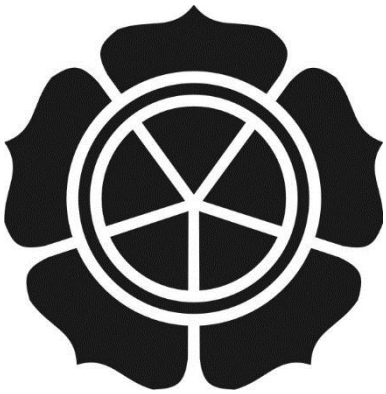
ANALISIS SERANGAN MALWARE MENGGUNAKAN WIRESHARK PADA SIMULASI JARINGAN DI MININET

SKRIPSI



disusun oleh:

Basilius Yance Pramono

12.11.6007

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015

ANALISIS SERANGAN MALWARE MENGGUNAKAN WIRESHARK PADA SIMULASI JARINGAN DI MININET

SKRIPSI

Untuk memenuhi sebagian persyaratan
Mencapai derajat Sarjana S1
pada jurusan Teknik Informatika

disusun oleh

Basilius Yance Pramono

12.11.6007

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015

PERSETUJUAN

SKRIPSI

ANALISIS SERANGAN MALWARE MENGGUNAKAN WIRESHARK PADA SIMULASI JARINGAN DI MININET

yang dipersiapkan dan disusun oleh

Basilius Yance Pramono

12.11.6007

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 8 September 2015

Dosen Pembimbing,

Bayu Setiaji, M.Kom

NIK. 190302216

PENGESAHAN

SKRIPSI

ANALISIS SERANGAN MALWARE MENGGUNAKAN WIRESHARK PADA SIMULASI JARINGAN DI MININET

yang disusun oleh

Basilius Yance Pramono

12.11.6007

telah dipertahankan di depan Dewan Penguji
pada tanggal 17 September 2015

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Ali Mustopa, M.Kom **NIK. 190302192**	
Bayu Setiaji, M.Kom **NIK. 190302216**	
Melwin Syafrizal, S.Kom, M.Eng **NIK. 190302105**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 29 September 2015

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 29 September 2015

Basilius Yance Pramono

NIM. 12.11.6007

MOTTO

- Lihatlah ke atas untuk memacu diri dan lihatlah ke bawah untuk bersyukur.
- Belajarlah mengalah hingga tak ada seorang pun mampu mengalahkanmu dan belajarlah merendah hingga tak seorang pun mampu merendahkanmu (Gobin Vashdev).
- Lakukanlah "SEKARANG" terkadang "NANTI" akan menjadi "TIDAK PERNAH".
- Saat-saat "LUAR BIASA SULIT" dalam perjuangan adalah "PERTANDA" bahwa "KESUKSESAN SUDAH MENDEKAT"
- Jangan menunggu karena tidak akan pernah ada waktu yang benar-benar tepat.

PERSEMBAHAN

Puji syukur kepada Tuhan yang maha kuasa, yang telah melimpahkan rahmat serta karuniaNya sehingga tugas akhir ini dapat terselesaikan dengan baik dan lancar.

Dengan segenap hati dan jiwa tugas akhir ini saya persembahkan kepada :

- Kedua orang tua, Bapak Marianus Sempana dan Ibu tercinta Maria Magdalena Yanti, yang telah memberikan segalanya, yang tak henti – hentinya memberikan doa dan dukungan serta semangat untuk saya.
- Adik tercinta Melania Fitri telah memberikan doa dan dukungan.
- Bapak dan Ibu Dosen STMIK AMIKOM Yogyakarta yang telah banyak memberikan ilmu selama penulis kuliah.
- Sahabat – sahabat saya, Ari, Anas, Azis, Danang, Fani, Bondan, Dono, Riki, Bima, Ikwan yang selalu mendukung dan menyemangati saya.
- Teman – teman kelas 12S1TI-04 yang selalu membantu, terimakasih banyak bimbingannya.
- Semua pihak yang telah membantu dalam penyusunan skripsi ini yang tidak dapat disebutkan satu persatu.

KATA PENGANTAR

Puji dan syukur penulis panjatkan untuk Tuhan yang Maha Esa yang telah memberikan rahmat, karunia dan kekuatan sehingga penulis dapat menyelesaikan skripsi yang berjudul **"Analisis Serangan Malware Menggunakan Wireshark Pada Simulasi Jaringan di Mininet"** dapat terselesaikan dengan baik dan tepat waktu.

Skripsi ini disusun sebagai salah satu syarat kelulusan bagi setiap mahasiswa STMIK AMIKOM Yogyakarta. Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program Strata-1 dan untuk memproleh gelar Sarjana Komputer.

