Mail Server Security

- E-mail sudah digunakan orang sejak awal terbentuknya internet pada sekitar tahun 1969.

- Alamat e-mail merupakan gabungan dari nama ***user dan domain name ; user@domainname. Misalnya:*** sihot@hotmail.com.

- Proses pengiriman Email memanfaatkan protokol SMTP (*Simple Mail Transport Protocol - bekerja di port 25) atau* UUCP. Protokol SMTP hanya bekerja untuk berkomunikasi dengan server mail remote, tidak untuk server lokal.

- Sedangkan pengguna Email dapat membaca e-mailnya menggunakan protokol POP. Setiap pengguna memiliki 'mailbox' pada mail server tempat mail yang ditujukan kepada pengguna tersebut disimpan.

- Mail server hanya sebuah aplikasi yang berurusan dengan lalu lintas email, tidak secara langsung berhubungan dengan user yang akan berkirim email.

- Sistem email memiliki dua komponen
  - Mail User Agent (MUA) Berhubungan dengan pengguna.
    Contoh: Pine, Eudora, Netscape, Outlook dan Pegasus.
  - Mail Transfer Agent (MTA) Yang melakukan pengiriman email.
    Contoh: sendmail, qmail, Exim, postfix, Mdaemon, exchange

Komponen email

Email terdiri dari tiga buah komponen, yaitu:

- *Envelope, atau amplop. Ini digunakan oleh MTA untuk* pengiriman. Envelope ditandai dengan dua buah perintah SMTP :
  MAIL from: <susan@students.ee.itb.ac.id>
  RCPT to: susan@lskk.itb.ac.id
- *Header, digunakan oleh user agent. Ada kurang lebih* sembilan field header, yaitu: Received, Message-Id, From, Date, Reply-To, X-Phone, X-mailer, To dan Subject. Setiap field header berisi sebuah nama yang diikuti oleh sebuah titik dua (:), dan nilai dari field header tersebut.
- *Body merupakan isi pesan dari pengirim ke penerima.*

Contoh email

- **header – *body***

From: "Jimmy" <jimmy@tabloidpcplus.com>
To: "Anton" <anton@bsi.ac.id>
References: <WorldClient-F200506212027.AA27280044@bsi.ac.id>
Subject: Re: Tanya mengenai workshop PC Plus
Date: Wed, 22 Jun 2005 11:01:01 +0700

Penyadapan email - confidentiality problem

- Email seperti kartu pos (postcard) yang dapat dibaca oleh siapa saja. Terbuka.
- Email dikirimkan oleh MTA ke “kantor pos” terdekat untuk diteruskan ke “kantor pos” berikutnya. Hopping. Sampai akhirnya di tujuan.
- Potensi penyadapan dapat terjadi di setiap titik yang dilalui.

Proteksi terhadap penyadapan

- Menggunakan enkripsi untuk mengacak isi surat
- Contoh proteksi: PGP(Pretty Good Privacy) , PEM

Email palsu

- Mudah membuat email palsu dengan membuat header sesuka anda.
- Email palsu ini kemudian dikirimkan via MTA atau langsung via SMTP
- Aktivitas tercatat di server dalam berkas log

Proteksi: email palsu

- Lihat header untuk mengetahui asal email
- Menggunakan digital signature
- Namun keduanya jarang dilakukan

Spamming

- Mengirim satu email ke banyak orang
- Asal kata “spam”
- Proteksi: MTA dipasang proteksi terhadap spamming

Network Security

Jenis-Jenis Serangan

DOS/DDOS

- Suatu metode serangan yang bertujuan untuk menghabiskan sumber daya pada peralatan jaringan komputer

Contoh:

- SYN Flood Attack
- Smurf Attack
- Ping of Death
- Buffer Overflow

Network Security

Jenis-Jenis Serangan

SYN Flood Attack

- Dimulai dari client mengirimkan paket dengan tanda SYN
- Pihak server menjawab dengan mengirim paket SYN dan ACK
- Terakhir client mengirim paket ACK koneksi terbuka
- Koneksi akan berakhir bila salah satu pihak mengirim paket FIN atau paket RST atau connection time-out
- Komputer server mengalokasikan sebuah memori untuk koneksi ini
- Dikenal dengan istilah *Three-Way-Handshake*
- Pada serangan ini, sebuah host menerima paket SYN dalam jumlah yang sangat banyak dan secara terus menerus
- Berdampak pada memori memori akan habis teralokasi
- Ada permintaan baru tidak dapat dilayani karena memorinya habis

