UAS Keamanan Informasi Kelas TI-PAGI

NAMA : HILDA ALFIANA NOVELASARI
NIM : 1310651084
KELAS : D

1. Aspek keamanan informasi mempunyai ruang lingkup yang luas. Menurut referensi dari ebook CISSP, ruang lingkup materi dari keamanan informasi terdiri dari 10 pokok permasalahan. Dari 10 pokok permasalahan tersebut, silakan buatlah resume salah satu pokok permasalahan dari keamanan informasi mengacu terhadap ebook CISSP yang sudah saya upload di elearning. Resume bukan hasil translate, melainkan inti-intinya saja dari materi yang sudah Anda pahami pada ebook tersebut. Hasil resume tidak boleh sama dengan teman-temannya, akan tetapi tema yang dibahas boleh sama.

Domain 3 : Information Security Governance and Risk Management (informasi Tata Kelola Keamanan dan Manajemen Risiko)

CHAPTER 3

Tugas profesional keamanan informasi adalah untuk mengevaluasi risiko terhadap kritis kami aset dan menyebarkan perlindungan untuk mengurangi risiko tersebut. Kami bekerja dalam berbagai peran: firewall insinyur, penguji penetrasi, auditor, manajemen, dll Benang merah adalah Risiko: itu adalah bagian dari deskripsi pekerjaan kami. Resiko adalah sesuatu yang berpotensi menimbulkan cidera/kerugian atau merupakan kombinasi da kemungkinan / peluang dan akibat.

ANALISIS RISIKO

Analisis Risiko akurat adalah keterampilan penting untuk keamanan informasi profesional. Kita harus menahan diri untuk standar yang lebih tinggi ketika menilai risiko. Kami keputusan risiko akan menentukan yang pengamanan kita menyebarkan untuk melindungi aset dan jumlah uang dan sumber daya yang kami habiskan melakukannya. Keputusan yang buruk akan menghasilkan di buang uang atau, bahkan lebih buruk, data dikompromikan. Analisis Risiko adalah suatu metode analisis yang meliputi faktor penilaian, karakterisasi, komunikasi, manajemen dan kebijakan yang berkaitan dengan risiko tersebut. Tahapan kegiatan analisis risiko antara lain meliputi: identifikasi hazard, proyeksi risiko, penilaian risiko, dan manajemen risiko. Penilaian risiko dapat dilakukan secara kuantitatif atau kualitatif.

Aktiva

Aset adalah sumber daya berharga Anda mencoba untuk melindungi. Aset dapat data, sistem,orang, bangunan, properti, dan sebagainya. Nilai atau kekritisan aset akan menentukan apa pengamanan Anda menyebarkan.

Ancaman dan kerentanan

UAS Keamanan Informasi Kelas TI-PAGI

Ancaman adalah segala sesuatu yang berpotensi dapat menyebabkan kerusakan pada aset. Ancaman termasuk gempa bumi, listrik padam, atau cacing berbasis jaringan.

Kerentanan adalah sebuah kelemahan yang memungkinkan ancaman untuk menyebabkan kerusakan. Contoh kerentanan (pencocokan ancaman kami sebelumnya) yang bangunan yang tidak dibangun untuk menahan gempa bumi, pusat data tanpa daya cadangan yang tepat, atau Microsoft Windows Sistem XP yang belum ditambal dalam beberapa tahun.

- Teknik Penilaian Risiko

Teknik penilaian risiko dapat dilakukan secara kualitatif atau kuantitatif.

Karakteristik penilaian kualitatif meliputi tipe efek kesehatan, estimasi frekuensi pemajanan (harian, mingguan, bulanan), lokasi hazard dalam hubungannya dengan tempat kerja. Sedangkan karakteristik penilaian kuantitatif meliputi data pengukuran pemajanan, konsentrasi zat, angka kesakitan/kematian, modeling analisis konsekuensi dari pemajanan terhadap hazard dan modeling frekuensi pemajanan.

a. Penilaian Kuantitatif Risiko

Kuantifikasi terhadap suatu risiko akan sangat tergantung pada kondisi nature hazard, kemudahan utk diukur (measurable) dan adanya suatu standar yg dipakai. Untuk mengkuantifikasi risiko, ketiga komponen risiko (frekuensi, probabilitas dan hasil jadi atau outcome) harus bisa diekspresikan secara matematika (modeling). Modeling merupakan teknik untuk melihat pola kejadian.

