ANALISIS SERANGAN MAN IN THE MIDDLE ATTACK (ARP SPOOFING) MENGGUNAKAN METODE LIVE FORENSIC

SKRIPSI

disusun oleh

NURLAELA

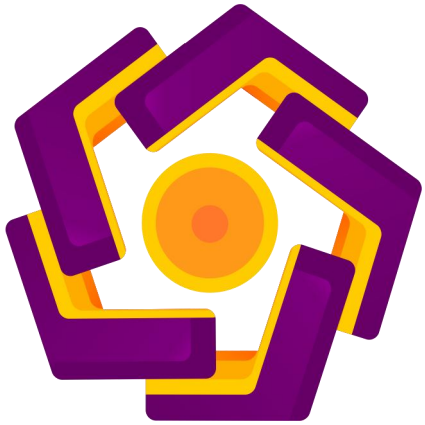
17.83.0027

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023

ANALISIS SERANGAN MAN IN THE MIDDLE ATTACK (ARP SPOOFING) MENGGUNAKAN METODE LIVE FORENSIC

SKRIPSI

untuk memenuhi sebagian persyaratan mencapai gelar Sarjana
pada Program Studi Teknik Komputer



disusun oleh

NURLAELA

17.83.0027

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS SERANGAN MAN IN THE MIDDLE ATTACK (ARP SPOOFING) MENGGUNAKAN METODE LIVE FORENSIC

yang dipersiapkan dan disusun oleh

NURLAELA

17.83.0027

telah disetujuai oleh Dosen Pembimbing Skripsi

pada tanggal 27 Februari 2023

Dosen Pembimbing,

Dony Ariyus, M.Kom
NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS SERANGAN MAN IN THE MIDDLE ATTACK (ARP SPOOFING) MENGGUNAKAN METODE LIVE FORENSIC

yang dipersiapkan dan disusun oleh

NURLAELA

17.83.0027

telah dipertahankan di depan Dewan Penguji
pada tanggal 27 Februari 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Banu Santoso, S.T., M.Eng **NIK. 190302327**	_____
Rina Pramitasari, S.Si., M.Cs **NIK. 190302335**	_____
Dony Ariyus, S.S., M.Kom **NIK. 190302128**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 27 Februari 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al fatah, S.Kom., M.Kom
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama Mahasiswa : NURLAELA
NIM : 17.83.0027

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS SERANGAN MAN IN THE MIDDLE ATTACK (ARP SPOOFING) MENGGUNAKAN METODE LIVE FORENSIC

Dosen Pembimbing : Dony Ariyus, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 27 Februari 2023