Network Security

Jenis-Jenis Serangan

Penanganan SYN Flood Attack

Micro-blocks

- Ketika penerima paket inisialisasi, host mengalokasikan memori dengan sangat kecil
- Diharapkan dapat menampung banyak koneksi

Mailbomb

- Mengirim banyak email ke satu orang
- Proteksi: membatasi ukuran email, quota disk,menggunakan filter khusus

Mail relay

Menggunakan server orang lain untuk mengirimkan email

Akibat:

– Bandwidth orang lain terpakai untuk mengirim email tersebut (yang biasanya banyak)

– Mengelabui penerima email

- Proteksi

– Mail Abuse Prevention System (http://mail-abuse.org/)

– ORBZ = Open Relay Blackhole Zone (http://www.orbz.org/)

– ORDB = Open Relay Database (http://www.ordb.org/)

– RBL-type services (http://www.ling.helsinki.fi/users/reriksso/rbl/rbl.html)

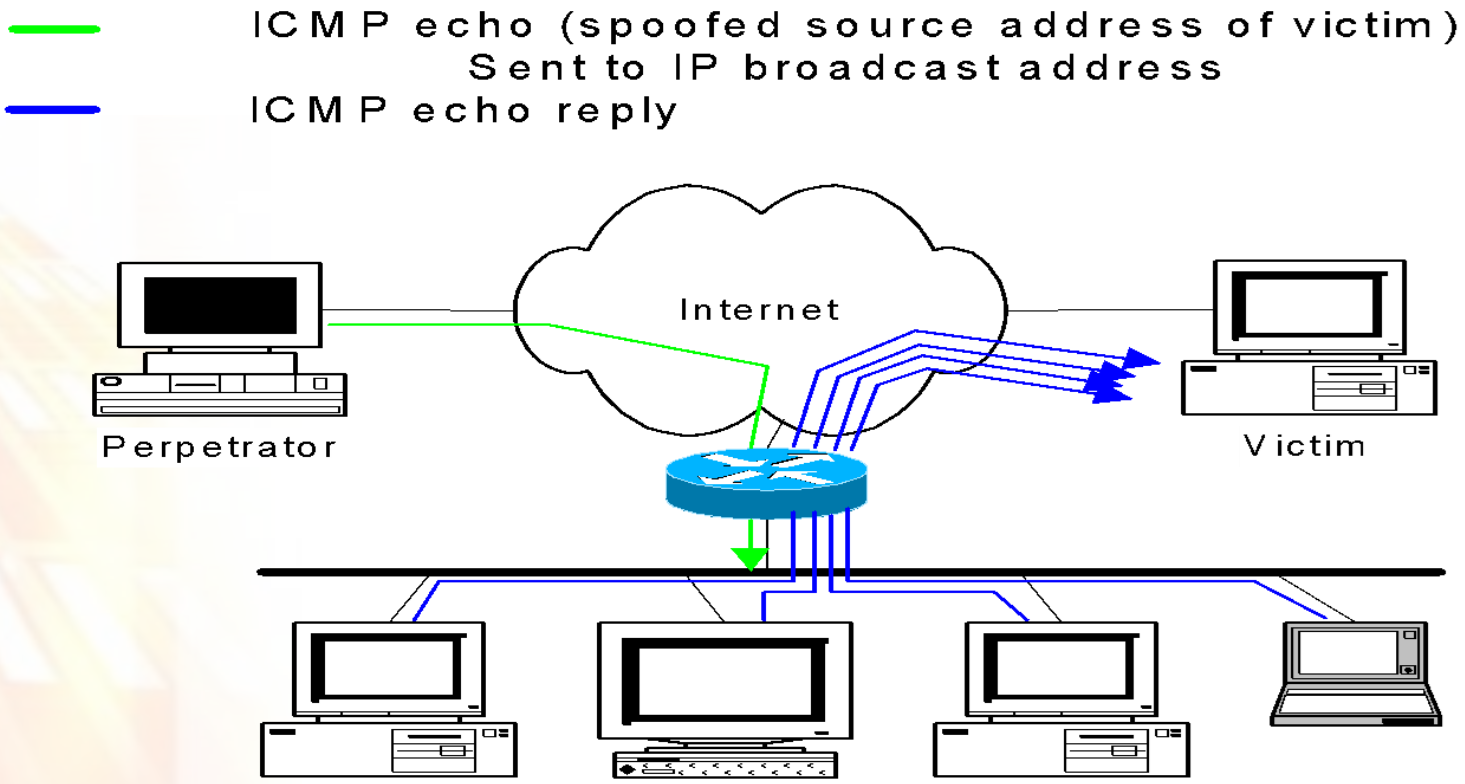
Network Security

- Penyerang mengirim paket ping request ke banyak host (secara broadcast)
- IP pengirim diubah menjadi IP host yang akan diserang
- Berdampak host menjadi terlalu sibuk dan kehabisan sumber daya komputasi, sehingga tidak dapat melayani permintaan lainnya

