IMPLEMENTASI FRAMEWORK MITM UNTUK MEMANTAU AKTIFITAS PENGGUNA DALAM SATU JARINGAN MENGGUNAKAN KALI LINUX

SKRIPSI

disusun oleh

Mohamad Arie Ajharie

15.11.9372

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019

IMPLEMENTASI FRAMEWORK MITM UNTUK MEMANTAU AKTIFITAS PENGGUNA DALAM SATU JARINGAN MENGGUNAKAN KALI LINUX

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana S1
pada Program Studi Informatika

disusun oleh

Mohamad Arie Ajharie

15.11.9372

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2019

PERSETUJUAN

SKRIPSI

IMPLEMENTASI FRAMEWORK MITM UNTUK MEMANTAU AKTIFITAS PENGGUNA DALAM SATU JARINGAN MENGGUNAKAN KALI LINUX

yang dipersiapkan dan disusun oleh

Mohamad Arie Ajharie

15.11.9372

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 05 Agustus 2019

Dosen Pembimbing,

Mulia Sulistiyono, M.Kom
NIK. 190302248

PENGESAHAN

SKRIPSI

IMPLEMENTASI FRAMEWORK MITM UNTUK MEMANTAU AKTIFITAS PENGGUNA DALAM SATU JARINGAN MENGGUNAKAN KALI LINUX

yang dipersiapkan dan disusun oleh
Mohamad Arie Ajharie

15.11.9372

telah dipertahankan di depan Dewan Penguji
pada 23 Agustus 2019

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Joko Dwi Santoso, M.Kom **NIK. 190302181**	
Mulia Sulistiyono, M.Kom **NIK. 190302248**	
Ichsan Wiratama, ST, M.Cs **NIK. 190302119**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 23 Agustus 2019

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.

NIK. 190302038

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, 23 Agustus 2019

Mohamad Arie Ajharie
NIM. 15.11.9372

MOTTO

إذالفتى حسب اعتقاده رفع # وكل من لم يعتقد لم ينتفع

"Ketika seorang pemuda kuat keyakinannya maka akan diangkat derajatnya dan setiap insan yang tidak memiliki keyakinan maka tidak akan bisa memberikan manfaat"

(Imam Syarafuddin Yahya Al-'Imrithi)

PERSEMBAHAN

Skripsi ini bukanlah sesuatu yang terbaik, namun penulis mempersembahkan skripsi ini kepada:

1. Kedua orang tua beserta segenap keluarga yang telah memberikan dukungan materi dan do'a untuk kelancaran dalam menempuh kuliah serta dalam penyelesaian skripsi ini.
2. Bapak Mulia Sulistiyono, M. Kom., selaku dosen pembimbing, yang telah memberikan pengarahan serta saran dalam menyelesaikan tugas akhir skirpsi ini.
3. Teman-teman dari kelas 15-S1IF-13, yang telah menjadi teman sekaligus keluarga selama perkuliahan di UNIVERSITAS AMIKOM YOGYAKARTA