Yang Menyatakan,

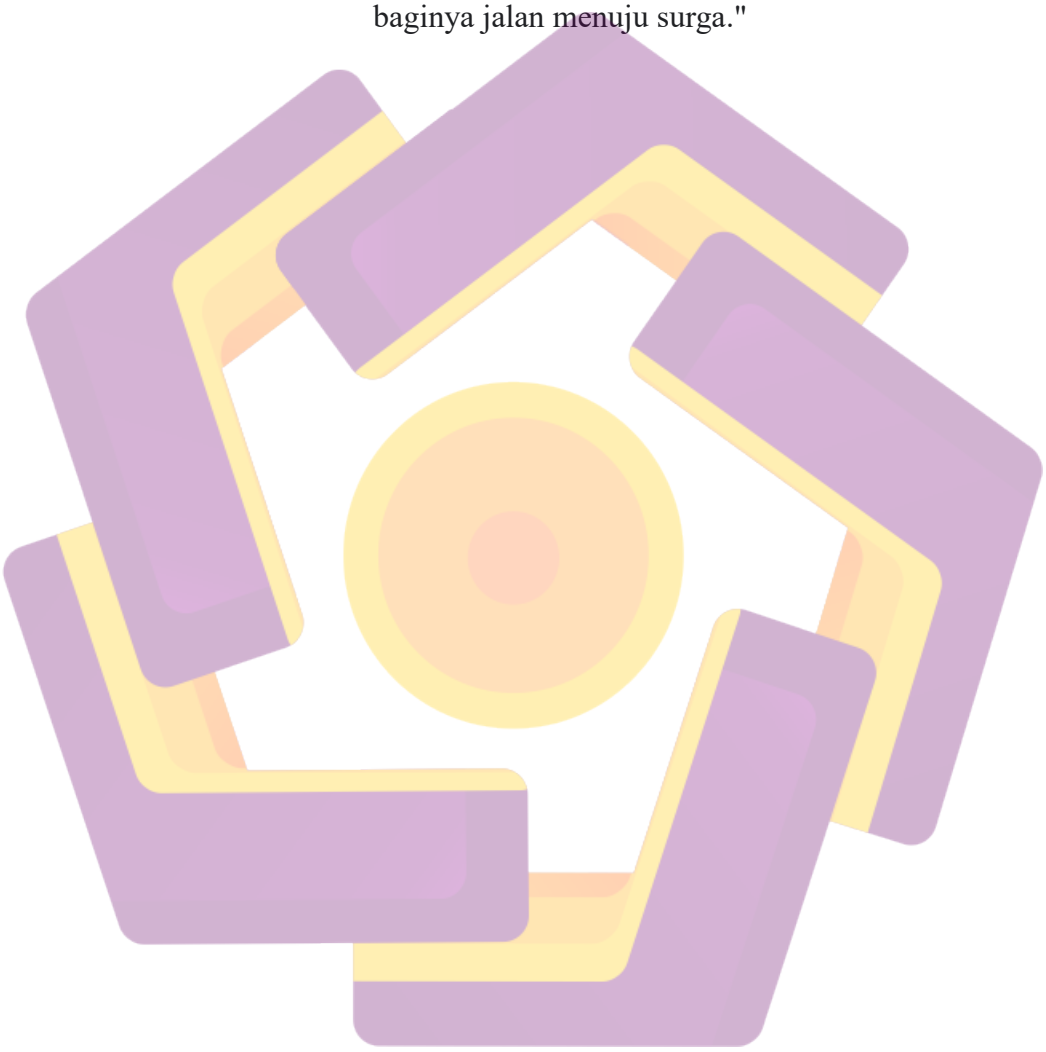
NURLAELA

iv

MOTTO

“Allah akan meninggikan derajat bagi hambanya yang menuntut ilmu dibandingkan dengan yang tidak menuntut ilmu”

"Siapa yang menempuh jalan untuk mencari ilmu, maka Allah akan mudahkan baginya jalan menuju surga."



HALAMAN PERSEMBAHAN

Puji dan syuqur tercurahkan kepada Allah SWT yang telah memberikan kesempatan dan ridho-nya yang selalu menemani setiap langkah dan kondisi hambanya. Alhamdulillah atas kehadiran baginda Muhammad SAW sebagai pelita,penerang dan dalam ilmu pengetahuan.

Skripsi ini penulis persembahkan kepada :

1. Kedua orang tua, bapak Abubakar BA dan ibunda Fatimah yang tidak pernah lelah berdo'a untuk kebaikan putra dan putrinya,memberi semangat sertadukungan dalam keadaan apapun serta tentang semua hal yang tidak bisa di ungkapkan dengan kata-kata..
2. Bapak Dony Ariyus, M.kom. Selaku dosen pembimbing yang selalu sedia meluangkan waktu dan tenaga untuk memberikan arahan dan petunjuk.
3. Kepada Abang dan Kakak saya Sahrul, Sulastri dan Jumrah yang selalumemberikan dukungan finansial di saat merasa butuh.
4. Kepada sahabat saya Lisa, Tansen, Andrian,Hafiz, Hardi, Tirta, Randika, Arif, Nurya. yang selalu memberikan semangat dan dorongan motivasi saat berada pada titik jenuh dalam menyelesaikan skripsi ini.
5. Kepada Muhammad Isra S.pd Selaku calon imam yang membangkitkan semangat penuh cinta yang tidak pernah lelah mengingatkan untuk selalu mengangkat tangan meminta dan memohon kepada sang pemilik.

KATA PENGANTAR

Puji dan syuqur saya panjatkan kepada Allah SWT atas ridho dan katunia-nya sehingga saya dapat menyelesaikan penyusunan skripsi ini. Adapun judul yang saya ajukan adalah "Analisis Serangan Man In The Middle Attack (ARP Spoofing) Menggunakan Metode Live Forensic".

Skripsi ini di ajukan untuk memenuhi syarat kelulusan mata kuliah skripsi di Fakultas Ilmu Komputer di Universitas Amikom Yogyakarta. Tidak dapat di sangkal bahwa butuh usaha yang keras dalam penyelesaikan pekerjaan skripsi ini. Namun, karya ini tidak akan selesai tanpa orang-orang tercinta di sekililing saya yang mendukung dan membantu.

