**LAPORAN PRAKTIKUM**

**KEAMANAN KOMPUTER**



**Disusun oleh:**

M TRIO PRASTYO BILLY WARDANI

(1400631022)

**PROGRAM STUDI MANAJEMEN INFORMATIKA FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH JEMBER**

**2015**

**Keamanan Komputer Mengapa dibutuhkan ?**

* *“information-based societ*y”, menyebabkan nilai informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi,
* Infrastruktur Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, sekaligus membuka potensi adanya lubang keamanan *(security hol*e)

**Kejahatan Komputer semakin meningkat karena :**

* Aplikasi bisnis berbasis TI dan jaringan komputer meningkat : online banking, e-commerce, Electronic data Interchange (EDI).
* Desentralisasi server.
* Transisi dari single vendor ke multi vendor.
* Meningkatnya kemampuan pemakai (user).
* Kesulitan penegak hokum dan belum adanya ketentuan yang pasti.
* Semakin kompleksnya system yang digunakan, semakin besarnya source code program yang digunakan.
* Berhubungan dengan internet.

**Klasifikasi kejahatan Komputer :**

Level Dangerous

Level annoying

Menurut David Icove [John D. Howard, *“An Analysis Of Security Incidents On The Internet 1989 - 199*5,” PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 1997.] berdasarkan lubang keamanan, keamanan dapat

diklasifikasikan menjadi empat, yaitu:

* **Keamanan yang bersifat fisik** *(physical securit*y): termasuk akses orang ke gedung, peralatan, dan media yang digunakan. Contoh :
* Wiretapping atau hal-hal yang ber-hubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.
* *Denial of servic*e, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diuta-makan adalah banyaknya jumlah pesan).
* *Syn Flood Attac*k, dimana sistem *(hos*t) yang dituju dibanjiri oleh permintaan sehingga dia menjadi ter-lalu sibuk dan bahkan dapat berakibat macetnya sistem *(han*g).
* **Keamanan yang berhubungan dengan orang (personel**), Contoh :
* Identifikasi user (username dan password)
* Profil resiko dari orang yang mempunyai akses (pemakai dan pengelola).

* **Keamanan dari data dan media serta teknik komunikasi** *(communication*s).
* **Keamanan dalam operas**i: Adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga ter-masuk prosedur setelah serangan *(post attack recover*y).

**Karakteristik Penyusup :**

* The Curious (Si Ingin Tahu) - tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang anda miliki.
* The Malicious (Si Perusak) - tipe penyusup ini berusaha untuk merusak sistem anda, atau merubah web page anda, atau sebaliknya membuat waktu dan uang anda kembali pulih.
* The High-Profile Intruder (Si Profil Tinggi) - tipe penyusup ini berusaha menggunakan sistem anda untuk memperoleh popularitas dan ketenaran. Dia mungkin menggunakan sistem profil tinggi anda untuk mengiklankan kemampuannya.
* The Competition (Si Pesaing) - tipe penyusup ini tertarik pada data yang anda miliki dalam sistem anda. Ia mungkin seseorang yang beranggapan bahwa anda memiliki sesuatu yang dapat menguntungkannya secara keuangan atau sebaliknya.

**Istilah bagi penyusup :**

* Mundane ; tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya.
* lamer (script kiddies) ; mencoba script2 yang pernah di buat oleh aktivis hacking, tapi tidak paham bagaimana cara membuatnya.
* wannabe ; paham sedikit metode hacking, dan sudah mulai berhasil menerobos sehingga berfalsafah ; HACK IS MY RELIGION.
* larva (newbie) ; hacker pemula, teknik hacking mulai dikuasai dengan baik, sering bereksperimen.
* hacker ; aktivitas hacking sebagai profesi.
* wizard ; hacker yang membuat komunitas pembelajaran di antara mereka.
* guru ; master of the master hacker, lebih mengarah ke penciptaan tools-tools yang powerfull yang salah satunya dapat menunjang aktivitas hacking, namun lebih jadi tools pemrograman system yang umum.

**ASPEK KEAMANAN KOMPUTER :**

Menurut Garfinkel [Simson Garfinkel, *“PGP: Pretty Good Privac*y,” O’Reilly & Associ-ates, Inc., 1995. ]

**1. Privacy / Confidentiality**

* Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.
* Privacy : lebih kearah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai *(use*r) tidak boleh dibaca oleh administrator.
* Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.
* Contoh : data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya.
* Bentuk Serangan : usaha penyadapan (dengan program *sniffe*r).
* Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

**Integrity**

* Defenisi : informasi tidak boleh diubah tanpa seijin pemilik informasi.
* Contoh : e-mail di *intercep*t di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
* Bentuk serangan : Adanya virus, *trojan hors*e, atau pemakai lain yang mengubah informasi tanpa ijin, “man in the middle attack” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

**Authentication**

* Defenisi : metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.
* Dukungan :
* Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking(untuk menjaga *“intellectual propert*y”, yaitu dengan menandai dokumen atau hasil karya dengan “tanda tangan” pembuat ) dan digital signature.
* Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

**Availability**

* Defenisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan.
* Contoh hambatan :
* *“denial of service attac*k” (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *dow*n, *han*g, *cras*h.
* *mailbom*b, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

**Access Control**

* Defenisi : cara pengaturan akses kepada informasi. berhubungan dengan masalah
* authentication dan juga privacy
* Metode : menggunakan kombinasi userid/password atau dengan
* menggunakan mekanisme lain.

