

FORENSIK DIGITAL
RANGKUMAN MATERI NETWORK FORENSIK DARI
BUKU COMPUTER HACKING FORENSIK INVESTIGATOR
BY EC-COUNCIL



NI KADEK AYU SITA CHRISTINA DEWI
1715051079

PROGRAM STUDI PENDIDIKAN TEKNIK INFORMATIKA
JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KEJURUAN
UNIVERSITAS PENDIDIKAN GANESHA
2020

Network Forensics

Module 7

Network forensics memastikan bahwa semua aliran data jaringan langsung terlihat, memungkinkan monitor untuk melihat penyalahgunaan orang dalam dan ancaman lanjutan. Forensik jaringan meliputi penyitaan dan analisis peristiwa jaringan untuk mengidentifikasi sumber serangan keamanan atau insiden masalah lainnya dengan menyelidiki file log.

Skenario

Jessica hilang dari rumahnya selama seminggu. Dia meninggalkan pesan karena ayahnya menyebutkan bahwa dia akan bertemu sekolahnya teman. Beberapa minggu kemudian mayat Jessica ditemukan di dekat a halaman pembuangan. Penyelidik dipanggil untuk menyelidiki kematian Jessica. Sebuah investigasi awal komputer dan log Jessica terungkap beberapa fakta yang membantu polisi melacak si pembunuh.

Network forensics adalah menangkap, merekam, dan menganalisis peristiwa jaringan untuk menemukan sumber insiden keamanan. Ada banyak alat analisis otomatis untuk keperluan forensik, tetapi tidak mencukupi, karena tidak ada metode mudah untuk mengenali lalu lintas palsu yang dihasilkan oleh penyerang dari kumpulan asli lalu lintas. Jaringan forensik diperlukan untuk menentukan jenis serangan terhadap jaringan dan lacak pelakunya.

Pemeriksaan forensik log memiliki dua kategori:

Postmortem

Penyelidik melakukan postmortem log untuk mendeteksi sesuatu yang sudah terjadi di jaringan / perangkat dan tentukan apa itu. seorang penyelidik dapat memeriksa file log beberapa kali. Bila dibandingkan dengan analisis real-time, itu adalah proses yang melelahkan, karena para penyelidik perlu memeriksa serangan itu secara rinci dan memberikan laporan akhir.

Analisis Real-Time

Analisis Real-Time adalah analisis yang dilakukan untuk proses yang sedang berlangsung. Analisis ini akan lebih banyak efektif jika penyelidik / administrator mendeteksi serangan dengan cepat.

Network Vulnerabilities (kerentanan network)

Kemajuan teknologi menyebabkan peningkatan pesat di Internet kompleksitas dan Network Vulnerabilities. Ada berbagai faktor internal dan eksternal yang membuat jaringan rentan.

Internal Network Vulnerabilities

Terjadi karena kelebihan bandwidth dan kemacetan.

- **Overextension of bandwidth:** Overextension of bandwidth terjadi ketika pengguna membutuhkan melebihi total sumber daya.
- **Kemacetan:** Kemacetan biasanya terjadi ketika pengguna perlu melebihi sumber daya khususnya sektor jaringan.

Sistem manajemen jaringan mengarahkan masalah dan perangkat lunak ini ke log atau solusi manajemen lainnya.

External Network Vulnerabilities

Terjadi karena ancaman seperti serangan DoS / DDOS dan jaringan intersepsi data.

Serangan Dos dan DDOS dihasilkan dari satu atau beberapa serangan. Serangan-serangan ini bertanggung jawab atas memperlambat atau menonaktifkan jaringan dan dianggap sebagai salah satu ancaman paling serius yang dihadapi jaringan.

Intersepsi data adalah kerentanan umum di antara LAN dan WLAN. Dalam jenis serangan ini, sebuah penyerang menyusup ke sesi aman dan dengan demikian memonitor atau mengedit data jaringan untuk mengakses atau edit operasi jaringan

Serangan umum yang biasanya terjadi pada jaringan:

A. Eavesdropping

Teknik untuk menghalau koneksi yang tidak aman dengan tujuan untuk mencuri informasi pribadi.

B. Data Modification

Begitu hacker mendapatkan akses ke informasi yang sensitif, langkah pertama yang dilakukan hacker adalah mengubah data tersebut.

C. IP Address Spoofing

Teknik yang digunakan untuk mendapatkan akses ke komputer secara tidak sah.

D. Denial of Service (DoS)

Hacker membanjiri target dengan traffic yang tidak valid, dengan demikian menyebabkan habisnya sumber daya yang tersedia pada target.

E. Man-In-The-Middle-Attack

Hacker membuat koneksi independen dengan korban dan menyampaikan pesan diantara mereka, serta membuat korban percaya bahwa percakapan yang terjadi adalah secara langsung.

F. Packet Sniffing

Tujuan untuk mendapatkan informasi sensitive seperti nama pengguna, kata sandi untuk tujuan tidak baik. Pada jaringan komputer, sniffing paket melacak paket jaringan. Perangkat lunak seperti Cain&Able digunakan untuk tujuan ini.

G. Enumeration

proses untuk mendapatkan informasi mengenai jaringan yang nantinya akan memudahkan untuk menyerang jaringan tersebut. Informasi yang didapatkan diantaranya:

- Topologi jaringan
- Daftar host yang hidup
- Architecture dan jenis traffic (seperti TCP, UDP, IPX)
- Potensi kerentanan dalam system host

H. Session Hijacking

Mengeksploitasi generasi mekanisme sesi token atau kontrol keamanan token dengan tujuan hacker dapat menciptakan koneksi tanpa izin kepada server target.

I. Buffer Overflow

Buffer memiliki kapasitas data. Jika data dihitung melebihi kapasitas sebenarnya dari buffer, maka buffer overflow akan muncul. Untuk mempertahankan perlu untuk menambah atau mengembangkan kapasitas data. Informasi tambahan mungkin akan merambat ke buffer sebelah sehingga akan menghancurkan atau menimpa data legal

J. Email Infection

Serangan ini menggunakan email sebagai media untuk menyerang sebuah jaringan. Membanjiri network dengan email spam dan lainnya adalah cara untuk menyerang jaringan yang akan menyebabkan serangan DoS.

K. Malware Attack

Malware adalah perangkat lunak yang diciptakan untuk menyerang system. Hacker akan memasasng pada computer target, dan malware akan merusak sitstem target

L. Password-based Attack

Serangan ini adalah serangan dimana hacker akan memberikan akses masuk sistem atau aplikasi untuk menduplikasi data masuk yang valid dan mendapatkan akses untuk masuk.

M. Riuter Attacks

Ini adalah tipe serangan dimana hacker mencoba berkompromi dengan router dan mendapatkan akses masuknya.

Serangan Khusus Untuk Jaringan Wireless :

A. Rogue acces Point attack

Hacker atau orang dalam membuat pintu belakang ke jaringan terpercaya dengan memasang titik akses tanpa jaminan di dalam firewall. Dan menggunakan access point untuk menyerang.

B. Client-Mis-Association

Klien dapat terhubung dengan AP di luar jaringan yang sah baik secara sengaja atau tidak sengaja. Hacker yang dapat terhubung pada jaringan tersebut secara sengaja dan melanjutkan dengan aktivitas berbahaya dapat menyalahgunakan situasi ini.

C. Misconfigured Access Point Attack

Serangan ini terjadi pada tidak terkonfigurasinya titik akses jaringan. Ketika eksploitasi berhasil dilakukan, maka seluruh jaringan akan rentan dan terbuka untuk diserang oleh hacker, Salah satu tujuannys ialah untuk mendapatkan nama pengguna dan kata sandi sehingga memiliki akses masuk.

D. Unauthorized Association

Pada serangan ini, hacker mengambil keuntungan dari titik akses lunak, yakni radio WLAN yang dimiliki beberapa laptop.

E. Ad Hoc Connection Attack

Hacker melakukan serangan menggunakan adaptor USB atau kartu nirkabel. Dalam metode ini, host terhubung pada jaringan tidak aman untuk menyerang jaringan tertentu atau menghindari akses titik keamanan.

F. HoneySpot Access Point Attack

Jika beberapa WLAN dihidupkan berdampingan pada area yang sama, pengguna dapat terhubung pada jaringan yang tersedia. Hacker mengambil keuntungan perilaku nirkabel klien dengan mengatur jaringan nirkabel yang tidak sah menggunakan AP. Aps yang dipasang oleh hacker adalah “honeypot” APs. Jika pengguna yang sah terhubung pada honeypot AP, itu menciptakan keamanan yang rentan dan akan menunjukkan informasi sensitif pengguna seperti identitas, nama pengguna, dan password pada hacker.

G. AP Mac Spoofing

Hacker dapat menkonfigurasi ulang alamat MAC sedemikian rupa sehingga dapat memunculkan akses resmi ke host dalam jaringan yang terpercaya. Alat yang digunakan untuk jenis serangan ini adalah changemas.sh, SMAC, dan Wicontrol.

H. Jamming Signal Attack

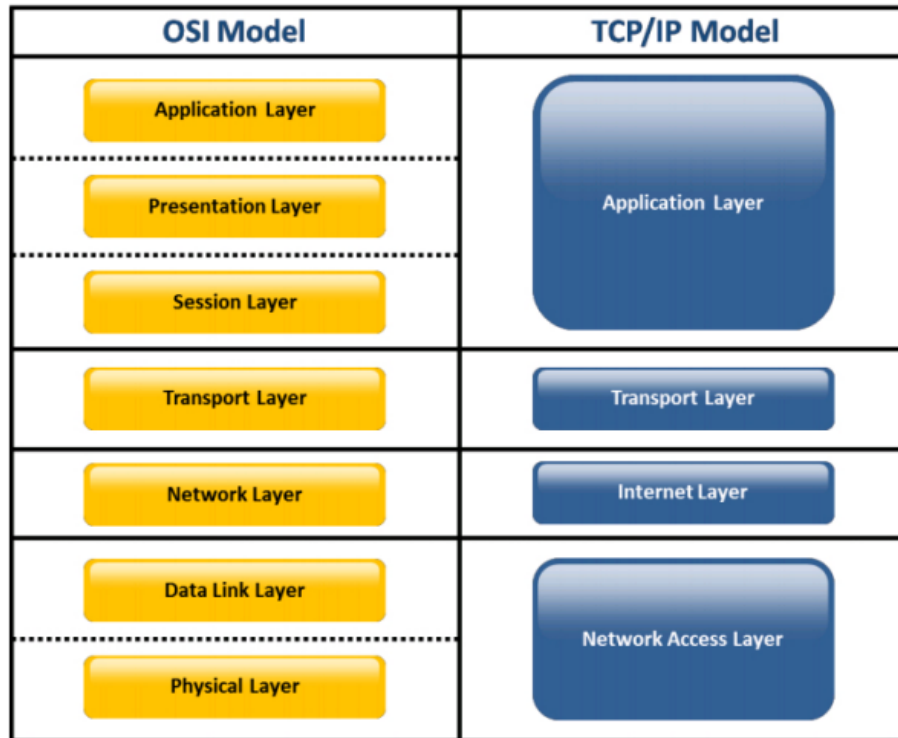
Pada serangan ini, hacker membuat macet sinyal WIFI untuk menghentikan semua traffic sah dari menggunakan titik akses. Hacker memblokir sinyal dengan mengirimkan traffic tidak sah dalam jumlah besar ke titik akses dengan menggunakan alat tertentu.

Where to Look for Evidence

Log berisi peristiwa yang terkait dengan segala aktivitas yang ditunjukkan oleh sistem atau jaringan. Log dikumpulkan di perangkat jaringan dan server aplikasi sebagai bukti bagi penyelidik untuk menginvestigasi hal-hal mengenai keamanan jaringan. Untuk itu analisis perlu memiliki pengetahuan model TCP/IP. Semua sistem yang mengirim dan menerima informasi memiliki program TCP/IP, dan TCP/IP program memiliki dua bagian yakni:

- **Higher Layer :** bagian ini mengelola informasi yang terkirim dan diterima dalam bentuk paket data berukuran kecil yang dikirim melalui internet dan bersatu dengan semua paket membentuk pesan utama.

- **Lower Layer** : bagian ini mengelola alamat dari setiap paket sehingga semua paket dapat mencapai tujuan yang benar.



Model TCP/IP dan model OSI tujuh bagian memiliki kesamaan dalam tampilan.

- **Layer 1 : Network Access Layer**

Bagian terendah dari model TCP/IP. Bagian ini menunjukkan bagaimana jaringan mentranfer data. Ini berisi protokol seperti Frame Relay, SMDS, Fast Ethernet, SLIP, PPP, FDDI, ATM, Ethernet, ARP, dan lainnya untuk membantu mesin mengirim data yang diinginkan kepada host lain dalam jaringan yang sama.

- **Layer 2 : Internet Layer**

Bagian ini mengelola pergerakan paket data dalam jaringan, dari sumber ke tujuan. Bagian ini berisi protokol seperti Internet Protocol (IP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Internet Group Management Protocol (IGMP), dan lain-lain. Internet Protocol (IP) merupakan protokol utama yang digunakan pada bagian ini.

