Prinsip Keamanan Informasi

Bab 7 - Teknologi Keamanan: Intrusion Detection, Access Control, dan Keamanan Perangkat Lain

Berdasarkan Keempat Edisi:

ME Whitman, HJ Mattord :. *Prinsip Keamanan Informasi*

School of Business, Departemen Teknologi Informasi

Jangan menunggu; waktu tidak akan pernah *tepat.* Mulai di mana Anda berdiri, dan bekerja dengan alat apa pun yang Anda mungkin memiliki perintah Anda, dan alat yang lebih baik akan ditemukan sebagai Anda pergi bersama.

Napoleon Hill (1883-1970) Pendiri Ilmu Sukses

Tujuan Pembelajaran

- Mengidentifikasi dan menggambarkan kategori dan model operasi dari sistem deteksi intrusi
- De fi ne dan menjelaskan pot madu, jaring madu, dan sistem sel empuk
- Daftar dan mendefinisikan kategori utama scanning dan alat analisis, dan menjelaskan spesifik alat yang digunakan dalam masing-masing kategori ini
- Menjelaskan berbagai metode kontrol akses, termasuk penggunaan mekanisme akses biometrik

Garis besar

pengantar

- Perlindungan aset organisasi tergantung sebanyak pada orang sebagai kontrol teknis
- solusi teknis, dipandu oleh kebijakan dan benar dilaksanakan sangat penting untuk program keamanan informasi
- teknologi canggih dapat digunakan untuk meningkatkan keamanan aset informasi

Intrusion Detection dan Pencegahan Sistem

- Sebuah intrusi adalah jenis serangan terhadap aset informasi di mana upaya penghasut untuk mendapatkan masuk ke sistem atau mengganggu operasi normal sistem dengan, hampir selalu, maksud untuk membahayakan berbahaya

- Sebuah sistem pencegahan intrusi (IPS) terdiri dari kegiatan yang berusaha untuk mencegah penyusupan dari terjadi

- Sebuah sistem deteksi intrusi (IDS) terdiri dari prosedur dan sistem yang dibuat dan dioperasikan untuk mendeteksi intrusi sistem

- Syarat deteksi intrusi / sistem pencegahan (IDPS) dapat digunakan untuk menggambarkan teknologi anti-intrusi saat ini

Intrusion Detection dan Pencegahan Sistem

IDPS Terminologi

- Waspada atau Alarm: Indikasi bahwa sistem baru saja diserang dan / atau terus diserang
- Negatif palsu: Kegagalan sistem IDS untuk bereaksi terhadap suatu peristiwa serangan yang sebenarnya
- False Positive: Alarm atau peringatan yang menunjukkan bahwa serangan sedang berlangsung atau bahwa serangan telah berhasil terjadi ketika, pada kenyataannya, belum ada serangan seperti itu.
- Kebisingan: peristiwa alarm yang akurat dan penting, tetapi tidak menimbulkan fi kan ancaman signifikan bagi keamanan informasi.
  serangan yang gagal adalah sumber yang paling umum dari IDPS kebisingan

Intrusion Detection dan Pencegahan Sistem

IDPS Terminologi (cont.)

- Kebijakan situs: Aturan dan kontra fi pedoman gurasi yang mengatur pelaksanaan dan pengoperasian IDPSs dalam organisasi

- Kesadaran Kebijakan situs: kemampuan sebuah IDPS untuk secara dinamis memodifikasi kebijakan situsnya reaksi / respon terhadap aktivitas lingkungan

- Kepercayaan diri Nilai: Sebuah nilai yang terkait dengan kemampuan sebuah IDPS untuk mendeteksi dan mengidentifikasi serangan dengan benar

- Penyaringan Alarm: Proses mengklasifikasikan peringatan serangan bahwa IDPS menghasilkan untuk membedakan dan positif semacam palsu dari serangan yang sebenarnya lebih e sien FFI

Kuis cepat

1. Sebuah) _____ merupakan indikasi bahwa sistem baru saja menyerang dan / atau terus diserang.

   Menjawab:

Kuis cepat

1. Sebuah) _____ merupakan indikasi bahwa sistem baru saja menyerang dan / atau terus diserang.

   Menjawab: alert (atau alarm)

Kuis cepat

1. Sebuah) _____ merupakan indikasi bahwa sistem baru saja menyerang dan / atau terus diserang.

   Menjawab: alert (atau alarm)

2. _____ adalah kegagalan sistem deteksi intrusi (IDS) untuk bereaksi terhadap suatu peristiwa serangan yang sebenarnya.

   Menjawab:

Kuis cepat

1. Sebuah) _____ merupakan indikasi bahwa sistem baru saja menyerang dan / atau terus diserang.

   Menjawab: alert (atau alarm)

2. _____ adalah kegagalan sistem deteksi intrusi (IDS) untuk bereaksi terhadap suatu peristiwa serangan yang sebenarnya.

   Menjawab: salah negatif

Kuis cepat

1. Sebuah) _____ merupakan indikasi bahwa sistem baru saja menyerang dan / atau terus diserang.

   Menjawab: alert (atau alarm)

2. _____ adalah kegagalan sistem deteksi intrusi (IDS) untuk bereaksi terhadap suatu peristiwa serangan yang sebenarnya.

   Menjawab: salah negatif

3. _____ adalah alarm / peringatan yang menunjukkan bahwa serangan sedang berlangsung atau bahwa serangan telah berhasil terjadi ketika, pada kenyataannya, belum ada serangan seperti itu.

   Menjawab:

Kuis cepat

1. Sebuah) _____ merupakan indikasi bahwa sistem baru saja menyerang dan / atau terus diserang.

   Menjawab: alert (atau alarm)

2. _____ adalah kegagalan sistem deteksi intrusi (IDS) untuk bereaksi terhadap suatu peristiwa serangan yang sebenarnya.

   Menjawab: salah negatif

3. _____ adalah alarm / peringatan yang menunjukkan bahwa serangan sedang berlangsung atau bahwa serangan telah berhasil terjadi ketika, pada kenyataannya, belum ada serangan seperti itu.

   Menjawab: positif palsu

Mengapa Menggunakan sebuah IDPS?

- Mencegah masalah perilaku dengan meningkatkan risiko yang dirasakan penemuan dan hukuman
- menemukan serangan dan pelanggaran keamanan lainnya
- menemukan dan berurusan dengan preambles serangan
- Dokumen ancaman yang ada pada organisasi

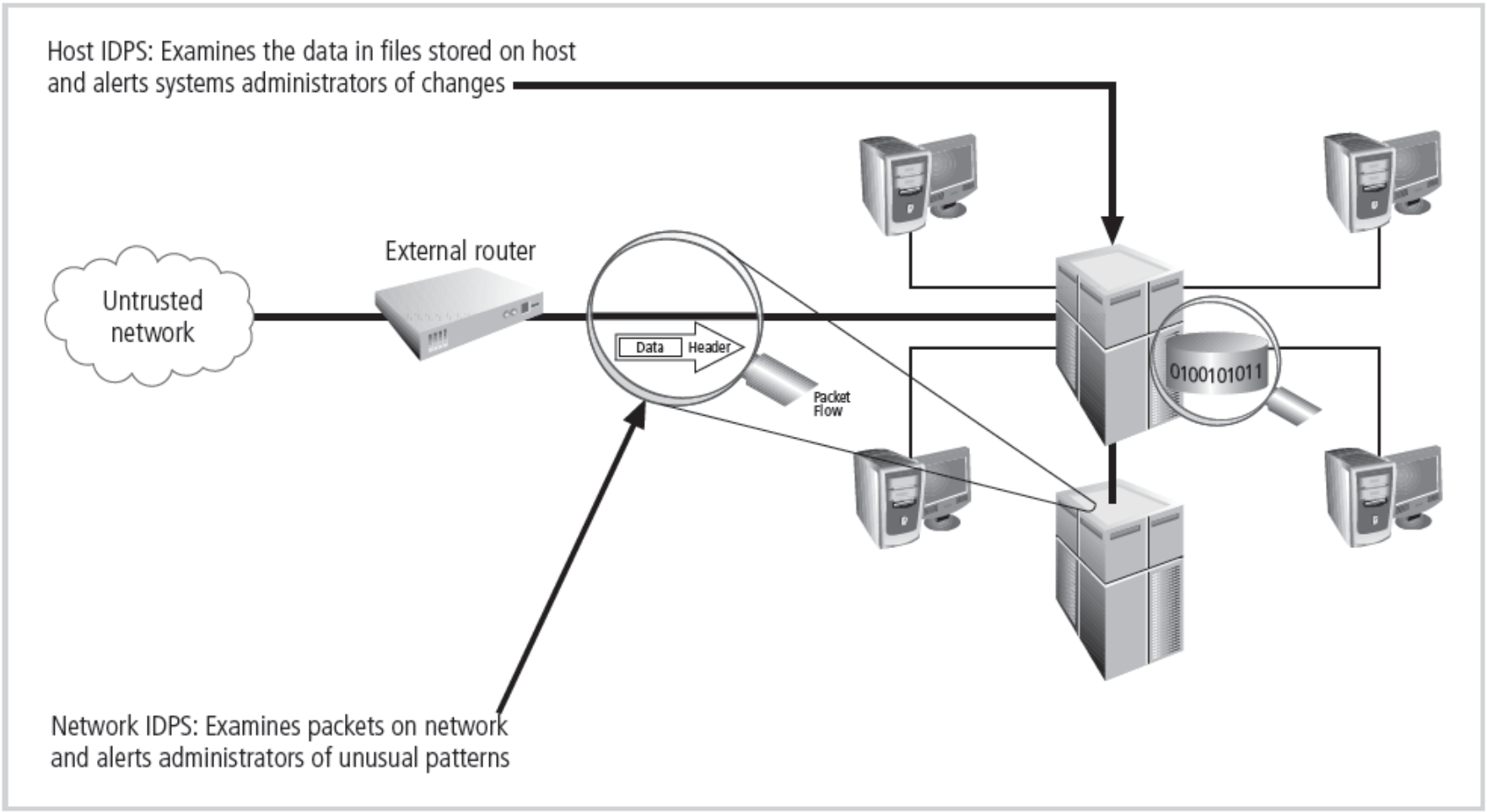
Mengapa Menggunakan sebuah IDPS?