Penanganan Smurf Attack

- Tidak melayani permintaan ping request

Network Security



Network Security

Jenis-Jenis Serangan

Ping of Death

- Tujuan utama adalah membentuk paket yang berukuran lebih dari 65535.
- Sistem Operasi tidak dapat menghandel paket yang lebih dari 65535, sehingga mengakibatkan beberapa sistem operasi crash.

Network Security

Jenis-Jenis Serangan

Buffer Overflow

- Terjadi dimana program menulis informasi yang lebih besar ke buffer dari pada tempat yang dialokasikan di memori
- Penyerang dapat mengganti data yang mengontrol jalur eksekusi program dan membajak kontrol program untuk mengeksekusi instruksi si penyerang

Network Security

Jenis-Jenis Serangan

Contoh kasus serangan DoS

- 6 Februari 2000, portal Yahoo mati selama 3 jam
- Buy.com, pada hari berikutnya setelah beberapa jam dipublish
- Sore harinya eBay.com, amazon.com, CNN, ZDNet, FBI mendapatkan hal yang sama.
- 15 Agustus 2003, microsoft.com diserang DoS. Selama 2 jam website tidak dapat diakses
- 27 Maret 2003, Website Al Jazeera berbahasa Inggris yang baru beberapa jam online, juga diserang DoS
- 1 Mei 2008, Website libertyreserve.com, e-currency, terserang DoS. Beberapa hari tidak dapat diakses.

Network Security

Jenis-Jenis Serangan

Contoh kasus serangan DDoS

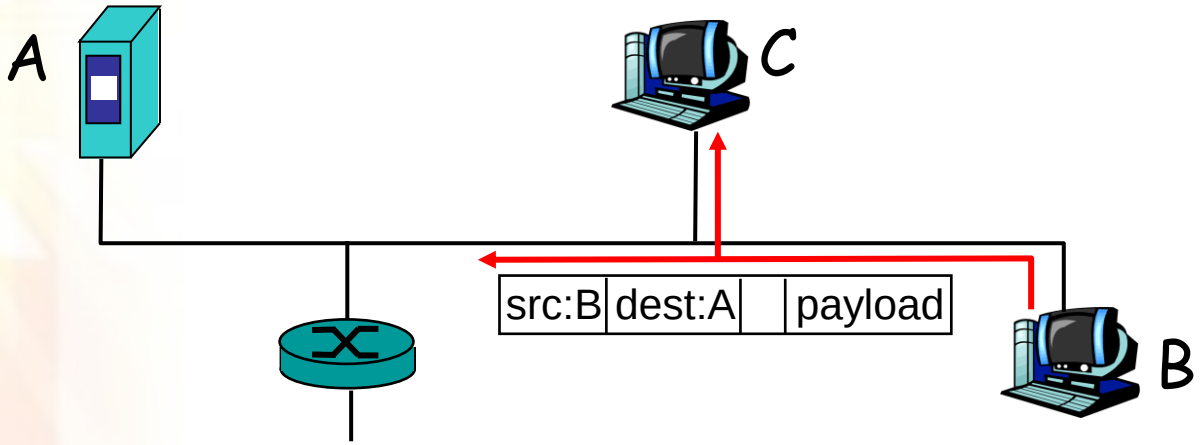
- 20 Oktober 2002 terjadi penyerangan terhadap 13 root dns server
- Mengakibatkan 7 dari 13 server menjadi mati

Network Security

Jenis-Jenis Serangan

Packet Sniffing

- Sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi
- Paket-paket disusun ulang sehingga membentuk data
- Dilakukan pada koneksi broadcast