- **Layer 3 : Transport Layer**

Layer diatas layer internet. Layer ini merupakan penyokong untuk aliran data antara dua perangkat dalam satu jaringan. Bagian transportasi mengizinkan entitas sebaya pada sumber dan tujuan perangkat untuk melakukan komunikasi. Bagian ini menggunakan banyak protokol diantaranya seperti (TCP) dan (UDP) yang sering digunakan.

- **Layer 4 : Application Layer**

Layer paling atas dari paket protokol TCP/IP. Bagian ini meliputi semua proses yang menggunakan protokol bagian transportasi, khususnya TCP and UDP, untuk mengirim data. Bagian memiliki banyak protokol seperti HTTP, Telnet, FTP, SMTP,NFS, TFTP, SNMP, dan DNS merupakan yang sering digunakan.

Log Files sebagai Bukti (Evidence)

1	Log files merupakan rekaman utama dari aktivitas user dalam sistem atau jaringan
2	penyelidik menggunakan log ini untuk memulihkan layanan yang diubah dan menemukan sumber kegiatan terlarang.
3	Masalah mendasar dari logs adalah ia dapat dengan mudah diubah. Seorang <i>attacker</i> dapat dengan mudah memasukan entrie yang salah kedalam log file.
4	Catatan komputer biasanya tidak dapat diterima sebagai bukti; mereka harus memenuhi kriteria tertentu untuk diterima sama sekali
5	Penuntut harus memberikan kesaksian yang tepat untuk menunjukkan bahwa kayu bulat itu akurat, dapat diandalkan, dan sepenuhnya utuh

Dalam investigasi forensic jaringan (digital), informasi log file membantu investigagor mengarah ke pelaku. Log files berisi data berharga, sumber daya yang berbeda pada jaringan/perangkat menghasilkan log files masing-masing bisa saja Sistem Operasi, IDS, firewall, dll. Log files yang dikumpulkan sebagai barang bukti harus mematuhi hukum tertentu agar dapat diterima di pengadilan; selain itu, diperlukan kesaksian ahli untuk membuktikan bahwa pengumpulan dan pemeliharaan log terjadi dengan cara yang dapat diterima

Laws and Regulation

Federal Information security management Act of 2002 (FISMA) :

FISMA adalah Federal Information security management Act of 2002 (Undang-undang manajemen keamanan Informasi Federal tahun 2002) yang menyatakan beberapa standar dan pedoman keamanan utama, sebagaimana disyaratkan oleh undang-undang Kongres.

FISMA menekankan perlunya setiap lembaga Federal menerapkan program seluruh organisasi untuk memberikan keamanan informasi untuk sistem informasi yang mendukung operasi dan asetnya. 11 NIST SP 800-53 adalah sumber utama kontrol keamanan yang direkomendasikan untuk agen-agen federal.

Gramm-Leach-Bliley Act (GLBA) : Gramm-Leach-Bliley Act mensyaratkan perusahaan Lembaga-keuangan yang menawarkan produk atau layanan keuangan. Manajemen log dapat bermanfaat dalam mengidentifikasi kemungkinan pelanggaran keamanan dan menyelesaikannya secara efektif

Health Insurance Portability and Accountability Act of 1996 (HIPAA) : The Health Insurance Portability and Accountability Act of 1996 (HIPAA) termasuk informasi kesehatan standar keamanan. NIST SP 800-66. Panduan Sumber Daya pengantar untuk menerapkan aturan keamanan Asuransi Kesehatan Portabilitas dan Akuntabilitas (HIPAA), mendaftar log terkait HIPAA

Sarbanes-Oxley Act (SOX) 2002: uu Sarbanes-Oxley 2002 (SOX) adalah sebuah uu yang dikeluarkan oleh kongres as pada tahun 2002 untuk melindungi para investor dari kemungkinan kegiatan akuntansi yang curang oleh perusahaan.

Payment Card Industry Data Security Standard (PCI DSS): standar keamanan kartu pembayaran dari industri kartu kredit (PCI DSS) adalah kepemilikan standar keamanan informasi untuk organisasi yang menangani informasi pemegang kartu untuk debit, kredit, prabayar, dompet, ATM, dan kartu POS utama.

Legality of using Log






Beberapa masalah hukum yang terlibat dalam pembuatan dan penggunaan logs yang harus diingat oleh organisasi dan simpatisan

1. Log harus dibuat secara masuk akal ontemporaneously dengan acara yang sedang diselidiki
--

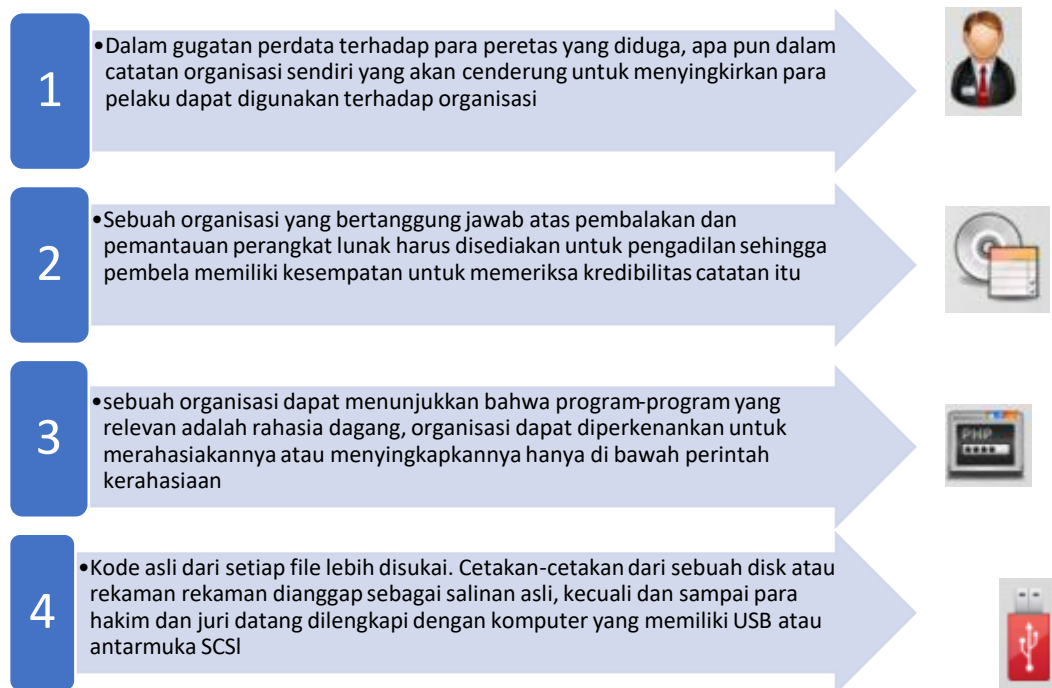
2. File Log harus diatur immutable pada sistem untuk mencegah gangguan
--

3. Seseorang dengan pengetahuan acara harus merekam informasi	4. Dalam hal ini, sebuah program yang menangani rekaman oleh karena itu catatan-catatan tersebut mencerminkan pengetahuan sebelumnya
5. Log harus disimpan sebagai praktek bisnis biasa	6. Kompilasi pandom data tidak diperbolehkan
7. Catatan harian yang ditetapkan setelah sebuah insiden dimulai tidak memenuhi syarat dalam pengecualian catatan bisnis	8. Simpan log biasa untuk digunakan sebagai bukti nanti

Legality of using Log (Cont'd)

	"Kustodian atau saksi lain yang cakap" harus membuktikan keakuratan dan integritas catatan itu. Ini dikenal sebagai otentikasi	
Penjaga tidak perlu menjadi programmer yang menulis perangkat lunak logging; Meskipun demikian, dia harus dapat memberikan kesaksian mengenai sistem apa yang digunakan, dari mana perangkat lunak yang relevan berasal, bagaimana dan kapan catatan-catatan diproduksi.		
	Seorang penjaga atau saksi lain yang memenuhi syarat juga harus memberikan kesaksian tentang keterandalan dan keteguhan perangkat keras dan perangkat lunak yang digunakan, termasuk logging software	
Sebuah catatan kegagalan atau keamanan pelanggaran pada mesin membuat log akan cenderung mendakwa bukti		
	Penyidik menyatakan bahwa sebuah mesin telah ditembus, log masuknya setelah titik itu adalah tersangka	

Legality of using Log (Cont'd)



Event Corelation

1	2	3	4
Peristiwa korelasi adalah proses menceritakan serangkaian peristiwa yang telah terjadi dalam interval waktu yang telah ditentukan sebelumnya	Proses ini mencakup analisis peristiwa untuk mengetahui bagaimana peristiwa itu bisa menambahkan untuk menjadi peristiwa yang lebih besar	Hal ini biasanya terjadi di platform manajemen log, setelah para pengguna menemukan log tertentu dengan sifat yang sama	Secara umum, proses korelasi dilaksanakan dengan bantuan perangkat lunak korrelator peristiwa sederhana

Event Correlation memiliki empat langkah yang berbeda, sebagai berikut:

Event Agregation menyusun peristiwa berulang untuk acara tunggal dan menghindari penggandaan peristiwa yang sama.

Event Masking Ia menghindari peristiwa yang menyebabkan sistem crash atau gagal.

Event Filtering menyaring atau membuang peristiwa yang tidak relevan

Root Cause Analysis Root cause analysis adalah bagian yang paling kompleks dalam hal korelasi. Event correlator mengidentifikasi semua perangkat yang

menjadi diakses karena kegagalan jaringan. Kemudian, peristiwa correlator mengkategorikan peristiwa menjadi peristiwa gejala dan penyebab penyebab peristiwa. Sistem ini menganggap peristiwa yang terkait dengan perangkat yang tidak dapat diakses sebagai peristiwa gejala, dan peristiwa non-gejala lainnya sebagai akar penyebab peristiwa

Jenis Event Korelasi

Jenis Event Kolerasi memiliki dua jenis berbeda berdasarkan platform yang sama dan berbeda, yaitu:

1. **Metode Kolerasi Platform yang sama**, dimana sebagai contoh di sebuah perusahaan dalam seluruh jaringannya menggunakan satu OS umum yang sama untuk semua server, kemudian melakukan pengumpulan entri log peristiwa, dengan melakukan analisis tren secara diagonal.
2. **Metode Kolerasi Lintas Pelatform**, merupakan metode kolerasi yang menggunakan berbagai OS dan platform perangkat keras jaringan yang berbeda dalam satu organisasi, misalnya menggunakan OS Windows, namun menggunakan firewall Linux dan gateway email.

Prasyarat Event Korelasi

Dalam melaksanakan Event Kolerasi terdapat beberapa persyaratan atau langkah-langkah yang harus dilakukan atau harus terpenuhi, yaitu:

1. **Syarat Transmisi Data**, dimana proses pengiriman data dari satu prangkat keamanan ke prangkat yang lain tanpa terpapar selama transmisi data, harus di enkripsi dan diautentifikasi, hingga transmisi mencapai titik konsolidasi dalam sistem otomatis
2. **Normalisasi**, dimana data yang telah di kumpulkan di ubah format lognya untuk satu atau log polimorfik yang dapat dengan mudah dimasukkan ke dalam database
3. **Pengurangan Data**, dimana data yang berulang harus di hapus dengan cara memfilter atau menggabungkan peristiwa serupa agar dapat di korelasi lebih efisien di mesin kolerasi

Pendekatan Event Korelasi

Ada beberapa jenis pendekatan dari Event Kolerasi, yaitu:

1. Pendekatan Berbasis Grafik, membangun grafik dengan node aech sebagai komponen sistem dan masing-masing tepi sebagai ketergantungan antara dua komponen

2. Pendekatan Berbasis Nerural Neural, menggunakan jaringan saraf untuk mendeteksi anomali dalam aliran peristiwa, akar penyebab peristiwa kesalahan, dll.
3. Pendekatan Berbasis Aturan, peristiwa dikorelasikan menurut seperangkat aturan sebagai berikut: kondisi untuk bertindak
4. Pendekatan Berbasis Codebook, menggunakan codebook untuk menyimpan serangkaian acara dan menghubungkannya

Pendekatan Event Korelasi (lanjutan)

Selain proses pendekatan sebelumnya, ada beberapa jenis pendekatan Event Kolerasi Lanjutan, yaitu:

1. Pendekatan Berbasis Lapangan, pendekatan dasar di mana peristiwa tertentu dibandingkan dengan bidang tunggal atau ganda dalam data yang dinormalisasi
2. Korelasi Lapangan Otomatis, memeriksa dan menyiapkan semua bidang secara sistematis dan sengaja untuk korelasi positif dan negatif di satu atau beberapa bidang
3. Parameter Paket / Korelasi Muatan untuk Manajemen Jaringan, digunakan untuk paket korelasi tertentu dengan paket lain dengan membuat daftar kemungkinan serangan baru dengan membandingkan paket dengan tanda tangan serangan
4. Pendekatan Berbasis Profil / Sidik Jari, Serangkaian set data dapat dikumpulkan dari data acara forensik seperti, sidik jari OS yang terisolasi, pemindaian port yang terisolasi, informasi sidik jari, dan penyambar untuk membandingkan data serangan tautan dengan profil penyerang lainnya untuk mengidentifikasi apakah suatu sistem adalah relay atau host yang sebelumnya dikompromikan, dan / atau untuk mendeteksi peretas yang sama dari lokasi yang berbeda.
5. Pendekatan Berbasis Kerentanan, untuk memetakan event IDS yang menargetkan host tertentu yang vulnarable dengan bantuan pemindai kerentanan unrtuk serangan pada host tertentu terlebih dahulu, dan memprioritaskan data serangan sehingga Anda dapat menanggapi titik masalah dengan cepat.
6. Korelasi Berbasis Port Terbuka, menentukan tingkat serangan yang berhasil dengan membandingkannya dengan daftar port terbuka yang tersedia di host dan yang sedang diserang
7. Korelasi Bayesian, mengasumsikan dan memprediksi apa yang dapat dilakukan penyerang selanjutnya setelah serangan dengan mempelajari statistik dan probabilitas, dan hanya menggunakan dua variable.
8. Waktu (Jam) atau Pendekatan Berbasis Peran, memonitor perilaku pengguna komputer dan memberikan peringatan jika sesuatu yang aneh ditemukan.
9. Rute Korelasi, mengekstrak informasi rute serangan dan menggunakan informasi itu untuk memilih data serangan lainnya

Memastikan Akurasi File Log

Kegiatan ini memastikan keandalan file log secara langsung tergantung pada akurasi dengan cara menyajikan file log dari sistem atau server yang diselidiki sebelum pengadilan dalam kondisi yang sama seperti yang tersedia sehingga modifikasi pada log dapat memengaruhi validitas seluruh log dan membuatnya curiga.