Penulis mengucapkan terima kasih kepada :

1. Allah SWT atas limpahan rahmat-nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Oleh karena itu semoga penulis dapat memberikan manfaat bagi orang-orang di kemudian hari.
2. Bapak Prof Dr. M. Suyanto, M.M. selaku Rektor Universitas Amikom Yogyakarta.
3. Bapak Dony Ariyus, M.Kom. Selaku dosen pembimbing yang telah memberikan bimbingan dan berbagai pengalaman kepada penulis.
4. Segenap Dosen Fakultas Ilmu Komputer yang telah mendidik dan memberikan ilmu selama kuliah dan seluruh staf serta karyawan di Universitas Amikom Yogyakarta yang selalu sabar melayani segala administrasi selama proses perkuliahan.
5. Bapak tercinta Abubakar BA dan ibunda tersayang yaitu Fatimah, Selaku kedua oang tua beserta keluarga yang selalu berdoa'a dan memberikan dukungan. Semoga selalu bersama hingga ke Surga-nya kelak.

6. Serta kerabat dan teman-teman yang memberikan semangat dan dorongan motivasi saat berada pada titik jenuh dalam menyelesaikan skripsi ini yang tidak dapat penulis sebutkan satu per satu.

Penulis menyadari masih banyak kekurangan dalam penulisan skripsi ini. Untuk itu, penulis sangat mengharapkan saran yang membangun agar tulisan ini dapat berguna untuk perkembangan ilmu pengetahuan kedepannya. Dan penulis berharap semoga skripsi ini dapat bermanfaat bagi sebagian pihak yang berkaitan dalam penulisan ini.

Yogyakarta, 27 Februari 2023

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Seiring perkembangan zaman para pengguna komputer dan internet semakin banyak, sehingga semakin maraknya tindak kejahatan di dunia maya saat ini yang melakukan sejumlah serangan dengan menggunakan berbagai metode contohnya adalah MITM yang bertujuan mendapatkan informasi pribadi dan sensitif dari para pengguna komputer dan internet. Para hacker memanfaatkan kerentanan keamanan ini untuk menjalankan serangan tersebut.

Pada jaringan komputer, protokol yang bertugas untuk untuk menerjemahkan IP address menjadi MAC Address adalah Address Resolution Protocol (ARP). Sifat stateless pada protokol ARP, menyebabkan protokol ARP memiliki celah dari segi keamanan. Celah ini dapat menimbulkan serangan terhadap ARP Protocol, disebabkan karena ARP request yang dikirimkan secara broadcast, sehingga semua host yang berada pada satu broadcast domain dapat merespon pesan ARP tersebut walaupun pesan tersebut bukan ditujukan untuknya. Serangan inilah yang biasa disebut dengan ARP Spoofing. Serangan ini dapat berimbas pada serangan serangan yang lain, seperti serangan Man In The Middle Attack, Packet Sniffing, dan Distributed Denial of Service.

Metode Live & Network Forensic digunakan untuk mengidentifikasi dan mendeteksi serangan ketika sistem dalam keadaan menyala. Berdasarkan hasil penelitian yang dilakukan terbukti bahwa dengan penggunaan metode Live Forensics, investigator dapat dengan cepat mendeteksi suatu serangan dan mengidentifikasi penyerangnya.

Kata Kunci: Incident Response, Digital Forensic, Man In The Middle Attack, Cybersecurity

ABSTRACT

Along with the development of the times, there are more and more computer and internet users, so that there are increasingly widespread crimes in cyberspace today which carry out a number of attacks using various methods, for example MITM which aims to obtain personal and sensitive information from computer and internet users. The hackers took advantage of this security vulnerability to carry out the attack.

On computer networks, the protocol responsible for translating IP addresses into MAC addresses is the Address Resolution Protocol (ARP). The stateless nature of the ARP protocol causes the ARP protocol to have a security gap. This vulnerability can cause attacks against the ARP Protocol, because ARP requests are sent by broadcast, so that all hosts in one broadcast domain can respond to the ARP message even though the message is not intended for them. This attack is commonly known as ARP Spoofing. This attack can have an impact on other attacks, such as Man In The Middle Attack, Packet Sniffing, and Distributed Denial of Service attacks.

The Live & Network Forensic method is used to identify and detect attacks when the system is on. Based on the results of the research conducted, it is proven that by using the Live Forensics method, investigators can quickly detect an attack and identify the attacker.

Keywords: Incident Response, Digital Forensic, Man In The Middle Attack, Cybersecurity