Elemen Keamanan

Elemen Keamanan Komputer

- Privacy / Confidentiality
- Integrity
- Availability
- Authentication
- Nonrepudiation

Confidentiality/ Privacy

Menjaga informasi dari orang yang tidak berhak mengakses.

Contoh Ancaman :

E-mail seorang pemakai (user) tidak boleh dibaca oleh orang lain termasuk administrator.

Menjaga rahasia yang berkaitan dengan data-data pribadi user seperti password, tanggal lahir ataupun data lainnya.

Integrity

Informasi yang di kirim secara menyeluruh, lengkap dan tidak diubah oleh pihak tertentu.

Contoh Ancaman **:**

E-mail di intercept di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.

Serangan : Man In the Middle Attack

Authentication

Pihak yang terlibat dengan pertukaran informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.

Dukungan :
Digital Signature : Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking(untuk menjaga “intellectual property”, 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

Ketersediaan informasi pada saat dibutuhkan

Contoh Ancaman :
Serangan DoS atau Denial Of Services, Suatu layanan (server) dikirimi permintaan (palsu) secara terus menerus sehingga tidak dapat melayani permintaan lain yang mengakibatkan server menjadi down, crash.

MailBomb yaitu alamat email user di kirim pesan oleh email lain yang tidak dikenal dengan ukuran yang besar dan terus menerus sehingga user kesulitan untuk mengakses alamat emailnya.

NonRepudiation

Menjaga agar seseorang tidak menyangkal telah melakukan sebuah transaksi

Contoh ancaman pada E-Commerce dan transaksi elektronik

Model Serangan

***Interruption*:** Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan *(availability*) dari sistem. Contoh serangan adalah “denial of service attack”.

***Interception*:** Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan.

Model Serangan

***Modification*n:** Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah informasi. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.

***Fabrication*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.

Istilah dalam Keamanan Komputer

- Bug atau kesalahan kode yang terdapat pada suatu sistem atau program
- Vulnerable atau kelemahan dalam sebuah sistem baik program, design ataupun implementasi.
- Threat adalah ancaman yang timbul karena adanya vulnerable
- Exploit (local, remote) Software, tool, teknik ataupun langkah-langkah untuk melakukan serangan terhadap salah satu elemen keamanan.
- Attack atau serangan.
- Patch atau Update terbaru dari suatu program atau sistem, dapat berupa penambahan fitur, meningkatkan performa atau memperbaiki kelemahan-kelemahan.
- Security hole atau lubang security
- Security issue atau isu tentang keamanan
- Penetration testing atau tindakan percobaan masuk ke sebuah sistem

Istilah dalam Keamanan Komputer

- Security Auditor / Security Analis atau orang-orang yang bekerja di bidang keamanan komputer, melakukan analisa dan audit terhadap suatu sistem.
- Attacker atau orang yang melakukan serangan pada suatu sistem.
- Intruder atau orang yang menyusup masuk ke dalam sebuah sistem
- Proof of Concept atau pembuktian dari teori-teori kelemahan

Istilah Pelaku Serangan

- **Black Hat Hacker**
  Hacker Perusak / Cracker
- **White Hat Hacker**
  Profesional yang bekerja pada perusahaan keamanan, security analys, security consultan
- **Grey Hat Hacker**
  Antara Black dan White Hat Hacker
- **Suicide Hacker**
  Teroris

Serangan Pada Sistem Keamanan Komputer

Morris: Pada bulan November 1988

Mahasiswa program Sarjana Robert Morris, menyebarkan apa yang kemudian disebut sebagai worm internet yang paling merusak sepanjang sejarah, berdasarkan jumlah komputer yang mati karenanya. Saat itu, lebih dari 10% dari layanan online lumpuh sehingga menyebaban kerugian lebih kurang **US$15 juta**

Serangan Pada Sistem Keamanan Komputer

Virus Melissa :

Ditulis oleh David Smith, Menyebar pada April 1999 virus ini menjadi salah satu yang paling merusak pada masa itu. Melissa mengilhami cara penyebaran virus saat ini, seperti Slammer dan SoBig. Melissa, merupakan virus macro yang menyusup di ratusan komputer, sejumlah pakar memperkirakan ada **sebanyak 20% dari komputer di internet lumpuh** ketika itu.

Serangan Pada Sistem Keamanan Komputer

- **Adrian Lamo**

  Adrian harus membayar **$ 65.000 untuk serangan ke intranet New York Times**, ia juga dihukum 6 bulan kurungan dan 2 tahun percobaan.

- **Jonathan James (Kamerad)**

  Jonathan meng-hacked password komputer dan nama pengguna Defense Threat Reduction Agency dan mampu memeriksa email-email rahasia dari organisasi ini, James juga meng-hack komputer NASA dan mencuri software dengan harga lebih dari **$ 1,7 juta,** sehingga mereka harus mematikan seluruh sistem komputer dan biaya pembayaran pajak **$ 41.000.**

Serangan Pada Sistem Keamanan Komputer

- **Kevin Mitnick**

  Hacker paling terkenal dalam sejarah komputer abad 20, dikarenakan dia adalah hacker pertama yang masuk ke dalam daftar orang yang paling dicari oleh FBI.

  Tsutomou Shimomura, **seorang ahli keamanan komputer** ternama, menemukan bahwa sistem miliknya telah disusupi. Si penyerang telah berhasil mencuri data dari komputer Shimomura yang digunakan dalam pemrograman ponsel dan sistem keamanan. Nilai dari perangkat lunak yang diambil dianggap lebih dari **US$500.000**.