Langkah-langkah untuk memastikan akurasi log file

1. Catat Semuanya
2. Perhatikan Waktu
3. Gunakan Beberapa Sensor
4. Hindari catatan yang Hilang

Karena file log bukti berharga dan bertindak sebagai bukti di pengadilan, penyelidik harus memastikan bahwa file tersebut akurat. Tanpa mengikuti pedoman tertentu saat mengumpulkan dan menyimpan file log, mereka tidak akan diterima sebagai bukti yang sah di pengadilan. Oleh karena itu, simpatisan harus mengikuti langkah-langkah yang disebutkan di atas untuk menjaga akurasi file log.

Log Segalanya

- Jangan menganggap bidang apa pun dalam file log sebagai kurang penting, karena setiap bidang dapat memainkan peran utama sebagai bukti, sehingga administrator jaringan harus selalu mengonfigurasi pengaturan log server untuk merekam setiap bidang yang tersedia
- Konfigurasi log IIS untuk merekam informasi pengguna web tentang web untuk mengumpulkan petunjuk tentang asal serangan baik pengguna yang masuk atau sistem eksternal

Konfigurasi server web untuk mencatat semua bidang yang tersedia. ini akan membantu dalam penyelidikan, karena setiap bidang menunjukkan beberapa informasi mengenai aktivitas yang terjadi pada sistem. Anda tidak dapat memprediksi bidang mana yang dapat memberikan informasi penting dan mungkin bukti.

Mencatat setiap aktivitas server yang mungkin adalah keputusan yang bijaksana. misalnya, seorang korban dapat mengklaim bahwa penyusup telah mengakses komputernya dan menginstal proxy pintu belakang. dalam hal ini, mencatat setiap aktivitas server dapat membantu penyelidik dalam mengidentifikasi asal mula lalu lintas dan pelaku kejahatan.

Menjaga Waktu

Dengan layanan windows time, administrator jaringan dapat menyinkronkan server mandiri ke sumber waktu eksternal. Jika anda menggunakan domain, layanan waktu akan secara otomatis disinkronkan ke pengontrol domain. Administrator jaringan dapat menyinkronkan server mandiri ke sumber waktu eksternal dengan mengatur entri registri tertentu

faktor waktu penting dalam catatan yang disajikan sebagai bukti; Oleh karena itu, pemeliharaan waktu yang tepat dan akurat adalah prasyarat untuk penyelidikan forensik. Disarankan untuk menyinkronkan server IIS menggunakan layanan windows time dengan sumber waktu eksternal. layanan windows time akan secara otomatis menyinkronkan pengontrol domain di domain. sinkronisasi dukungan server mandiri dengan menetapkan sumber eksternal melalui entri registri, dengan cara berikut:

key :HKLM\SYSTEM\CurrentControllerSet\Services\W32Time\Parameters\

Value name: Type

Type:REG_SZ

Value data: NTP

key :HKLM\SYSTEM\CurrentControllerSet\Services\W32Time\Parameters\

Value name: NtpServer

Type:REG_SZ

Value data: tock.usno.navy.mil

key :HKLM\SYSTEM\CurrentControllerSet\Services\W32Time\Parameters\

Value name: period

Type:REG_SZ

Value data: 25

Kenapa Mengsinkronkan Waktu Komputer?

Ketika seorang administrator sedang menyelidiki intrusi dan peristiwa keamanan yang melibatkan banyak komputer, penting untuk menyinkronkan jam komputer. Jika jam komputer tidak disinkronkan, menjadi hampir mustahil untuk menyelesaikan tindakan yang dicatat di komputer yang berbeda secara akurat. Jika jam pada komputer ini tidak akurat, juga menjadi sulit untuk mengkorelasikan kegiatan yang dicatat dengan tindakan luar seperti secara teratur mengidentifikasi, memeriksa dan menganalisis sistem file log primer serta memeriksa file log yang dihasilkan oleh sistem deteksi intrusi dan firewall.

Masalah yang dihadapi oleh pengguna atau organisasi ketika waktu komputer tidak dalam sinkronisasi meliputi yang berikut:

1. Jika komputer menampilkan waktu yang berbeda, maka sulit untuk mencocokkan tindakan dengan benar di komputer yang berbeda. misalnya, pertimbangkan opsi obrolan melalui messenger apa pun. dua tipe dengan

jam berbeda berkomunikasi, dan karena jam berbeda, log menunjukkan waktu yang berbeda. sekarang, jika seorang pengamat memeriksa file log dari kedua sistem, ia akan menghadapi kesulitan dalam membaca percakapan.

2. Jika komputer yang terhubung dalam jaringan internal (organisasi) memiliki waktu yang disinkronkan tetapi waktunya salah, pengguna atau penyelidik mungkin menghadapi kesulitan dalam mengkorelasikan kegiatan yang dicatat dengan tindakan luar, seperti melacak intrusi.
3. Kadang-kadang, pada satu sistem, beberapa aplikasi membuat pengguna bingung ketika waktu melompat maju. misalnya, penyelidik tidak dapat mengidentifikasi pengaturan waktu dalam sistem basis data yang terlibat dalam layanan seperti transaksi e-commerce atau pemulihan kerusakan

Apakah Network Time Protocol (NTP)?

NTP adalah protokol standar internet (buntu di atas TCP / IP) yang digunakan untuk menyinkronkan jam komputer klien dengan mengirimkan permintaan waktu ke server yang dikenal dan memperoleh cap waktu server. Menggunakan stempel itu, itu menyesuaikan waktu klien.

Fitur NTP:

- Toleran terhadap kesalahan dan secara otomatis mengkonfigurasi otomatis
- Menyinkronkan akurasi hingga satu milidetik
- Dapat digunakan untuk menyinkronkan semua komputer dalam jaringan
- Menggunakan waktu UTC
- Tersedia untuk setiap jenis komputer

Network Time Protocol (NTP) adalah protokol yang digunakan untuk menyinkronkan waktu komputer yang terhubung ke jaringan. NTP adalah protokol internet standar (dibangun di atas TCP / IP) yang menjamin sinkronisasi sempurna jam komputer dalam jaringan komputer sejauh milidetik. itu berjalan melalui packet-switched dan jaringan data latensi variabel dan menggunakan port UDP 123 sebagai lapisan transportnya.

Selain itu, NTP juga menyinkronkan jam workstation klien. ini berjalan sebagai program latar belakang berkelanjutan pada komputer, menerima cap waktu server dan mengirimkan permintaan waktu berkala ke server, sering kali bekerja untuk menyesuaikan jam komputer klien. fitur protokol ini tercantum di bawah ini:

- Menggunakan waktu referensi.

- NTP akan memilih waktu yang paling tepat kemudian ada banyak sumber waktu.
- Mudah diakses.
- Menggunakan resolusi 2^{32} detik untuk memilih waktu referensi paling akurat.
- Menggunakan pengukuran dari contoh sebelumnya untuk menghitung waktu dan kesalahan saat ini, jika jaringan tidak tersedia.
- Ketika menggunakan jaringan tidak dapat dihindari, itu dapat memperkirakan waktu referensi dengan membandingkan waktu sebelumnya.

Menggunakan Sensor Berganda

Gunakan beberapa sensor (forewall, IDS, dll.) untuk merekam log. ini membantu membuktikan kredibilitas log jika dua perangkat terpisah mencatat informasi yang sama. Gabungkan juga log dari perangkat yang berbeda dapat memperkuat nilai masing-masing. Log dari firewall, IDS, IPS mungkin dapat membuktikan bahwa suatu sistem dengan alamat IP tertentu telah mengakses server tertentu pada titik waktu tertentu.

Menghindari Logs Hilang

- Ketika server web offline kata sandinya dimatikan, file log tidak dibuat. Ketika log hilang, sulit untuk mengetahui apakah server sebenarnya offline dimatikan, atau jika file log dihapus.
- Administrator dapat menjadwalkan beberapa klik ke server menggunakan alat penjadwalan dan kemudian menyimpan log dari hasil hit ini untuk menentukan kapan server aktif untuk mengatasi masalah ini. Jika logs hit menunjukkan bahwa server sedang online dan aktif pada saat data file log hilang, administrator tahu bahwa file log yang hilang mungkin telah dihapus.

Menerapkan manajemen log.

Manajemen log adalah proses berurusan dengan sejumlah besar log dan catatan yang dihasilkan system yang terdiri dari perangkat keras, perangkat lunak, jaringan, dan media yang digunakan untuk menghasilkan, mengirim, menyimpan, menganalisis, dan membuang data log. Itu mencakup semua proses dan teknik yang digunakan untuk mengumpulkan, mengumpulkan, menganalisis, dan melaporkan pesan log yang dihasilkan oleh perusahaan. Infrastruktur manajemen log biasanya terdiri dari tiga tingkatan berikut:

1. pembuatan log,
2. analisis dan penyimpanan log,

3. pemantauan log

Log adalah kumpulan entri atau catatan peristiwa, dan setiap entri menyertakan informasi terperinci tentang semua peristiwa yang terjadi dalam jaringan. Dengan meningkatnya workstation, server jaringan, dan layanan komputasi lainnya, volume dan variasi log juga meningkat. Untuk mengatasi masalah ini, manajemen log diperlukan. Infrastruktur manajemen log biasanya terdiri dari tiga tingkatan berikut:

1. Pembuatan log: tingkat pertama dari infrastruktur manajemen log termasuk host yang menghasilkan data log. Data log dapat dibuat tersedia untuk server log di tingkat kedua melalui dua cara. Host pertama menjalankan layanan atau aplikasi klien log yang membuat data log tersedia untuk server log melalui jaringan. Kedua, tuan rumah memungkinkan server untuk mengotentikasi dan mengambil salinan file log ke server.
2. Analisis dan penyimpanan log: tingkat kedua terdiri dari server log yang menerima data log atau salinan data log dari host. Data log ditransfer dari host ke server dalam atau hampir secara real time. data juga melakukan perjalanan dalam batch berdasarkan pada shcedule atau pada jumlah data log yang menunggu, server Log atau pada basis data terpisah berfungsi menyimpan data log
3. Pemantauan log: tingkat ketiga infrastruktur manajemen log berisi konsol yang memantau dan meninjau data log. Konsol ini juga meninjau hasil analisis yang dianalisa dan menghasilkan laporan.

Fungsi Infrastruktur Manajemen Log

Sistem manajemen log melakukan fungsi-fungsi berikut:

- Log parsing: Log parsing mengacu pada mengekstraksi data dari log sehingga nilai-nilai yang diurai dapat digunakan sebagai input untuk proses logging lainnya.
- Penyaringan peristiwa (Event Filtering): Penyaringan peristiwa adalah penindasan entri log melalui analisis, pelaporan, atau penyimpanan jangka panjang karena karakteristiknya menunjukkan bahwa mereka tidak mungkin berisi informasi yang menarik.
- Agregasi acara (Event Aggregation): Agregasi acara adalah proses di mana entri yang sama dikonsolidasikan ke dalam satu entri yang berisi hitungan jumlah kemunculan acara.
- Rotasi log (Log Rotation): Rotasi log menutup file log dan membuka file log baru setelah menyelesaikan file pertama. Ini dilakukan sesuai dengan jadwal (mis., Setiap jam, harian, mingguan) atau ketika file log mencapai ukuran tertentu.
- Pengarsipan dan penyimpanan log (Log Archival and Retention): Pengarsipan log mengacu pada penyimpanan log untuk periode waktu yang panjang, biasanya pada media yang dapat dilepas, jaringan area penyimpanan (SAN), atau alat arsip khusus atau server log. Investigator

perlu menyimpan log, untuk memenuhi persyaratan hukum dan / atau peraturan. Retensi log adalah pengarsipan log secara teratur sebagai bagian dari kegiatan operasional standar.

