STATICS FORENSICS TERHADAP SERANGAN MAN IN THE MIDDLE BERBASIS ARP POISONING

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

ICHSAN TAJI PUTRA

19.83.0365

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

STATICS FORENSICS TERHADAP SERANGAN MAN IN THE MIDDLE BERBASIS ARP POISONING

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer

disusun oleh

ICHSAN TAJI PUTRA

19.83.0365

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

HALAMAN PERSETUJUAN

SKRIPSI

STATICS FORENSICS TERHADAP SERANGAN MAN IN THE MIDDLE BERBASIS ARP POISONING

yang disusun dan diajukan oleh

ICHSAN TAJI PUTRA

19.83.0365

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal **26 Juli 2023**

Dosen Pembimbing,

Subektiningsih, M.Kom
NIK. 190302413

HALAMAN PENGESAHAN

SKRIPSI

STATICS FORENSICS TERHADAP SERANGAN MAN IN THE MIDDLE BERBASIS ARP POISONING

yang disusun dan diajukan oleh

ICHSAN TAJI PUTRA

19.83.0365

Telah dipertahankan di depan Dewan Penguji
pada tanggal 26 Juli 2023

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Banu Santoso, S.T., M.Eng **NIK. 190302327**	
Jeki Kuswanto, M.Kom **NIK. 190302456**	
Subektiningsih, M.Kom **NIK. 190302413**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 26 Juli 2023

DEKAN FAKULTAS ILMU KOMPUTER

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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : ICHSAN TAJI PUTRA
NIM : 19.83.0365

Menyatakan bahwa Skripsi dengan judul berikut:

STATIC FORENSICS TERHADAP SERANGAN MAN IN THE MIDDLE BERBASIS ARP POISONING

Dosen Pembimbing : Subektiningsih, 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, 26 Juli 2023

Yang Menyatakan,

Ichsan Taji Putra

HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT atas limpahan rahmat, hidayah, karunia-Nya sehingga saya dapat menyelesaikan skripsi saya dengan lancar dan sebaik-baiknya. Skripsi ini saya persembahkan untuk:

1. Terimakasih kepada Ibu dan Bapak saya serta adik saya satu-satunya, yang selalu mendoakan, memberi semangat, dan memberikan fasilitas yang saya butuhkan,
2. Berterimakasih kepada saya sendiri, karena sudah mau berjuang dan tidak menyerah untuk mencapai hasil yang diharapkan.
3. Terimakasih kepada Ibu Subektiningsih, M.Kom selaku dosen pembimbing saya yang baik dan sabar dalam membimbing saya serta memberikan saya arahan dalam menyelesaikan penyusunan skripsi ini.
4. Terimakasih kepada seluruh Dosen Teknik Komputer atas ilmu yang diberikan, motivasi, dan cerita serta kenangan yang akan saya ingat terus hingga masa mendatang.
5. Kepada teman sudah saya anggap sebagai saudara sejak smp khususnya bayu, halwa, rasyid, awang, dimas.
6. Terimakasih juga buat sahabat saya disaat kuliah ini nevy, saiful, prayitno, jefri, diyah, oka, nana, ingka, azkia yang telah mendorong semangat saya agar lancar dalam mengerjakan skripsi ini.

KATA PENGANTAR

Alhamdulillah puji syukur penulis panjatkan kepada Allah SWT yang telah memberikan banyak sekali rahmat dalam kehidupan penulis sehingga dapat menyelesaikan skripsi dengan judul " *Static Forensics Terhadap Serangan Man In The Middle Berbasis ARP Poisoning*".

Skripsi ini disusun sebagai syarat memperoleh gelar Sarjana Komputer pada Program Studi S1 Teknik Komputer Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.