Frekuensi dapat diekspresikan dengan menggunakan data riwayat pemajanan atau incident record. Probabilitas dapat dibuat skala dengan rentang nilai ($0 < P < 1$). Hasil jadi (outcome) atau konsekuensi dari hasil pemajanan terhadap suatu hazard dapat diukur sebagai berikut: jumlah kasus kematian atau cedera, kasus sakit serius dan biaya kerusakan (lost cost). Kelemahan penilaian risiko kuantitatif, antara lain sifatnya sangat natur sehingga tidak memperhatikan persepsi dan perlakuan terhadap hazard.

Hal lain yang dapat dilakukan secara kuantifikasi, misalnya untuk modeling kebakaran (fire and explosion). Penilaian kuantitatif risiko ini pada umumnya sangat aplikatif untuk chemical atau process engineers. Contoh penilaian kuantitatif, misalnya penentuan LD50 dan LC50. Keduanya adalah modeling utk penilaian lethal dose dan lethal concentration dengan pengukuran durasi pemajanan, konsentrasi atau dosis hazard dan hasil jadi (kematian).

b. Penilaian Kualitatif Risiko

Metode penilaian risiko secara kualitatif terkesan subjektif dan memberi peluang multiinterpretasi dan debat. Persepsi risiko bisa bervariasi untuk setiap orang. Ada beberapa metode yang dapat diterapkan

- Fine’s Risk Score

Fine’s risk score adalah model untuk melakukan penilaian risiko dengan formula sbb: Risiko adalah hasil pengalian faktor-faktor yang terdiri dari: konsekuensi x faktor exposure x faktor probabilitas ($R = C \times E \times P$).

UAS Keamanan Informasi Kelas TI-PAGI

Proses Manajemen Risiko
Manajemen resiko merupakan desain prosedur serta implementasi prosedur untuk mengelola suatu resiko usaha. Manajemen resiko merupakan antisipasi atas semakin kompleksnya aktivitas badan usaha atau perusahaan yang dipicu oleh perkembangan ilmu pengetahuan dan kemajuan teknologi (Kasidi, 2010).
Manajemen Risiko Panduan untuk Teknologi Informasi Sistem, panduan menjelaskan proses Analisis Risiko 9-langkah:

1. Sistem Karakterisasi
2. Ancaman Identifikasi
3. Kerentanan Identifikasi Analisis
4. Kontrol Penentuan
5. Kemungkinan
6. Analisa Dampak
7. Penentuan Risiko
8. Kontrol Rekomendasi
9. Hasil Dokumentasi

KEAMANAN INFORMASI TATA
Keamanan Informasi Pemerintahan adalah keamanan informasi di tingkat organisasi: manajemen senior, kebijakan, proses, dan staf. Itu juga merupakan prioritas organisasi disediakan oleh kepemimpinan senior, yang diperlukan untuk informasi yang berhasil program keamanan.

Kebijakan keamanan dan dokumen terkait
Dokumen seperti kebijakan dan prosedur adalah bagian yang diperlukan dari setiap sukses program keamanan informasi. Dokumen-dokumen ini harus didasarkan pada realitas: mereka tidak dokumen idealis yang duduk di rak-rak mengumpulkan debu. Mereka harus mencerminkan dunia nyata dan memberikan bimbingan pada benar (dan kadang-kadang diperlukan) cara melakukan hal-hal.

Polis
Kebijakan yang arahan manajemen tingkat tinggi. Kebijakan adalah wajib: jika Anda tidak setuju dengan kebijakan pelecehan seksual perusahaan Anda, misalnya, Anda tidak memiliki pilihan untuk tidak mengikutinya.

Prosedur
Prosedur adalah langkah-demi-langkah panduan untuk menyelesaikan tugas. Mereka tingkat rendah dan spesifik. Seperti kebijakan, prosedur wajib.