- Kompresi log (Log Compression): Kompresi log adalah proses menyimpan file log dengan cara yang mengurangi jumlah ruang penyimpanan yang diperlukan untuk file tersebut tanpa mengubah arti isinya. Ini sering dilakukan ketika log diputar atau diarsipkan.
- Pengurangan log (Log Reduction): Pengurangan log menghapus entri yang tidak dibutuhkan dari log untuk membuat log baru yang lebih kecil. Proses serupa adalah pengurangan peristiwa, yang menghapus bidang data yang tidak dibutuhkan dari semua entri log.
- Konversi log (Log Conversion): Konversi log adalah penguraian log dalam satu format dan menyimpan entri dalam format kedua. Misalnya, konversi dapat mengambil data dari log yang disimpan dalam database dan menyimpannya dalam format XML dalam file teks.
- Normalisasi log (Log Normalization): Dalam normalisasi log, setiap bidang data log dikonversi ke representasi data tertentu dan dikategorikan secara konsisten. Salah satu penggunaan normalisasi yang paling umum adalah menyimpan tanggal dan waktu dalam format tunggal
- Pemeriksaan integritas file log (Log File Integrity Checking) : Pemeriksaan integritas file log melibatkan penghitungan intisari pesan untuk setiap file dan penyimpanan intisari pesan dengan aman untuk memastikan deteksi perubahan yang dibuat pada log yang diarsipkan.
- Korelasi peristiwa (Event Correlation): Korelasi peristiwa adalah menentukan hubungan antara dua atau lebih entri log. Bentuk korelasi peristiwa yang paling umum adalah korelasi berbasis aturan, yang cocok dengan banyak entri log dari satu sumber atau beberapa sumber berdasarkan nilai yang dicatat, seperti cap waktu, alamat IP, dan jenis peristiwa.
- Log melihat (Log Viewing): Log melihat menampilkan entri log dalam format yang dapat dibaca manusia. Sebagian besar generator log menawarkan semacam kemampuan melihat log; utilitas melihat log pihak ketiga juga tersedia. Beberapa pemirsa log menyediakan kemampuan pemfilteran dan agregasi.
- Pelaporan log (Log Reporting): Pelaporan log menampilkan hasil analisis log. Hal ini sering dilakukan untuk merangkum kegiatan yang signifikan selama periode waktu tertentu atau untuk mencatat informasi terperinci terkait dengan peristiwa atau serangkaian peristiwa tertentu.
- Pembersihan log (Log Clearing): Pembersihan log menghapus semua entri dari log yang mendahului tanggal dan waktu tertentu. Ini sering dilakukan untuk menghapus data log lama yang tidak lagi diperlukan pada sistem karena tidak penting atau karena telah diarsipkan.

Pengujian dalam Manajemen Log

Ada tiga masalah utama terkait manajemen log. Yang pertama adalah pembuatan dan penyimpanan log; yang kedua adalah melindungi log; dan yang

ketiga adalah menganalisis log. Mereka adalah tantangan paling penting dari manajemen log yang akan berdampak pada penyelidikan forensik.

- Pembuatan dan penyimpanan log (Log Creation and Storage): Ada sejumlah besar log yang dihasilkan dari beberapa sumber daya sistem yang berukuran besar dan sulit disimpan. Format log adalah hal lain yang membuatnya sulit untuk mengelola log karena perangkat yang berbeda dan sistem pemantauan log menghasilkan log dengan format yang berbeda.
- Perlindungan log (Log Protection): Merupakan pertimbangan utama dalam investigasi karena bukti yang dimilikinya sangat berharga. Jika simpatisan tidak menangani log dengan benar selama pemeriksaan forensik, file kehilangan integritasnya dan menjadi tidak valid sebagai bukti.
- Analisis Log (Log Analysis): Memastikan analisis log yang tepat diperlukan. Namun, analisis log bukan pekerjaan prioritas tinggi untuk administrator. Analisis log adalah hal terakhir yang harus dilakukan untuk administrator karena terjadi setelah insiden terjadi. Oleh karena itu, ada kekurangan alat dan profesional terampil untuk analisis log, menjadikannya kelemahan utama.

Memusatkan Log

Logging terpusat (Centralized logging) didefinisikan sebagai kumpulan log sistem, dan jaringan komputer untuk sekelompok sistem di lokasi atau server terpusat yang membantu administrator melakukan pencadangan dan pengambilan yang mudah. Selain memungkinkan administrator untuk memeriksa log pada setiap sistem secara teratur dan efisien dengan frekuensi yang diperlukan untuk mendeteksi pelanggaran keamanan dan aktivitas yang tidak biasa.

Pencatatan terpusat menawarkan hal-hal berikut:

- Jejak dapat ditinjau jika mesin klien dikompromikan.
- Hal ini memungkinkan tempat pusat untuk menjalankan skrip pemeriksaan log
- Ini sangat aman tanpa yang lain
- Paket disaring / firewall untuk memungkinkan hanya mesin yang disetujui
- Log dapat dikirim ke alamat email apa saja untuk analisis harian.
- Ini memiliki kemampuan cadangan dan pemulihan yang sesuai

Semua sistem manajemen kejadian keamanan (SEM) memberikan solusi untuk acara keamanan yang terkait dengan pengumpulan, pemrosesan, dan penyimpanan. Server SEM khusus digunakan untuk memusatkan fungsi sehingga acara keamanan dikelola secara terpusat. Menyediakan cadangan terpusat, dan juga akan bermanfaat dalam mendeteksi dan menganalisis peristiwa. Server dipertahankan pada dua level:

1. Server SEM lokal
2. Master SEM server Server SEM lokal mengumpulkan, memproses, dan mengantri semua acara dan meneruskan tugas lebih lanjut ke master SEM.

Server master SEM menjalankan fungsi pemrosesan dan penyimpanan peristiwa keamanan selanjutnya untuk analisis, pelaporan, dan tampilan. Biasanya, sistem yang sangat terkonfigurasi diperlukan untuk master SEM karena membutuhkan kapasitas penyimpanan yang besar, karena bergantung pada ruang penyimpanan yang tersedia di server SEM pusat, peristiwa keamanan disimpan untuk periode mulai dari beberapa minggu hingga bulan.

Syslog

Syslog adalah standar de-facto untuk acara sistem logging, sistem pencatatan komprehensif yang mengelola informasi yang dibuat oleh kernel dan utilitas sistem. Ini adalah protokol klien / server yang digunakan untuk meneruskan pesan log di jaringan IP ke penerima syslog. Penerima syslog ini juga disebut sebagai server syslog, daemon syslog, atau syslogd. Istilah "syslog" mengacu pada protokol syslog dan aplikasi atau pustaka yang mengirim pesan syslog. Secara umum, syslog digunakan untuk mengelola dan memantau sistem komputer dan audit keamanan.

Syslog menggunakan TCP atau UDP untuk mentransfer pesan. Pesan log dikirim dalam format teks yang jelas. Perangkat dan penerima yang berbeda mendukung syslog di berbagai platform.

Syslog di Sistem mirip Unix

Sumber: <http://www.cs.umsi.edu>

Dalam sistem mirip UNIX, ini adalah jantung dari Linux logging. Fungsi syslog mengirim pesan ke logger sistem. Ia dikontrol melalui file konfigurasi `/etc/syslog.conf`. Itu mengurutkan pesan sesuai dengan sumber dan rute mereka ke berbagai tujuan sehingga melakukan beberapa fungsi, seperti berikut ini:

- Mengirim pesan ke syslogd
- Mencatatnya dalam log sistem yang sesuai
- Menuliskannya ke konsol system
- Meneruskannya ke daftar pengguna

Fasilitas syslog didasarkan pada dua elemen utama :

- `/etc/syslogd` (the daemon)
- `/etc/syslog.conf` file konfigurasi

Ada tiga bagian syslog :

1. syslogd

- Logging daemon, bersama dengan file config `/etc/syslog.conf`.
- Mulai saat boot dan berjalan terus menerus.
- Membaca dan meneruskan pesan sistem ke file log yang sesuai dan / atau pengguna.
- Program menulis entri ke `/dev/log` atau `/var/run/log`, yang bisa berupa soket, pipa bernama, atau modul STREAM.
- Pada Solaris, driver log STREAM adalah `/dev/log`.

- Syslogd membaca pesan dari file, berkonsultasi dengan file konfigurasinya, dan mengirim pesan ke tujuan yang sesuai.
 - Catat pesan tanda (tanda waktu) setiap 20 menit pada prioritas LOG_INFO ke fasilitas yang diidentifikasi sebagai tanda pada file syslog.conf.
 - Pada beberapa sistem, syslogd juga dapat membaca pesan kernel dari perangkat / dev / klog.
 - Menulis ID prosesnya ke file /etc/syslog.pid:
 - Memudahkan mengirim sinyal ke syslogd dari skrip.
 - Mulai ulang syslogd dengan
 - kill -HUP ' / bin / cat /etc/syslog.pid'
 - Mengompresi atau memutar file log yang dibuka oleh syslogd memiliki hasil yang tidak terduga.
 - Dikendalikan oleh file /etc/syslog.conf
 - menggunakan format:
 - selector <TAB>action
 - Contoh: user.err / var / adm / messages
 - Syslogd menghasilkan pesan berwaktu yang dicatat jika tanda fasilitas muncul di syslog.conf untuk menentukan tujuan bagi mereka.
2. **openlog**: Menginisialisasi logging dengan menggunakan nama fasilitas yang ditentukan.
 3. **logger**: menambahkan entri ke log system.

Keuntungan dari Server Syslog Terpusat:

Dalam pengaturan syslogging terpusat, server umum menerima semua pesan dan log syslog dari semua sistem komputer yang terhubung ke jaringan. Ia menerima pesan dan log syslog dari semua server UNIX; Server Windows; dan perangkat jaringan seperti router, switch, hub, firewall, dll.

Ada banyak keuntungan dari syslogging terpusat, sebagai berikut:

- Syslog pusat disimpan pada segmen berbeda untuk keamanan penyimpanan.
- Seorang hacker akan merasa sulit untuk menghapus log.
- Pesan log memungkinkan serangan bersama di berbagai platform
- Ini memiliki kebijakan cadangan yang mudah.
- Alat-alat seperti Swatch menghasilkan peringatan real-time, yang membantu untuk terus memonitor file log.

Pencatatan Biner Terpusat IIS

Pencatatan biner terpusat IIS merupakan proses dimana sebagian besar situs web mengirimkan data log biner dan tersebar ke satu file log. Ketika IIS meng-host beberapa situs web, proses pembuatan banyak file log yang diformat dan menulis

data log ke hard disk mengkonsumsi sumber daya CPU dan memori dan dengan demikian menciptakan masalah kinerja. Pencatatan biner terpusat IIS mengurangi sumber daya sistem yang digunakan untuk pencatatan dan menyediakan data log lengkap untuk organisasi yang membutuhkannya.

Integritas Sistem

Integritas sistem adalah integritas data, aplikasi, dan perangkat lunak pada sistem. Memastikan integritas sistem berarti menjaga dan melindungi integritas seluruh system, hal ini sangat penting karena sistem menyimpan semua log yang berkaitan dengan intrusi. Karena berani memenuhi ini, pengadilan tidak akan menerima bukti. Untuk mencapai integritas sistem, kita harus mengikuti pedoman yang telah ditentukan.

Kontrol Akses

Kontrol akses memberikan hak istimewa kepada pengguna, personalia, atau penyelidik. Setelah pembuatan file log, sangat penting untuk menghindari akses file atau audit oleh pengguna yang sah dan tidak sah. Jika file log diaudit dengan benar dan diamankan menggunakan izin NTFS, maka dapat memiliki bukti yang terdokumentasi dalam membangun kredibilitasnya. Dalam hal ini diperlukan pemeriksaan keaslian file log untuk proses pengadilan :

- File log adalah otentik hanya jika penyelidik dapat membuktikan bahwa mereka telah menjaga integritas file log dari saat pengumpulan awal.
- Secara umum, file log dapat dengan mudah diubah karena mereka adalah file teks sederhana.
- Dalam keadaan standar seperti itu, file log dapat dibuktikan otentik dengan mengikuti beberapa tips:
 - Pindahkan log - Anda harus mempertimbangkan bahwa file log dikompromikan jika server telah dikompromikan.
 - Pindahkan log ke server master dan kemudian ke media penyimpanan sekunder seperti DVD atau disk.