- Mencegah masalah perilaku dengan meningkatkan risiko yang dirasakan penemuan dan hukuman
- menemukan serangan dan pelanggaran keamanan lainnya
- menemukan dan berurusan dengan preambles serangan
- Dokumen ancaman yang ada pada organisasi
- Bertindak sebagai kontrol kualitas untuk desain keamanan dan administrasi, terutama perusahaan besar dan kompleks
- Menyediakan informasi yang berguna tentang gangguan bahwa tempat take

Jenis IDP Systems (IDPS)

- IDPSs beroperasi sebagai jaringan berbasis atau berbasis host
- SEBUAH IDPS berbasis jaringan difokuskan pada melindungi aset informasi jaringan
- Dua subtipe khusus dari IDPS berbasis jaringan adalah:
  1. yang IDPS nirkabel
  2. analisis perilaku jaringan (NBA) IDPS
- SEBUAH IPDS berbasis host melindungi aset informasi server atau host

Jenis IDP Systems (IDPS)



Gambar 7-1 Intrusion Detection dan Pencegahan Sistem

Jenis IDP Systems (IDPS)

IDPS jaringan Berbasis (NIDPS)

- Resides di komputer atau alat yang terhubung ke segmen jaringan organisasi; terlihat tanda-tanda serangan
- Ketika memeriksa paket, sebuah NIDPS mencari pola serangan
- Dipasang di spesifik tempat dalam jaringan di mana ia dapat menonton tra FFI c masuk ke dan keluar dari segmen jaringan tertentu

Jenis IDP Systems (IDPS)

pencocokan tanda tangan NIDPS

- Untuk mendeteksi serangan, NIDPSs mencari pola serangan
- Hal ini dilakukan dengan pelaksanaan TCP / IP tumpukan yang menyerupai paket dan berlaku:
  - stack protokol veri protokol aplikasi fi kasi
  - verifikasi
- Dalam proses stack protokol verifikasi, NIDPSs mencari pelanggaran dalam struktur protokol paket , Sedangkan pada protokol aplikasi verifikasi penampilan untuk pelanggaran dalam penggunaan protokol paket .

Jenis IDP Systems (IDPS)

Keuntungan dari NIDPSs

- desain jaringan yang baik dan penempatan NIDPS perangkat dapat memungkinkan organisasi untuk menggunakan beberapa perangkat untuk memonitor jaringan besar
- NIDPSs adalah perangkat biasanya pasif dan dapat digunakan dalam jaringan yang ada dengan sedikit atau tanpa gangguan terhadap operasi jaringan yang normal
- NIDPSs biasanya tidak rentan terhadap serangan langsung dan mungkin tidak terdeteksi oleh penyerang

Jenis IDP Systems (IDPS)

Kekurangan dari NIDPSs

- Dapat menjadi kewalahan volume jaringan dan gagal untuk mengenali serangan
- Membutuhkan akses ke semua tra FFI c dipantau
- Tidak dapat menganalisis paket dienkripsi
- tidak dapat dipercaya memastikan apakah serangan itu berhasil atau tidak
- Beberapa bentuk serangan tidak mudah dilihat oleh NIDPSs, secara khusus yang melibatkan paket terfragmentasi

Jenis IDP Systems (IDPS)

- wireless NIDPS
  - Monitor dan analisis jaringan nirkabel tra FFI c
  - Masalah yang terkait dengan itu meliputi keamanan fisik, berbagai sensor, jalur akses dan lokasi switch nirkabel, koneksi jaringan kabel, biaya
- sistem analisis perilaku jaringan
  - Memeriksa jaringan tra FFI c untuk mengidentifikasi masalah yang terkait dengan aliran dari tra FFI c
  - Jenis acara umumnya terdeteksi termasuk serangan DoS, scanning, cacing, layanan aplikasi tak terduga, pelanggaran kebijakan

Jenis IDP Systems (IDPS)

IDPS Host-Based

- Resides pada komputer tertentu atau server dan monitor aktivitas hanya pada sistem yang
- Benchmark dan memantau status sistem kunci fi les dan mendeteksi ketika penyusup menciptakan, modi fi es, atau menghapus fi les
- Paling HIDPSs bekerja pada prinsip con fi gurasi atau manajemen perubahan
- Keuntungan atas NIDPS : Biasanya dapat diinstal sehingga dapat mengakses informasi dienkripsi saat bepergian melalui jaringan

Jenis IDP Systems (IDPS)

keuntungan HIDPS

- dapat mendeteksi acara lokal pada sistem host dan mendeteksi serangan yang mungkin menghindari sebuah IDPS berbasis jaringan
- fungsi pada sistem host, di mana dienkripsi tra FFI c akan telah didekripsi dan tersedia untuk pengolahan
- Bukan ff tercermin dengan menggunakan protokol jaringan diaktifkan
- dapat mendeteksi inkonsistensi dalam bagaimana aplikasi dan sistem program yang digunakan dengan memeriksa catatan yang disimpan dalam log audit

Jenis IDP Systems (IDPS)

Kekurangan dari HIDPS

- Pose isu-isu manajemen yang lebih
- rentan baik untuk mengarahkan serangan dan serangan terhadap sistem operasi host
- Tidak mendeteksi pemindaian multi-host, atau pemindaian perangkat jaringan non-tuan
- Rentan beberapa denial-of-service serangan
- Bisa menggunakan jumlah besar ruang disk
- Bisa di fl ik overhead kinerja pada sistem host

Metode Deteksi IDPS

- IDPSs menggunakan berbagai metode pendeteksian untuk memonitor dan mengevaluasi jaringan tra FFI c

- Tiga metode mendominasi:

  1. berbasis signature IDPS
  2. Statistik berbasis anomali IDPS
  3. IDPS inspeksi stateful packet

Metode Deteksi IDPS

Signature Berbasis IDPS

- Memeriksa data tra FFI c di mencari pola yang cocok diketahui tanda tangan
- Banyak digunakan karena banyak serangan memiliki tanda tangan yang jelas dan berbeda
- Masalah dengan pendekatan ini adalah bahwa sebagai strategi serangan baru diidentifikasi, database IDPS ini tanda tangan harus terus diperbarui

Metode Deteksi IDPS

IDPS statistik Anomali Berbasis

- Itu statistik anomali berbasis IDPS (Stat IDPS) aktivitas jaringan sampel untuk dibandingkan dengan tra FFI c yang dikenal menjadi normal

- Ketika aktivitas diukur adalah parameter dasar luar, IDPS akan memicu peringatan

- Keuntungan dari IDPS stat: dapat mendeteksi jenis serangan baru

- Kekurangan IDPS stat: Membutuhkan pengolahan kapasitas jauh lebih overhead dan dari berbasis signature. Juga, dapat menghasilkan banyak positif palsu.

Metode Deteksi IDPS

Stateful Protokol Analisis IDPS

- analisis protokol Stateful (SPA) adalah proses yang membandingkan telah ditentukan pro fi les dari definisi fi de aktivitas jinak untuk setiap negara protocol terhadap peristiwa yang diamati untuk mengidentifikasi penyimpangan
- SPA toko dan penggunaan data yang relevan terdeteksi dalam sesi untuk mengidentifikasi gangguan yang melibatkan beberapa permintaan / tanggapan; memungkinkan IDPS untuk lebih mendeteksi khusus, serangan multi-session
- kekurangan: kompleksitas analitis; pengolahan biaya overhead; mungkin gagal untuk mendeteksi kecuali protokol melanggar perilaku yang mendasar; dapat menyebabkan masalah dengan protokol itu memeriksa.

