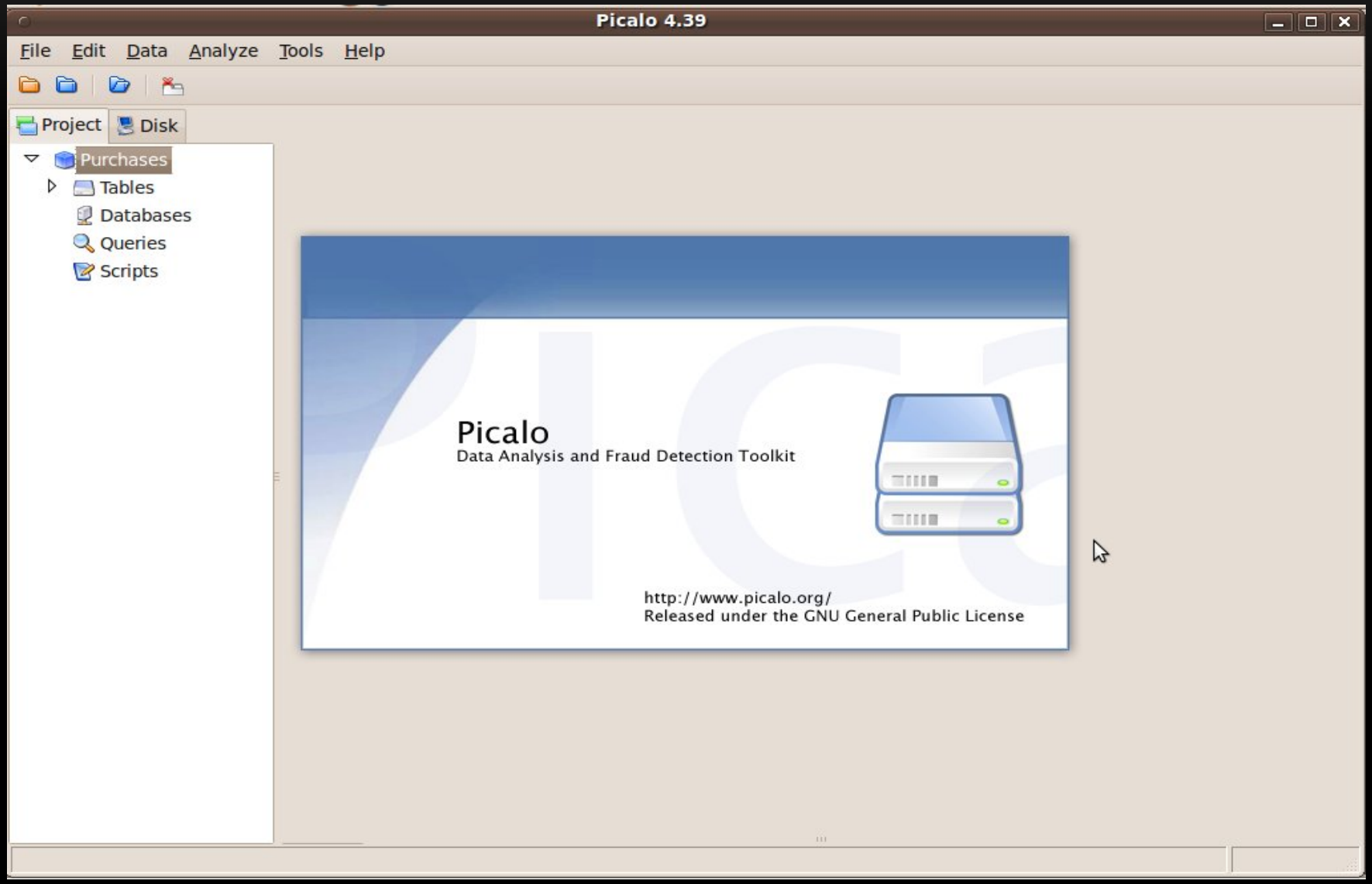
Untuk mengimport file Excel Excel, XML, EBCDIC, CSV dan TSV kedalam database

JENIS DOKUMEN YANG DAPAT DIGUNAKAN

Jenis dokumen yang dapat dianalisi pada picalo adalah sebagai berikut :

- CSV/TSV files,
- EBCDIC files,
- MS Excel files,
- log files,
- text files,

CONTOH


Picalo 4.39
File Edit Data Analyze Tools Help
Project Disk
Purchases
Tables
Databases
Queries
Scripts
Picalo
Data Analysis and Fraud Detection Toolkit
http://www.picalo.org/
Released under the GNU General Public License

KESIMPULAN

Picalo adalah sebuah aplikasi yang dapat digunakan untuk memeriksa fraud, data miner, dan data analisis lainnya.

REFERENCE :

https://aisyahoctav.weebly.com/softskill/review-software-audit-teknologi-informasi

https://www.slideshare.net/triyulianto182/picalo-tool-audit

https://pypi.org/project/picalo/

Nama : Fitrianto Puja Kesuma

NIM : 182420082

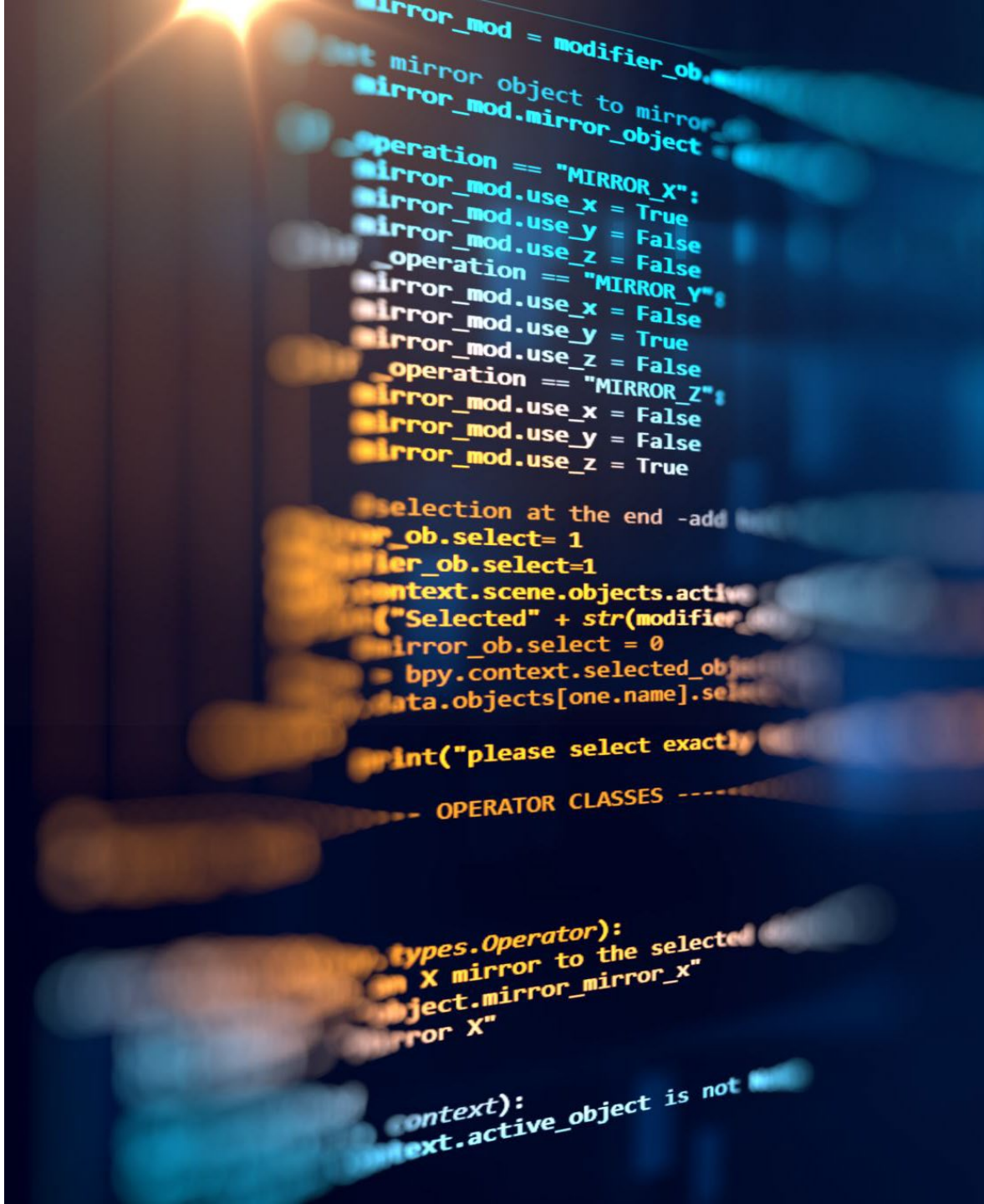
Tool-tool yang dapat digunakan untuk membantu pelaksanaan Audit Teknologi Informasi. Tidak dapat dipungkiri, penggunaan tool-tool tersebut memang sangat membantu Auditor Teknologi Informasi dalam menjalankan profesinya, baik dari sisi kecepatan maupun akurasinya.

A. ACL

ACL (Audit Command Language) merupakan sebuah software CAAT (Computer Assisted Audit Techniques) yang sudah sangat populer untuk melakukan analisa terhadap data dari berbagai macam sumber. ACL for Windows (sering disebut ACL) adalah sebuah software TABK (TEKNIK AUDIT BERBASIS KOMPUTER) untuk membantu auditor dalam melakukan pemeriksaan di lingkungan sistem informasi berbasis komputer atau Pemrosesan Data Elektronik.

SOFTWARE IT AUDIT

Manage Engine AD Audit Plus



JENIS RESIKO AUDIT

Control Risk (Risiko Pengendalian)
Adalah ukuran penetapan auditor akan kemungkinan adanya kekeliruan (salah saji) dalam segmen audit yang melampaui batas toleransi yang tidak terdeteksi atau tercegah oleh struktur pengendalian intern klien.

SALAH SATU RESIKO YANG MUNGKIN MUNCUL DI BIDANG IT

Data Breach

merupakan salah satu jenis serangan cyber yang dapat mengancam bisnis Anda. Data breach atau pelanggaran data merupakan suatu kondisi di mana hacker mampu menyusup masuk ke dalam sistem dan mengekstraksi data-data penting di dalamnya.

Hal ini mampu membawa berbagai dampak negatif untuk bisnis, mulai dari tercurinya data-data sensitif sampai hilangnya kepercayaan pelanggan. Untuk menghindarinya,

APA SAJA YANG DAPAT MENYEBABKAN DATA BREACH DAPAT TERJADI.

