KEAMANAN INFORMASI
UAS

DI SUSUN OLEH:

NAMA : SULAIMAN

NIM : 1410651021

KELAS : E

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER
2015

❖ Soal no 1

Information Security Governance and Risk Management

(informasi Tata Kelola Keamanan dan Manajemen Risiko)

1. Analisis resiko
   Semua profesional para ahli keamanan informasi menilai resiko adalah sifat kedua di karnakan terlalu sering kita melakukan.
   Analisis resiko yang akurat adalah suatu keterampilan paling penting untuk ke amanan informasi
   Sebuah keputusan akan menentukan bagai mana aset kita bisa terlindungi dari beberapa kejahatan dunia maya.
   Sebuah keputusan yang buruk akan menghasilkan aset kita menurun baik itu dari segi material atau pun sebagai nya.
   a. Aset adalah sumber daya yang sangat berharga yang harus di lindungi oleh kita baik itu semacam data, sistem, orang, bangunan, dan lain sebagai nya.
   b. Ancaman dan kerentanan.

   Ancaman adlah segala sesuatu yang berpotensi dapat enyebabkan kerusakan pada aset yang kita miliki.
   Ancaman dapat di katagorikan seperti gempa bumi, pemadaman listrik, atau pun cacing berbasis jaringan dimana kesemua itu akan menghasilakan kerugian yang sangat besar bagi asaet yang kita miliki.
   Kerentana adalh kelemahan yang memungkinkan akan menimbulkan kerusakan kerusakan .contoh : pada sistem microsoft windows xp yang mana di dalam sistem tersebut banyak kekurangan yang belum di perbaiki selama beberapa tahun terakhir.
2. Matrix analisis resiko
   Matrix analisi resiko menggunakan kuadran untuk menentukan kemungkinan ada resiko yang bakalan terjadi dan dampak yang akan di alami oleh pengguna.
   Matrix analisis resiko memungkinkan anda untuk melakukan kualitatif dan kuantitatif berdasarkan kemungkinan yang sudah dikira sebelumnya.
   Sedangkan cara penanggulangan resiko rendah harus ditangini dengan proses normal sedangkan resiko yang moderat atau berat kita memerlukan penangan husus untuk memecahkan masalah tersebut.
   Tujuan dari matrix tersebut adalah untuk mengidintifikasi resiko yang tinggi.

3. Calculating Annualized Loss Expectancy

   The Annualized Loss Expectancy (ALE) perhitungan memungkinkan Anda untuk menentukan biaya tahunan kerugian akibat risiko.
   Setelah dihitung, ALE memungkinkan Anda untuk membuat keputusan untuk mengurangi risiko.
   a. Asset Value

   ada dua aset adalah suatu aset yang berwujud di mana aset tersebut ada dan nyata di hadapan kita atau terlihat oleh pandangan kita seperti komputer bangunan rumah dan lain sebagai nya.

Dan aset tidak berwujud misalnya nilai loyalitas dari sebuah merek .
Menurut salah satu ilmuan ada tiga metode untuk menghitung sebuah nilai

• "Pendekatan Pasar: Pendekatan ini mengasumsikan bahwa nilai wajar aset mencerminkan
harga yang sebanding aset telah dibeli dalam transaksi di bawah
kondisi yang sama.

• Pendekatan Pendapatan: Pendekatan ini didasarkan pada premis bahwa nilai dari keamanan atau aset adalah nilai sekarang dari kapasitas produktif masa depan yang merupakan aset
akan menghasilkan lebih dari sisa masa manfaatnya.
• Pendekatan Biaya: Pendekatan ini memperkirakan nilai wajar aset dengan mengacu biaya yang akan dikeluarkan untuk menciptakan atau mengganti aset. "

