Keamanan Sistem Informasi

Girindro Pringgo Digdo

2014

Agenda

- Evaluasi Keamanan Sistem Informasi
- Sumber Lubang Keamanan
- Penguji Keamanan Sistem
- Probing Services
- Penggunaan Program
- Program Pemantau Jaringan

Evaluasi Keamanan SI

Meski sebuah sistem informasi sudah dirancang memiliki perangkat pengamanan, dalam operasi masalah keamanan harus selalu dimonitor. Hal ini disebabkan oleh beberapa hal, antara lain:

- Ditemukannya lubang keamanan (security hole) yang baru.

  Perangkat lunak dan perangkat keras biasanya sangat kompleks sehingga tidak mungkin untuk diuji seratus persen. Terkadang ada lubang keamanan yang ditimbulkan oleh kecerobohan implementasi.

Evaluasi Keamanan SI

- Kesalahan konfigurasi.

  Terkadang karena lalai atau lupa, konfigurasi sebuah sistem kurang benar sehingga menimbulkan lubang keamanan.

  Misalnya mode (permission atau kepemilikan) dari berkas yang menyimpan password (/etc/passwd di sistem UNIX) secara tidak sengaja diubah sehingga dapat diubah atau ditulis oleh orang-orang yang tidak berhak.

Evaluasi Keamanan SI

- Penambahan perangkat baru (hardware dan/atau software).

  Menyebabkan menurunnya tingkat security atau berubahnya metode untuk mengoperasikan sistem.

  Operator dan administrator harus belajar lagi. Dalam masa belajar ini banyak hal yang masih menjadi masalah, misalnya server atau software masih menggunakan konfigurasi awal dari vendor (dengan password yang sama).

Sumber Lubang Keamanan

Lubang keamanan (security hole) dapat terjadi karena beberapa hal:

- Salah desain (design flaw).
- Salah implementasi.
- Salah konfigurasi.
- Salah penggunaan.

Sumber Lubang Keamanan

- Salah desain (design flaws)

  Lubang keamanan yang ditimbulkan oleh salah desain umumnya jarang terjadi. Akan tetapi apabila terjadi sangat sulit untuk diperbaiki. Akibat desain yang salah, maka meskipun ia diimplementasikan dengan baik, kelemahan dari sistem akan tetap ada.

Sumber Lubang Keamanan

Contoh:

Algoritma enkripsi ROT13 atau Caesar Cipher, dimana karakter digeser 13 huruf atau 3 huruf. Meskipun diimplementasikan dengan programming yang sangat teliti, siapapun yang mengetahui algoritmanya dapat memecahkan enkripsi tersebut.

Sumber Lubang Keamanan

- Salah implementasi

  Banyak program yang diimplementasikan secara terburu-buru sehingga kurang cermat dalam pengkodean. Akibatnya cek atau testing yang harus dilakukan menjadi tidak dilakukan.

Sumber Lubang Keamanan

Contoh:

Lupa (tidak tahu?) memfilter karakter-karakter yang aneh-aneh yang dimasukkan sebagai input dari sebuah program (misalnya input dari HTML Script) sehingga sang program dapat mengakses berkas atau informasi yang semestinya tidak boleh diakses.

Sumber Lubang Keamanan

- Salah konfigurasi

  Contoh:

  Berkas yang semestinya tidak dapat diubah oleh pemakai secara tidak sengaja menjadi ”writeable”.

  phpmyadmin?

Sumber Lubang Keamanan

- Salah penggunaan

  Kesalahan menggunakan program yang dijalankan dengan menggunakan account root (super user) dapat berakibat fatal.

Sumber Lubang Keamanan

Contoh:

Administrator baru yang teledor dalam menjalankan perintah "rm -rf" di sistem UNIX (yang menghapus berkas atau direktori beserta sub direktori di dalamnya).

Penguji Keamanan Sistem

Karena banyaknya hal yang harus dimonitor, administrator dari sistem informasi membutuhkan “automated tools”, perangkat pembantu otomatis, yang dapat membantu menguji atau mengevaluasi keamanan sistem yang dikelola.

Penguji Keamanan Sistem

Untuk sistem yang berbasis UNIX ada beberapa tools yang dapat digunakan, antara lain:

- Tripwire
- SAINT
- COPS
- ?