Pembuatan skripsi ini pun tidak lepas dari berbagai pihak yang telah banyak membantu. Untuk itu pada kesempatan ini penulis ingin mengucapkan terima kasih kepada :

1. Tuhan yang maha kuasa atas rahmat-Nya.
2. Orang Tua tercinta Bapak Marianus Sempana dan Ibu Maria Magdalena Yanti serta adik saya Melania Fitri yang banyak memberikan bantuan moril, material, arahan dan selalu mendoakan keberhasilan dan keselamatan selama menempuh pendidikan.
3. Bapak Prof. Dr. M. Suyanto, M.M selaku ketua Sekolah Tinggi Manajemen Informatika dan Komputer STMIK AMIKOM Yogyakarta.
4. Bapak Sudarmawan, MT selaku ketua jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
5. Bayu Setiaji, M.Kom selaku dosen pembimbing yang telah banyak membantu dan membimbing dalam proses pengerjaan skripsi ini.
6. Bapak dan Ibu Dosen STMIK AMIKOM Yogyakarta yang telah banyak memberikan ilmu selama penulis kuliah.
7. Teman-teman 12 S1-TI-04

8. Semua pihak yang tidak dapat penulis sebut satu persatu yang telah membantu dalam penyelesaian penulisan skripsi ini.

Dalam pelaksanaan dan pembuatan program serta skripsi ini saya menyadari bahwa masih banyak kekurangan-kekurangan baik yang disadari maupun tidak disadari, oleh karena itu saya sangat mengharapkan kritik dan saran yang membangun serta masukan dari para pembaca.

Semoga skripsi ini memberikan manfaat bagi pembaca maupun bagi kepustakaan ilmu baik pada Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta maupun bagi dunia pengetahuan Teknologi Informasi di Indonesia.

DAFTAR ISI

LAMPIRAN

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Komputer yang terhubung ke internet akan memperbesar kemungkinan terjadinya ancaman atau gangguan terhadap keamanan sistem jaringan. *Malware* dalam bentuk *virus, worm, dan trojan horses* merupakan ancaman bagi keamanan dalam jaringan komputer. *Malware* telah dirancang secanggih mungkin untuk membuat celah didalam sistem. Setiap orang mengalami kemungkinan besar untuk terserang *malware* dalam sistem komputer yang dimiliki karena *malware* dapat menyerang melalui media disk maupun internet, sms, chat.

Banyak yang beranggapan serangan *malware* dapat ditangani dengan antivirus. *Malware* mempunyai sistem pertahanan sendiri dan sangat dimungkinkan untuk menyembunyikan diri dari antivirus pada komputer atau bahkan bahayanya bisa menginfeksi antivirus itu sendiri. Dengan alasan tersebut dibutuhkan sebuah solusi dari serangan *malware*. Analisis serangan *malware* menekankan pada proses monitoring. Monitoring untuk melihat terjadi serangan malware pada sistem komputer dapat dilihat dengan wireshark pada simulator dimininet.

Dalam penelitian ini dilakukan pada jaringan dengan menggunakan wireshark pada simulator mininet bertujuan untuk mengetahui serangan *malware* pada sistem komputer untuk memberikan proteksi. Pada tahap ini pemasangan firewall dan antivirus akan meminimalisir serangan malware dengan membatasi port yang diakses. *Malware* dapat ditangani dengan mengetahui cara kerja kemudian dianalisa untuk mengetahui informasi yang dibawa oleh *malware* ketika melakukan serangan kedalam sistem komputer.

Kata kunci : Malware, Mininet, Wireshark, Firewall, Jaringan

ABSTRACT

A computer connected to the internet will enlarge the possibility of threat or disruption of network system security. Malware in the form of viruses, worms, and trojan horses is a threat to the security in computer networks. Malware has been designed as powerful as possible to create a loophole in the system. Each person's experience is likely to be stricken with malware in computer systems owned because malware can invade through the disk media or the internet, sms, chat.

Many who assume malware attacks can be dealt with antivirus. Malware has its own defense system and it is very possible to hide itself from antivirus on a computer or even the danger could infect the antivirus itself. With the excuse it needs a solution from malware attacks. Analysis of malware attacks highlight the monitoring process. Monitoring to see the occurred malware attacks on computer systems can be seen with wireshark on a simulator dimininet.

In the study conducted on the network using wireshark on a simulator mininet aims to know the attacks of malware on your computer system to provide protection. At this stage of the installation of firewall and antivirus will minimize malware attacks by limiting the ports are accessible. Malware can be handled by knowing how to work and then analyzed to find out the information carried by the malware when an attack into the computer system.

Keywords: Malware, Mininet, Wireshark, Firewall, Jaringan