ANALISIS FORENSIK PADA APLIKASI *NETWORK INTRUSION DETECTION SYSTEM* (NIDS) UNTUK MENDETEKSI SERANGAN PAKET *SNIFFING*

SKRIPSI

disusun oleh

Stefanus Triono ms

16.11.0595

PROGRAM SARJANA

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER UNIVERSITAS

AMIKOM YOGYAKARTA

YOGYAKARTA

2016

ANALISIS FORENSIK PADA APLIKASI *NETWORK INTRUSION DETECTION SYSTEM* (NIDS) UNTUK MENDETEKSI SERANGAN PAKET *SNIFFING*

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Sistem Informasi

disusun oleh

Stefanus Triono ms

16.11.0595

PROGRAM SARJANA

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2020

PERSETUJUAN

SKRIPSI

ANALISIS FORENSIK PADA APLIKASI *NETWORK INTRUSION DETECTION SYSTEM* (NIDS) UNTUK MENDETEKSI SERANGAN PAKET *SNIFFING*

yang dipersiapkan dan disusun oleh

Stefanus Triono ms

16.11.0595

telah disetujuai oleh Dosen Pembimbing Skripsi

pada tanggal 09 November 2020

Dosen Pembimbing,

Nila Feby Puspitasari, S.Kom, M.Cs

NIK. 190302161

PENGESAHAN

SKRIPSI

ANALISIS FORENSIK PADA APLIKASI *NETWORK INTRUSION DETECTION SYSTEM* (NIDS) UNTUK MENDETEKSI SERANGAN PAKET *SNIFFING*

yang dipersiapkan dan disusun oleh

Stefanus Triono ms

16.11.0595

telah dipertahankan di depan Dewan Penguji
pada tanggal 17 November 2020

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Andika Agus Slameto, M.Kom **NIK. 190302109**	_____
Agung Nugroho, M.Kom **NIK. 190302242**	_____
Nila Feby Puspitasari, S.Kom, M.Cs **NIK. 190302161**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 19 Desember 2020

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, 19 Desember 2020

Stefanus Triono ms

NIM. 16.11.0595

MOTTO

" LEARN FROM YESTERDAY, LIVE FOR TODAY, HOPE FOR TOMORROW. THE IMPORTANT THING IS NOT TO STOP QUESTIONING "

(ALBERT EINSTEIN)

" THERE IS NO EASY WALK TO FREEDOM ANYWHERE, AND MANY OF US WILL HAVE TO PASS THROUGH THE VALLEY OF THE SHADOW OF DEATH. AGAIN AND AGAIN BEFORE WE REACH THE MOUNTAIN TOP OF OUR DESIRES "

(NELSON MANDELA)

" MANY OF LIFE'S FAILURES ARE PEOPLE WHO DID NOT REALIZE HOW CLOSE THEY WERE TO SUCCESS WHEN THEY GAVE UP "

(THOMAS A. EDISON)

PERSEMBAHAN

Penulisan skripsi ini penulis persembahkan kepada :

1. Tuhan Yang Maha Esa yang telah memberikan segala kemampuan, kekuatan, keelancaran dan kemudahan menyelesaikan skripsi.
2. Kedua orang tua saya serta kakak dan adik saya yang selalu memberikan doa, semangat dan motivasi.
3. Dosen pembimbing Ibu Nila Feby Puspitasari, S.Kom, M.Cs yang telah membimbing saya, telah memberikan masukan dan motivasinya.
4. Bunda Kristin yang telah memberikan semangat menyelesaikan skripsi dan doa disaat pendadaran.
5. Teman saya Desi dan Fajar yang telah membantu disaat sudah pusing, memberikan masukan dan motivasinya.
6. Teman saya panglima Enge yang sudah menemani, memberi semangat, membantu saat pusing dan berdongeng saat pengerjaan skripsi.
7. Teman saya Ray, Mia dan Rifky yang memberikan semangat dan motivasi sekaligus teman jalan – jalan supaya tidak pusing.
8. Teman saya Tiara yang memberikan motivasi dan semangat untuk cepat menyelesaikan skripsi dengan omelannya.
9. Temn saya Arin yang selalu ada dan mendengarkan keluh kesah dan memberikan masukan dan motivasinya.

Penulis

Stefanus Triono ms

KATA PENGANTAR

Puji syukur penulis persembahkan kepada Tuhan Yang Maha Esa yang telah memberikan segala kekuatan, berkat dan rahmat-Nya sengingga penulis dapat menyelesaikan skripsi ini sesuai dengan waktu yang diinginkan oleh penulis. Skripsi ini disusun sebagai salah satu syarat kelulusan bagi setiap mahasiswa Universitas Amikom Yogyakarta. Selain juga sebagai bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program Strata-I dan memperoleh gelar Sarjana Komputer.

1. Universitas Amikom Yogyakarta selaku pihak yang telah mengizinkan melakukan penelitian.
2. Bapak Prof. Dr. M. Suyanto, MM selaku ketua Universitas Amikom Yogyakarta.
3. Bapak Sudarmawan, S.T., M.T selaku ketua program studi Informatika Universitas Amikom Yogyakata.
4. Ibu Nila Feby Puspitasari, S.Kom, M.Cs selaku dosen pembimbing yang telah bersedia memberi pengarahan dan bimbingan dalam penyusunan skripsi ini.
5. Kedua orang tua dan keluarga yang selalu memberi semangat, doa dan motivasi.
6. Teman-teman yang telah mendukung dan membantu memberikan masukan untuk skripsi ini

Yogyakarta, 19 Desember 2020

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Sebelumya salah satu jenis serangan yang bisa terjadi adalah *sniffing*, dengan melakukan *sniffing*, *intruder* dapat membaca paket data yang lewat pada jaringan sehingga dapat mengakibatkan terjadinya kebocoran informasi penting seperti data pribadi, *username*, *password* dan lain-lain.

Penelitian kali ini peneliti akan melakukan penelitian tentang analisis forensik terhadap serangan *sniffing* berbasis *arp spoofing* untuk mendeteksi serangan peneliti menggunakan aplikasi IDS snort, sedangkan untuk melakukan serangan menggunakan aplikasi Ettercap.

Setelah terjadinya serangan peneliti mengumpulkan bukti-bukti dari *log* snort yang kemudian dilakukan proses analisis untuk menemukan pelaku dan asal serangan tersebut, dan dari proses analisis forensik.

Kata Kunci: **Forensik, *Sniffing***

ABSTRACT

Previously, one type of attack that could occur was sniffing, by sniffing, intruders could read data packets passing on the network so that it could lead to leakage of important information such as personal data, usernames, passwords and others.

This research, researchers will conduct research on forensic analysis of sniffing attacks based on arp spoofing to detect attacks by researchers using the IDS snort application, while to carry out attacks using the Ettercap application.

After the attack, the researcher collected evidence from the snort log which was then carried out by an analysis process to find the perpetrator and origin of the attack, and from the forensic analysis process.

Keyword: **Forensik**, ***Sniffing***