Tanda Tangan, Enkripsi, Dan Checksum

Tanda tangan adalah identitas pengirim yang dikirimkan bersama dengan data. Tanda tangan digunakan di lingkungan kunci publik dan menyediakan layanan otentikasi dan integritas.

Tanda tangan, enkripsi, dan checksum membantu membuktikan keaslian log:

- Gunakan tanda tangan file untuk membuat file log lebih aman
- Untuk menghasilkan hash MD5 untuk file, gunakan alat Fsum
- Simpan tanda tangan dan hash bersama dengan log
- Simpan salinan aman di lokasi yang terpisah dan aman

FSUM

FSUM merupakan utilitas baris perintah untuk verifikasi integritas file. Ia menawarkan pilihan 13 fungsi hash dan checksum untuk intisari pesan file dan perhitungan checksum.

Work With Copies

File log asli diperlukan untuk proses pengadilan, oleh karena itu, penyelidik perlu membuat salinan dari file log asli untuk menjaga yang asli dan memproduksinya di pengadilan. Pedoman untuk simpatisan saat melakukan analisis log meliputi beberapa hal sebagai berikut:

- Jangan pernah melakukan analisis file log pada file asli; pastikan hanya menggunakan salinan untuk tujuan ini
- Sangat penting untuk membuat salinan sebelum melakukan analisis file log atau pemrosesan pos.
- File log asli yang tak tersentuh diperlukan bagi penyelidik atau pengguna untuk menetapkan keaslian log dalam insiden keamanan
- Jika penyelidik menggunakan file log sebagai bukti pengadilan, perlu untuk menunjukkan file log asli dalam bentuk aslinya.

Chain Of Custody

Chain of custody adalah dokumentasi dari semua tindakan yang diambil selama investigasi. Tidak hanya mendokumentasikan semua tindakan tetapi juga mendokumentasikan informasi tentang bukti dan perlunya menyelesaikan kasus. Para peneliti dapat menggunakan metode teknis atau non-teknis, seperti otentikasi MD5, untuk mempertahankan lacak balak.

Otentikasi MD5 : Ini adalah algoritma yang digunakan untuk menjaga integritas file log. Algoritma ini menggunakan nilai hash 128-bit untuk file log tertentu untuk melindungi file dari segala jenis perubahan.

File Log Kondensasi

Syslog adalah file log yang penting untuk menyortir dan merutekan pesan log. Dengan sejumlah besar file log syslog, menjadi sulit bagi tim forensik untuk memfilter entri log yang penting. Untuk tujuan ini, perlu menggunakan alat-alat seperti Swatch dan Logcheck untuk memfilter file log tergantung pada persyaratan. Alat yang digunakan adalah sebagai berikut:

Swatch

Sumber: [https:// sourcef orge. bersih / proyek / carikan](https://sourceforge.net/projects/swatch/)

Swatch adalah alat yang digunakan untuk memantau file log yang dihasilkan oleh fasilitas syslog UNIX

Logcheck

Sumber: <http://logcheck.org>

Logcheck adalah utilitas yang memungkinkan administrator sistem untuk melihat file log, yang diproduksi oleh host di bawah kendali mereka. Ini dilakukan dengan mengirimkan ringkasan file log ke host, setelah terlebih dahulu memfilter entri "normal".

Mekanisme Analisis Forensik Jaringan

Mekanisme analisis forensik jaringan ini mencakup menyajikan bukti, memanipulasi, dan penalaran otomatis.

Analyst Interface

Analyst Interface menyediakan visualisasi grafik bukti dan hasil penalaran kepada analis, yang meneruskan umpan balik ke pembuatan grafik dan komponen penalaran.

Pengumpulan Bukti

Pengumpulan bukti melibatkan pengumpulan bukti intrusi dari jaringan dan host yang sedang diselidiki.

Pemrosesan Bukti

Bukti preprocessing berkaitan dengan analisis jenis bukti yang tegas, seperti peringatan intrusi, ke dalam format yang sesuai dan mengurangi pengulangan dalam bukti tingkat rendah melalui agregasi.

Penyimpanan Bukti

Setelah preprocessing, bukti intrusi yang dikumpulkan disimpan dalam penyimpanan bukti.

Pembuatan Grafik Bukti

Manipulasi grafik bukti menghasilkan dan memperbarui grafik bukti menggunakan bukti intrusi dari penyimpanan.

Menyerang Reasoning

Attack reasoning adalah proses penalaran otomatis berdasarkan grafik bukti.

Serang Basis Pengetahuan

Basis pengetahuan serangan mencakup pengetahuan tentang eksploitasi sebelumnya.

Basis Pengetahuan Aset

Basis pengetahuan aset mencakup pengetahuan tentang jaringan dari fundamental dan host yang sedang diselidiki.

Pada tahap awal, bukti yang dikumpulkan adalah pra-diproses dan disimpan dalam penyimpanan bukti. Modul pembuatan grafik membuat grafik bukti dengan bukti yang diambil dari penyimpanan. Selanjutnya, modul penalaran memperoleh inferensi otomatis berdasarkan grafik bukti dan menyajikan hasilnya kepada analis. Melalui modul antarmuka, analis dapat memberikan pendapat ahli dan informasi out-of-band, terutama melalui dua pendekatan yakni dengan cara mengedit grafik bukti secara langsung dan yang kedua kirim pertanyaan untuk mengambil bukti spesifik.

Selanjutnya, proses penalaran dilakukan pada grafik bukti yang diperbarui untuk hasil yang lebih baik.

Log Capturing and Analysis (Tools : GFI EventManager)

Fitur:

- Analisis data log, termasuk perangkat SNMP, log peristiwa Windows®, log W3C, log berbasis teks, Syslog, SQL Server®, dan log audit Oracle®
- Memberikan laporan spesifik untuk beberapa tindakan kepatuhan utama serta laporan standar lainnya
- Grafik yang diaktifkan dengan filter memberikan akses ke data penting yang Anda butuhkan
- GFI EventsManager menawarkan kontrol granular data log yang mendalam untuk dengan mudah mengklasifikasikan informasi dari sistem.
- GFI EventsManager menawarkan penyimpanan data log yang aman sesuai dengan standar industri dan praktik terbaik keamanan.

Tools : Penganalisis EventLog

Fitur :

- Menawarkan manajemen log untuk keamanan jaringan
- Memantau log aplikasi dan menghasilkan laporan
- Tetap mendapatkan informasi tentang kegiatan acara secara waktu nyata
- Menawarkan pendekatan holistik untuk keamanan jaringan IT
- Periksa apakah audit siap dan patuh

Log Capturing and Analysis (Tools : Cont'd)

- Kibana

Kibana adalah platform visualisasi data open-source yang memungkinkan interaksi dengan data melalui antar muka pengguna grafis.

- Syslog-ng

Syslog-ng adalah pengumpulan, penguraian, klasifikasi dan korelasi log dari seluruh infrastruktur dan menyimpan atau merutekannya ke log untuk alat analisis.

- Rsyslog

Rsyslog adalah system untuk pemrosesan log. Menawarkan fitur keamanan dan desain modulator, menerima input dari berbagai sumber, mengubahnya dan mengeluarkan hasilnya menjadi beragam tujuan.

- Firewall Analyzer

ManageEngine Firewall Analyzer adalah log analytics dan perangkat lunak manajemen konfigurasi itu membantu administrator jaringan untuk mengumpulkan, mengarsipkan, analisis log perangkat keamanan mereka dan selanjutnya menghasilkan laporan forensik.

- Simple Event Correlator (SEC)

SEC adalah alat korelasi peristiwa untuk pemrosesan acara, yang dapat dimanfaatkan untuk pemantuan, pengelolaan jaringan dan keamanan, deteksi penipuan dan tugas lain apapun yang melibatkan korelasi peristiwa.

- OSSEC

OSSEC adalah system deteksi instruksi berbasis host yang open-source. Ia melakukan log analisis, pemeriksaan integritas, pemantauan registrasi windows, deteksi rootkit, peringatan real-time dan respon aktif.

- Ipswitch Log Management

Ipswitch Log Management adalah alat otomatis yang mengumpulkan, menyimpan, arsip, dan mencadangkan Syslog, acara windows, atau log W3C / IIS.

- Variaoto Server Manager

Alat ini memungkinkan untuk melihat dan melaporkan data log peristiwa dan mengisolasi entri log parsial dengan memisahkan beberapa log menjadi satu tampilan, menyembunyikan entri duplikat dan memfilter hasilnya.

- Log Management Utility

Utilitas Manajemen Log memungkinkan seseorang untuk mengumpulkan, menyimpan, menelusuri dan mencari log audit MFP dengan lancar dan

untuk jangka waktu yang lebih lama dari PC, memberikan lebih banyak waktu untuk mengelola dan menganalisis kondisi setiap MFP

- **Snare**
Snare membantu mengumpulkan dan memfilter data peristiwa IT untuk pemantauan, analisis, audit, dan pengarsipan keamanan yang penting.
- **Splunk Enterprise**
Splunk Enterprise memungkinkan penyelidik untuk mengumpulkan, menganalisis, dan menindaklanjuti nilai data besar yang belum dimanfaatkan yang dihasilkan oleh infrastruktur teknologi, sistem keamanan, dan aplikasi bisnis yang memberi mereka wawasan untuk mendorong kinerja operasional dan hasil bisnis.
- **Loggly**
Loggly menawarkan layanan berbasis cloud yang menambang data log secara real time dan mengungkapkan apa yang diperlukan, sehingga Anda memiliki wawasan yang Anda butuhkan untuk menghasilkan log.
- **vRealize Log Insight**
Merevitalisasi wawasan log memberikan manajemen log heterogen dan scalable dengan dashboard intuitif, dapat ditindaklanjuti, analitik canggih dan ekstensibilitas pihak ketiga yang luas, sehingga memberikan visibilitas operasional dan pemecahan masalah yang lebih cepat.
- **Sumo Logic**
Sumo Logic digunakan untuk membangun, menjalankan dan mengamankan aplikasi modern.
- **TIBCO LogLogic**
Alat ini digunakan untuk memanfaatkan data log dan mesin untuk memberikan wawasan tentang efisiensi operasionalnya.
- **Logscape**
Alat ini memungkinkan pencarian, memvisualisasikan file log dan data operasional.
- **ArcSight ESM**
HPE Security ArcSight ESM adalah aplikasi manajemen keamanan yang menggabungkan korelasi peristiwa dan analitik keamanan untuk

mengidentifikasi dan memprioritaskan ancaman secara waktu nyata, di sana dengan memfasilitasi tanggapan dan perbaikan segera.

- XpoLog Log Management

Platform manajemen log Xpolog membantu dalam analisis, visualisasi, pemantauan, dan penambahan data log otomatis yang mendalam. Xpolog memungkinkan optimalisasi operasi IT dan visibilitas untuk semua jenis data log sistem.

- LogRhythm

Platform intelijen dan analitik keamanan LogRhythm memungkinkan organisasi mendeteksi, memprioritaskan, dan menetralkan ancaman dunia maya yang menembus batas atau berasal dari dalam.

- Sawmill

Sawmill akan membantu menganalisis, memantau, dan mengingatkan berbagai sistem. ini menyediakan fitur pemrosesan log dan pelaporan untuk mendapatkan wawasan tentang data jaringan.

- McAfee Enterprise Log Manager

McAfee enterprise Log Manager mengumpulkan, mengompres, menandatangani, dan menyimpan semua acara asli dengan jejak audit aktivitas yang jelas yang tidak dapat ditolak.

- Log and event Manager

Log and event Manager adalah SIEM yang memudahkan penggunaan log untuk keamanan, kepatuhan, dan pemecahan masalah.

- Papertrail

Papertrail digunakan untuk alat log hemat waktu, grup sistem fleksibel, akses tim-lebar, arsip jangka panjang, bagan, ekspor analitik, dan pemantauan webhooks.

- EventReporter

EventReporter adalah prosesor log kejadian windows dan forwarder syslog. ini digunakan untuk menggabungkan beberapa log peristiwa dan membuat repositori pusat.

- Kiwi Log Viewer

Kiwi Log Viewer memungkinkan pemantauan berkas Log untuk perubahan. Itu dapat menampilkan perubahan secara langsung dan memungkinkan pemantauan otomatis dari entri berkas catatan untuk kata kunci, ungkapan, atau pola spesifik.