Metode Deteksi IDPS

Monitor Berkas log

- Log fi le Monitor (LFM) mirip dengan NIDPS
- Ulasan log fi les yang dihasilkan oleh server, perangkat jaringan, dan bahkan lainnya IDPSs pola dan tanda tangan
- Pola serangan secara nyata mungkin jauh lebih mudah untuk mengidentifikasi ketika seluruh jaringan dan sistem yang dipandang secara holistik
- Membutuhkan alokasi sumber daya yang cukup karena akan melibatkan pengumpulan, gerakan, penyimpanan, dan analisis jumlah besar data log

Perilaku IDPS Response

- Sekali IDPS mendeteksi situasi jaringan anomali, ia memiliki sejumlah pilihan

- IDPS tanggapan dapat diklasifikasikan sebagai aktif atau pasif
  - respon aktif: mengumpulkan informasi tambahan tentang gangguan itu, memodifikasi lingkungan jaringan, mengambil tindakan terhadap intrusi
  - respon pasif: pengaturan o alarm ff atau kation fi noti, pengumpulan data pasif melalui SNMP (Simple Network Management Protocol) perangkap

Memilih IDPS Pendekatan dan Produk

- Teknis dan kebijakan pertimbangan:
  - Apa lingkungan sistem Anda? Apa tujuan keamanan dan
  - tujuan? Apa kebijakan keamanan yang ada?
  -
- persyaratan organisasi dan kendala:
  - Apa saja persyaratan yang dipungut dari luar organisasi?
  - Apa kendala sumber daya organisasi Anda?

Memilih IDPS Pendekatan dan Produk

- IDPSs fitur produk dan kualitas:
  - Adalah produk su FFI sien terukur untuk lingkungan Anda? Bagaimana
  - produk diuji?
  - Bagaimana tingkat pengguna keahlian ditargetkan oleh produk? Adalah produk yang
  - dirancang untuk berkembang sebagai organisasi tumbuh? Apa saja ketentuan
  - dukungan untuk produk?

Kekuatan dari IDPSs

- Pemantauan dan analisis peristiwa sistem dan perilaku pengguna
- negara keamanan pengujian sistem con gurations fi
- keamanan negara baselining sistem dan perubahan pelacakan
- Mengenali pola peristiwa sistem serangan pencocokan dikenal
- Mengenali pola aktivitas yang bervariasi dari aktivitas normal

Keterbatasan IDPSs

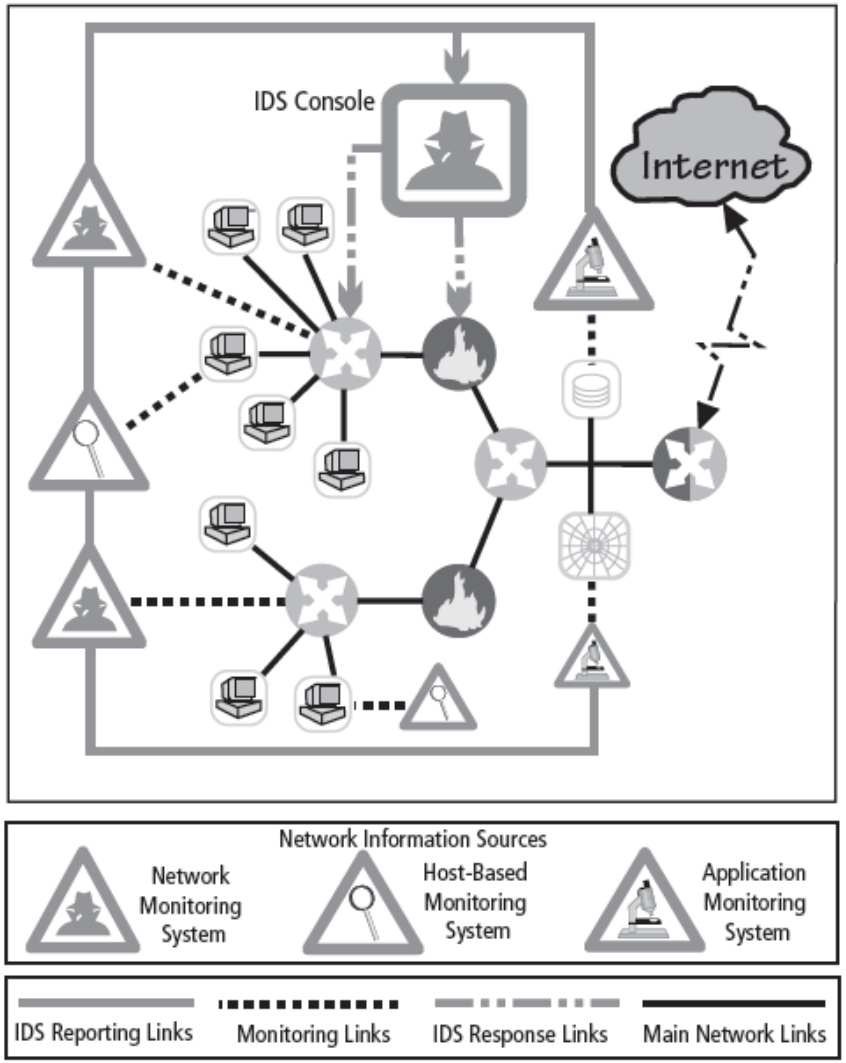
- Kompensasi untuk hilang mekanisme lemah / keamanan dalam infrastruktur perlindungan
- Seketika mendeteksi, melaporkan, menanggapi serangan ketika ada jaringan berat atau beban pengolahan
- Mendeteksi serangan baru atau varian serangan yang ada
- E ff ectively menanggapi serangan oleh penyerang canggih
- serangan menyelidiki tanpa campur tangan manusia

Deployment dan Implementasi dari IDPS

- Sebuah IDPS dapat diimplementasikan melalui salah satu tiga strategi kontrol dasar

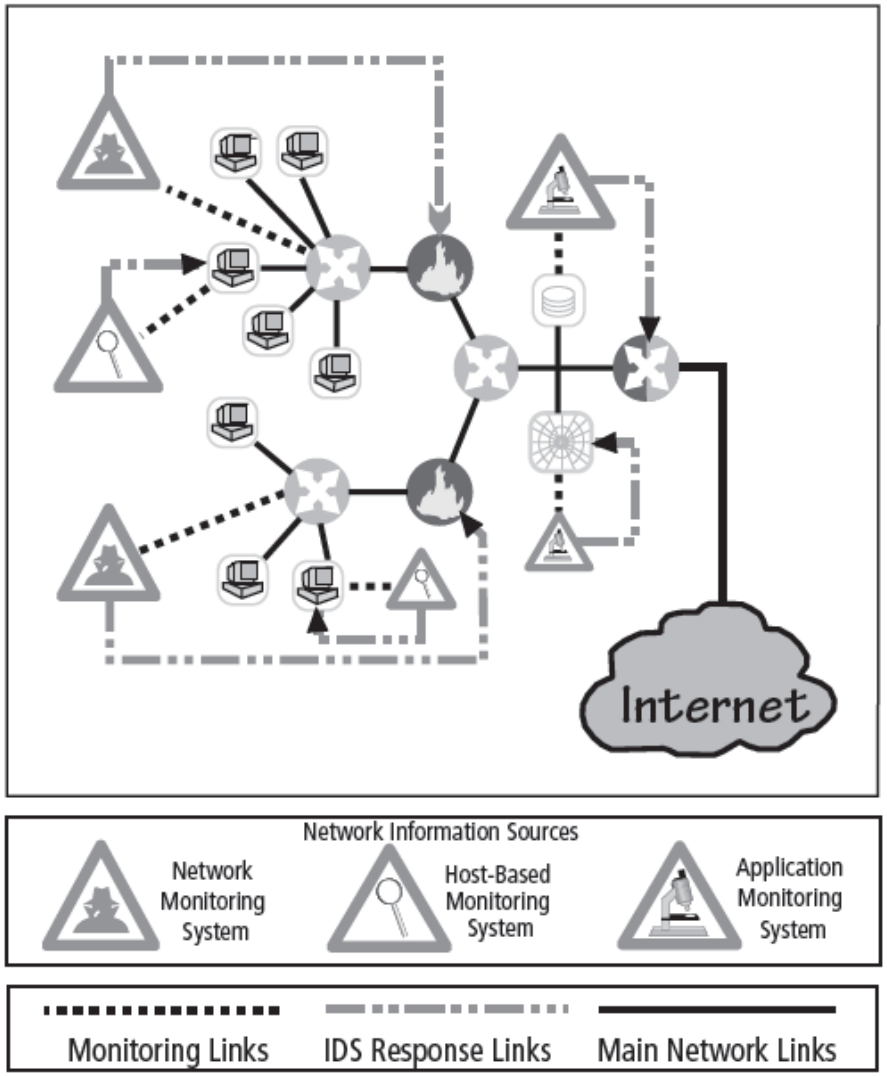
1. Terpusat: semua fungsi kontrol IDPS diimplementasikan dan dikelola di satu lokasi pusat
2. Sepenuhnya didistribusikan: semua fungsi kontrol yang diterapkan di lokasi fisik dari masing-masing komponen IDPS
3. Sebagian didistribusikan: menggabungkan dua; sementara agen individu masih bisa menganalisis dan merespon ancaman lokal, mereka melaporkan ke fasilitas pusat hirarkis untuk memungkinkan organisasi untuk mendeteksi serangan yang meluas

