KEAMANAN JARINGAN KOMPUTER

“DIGITAL FORENSIK”

OLEH :

AGUS JULIANSYAH

09011181320034

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

- **TUGAS :**

Cari video Teleconference tentang "Digital Forensic". Tonton video tersebut, kemudian buat kesimpulan dari video tersebut.

DEFINISI DEGITAL FORENSIK

Digital forensik adalah kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum.

Dari definisi diatas dapat disimpulkan bahwa digital forensik adalah penggunaan teknik analisis dan investigasi untuk mengidentifikasi, mengumpulkan, memeriksa dan menyimpan bukti/informasi yang secara magnetis tersimpan/disandikan pada komputer atau media penyimpanan digital sebagai alat bukti dalam mengungkap kasus kejahatan yang dapat di pertanggungjawabkan secara hukum. Karena luasnya lingkup yang menjadi objek penelitian dan pembahasan digital forensik maka ilmu digital forensik dibagi kedalam beberapa bagian yaitu: firewall forensics, network forensics, database forensics, dan mobile device forensics.

Link video :

https://www.youtube.com/watch?v=zjK-JThLg_Y

Judul video : tools for digital forensic investigation

PENJELASAN SINGKAT:

Dari link video di atas menjelasakan tentang 10 free tools for digital forensic investigation.

1. **SANS SIF**

   SANS Investigative Toolkit Forensik (SIFT) adalah Live CD berbasis Ubuntu yang mencakup semua alat yang Anda butuhkan untuk melakukan penyelidikan forensik atau insiden respon yang mendalam. Mendukung analisis Saksi Ahli Format (E01), Advanced Forensik Format (AFF), dan RAW (dd) format bukti. SIFT termasuk alat seperti log2timeline untuk menghasilkan garis waktu dari sistem log, pisau bedah untuk data file ukiran, Rifiuti untuk memeriksa recycle bin, dan banyak lagi. Bila Anda boot pertama ke lingkungan SIFT, saya sarankan Anda menjelajahi dokumentasi pada desktop

untuk membantu Anda menjadi terbiasa dengan apa alat yang tersedia dan bagaimana menggunakannya. Ada juga penjelasan yang baik dari mana untuk menemukan bukti pada sistem.Gunakan menu bar bagian atas untuk membuka alat, atau memulai secara manual dari jendela terminal.

2. **Sleuth Kit (+ otopsi)**

The Sleuth Kit adalah open source forensik digital toolkit yang dapat digunakan untuk melakukan analisis mendalam dari berbagai macam file sistem. Otopsi pada dasarnya adalah sebuah GUI yang duduk di atas The Sleuth Kit. Muncul dengan fitur seperti Analisis Timeline, Hash Filtering, File Analisis Sistem dan Kata Kunci Mencari di luar kotak, dengan kemampuan untuk menambahkan modul lain untuk fungsi diperpanjang. Ketika Anda memulai otopsi, Anda dapat memilih untuk membuat kasus baru atau memuat yang sudah ada. Jika Anda memilih untuk membuat kasus baru Anda akan perlu memuat gambar forensik atau disk lokal untuk memulai analisis Anda. Setelah proses analisis selesai, gunakan node pada panel sebelah kiri untuk memilih yang menghasilkan untuk melihat.

3. **FTK Imager**

FTK Imager adalah alat pratinjau data dan pencitraan yang memungkinkan Anda untuk memeriksa file dan folder pada hard drive lokal, drive jaringan, CD / DVD, dan meninjau konten gambar forensik atau memori kesedihan. Menggunakan FTK Imager Anda juga dapat membuat SHA1 atau MD5 hash dari file, ekspor file dan folder dari gambar forensik ke disk, review dan memulihkan file yang dihapus dari Recycle Bin (memberikan bahwa blok data mereka belum ditimpa), dan mount gambar forensik untuk melihat isinya pada Windows Explorer. Ketika Anda memulai FTK Imager, pergi ke 'File> Add Bukti Barang ...' untuk memuat sepotong bukti ulasan. Untuk membuat gambar forensik, pergi ke 'File> Buat Disk Image ...' dan memilih sumber Anda ingin forensik gambar.

4. **DEFT**

   DEFT adalah Linux Live CD yang bundel beberapa gratis dan open source komputer alat forensik paling populer yang tersedia. Hal ini bertujuan untuk membantu dengan Respon Insiden, Cyber Intelligence dan skenario Forensik Komputer. Antara lain, berisi alat untuk Ponsel Forensik, Network Forensik, Data Recovery, dan Hashing. Bila Anda boot menggunakan DEFT, Anda ditanya apakah Anda ingin memuat lingkungan hidup atau menginstal DEFT ke disk. Jika Anda memuat lingkungan hidup Anda dapat menggunakan cara pintas pada menu bar aplikasi untuk meluncurkan alat yang diperlukan.