- **Event Log Explorer**
Event Log Explorer adalah solusi perangkat lunak untuk melihat, menganalisa dan memantau peristiwa yang direkam di Log Microsoft Windows Event. Event Log Explorer menyederhanakan analisis Log peristiwa (keamanan, aplikasi, sistem, pengaturan, layanan direktori, DNS, dan lain-lain).
- **Weblog Expert**
Weblog Expert adalah sebuah analisis log akses. Ini menyediakan informasi mengenai pengunjung situs: statistik kegiatan, file yang diakses, alamat yang melalui situs, informasi mengenai rujukan halaman, mesin pencari, peramban, sistem operasi, dan banyak lagi. Weblog Expert dapat menganalisis log of Apache, server web IIS dan Nginx bahkan dapat membaca Gz dan ZIP file log terkompresi, yang mencegah perlunya untuk membongkar mereka secara manual.
- **ELM Enterprise Manager**
ELM Enterprise Manager Elevates Windows pemantauan untuk real time. Peristiwa log dikumpulkan terpercaya setelah ditulis.
- **Event Sentry**
Event Sentry menerima peringatan kritis dan konsolidates semua log. Event Sentry menawarkan set aturan canggih untuk memastikan anda hanya mendapatkan peringatan yang anda butuhkan.
- **LogMeister**
Alat ini memonitor log peristiwa Windows, syslog, dan log teks di server di seluruh jaringan, memberikan notifikasi tentang peristiwa kunci dan memperkenankan tindakan penting dan tepat waktu yang pantas.
- **InTrust**
Infra merah memungkinkan pengumpulan data, penyimpanan, pencarian, dan analisis secara besar-besaran berupa data dari berbagai sumber data, sistem, dan perangkat di satu tempat.
- **Alert Logic Log Manager**
Notifikasi manajer Log logika dengan ActiveWatch adalah solusi keamanan as-as-service (SaaS) yang memenuhi persyaratan kepatuhan dan mengidentifikasi isu keamanan di seluruh lingkungan, termasuk public cloud. Mengumpulkan, memproses, dan menganalisa data.

- **Sentinel Log manager**
Sentinel pengelola Log merupakan alat perangkat lunak yang memungkinkan pengumpulan, penyimpanan, analisis, dan pengelolaan peristiwa infrastruktur dan catatan keamanan.
- **Tripwire Log Center**
Tripwire Log Center menormalisasi data dari server, keamanan dan perangkat jaringan, serta aplikasi, mengintegrasikan mereka dengan Tripwire Enterprise dan Tripwire IP360m untuk menyediakan Perlindungan dan keamanan endpoint.
- **Manajemen keamanan AlienVault**
AlienVault Unified Security managementment (USM) adalah sebuah platform yang menyediakan pengawasan keamanan yang terpadu, terkoordinasi, manajemen acara keamanan dan pelaporan, kecerdasan ancaman yang berkelanjutan dan beberapa fungsi keamanan tanpa banyak konsol.
- **MyEventViewer**
MyEventViewer memungkinkan pengguna untuk menonton beragam catatan peristiwa dalam satu daftar. Sebagai tambahan MyEventViewer memungkinkan pemilihan beberapa benda peristiwa dengan mudah dan menyimpannya untuk HTML/Text/XML file atau menyalurkannya ke papan klip (Ctrl+C) dan memasukkannya ke Excel.
- **WinAgents EventLog Translation Service**
Layanan penerjemahan zat winagent EventLog adalah server yang memonitor log peristiwa Windows dan meneruskan peristiwa yang muncul untuk pemrosesan lebih lanjut.
- **EventTracker Enterprise**
EventTracker Enterprise adalah alat manajemen log dan mencakup fitur seperti integritas berkas: pemantauan, mengubah Audit, penilaian konfigurasi, integrasi cloud, korelasi peristiwa, dan pemantauan media yang dapat digunakan.
- **Logstash**
Logstash adalah jaringan data yang membantu proses log dan data peristiwa lainnya dari berbagai sistem. Logstash dapat terhubung ke berbagai sumber dan stream data dalam skala untuk sistem analisis pusat.
- **SecurityCenter CV**
Security Center Continuous View (Security Center CV) mengumpulkan data dari banyak sensor untuk memberikan analisis lanjutan tentang kerentanan, ancaman, jaringan lalu lintas, dan informasi peristiwa dan memberikan tampilan yang berkelanjutan keamanan di seluruh lingkungan.
- **The Elastic Stack**

The Elastic Stack dengan sumber terbuka, yaitu Elasticsearch, Kibana, logstash, dan Beats, membantu mendapatkan data dari sumber mana pun dalam format dan pencarian, analisa, dan visualisasi secara langsung.

- **CorreLog**
CorreLog adalah solusi untuk cross-platform IT keamanan log manajemen dan acara korelasi log. Memungkinkan koleksi log peristiwa seluruh sistem distribusi dan mainframe.
- **Assuria Log Manager**
Alat ini digunakan untuk pengumpulan secara forensik catatan suara dari hampir semua sumber ke toko pusat. Ini memungkinkan manajemen otomatis seluruh perusahaan dari log, termasuk rotasi log
- **BlackStratus LOGStorm**
LOGStorm" adalah solusi manajemen log dan pemantauan log yang menggabungkan manajemen log dengan teknologi korelasi, real-time peristiwa korelasi log dan pemantauan log-log, dan sistem respon peristiwa terpadu.
- **Powerbroker Event Vault**
Beyond dtrust PowerBroker acara Vault automates dan memotong koleksi dan manajemen log Microsoft Windows standar.
- **Logsene**
Menggunakan Logsene, semua log dapat diakses di satu tempat. Hal ini memungkinkan untuk memeriksa log melalui UI atau Elasticsearch API dan korelasi log dengan metrik kinerja via SPM
- **Saas Log Manajemen**
Manajemen Log Saas adalah solusi yang bekerja dengan manajemen Log CloudAccess SIEM untuk menyediakan penyimpanan yang aman dan manajemen data peristiwa sepanjang kehidupan.
- **ApexSql Log**
ApexSql log adalah pembaca log transaksi transaksi database server sql yang dapat menyajikan semua informasi dalam format yang dapat diubah manusia
- **FortisIEM**
Ini adalah informasi keamanan dan manajemen acara (SIEM) yang digunakan untuk mendeteksi dan memulihkan keamanan acara. Ini menawarkan keamanan, kinerja, dan manajemen kepatuhan.
- **Graylog**
Ini adalah alat manajemen log open-source yang digunakan untuk mencari, menganalisa, dan membuat peringatan di semua berkas catatan.

Menganalisa Catatan Router

- Routers menyimpan catatan koneksi jaringan dengan detail seperti tanggal, waktu, sumber dan tujuan serta port yang digunakan
- Informasi ini dapat membantu penyelidikan dalam memverifikasi cap waktu serangan dan korelasi berbagai peristiwa untuk menemukan sumber dan tujuan IP
- Router memiliki banyak standar untuk menyimpan rincian log dari jaringan

Dalam penyelidikan jaringan forensik, penyidik mengumpulkan log dari router untuk memeriksa dan menentukan rincian seperti alamat IP dan protokol. Pengalihan log ke server syslog dilakukan dengan cara berikut :

```
#config terminal logging 192.168.1.1
```

Selama jaringan apapun hacking, atau skenario akses yang tidak sah, semua log berkaitan dengan serangan akan disimpan dalam perangkat dikompromikan, yang mungkin router/switch, database, ID, server ISP router, atau aplikasi. Hampir semua peralatan jaringan profesional memungkinkan pencatatan peristiwa, akan tetapi, karena keterbatasan daya ingat, alat-alat ini tidak dapat menyimpan gelondongan itu untuk waktu yang lama. Oleh karena itu, para administrator mengumpulkan dan menyimpan catatan-catatan ini secara teratur.

Bukti berkumpul dari ARP

- ARP di router, router berguna untuk penyelidikan jaringan serangan, karena meja berisi alamat IP asosiasi dengan alamat MAC masing-masing
- seorang investigator dapat melihat meja ARP di jendela dengan mengeluarkan perintah ARP
- Tabel ARP yang dipertahankan di router sangat penting, karena dapat memberikan informasi tentang alamat MAC dari semua host yang terlibat dalam komunikasi terbaru

Router mengikuti standar yang berbeda untuk menyimpan log di jaringan. Tidak perlu setiap router mengikuti standar yang sama. Misalnya, file log berisi detail seperti tanggal, waktu, alamat IP sumber, port-sumber, URL yang diakses, alamat IP URL, dan port yang digunakan. Perincian ini mungkin bermanfaat bagi penyerang selama investigasi. Sintaks file log dari router lain mungkin berbeda.

Perangkat lunak jaringan Cisco IOS adalah perangkat lunak jaringan yang digunakan adalah router Cisco. IOS mengintegrasikan layanan penting bisnis dan dukungan platform perangkat keras. Teknologi keamanan iOS bertindak sebagai perisai untuk proses bisnis terhadap serangan dan gangguan serta melindungi privasi, serta mendukung kebijakan dan kontrol kepatuhan terhadap peraturan. Perangkat jaringan transit berisi pesan syslog yang memberikan wawasan dan menjelaskan konteks insiden keamanan.

Ada delapan tingkat keparahan klasifikasi pesan syslog pada router Cisco IOS. Ada nomor dan nama yang sesuai untuk setiap tingkat keparahan untuk identifikasi, seperti berikut ini :


Level	Sistem	Deskripsi
Emergency	0	Pesan sistem tidak dapat digunakan
Alert	1	Pesan segera diperlukan tindakan
Critical	2	Pesan kondisi kritis
Error	3	Pesan kondisi kesalahan
Warning	4	Pesan kondisi peringatan
Notification	5	Pesan normal tetapi signifikan
Information	6	Pesan informasi
Debugging	7	Pesan debugging

Mnemonic	Severity	Deskripsi
%SEC-6-IPACCESSLOGDP	6	Paket yang cocok dengan kriteria log untuk daftar akses yang diberikan telah terdeteksi
%SEC-6-IPACCESSLOGNP	6	Paket yang cocok dengan kriteria log untuk daftar akses yang diberikan telah terdeteksi
%SEC-6-IPACCESSLOGP	6	Paket yang cocok dengan kriteria log untuk daftar akses yang diberikan telah terdeteksi(TCP/UDP)
%SEC-6-IPACCESSLOGRL	6	Beberapa log pencocokan paket tidak terjawab karena pesan log daftar akses dibatasi tarifnya, atau tidak ada buffer log daftar akses yang tersedia.
%SEC-6-IPACCESSLOGRP	6	Paket yang cocok dengan kriteria log untuk daftar akses yang diberikan telah terdeteksi

%SEC-6-IPACCESSLOGS	6	Paket yang cocok dengan kriteria log untuk daftar akses yang diberikan terdeteksi
%SEC-4-TOOMANY	4	Sistem tidak dapat memproses paket karena tidak ada cukup ruang untuk semua opsi header IP yang diinginkan. Paket telah dibuang.
%SEC-6-ACCESSLOGP	6	Paket yang cocok dengan kriteria log untuk daftar akses yang diberikan terdeteksi
%SEC-6-ACCESSLOGDP	6	Paket yang cocok dengan kriteria log untuk daftar akses yang diberikan terdeteksi
%SEC-6-ACCESSLOGNP	6	Paket yang cocok dengan kriteria log untuk daftar akses yang diberikan terdeteksi


Cisco ASA menyediakan pesan log yang berguna dalam perangkat lunak CISCO IOS. Pesan log router tidak mengandung pengidentifikasi numerik yang membantu dalam mengidentifikasi pesan. Di bawah ini adalah daftar pesan log router dengan deskripsi terperinci, yang paling mungkin berguna saat menganalisis insiden terkait keamanan.

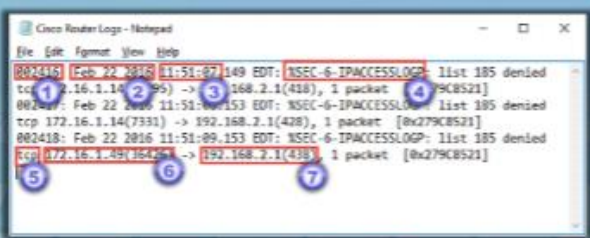
Analyzing Router Logs: Cisco (Cont'd)



The Cisco router log details are as follows:

1. Event ID
2. Date
3. Time
4. Identifier
5. Protocol applied
6. Source IP address
7. Destination IP address





```

002418: Feb 22 2016 11:51:09 EDT: %SEC-6-IPACCESSLOGP: list 185 denied
tcp 172.16.1.14(295) -> 192.168.2.1(418), 1 packet [0x279C8521]
002417: Feb 22 2016 11:51:09 EDT: %SEC-6-IPACCESSLOGP: list 185 denied
tcp 172.16.1.14(7331) -> 192.168.2.1(428), 1 packet [0x279C8521]
002418: Feb 22 2016 11:51:09 EDT: %SEC-6-IPACCESSLOGP: list 185 denied
tcp 172.16.1.14(7331) -> 192.168.2.1(418), 1 packet [0x279C8521]

```

Copyright © by Cisco. All Rights Reserved. Reproduction is Strictly Prohibited.

Pada slide di atas, ada tangkapan layar yang berisi LOGS dengan detail seperti ID peristiwa, data, waktu, pengidentifikasi, protokol yang diterapkan, alamat IP sumber, dan alamat IP tujuan. Berdasarkan pengidentifikasi yang (4) dalam lembar log, tingkat keparahan log diketahui pada saat menganalisis insiden terkait keamanan.