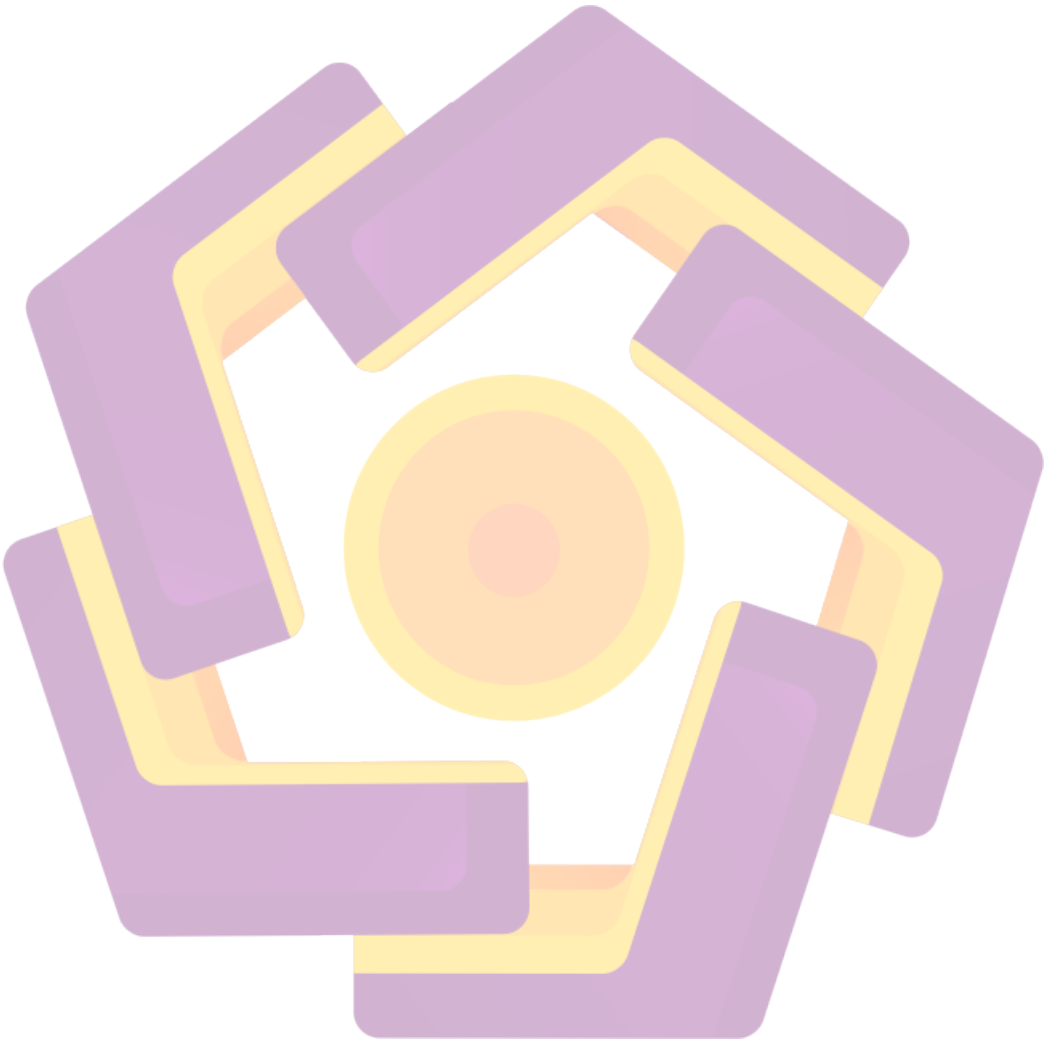
KATA PENGANTAR

Puji syukur kita panjatkan kepada Allah SWT karena Rahmat dan Karunia-Nya sehingga penulis dapat menyelesaikan laporan skripsi ini dengan judul "Implementasi Framework MITM Untuk Memantau Aktifitas Pengguna Dalam Satu Jaringan Menggunakan Kali Linux". Keberhasilan dalam menyelesaikan pembuatan laporan skripsi ini adalah berkat bantuan dan dukungan dari berbagai pihak. Maka dari itu pada kesempatan kali ini penulis mengucapkan terimakasih sebesar-besarnya kepada:

1. Prof. Dr. M. Suyanto, M. M selaku Rektor Universitas Amikom Yogykarta.
2. Ibu Krisnawati, S. Si, M. T., selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Sudarmawan, M. T., selaku Kaprodi Universitas AMIKOM Yogyakarta
4. Bapak Mulia Sulistiyono, M. Kom., selaku dosen pembimbing.
5. Bapak Tristanto Ari Aji, M. Kom., selaku dosen wali
6. Bapak / Ibu Dosen khususnya Jurusan Informatika di Universitas Amikom Yogyakarta yang telah membekali penulis dengan beberapa disiplin ilmu yang berguna.
7. Kedua orang tua penulis yang telah membesarkan, mendidik, dan selalu memberikan dukungan materi maupun moril serta do'a untuk menunjang perjalanan hidup
8. Keluarga, sahabat, teman, dan semua pihak yang telah membantu dan mendukung sehingga terselesainya skripsi ini.