Pada kesempatan ini, penulis ingin menyampaikan rasa terimakasih kepada pihak-pihak yang telah memberi dukungan, arahan, bimbingan, dan semangat sehingga penulis dapat menyelesaikan skripsi ini dan berjalan lancar, untuk itu penulis mengucapkan terimakasih kepada:

1. Allah SWT atas Karunia-Nya, sehingga penulis dapat menyelesaikan skripsi dengan lancar dan semoga bermanfaat di kemudian hari.
2. Bapak Prof. DR. M. Suyanto, M.M selaku Rektor Universitas Amikom Yogyakarta.
3. Bapak Hanif Al Fatta,S.Kom., M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. Bapak Dony Ariyus, S.S., M.Kom. selaku Ketua Program Studi S1 Teknik Komputer Universitas Amikom Yogyakarta.
5. Ibu Subektiningsih, M.Kom selaku Dosen Pembimbing yang telah bersedia meluangkan waktunya untuk membimbing dan mengarahkan dalam penyusunan skripsi ini.
6. Ibu, Bapak, dan Adik yang tidak pernah berhenti mendoakan, memberi semangat serta dukungan.
7. Serta kerabat dan sahabat maupun teman yang tidak bisa penulis sebutkan satu per satu.

Dalam penyusunan skripsi ini penulis menyadari masih jauh dari kata sempurna karena terbatasnya pengalaman dan pengetahuan penulis, penulis mengharapkan skripsi kedepannya dapat memberikan manfaat pada pihak

yang membutuhkan serta dapat menjadi acuan dalam melakukan penelitian kedepannya. Penulis juga mengharapkan kritik, saran, serta masukan yang dapat membantu menyempurnakan skripsi ini.

Yogyakarta, 10 Juli 2023

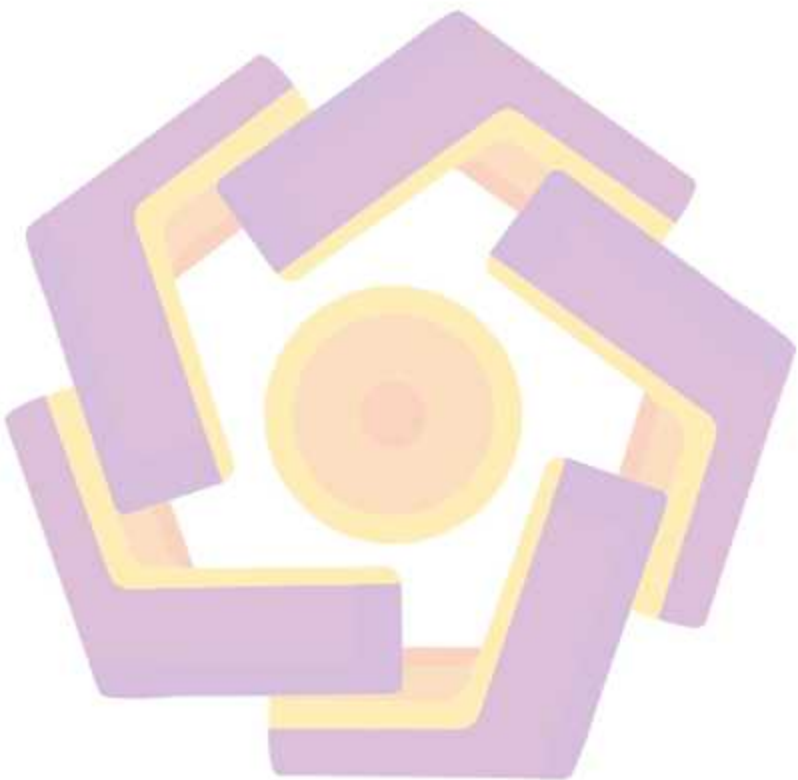
Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN



DAFTAR LAMBANG DAN SINGKATAN

NIST	National Institute of Standards and Technology
AP	Access Point
MD5	Message-Digest algorithm 5
SHA1	Secure Hash Algorithm 1
ARP	Address Resolution Protocol
WLAN	Wireless Local Area Network
MITM	Man In The Middle
IP	Internet Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

DAFTAR ISTILAH

Port Forwarding	kamuflase alamat ip target
Static Forensic	forensik saat keadaan sistem mati
Capture	perekaman atau penangkapan

INTISARI

Data pengguna internet tiap tahun mengalami peningkatan, segala bentuk aktivitas baik di organisasi maupun individu kini tidak terlepas dari penggunaan sebuah jaringan. Kemudahan akses informasi menggunakan jaringan menjadi hal positif bagi setiap orang namun disisi lain terdapat hal negatif yaitu aktivitas dari pihak yang tidak bertanggungjawab diantaranya melalui serangan *ARP Poisoning*.