1. **Kredensial yang lemah**

Kredensial atau kata sandi yang lemah menjadi salah satu penyebab data breach dapat terjadi. Kata sandi dibuat dengan tujuan untuk mengamankan sistem. Namun sayangnya masih banyak yang menggunakan kata sandi dengan frasa sederhana seperti Password1 atau 123456. Jika hacker dapat menemukan kata sandi yang Anda gunakan, mereka dapat dengan mudah masuk ke dalam sistem dan mengakses data-data sensitif di dalamnya. Oleh karena itu, penting bagi perusahaan untuk selalu menggunakan kata sandi yang kuat dan secara regular memperbaruinya.

2. **Adanya kerentanan di dalam aplikasi**

Sebagian besar hacker akan melakukan sejumlah serangan ketika mereka menemukan kerentanan dalam sebuah sistem. Itulah sebabnya, penting bagi perusahaan untuk melakukan penetration testing secara rutin. Penetration testing dapat membantu perusahaan untuk menemukan celah keamanan agar bisa segera ditambal atau diperbaiki.

3. Malware

Malware (malicious software) merupakan suatu program atau file berbahaya yang dibuat dengan tujuan jahat. Peretas dapat menyebarluaskan malware ketika sistem memiliki kerentanan keamanan. Mereka juga dapat menanamkan malware ketika karyawan Anda secara tidak sadar mengklik tautan berbahaya yang dikirim melalui email. Berbagai serangan malware ini biasanya digunakan oleh peretas untuk menghilangkan langkah otentikasi yang digunakan untuk melindungi sistem.

4. **Orang dalam yang berbahaya**

Selain karena faktor kesalahan teknis, data breach juga dapat terjadi karena faktor kesengajaan. Beberapa karyawan Anda mungkin memiliki akses untuk melihat data sensitif perusahaan. Terkadang karena iming-iming imbalan berupa uang, karyawan dapat menyalahgunakannya dan memberikan akses tersebut kepada peretas. Jika peretas berhasil membujuk karyawan Anda, mereka dapat mengakses data dengan mudah tanpa harus mengekploitasi sistem untuk menemukan celah keamanan.

Sumber Infografis : https://hostingtribunal.com/blog/biggest-data-breach-statistics/

SOFTWARE IT AUDIT

Penggunaan software IT audit untuk melakukan pemantauan dan pengujian terhadap aktivitas yang dilakukan user terhadap devices di organisasi

Melakukan pengujian untuk mengetahui apakah sistem yang digunakan memiliki celah keamanan yang dapat diretas oleh pihak yang tidak bertanggung jawab

Mengontrol setiap perubahan yang terjadi pada sistem.

ManageEngine
ADAudit Plus

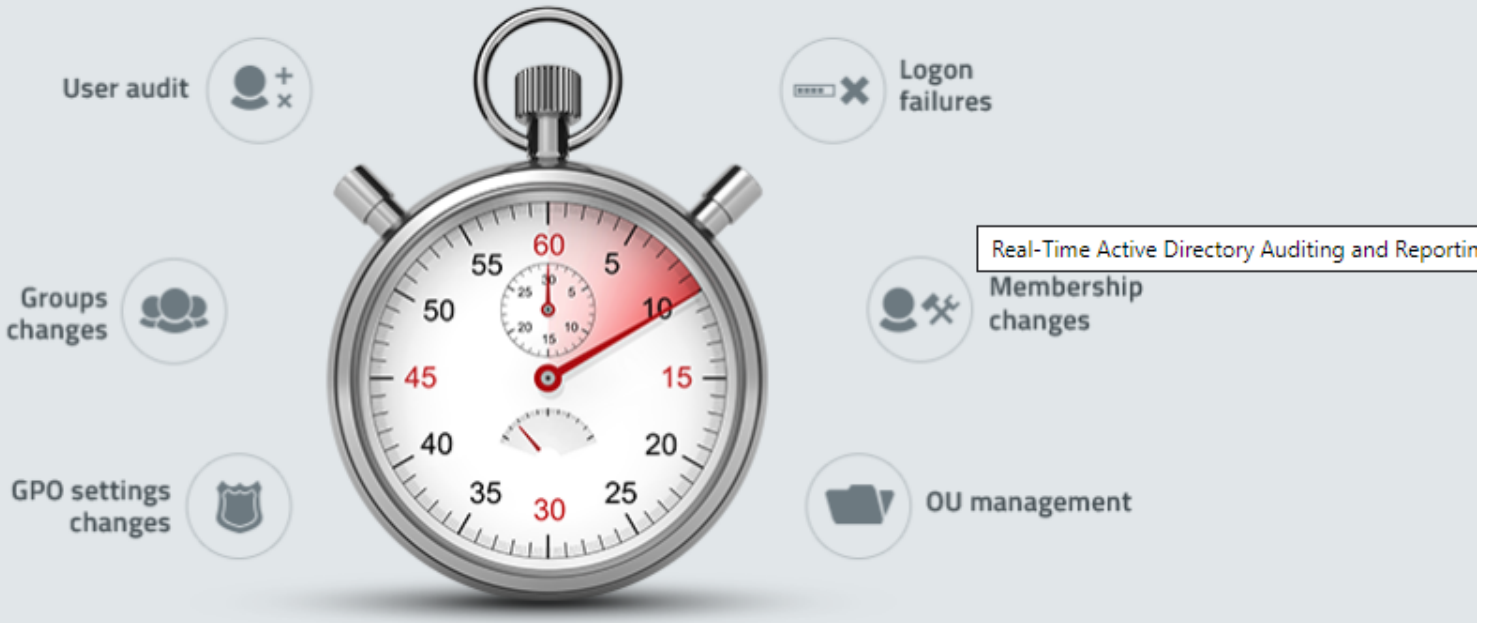
Products Store Partners Support |

Overview Features Demo Resources Get Quote Support Download

Real-Time Auditing for Active Directory

with 200+ audit reports & e-mail alerts

Download



ACTIVE DIRECTORY AUDITING

LOGON/LOGOFF AUDITING

FILE SERVER AUDITING

WINDOWS SERVERS AUDITING

REAL-TIME WINDOWS ACTIVE DIRECTORY AUDITING

In real-time, ensure critical resources in the network like the Domain Controllers are audited, monitored and reported with the entire information on AD objects - Users, Groups, GPO, Computer, OU, DNS, AD Schema and Configuration changes with 200+ detailed event specific GUI reports and email alerts.

Insider Threats

User Logon

Compliance

Reports & Alerts

Data Archiving

GPO Settings

WINDOWS LOGON/LOGOFF AUDITING

Audit the critical user workstation logon & logoff time to monitor the logon duration, logon failures, logon history and terminal services activity. View & Schedule graphical reports with Email alerts for periodic analysis & quick response during security threats.

Logon / Logoff

Compliance

Data Archiving

Reports & Alerts

All Workstation Reports

WINDOWS FILE SERVER AUDITING

Securely track the file creation, modification & deletion from an authorized / unauthorized access, with detailed forensics of security and permission changes to the documents in their files / folder structure and shares.

File Servers

Access Permissions

Failover Clusters

NetApp Filers

EMC Servers

All File Server Reports

WINDOWS SERVERS AUDITING

Track the Logon/Logoff, Schedule to track events like RADIUS Logon, Terminal Services Activity, Logon Duration and Logon History. Audit related processes can be kept tab by Tracking Windows Schedule jobs.

Windows Servers

Printer Auditing

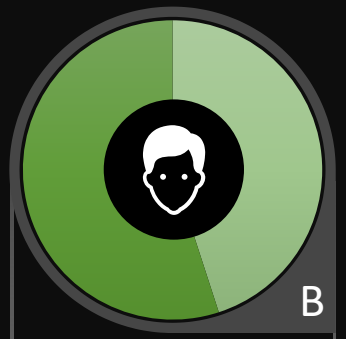
File integrity Monitoring

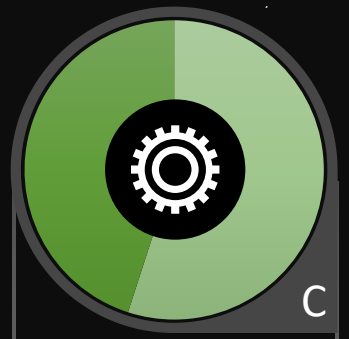
Compliance

Reports & Alerts

All Windows Servers Reports

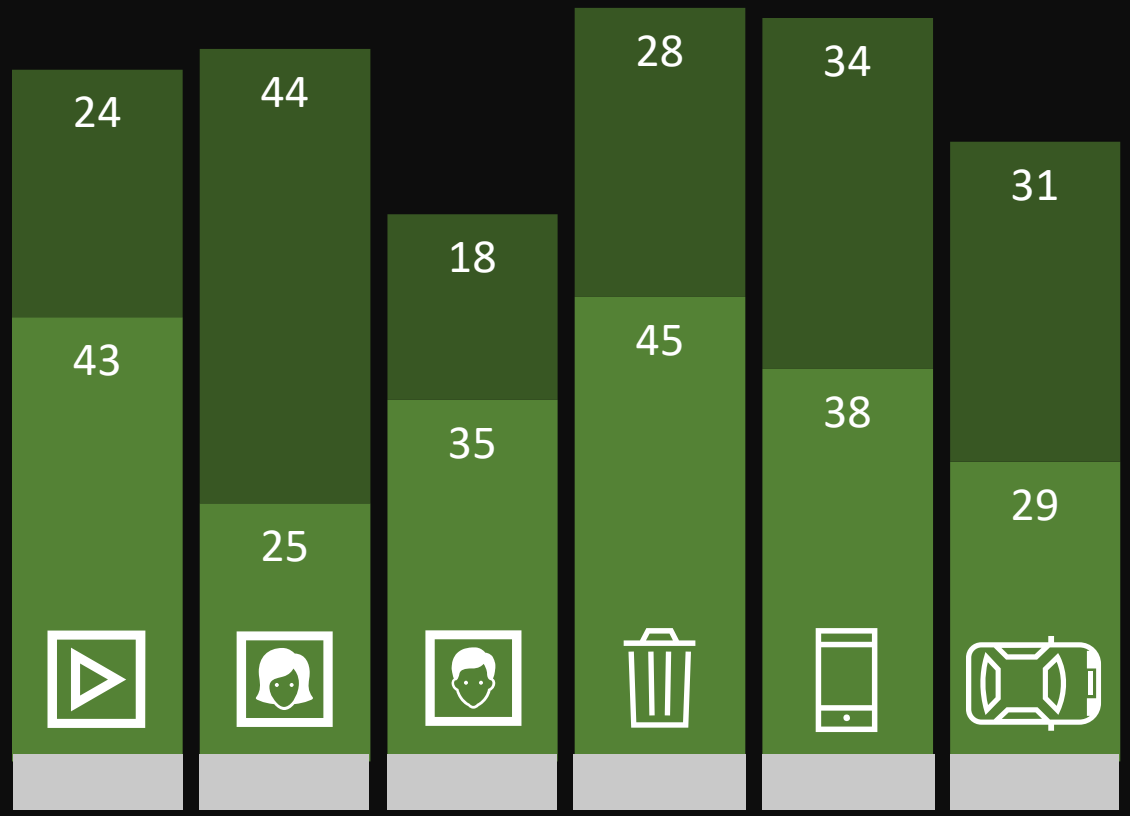
DEMO : HTTPS://WWW.YOUTUBE.COM/WATCH?V=X6SJRLSDQQU





Hendri

182420098



Apa itu SEO..?