4. Anggaran dan metrik
   Ketika dikombinasikan dengan Analisis Risiko, Total Cost of Ownership dan Imbal
   Perhitungan investasi faktor dalam penganggaran yang tepat. Beberapa organisasi memiliki
   posisi dana keamanan informasi yang cukup, namun mereka sering dikompromikan. Mengapa? Jawabannya adalah biasanya karena mereka dikurangi risiko yang salah.
   Mereka menghabiskan uang mana mungkin belum perlu dan mengabaikan risiko yang lebih besar.
   Metrik dapat sangat membantu proses penganggaran keamanan informasi.
   Mereka membantu menggambarkan risiko yang berpotensi mahal dan menunjukkan efektivitas dan potensi penghematan biaya kontrol yang ada.
   Mereka juga dapat penyebabkan kemanan informasi jadi juara.
   Pilihan risiko
   Setelah kami telah dinilai risiko, kita harus memutuskan apa yang harus dilakukan. Pilihan termasuk menerima
   risiko, mengurangi atau menghilangkan risiko, mentransfer risiko, dan menghindari risiko.
   Menerima risiko
   Beberapa risiko dapat diterima: dalam beberapa kasus, lebih murah untuk meninggalkan aset yang tidak dilindungi karena risiko tertentu, daripada membuat usaha (dan menghabiskan uang) yang diperlukan untuk melindunginya. Hal ini tidak bisa menjadi keputusan yang bodoh: risiko harus dipertimbangkan, dan semua Pilihan harus dipertimbangkan sebelum menerima risiko.

Ada 9 langkah untuk menjelaskan proses Analisis Risiko

1. Sistem Karakterisasi

2. Ancaman Identifikasi

3. Kerentanan Identifikasi Analisis

4. Kontrol Penentuan

5. Kemungkinan

6. Dampak Analysi kehidupan manusia atau keamanan, di mana menerima risiko bukanlah pilihan.

7. Penentuan Risiko

8. Kontrol Rekomendasi

9. Hasil Dokumentasi

5. KEAMANAN INFORMASI

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.

Komponen kebijakan Program

Semua kebijakan harus mengandung komponen-komponen dasar:

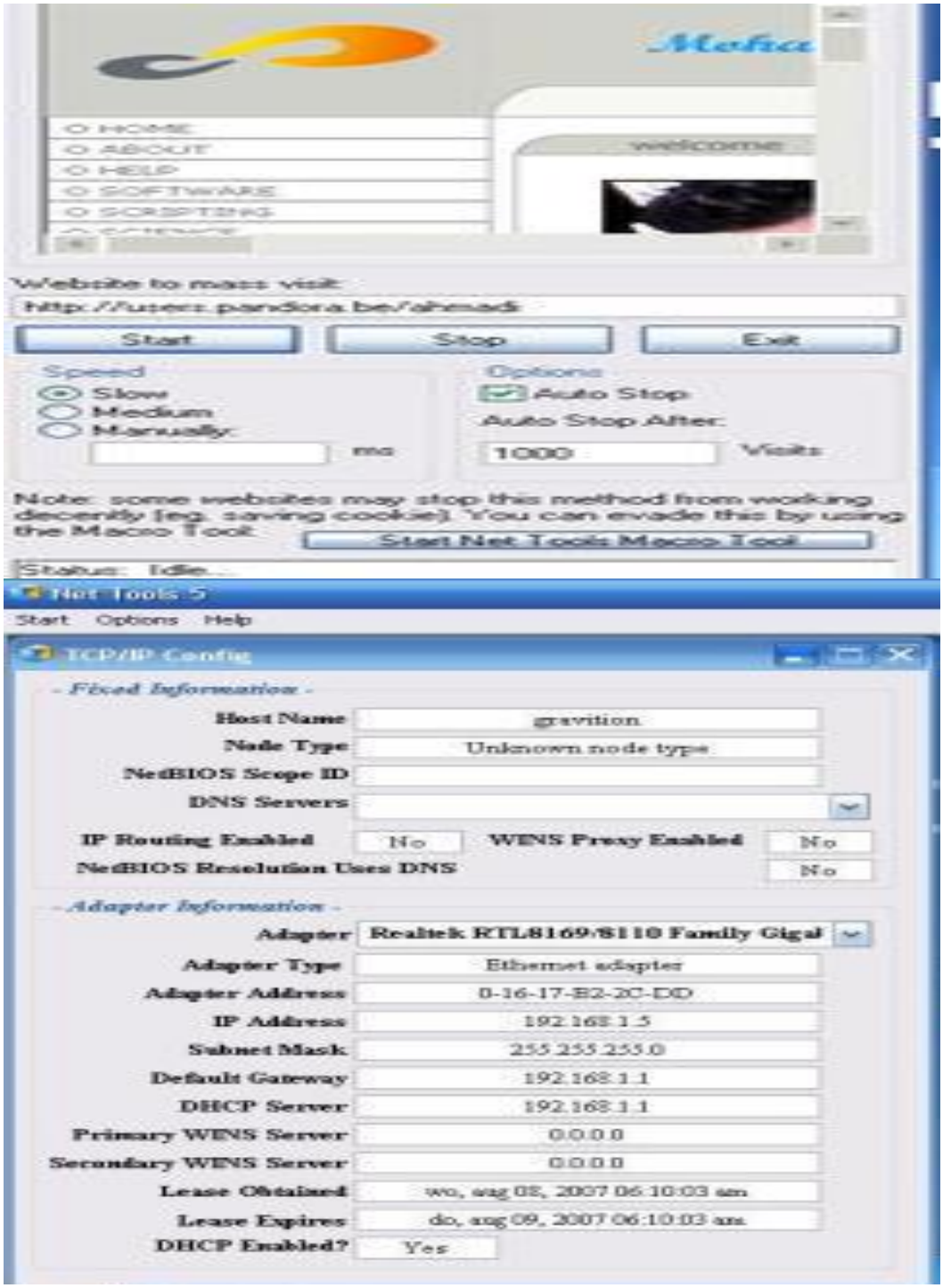
- Tujuan
- Lingkup
- Tanggung Jawab
- Kepatuhan