**Non-repudiation**

* Defenisi : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

**Security Attack Models**

Menurut W. Stallings [William Stallings, *“Network and Internetwork Securit*y,” Prentice

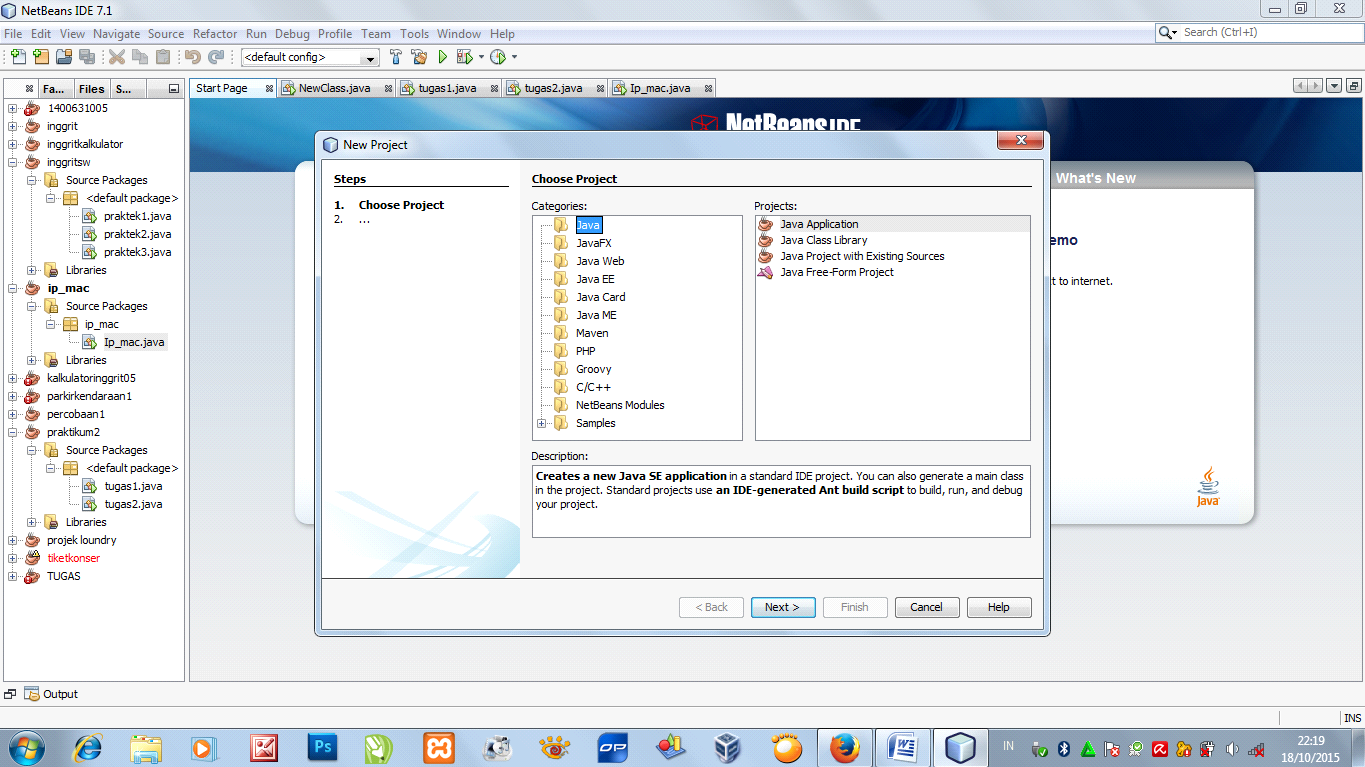
Hall, 1995.] serangan *(attac*k) terdiri dari :

* ***Interruptio*n:** Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan *(availabilit*y) dari sistem. Contoh serangan adalah “denial of service attack”.
* ***Interceptio*n:** Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan *(wiretappin*g).
* ***Modificatio*n:** Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.
* ***Fabricatio*n:** Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