SEO adalah singkatan dari "search engine optimization" (pengoptimalan mesin telusur) atau "search engine optimizer". Penggunaan jasa SEO adalah keputusan besar yang dapat meningkatkan peringkat situs Anda dan menghemat waktu, tapi juga berisiko tinggi terhadap situs dan reputasi. Pastikan meneliti kemungkinan keuntungan serta kelemahan yang dapat ditimbulkan oleh SEO yang tidak bertanggung jawab terhadap situs Anda. Banyak SEO dan agen serta konsultan lain yang menyediakan layanan yang bermanfaat bagi pemilik situs web, meliputi:

Ulasan tentang konten atau struktur situs Anda

Saran teknis tentang pengembangan situs web: misalnya, hosting, pengalihan, halaman error, dan penggunaan JavaScript

Pengembangan konten

Manajemen kampanye pengembangan bisnis online

Penelitian kata kunci

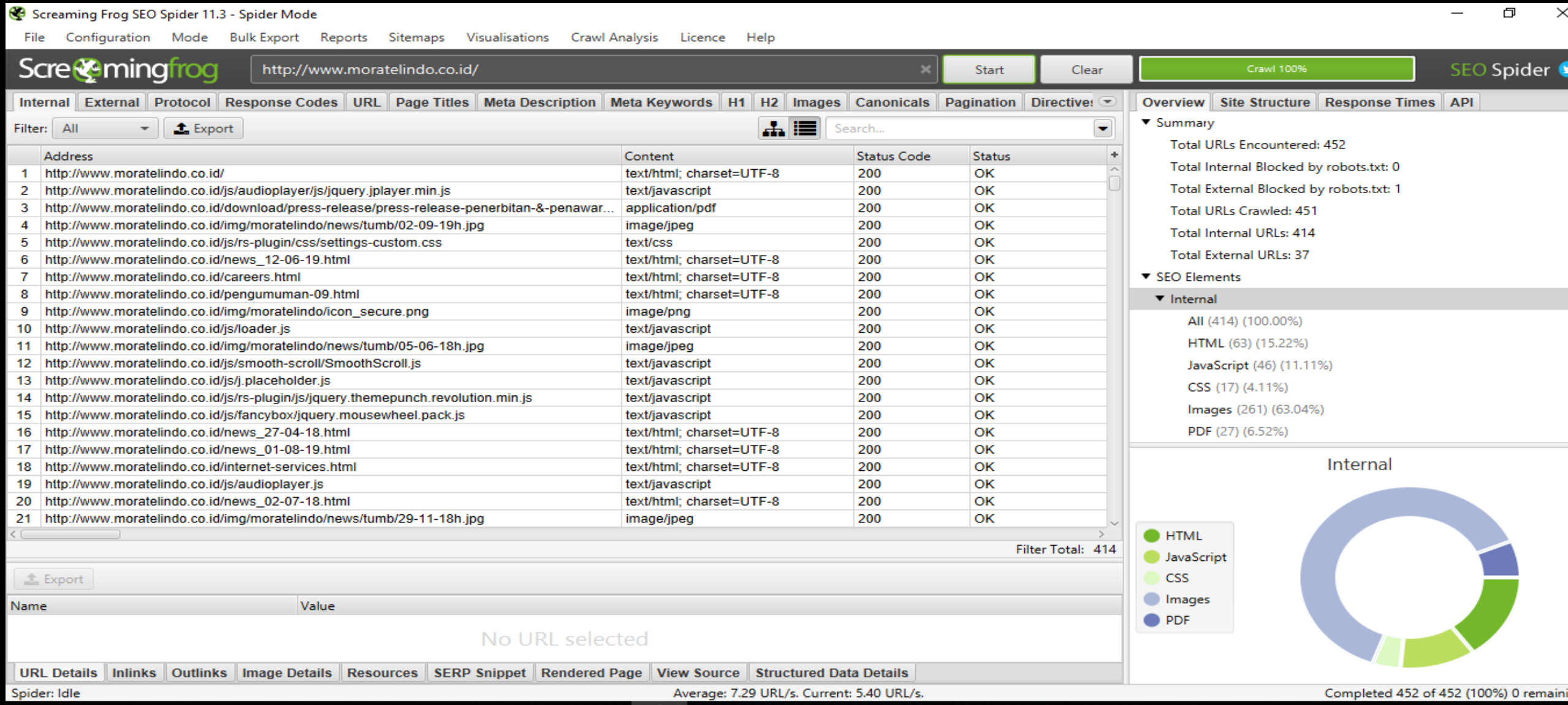
Pelatihan SEO

Keahlian dalam pasar dan geografis tertentu.

Apa itu Screaming Frog?

Screaming Frog SEO Spider adalah sebuah aplikasi desktop yang kecil, Anda dapat menginstal secara lokal di komputer PC, Mac, atau Linux. Dia menjelajahi link, gambar, CSS, dll situs web dari sudut pandang SEO. Yang pada dasarnya memberitahu Anda apa yang akan search spider lihat ketika dia menjelajahi situs web.
Informasi ini memungkinkan Anda untuk dengan cepat menganalisa, audit dan meninjau situs dari perspektif SEO onsite. Hal ini dapat menghemat satu ton pekerjaan, karena secara manual menganalisis setiap halaman website besar bisa sangat menantang.

Screaming Frog



Kesimpulan

Dengan Screaming Frog SEO Spider Anda dapat menganalisis beberapa elemen di tempat, seperti judul halaman, meta descriptions, struktur URL, kode respon, gambar, dll. Ini adalah alat yang hebat untuk membantu Anda mengoptimalkan sebuah situs web dan meningkatkan kinerja di halaman hasil pencarian. Selain itu; itu benar-benar gratis, sehingga seharusnya menjadi alat wajib dalam toolbox setiap desainer web!

IT Audit Tools

NMAP (Network Mapper)

- Ilsa Palingga Ninditama
- Rahma Fitriyani
- Ricca Verana Sari
- Safta Hastini
- Uci Suryani

NMAP (Network Mapper)

Open source untuk melakukan eksplorasi jaringan dan audit keamanan. Nmap didesain untuk mampu menscan network yang besar, walau NMAP juga sangat handal untuk melakukan scan pada satu host tertentu.

Nmap mempergunakan IP paket raw untuk menentukan host yang aktif pada jaringan, service (nama aplikasi dan versi) yang disediakan oleh host, operating system (versi OS) yang sedang berjalan, tipe filter/firewall yang dipakai, dan karakteristik lainnya.

Nmap biasanya dipakai juga untuk audit keamanan, banyak sistem dan network admin menemukan kemudahan untuk pemakaiannya untuk pemakaian rutin, seperti network inventory,manajemen jadwal update service, monitoring host or service uptime.

Fungsi

NMAP

- Untuk mengeksplorasi jaringan seperti banyaknya administrator system dan jaringan yang menggunakan aplikasi
- Menemukan banyak fungsi dalam inventori jaringan
- Mengatur jadwal peningkatan service.
- Memonitor host atau waktu pelayanan.