Deployment dan Implementasi dari IDPS



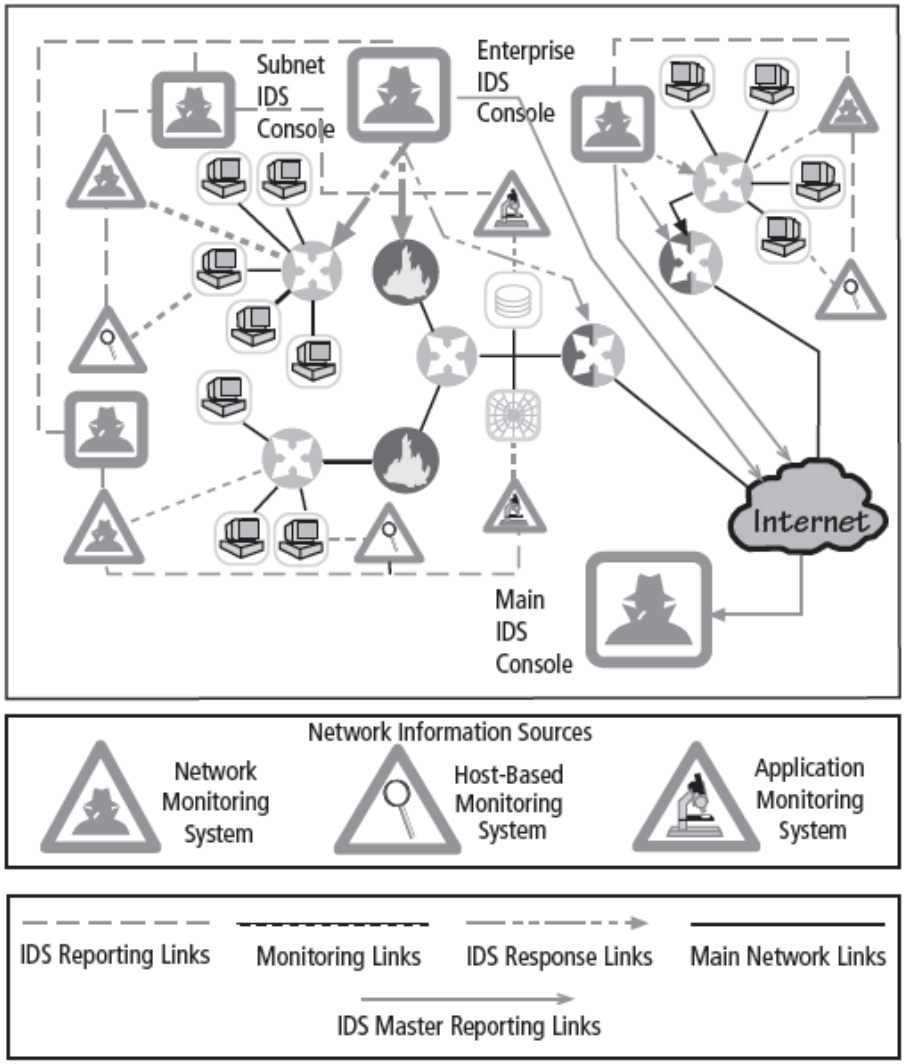
Gambar 7-4 Terpusat IDPS Kontrol [13]

Deployment dan Implementasi dari IDPS



Gambar 7-5 Fully Distributed IDPS Kontrol [14]

Deployment dan Implementasi dari IDPS



Gambar 7-6 sebagian Distributed IDPS Kontrol [15]

Deployment dan Implementasi dari IDPS

IDPS Deployment

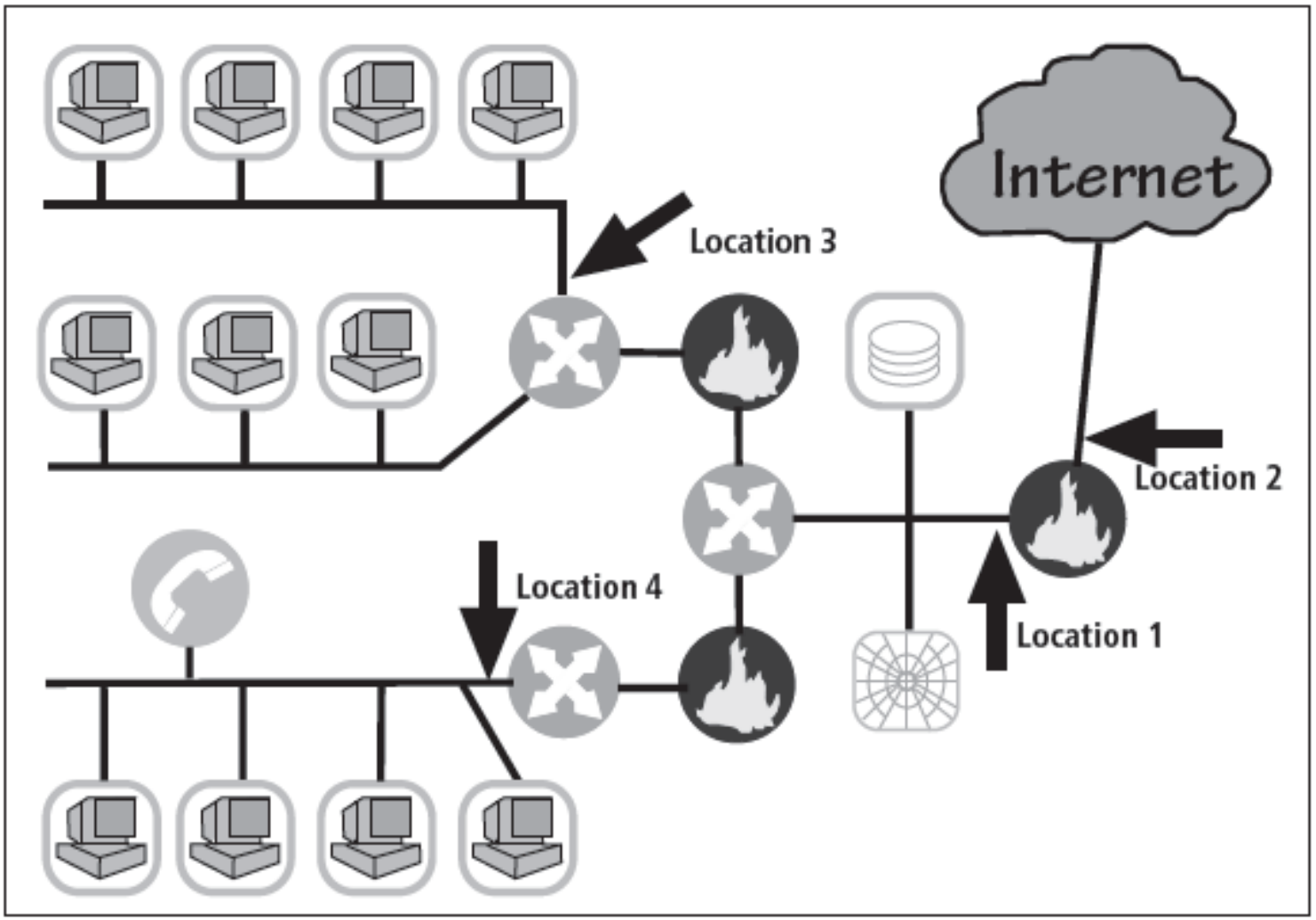
- Seperti keputusan tentang strategi pengendalian , Keputusan tentang di mana untuk menemukan unsur-unsur sistem deteksi intrusi dapat seni itu sendiri
- Perencana harus memilih strategi penyebaran yang didasarkan pada analisis yang cermat dari persyaratan keamanan informasi organisasi tetapi, pada saat yang sama, menyebabkan dampak minimal
- NIDPS dan HIDPS dapat digunakan bersama-sama untuk menutupi kedua sistem individual yang terhubung ke jaringan organisasi dan jaringan sendiri

Deployment dan Implementasi dari IDPS

IDPSs Menggelar Jaringan Berbasis

- NIST merekomendasikan empat lokasi untuk NIDPS sensor:
  1. Lokasi 1: Di balik setiap fi firewall eksternal, di DMZ jaringan
  2. Lokasi 2: Di luar sebuah fi firewall eksternal
  3. Lokasi 3: Pada tulang punggung jaringan utama
  4. Lokasi 4: Pada subnet kritis

Deployment dan Implementasi dari IDPS



Gambar 7-7 Jaringan IDPS Sensor Lokasi 17

Deployment dan Implementasi dari IDPS

Menyebarkan Host-Based IDPSs

- implementasi yang tepat dari HIDPSs bisa menjadi melelahkan dan tugas yang memakan waktu
- Deployment dimulai dengan menerapkan sebagian besar sistem kritis pertama
- Instalasi terus sampai baik semua sistem dipasang atau mencapai organisasi yang direncanakan tingkat cakupan itu bersedia untuk hidup dengan

Kuis cepat

1. _____ melibatkan kegiatan yang mengumpulkan informasi tentang organisasi dan kegiatan jaringan dan aset.