JUNOS adalah sistem operasi yang berjalan pada perangkat jaringan Juniper. Sistem operasi menyediakan dua fungsi:

1. Pencatatan sistem

Sistem logging menghasilkan pesan syslog yang merekam peristiwa di router yang berkaitan dengan login, kegagalan login, penghentian tidak terduga dari proses rekan, dan penutupan router jika terjadi panas berlebih.

2. Menelusuri

Tracing terutama berkaitan dengan protokol routing. Ia menyimpan semua informasi yang berkaitan dengan operasinya; pertukaran paket selama awal proses atau mentransfer pembaruan yang dijadwalkan.

Fungsi di atas menyimpan pesan log ke file. Log router Juniper secara default disimpan dalam pesan nama file. Router menyimpan log pesan ke file. File-file log disimpan di / var / log / lokasi, dan nama path sama untuk router M-, MX-, dan T-series, untuk router seri-J file-file tersebut disimpan di adalah / cf / var / log.

Menganalisis Log Firewall

1. Firewalls adalah titik masuk pertama untuk sebuah jaringan dan menyimpan detail semua paket data yang bergerak kedalam dan keluar dari sebuah jaringan.
2. Log firewall mengumpulkan lalu lintas data jaringan seperti request source dan tujuan, port yang digunakan, waktu dan tanggal, prioritas, dll
3. Rincian ini akan membantu peneliti mengkolerasi data dengan file mencurigakan lainnya untuk menemukan sumber dan target lain dari sebuah serangan
4. Jaringan firewall hadir dengan manajemen software yang memungkinkan pengguna untuk memantau logs, kontrol setting keamanan dan melakukan pemeliharaan tugas lain melalui firewall
5. Para invwstigator perlu menganalisis log secara hati-hati, berdasarkan timing dan IP Address yang mencurigakan.

6. Periksa request yang dihasilkan aplikasi, DNS queries, IP address yang mencurigakan dan URLs

Sebuah Firewall adalah perangkat lunak atau perangkat keras yang membantu mencegah hacker dan beberapa jenis dari malware dari mendapatkan ke setiap PC melalui sebuah jaringan atau internet. Log file firewall dapat digunakan untuk menentukan penyebab kegagalan program. Para penyelidik dapat menggunakan log untuk mengidentifikasi aktivitas berbahaya, meskipun firewall tidak memberikan informasi lengkap yang diperlukan untuk melacak sumber aktivitas tetapi memberikan beberapa wawasan tentang sifat dari aktivitas tersebut.

Log adalah file plaintext dan dapat dilihat menggunakan editor teks apa pun. Periode penyimpanan log tergantung pada batas penyimpanan yang ditetapkan untuk file. Log yang lebih baru menggantikan yang lama.

Selama waktu serangan keamanan, catatan ini dapat memberi para penyelidik gagasan tentang pelanggaran tersebut. Penyelidik dapat mengkorelasikan log ini dengan file bermanfaat lainnya untuk mendeteksi sumber dan target serangan lainnya.

Dalam satu atau lain cara, pesan log sangat berguna; dalam banyak kasus, sebagian kecil pesan log pada awalnya akan memberikan manfaat paling besar. Setelah memeriksa kejadian ini, simpatisan dapat memperluas cakupan analisis mereka dengan mencari detail tambahan.

Log firewall Cisco berisi tanggal dan waktu, pesan mnemonic, aksi firewall, alamat IP sumber dan port, alamat dan port IP tujuan, jenis permintaan. Semua benda ini bermanfaat bagi simpatisan dalam proses investigasi.

Dengan menggunakan aplikasi Check Point Log viewer untuk melihat log firewall pos pemeriksaan. Aplikasi ini menggunakan kode warna untuk membedakan tingkat kesalahan, sebagaimana disebutkan dalam tabel di bawah ini (Tabel 4).

Event Log Color Coding	
Red	An Error message
Orange	A warning message
Blue	An information

Tabel 7.1: Pengodean warna Eventlog di log firewall pos pemeriksaan

ICON mewakili setiap tindakan dalam penampil log firewall Checkpoint, seperti yang ditunjukkan pada slide.

Analisis IDS Log

Selain memantau dan menganalisis peristiwa untuk mengidentifikasi kegiatan yang tidak diinginkan, semua jenis teknologi IDS biasanya melakukan fungsi-fungsi berikut:

- Merekam informasi yang berkaitan dengan peristiwa yang diamati: IDS biasanya mencatat Informasi secara lokal dan mengirimkan informasi ini ke sistem yang terpisah seperti server logging terpusat, informasi keamanan dan solusi manajemen acara (SIEM), dan sistem manajemen perusahaan.
- Memberitahu administrator keamanan: IDS memberi tahu administrator keamanan jaringan melalui email, halaman, pesan antarmuka pengguna IDS, perangkat protokol manajemen jaringan (SNMP) sederhana, pesan sistem tog, dan program dan skrip yang ditentukan pengguna.
- Memproduksi laporan: IDS menawarkan repofis yang merangkum acara yang dipantau atau memberikan rincian tentang acara tertentu yang menarik.

Menganalisis Log IDS: Juniper (Lanjutan)

Di Juniper IDS, sistem mencatat peristiwa saat mencapai ambang naik dan reset untuk penggunaan memori, penggunaan CPU, penggunaan ruang disk, atau jumlah maksimum sesi aktif, sesuai standar. Ambang batas default adalah 90%. Log peristiwa Juniper IDS disimpan di Network and Security Manager (NSM), yang ada di dalam perangkat.

Menganalisis Log IDS: Juniper (Lanjutan)

Rincian yang disediakan oleh IDS dalam log meliputi:

1. Tanggal dan Waktu
2. Alamat IP perangkat
3. Jenis serangan
4. Alamat Sumber
5. Port Sumber
6. Alamat Tujuan
7. Beratnya serangan

Objek-objek ini membantu simpatisan dalam penyelidikan melanjutkan lebih lanjut.

Menganalisis Log IDS: Checkpoint

Checkpoint IPS memiliki perangkat lunak bawaan untuk mengelola perangkat. Pengguna dapat melihat dan menganalisis log menggunakan perangkat lunak ini. Langkah-langkah untuk melihat dan mengakses log di IDS Checkpoint :

- Pergi ke SmartDashboard, klik SmartConsole pilih SmartView Tracker
- Pilih tab Network & Endpoint, rentangkan Predefined → Network Security Blades → IPS Blade
- Double-klik Semua untuk melihat informasi log lengkap

Menganalisis Log IDS: Checkpoint (lanjutan)

Log Titik Periksa menyediakan informasi lalu lintas jaringan untuk memungkinkan penyesuaian bandwidth.

Menganalisis Log Honeypot

1. Honeypots adalah perangkat yang berpura-pura berisi informasi yang sangat berguna untuk memikat penyerang dan menemukan keberadaan dan teknik mereka.
2. Kippo adalah salah satu honeypots yang paling umum digunakan.
3. Log yang disimpan di Kippo berisi informasi berikut:
 - 1) Stempel waktu
 - 2) Jenis sesi
 - 3) ID Sesi dan alamat IP Sumber
 - 4) Pesan dengan detail lainnya

Honeypots adalah perangkat penipuan yang dirancang sedemikian rupa sehingga menarik penyerang untuk berkompromi dengan sistem informasi dalam suatu kelompok. Honeypots adalah sistem boneka yang digunakan untuk memahami strategi penyerang dan melindungi organisasi dari serangan.

Kippo adalah salah satu Honeypots yang biasa digunakan untuk mengelabui penyerang dan memahami metodologi mereka sehingga meminimalkan risiko serangan

DHCP Logging

- Log DHCP disimpan dalam C: \ Windows \ System32 \ dhcp pada folder server DHCP
- Format file log server DHCP
 - ID, Date, Time, Description, IP Address, Host Name, MAC Address

ID	Kode ID Peristiwa DHCP
Date	Tanggal di mana entri ini dicatat di server DHCP
Time	Waktu di mana entri ini dicatat di server DHCP
Description	Penjelasan atau acara server DHCP ini
IP Address	Alamat IP klien DHCP
Host Name	Nama host dari klien DHCP
MAC Address	Alamat kontrol akses media (MAC) yang digunakan oleh adaptor jaringan perangkat keras klien

Server DHCP dalam jaringan mengalokasikan alamat IP ke komputer selama permulaannya. Oleh karena itu, log server DHCP berisi informasi mengenai sistem yang diberikan alamat IP tertentu ke server,

Evidence Gathering at the Data-Link Layer: DHCP Database

- Basis data DHCP menyediakan sarana untuk menentukan MAC, alamat yang terkait dengan komputer yang ditahan
- Basis data ini membantu DHCP untuk menyimpulkan alamat MAC jika DHCP tidak dapat mempertahankan log permintaan permanen
- Server DHCP menyimpan daftar pertanyaan terbaru bersama dengan alamat MAC dan alamat IP
- Basis data dapat ditanyakan dengan memberikan durasi waktu di mana alamat IP yang diberikan mengakses server

Basis data DHCP menyediakan sarana untuk menentukan alamat MAC yang terkait dengan komputer yang ditahan. Basis data ini membantu DHCP untuk menyimpulkan alamat MAC jika DHCP tidak dapat mempertahankan log permanen dari permintaan tunggal yang diterima. Server DHCP menyimpan daftar pertanyaan terbaru bersama dengan alamat MAC dan alamat IP. Penyelidik juga dapat merujuk tabel ARP selama investigasi untuk menentukan alamat MAC. Tabel ARP yang dikelola pada router sangat penting, karena dapat memberikan informasi tentang alamat MAC dari semua host yang terlibat dalam komunikasi baru-baru ini.

ODBC Logging

ODBC logging mencatat kumpulan bidang data tetap dalam database yang kompatibel dengan ODBC, seperti Microsoft Access atau Microsoft SQL Server.

Dengan pendataan ODBC, database harus disiapkan untuk menerima data dan database ini harus ditentukan untuk merekam file log.

Why Investigate Network Traffic?

Beberapa alasan simpatisan menganalisis lalu lintas jaringan:

1. Untuk mencari lalu lintas jaringan yang mencurigakan
2. Untuk mengetahui jaringan mana yang menghasilkan lalu lintas bermasalah dan dari mana lalu lintas dikirim atau diterima
3. Untuk mengidentifikasi masalah jaringan

Investigasi lalu lintas jaringan dapat membantu administrator atau penyelidik untuk mengetahui apakah lalu lintas normal dan tidak normal. Mereka dapat menjalankan fungsi-fungsi berikut:

- Mendeteksi setiap aktivitas mencurigakan di lingkungan dan mencoba untuk meminimalkan keparahan serangan itu
- Identifikasi dan hindari gangguan keamanan
- Mendeteksi jika penyerang merusak sistem dan menghapus file yang hanya bukti berbasis jaringan yang dapat membantu penyelidik untuk analisis forensik
- Identifikasi kegiatan yang mencurigakan
- Sesuaikan bandwidth sesuai penggunaan.

Evidence Gathering via Sniffing

- Sniffer mengumpulkan lalu lintas dari jaringan dan mengangkut lapisan selain dari lapisan fisik dan data-link
- Administrator harus mengonfigurasi sniffer untuk ukuran frame yang akan ditangkap
- Sniffer adalah perangkat lunak atau perangkat keras komputer yang dapat mencegat dan mencatat lalu lintas yang melewati jaringan digital atau bagian dari jaringan
- Port yang terbentang, ketukan perangkat keras membantu mengendus jaringan yang diaktifkan

Sniffing Tool: Wireshark

1. Ini memungkinkan Anda menangkap dan secara interaktif menelusuri lalu lintas yang berjalan di jaringan komputer

2. Wireshark menggunakan Winpcap untuk menangkap paket, oleh karena itu, ia hanya dapat menangkap paket di jaringan yang didukung oleh Winpcap
3. Ini menangkap lalu lintas jaringan langsung dari Ethernet, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, jaringan FDDI
4. File yang diambil dapat diedit secara terprogram melalui baris perintah
5. Seperangkat filter untuk tampilan data yang disesuaikan dapat disempurnakan menggunakan filter tampilan

Wireshark adalah penganalisa protokol jaringan GUI. Ini memungkinkan pengguna menelusuri data paket secara interaktif dari jaringan langsung atau dari file tangkapan yang disimpan sebelumnya. Format file capture asli Wireshark adalah dalam format libcap, yang juga merupakan format yang digunakan oleh tcpdump dan berbagai alat lainnya. Wireshark tidak memerlukan identifikasi jenis file yang dibaca pengguna; itu akan menentukan jenis file dengan sendirinya. Wireshark juga mampu membaca format file apa pun yang dikompres dengan menggunakan zip. Selain itu, Wireshark memiliki fitur-fitur lain, ia dapat mengumpulkan semua paket dalam cakupan TCP dan menunjukkan kepada pengguna data ASCII (atau EBCDIC, atau hex) dalam percakapan itu. Filter tampilan di Wireshark sangat kuat. Pustaka pcap melakukan pengambilan paket. Sintaks filter tangkapan mengikuti aturan pustaka pcap. Sintaks ini berbeda dari sintaksis filter tampilan. Dukungan file terkompresi menggunakan perpustakaan zlib. jika pustaka zlib tidak ada, Wireshark akan mengkompilasi, tetapi tidak akan bisa membaca file terkompresi. Opsi -r dapat digunakan untuk menentukan nama path untuk membaca file yang diambil atau untuk menentukan nama path sebagai argumen baris perintah.