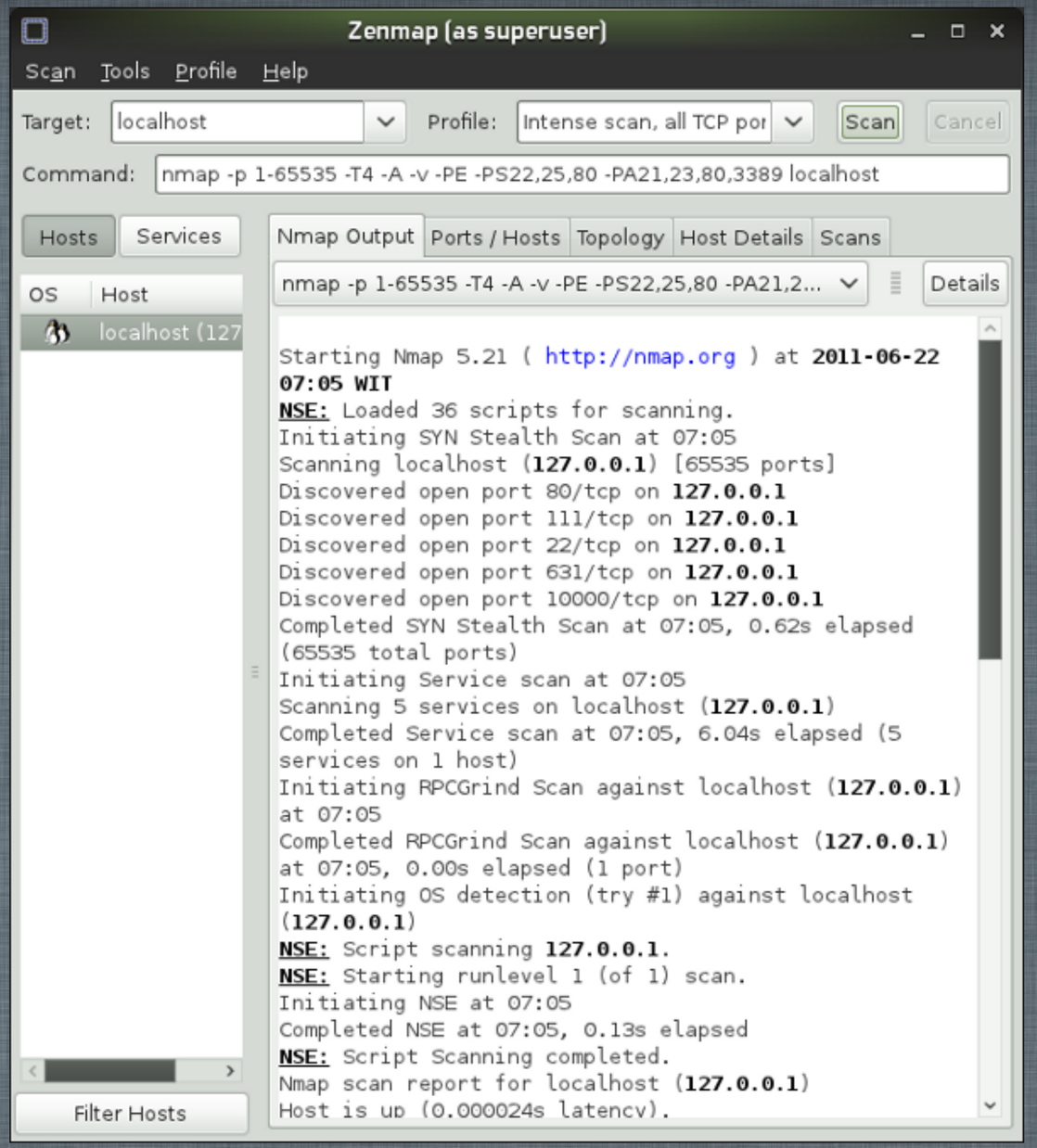
Contoh Penggunaan NMAP Dengan Menggunakan Command Line:

```
wdzgouch@server1:~> nmap localhost

Starting Nmap 5.21 ( http://nmap.org ) at 2011-06-22 10:28 WIT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00028s latency).
rDNS record for 127.0.0.1: linux-34ar.site
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
631/tcp   open  ipp
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Contoh Tampilan Penggunaan NMAP dengan menggunakan Aplikasi GUI: Zenmap.



KESIMPULAN

NMAP adalah sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Output NMAP adalah sebuah daftar target host yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan.

That’s all!

Thank you! ☺

Nama : Indri Endang Lestari (MTI19AR2)

ACL (Audit Command Language)

Perkembangan yang pesat profesi internal audit merefleksikan bahwa betapa pentingnya pemeriksaan (auditor) internal pada team manajemen. Hal ini dapat terlihat dari banyaknya auditor yang dipekerjakan pada suatu perusahaan yang akan mengevaluasi performasi manajemen dan memberikan pendapat yang independent. Adapun salah satu tools yang digunakan auditor untuk melakukan audit adalah ACL (Audit command language)

ACL adalah sebuah software yang dirancang secara khusus untuk menganalisa data dan menghasilkan laporan audit, baik untuk pengguna biasa (common/ nontechnical users) maupun pengguna ahli (expert users). ACL mulai dikembangkan sejak tahun 1970an oleh Prof. Hart J. Will dari Canada dan kemudian dikelola oleh ACL Services Ltd Vancouver, Canada. Dan merupakan Pemimpin pasar dalam teknologi pengambilan data, analisis data, serta pelaporan, (hasil survey tahunan *The Institute of Internal Auditors*, USA, 2005).

ACL juga merupakan Tools yang paling diminati untuk dapat membantu proses analisis data secara interaktif dalam menghasilkan informasi yang tepat guna bagi keperluan pengambilan keputusan yang tepat bagi manajemen. ACL juga merupakan suatu sistem berbasis windows yang bersifat '*Graphical User Interface* (GUI)' dan sangat mudah digunakan ('*User Friendly'*) untuk melakukan suatu proses analisis data serta monitoring. ACL telah dikembangluaskan dengan fungsi untuk memenuhi kebutuhan analisis data seluruh aktivitas bisnis operasional di dalam perusahaan, Di antaranya di bidang Audit untuk analisis data, pencocokan & pembandingan data, laporan penyimpangan, dsb; bidang IT (Information Technology) untuk data migration, data cleansing, data matching, data integrity testing; selain itu juga untuk analisis, konsolidasi,

rekonsiliasi data dan pelaporan pada divisi lain seperti Keuangan, Pemasaran, Distribusi, Operasional, dan lain sebagainya.

Adapun keuntungan menggunakan Tools ACL dalam melakukan audit adalah mudah dalam penggunaan, built- in audit dan analisis data secara fungsional, kemampuan menangani ukuran file yang tidak terbatas, kemampuan mengekspor hasil audit, pembuatan laporan berkualitas tinggi

Adapun manfaat audit menggunakan ACL adalah :

- Dapat membantu dalam mengakses data baik langsung *(direct)* kedalam sistem jaringan ataupun *indirect* (tidak langsung) melalui media lain seperti softcopy.
- Menempatkan kesalahan dan potensial "fraud" sebagai pembanding dan menganalisa file-file menurut aturan-aturan yang ada.
- Mengidentifikasi kecenderungan/gejala-gejala, dapat juga menunjukan dengan tepat sasaran pengecualian data dan menyoroti potensial area yang menjadi perhatian.
- Mengidentifikasi proses perhitungan kembali dan proses verifikasi yang benar.
- Mengidentifkasi persoalan sistem pengawasan dan memastikan terpenuhinya permohonan dengan aturan-aturan yang telah ditetapkan.
- Menganalisa account receivable/payable atau beberapa transaksi lain dengan menggunakan basis waktu yang sensitive.

Adapun 5 Siklus data ACL :

- **Perencanaan**, Rencanakan pekerjaan anda sebelum memulai sebuah project. Dengan merumuskan jelas tujuanya sebelum mulai analisis, dengan mengembangkan strategi dan waktu serta sumber daya.

- **Akses Data**, Langkah berikutnya adalah mengakses data yang digariskan dalam rencana strategis. Dengan mencari, meminta, dan mentransfer data sebelumnya untuk membacanya dengan ACL.
- Integritas data Verifikasi Data, Setelah menerima data, maka diperlukan untuk menguji integritas. Jika anda memulai project anda tanpa harus diverifikasi terlebih dahulu data yang integritas, ada kemungkinan tidak lengkap atau tidak benar.
- Analisis Data , dalam analisis tahap melakukan tes yang diperlukan untuk mencapai tujuan. Anda mungkin akan menggunakan kombinasi perintah, filter, dan hitungan dalam analisis Anda.
- Pelaporan Hasil, tergantung pada proyek tersebut, Anda mungkin perlu membuat laporan dari yang dihasilkan. ACL dapat membuat berbagai jenis laporan, termasuk multiline, detail, dan ringkasan laporan

Unsur-Unsur Data dalam Analisis ACL :

- Commands, Command pada ACL merupakan perintah analisis standar yang ada pada ACL seperti perintah statistik. Stratify (menstratifikasi), Aging (umur) dsb. Perintah tersebut dapat menghasilkan output dalam bentuk file, screen(layar), print dan grafik.
- Expressions (Ekspresi), Expressions adalah pernyataan yang digunakan terutama untuk membuat filter dan computed fields. Melakukan perhitungan, menentukan kondisi logis, atau menciptakan nilai-nilai yang tidak ada pada data file. Expressions dapat diberi nama dan disimpan sebagai bagian dari suatu proyek atau digunakan langsung.