   Menjawab:

Kuis cepat

1. _____ melibatkan kegiatan yang mengumpulkan informasi tentang organisasi dan kegiatan jaringan dan aset.

   Menjawab: footprinting

Kuis cepat

1. _____ melibatkan kegiatan yang mengumpulkan informasi tentang organisasi dan kegiatan jaringan dan aset.

   Menjawab: footprinting

2. Benar atau salah: berbasis signature teknologi IDPS secara luas digunakan karena banyak serangan memiliki tanda tangan yang jelas dan berbeda.

   Menjawab:

Kuis cepat

1. _____ melibatkan kegiatan yang mengumpulkan informasi tentang organisasi dan kegiatan jaringan dan aset.

   Menjawab: footprinting

2. Benar atau salah: berbasis signature teknologi IDPS secara luas digunakan karena banyak serangan memiliki tanda tangan yang jelas dan berbeda.

   Menjawab: Benar

Kuis cepat

1. _____ melibatkan kegiatan yang mengumpulkan informasi tentang organisasi dan kegiatan jaringan dan aset.

   Menjawab: footprinting

2. Benar atau salah: berbasis signature teknologi IDPS secara luas digunakan karena banyak serangan memiliki tanda tangan yang jelas dan berbeda.

   Menjawab: Benar

3. Dalam (n) _____ IDPS strategi pengendalian, semua kontrol IDPSs fungsi diimplementasikan dan dikelola di satu lokasi pusat.

   Menjawab:

Kuis cepat

1. _____ melibatkan kegiatan yang mengumpulkan informasi tentang organisasi dan kegiatan jaringan dan aset.

   Menjawab: footprinting

2. Benar atau salah: berbasis signature teknologi IDPS secara luas digunakan karena banyak serangan memiliki tanda tangan yang jelas dan berbeda.

   Menjawab: Benar

3. Dalam (n) _____ IDPS strategi pengendalian, semua kontrol IDPSs fungsi diimplementasikan dan dikelola di satu lokasi pusat.

   Menjawab: terpusat

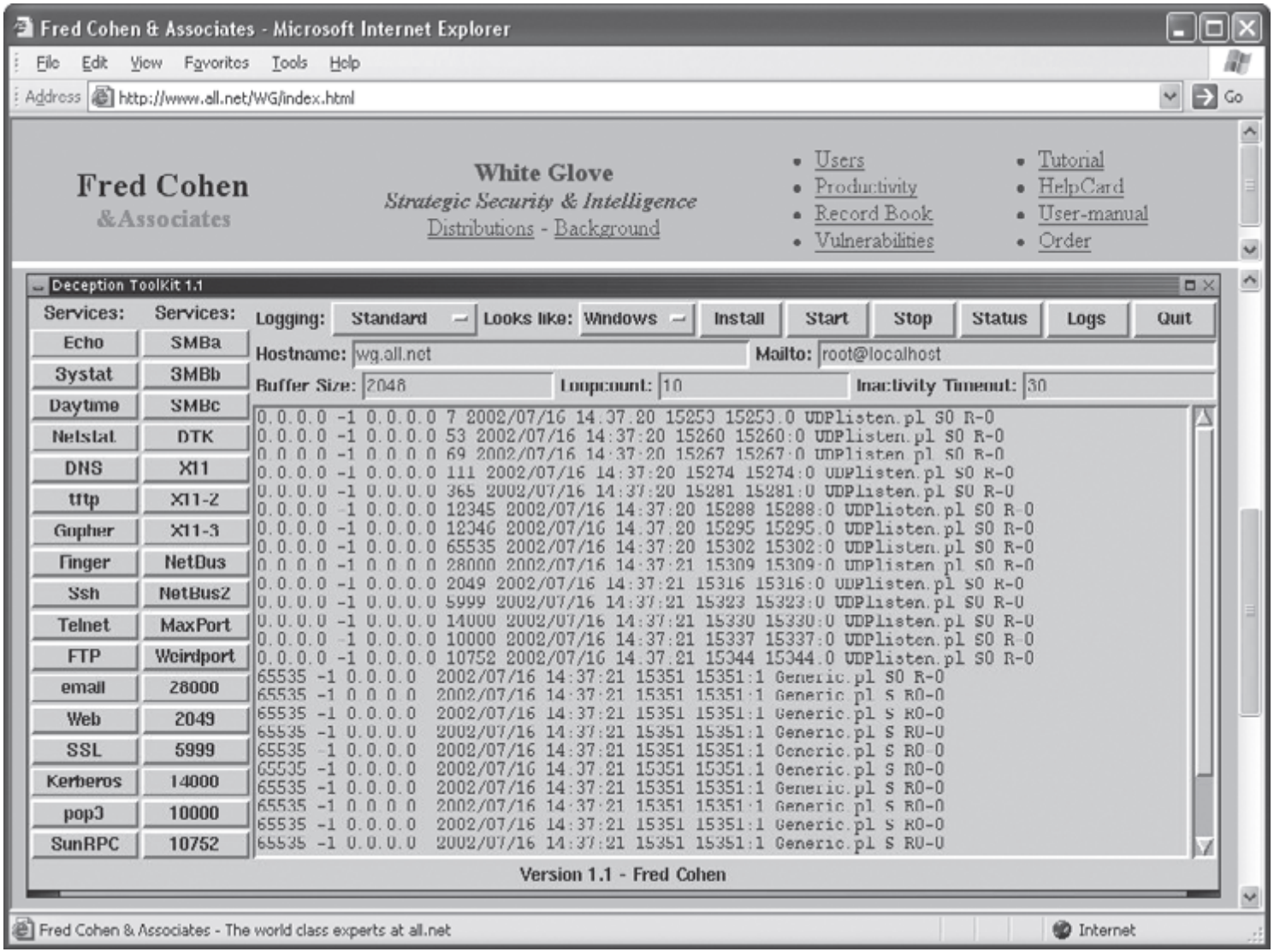
Honeypots, Honeynets, dan Sistem Sel Padded

- honeypots: Sistem umpan yang dirancang untuk memikat calon penyerang jauh dari sistem kritis dan mendorong serangan terhadap diri mereka sendiri

- Honeynets: koleksi honeypots menghubungkan beberapa sistem madu pot pada subnet

- Honeypots dirancang untuk:
  - Alihkan penyerang dari mengakses sistem kritis Mengumpulkan informasi
  - tentang aktivitas penyerang Mendorong penyerang untuk tetap pada sistem
  - cukup lama bagi administrator untuk acara dokumen dan, mungkin, merespon

Honeypots, Honeynets, dan Sistem Sel Padded



Gambar 7-8 Deception Toolkit

Honeypots, Honeynets, dan Sistem Sel Padded

- SEBUAH sel yg diberi lapisan-lapisan empuk adalah pot madu yang telah dilindungi sehingga tidak dapat dengan mudah dikompromikan
- Selain menarik penyerang dengan menggoda data, sebuah sel empuk beroperasi di tandem dengan tradisional IDS
- Ketika IDS mendeteksi penyerang, mulus transfer mereka untuk lingkungan khusus simulasi di mana mereka dapat menyebabkan tidak membahayakan -the sifat lingkungan host ini adalah apa yang memberi mendekati sel empuk nama

Honeypots, Honeynets, dan Sistem Sel Padded

Keuntungan

- Penyerang dapat dialihkan ke target bahwa mereka tidak dapat merusak
- Administrator memiliki waktu untuk memutuskan bagaimana merespon penyerang
- tindakan penyerang dapat dengan mudah dan lebih luas dipantau, dan catatan dapat digunakan untuk kembali model ancaman fi ne dan meningkatkan perlindungan sistem
- Madu pot mungkin e ff efektif pada penangkapan orang dalam yang mengintai di sekitar jaringan

Honeypots, Honeynets, dan Sistem Sel Padded

kekurangan

- implikasi hukum dari menggunakan perangkat tersebut tidak baik de fi ned
- Honeypots dan sel empuk belum terbukti teknologi keamanan umum yang bermanfaat
- Seorang penyerang ahli, setelah dialihkan ke dalam sistem umpan, mungkin menjadi marah dan meluncurkan serangan lebih bermusuhan terhadap sistem organisasi
- Administrator dan manajer keamanan akan membutuhkan tingkat keahlian yang tinggi untuk menggunakan sistem ini

Perangkap dan Trace Sistem

- Perangkap dan jejak sistem menggunakan kombinasi teknik untuk mendeteksi insiden intrusi dan jejak kembali ke sumber mereka
- Perangkap biasanya terdiri dari madu pot atau sel empuk dan alarm
- kelemahan hukum untuk menjebak dan jejak:
  - Daya tarik: proses menarik perhatian ke sistem dengan menempatkan menggiurkan bit informasi di lokasi kunci
  - jebakan: aksi memikat seseorang ke dalam melakukan kejahatan untuk mendapatkan keyakinan
  - Bujukan adalah hukum dan etika, sedangkan jeratan tidak

Aktif Intrusion Prevention

- Beberapa organisasi melaksanakan penanggulangan aktif untuk serangan berhenti
- **Salah satu alat (LaBrea) Mengambil terpakai AKU P ruang alamat untuk berpura-pura menjadi** komputer dan memungkinkan penyerang untuk menyelesaikan permintaan sambungan, tapi kemudian memegang sambungan terbuka

Kuis cepat

1. _____ adalah umpan sistem yang dirancang untuk memikat calon penyerang jauh dari sistem kritis.