Standar
Sebuah standar menggambarkan penggunaan khusus dari teknologi, sering diterapkan untuk perangkat keras dan software.

UAS Keamanan Informasi Kelas TI-PAGI

Pedoman
Pedoman adalah rekomendasi (yang diskresioner).

Baseline

Baseline cara seragam menerapkan safeguard a. Baseline adalah diskresioner: dapat diterima mengeras sistem tanpa mengikuti benchmark tersebut, selama itu setidaknya aman seperti system mengeras menggunakan tolok ukur.

Outsourcing dan offshoring
Outsourcing adalah penggunaan pihak ketiga untuk menyediakan dukungan teknologi informasi layanan yang sebelumnya dilakukan di rumah.

Privasi
Privasi adalah perlindungan kerahasiaan informasi pribadi.

kelalaian
Kelalaian adalah kebalikan dari perawatan karena . Ini adalah konsep hukum yang penting .

COBIT
COBIT (Kontrol Tujuan Informasi dan Teknologi yang terkait) adalah kontrol kerangka kerja untuk mempekerjakan pemerintahan keamanan informasi praktik terbaik dalam sebuah organisasi . COBIT dikembangkan oleh ISACA (Audit Sistem Informasi dan Control Association.

ITIL
ITIL (Information Technology Infrastructure Library) adalah suatu kerangka kerja untuk menyediakan pelayanan terbaik di IT Service Management (ITSM) .

UAS Keamanan Informasi Kelas TI-PAGI

2. Cari software atau tools pendukung keamanan informasi kemudian cobalah fungsional software tersebut untuk menangani kasus tertentu. Buatlah step by step yang terdiri dari screenshot, keterangan gambar, dan analisis. Misalnya penggunaan wireshark dalam melakukan analisis paket data jaringan (pcap file), penggunaan ftk forensic untuk mengetahui file steganografi, dan lain sebagainya. Review software boleh sama, akan tetapi kasusnya harus berbeda dengan temen-temennya.

IP Scanner (Angry IP Scanner)

Angry IP Scanner merupakan software yang dapat melakukan scanning IP address. Software ini berguna sekali untuk membantu anda menjaga, mengelola, dan menginventorisasi jaringan dalam hal ini IP Address. Sebagai system administrator, alat ini sangat membantu dalam menghemat waktu dan pikiran ketika mengawasi jaringan dari tangan jahil yg terhubung ke jaringan. Ketika ada alat (laptop / workstation / apapun itu) yg mencurigakan yg terhubung dengan jaringan, dapat langsung mengetahuinya sesegera mungkin. SOftware ini menggunakan konsep dasar IP Addressing.

Istilah-istilah utama dalam angry IP scanner :

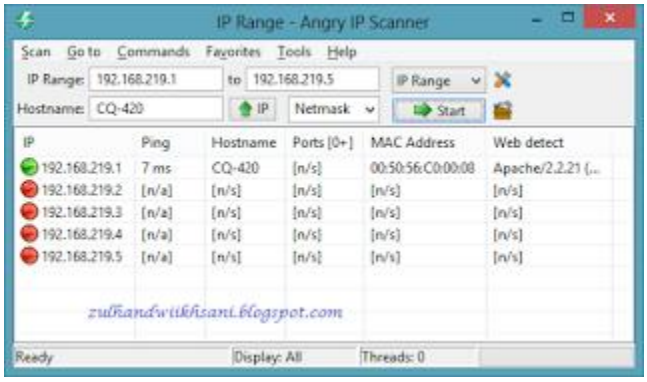
- Feeder - generator alamat IP untuk pemindaian. Scanner Angry IP menyediakan berbagai jenis pengumpan: Rentang IP, Acak, dan File Daftar IP. Anda dapat memilih pengumpan menggunakan combo box di sebelah tombol Start.
- Fetcher - mengumpulkan informasi spesifik tentang host, misalnya ping waktu, hostname, port terbuka. Feeders biasanya mewakili kolom dalam daftar hasil pemindaian. Anda dapat memilih fetchers tambahan dengan memilih "Tools-> fetchers Pilih" dari menu.
- Alive Host - adalah tuan rumah, menanggapi ping. Ini adalah biru dalam daftar hasil.
- Dead Host - adalah tuan rumah, tidak menanggapi ping (merah dalam daftar). Namun, masih mungkin memiliki port terbuka (jika blok firewall ping). Dalam rangka untuk memindai host ini penuh, periksa "memindai host mati" dalam dialog Alat-> Preferences.
- Opened Port - port TCP, menanggapi upaya koneksi. Host dengan port terbuka hijau dalam daftar hasil.
- Filterred Port - port TCP, tidak menanggapi bahwa itu ditutup (tidak ada paket RST). Port ini biasanya khusus diblokir oleh firewall untuk beberapa alasan.