    - Filter adalah ekspresi logika yang memungkinkan Anda memilih jenis data yang Anda ingin lihat. Sebagai contoh, Anda dapat membuat Filter yang memilih hanya records yang berada dalam rentang tanggal tertentu.

- Computed Fields adalah dikenal juga sebagai calculated field, adalah virtual field yang menggunakan data yang berasal dari ekspresi atau variabel tertentu. Ini tidak berisi data fisik. Sebagai contoh, Anda dapat membuat sebuah field baru yang merupakan hasil dari nilai-nilai di dua field lainnya. Anda juga dapat menyisipkan ke dalam tabel nilai tertentu seperti suku bunga atau kondisi logis..

- Function, Function adalah sesuatu yang pasti yang sudah ada dalam function di ACL dengan menggunakan variabel, untuk melaksanakan suatu perhitungan atau perintah atas data yang telah ditetapkan.
- Variable, adapun variabelnya adalah :
  - Interface ACL, Pada saat pertama membuka ACL, anda akan dihadapkan layar seperti dibawah ini, dengan tampilan Welcome Tab, Project Navigator, dan Status Bar.
  - Welcome Tab, merupakan tampilan yang menunjukan macam-macam project yang pernah dibuat dan disimpan di ACL. Karena sistem ACL sudah menggunakan sistem seperti di website, jadi anda tinggal mengklik untuk memilihnya.
  - Project Navigator, merupakan tampilan dimana Tabel dan Log sedang dalam pengerjaan dalam suatu project di ACL.
  - Status Bar, Tampilan Status Bar menunjukan informasi tentang tabel yang sedang dibuka, termasuk nama tabel tersebut, number record, dan tampilan filter jika sedang diaktifkan.

Judul Tugas	IT audit Tools/ SEO Audit Tools
MK	IT Audit
Mahasiswa	M. Riski Qisthiano (182420040)
Tanggal	21-11-2019

Software Audit	ACL (audit command language,ACL Service Ltd)
Fungsi Software	ACL (*Audit Command Language*) adalah sebuah software CAAT (*Computer Assisted Audit Techniques*) untuk melakukan analisa terhadap data dari berbagai macam sumber. ACL for Windows (sering disebut ACL) yaitu sebuah software TABK (Teknik Audit Berbasis Komputer) untuk membantu auditor dalam melakukan pemeriksaan di lingkungan sistem informasi berbasis komputer atau Pemrosesan Data Elektronik.

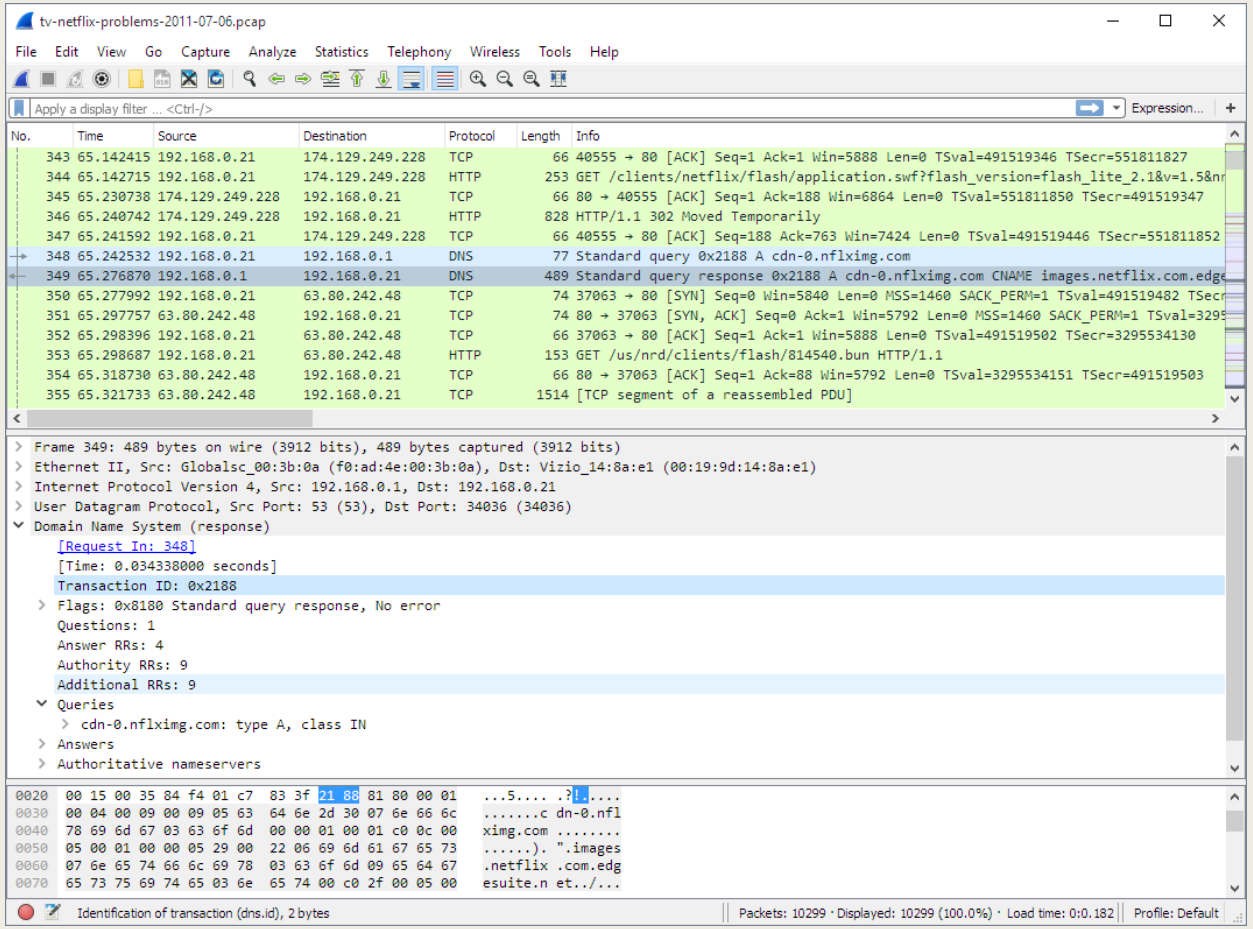
SOFTWARE IT AUDIT TOOLS

WIRESHARK

Disusun Oleh:

1. Muhammad Irvai
2. Muhammad Diah Maulidin
3. Nurhachita
4. Sahirillah

Pengertian Wireshark



- Wireshark adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis.

Pengertian Wireshark

- Wireshark adalah sebuah program analisa paket jaringan yang akan mencoba untuk menangkap paket jaringan dan mencoba untuk menampilkan data paket sedetail mungkin. Sehingga dapat melogikakan atau memikirkan sebuah packet analyzer jaringan sebagai alat ukur yang digunakan untuk memeriksa apa yang terjadi di dalam kabel jaringan
- Wireshark mampu menangkap dan paket-paket data/informasi yang ada di dalam jaringan, sehingga data tersebut dapat kita analisa untuk berbagai keperluan, diantaranya:
  - *Troubleshooting masalah di jaringan*
  - *Memeriksa keamanan jaringan*
  - *Sniffer data-data privasi di jaringan*

Tujuan Penggunaan Wireshark

- Beberapa tujuan penggunaan wireshark, yaitu:
  - *administrator jaringan menggunakannya untuk memecahkan masalah jaringan*
  - *insinyur keamanan jaringan menggunakannya untuk memeriksa masalah keamanan*
  - *pengembang menggunakannya untuk men-debug implementasi protocol*
  - *beberapa orang menggunakannya untuk mempelajari protokol jaringan internal*

Tujuan Penggunaan Wireshark

- Wireshark dapat membaca:

- Ethernet
- Token-Ring
- Serial(PPP dan SLIP)
- 802.11 wireless LAN
- Koneksi ATM
- Mengetahui IP chatter(seseorang)
- Proses transmisi dan
- Transmisi data antar komputer

Contoh Penggunaan Wireshark

- Contoh penggunaan WireShark:
  - *Admin sebuah jaringan menggunakannya untuk troubleshooting masalah-masalah di jaringan.*
  - *Teknisi keamanan jaringan menggunakan untuk memeriksa keamanan jaringan.*
  - *Pengembang software biasa menggunakan untuk men-debug implementasi protokol jaringan dalam software.*
  - *Banyak orang menggunakan Wireshark untuk mempelajari protokol jaringan secara lebih terperinci.*
  - *Selain itu digunakan sebagai sniffer atau pencari/pendeteksi data-data privasi jaringan.*

Fitur dan Kelebihan Penggunaan Wireshark

- Fitur dan kelebihan WireShark:
  - *Tersedia untuk Linux dan Windows.*
  - *Menangkap paket data secara langsung dari sebuah network interface.*
  - *Mampu menampilkan informasi yang sangat terperinci mengenai hasil tangkapan tersebut.*
  - *Dapat melakukan import dan export hasil tangkapan dari atau ke komputer lain.*
  - *Pencarian paket menggunakan berbagai macam kriteria filter/pemilahan.*
  - *Dapat membuat berbagai macam tampilan statistika*

Kesimpulan

Wireshark adalah tool open source terkemuka yang banyak di gunakan untuk melakukan analisis dan pemecah masalah jaringan, Memungkinkan untuk mengetahui masalah di jaringan. Pengembangan Wireshark berkembang berkat kontribusi relawan ahli jaringan di seluruh dunia. Wireshark di buat dengan bahasa C, C+.

Referensi Wireshark

- http://wireshark.org
- https://seruni.id/cara-menggunakan-wireshark/
- https://medium.com/@kitaadmin/wireshark-adalah-pengertian-dan-fungsi-256dc09c8292
- http://elektro.um.ac.id/wp-content/uploads/2016/05/Modul-Praktikum-3-Analisa-Jaringan-Menggunakan-WireShark.pdf