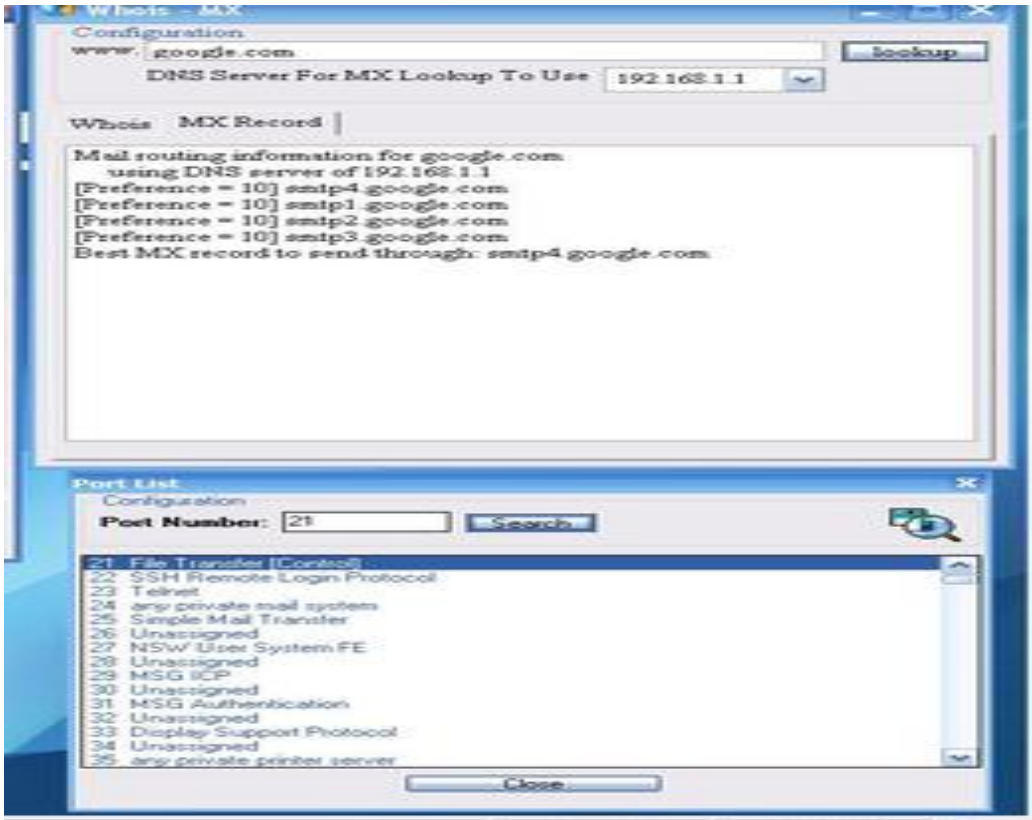
Tujuan menggambarkan kebutuhan untuk kebijakan, biasanya untuk melindungi kerahasiaan, integritas, dan ketersediaan data yang dilindungi.