UAS Keamanan Informasi Kelas TI-PAGI

Cara kerja aplikasi ini ada 3, yaitu IP range, Random, dan IP list file.

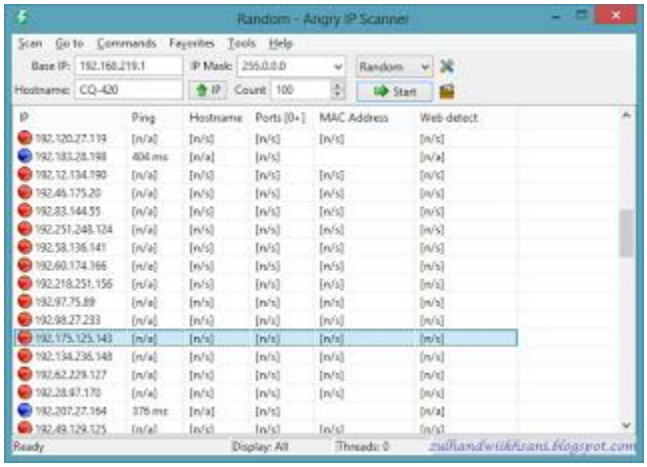
1) **IP range**

Perintah ini memberikan alamat ip range misal range dari 192.168.219.1 sampai 192.168.219.5. Dengan perintah itu, aplikasi ini akan menjalankan dengan cara menscan apakah alamat ip dari range 192.168.219.1 sampai 192.168.219.5 terdapat alamat ip yang aktif atau tidak aktif. Dapat terlihat pada gambar berikut.



2) **Random**

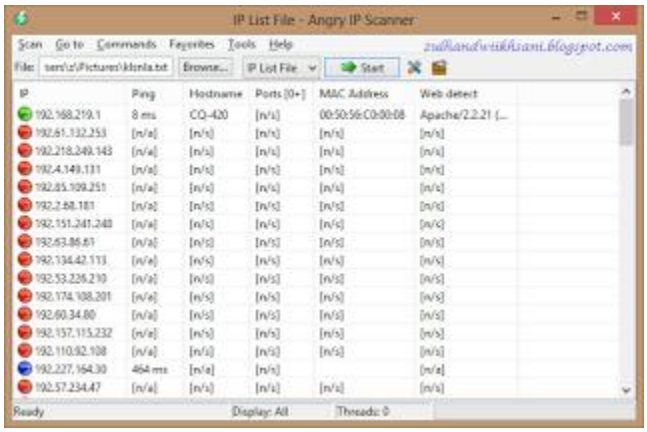
Dengan perintah tersebut, aplikasi ini akan menscan dengan cara random atau acak dan terdapat count yang menunjukkan banyaknya alamat ip yang akan discan/dilacak. dapat dilihat dari gambar berikut.



UAS Keamanan Informasi Kelas TI-PAGI

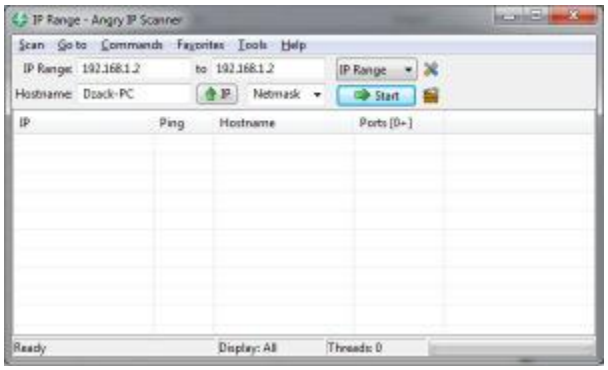
3) IP list file

Dengan peritah ini, aplikasi akan meminta file dengan jenis extensi .txt, .csv, .xml, dan .list yang sebelumnya disimpan disebuah harddisk atau sejenisnya.