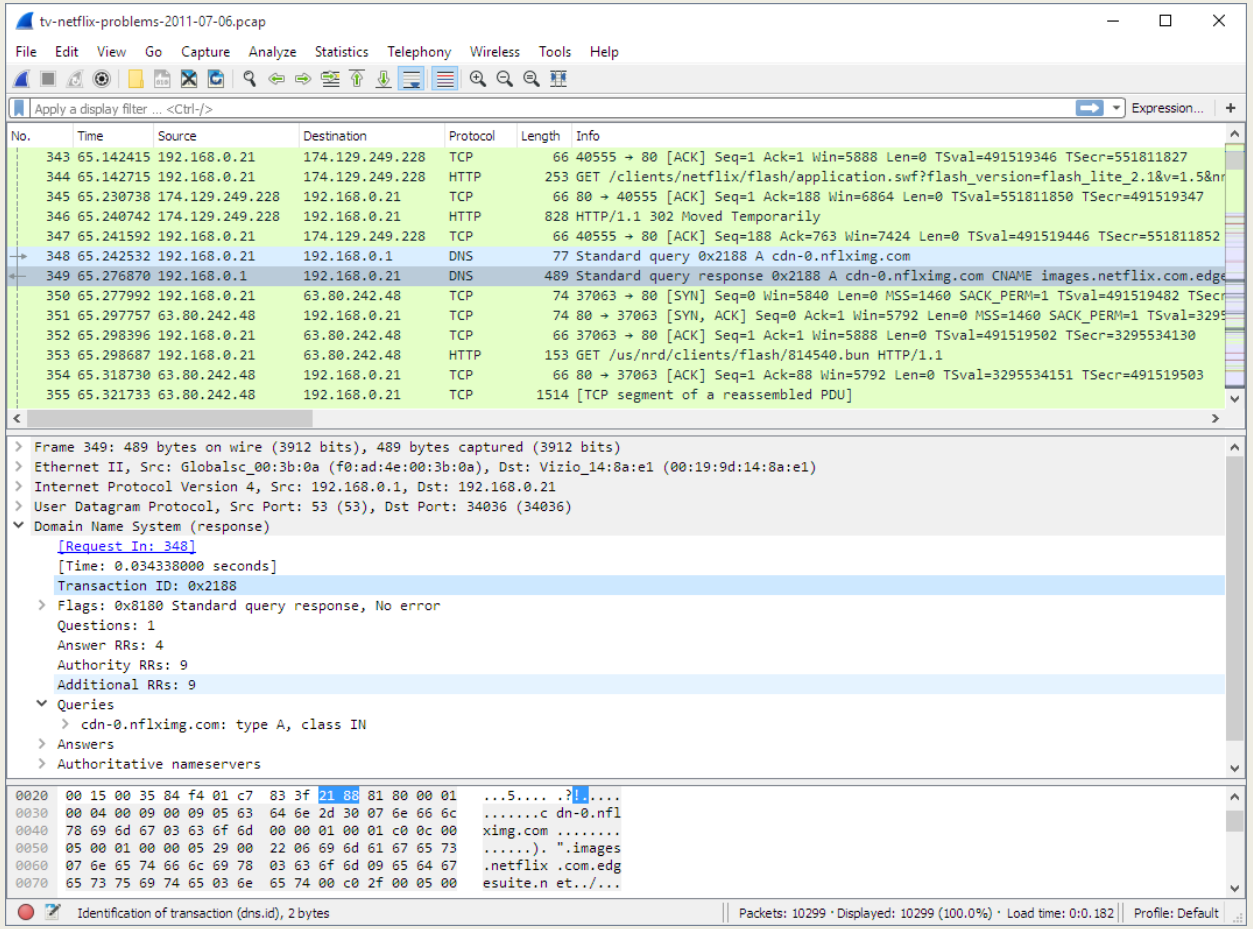
SOFTWARE IT AUDIT TOOLS

WIRESHARK

Disusun Oleh:

1. Muhammad Irvai
2. Muhammad Diah Maulidin
3. Nurhachita
4. Sahirillah

Pengertian Wireshark



- Wireshark adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis.

Pengertian Wireshark

- Wireshark adalah sebuah program analisa paket jaringan yang akan mencoba untuk menangkap paket jaringan dan mencoba untuk menampilkan data paket sedetail mungkin. Sehingga dapat melogikakan atau memikirkan sebuah packet analyzer jaringan sebagai alat ukur yang digunakan untuk memeriksa apa yang terjadi di dalam kabel jaringan
- Wireshark mampu menangkap dan paket-paket data/informasi yang ada di dalam jaringan, sehingga data tersebut dapat kita analisa untuk berbagai keperluan, diantaranya:
  - *Troubleshooting masalah di jaringan*
  - *Memeriksa keamanan jaringan*
  - *Sniffer data-data privasi di jaringan*

Tujuan Penggunaan Wireshark

- Beberapa tujuan penggunaan wireshark, yaitu:
  - *administrator jaringan menggunakannya untuk memecahkan masalah jaringan*
  - *insinyur keamanan jaringan menggunakannya untuk memeriksa masalah keamanan*
  - *pengembang menggunakannya untuk men-debug implementasi protocol*
  - *beberapa orang menggunakannya untuk mempelajari protokol jaringan internal*

Tujuan Penggunaan Wireshark

- Wireshark dapat membaca:

- Ethernet
- Token-Ring
- Serial(PPP dan SLIP)
- 802.11 wireless LAN
- Koneksi ATM
- Mengetahui IP chatter(seseorang)
- Proses transmisi dan
- Transmisi data antar komputer

Contoh Penggunaan Wireshark

- Contoh penggunaan WireShark:
  - *Admin sebuah jaringan menggunakannya untuk troubleshooting masalah-masalah di jaringan.*
  - *Teknisi keamanan jaringan menggunakan untuk memeriksa keamanan jaringan.*
  - *Pengembang software biasa menggunakan untuk men-debug implementasi protokol jaringan dalam software.*
  - *Banyak orang menggunakan Wireshark untuk mempelajari protokol jaringan secara lebih terperinci.*
  - *Selain itu digunakan sebagai sniffer atau pencari/pendeteksi data-data privasi jaringan.*

Fitur dan Kelebihan Penggunaan Wireshark

- Fitur dan kelebihan WireShark:
  - *Tersedia untuk Linux dan Windows.*
  - *Menangkap paket data secara langsung dari sebuah network interface.*
  - *Mampu menampilkan informasi yang sangat terperinci mengenai hasil tangkapan tersebut.*
  - *Dapat melakukan import dan export hasil tangkapan dari atau ke komputer lain.*
  - *Pencarian paket menggunakan berbagai macam kriteria filter/pemilahan.*
  - *Dapat membuat berbagai macam tampilan statistika*

Kesimpulan

Wireshark adalah tool open source terkemuka yang banyak di gunakan untuk melakukan analisis dan pemecah masalah jaringan, Memungkinkan untuk mengetahui masalah di jaringan. Pengembangan Wireshark berkembang berkat kontribusi relawan ahli jaringan di seluruh dunia. Wireshark di buat dengan bahasa C, C+.

Referensi Wireshark

- http://wireshark.org
- https://seruni.id/cara-menggunakan-wireshark/
- https://medium.com/@kitaadmin/wireshark-adalah-pengertian-dan-fungsi-256dc09c8292
- http://elektro.um.ac.id/wp-content/uploads/2016/05/Modul-Praktikum-3-Analisa-Jaringan-Menggunakan-WireShark.pdf

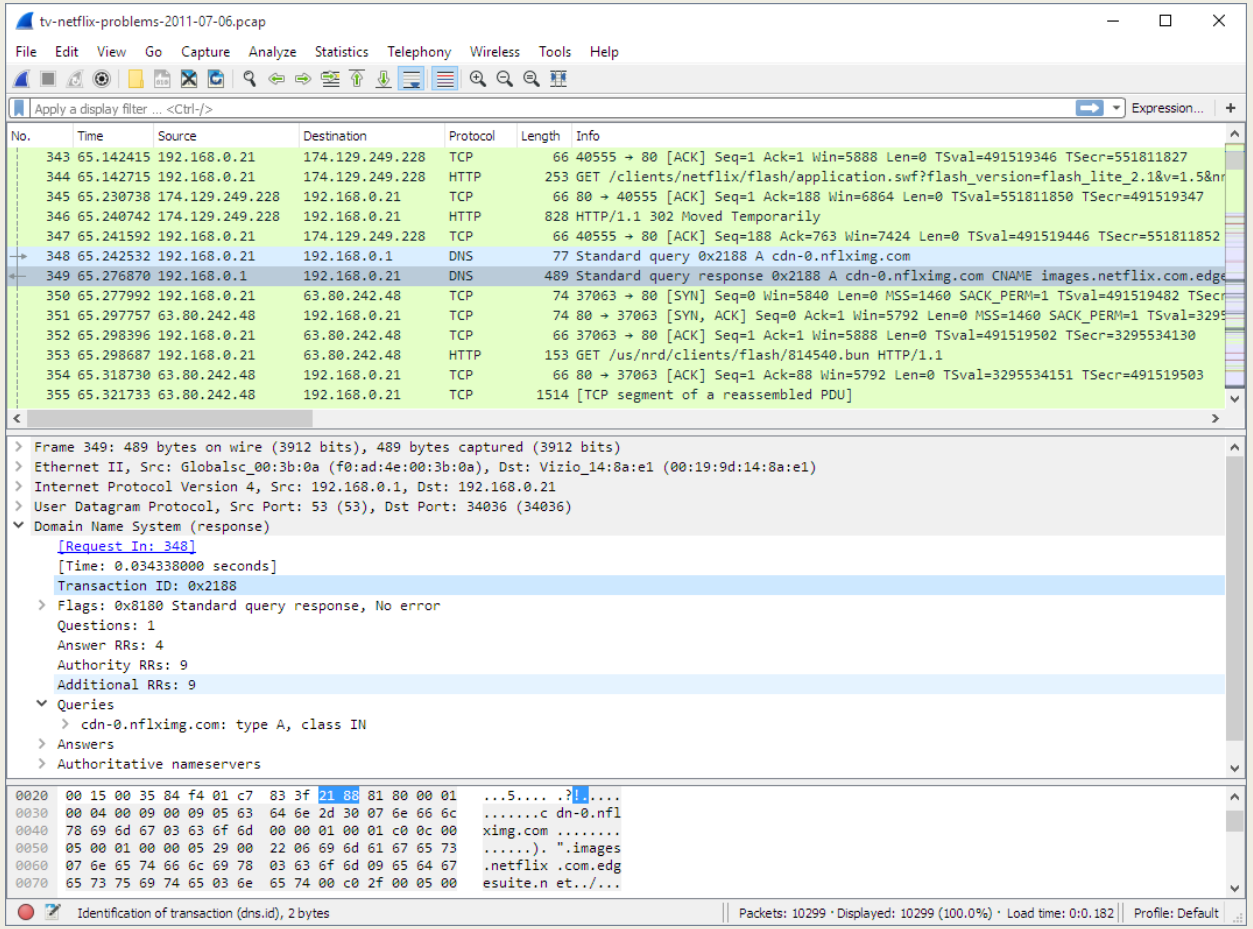
SOFTWARE IT AUDIT TOOLS

WIRESHARK

Disusun Oleh:

1. Muhammad Irvai
2. Muhammad Diah Maulidin
3. Nurhachita
4. Sahirillah

Pengertian Wireshark



- Wireshark adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis.

Pengertian Wireshark

- Wireshark adalah sebuah program analisa paket jaringan yang akan mencoba untuk menangkap paket jaringan dan mencoba untuk menampilkan data paket sedetail mungkin. Sehingga dapat melogikakan atau memikirkan sebuah packet analyzer jaringan sebagai alat ukur yang digunakan untuk memeriksa apa yang terjadi di dalam kabel jaringan
- Wireshark mampu menangkap dan paket-paket data/informasi yang ada di dalam jaringan, sehingga data tersebut dapat kita analisa untuk berbagai keperluan, diantaranya:
  - *Troubleshooting masalah di jaringan*
  - *Memeriksa keamanan jaringan*
  - *Sniffer data-data privasi di jaringan*

Tujuan Penggunaan Wireshark

- Beberapa tujuan penggunaan wireshark, yaitu:
  - *administrator jaringan menggunakannya untuk memecahkan masalah jaringan*
  - *insinyur keamanan jaringan menggunakannya untuk memeriksa masalah keamanan*
  - *pengembang menggunakannya untuk men-debug implementasi protocol*
  - *beberapa orang menggunakannya untuk mempelajari protokol jaringan internal*

Tujuan Penggunaan Wireshark

- Wireshark dapat membaca:

- Ethernet
- Token-Ring
- Serial(PPP dan SLIP)
- 802.11 wireless LAN
- Koneksi ATM
- Mengetahui IP chatter(seseorang)
- Proses transmisi dan
- Transmisi data antar komputer

Contoh Penggunaan Wireshark

- Contoh penggunaan WireShark:
  - *Admin sebuah jaringan menggunakannya untuk troubleshooting masalah-masalah di jaringan.*
  - *Teknisi keamanan jaringan menggunakan untuk memeriksa keamanan jaringan.*
  - *Pengembang software biasa menggunakan untuk men-debug implementasi protokol jaringan dalam software.*
  - *Banyak orang menggunakan Wireshark untuk mempelajari protokol jaringan secara lebih terperinci.*
  - *Selain itu digunakan sebagai sniffer atau pencari/pendeteksi data-data privasi jaringan.*

Fitur dan Kelebihan Penggunaan Wireshark

- Fitur dan kelebihan WireShark:
  - *Tersedia untuk Linux dan Windows.*
