Network Security

YAYASAN SASMITA JAYA

Program Studi Teknik Informatika, Universitas Pamulang

Network Security

Apa itu jaringan komputer?

- 2 atau lebih komputer yang saling terinterkoneksi dan dapat saling bertukar informasi
- Jaringan komputer terbagi atas beberapa lapisan yang saling independen satu sama lain
- Lapisan-lapisan ini disebut protokol
- Lapisan-lapisan yang dimiliki:
  - Physical
  - Data Link
  - Network
  - Transport
  - Session
  - Presentasion
  - Application
- Disebut juga OSI (Open System Interconnection)

Network Security

Apa itu jaringan komputer?

- Contoh protokol: TCP/IP, IPX/SPX, APPLETALK, NETBEUI, dll.
- Yang banyak digunakan adalah TCP/IP
- Terdiri dari 4 lapisan
  - Link (Lapisan OSI 1 dan 2)
  - Internetwork (Lapisan OSI 3)
  - Transport (Lapisan OSI 4 dan 5)
  - Application (Lapisan OSI 5 sampai 7)

Network Security

Proteksi Jaringan Komputer

Layer 2

- Mac Address Authentication

  Pengontrolan dilakukan pada switch/hub dan wireless access point
- WEP/WPA (Wired Equivalent Privacy/Wi-Fi Protected Access)

  Data yang dikirim dienkripsi terlebih dahulu

Layer 3

- Perlindungan dilakukan berdasarkan alamat IP dan Port

Network Security

Proteksi Jaringan Komputer

Layer 4/5

- Pengamanan lebih difokuskan dalam mengamankan data yang dikirim

  Misalnya dengan VPN (Virtual Private Network)

Layer 7

Metode yang digunakan

- SSL (Secure Socket Layer)

  Misalnya
  - mengakses url web: https://domain.com
  - mengakses komputer remote dengan ssh (secure shell) dan scp (secure copy)

Network Security

Proteksi Jaringan Komputer

- Application firewall
  - Pemeriksaan dilakukan pada keseluruhan data yang diterima oleh aplikasi
  - Paket data disatukan kemudian diperiksa apakah data yang dikirimkan berbahaya atau tidak
  - Bila ditemukan berbahaya untuk sebuah aplikasi, data tersebut disingkirkan atau dibuang
  - Dipasang di setiap komputer,
  - Dapat mengakibatkan lamanya data yang sampai ke aplikasi.
  - Contoh: Pengecekan email pada email client

Network Security

Jenis-jenis serangan:

- DOS/DDOS (Denial of Services/Distributed Denial of Services)
- Packet Sniffing
- IP Spoofing
- DNS Forgery

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

Network Security

Jenis-Jenis Serangan

Smurf Attack

- Menggunakan paket ping request
- **PING** akan mengirim satu paket data ke salah satu alamat, lalu alamat-nya akan membalas prosesnya dicatat dalam bentuk lamanya waktu

```
C:\WINDOWS>ping 204.50.137.29

Pinging 204.50.137.29 with 32 bytes of data:

Reply from 204.50.137.29: bytes=32 time=21ms TTL=252
Reply from 204.50.137.29: bytes=32 time=34ms TTL=252
Reply from 204.50.137.29: bytes=32 time=19ms TTL=252
Reply from 204.50.137.29: bytes=32 time=37ms TTL=252

Ping statistics for 204.50.137.29:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum =  37ms, Average =  27ms
```