Serangan Pada Sistem Keamanan Komputer

Dani Firmansyah :
Membobol situs KPU 2004 dan mengubah nama-nama partai di dalamnya menjadi nama-nama unik seperti Partai Kolor Ijo, Partai Mbah Jambon, Partai Jambu, dan lain sebagainya.

2009 : Perang cyber antara hacker indonesia dan hacker malaysia, aksi deface website-website resmi kedua negera, sebanyak kurang lebih 125 situs terinfeksi serangan hacker.

Ancaman Pada Sistem Keamanan Komputer

Ancaman Pada Sistem Keamanan Komputer

- Social engineering
- Keamanan fisik
- Security hole pada sistem operasi dan services
- Serangan pada jaringan komputer
- Serangan via aplikasi berbasis web
- Trojan, backdoor, rootkit, keylogger, Virus, worm

Social Engineering

Ancaman

- Mengaku sebagai penanggung jawab sistem untuk mendapatkan account user

Solusi

- Mendidik semua lapisan user yang terdapat di suatu perusahaan.

Keamanan Fisik

Ancaman

- Pembobolan ruangan sistem komputer
- Penyalahgunaan account yang sedang aktif yang ditinggal pergi oleh user
- Sabotase infrastruktur sistem komputer (kabel, router, hub dan lain-lain)

Solusi

- Konstruksi bangunan yang kokoh
- Pengamanan secara fisik infrastruktur sistem komputer
- CPU ditempatkan di tempat yang aman
- Router, Switch, dan peralatan jaringan ditempatkan yang aman dari jangkauan.

Security hole pada OS dan Services

Ancaman

- Bug dan Buffer over flow yang menyebabkan local/remote exploit
- Kesalahan konfigurasi
- Installasi default yang mudah diexploit

Bug dan Buffer Overflow

- **BUG**

  Suatu kesalahan desain pada suatu perangkat keras komputer atau perangkat lunak komputer yang menyebabkan peralatan atau program itu tidak berfungsi semestinya.

- **Buffer Overflow**

  Serangan Buffer overflow terjadi ketika si Attacker memberikan input yang berlebihan pada program yang di jalankan, sehingga program mengalami kelebihan muatan dan memory tidak dapat mengalokasikannya. Ini memberikan kesempatan kepada Attacker untuk menindih data pada program dan men-takeover kontroll program yang dieksekusi attacker.

Bug dan Buffer Overflow

Pencegahan

Sisi Programmer:

Coding dengan teliti dan sabar sehingga kemungkinan kekeliruan coding yang menyebabkan buffer over flow dapat dihindari

Sisi User

Selalu mengikuti informasi bug-bug melalui milis dan situs-situs keamanan (Securityfocus.com dan lain-lain)
Update..update..update

Kesalahan Konfigurasi

Ancaman

Sistem dapat diakses dengan mudah dari host yang tidak berhak
Privilege yang dapat diexploitasi

Pencegahan

Pengaturan hak akses host yang ketat
Pengaturan *privilege* yang ketat

Instalasi Default

Ancaman

- Services yang tidak diperlukan memakan *resource*
- Semakin banyak services semakin banyak ancaman karena bug-bug yang ditemukan
- Password default mudah ditebak
- Sample program dapat diexploitasi
- Dan lain-lain

Pencegahan

- Nyalakan services yang diperlukan saja
- Konfigurasikan seaman mungkin
- Buang semua yang tidak diperlukan setelah installasi
- Dan lain-lain

Ancaman Pada Jaringan Komputer

Ancaman

- Sniffing (penyadapan)
- Spoofing (pemalsuan)
- Session hijacking (pembajakan)
- DOS / DDOS attack

Sniffing

Bagaimana Sniffing terjadi?

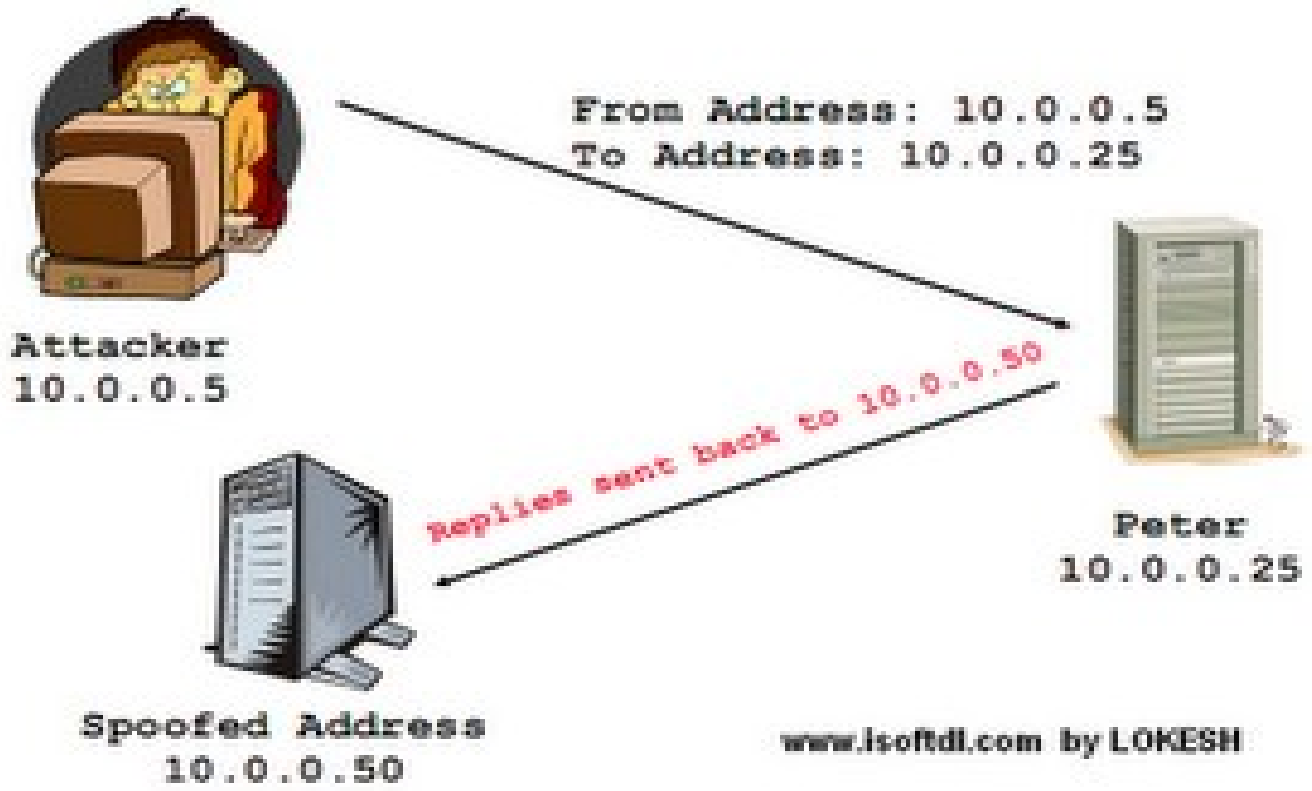
Tindakan penyadapan pada lalu lintas jaringan komputer