  - *Menangkap paket data secara langsung dari sebuah network interface.*
  - *Mampu menampilkan informasi yang sangat terperinci mengenai hasil tangkapan tersebut.*
  - *Dapat melakukan import dan export hasil tangkapan dari atau ke komputer lain.*
  - *Pencarian paket menggunakan berbagai macam kriteria filter/pemilahan.*
  - *Dapat membuat berbagai macam tampilan statistika*

Kesimpulan

Wireshark adalah tool open source terkemuka yang banyak di gunakan untuk melakukan analisis dan pemecah masalah jaringan, Memungkinkan untuk mengetahui masalah di jaringan. Pengembangan Wireshark berkembang berkat kontribusi relawan ahli jaringan di seluruh dunia. Wireshark di buat dengan bahasa C, C+.

Referensi Wireshark

- http://wireshark.org
- https://seruni.id/cara-menggunakan-wireshark/
- https://medium.com/@kitaadmin/wireshark-adalah-pengertian-dan-fungsi-256dc09c8292
- http://elektro.um.ac.id/wp-content/uploads/2016/05/Modul-Praktikum-3-Analisa-Jaringan-Menggunakan-WireShark.pdf

REVIEW ACL (AUDIT COMMAND LANGUAGE)

Pengertian ACL

- ACL for Windows (sering disebut ACL) adalah sebuah program untuk membantu akuntan dalam melakukan pemeriksaan di lingkungan sistem informasi berbasis komputer atau Pemrosesan Data Elektronik. ACL secara khusus dirancang untuk menganalisa data, memanipulasi data dan mengekspor data sehingga membuatnya menjadi lebih berguna bagi auditor.
- ACL adalah sebuah software yang dirancang secara khusus untuk menganalisa data dan menghasilkan laporan audit baik untuk pengguna biasa (common/ nontechnical users) maupun pengguna ahli (expert users)
- ACL dapat mengerjakan berbagai tipe format data. Data yang dihasilkan oleh komputer, disimpan dalam karakter-karakter yang disebut byte. ACL dapat membaca data dari berbagai macam sistem yang terbentang mulai dari model sistem mainframe lama hingga ke relational database modern.
- ACL adalah aplikasi yang hanya 'read-only', ACL tidak pernah mengubah data sumber asli sehingga aman untuk menganalisis jenis live-data. Keanekaragaman sumber data dan teknologi akses data, cara mengakses data juga bervariasi dari satu sumber data ke lain. ACL membaca beberapa sumber data secara langsung dengan mengimport dan menyalin sumber data sehingga dapat dianalisis. Banyak jenis data modern saat ini berisi berisi informasi tentang layout record, seperti jumlah record, nama field, panjang field dan tipe data tiap field. Ketika semua informasi ini ada dalam sumber data, atau dalam suatu file definisi eksternal yang terkait, ACL memperoleh ini informasi secara otomatis. Jika informasi tidak menyajikan, maka harus mengacu pada suatu dokumen seperti layout record atau suatu kamus data dan mendefinisikan menggunakan ACL dengan manual.

Paling tidak ada 2 jenis yang utama dalam pengkodean dalam komputer, yaitu:

1. EBCDIC (Extended Binary Coded Decimal Interchang Code) – format ini seringkali ditemukan pada komputer jenis IBM Mainframe.

2. ASCII (American Standard Code for Information Interchange) – format ini hampir digunakan dibanyak komputer. ACL dapat membaca langsung baik jenis EBCDIC atau ASCII, sehingga tidak perlu untuk menngkonversi kedalam bentuk lain.

Perusahaan ACL

- ACL adalah salah satu jenis audit software yang termasuk dalam kategori Genaralized Audit Software (GAS). Seperti halnya aplikasi GAS yang lainnya, ACL hanya dapat digunakan untuk mengumpulkan dan mengevaluasi bukti yang dihasilkan dari pemrosesan transaksi perusahaan sehingga ACL lebih cenderung digunakan untuk menilai post transactions daripada current transaction. Setelah mengulang apa itu ACL sekarang kita belajar tentang bagaiana sejarah dari ACL ini.
- Prof Hart J. Will yang mengembangkan aplikasi ACL ini. Dikembangkannya ACL ini dimulai pada tahun 1970-an. Hart tidak sendiri mengembangkan aplikasi ini. Dia mengembangkan ACL ini melalui perusahaan yang bernama ACL Services Ltd yang ada di Kanada. Perusahaan ini sebenarnya khusus membuat aplikasi-aplikasi komputer. Sehingga kegiatan utamanya adalah membuat dan menjual aplikasi analisis data, aplikasi tata kelola, aplikasi manajemen resiko dan aplikasi kepatuhan.
- Harmut (Hart) J. Will. adalah seorang Profesor Emeritus Akuntansi, Auditing dan Sistem Informasi manajemen di Sekolah Administrasi Publik di Victoria. Penemuan dia bernama ACL ini disebut-sebut sebagai evolusi pendekatan audit audit.
- Awal mula Hart mengembangkan ACL dimulai pada tahun 1960 ketika dia berada di Berlin yang sedang menyelesaikan tesisnya. ACL yang dia kembangkan itu selesai pada tahun 1968 ketika dia berada di Illinois. Awal mula sistem yang dia buat adalah kerangka Manajemen Sistem Informasi yang isisnya adalah Bank Data dan Bank Model. Selanjutnya dikembangkan sedemikian rupa sehingga jadilah aplikasi audit yang bernama ACL.

Fungsi ACL

- Bidang Auditor

  Pengguna ahli ini memiliki latar belakang yang memungkinkan dia menjadi seorang auditor sehingga ACL yang digunakannya bisa ditafsirkan dan digunakan untuk mempermudah pekerjaannya sebagai auditor. Manfaat ACL yang dapat dirasakan oleh seorang auditor dalam penggunaan ACL ini adalah ACL bisa membantu auditor dalam melaksanakan tugasnya yaitu mengaudit laporan keuangan perusahaan secara

fokus, cepat, efisien dan akurat. Karena teknologi pada intinya dibuat untuk mempermudah pekerjaan manusia, untuk mengurangi kesalahan yang bisa terjadi dan untuk mempercepat pekerjaan.

- Bidang Manajemen