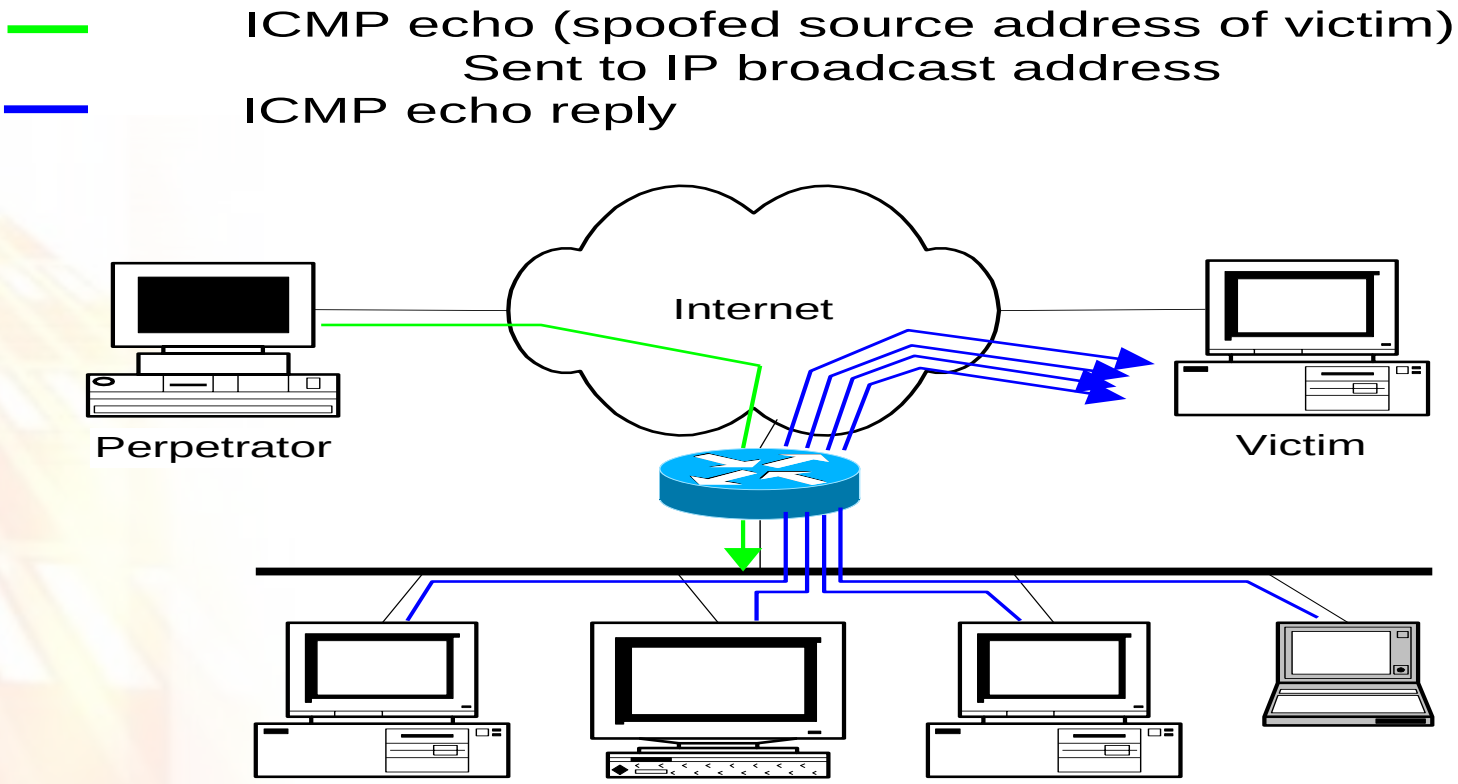
Network Security

- 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

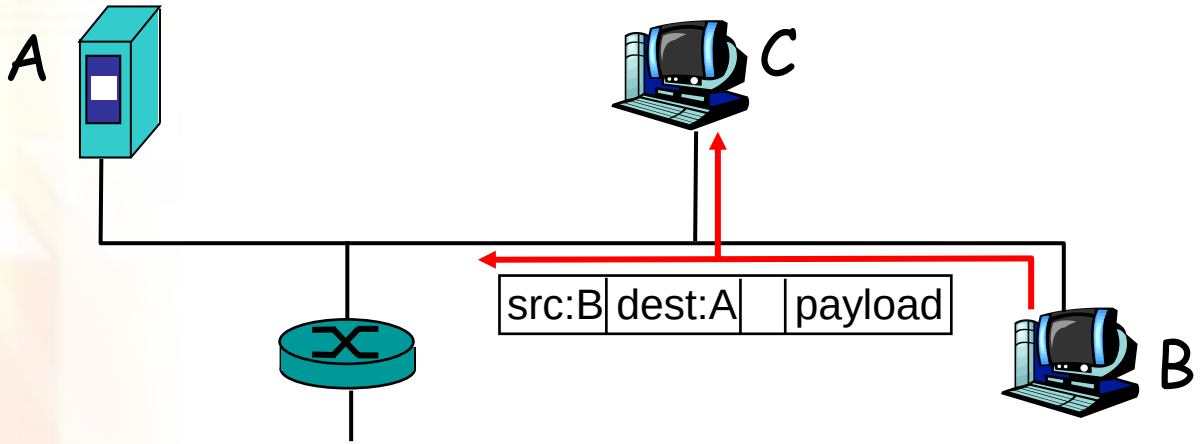
- 20 Oktober 2002 terjadi penyerangan terhadap 13 root dns server
- Mengakibatkan 7 dari 13 server menjadi mati

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

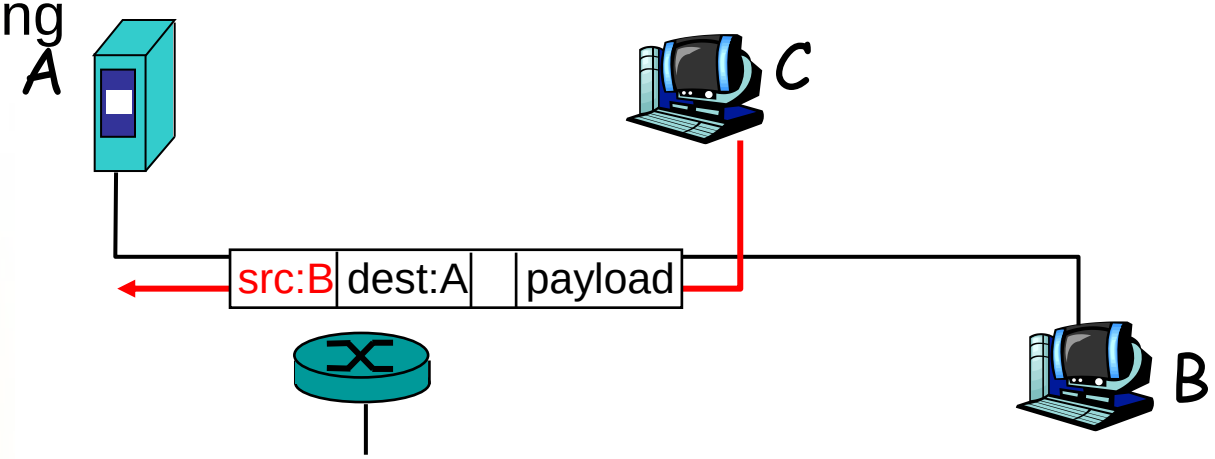
- Berguna untuk memonitoring suatu jaringan terhadap paket-paket yang tidak normal
- Dapat mengetahui pengirim dari paket-paket yang tidak normal

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