Probing Services

Servis di Internet umumnya dilakukan dengan menggunakan protokol TCP atau UDP. Setiap servis dijalankan dengan menggunakan port yang berbeda, misalnya:

- HTTP; TCP port 80
- FTP; TCP port 21

Probing Services

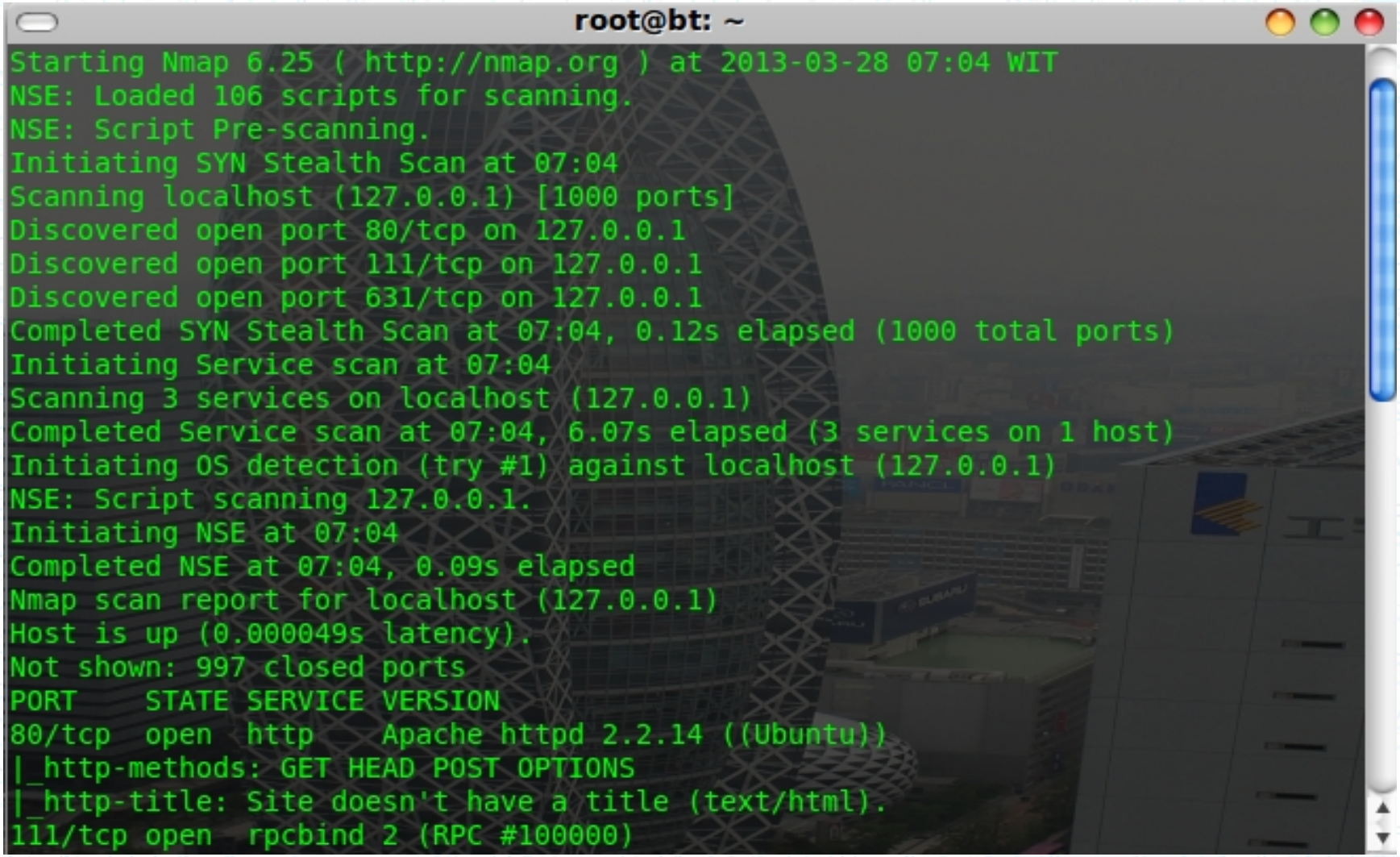
- Pemilihan servis apa saja tergantung kepada kebutuhan dan tingkat keamanan yang diinginkan.
- Seringkali sistem yang dibeli atau dirakit menjalankan beberapa servis utama sebagai "default". Terkadang beberapa servis harus dimatikan karena ada kemungkinan dapat dieksploitasi oleh cracker.