Teknik ini merupakan turunan dari serangan *Man In The Middle* yaitu penyadapan komunikasi dua arah, pada dasarnya *attacker* berada ditengah-tengah komunikasi diantara dua perangkat. Teknik *ARP Poisoning* memanfaatkan celah komunikasi secara *broadcast* pada protokol ARP. Komunikasi jaringan pada *local area network* dimulai ketika host mengirimkan sebuah paket ARP secara *broadcast* dengan membawa sebuah alamat IP tujuan, host yang memiliki alamat IP akan membalas dengan mengirimkan ARP secara *unicast*. Proses tersebut juga yang digunakan oleh penyerang untuk melakukan serangan *spoofing/poisoning* dengan mengirimkan informasi palsu ke pada host yang sah dalam jaringan. Saat serangan dilakukan maka host akan memperbarui ARP *table cache* yang dimiliki tanpa disadari, hal ini terjadi juga karena pada protokol ARP bersifat *stateless* atau tidak ada sebuah mekanisme pemeriksaan. Sehingga saat ada ARP *reply* yang datang ke host maka tidak akan dilakukan pemeriksaan terkait dengan kebenaran alamat IP dan MAC, dan akan disimpan pada ARP *table cache*.

Tujuan penelitian ini adalah menemukan informasi penting dari hasil analisis dan menyusunnya menjadi bentuk laporan investigasi. Metode forensik yang digunakan adalah *Static* dan *Network Forensic* dengan menerapkan framework NIST SP 800-86. Hasil dari penelitian ini didapatkan informasi dari bukti digital berupa *IP Address, Mac Address attacker*, dan kapan waktu serangan tersebut terjadi. Selanjutnya tindakan pemblokiran *IP* dan *Mac Address attacker* dilakukan untuk mencegah pencurian identitas lagi dalam jaringan.

Kata kunci: Man In The Middle, ARP Poisoning, NIST, Digital Forensic.

ABSTRACT

Internet user data has been increasing every year, and all forms of activities, both in organizations and individuals, are now inseparable from the use of a network. The ease of accessing information using a network is a positive aspect for everyone, but on the other hand, there are negative aspects, such as activities from irresponsible parties, including ARP Poisoning attacks.

This technique is a derivative of the Man In The Middle attack, which involves eavesdropping on two-way communication. Essentially, the attacker positions themselves in the middle of the communication between two devices. ARP Poisoning technique exploits the broadcast communication vulnerability in the ARP protocol. Network communication in a local area network starts when a host sends an ARP packet as a broadcast carrying a target IP address, and the host with that IP address replies by sending an ARP unicast. Attackers use this process to conduct spoofing/poisoning attacks by sending false information to legitimate hosts in the network. When an attack is carried out, the host updates its ARP table cache without realizing it. This also occurs because the ARP protocol is stateless, meaning there is no verification mechanism. Therefore, when an ARP reply arrives at the host, no verification of the correctness of the IP and MAC addresses is performed, and it is stored in the ARP table cache.

The purpose of this research is to discover important information through analysis and compile it into an investigation report. The forensic methods used are Static and Network Forensics, applying the NIST SP 800-86 framework. The research results reveal crucial information from digital evidence, such as the IP address, MAC address of the attacker, and the time the attack occurred. Subsequently, the action of blocking the attacker's IP and MAC addresses is taken to prevent identity theft within the network.

Keywords: *Man In The Middle, ARP Poisoning, NIST, Digital Forensics.*