Pencegahan

Menggunakan Enkripsi (SSL, SSH, PGP, dan lain-lain)

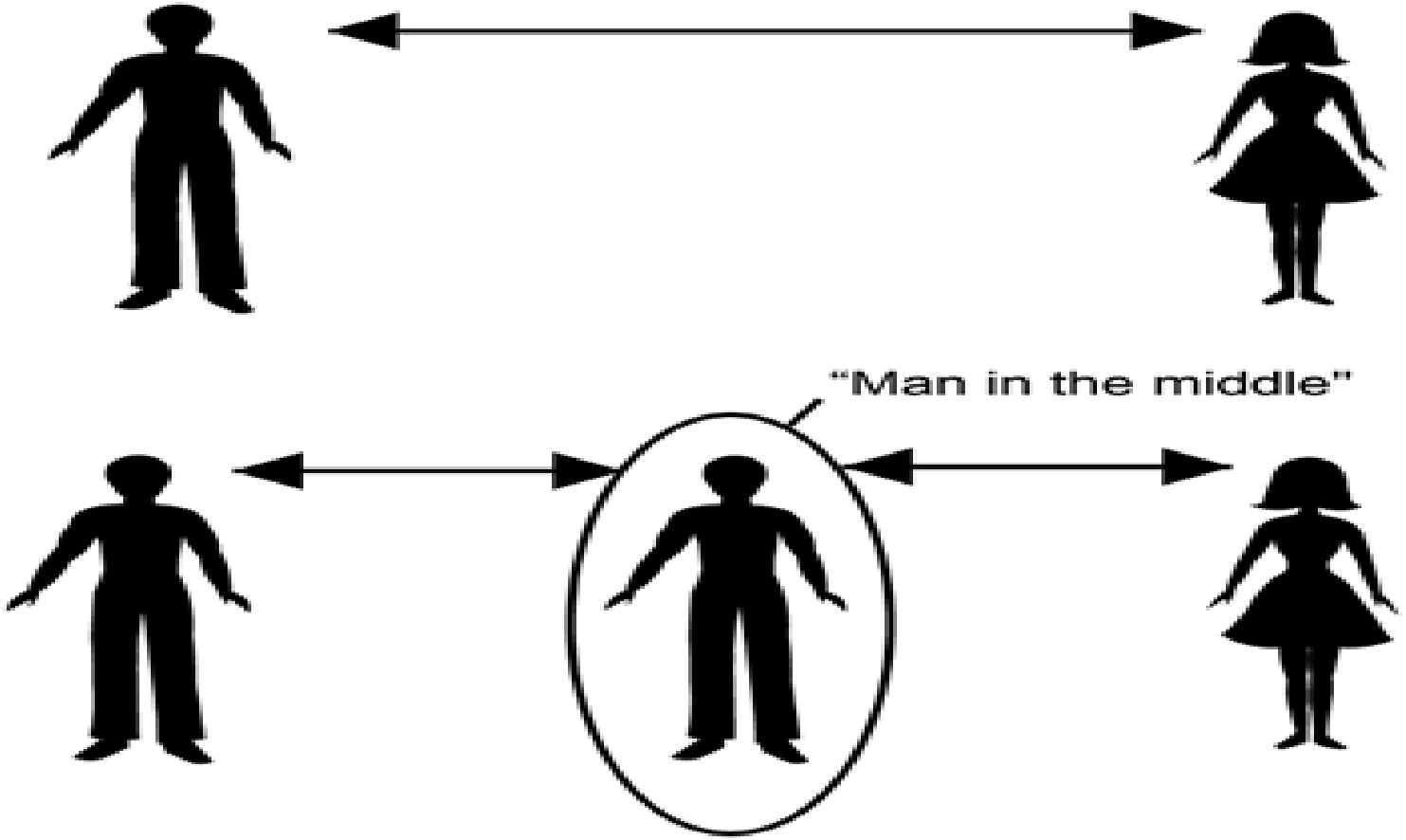
Spoofing

- IP Spoofing
  Pemalsuan Source IP Address

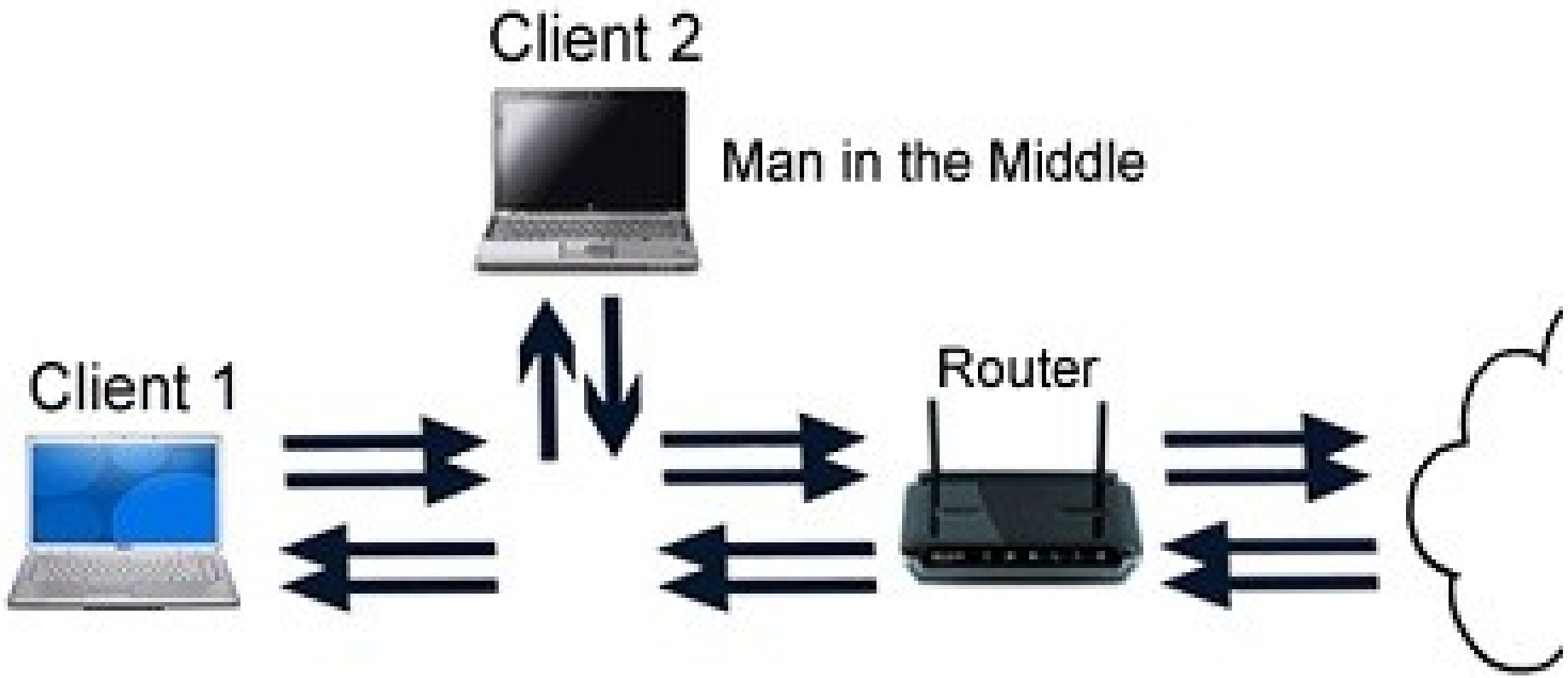


Spoofing

- Spoofing atau Pemalsuan Middle Attack

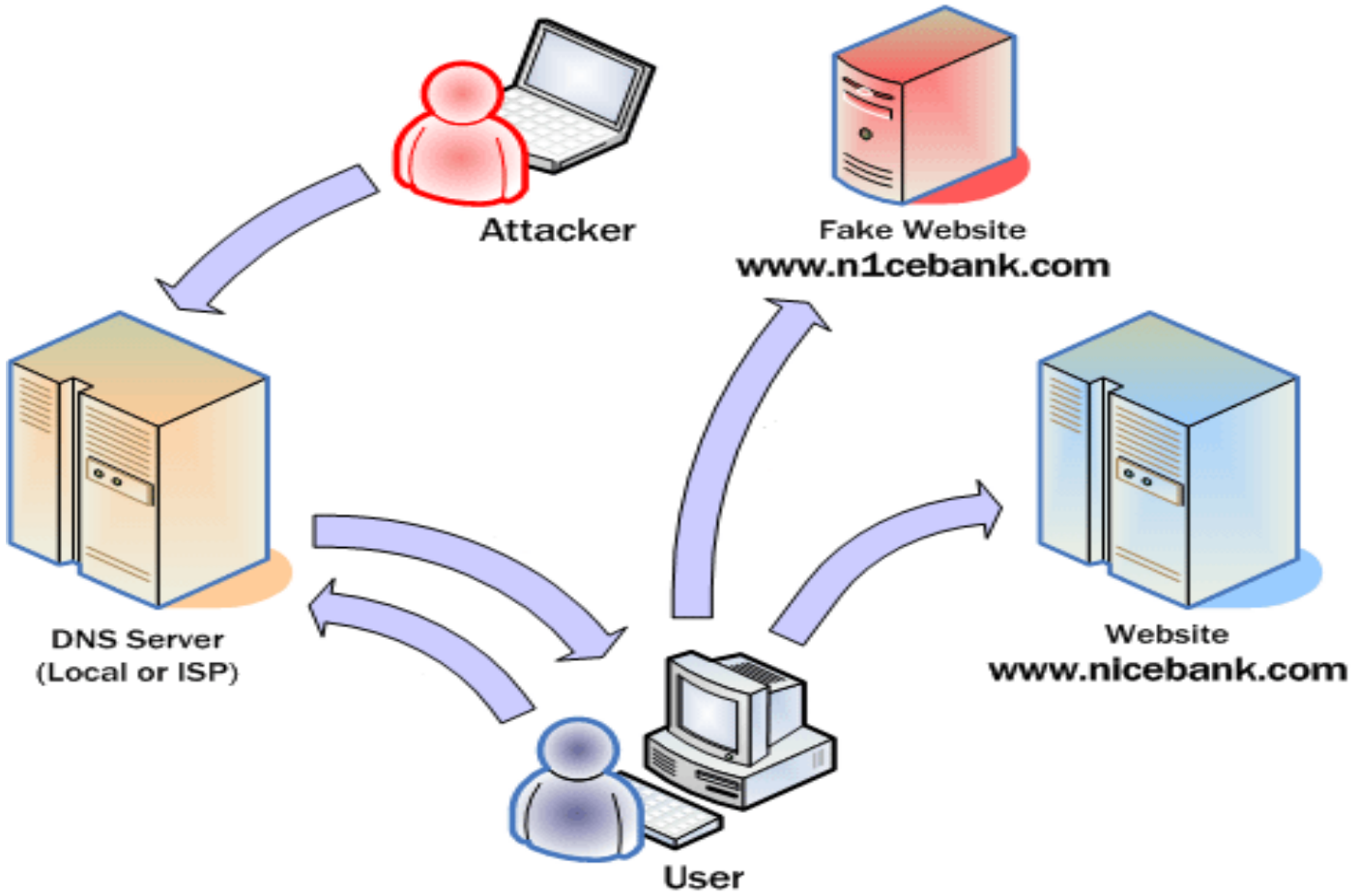


Middle Attack



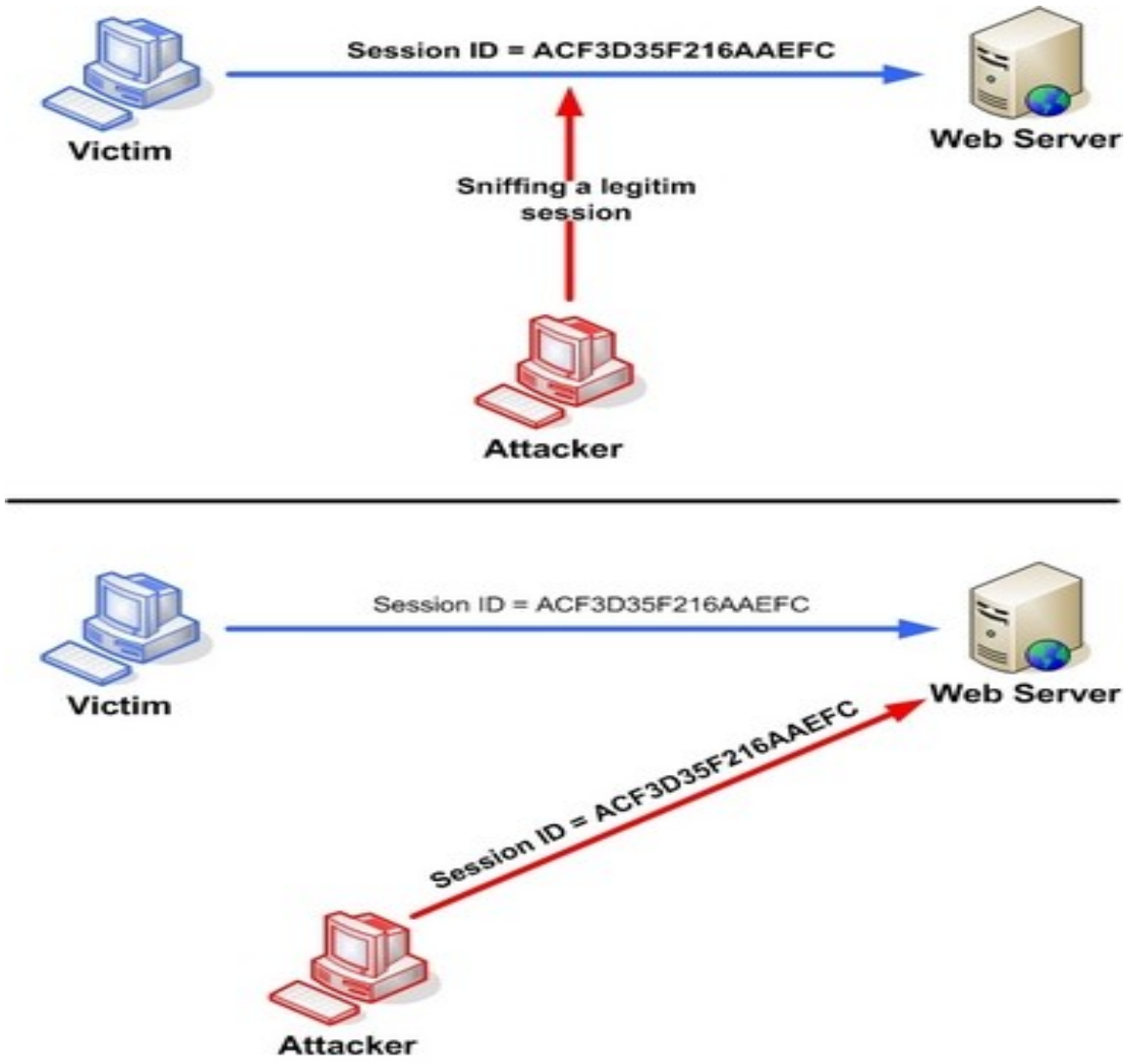