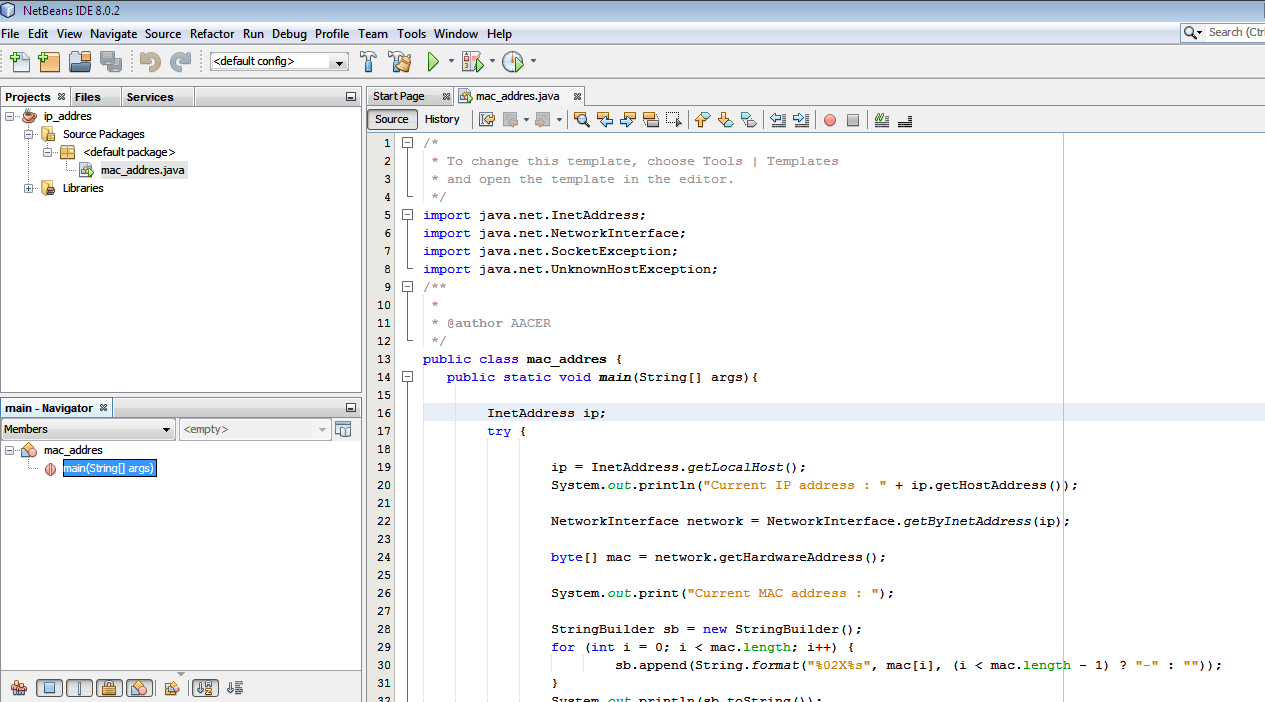
TUGAS !

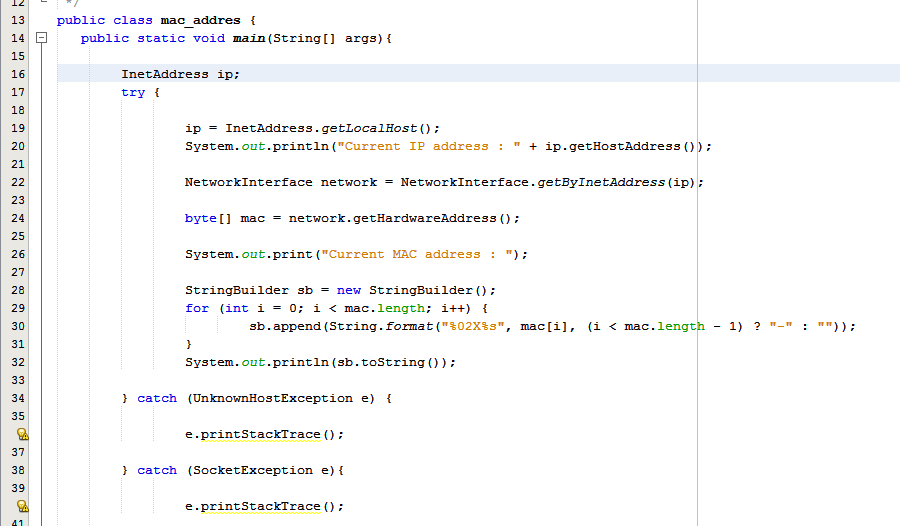
Buatlah sebuah program untuk mengetahui ip dan mac address pada komputermu dengan menggunakan netbeen.

* Buka aplikasi netbeens dan buat project baru

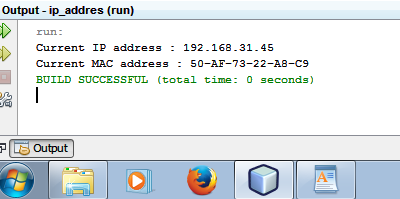


* Setelah itu ketik source kode seperti di bawah ini





* Dan seperti berikut output yang mengeluarkan ip dan mac address pada komputer kita.



1. KESIMPULAN : NetworkInterfaceNetworkInterface.getHardwareAddress () metode ini hanya diperbolehkan untuk mengakses alamat MAC localhost, bukan host remote alamat

MAC.