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

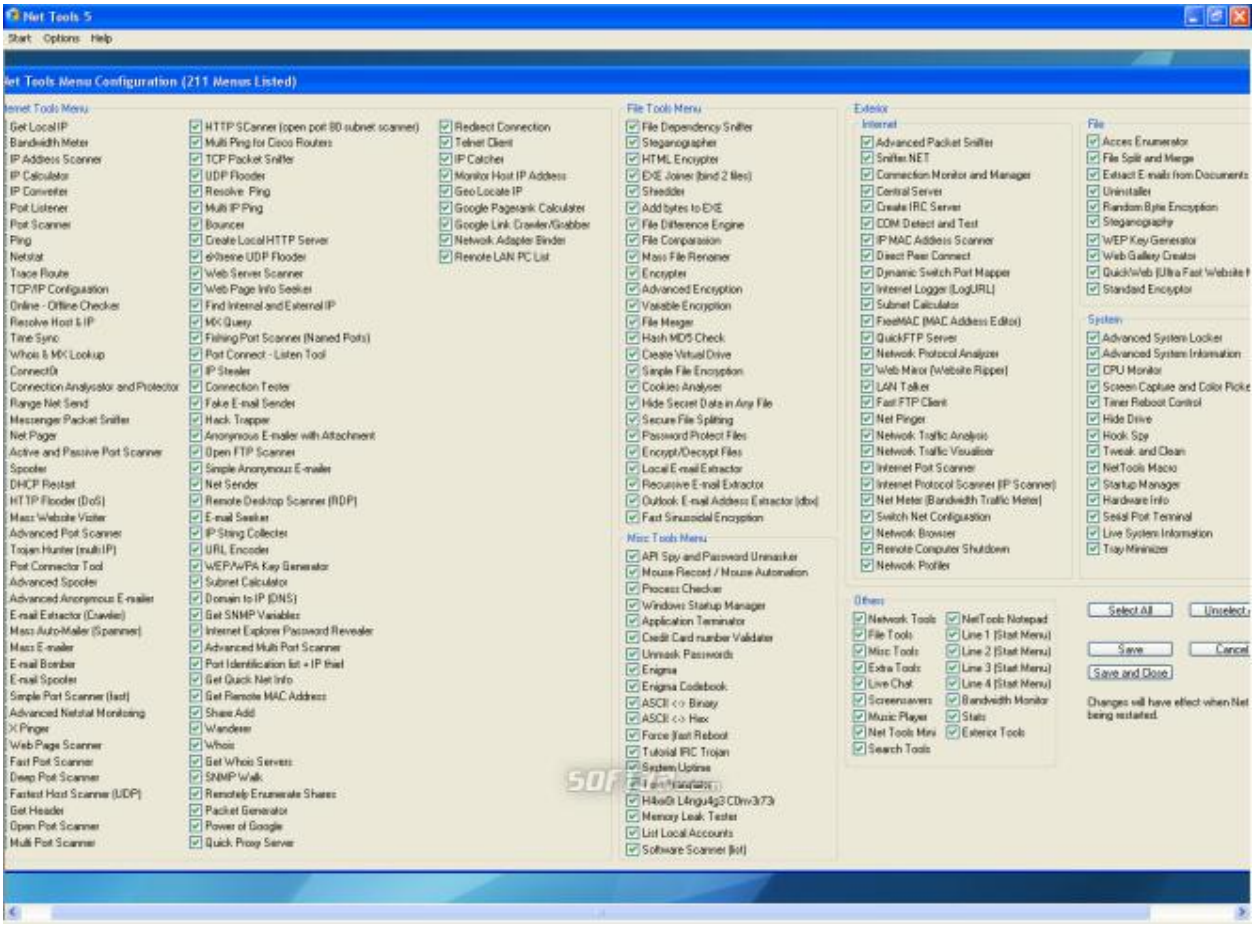
Berikut ini adalah contoh prosedur sederhana untuk membuat user baru:
1. Menerima formulir permintaan baru-pengguna dan memverifikasi kelengkapan.
2. Pastikan bahwa manajer pengguna telah menandatangani formulir.
3. Pastikan bahwa pengguna telah membaca dan setuju dengan kebijakan keamanan akun pengguna.
4. Klasifikasikan peran pengguna dengan mengikuti prosedur peran-tugas NX-103.
5. Pastikan bahwa pengguna telah memilih "kata rahasia," seperti gadis ibu mereka nama, dan masukkan ke dalam profil akun help desk.
6. Buat account dan menetapkan peran yang tepat.
7. Menetapkan kata rahasia sebagai password awal dan mengatur "Angkatan pengguna untuk mengubah
password pada login berikutnya untuk 'Benar'. "
8. E-surat dokumen Akun Baru ke pengguna dan manajer mereka.