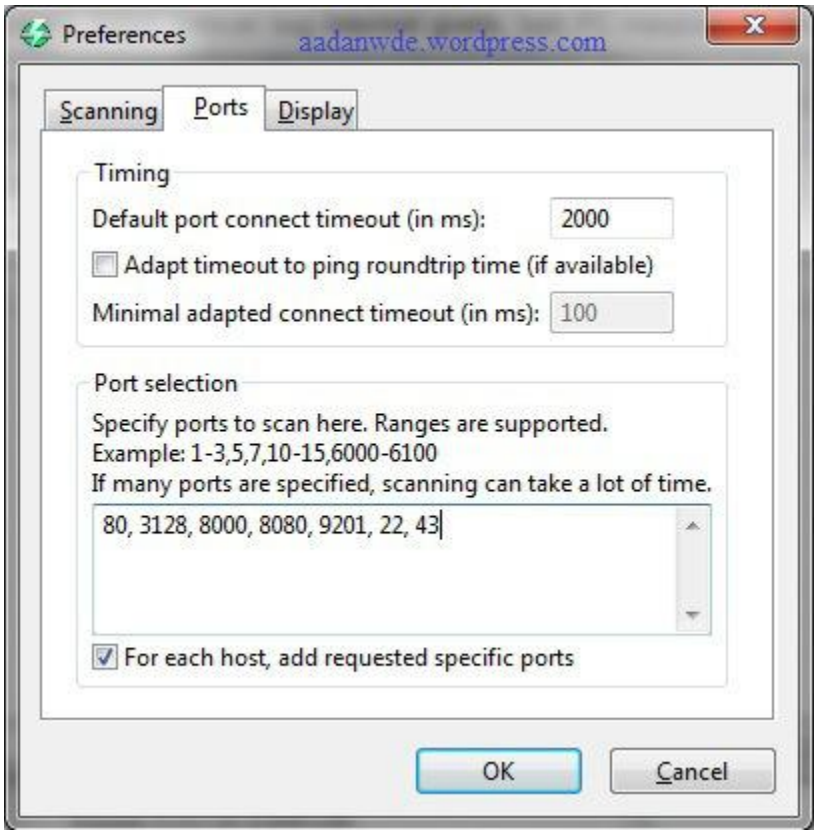


- **CONTOH MENGGUNAKAN IP RANGE**

a) Buka Program IP Scanner (berikut tampilan awal)