Probing Services

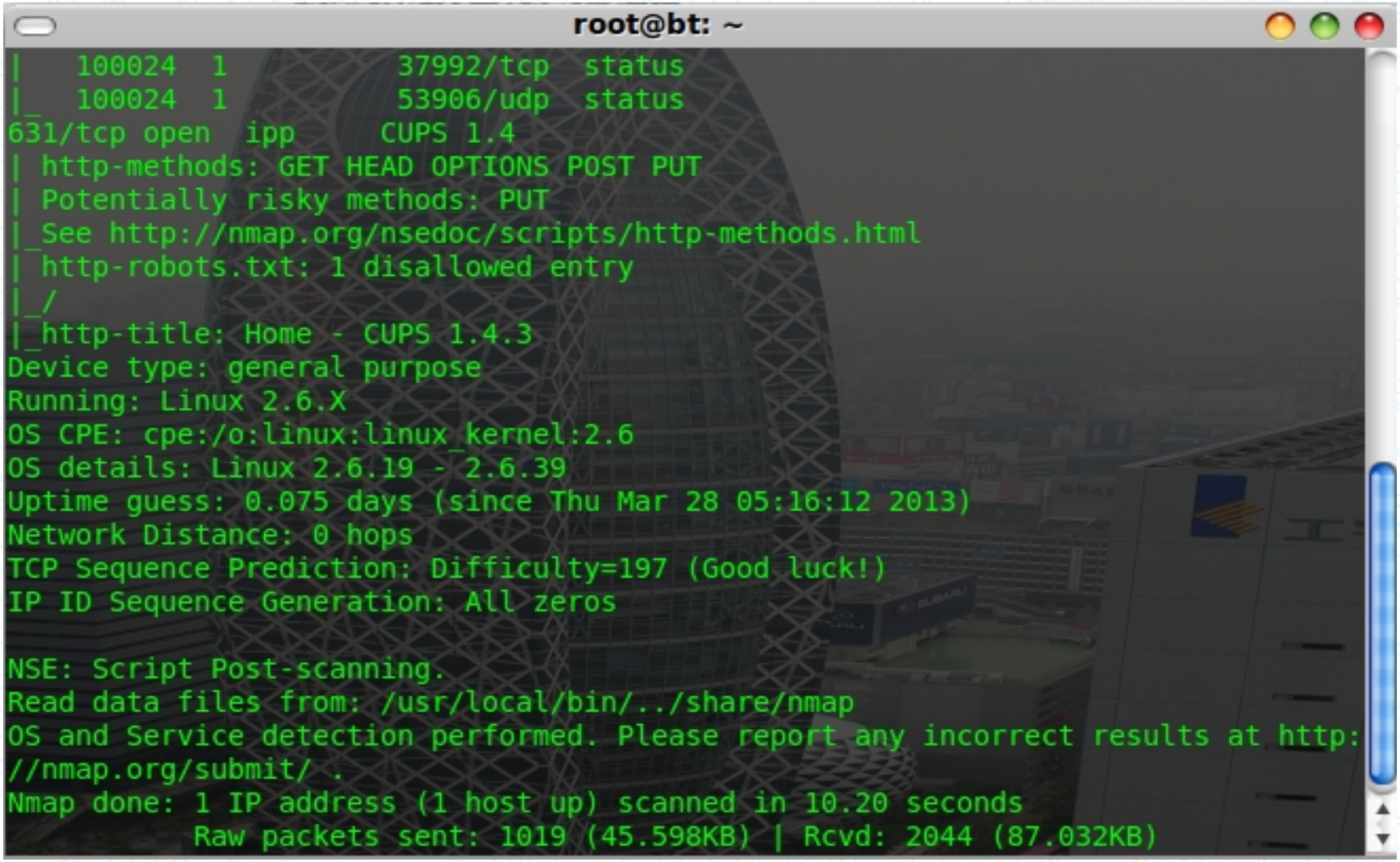
- Ada beberapa tools yang dapat digunakan untuk melakukan “probe” (meraba) servis apa saja yang tersedia.

  Program ini juga dapat digunakan oleh kriminal untuk melihat servis apa saja yang tersedia di sistem yang akan diserang dan berdasarkan data-data yang diperoleh dapat melancarkan serangan.

Probing Servis



Probing Servis



Probing Servis

Beberapa tools probing:

- Nmap
- Strobe
- Tcpprobe

Penggunaan Program

- Salah satu cara untuk mengetahui kelemahan sistem informasi anda adalah dengan menyerang diri sendiri.
- Jangan menggunakan program-program tersebut untuk menyerang sistem lain (sistem yang tidak anda kelola).

Penggunaan Program

Dua jenis program penyerang :

- Aktif

  Program penyerang yang sifatnya agresif melumpuhkan sistem yang dituju.