- SOAL NO 2
  Aplikasi net tool 5
  NET TOOLS adalah sebuah alat bantu hacking yang mudah dan serba guna, tools disini berarti sebuah program siap pakai dimana sebagian besar source code atau listing programnya memiliki perintah dan fungsi untuk menelisik kesalahan/kelemahan (bugs) pada mesin atau system komputer yang dipakai maupun komputer lain
  Di sini untuk mengaman kan suatu jaringan melalui mengubah alamat IP yang ada pada komputer kita


HOME
ABOUT
HELP
SOFTWARE
SCRIPTING
WELCOME
Website to mass visit:
http://users.pandora.be/ahead
Start
Stop
Exit
Speed
Slow
Medium
Manually
ms
Options
Auto Stop
Auto Stop After:
1000
Visits
Note: some websites may stop this method from working decently (eg. saving cookie). You can evade this by using the Macro Tool.
Start Net Tools Macro Tool
Status: Idle...
Net Tools 5
Start Options Help
TCP/IP Config
- Fixed Information -
Host Name
gravition
Node Type
Unknown node type
NetBIOS Scope ID
DNS Servers
IP Routing Enabled
No
WINS Proxy Enabled
No
NetBIOS Resolution Uses DNS
No
- Adapter Information -
Adapter
Realtek RTL8169/8110 Family Gigal
Adapter Type
Ethernet adapter
Adapter Address
0-16-17-E2-2C-DD
IP Address
192.168.1.5
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DHCP Server
192.168.1.1
Primary WINS Server
0.0.0.0
Secondary WINS Server
0.0.0.0
Lease Obtained
wo, aug 08, 2007 06:10:03 am
Lease Expires
do, aug 09, 2007 06:10:03 am
DHCP Enabled?
Yes


Configuration
www. google.com
Lookup
DNS Server For MX Lookup To Use
192.168.1.1
Whois
MX Record
Mail routing information for google.com
using DNS server of 192.168.1.1
[Preference = 10] smtp4.google.com
[Preference = 10] smtp1.google.com
[Preference = 10] smtp2.google.com
[Preference = 10] smtp3.google.com
Best MX record to send through: smtp4.google.com
Port List
Configuration
Port Number:
21
Search
21 File Transfer [Control]
22 SSH Remote Login Protocol
23 Telnet
24 any private mail system
25 Simple Mail Transfer
26 Unassigned
27 NSW User System FE
28 Unassigned
29 MSG ICP
30 Unassigned
31 MSG Authentication
32 Unassigned
33 Display Support Protocol
34 Unassigned
35 any private printer server
Close


Packet Generator
IP or Host
192.168.1.16
Remote Port
80
Pre-defined
PING 0.0.0.0 -ICMP 255
Save
String
GET:/
Output in MS-DOS
Ping
Open
Danger Packet
0.0.0 GET:RChar*2100byte
Speed of transmission
Start Flood
Stop



Kesimpulan : masalah network security timbul dari konetivitas jaringan komputer lokal yang kita miliki dengan wide area network (seperti internet. Selama jaringan network kita tidak terkoneksi dengan internet maka network scurity tidak begitu penting.