

**Contoh Penulisan ABSTRAK dalam bahasa Indonesia pada Buku
TUGASAKHIR (BUKAN PADA FORMAT JURNAL)**

ABSTRAK

(Ukuran Font 14)

**STUDI DAN ANALISIS ICMP TRACEBACK UNTUK
PENANGANAN SERANGAN DISTRIBUTED DENIAL of
SERVICE PADA JARINGAN KOMPUTER**

(Ukuran Font 13)

Oleh

(Ukuran Font 12)

Nama Mahasiswa

10102xxx

(Ukuran Font 13)

(Isi ABSTRAK Ukuran Font 12, ukuran spasi 1)

Serangan *Distributed Denial of Service* (DDoS) muncul pertama kali di summer1999. Serangan macam ini dapat melibatkan ratusan atau beribu-ribu mesin *weakly-secured* (sistem keamanan lemah), serangan ini menyebabkan kerusakan pada program servis standar jaringan, dan melemahkan konfigurasi sistem operasi. Setelah menerobos komputer (lewat *hacking*), attacker menginstal software DDoS pada mesin-mesin tersebut, sehingga *attacker* dapat mengendalikan semua mesin untuk melakukan serangan secara terkoordinasi ke korban. Cara lain menginstall software di komputer lain adalah menggunakan *social engineering* lewat e-mail atau chat lewat internet. Serangan DDoS secara khas membuat bandwidth meningkat, kapasitas pemrosesan router meningkat, *resource network* menjadi *stack*, dan membuat koneksi ke jaringan korban sulit.

Serangan DDoS sangat sukar dicegah oleh karena sifat jaringan Internet terbuka, basis interkoneksi ke Internet adalah protokol, ini dapat digunakan sebagai beberapa cara untuk meniadakan servis. Hal yang sulit dan kadang-kadang mustahil untuk mendeteksi asal suatu serangan terdistribusi sebab *hackers* dapat menyembunyikan identitas mereka dengan menggunakan pihak ketiga, seperti lewat *private channel* pada IRC (*Internet Relay Chat*). Mereka juga dapat memberikan *IP address* palsu, spoofing, ke dalam paket yang dikirimkan ke mesin *intermediate* (perantara).

Banyak paper yang menuliskan metode penanggulangan serangan DDoS seperti *ICMP Traceback*, *Probabilistic IP Traceback*, *Phusback*, *Tunneling - IP Overlay*, *Mengontrol flooding*, *Ingress Filtering*, *Egress Filtering*, *Center track*, dan *Honeypots*.

Dst.....

**Contoh Penulisan ABSTRAK dalam bahasa Inggris pada Buku
TUGASAKHIR (BUKAN PADA FORMAT JURNAL)**

ABSTRACT

(Ukuran Font 14)

**STUDY AND ANALYSIS ICMP TRACEBACK FOR DEFENSE
AGAINST DISTRIBUTED DENIAL of SERVICE ATTACKS IN
COMPUTER NETWORK**

(Ukuran Font 13)

by

(Ukuran Font 12)

Nama Mahasiswa

10102xxx

(Ukuran Font 13)

(Isi ABSTRACT Ukuran Font 12, ukuran spasi 1)

Distributed denial of service (DDoS) attacks first appeared in the summer 1999. This kind of attack can involve breaking into hundreds or thousands of weakly secured machines, using well-known defects in standard network service programs, and common weak configurations in operating systems. After breaking into computers the attacker installs DDoS software on them, allowing him to control all these burgled machines to launch coordinated attacks on victim sites. Another way to get software installed on other computers is to use social engineering by e-mail or Internet chat. These attacks typically exhaust bandwidth, router processing capacity, or network stack resources, breaking network connectivity to the victims.

DDoS attacks are difficult to prevent because of the open, interconnected nature of the Internet and its underlying protocols, which can be used in several ways to deny service. It is difficult and sometimes impossible to detect the origin of a distributed attack because hackers may hide their identity using third parties, such as private chat channels on IRC (Internet Relay Chat). They can also insert a false return IP address, spoofing, into the packets that an intermediate machine sends.

Many paper writing down method handling of DDOS attacks like : ICMP Traceback, Probabilistic IP Traceback, Phusback, Tunneling - IP Overlay, Controlling flooding, Ingress Filtering, Egress Filtering, Center Track, and Honeypots

Next explain.....