DNS Spoofing

- DNS Spoofing

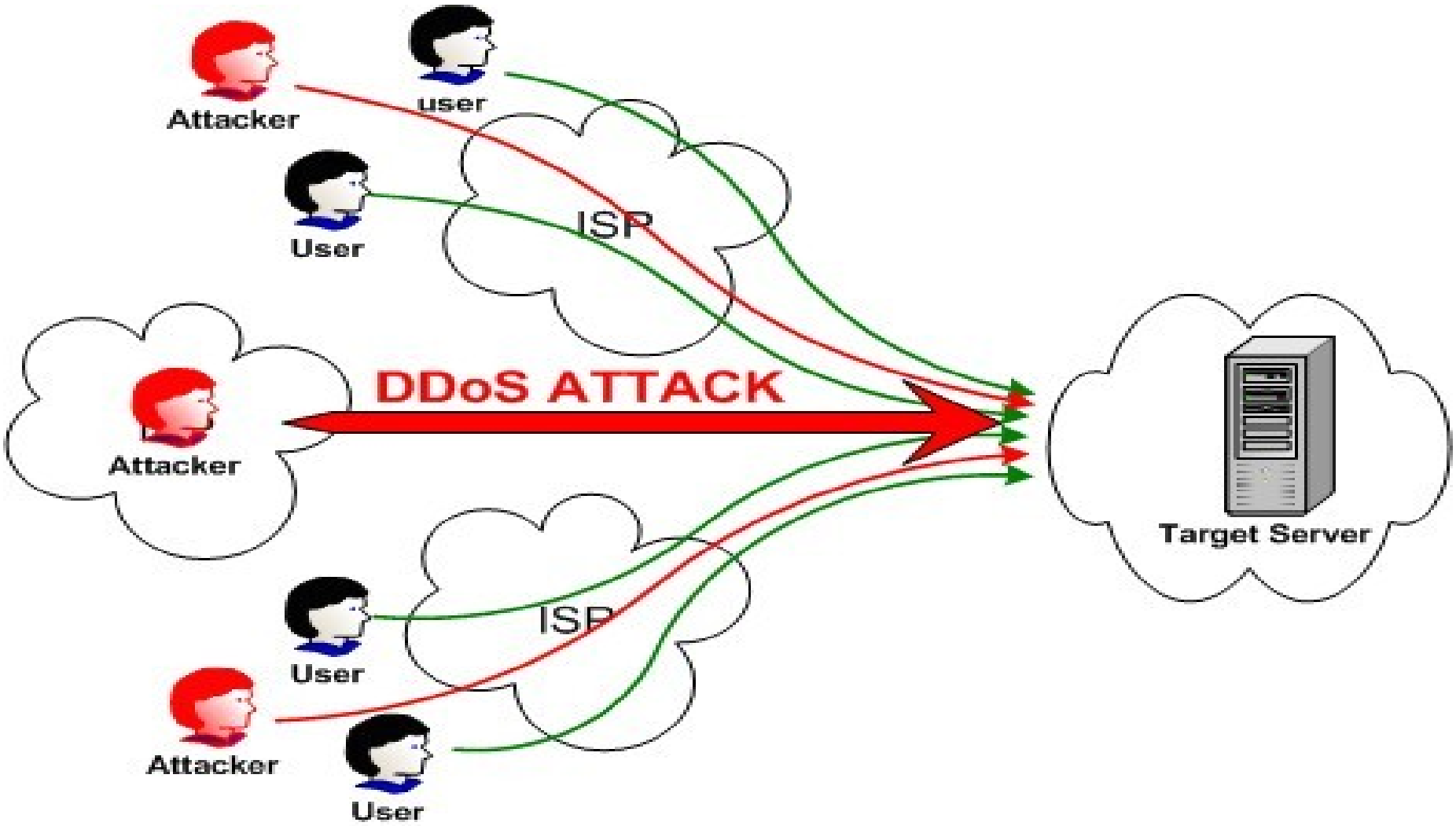


Session Hijacking

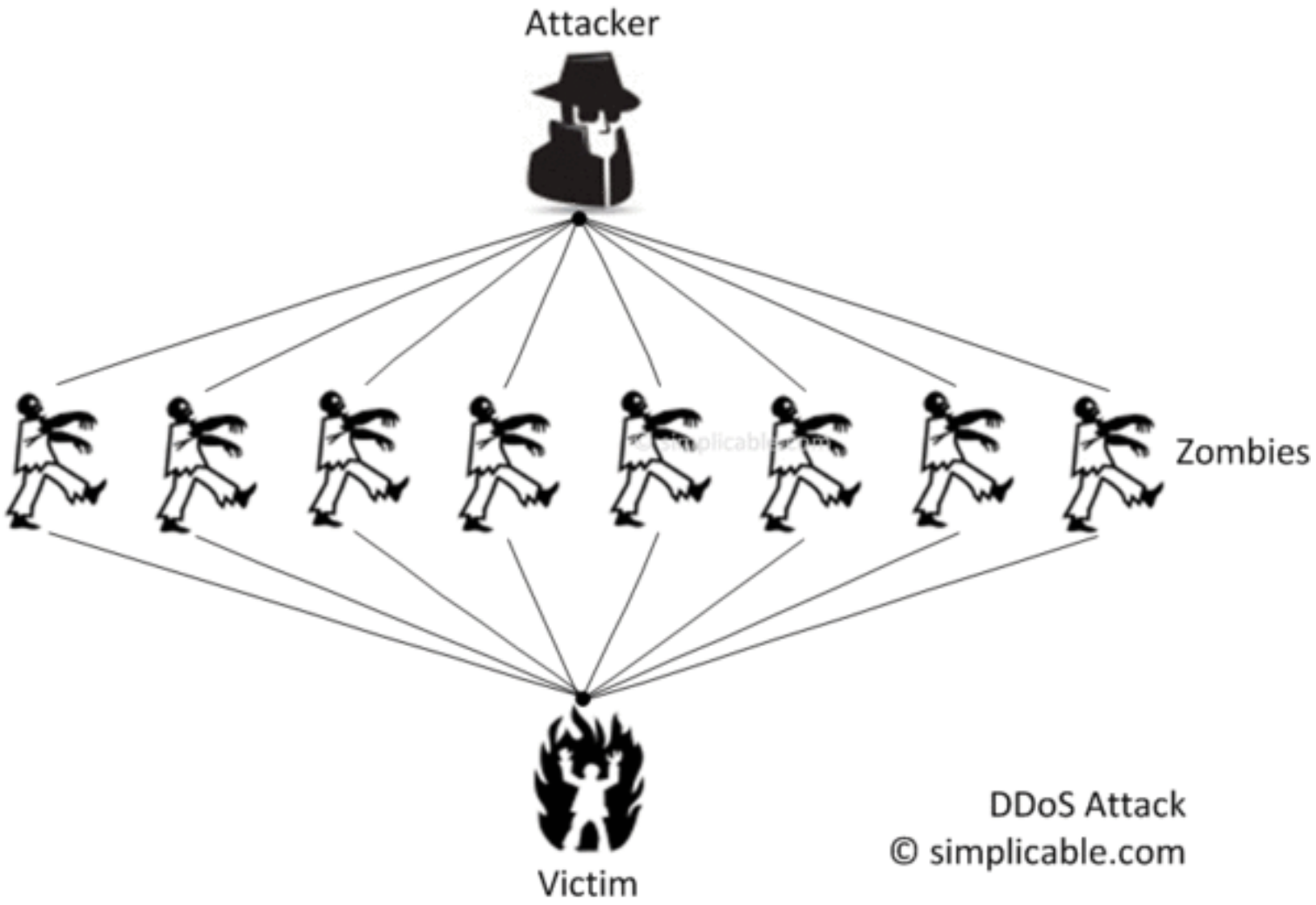
Pembajakan Sesi



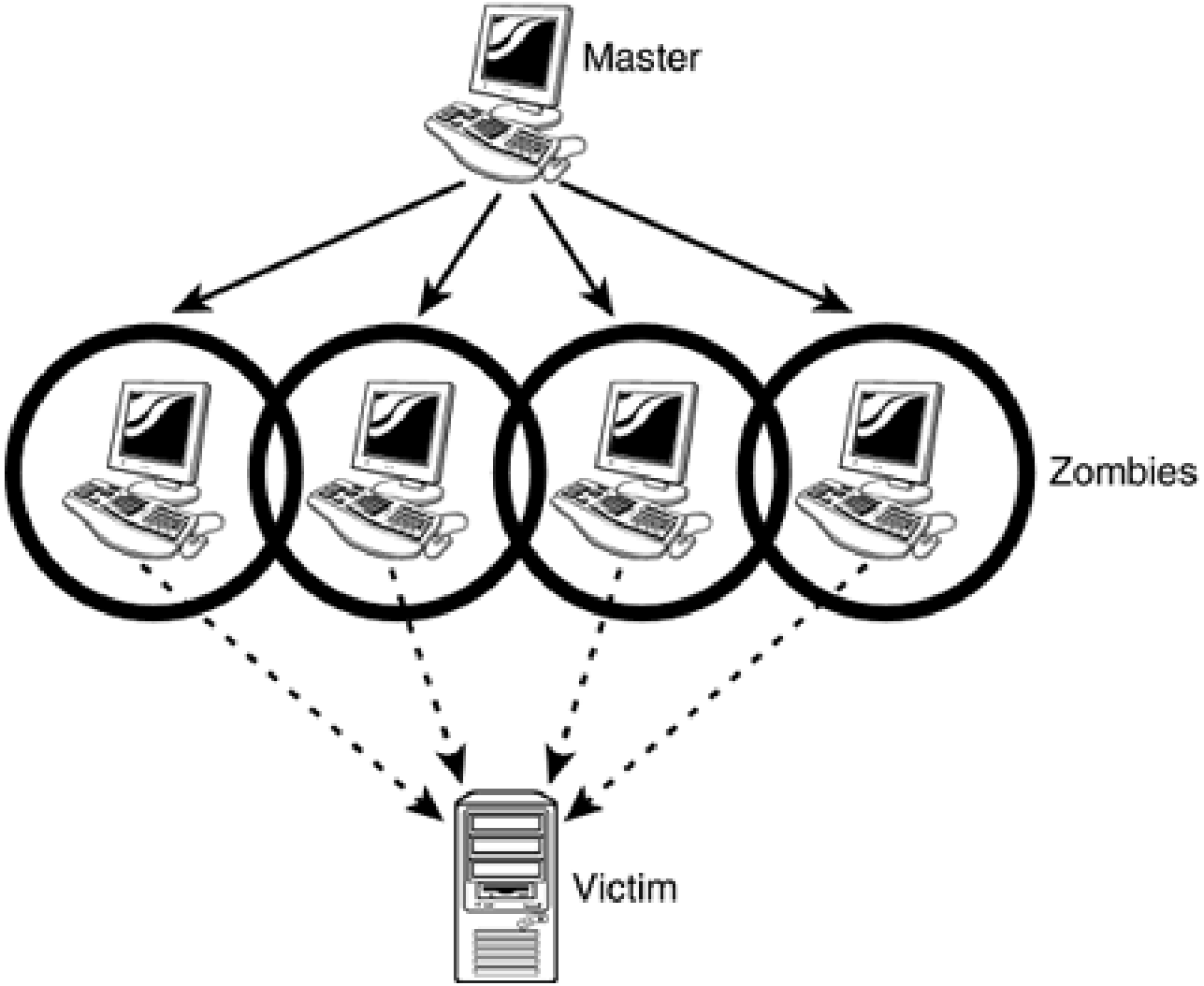
DOS / DDOS Attack



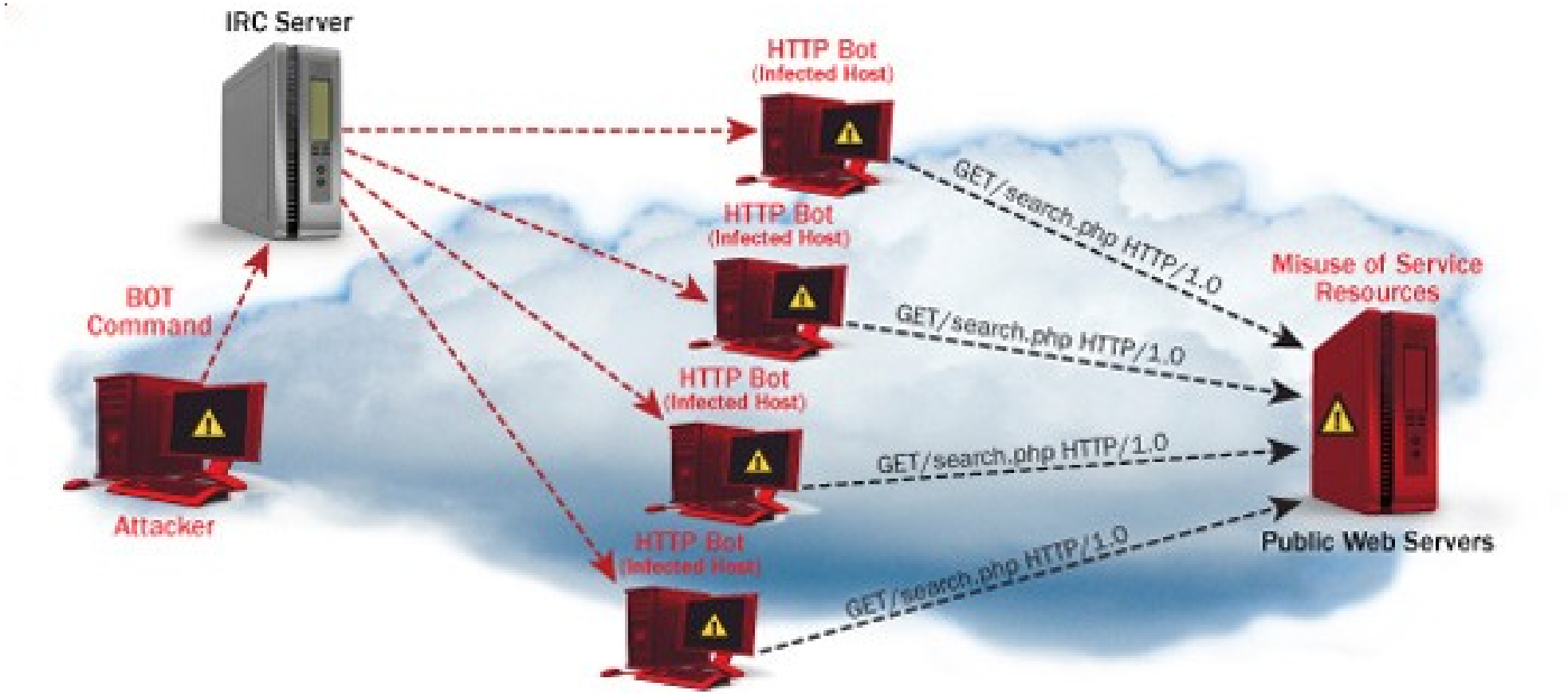
DDOS



DDOS



DDOS Bot


IRC Server
HTTP Bot
(Infected Host)
HTTP Bot
(Infected Host)
HTTP Bot