   Menjawab:

Kuis cepat

1. _____ adalah umpan sistem yang dirancang untuk memikat calon penyerang jauh dari sistem kritis.

   Menjawab: honeypots

Kuis cepat

1. _____ adalah umpan sistem yang dirancang untuk memikat calon penyerang jauh dari sistem kritis.

   Menjawab: honeypots

2. _____ adalah kumpulan pot madu yang menghubungkan beberapa sistem madu pot pada subnet.

   Menjawab:

Kuis cepat

1. _____ adalah umpan sistem yang dirancang untuk memikat calon penyerang jauh dari sistem kritis.

   Menjawab: honeypots

2. _____ adalah kumpulan pot madu yang menghubungkan beberapa sistem madu pot pada subnet.

   Menjawab: jaring madu

Kuis cepat

1. _____ adalah umpan sistem yang dirancang untuk memikat calon penyerang jauh dari sistem kritis.

   Menjawab: honeypots

2. _____ adalah kumpulan pot madu yang menghubungkan beberapa sistem madu pot pada subnet.

   Menjawab: jaring madu

3. Sebuah) _____ adalah pot madu yang telah dilindungi sehingga tidak dapat dengan mudah dikompromikan.

   Menjawab:

Kuis cepat

1. _____ adalah umpan sistem yang dirancang untuk memikat calon penyerang jauh dari sistem kritis.

   Menjawab: honeypots

2. _____ adalah kumpulan pot madu yang menghubungkan beberapa sistem madu pot pada subnet.

   Menjawab: jaring madu

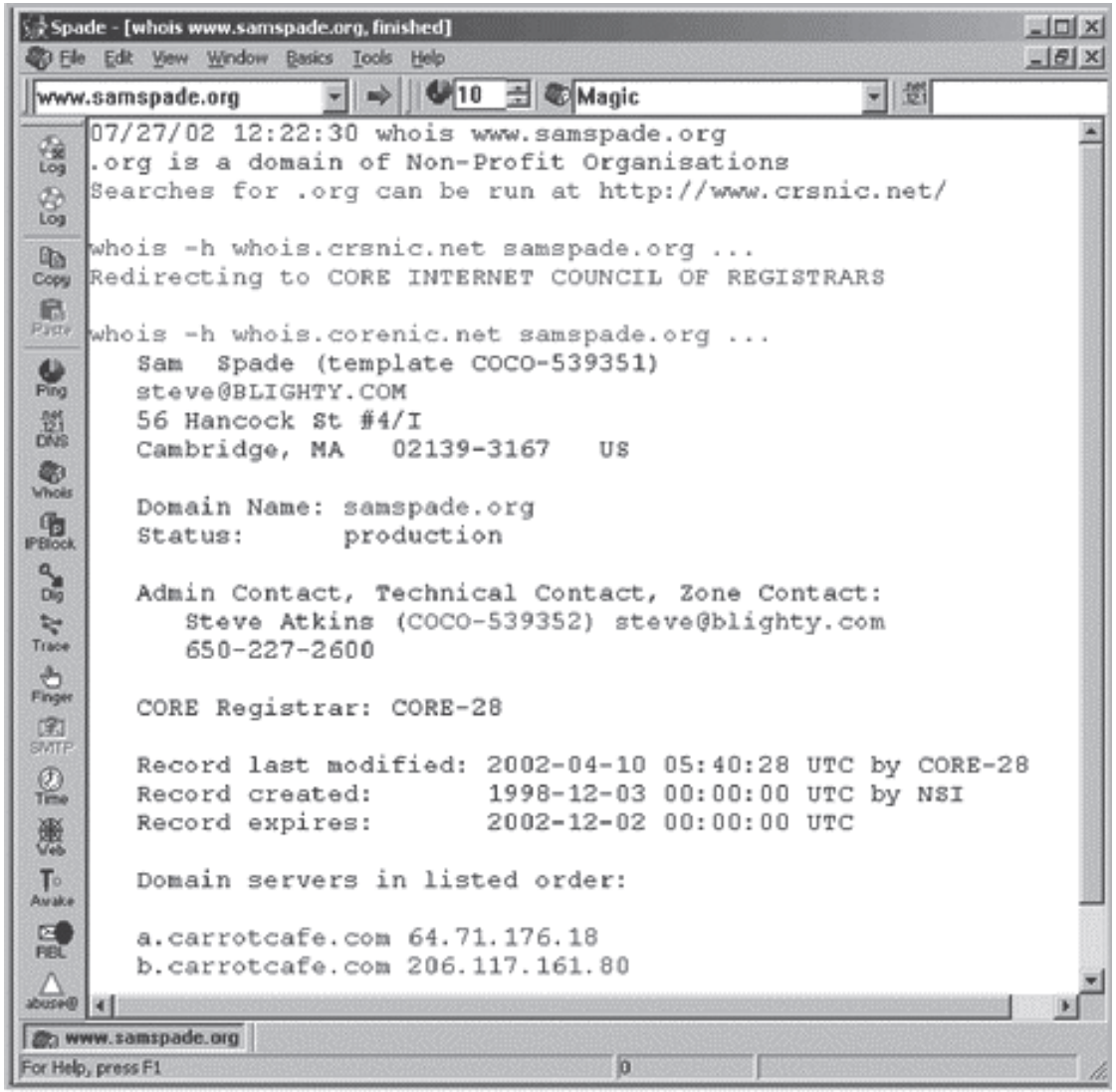
3. Sebuah) _____ adalah pot madu yang telah dilindungi sehingga tidak dapat dengan mudah dikompromikan.

   Menjawab: sel yg diberi lapisan-lapisan empuk

Scanning dan Alat Analisis

- Biasanya digunakan untuk Informasi mengumpulkan bahwa penyerang akan perlu untuk memulai serangan yang sukses
- protokol serangan serangkaian langkah atau proses yang digunakan oleh penyerang, dalam urutan logis, serangan peluncuran terhadap sistem target atau jaringan
- footprinting: penelitian terorganisir alamat Internet yang dimiliki atau dikendalikan oleh organisasi target

Scanning dan Alat Analisis



Gambar 7-9 Sam Spade

Scanning dan Alat Analisis (cont.)

- fingerprinting: survei sistematis semua alamat Internet sasaran organisasi yang dikumpulkan selama fase footprinting
- Fingerprinting mengungkapkan informasi yang berguna tentang struktur internal dan alam operasional sistem target atau jaringan untuk serangan diantisipasi
- Alat ini berharga untuk bek jaringan karena mereka dapat dengan cepat menentukan bagian-bagian dari sistem atau jaringan yang memerlukan perbaikan cepat untuk menutup kerentanan

Port Scanner

- Alat yang digunakan oleh kedua penyerang dan pembela untuk mengidentifikasi komputer aktif pada jaringan dan informasi berguna lainnya
- Dapat memindai untuk jenis spesifik dari komputer, protokol, atau sumber daya, atau scan mereka dapat generik
- Semakin spesifik scanner adalah, semakin baik dapat memberikan penyerang dan pembela informasi yang berguna

Scanning dan Alat Analisis

TCP Port Numbers	TCP Service
20 and 21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name Services (DNS)
67 and 68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol (POP3)
161	Simple Network Management Protocol (SNMP)
194	IRC chat port (used for device sharing)
443	HTTP over SSL
8080	Used for proxy services

Tabel 7-1 Pilih Umum Digunakan Nomor Port

Analisis firewall Alat

- Beberapa alat mengotomatisasi penemuan terpencil aturan firewall fi dan membantu administrator dalam menganalisa mereka
- Administrator yang merasa waspada menggunakan alat yang sama yang penyerang penggunaan harus ingat:
  - Ini adalah niat dari pengguna yang akan menentukan bagaimana informasi yang dikumpulkan akan digunakan
  - Dalam rangka untuk mempertahankan komputer atau jaringan dengan baik, perlu untuk memahami cara-cara itu bisa diserang
- Sebuah alat yang dapat membantu menutup terbuka atau buruk con fi gured fi firewall akan membantu jaringan bek meminimalkan risiko dari serangan

Sistem Operasi Deteksi Alat

- Mendeteksi komputer target Sistem operasi (OS) sangat berharga untuk seorang penyerang
- Ada banyak alat-alat yang menggunakan protokol jaringan untuk menentukan remote komputer OS
- seperti kebanyakan OS memiliki cara unik untuk menanggapi ICMP (Internet Control Message Protocol) permintaan, alat-alat ini sangat handal dalam fi nding pertandingan dan dengan demikian mendeteksi OS dari komputer remote.