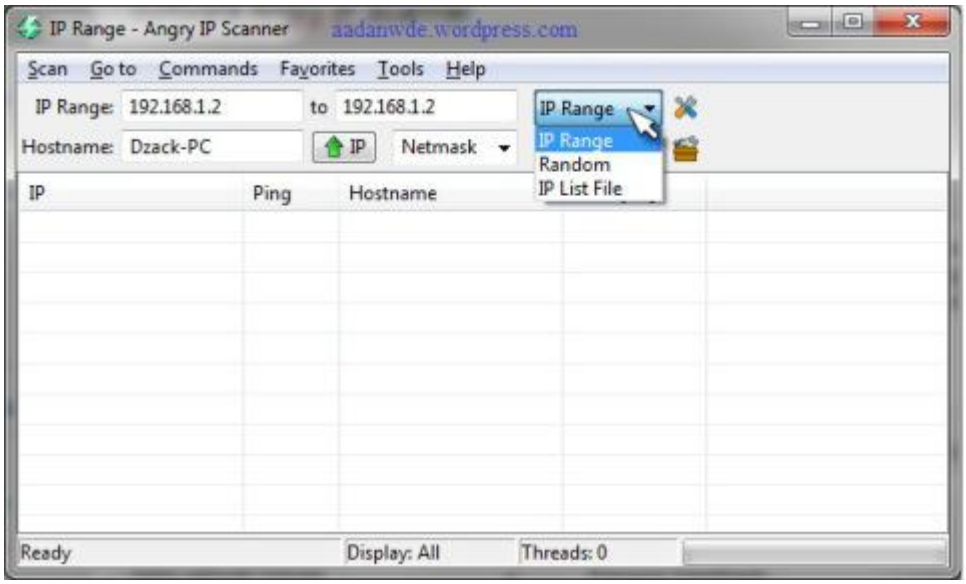


b) Buka tab Tools, kemudian pilih Preferences, lalu pilih tab Ports. Pada kolom Port selection, cukup isi dengan port 80, 3128, 8000, 8080, 9201. Sebagi tambahan, bagi yang nyari IP buat SSH tunnel, tambahkan port 22 dan 443. (info lebih lanjut mengenai Port-portnya dapat di lihat lewat ‘Google’)

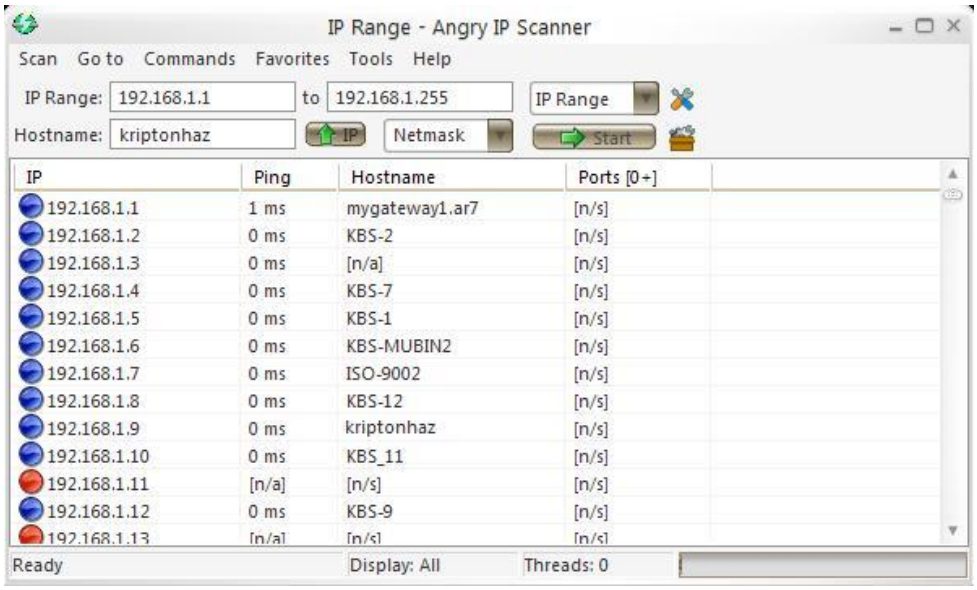


Untuk menscan port, saran saya sebaiknya anda belajar terlebih dahulu mengenai vulnerability atau kelemahan dari port.

c) Cara penggunaannya ada 3 metode. Pertama, *IP Range* yang menscan IP diantara dua IP yang menjadi patokan, misal 82.145.216.1-82.145.216.40. Kedua, *Random* yang menscan IP secara acak, misal 195.189.142.6. Ketiga, *IP List File* yang menscan IP yang telah tersimpan sebelumnya.



4. Setelah memilih metodenya, kemudian klik start dan tunggu sampai selesai. Dan akan keluar Hasilnya.



UAS Keamanan Informasi Kelas TI-PAGI

Terlihat pada layar ada informasi mengenai IP, Ping, Hostname, dan Port. Tampilan biru pada kolom IP menandakan IP tersebut aktif sedangkan yang berwarna merah tidak aktif. Untuk Ping yakni seberapa bagus koneksi yang dilakukan, semakin rendah nilainya semakin bagus koneksinya. Untuk hostname yakni nama komputer yang digunakan, terlihat ada n/a disana entah mengapa mungkin komputer dengan IP tersebut dipasang firewall pihak ketiga semacam zone alarm atau comodo sehingga tidak bisa di resolve Hostname nya. Untuk Port kosong karena secara default software ini tidak menscan port.