Semoga segala bentuk dukungan dan bantuan dari pihak yang telah penulis sebutkan dapat menjadi amalan dan berkah dan mendapat balasan dari Tuhan Y.M.E. Penulis menyadari, laporan skripsi ini masih banyak kelemahan dan kekurangan nya. Karena itu kritik dan saran yang membangun akan diterima

dengan senang hati, mudah – mudahan keberadaan Tugas Akhir ini dapat bermanfaat dan menambah wawasan kita.



DAFTAR ISI

COVER i
JUDUL ii
PERSETUJUAN iii
PENGESAHAN iv
PERNYATAAN v
MOTTO vi
PERSEMBAHAN vii
KATA PENGANTAR viii
DAFTAR ISI x
DAFTAR TABEL xiii
DAFTAR GAMBAR xiv
INTISARI xvi
ABSTRACT xvii
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Maksud dan Tujuan Penelitian 2
1.5 Manfaat Penelitian 3
1.6 Metode Penelitian 3
1.6.1 Metode Pengumpulan Data 3
1.6.2 Metode Analisis 4
1.6.3 Metode Perancangan 4
1.6.4 Metode Testing 4
1.7 Sistematika Penulisan 4
BAB II LANDASAN TEORI 6

2.1 Tinjauan Pustaka 6
2.2 Dasar Teori 9
2.2.1 Jaringan Komputer 9
2.2.2. Topologi Jaringan 9
2.2.3. Jenis Jaringan Komputer 12
2.2.4 Internet 13
2.2.5 WLAN: *Wireless* LAN IEEE 802.11 14
2.2.6 Hypertext Transfer Protocol (HTTP) 16
2.2.7 HTTPS (*Hypertext Transfer Protocol Secure*) 16
2.2.8 Kali Linux 17
2.2.9 MITM (*Man In The Middle*) *Attack* 17
2.2.10 Framework MITMF 18
2.2.11 ARP 18
2.2.12 Sniffing 19
2.2.13 SSLStrip 19
2.2.14 Metode *Manual Penetration Testing* 20
BAB III METODE PENELITIAN 22
3.1 Metode Pengumpulan Data 22
3.1.1 Studi Pustaka 22
3.2 Metode Analisis 22
3.2.1 Alat dan Bahan 22
3.3 Metode Perancangan 25
3.4 Alur Penelitian 26
3.5 Metode Testing 27
3.5.1 *Data Collection* & *Vulnerability Assessment* 27
3.5.2 *Actual Exploit* 28
3.5.3 *Report Preparation* 28
BAB IV HASIL DAN PEMBAHASAN 29
4.1 *Data Collection & Vulnerabillity Assessment* 29

4.1.1 Pencarian Informasi IP Gateway 29
4.1.2 Pencarian Data *IP Address* yang aktif 29
4.1.3 Pencarian Informasi berdasarkan *IP Address* 32
4.2 *Actual Exploit* 35
4.2.1 Implementasi 35
4.2.2 Pengujian 38
4.3 *Report Preparation* 42
BAB V PENUTUP 44
5.1 Kesimpulan 44
5.2 Saran 44
DAFTAR PUSTAKA 46

DAFTAR TABEL

Tabel 2. 1 Matrik Literatur Review dan Posisi Penelitian 8
Tabel 4. 1 Data IP address aktif 31
Tabel 4. 2 Informasi IP address 192.68.1.1..... 32
Tabel 4. 3 Informasi IP address 192.168.1.100..... 33
Tabel 4. 4 Informasi IP address 192.168.1.101..... 34
Tabel 4. 5 Informasi IP address 192.168.1.102..... 34
Tabel 4. 6 Informasi IP address 192.168.1.103..... 35
Tabel 4. 7 Laporan hasil pengujian 43