  Dalam suatu peruahaan ada bagian keuangannya, bagian keuangan inilah yang dimaksudnya manajemen. Bagian keuangan bisa melakukan analisis suatu data perusahaan menggunakan ACL untuk tujuan tertentu seperti melakukan analisis terhadap penjualan, bagaimana trending penjualan dan lain sebagainya. Selain digunakan manajemen untuk melakukan analisis data ACL juga bisa dilakukan untuk pengujian pengendalian perusahaan. Kalau sudah masuk kedalam pengendalian internal ini menyangkut auditing. Pengendalian internal sangat diperlukan untuk mengetahui apakah kemungkinan perusahaan melakukan kecurangan tinggi atau tidak. Penjelasan lebih dalam tentang pengendalian internal akan dibahas dalam auditing. ACL juga bisa digunakan manajemen dalam pembuatan laporan yang diinginkan. Manajemen dapat menggunakan ACL untuk :

  1. Analisis data
  2. Pengujian pengendalian perusahaan
  3. Pembuatan laporan keuangan yang diinginkan

Fitur dan kemampuan ACL Software Tools :

1. ***Universal Data Access***, yaitu dapat mengakses data dari hampir semua jenis ***database*** yang ada (DBF, XLS, Text File, report file, Oracle, SQL, DB2, AS/400 FDF, COBOL, dsb) dan semua ***platform*** (PC, ***minicomputer***, dan ***mainframe***).
2. Jumlah Data Besar, yaitu kemampuan dalam mengakses dan memproses data dalam jumlah yang sangat besar (hingga ratusan juta ***record***).
3. Kecepatan Waktu Proses, kemampuannya untuk memproses dalam waktu yang singkat walaupun data yang diproses dalam jumlah yang besar.
4. Integritas Data, dengan kemampuan mengakses database 100% (tanpa metode ***sampling***) serta data yang bersifat ***Read Only*** yang dapat menjamin orisinalitas, keamanan dan integritas data untuk pengolahan menjadi informasi yang bermanfaat bagi ***user*** dan manajemen.
5. Automasi, pembuatan aplikasi audit yang sangat cepat dan mudah untuk melakukan automasi analisis data untuk efisiensi proses kerja.

6. ***Multi File Process***, dapat digunakan untuk menangani beberapa file sekaligus, tanpa mengganggu operasional teknologi informasi yang dijalankan oleh perusahaan.
7. ***Log File Navigation***, dilengkapi dengan ***log file*** untuk pencatatan proses analisis yang telah dilakukan sehingga menghasilkan suatu ***audit trail*** yang komprehensif.
8. Fungsi Analisis yang Lengkap, dilengkapi fungsi-fungsi analisis yang sangat lengkap yang dapat dengan mudah dikombinasikan dalam menghasilkan temuan-temuan yang tidak pernah terkirakan sebelumnya.
9. Pelaporan yang Handal, kemudahan untuk merancang laporan yang handal sarat informasi yang bermanfaat serta dapat dikirimkan secara otomatis via email atau integrasi ke dalam ***software*** aplikasi Crystal Report.
10. IT Audit, kemudahan dalam menguji integritas data dan menganalisis data yang ada di dalam ***database*** ataupun menganalisis ***user-user*** yang telah masuk ke dalam suatu jaringan/***network***.

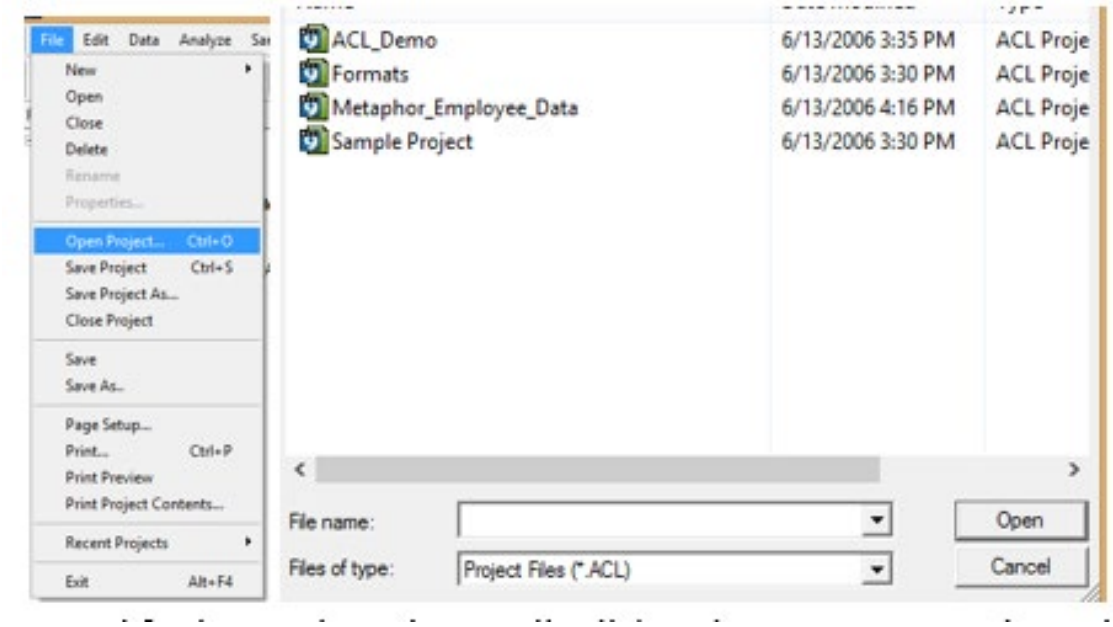
Manfaat menggunakan ACL Software Tools :

- Dapat membantu dalam mengAkses data baik langsung (***Direct***) kedalam system jaringan ataupun tidak langsung (***InDirec***t) melalui media lain seperti ***softcopy*** dalam bentuk ***teks file/report***.
- Menempatkan kesalahan dan potensial ***fraud*** sebagai pembanding dan menganalisa ***file-file*** menurut aturan-aturan yang ada.
- Mengidentifikasi kecenderungan/gejala-gejala, dapat juga menunjukan dengan tepat/sasaran pengecualian data dan menyoroti potensial area yang menjadi perhatian.
- Mengidentifikasi proses perhitungan kembali dan proses verifikasi yang benar.
- Mengidentifikasi persoalan sistem pengawasan dan memastikan terpenuhinya permohonan dengan aturan-aturan yang telah ditetapkan.
- ***Aging*** dan menganalisa ***Account Receivable/Payable*** atau beberapa transaksi lain dengan menggunakan basis waktu yang sensitif.
- Memulihkan biaya atau pendapatan yang hilang dengan pengujian data pada data-data duplikasi pembayaran, menguji data-data nomor ***Invoice***/Faktur yang hilang atau pelayanan yang tidak tertagih.
- Menguji terhadap hubungan antara authorisasi karyawan dengan ***supplier***.
- Melakukan proses ***Data Cleansing*** dan ***Data Matching*** atau pembersihan data dari data-data duplikasi terutama dari kesalahan pengetikan oleh ***End-User***.

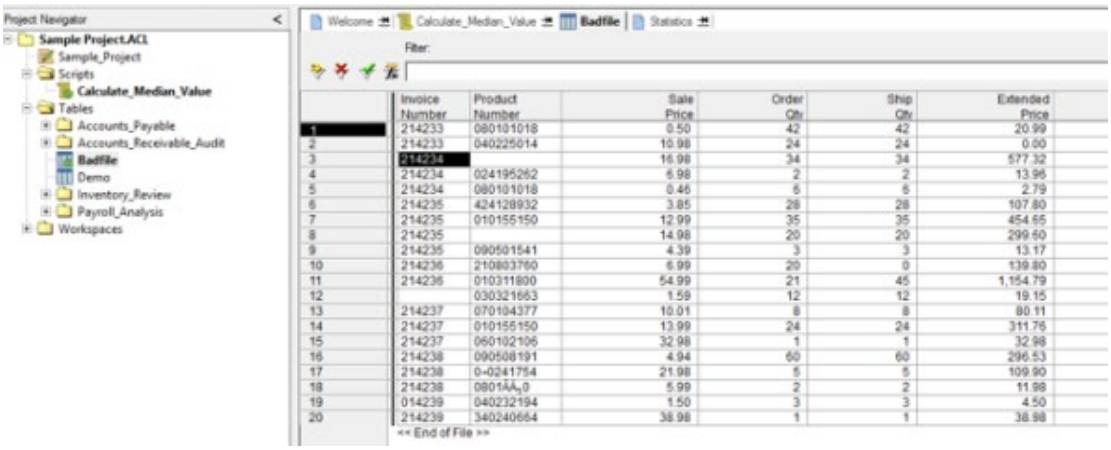
- Dapat melaksanakan tugas pengawasan dan pemeriksaaan dengan lebih fokus, cepat, efisien, dan efektif dengan lingkup yang lebih luas dan analisa lebih mendalam. Mengidentifikasi penyimpangan (***Fraud Detection***) dapat dilakukan dengan cepat dan akurat sehingga memiliki waktu lebih banyak alam menganalisa data dan pembuktian.

- **Review Software ACL 9**

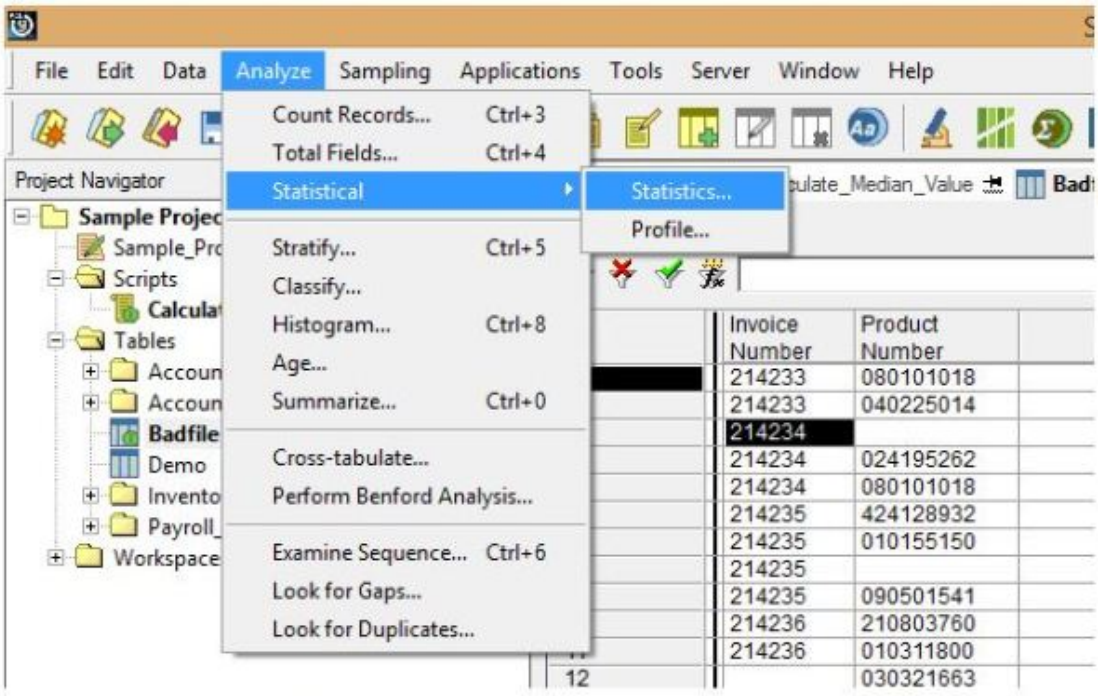
  Contoh menggunakan acl pada versi acl 9 untuk melihat data berupa statistika



  Pada software acl 9 ada sample project yg disediakan, langsung open project saja dan pilih Sample Project.acl

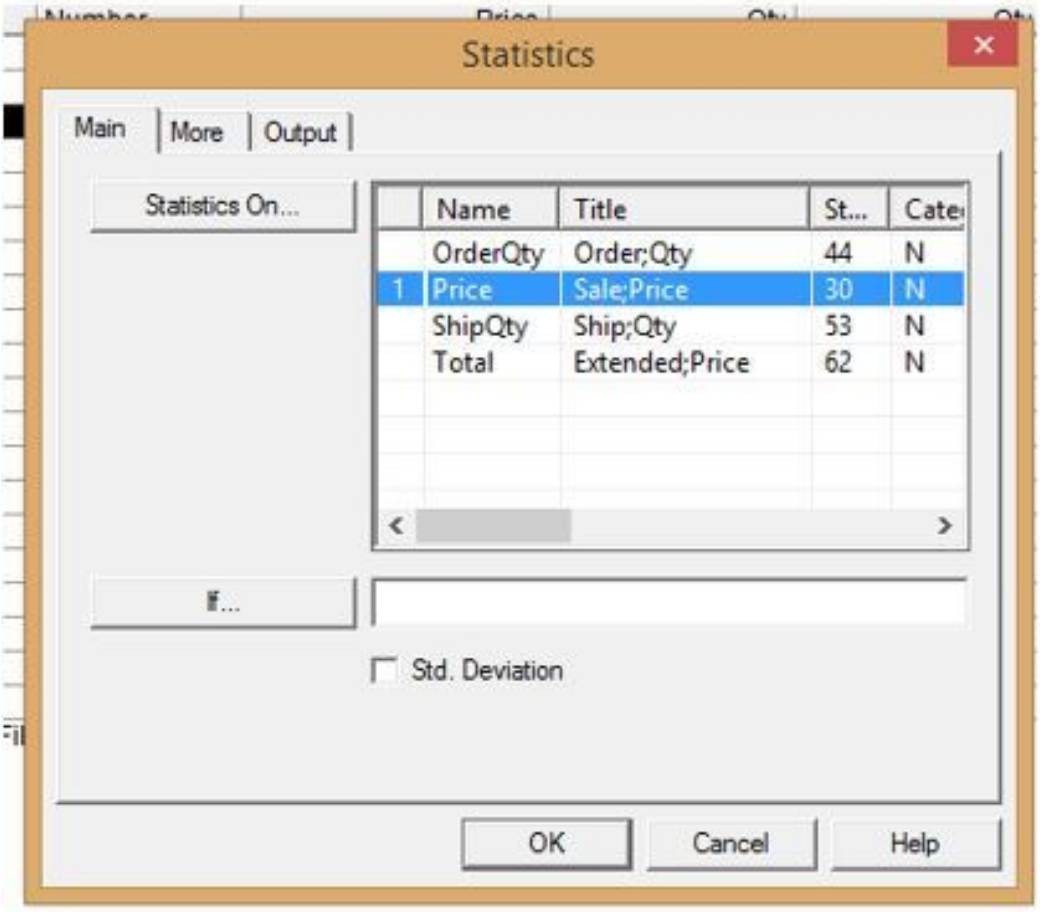


Pada software ACL setelah open sample project, akan menampilkan data berikut pada file BadFile

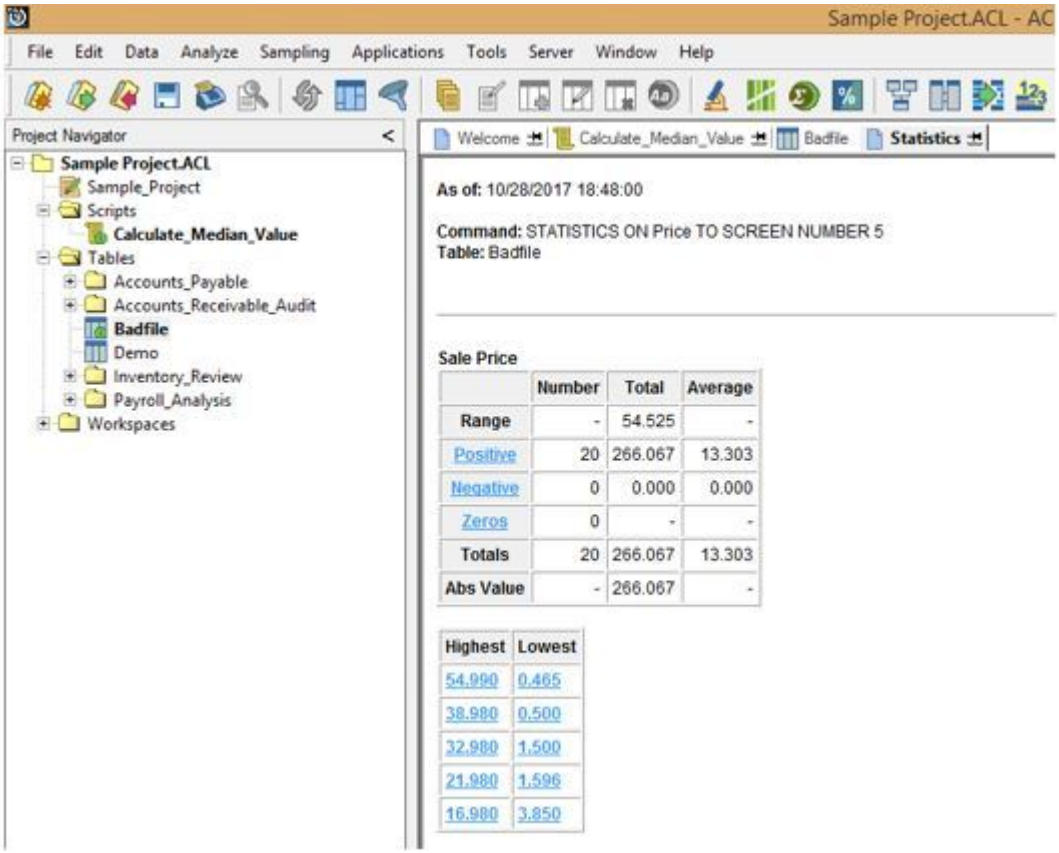


pilih menu Analyze dan pilih Statistical > Statistics...

pilih menu Analyze dan pilih Statistical > Statistics…



Pilih baris yang akan ditampilkan statistiknya, lalu klik OK



Hasil statistika bisa terlihat disini sehingga memudahkan untuk mengaudit dan menganalisa data.