Forensik

?? http://www.forensicswiki.org/

18.1 Keterbatasan Forensik

Tidak adanya bukti bukan bukti ketiadaan. ? Ilmiah? C pepatah (http://en.wikipedia.org/wiki/Argument\_from\_ kebodohan)

Forensik memiliki batas. Sebagai contoh, tidak jarang ketika berhadapan dengan penyusup terampil untuk? Nd bahwa mereka telah symlinked sejarah shell? Le ke / dev / null, atau bahwa baris terakhir log? Le adalah sesuatu seperti rm / var / log / sudo atau pesta -i. Hal ini bahkan mungkin bahwa musuh yang sangat terampil dan disiplin akan meninggalkan sistem dalam keadaan bahwa forensik menunjukkan satu hal, tetapi disinformasi; Aku belum pernah mendengar apa pun yang halus dalam praktek, tapi sekali lagi, apa yang kemungkinan saya akan? Ketika Anda terganggu, Anda tidak tahu kapan itu awalnya terjadi, dan sehingga backup jarang digunakan; seseorang tidak bisa memastikan apakah backup berisi pintu belakang. Dengan demikian, tampaknya seperti satu-satunya cara untuk memastikan pemusnahan adalah untuk menghapus keadaan apapun mesin yang mungkin dikompromikan atau rusak, dan mulai dari awal. Namun, sebelum melakukannya, Anda harus melakukan yang terbaik untuk membuat salinan lengkap dari sistem dikompromikan untuk analisis forensik. Anda ingin mengidentifikasi vektor intrusi mungkin dan pastikan sistem baru tidak memiliki kerentanan yang sama, jangan sampai situasi terulang.

2This adalah respons standar untuk orang-orang yang mendirikan jammers dalam pertempuran militer. Jangan mencobanya di rumah.

85

18.2 Remnant data

? Dihapus? tapi tidak ditimpa.

?? IzzySoft ext3undel (http://projects.izzysoft.de/trac/ext3undel)

18.3 Ephemeral data

Seperti data dalam halaman? Le. Ini berharga karena orang biasanya tidak menyadari itu ada, dan jadi gagal untuk menghapus itu.

18.4 Remnant data

Seperti data baru-dihapus dalam dokumen Word. Rupanya itu hanya dump memori, eww. Ini menarik karena tidak biasanya terlihat.

18,5 Data Tersembunyi

Seperti UUIDs tertanam dalam dokumen ce MS O?. Hal ini bahkan dimungkinkan untuk mengidentifikasi komputer dari jarak jauh dengan TCP mereka jam condong (http://www.caida.org/ publikasi / makalah / 2005 / sidik jari /).

18,6 Metadata

Seperti waktu akses. Shimomura menggunakan akses kali untuk? Angka apa dikompilasi Mitnick.

?? Toolkit ini Koroner (http://www.porcupine.org/forensics/tct.html)

?? The Sleuth Kit (http://www.sleuthkit.org/)

18.7 Menemukan Kunci Enkripsi dan Encrypted data

?? Bermain Hide and Seek dengan Keys Tersimpan (http://www.cs.jhu.edu/~astubble/ 600,412 / sc-kertas / keys2.pdf)

86

18,8 Inference Forensik

Seringkali, apa menyebutkan statusnya? Es sebagai bukti di ruang sidang bukanlah hal yang sama Cian matematis menganggap bukti. Selanjutnya, dalam kasus perdata di AS Anda tidak perlu bukti, hanya dominan bukti. Dan kecerdasan (atau sekarang, terorisme) kewajiban-investigasi biasanya memiliki jauh lebih sedikit dari beban pembuktian. Dan bahkan jika Anda akan untuk bukti kuat, Anda hampir tidak pernah memulai penyelidikan dengan itu; itu sebabnya itu disebut penyelidikan. Dengan demikian, firasat yang cukup berharga.

Jika Anda percaya bahwa seseorang membunuh seseorang di dapur, dan ada tempat pemutih residu pada? Oor tetapi dalam pola hujan rintik-rintik darah, maka Anda cukup bisa berasumsi bahwa ia tidak hujan rintik-rintik pemutih pada dapur? Oor, walaupun itu adalah mungkin dalam teori. Jadi, jika melakukan hal A menyiratkan B, dan satu tidak mungkin untuk melakukan B saja, maka jika B ditunjukkan, seseorang dapat menyimpulkan kemungkinan A.

19 Privasi

? Anda memiliki nol privasi tetap. Dapatkan lebih dari itu.? ? Scott McNealy, CEO Sun Microsystems, 21 Jan 1999

19,1 Sistem Mix Berbasis

Sistem Mix berbasis dasarnya bergantung pada node memiliki beberapa input dan output, dan seorang pengamat luar tidak bisa membedakan mana peta yang karena mereka dienkripsi pada satu atau (idealnya) kedua belah pihak, dan mungkin ada penundaan acak antara input dan output. Kadang-kadang bercampur beroperasi dengan satu output bertepatan dengan satu input, sehingga sejumlah tra? C diperlukan untuk menyimpannya? Hidup ?. Tugas campuran adalah untuk menyembunyikan hubungan antara input pesan dan outputnya. Umumnya komunikasi keluar dari sistem campuran tidak terenkripsi, yang berarti node keluar memiliki lebih hak istimewa untuk melihat tra? C dari node lain dalam? Awan ?.

19.1.1 Anonymous remailers

Anonymous remailers berusaha untuk mail hal melalui jaringan membingungkan dalam upaya untuk menyembunyikan yang awalnya mengirim email.

?? http://en.wikipedia.org/wiki/Remailer

19.1.2 Massa

Massa berusaha untuk menyembunyikan individu tindakan browsing web di hub-bub kerumunan pengguna.

87

?? http://en.wikipedia.org/wiki/Crowds

19.1.3 Tor

The Onion Router (TOR) pada awalnya merupakan proyek militer yang diarahkan web tra? C sekitar dengan cara yang membingungkan.

?? http://www.torproject.org/

19,2 Distro

?? Tin Foil Hat Linux (http://tinfoilhat.shmoo.com/)

?? Anonym.OS (http://sourceforge.net/projects/anonym-os/)a

Please help Google Translate improve quality for your language here.

Google Terjemahan untuk Bisnis:Perangkat Penerjemah