DAFTAR GAMBAR

Gambar 2. 1 Topologi Bus 9
Gambar 2. 2 Topologi Ring 10
Gambar 2. 3 Topologi Star 10
Gambar 2. 4 Topologi Daisy-Chain 11
Gambar 2. 5 Topologi Tree 11
Gambar 2. 6 Topologi Mesh 12
Gambar 2. 7 Bagan Ilustrasi MITM Attack pada Application layer 18
Gambar 2. 8 Metode *Penetration Testing* 21
Gambar 3. 1 Topologi jaringan yang digunakan 25
Gambar 3. 2 Alur penelitian 26
Gambar 4. 1 Informasi Gateway 29
Gambar 4. 2 Pencarian IP address aktif menggunakan nmap 31
Gambar 4. 3 Informasi IP address 192.168.1.1 32
Gambar 4. 4 Informasi IP Address 192.168.1.100 33
Gambar 4. 5 Informasi *IP address* 192.168.1.101 33
Gambar 4. 6 Informasi IP address 192.168.1.102 34
Gambar 4. 7 Informasi IP address 192.168.1.103 35
Gambar 4. 8 Install paket library 36
Gambar 4. 9 Download MITMF 36
Gambar 4. 10 Download dan update submodule MITMF 36
Gambar 4. 11 Instalasi paket requirements 37
Gambar 4. 12 Mengaktifkan IP forwarding 37
Gambar 4. 13 Menjalankan MITMF 37
Gambar 4. 14 Monitoring *IP Address 192.168.1.101* 39
Gambar 4. 15 Mengakses website HTTP 39
Gambar 4. 16 Hasil monitoring *IP Address 192.168.1.101* 40
Gambar 4. 17 Monitoring IP address 192.168.1.102 41
Gambar 4. 18 Tampilan website setelah dialihkan HTTPS ke HTTP 41

Gambar 4. 19 Percobaan input data login 42
Gambar 4. 20 Hasil monitoring IP address 192.168.1.102 42

INTISARI

Kemajuan teknologi informasi yang semakin kencang harus diimbangi dengan kemampuan untuk melakukan pengamanan terhadap informasi. Berbagai masalah penyerangan jaringan yang bertujuan merugikan pengguna perlu kita pahami bagaimana konsep penyerangan tersebut.

Serangan MITM (*Man In The Middle*) membelokan traffic paket data melewati perangkat penyerang. Perangkat penyerang mengaku sebagai router ketika berkomunikasi dengan client dan mengaku client ketika berkomunikasi dengan router. *Tools* MITMF mampu menjalankan program sslstrip dimana website yang menggunakan teknologi SSL (HTTPS) akan dipaksa menjadi HTTP.

Penyerang harus berada dalam satu jaringan dan pada saat *tools* MITMF diaktifkan secara otomatis akan melakukan serangan sekaligus melakukan paket sniffing dan menampilkan secara langsung pada terminal. Website yang tidak menggunakan teknologi SSL akan menampilkan informasi tanpa enkripsi.

Kata Kunci: *Man in the middle, MITM, Sniffing, MITMF*

ABSTRACT

Information technology advances that are getting tighter must be balanced with the ability to secure information. Various problems with network attacks aimed at harming users need to be understood by us about the concept of the attack. The Man In The Middle attack bends data packet traffic over the attack device.

The attacker device claims to be a router when communicating with the client and claims the client when communicating with the router. MITMF is able to run the sslstrip program where websites that use SSL (HTTPS) technology will be forced into HTTP.

The attacker must be in one network and when MITMF is activated it will automatically attack while carrying out sniffing packages and displaying directly on the terminal. Websites that do not use SSL technology will display information without encryption.

Keywords: *Man in the middle, MITM, Sniffing, MITMF*