(Infected Host)
HTTP Bot
(Infected Host)
BOT
Command
Attacker
GET/search.php HTTP/1.0
GET/search.php HTTP/1.0
GET/search.php HTTP/1.0
GET/search.php HTTP/1.0
Misuse of Service
Resources
Public Web Servers

Serangan Pada Aplikasi Web

- Unvalidated Input
  - Cross Site Scripting (XSS)
  - Code Injection

- Privileges / Kesalahan Hak Akses (Shell Upload)
- Server Configuration
- Password Encryption

Virus Family

Virus, Trojan, backdoor, keylogger, worm
Program-program kecil yang dapat membahayakan komputer.

Virus
sebuah program kecil yang bisa menggandakan dirinya sendiri dalam media penyimpanan suatu komputer.

Worm
Worm berdiri sendiri dan tidak membutuhkan interaksi terhadap dirinya (exe). Worm mampu menduplikasi dirinya sendiri di dalam komputer dalam jumlah yang sangat banyak. Umumnya worm di desain untuk menyerang email dan mengirimkannya ke semua daftar kontak email

Trojan
Program yang kelihatan seperti program yang valid atau normal, tetapi sebenarnya program tersebut membawa suatu kode dengan fungsi-fungsi yang sangat berbahaya bagi komputer Anda.

Virus

- Backdoor
  Bagian dari trojan yang membuka “pintu belakang” pada PC sebagai akses untuk hacker. Sebagian hacker bahkan berhasil mendapatkan kendali penuh atas PC dengan menggunakan backdoor ini.

- Keylogger
  Keylogger merupakan software/hardware yg bekerja dengan cara merekam setiap tombol yang ditekan pada keyboard