5. **Volatilitas**

   Volatilitas adalah kerangka kerja forensik memori untuk respon insiden dan analisis malware yang memungkinkan Anda untuk mengekstrak artefak digital dari volatile memory (RAM) kesedihan. Menggunakan Volatilitas Anda dapat mengekstrak informasi tentang proses yang berjalan, soket jaringan terbuka dan koneksi jaringan, DLL dimuat untuk setiap proses, gatal-gatal registri cache, ID proses, dan banyak lagi.

6. **LastActivityView**

   LastActivityView memungkinkan Anda untuk melihat tindakan apa yang diambil oleh pengguna dan apa peristiwa yang terjadi pada mesin. Kegiatan seperti menjalankan file eksekusi, membuka file / folder dari Explorer, aplikasi atau system crash atau pengguna melakukan instalasi software akan login. Informasi yang dapat diekspor ke / XML / file HTML CSV. Alat ini berguna ketika Anda perlu membuktikan bahwa pengguna (atau akun) melakukan tindakan ia mengatakan mereka tidak.Ketika Anda memulai LastActivityView, segera akan mulai menampilkan daftar tindakan yang diambil pada mesin itu sedang berjalan di. Urutkan berdasarkan waktu tindakan atau menggunakan tombol pencarian untuk mulai menyelidiki apa tindakan yang diambil pada mesin.

7. HxD

   HxD adalah hex editor yang user-friendly yang memungkinkan Anda untuk melakukan editing lowlevel dan memodifikasi dari disk mentah atau memori utama (RAM). HxD dirancang dengan mudah penggunaan dan kinerja dalam pikiran dan dapat menangani file

besar tanpa masalah. Fitur termasuk mencari dan mengganti, mengekspor, checksum / mencerna, built-in file shredder, Rangkaian atau pemecahan file, generasi statistik dan banyak lagi.Dari antarmuka HxD mulai analisis Anda dengan membuka file dari 'File>Open', memuat disk dari 'Ekstra > Terbuka disk yang ...' atau memuat proses RAM dari

'Ekstra> Buka RAM.

8. **CAINE**

   CAINE (Computer Aided Investigative Environment) adalah Linux Live CD yang berisi kekayaan alat forensik digital. Fitur termasuk GUI yang user-friendly, pembuatan laporan semi-otomatis dan alat-alat untuk Mobile Forensik, Network Forensik, Data Recovery dan banyak lagi.Bila Anda boot ke lingkungan CAINE Linux, Anda dapat meluncurkan alat forensik digital dari antarmuka CAINE (shortcut di desktop) atau dari shortcut setiap alat dalam folder 'Tools Forensik' pada bar menu aplikasi

9. **Mandiant RedLine**

   RedLine menawarkan kemampuan untuk melakukan memori dan analisis host tertentu mengajukan. Ini mengumpulkan informasi tentang proses yang berjalan dan driver dari memori, dan mengumpulkan file sistem metadata, data registri, log peristiwa, informasi jaringan, layanan, tugas, dan sejarah Internet untuk membantu membangun profil penilaian ancaman secara keseluruhan. Ketika Anda memulai RedLine, Anda akan diberikan pilihan untuk Kumpulkan Data atau Analisa Data. Kecuali Anda sudah memiliki berkas dump memori yang tersedia, Anda harus membuat kolektor untuk mengumpulkan data dari mesin dan biarkan proses yang berjalan sampai selesai. Setelah Anda memiliki berkas dump memori untuk tangan Anda dapat memulai analisis Anda.

   Mandiant readline juga memiliki running processes, driver file system metadata dan event logs.

10. **PlainSight**

    PlainSight adalah Live CD berdasarkan Knoppix (distribusi Linux) yang memungkinkan

Anda untuk melakukan tugas-tugas forensik digital seperti melihat sejarah internet, ukiran data, USB penggunaan perangkat pengumpulan informasi, memeriksa memori fisik kesedihan, penggalian hash password, dan banyak lagi. Bila Anda boot ke PlainSight, muncul sebuah jendela yang meminta Anda untuk memilih apakah Anda ingin melakukan scan, memuat file atau menjalankan wizard. Masukkan seleksi untuk memulai proses ekstraksi data dan analisis.

KESIMPULAN

Dari penjelasan singkat tentang 10 free tools for digital forensic investigation di atas bahwa kita bias membantu Anda melakukan investigasi forensic digital. Entah itu untuk kasus internal SDM, penyelidikan akses tidak sah ke server, atau jika Anda hanya ingin belajar keterampilan baru, suite ini dan utilitas akan membantu Anda melakukan memori analisis forensik, hard drive analisis forensik, forensik eksplorasi gambar, pencitraan forensik dan forensik mobile. Dengan demikian, mereka semua memberikan kemampuan untuk membawa kembali informasi mendalam tentang apa yang "di bawah tenda" dari sebuah sistem.Pada pembahasan ini kita sudah mengenal dan mengetahui tentang kontribusi dari tool open source terhadap digital forensik. Jika kamu memiliki koleksi tool digital forensik lainnya silahkan memulai diskusi dengan cara menuliskannya dikotak komentar dibagian bawah.