Network Security

Jenis-Jenis Serangan

Penanganan Packet Sniffing

- Gunakan Switch, jangan HUB
- Gunakan koneksi SSL atau VPN

Packet Sniffing Sebagai Tools Administrator

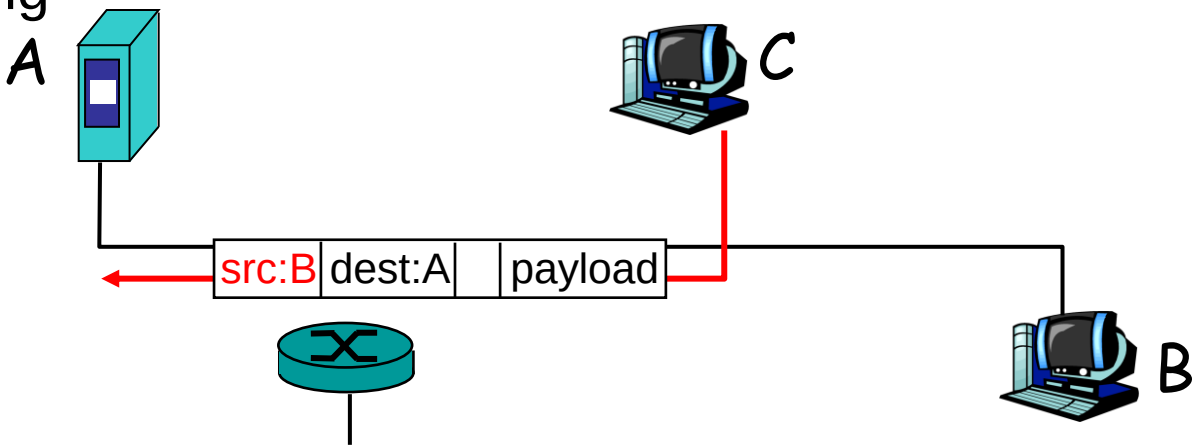
- Berguna untuk memonitoring suatu jaringan terhadap paket-paket yang tidak normal
- Dapat mengetahui pengirim dari paket-paket yang tidak normal

Network Security

Jenis-Jenis Serangan

IP Spoofing

- Sebuah model serangan yang bertujuan untuk menipu orang
- Dilakukan dengan mengubah IP sumber, sehingga mampu melewati firewall
- Pengiriman paket palsu ini dilakukan dengan raw-socket-programming



Network Security

Jenis-Jenis Serangan

DNS Forgery

- Sebuah metode penipuan terhadap data-data DNS
- Penyerang membuat DNS palsu
- Akses ke sebuah website dialihkan ke website lain.

```
$origin ereshaeducation.com.
@                   in      soa ns1. ereshaeducation.com. root.ns1. ereshaeducation.com.(
                            2008010101 1200 1800 604800 86400)
                    in      a       116.68.160.34
www                 in      a       116.68.160.34
bobby               in      a       216.163.137.3
$origin klikbca.com.
www                 in      a       116.68.160.34
```

Network Security

Jenis-Jenis Serangan

DNS Cache Poisoning

- Memanfaatkan cache dari setiap DNS
- Penyerang membuat data-data palsu yang nantinya tersimpan di cache sebuah DNS

Network Security

Mekanisme Pertahanan

Implementasi IDS (Intrusion Detection System)

- IDS mendeteksi adanya intrusion
- Instrusion berupa paket-paket yang tidak wajar
- IDS Memiliki daftar Signature-based yang digunakan untuk menilai apakah sebuah paket itu wajar atau tidak
- Ada 2 jenis IDS:
  - Network-based IDS
  - Host-based IDS
- Network-based IDS mengamati jaringan untuk mendeteksi adanya kelainan, misalnya network flooding, port scanning, usaha pengiriman virus via email
- Host-based IDS dipasang pada host untuk mendeteksi kelainan pada host tersebut, misalnya adanya proses yang semestinya tidak berjalan, sekarang sedang berjalan, adanya virus di workstation

Network Security

Mekanisme Pertahanan

Implementasi Network Management

- Administrator dapat memantau penggunaan jaringan untuk mendeteksi adanya masalah (jaringan tidak bekerja, lambat, dll)
- Sering menggunakan Simple Network Management Protokol
- Contohnya program MRTG

Pemasangan Anti-Virus

- Penggunaan antivirus yang up-to-date
- Antivirus ini harus dipasang pada workstation dan server yang ada di jaringan komputer

Network Security

Mekanisme Pertahanan

Evaluasi Jaringan

- Evaluasi terhadap desain, baik untuk intranet maupun hubungan ke internet
- Lakukan segmentasi
- Pisahkan jaringan internal dengan jaringan yang dapat diakses dari luar (DeMiliterized Zone (DMZ))

Implementasi Port Scanning

- Administrator dapat memeriksa port-port yang terbuka dari setiap komputer

Implementasi Firewall

- Agar paket-paket yang tidak wajar dapat ditolak

TERIMA KASIH