- Pasif

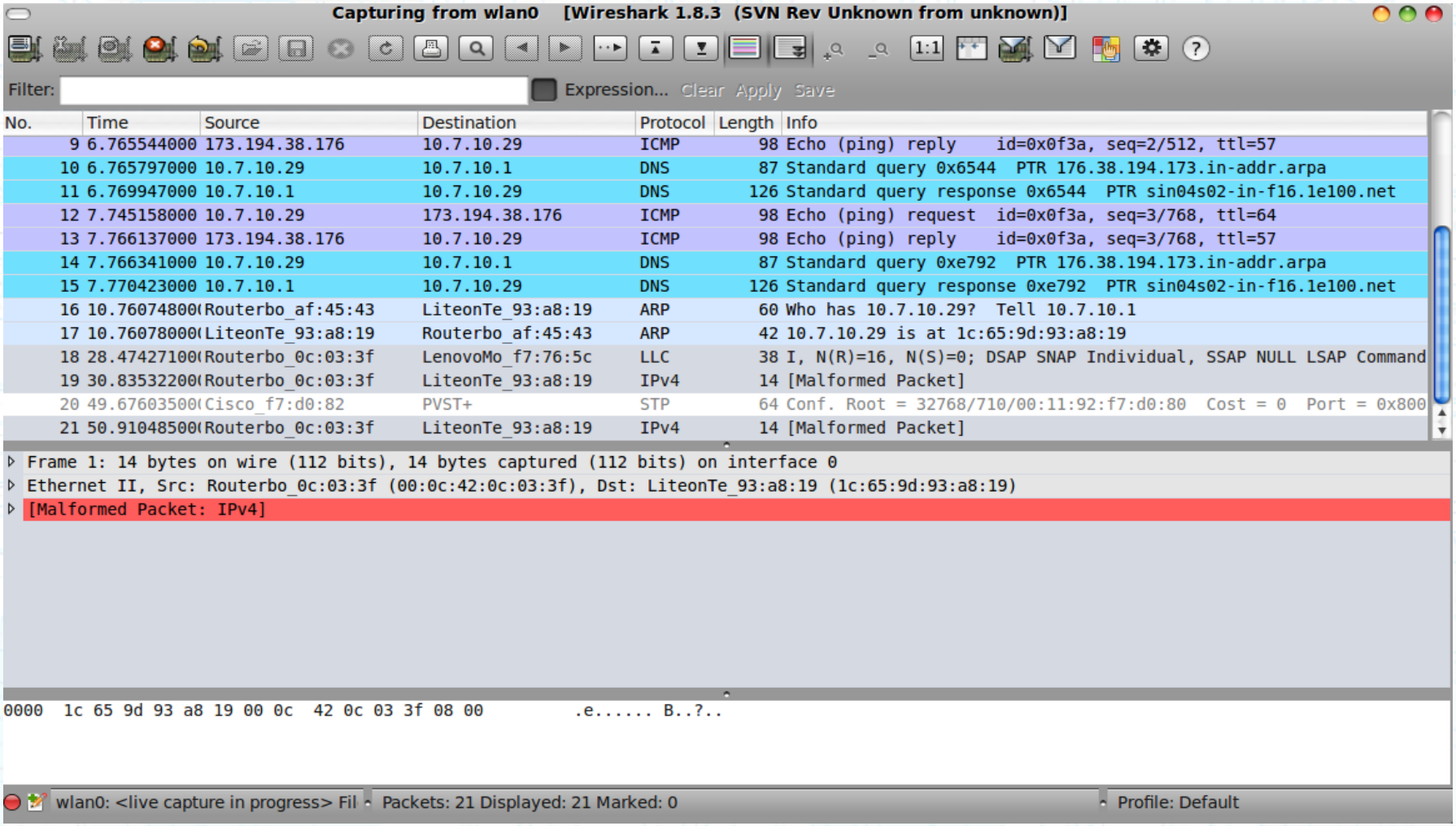
  Program penyerang yang sifatnya melakukan pencurian atau penyadapan data.

Penggunaan Program

Contoh program:

- Pcapture
- Tcpdump
- Wireshark

Penggunaan Program



Program Pemantau Jaringan

- Sistem pemantau jaringan (network monitoring) dapat digunakan untuk mengetahui adanya lubang keamaman.
- Dengan pemantau jaringan dapat juga dilihat usaha-usaha untuk melumpuhkan sistem dengan melalui denial of service attack (DoS) dengan mengirimkan paket yang jumlahnya berlebihan.
- Network monitoring biasanya dilakukan dengan menggunakan protokol SNMP (Simple Network Management Protocol).

Program Pemantau Jaringan

Contoh-contoh program network monitoring / management antara lain:

- Etherboy (Windows), Etherape (Unix)
- HP Openview (Windows)
- Packetboy (Windows), Packetman (Unix)
- SNMP Collector (Windows)
- Webboy (Windows)

Program Pemantau Jaringan