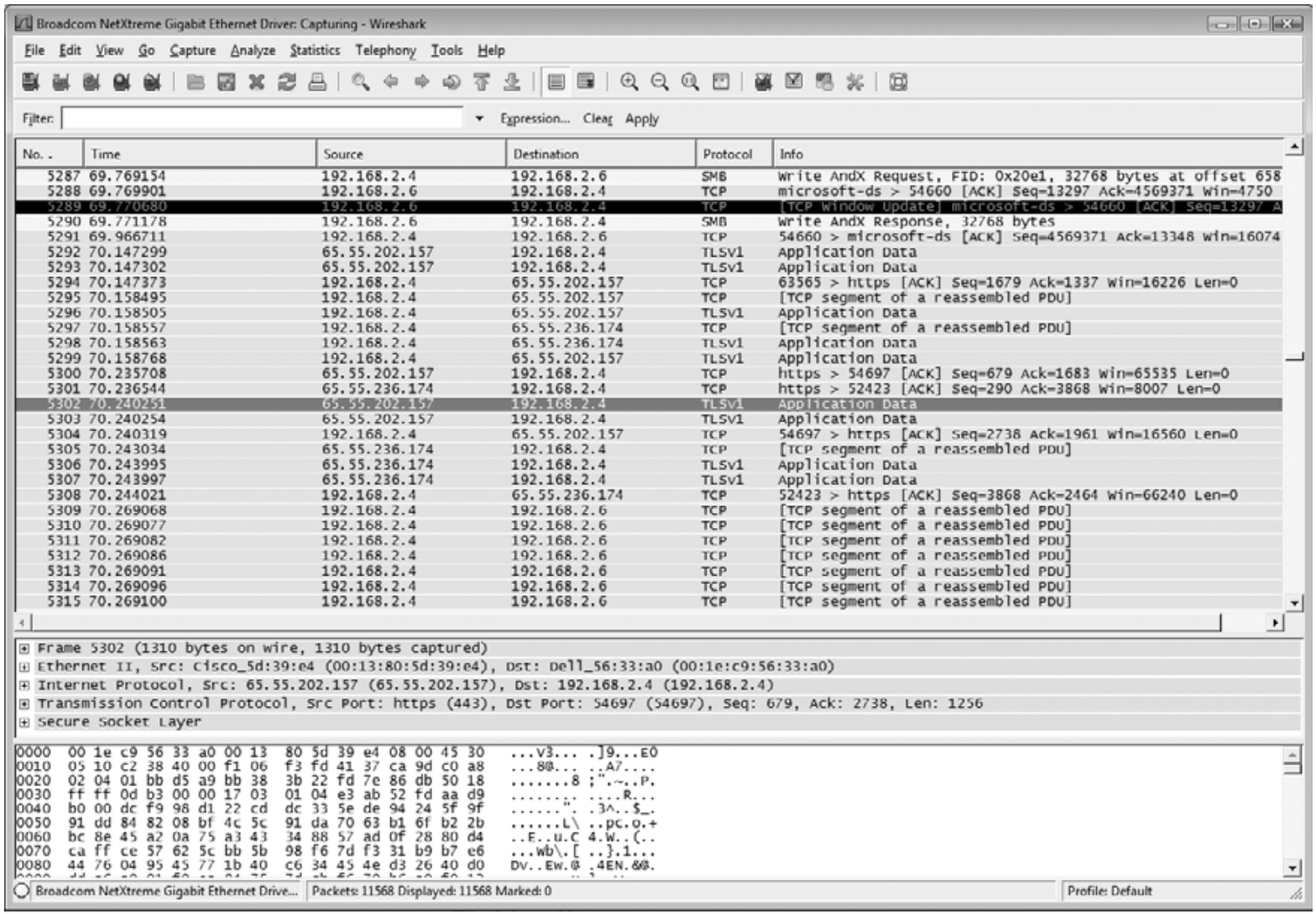
Scanner kerentanan

- scanner kerentanan aktif jaringan scan informasi sangat rinci; memulai tra FFI c untuk menentukan lubang
- scanner kerentanan pasif mendengarkan pada jaringan dan menentukan versi rentan dari kedua server dan client software
- scanner kerentanan pasif memiliki kemampuan untuk mendapati sisi klien kerentanan biasanya tidak ditemukan dalam scanner aktif

Packet Sni ff ers

- SEBUAH packet sni ff er adalah alat jaringan yang mengumpulkan salinan paket dari jaringan dan analisis mereka
- Hal ini dapat memberikan administrator jaringan informasi berharga untuk mendiagnosis dan mengatasi masalah jaringan
- Di tangan yang salah, a ff er sni dapat digunakan untuk menguping pada jaringan tra FFI c
- Menggunakan packet sni ff er secara hukum, administrator harus berada di jaringan bahwa organisasi memiliki, berada di bawah otorisasi langsung dari pemilik jaringan, dan memiliki pengetahuan dan persetujuan dari pencipta konten

Packet Sni ff ers



Gambar 7-17 Wireshark

Scanning dan Alat Analisis (cont.)

Keamanan Wireless Tools

- Sebuah organisasi yang menghabiskan semua waktunya mengamankan jaringan kabel dan daun jaringan nirkabel untuk beroperasi dengan cara apapun adalah membuka dirinya untuk pelanggaran keamanan
- Sebagai seorang profesional keamanan, Anda harus menilai risiko jaringan nirkabel
- SEBUAH toolkit keamanan nirkabel harus mencakup kemampuan untuk sni ff nirkabel tra FFI c, memindai host nirkabel, dan menilai tingkat privasi atau kerahasiaan sebuah ff orded pada jaringan nirkabel

Kuis cepat

1. **Benar atau salah:** Sebuah toolkit keamanan nirkabel harus mencakup

   kemampuan untuk sni ff nirkabel tra FFI c, memindai host nirkabel, dan menilai tingkat privasi atau kerahasiaan sebuah ff orded pada jaringan nirkabel.

   Menjawab:

Kuis cepat

1. Benar atau salah: Sebuah toolkit keamanan nirkabel harus mencakup

   kemampuan untuk sni ff nirkabel tra FFI c, memindai host nirkabel, dan menilai tingkat privasi atau kerahasiaan sebuah ff orded pada jaringan nirkabel.

   Menjawab: Benar

Kuis cepat

1. Benar atau salah: Sebuah toolkit keamanan nirkabel harus mencakup

   kemampuan untuk sni ff nirkabel tra FFI c, memindai host nirkabel, dan menilai tingkat privasi atau kerahasiaan sebuah ff orded pada jaringan nirkabel.

   Menjawab: Benar

2. _____ adalah penelitian yang terorganisir dari alamat Internet yang dimiliki atau dikendalikan oleh organisasi sasaran.

   Menjawab:

Kuis cepat

1. Benar atau salah: Sebuah toolkit keamanan nirkabel harus mencakup

   kemampuan untuk sni ff nirkabel tra FFI c, memindai host nirkabel, dan menilai tingkat privasi atau kerahasiaan sebuah ff orded pada jaringan nirkabel.

   Menjawab: Benar

2. _____ adalah penelitian yang terorganisir dari alamat Internet yang dimiliki atau dikendalikan oleh organisasi sasaran.

   Menjawab: footprinting

Kuis cepat

1. Benar atau salah: Sebuah toolkit keamanan nirkabel harus mencakup kemampuan untuk sni ff nirkabel tra FFI c, memindai host nirkabel, dan menilai tingkat privasi atau kerahasiaan sebuah ff orded pada jaringan nirkabel.

   Menjawab: Benar

2. _____ adalah penelitian yang terorganisir dari alamat Internet yang dimiliki atau dikendalikan oleh organisasi sasaran.

   Menjawab: footprinting

3. Sebuah) _____ adalah alat jaringan yang mengumpulkan salinan paket dari jaringan dan analisis mereka.

   Menjawab:

Kuis cepat

1. Benar atau salah: Sebuah toolkit keamanan nirkabel harus mencakup kemampuan untuk sni ff nirkabel tra FFI c, memindai host nirkabel, dan menilai tingkat privasi atau kerahasiaan sebuah ff orded pada jaringan nirkabel.

   Menjawab: Benar

2. _____ adalah penelitian yang terorganisir dari alamat Internet yang dimiliki atau dikendalikan oleh organisasi sasaran.