Fitur-fiturnya meliputi:

- Memungkinkan penelusuran data jaringan yang diambil
- Menangkap file yang dikompres dengan gzip dan dapat mendekompresnya
- Aturan warna dapat diterapkan pada daftar paket untuk analisis intuitif yang cepat
- Memungkinkan mengeksport keluaran ke XML, PostScript, CSV, atau plaintext.

Ikuti Aliran TCP di Wireshark

Saat bekerja dengan protokol berbasis TCP, akan sangat membantu untuk melihat data dari aliran TCP dengan cara yang dilihat oleh aplikasi jika penyidik mencari kata sandi dalam aliran Telnet atau mencoba memahami aliran data. Pengguna hanya perlu memilih paket TCP di daftar paket dari aliran / koneksi yang sesuai dan pilih item menu TCP Stream ikuti dari Wireshark Tools.

Wireshark memiliki beragam filter tampilan. Mereka memungkinkan penelusuran ke lalu lintas yang tepat yang dibutuhkan dan merupakan dasar dari banyak fitur Wireshark.

Tampilan penyaringan berdasarkan protokol:

Ketikkan protokol di kotak Filter, misalnya: arp, http, tcp, udp, dns

Fitur:

- Analisis paket berkecepatan tinggi untuk mendeteksi masalah dengan cepat
- Menganalisis file multi-terabyte dengan cepat
- Pelaporan profesional yang dapat dipahami semua orang
- Tidak ada biaya untuk analisis multi-segmen
- Integrasi tanpa batas dengan Wireshark

WinDump

WinDump adalah versi Windows tcpdump, penganalisa jaringan baris perintah untuk UNIX. WinDump sepenuhnya kompatibel dengan tcpdump dan digunakan untuk menonton, mendiagnosis, dan menyimpan ke lalu lintas jaringan disk sesuai dengan berbagai aturan kompleks. Itu dapat berjalan di bawah Windows 95, 98, ME, NT, 2000, XP, 2003, dan Vista.

Capsa

Capsa adalah penganalisa jaringan portabel untuk LAN dan WLAN yang melakukan pengambilan paket, pemantauan jaringan, analisis protokol tingkat lanjut, penguraian paket yang mendalam, dan diagnosis ahli otomatis

Fitur

- Identifikasi dan analisis lebih dari 300 protokol jaringan, serta aplikasi jaringan berdasarkan protokol.
- Pantau bandwidth dan penggunaan jaringan dengan menangkap paket data yang dikirimkan melalui jaringan dan memberikan ringkasan dan informasi pengodean tentang paket-paket ini.
- Lihat statistik jaringan, memungkinkan penangkapan dan interpretasi data pemanfaatan jaringan.
- Monitor lalu lintas Internet, email, dan pesan instan, membantu menjaga produktivitas karyawan agar tetap maksimal.
- Diagnosis dan temukan masalah jaringan dengan mendeteksi dan mencari host yang mencurigakan.

- Memetakan detail, termasuk lalu lintas, alamat IP, dan MAC dari masing-masing host di jaringan, memungkinkan untuk memudahkan identifikasi setiap host dan lalu lintas yang melewati masing-masing.
- Visualisasikan seluruh jaringan dalam bentuk elips yang menunjukkan koneksi dan lalu lintas antara setiap host.

OmniPeek

OmniPeek memberikan visibilitas real-time dan analisis pakar jaringan ke setiap bagian jaringan dari satu antarmuka, termasuk Ethernet, Gigabit, 10 Gigabit, nirkabel 802.11a / b / g / n, VoIP, dan video ke kantor jarak jauh.

Fitur:

- Manajemen kinerja jaringan dan pemantauan jaringan, termasuk segmen jaringan di kantor jarak jauh.
- Memantau statistik jaringan utama secara real time, menggabungkan beberapa file, dan langsung menelusuri paket menggunakan dashboard interaktif "Kompas"
- Manajemen mulus semua probe perangkat lunak OmniEngine, dan perekam jaringan Omnipliance dan TimeLine dalam jaringan.
- Dukungan terintegrasi untuk Ethernet, Gigabit, 10 Gigabit, nirkabel 802.11a / b / g / n (termasuk 3-stream), VoIP, video, MPLS, dan VLAN
- Intuitive drill-down untuk memahami yang mana node sedang berkomunikasi, protokol dan sub-protokol mana yang sedang ditransmisikan, dan karakteristik lalu lintas mana yang memengaruhi kinerja jaringan
- Lengkap suara dan video melalui pemantauan waktu nyata IP, termasuk dashboard multimedia tingkat tinggi, catatan data panggilan (CDR) dan pensinyalan komprehensif dan analisis media

Observer

Observer adalah perangkat lunak yang digunakan untuk pemecahan masalah dalam jaringan. Ini memiliki fitur seperti analisis ahli, alat VoIP, analisis aplikasi yang mendalam, dinamika koneksi, rekonstruksi aliran, dan banyak lagi, selain menawarkan dukungan untuk manajemen perangkat SNMP dan RMON.

Colasoft Packet Builder

Colasoft Packet Builder memungkinkan pembuatan paket jaringan khusus; pengguna dapat menggunakan alat ini untuk memeriksa perlindungan jaringan terhadap serangan dan penyusup. Alat ini mencakup fitur pengeditan. Selain

memungkinkan pengeditan HEX umum dari data mentah, fitur editor dekoding yang memungkinkan untuk mengedit nilai bidang protokol khusus.

Investigator NetWitness

Investigator NetWitness menangkap lalu lintas langsung dan memproses file paket dari hampir semua perangkat pengumpulan jaringan yang ada untuk dianalisis. Alat ini dapat secara lokal memproses file paket dan merekam secara real time dari ketukan jaringan atau port span dengan wawasan langsung ke lalu lintas jaringan. Alat ini adalah aplikasi interaktif utama AppSuite NetWitness.

Ace Password Sniffer

Ace Password Sniffer adalah utilitas pemulihan kata sandi yang menangkap kata sandi yang terlupakan. Digunakan untuk memonitor aktivitas web dan memonitor penyalahgunaan kata sandi. Mendukung dan menangkap kata sandi melalui http, ftp, smtp, pop3, dan telnet, termasuk beberapa kata sandi email web. Alat Ini juga bertindak sebagai utilitas pemantauan diam-diam dan digunakan untuk memulihkan kata sandi jaringan, untuk menerima kata sandi jaringan anak-anak untuk orang tua, dan untuk memonitor penyalahgunaan kata sandi untuk administrator server.

IPgrab

IPgrab adalah endapan paket sniffer untuk host UNIX.

Big Mother

Big Mother adalah switchsniff dengan nol konfigurasi yang digunakan sebagai alat pemantauan aktivitas internet. ini adalah program menguping yang menggunakan sniffer switch untuk menangkap dan menganalisis lalu lintas komunikasi melalui jaringan. Program akan mengatur sendiri dan melakukan pemantauan konten dan kontrol akses untuk menjaga anggota keluarga atau karyawan bertanggung jawab atas tindakan ini.

EtherDetect Packet Sniffer

EtherDetect Packet Sniffer adalah alat sniffing yang dapat menangkap paket penuh yang diatur oleh koneksi tcp atau utas UDP dan secara pasif memonitor jaringan, dengan instalasi program pada PC target. Memungkinkan tampilan paket dalam format Hex dan penampil sorotan sintaksis.

Fitur:

- Mengatur paket yang diberi caput dalam tampilan koneksi-oriented
- Menangkap paket Ip di LAN dengan hampir tidak ada paket yang hilang.
- Berfungsi sebagai penganalisa waktu-nyata, memungkinkan tampilan konten langsung saat mengambil dan menganalisis.
- Mengaktifkan parse dan mendekode berbagai protokol jaringan.
- Mendukung penghematan paket yang diambil untuk dibuka kembali sesudahnya.
- Mengizinkan penyorotan sintaksis untuk aplikasi dalam format HTML, HTTP, dan XML.

dsniff

dsniff ini adalah alat untuk audit jaringan dan pengujian penetrasi. Dsniff secara pasif memonitor jaringan untuk data, kata sandi, email, file, dll. Selanjutnya, arpspoof, dnsspoof, dan macof memfasilitasi intersepsi lalu lintas jaringan yang biasanya tidak tersedia bagi penyerang.

EffeTech HTTP Sniffer

EffeTech HTTP Sniffer ini adalah sniffer paket HTTP, penganalisa protokol, dan perangkat lunak pemasangan kembali file berdasarkan pada platform windows. Sniffer ini mendedikasikan dirinya untuk menangkap paket IP yang berisi protokol HTTP, membangun kembali sesi HTTP, dan menyusun kembali file yang dikirim melalui protokol HTTP. Dengan memberikan utilitas monitoring HTTP yang mudah digunakan dan memenangkan penghargaan, Alat ini telah menjadi pilihan manajer, administrator jaringan, dan pengembang yang disukai di seluruh dunia. Informasi tentang lalu lintas HTTP dapat diterima oleh semua melalui LAN.

Ntopng

Ntopng ini adalah probe lalu lintas jaringan yang menunjukkan penggunaan jaringan, mirip dengan apa yang dilakukan perintah Unix populer. Ntopng didasarkan pada libpcap, dan berjalan di setiap platform Unix, MacOSX dan Windows. Pengguna Ntopng menggunakan peramban web untuk bernavigasi melalui ntop (yang bertindak sebagai server web) informasi lalu lintas dan mendapatkan dump status jaringan. Dalam kasus terakhir, ntopng bertindak sebagai agen mirip-RMON sederhana dengan antarmuka web tertanam.

Fitur:

- Mengurutkan lalu lintas jaringan menurut banyak kriteria, termasuk alamat IP, port, protokol L7, throughput, AS.
- Menunjukkan lalu lintas jaringan dan host aktif IPv4 / v6.
- Menghasilkan laporan tentang berbagai metrik jaringan seperti throughput, protokol aplikasi.
- Simpan di statistik lalu lintas persisten disk dalam format RRD.
- Host geo-lokal dan menampilkan laporan sesuai dengan lokasi host.
- Menghasilkan lalu lintas HTTP dengan mengecualikan layanan karakterisasi yang disediakan oleh Google dan Daftar Hitam HTTP.
- Tampilkan distribusi Lalu Lintas Ip di antara berbagai protokol.
- Menganalisis lalu lintas IP dan mengurutkan menurut sumber / tujuan.
- Menghasilkan statistik lalu lintas network HTML5 / AJAX.

Ettercap

Ettercap ini adalah paket komprehensif untuk serangan man-in-the-middle. Fitur mengendus/sniffing koneksi langsung, pemfilteran konten dengan cepat, dan banyak trik menarik lainnya. Mendukung diseksi aktif dan pasif dari banyak protokol dan mencakup banyak fitur untuk analisis jaringan dan host.

SmartSniff

SmartSniff ini adalah utilitas pemantauan jaringan yang menangkap paket TCP / IP yang melewati adaptor jaringan dan menampilkan data yang ditangkap sebagai urutan percakapan antara klien dan server. Memungkinkan melihat percakapan TCP / IP di Ascii atau sebagai hex dump.

EtherApe

EtherApe ini adalah monitor jaringan grafis untuk UNIX yang dimodelkan setelah etherman. Menampilkan lapisan tautan, mode IP dan TCP, dan secara grafik menampilkan aktivitas jaringan. Host dan tautan berubah ukuran seiring dengan lalu lintas.

Network Probe

Network Probe ini adalah monitor jaringan dan penganalisa protokol untuk memonitor alat lalu lintas jaringan. Dapat menemukan sumber dari setiap jaringan yang lambat. Menampilkan protokol yang digunakan pada jaringan, host yang mana mengirim dan menerima data, dari mana lalu lintas berasal, dan kapan semua

terjadi. Memungkinkan mengonfigurasi sedemikian rupa sehingga dapat memberi tahu jika ada sesuatu yang tidak biasa terjadi dan dapat secara proaktif memperbaiki masalah sebelum berkembang menjadi masalah serius.

WebSiteSniffer

WebSiteSniffer ini adalah alat packet sniffer untuk menangkap semua file Web yang diunduh oleh browser Web saat menjelajah internet dan menyimpannya di hard drive di bawah folder dasar yang dipilih. Memungkinkan pengguna untuk menangkap semua jenis file situs web yang diperlukan: File HTML, File Teks, File XML, File CSS, File Video / Audio, Gambar, Script, dan file Flash (.swf). Saat mengambil file situs Web, jendela utama menampilkan statistik umum tentang file yang dibebani untuk setiap situs Web / nama host, termasuk ukuran total semua file (terkompresi dan tidak terkompresi) dan jumlah total file untuk setiap jenis file.