   Menjawab: footprinting

3. Sebuah) _____ adalah alat jaringan yang mengumpulkan salinan paket dari jaringan dan analisis mereka.

   Menjawab: packet sni ff er

Kontrol Biometric Access

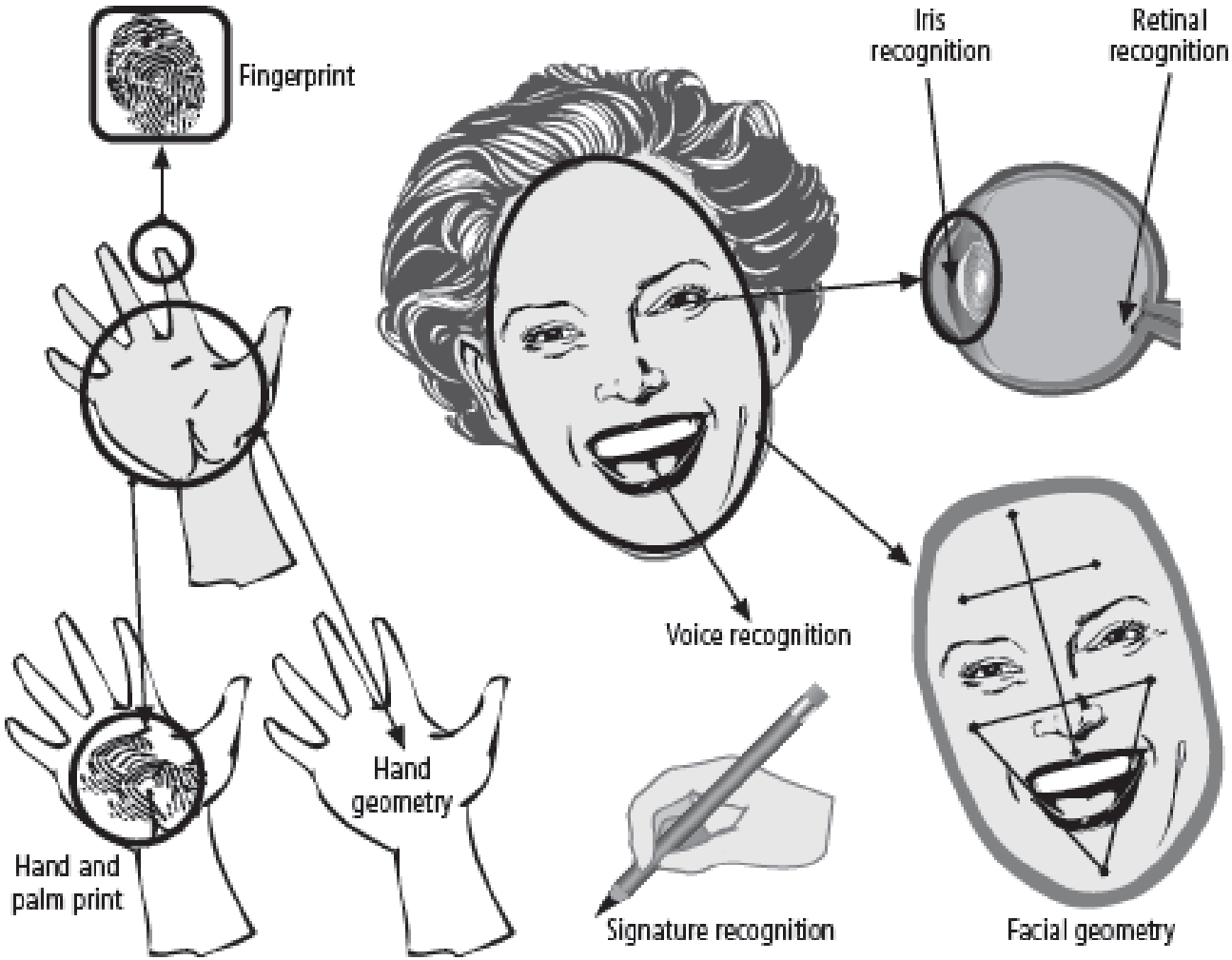
- Berdasarkan penggunaan beberapa karakteristik manusia terukur atau sifat untuk mengotentikasi identitas pengguna sistem yang diusulkan (a pemohon)

- Bergantung pada pengakuan

- termasuk fi ngerprint perbandingan, perbandingan cetak sawit, geometri tangan, pengenalan wajah menggunakan kartu id fotografi atau kamera digital, cetak retina, iris pola

- Karakteristik dianggap benar-benar unik: sidik jari, retina mata, iris mata

Kontrol Biometric Access



Karakteristik Gambar 7-20 Biometric Recognition

E ff efektivitas dari Biometrics

- teknologi biometrik dievaluasi tiga kriteria dasar:
  1. Salah afkir: penolakan pengguna yang sah
  2. Salah menerima tingkat: penerimaan pengguna yang tidak diketahui
  3. tingkat kesalahan Crossover (CER): titik di mana palsu menolak dan palsu menerima tarif menyeberang ketika grafiknya

Akseptabilitas Biometrics

- SEBUAH keseimbangan harus dicapai antara bagaimana diterima sistem keamanan adalah untuk para penggunanya dan bagaimana e ff efektif itu adalah dalam menjaga keamanan
- Banyak sistem biometrik yang sangat handal dan e ff efektif dianggap membosankan
- Akibatnya, banyak profesional keamanan informasi, dalam sebuah e ff ort untuk menghindari konfrontasi dan kemungkinan boikot pengguna kontrol biometrik, tidak menerapkannya

Akseptabilitas Biometrics

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand Vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L

Tabel 7-3 Peringkat dari Biometric Efektivitas dan Penerimaan H = Tinggi, M = Medium, L = Rendah

Direproduksi dari The '123' dari Biometric Technology, 2003, oleh Yun, Yau Wei [22]

Kuis cepat

1. _____ adalah tingkat di mana pengguna otentik ditolak atau dicegah akses ke daerah-daerah yang berwenang.

   Menjawab:

Kuis cepat

1. _____ adalah tingkat di mana pengguna otentik ditolak atau dicegah akses ke daerah-daerah yang berwenang.

   Menjawab: Salah afkir

Kuis cepat

1. _____ adalah tingkat di mana pengguna otentik ditolak atau dicegah akses ke daerah-daerah yang berwenang.

   Menjawab: Salah afkir

2. _____ adalah tingkat di mana pengguna tidak sah diizinkan akses ke sistem atau daerah.

   Menjawab:

Kuis cepat

1. _____ adalah tingkat di mana pengguna otentik ditolak atau dicegah akses ke daerah-daerah yang berwenang.

   Menjawab: Salah afkir

2. _____ adalah tingkat di mana pengguna tidak sah diizinkan akses ke sistem atau daerah.

   Menjawab: Salah menerima tingkat

Kuis cepat

1. _____ adalah tingkat di mana pengguna otentik ditolak atau dicegah akses ke daerah-daerah yang berwenang.

   Menjawab: Salah afkir

2. _____ adalah tingkat di mana pengguna tidak sah diizinkan akses ke sistem atau daerah.

   Menjawab: Salah menerima tingkat

3. _____ adalah tingkat di mana jumlah penolakan palsu sama dengan jumlah akseptasi palsu (tingkat kesalahan yang sama).

   Menjawab:

Kuis cepat

1. _____ adalah tingkat di mana pengguna otentik ditolak atau dicegah akses ke daerah-daerah yang berwenang.

   Menjawab: Salah afkir

2. _____ adalah tingkat di mana pengguna tidak sah diizinkan akses ke sistem atau daerah.

   Menjawab: Salah menerima tingkat

3. _____ adalah tingkat di mana jumlah penolakan palsu sama dengan jumlah akseptasi palsu (tingkat kesalahan yang sama).

   Menjawab: tingkat kesalahan Crossover (CER)

Kuis cepat

1. _____ adalah tingkat di mana pengguna otentik ditolak atau dicegah akses ke daerah-daerah yang berwenang.

   Menjawab: Salah afkir

2. _____ adalah tingkat di mana pengguna tidak sah diizinkan akses ke sistem atau daerah.

   Menjawab: Salah menerima tingkat

3. _____ adalah tingkat di mana jumlah penolakan palsu sama dengan jumlah akseptasi palsu (tingkat kesalahan yang sama).

   Menjawab: tingkat kesalahan Crossover (CER)

4. Benar atau salah: Banyak sistem biometrik yang sangat handal dan e ff efektif dianggap agak mengganggu untuk pengguna.

   Menjawab:

Kuis cepat

1. _____ adalah tingkat di mana pengguna otentik ditolak atau dicegah akses ke daerah-daerah yang berwenang.

   Menjawab: Salah afkir

2. _____ adalah tingkat di mana pengguna tidak sah diizinkan akses ke sistem atau daerah.

   Menjawab: Salah menerima tingkat

3. _____ adalah tingkat di mana jumlah penolakan palsu sama dengan jumlah akseptasi palsu (tingkat kesalahan yang sama).

   Menjawab: tingkat kesalahan Crossover (CER)

4. Benar atau salah: Banyak sistem biometrik yang sangat handal dan e ff efektif dianggap agak mengganggu untuk pengguna.

   Menjawab: Benar

Sumber daya tambahan

1. Sangat halus

   http://www.ethereal.com

2. Kontrol acdcess Digital Personal Biometric

   http://www.digitalpersona.com

3. LaBrea “Sticky Honeynet”

   http://labrea.sourceforge.net

4. Berbasis host Intrusion Prevention

   http://netsecurity.about.com/cs/ fi rewallbooks / a / aa050804.htm