Lembar Pengesahan Pembimbing

INVESTIGASI LIVE FORENSIK DARI SISI PENGGUNA UNTUK MENGANALISA SERANGAN MAN IN THE MIDDLE ATTACK BERBASIS EVIL TWIN

Nama: Muhammad Sabri Ahmad

NIM: 14917154

Yogyakarta, Januari 2017

Pembimbing I	Pembimbing II
Dr.Imam Riadi, M.Kom	Yudi Prayudi,.S.Si.,M.Kom

Lembar Pengesahan Penguji

INVESTIGASI LIVE FORENSIK DARI SISI PENGGUNA UNTUK MENGANALISA SERANGAN MAN IN THE MIDDLE ATTACK BERBASIS EVIL TWIN

Nama: Muhammad Sabri Ahmad

NIM: 14917154

Yogyakarta, Januari 2017

Tim Penguji,

Dr. Imam Riadi, M.Kom
Ketua

Yudi Prayudi, S.SI., M.Kom
Anggota I

Dr Bambang Sugiantoro.,M.Kom
Anggota II

Mengetahui,
Direktur Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia

Dr. R. Teduh Dirgahayu, ST., M.Sc

Abstrak

MITM Based Evil Twin menjadi suatu ancaman yang berbahaya bagi para pengguna jaringan *Wifi*. Pelaku penyerangan ini memanfaatkan AP (*access point*) palsu dengan setingan *gateway* yang berbeda dengan *legitimate* AP, sehingga jenis serangan ini menjadi cukup sulit untuk dideteksi. Proses pengungkapan kasus serangan *MITM based Evil Twin* hanya sebatas mendeteksi aktivitas serangan dan belum ada pembahasan lebih lanjut terkait digital forensik, hal ini di sebabkan karena masih kurangnya SOP (*standart operational Procedure*) dalam menangani kasus ini. Penelitian ini dilakukan dengan tujuan untuk membuat suatu model forensik berdasarkan tahapan analisa dalam kasus *MITM based Evil Twin.*

Proses dalam investigasi *MITM based Evil Twin* dilakukan dengan menggunakan metode *live* forensik berbasis *user side*, kemudian dibagi kedalam dua fokus penelitian yaitu, proses analisa *Wifi scanning* untuk melakukan investigasi serangan *Evil Twin* dengan menganalisa atribut maupun kegitan-kegitan yang mencurigakan lainya. Analisa investigasi serangan *MITM* dilakukan dengan menganalisa *network traffic* dalam *area Evil Twin.*

Hasil investigasi forensik dalam penelitian, menghasilkan suatu model investigasi ENFGP (*Extendend* NFGP) yang dibagi menjadi 10 tahapan dan terdiri atas 30 langkah – langkah penyelesaian, yang didapatkan melalui proses pengujian dan implenmentasi metode pada kasus serangan *MITM Based Evil Twin* serta pengujian lebih lanjut berdasarkan beberapa model forensik sebelumnya.

Kata kunci: *Wifi, Evil Twin, Live, forensik, MITM.*

Abstract

Based MITM Evil Twin become a dangerous threat to the Wifi network users. The perpetrators of the attacks take advantage of the AP (access point) with a fake gateway settings that differ from legitimate AP, so that this type of attack is becoming quite difficult to detect. The disclosure of MITM attack case based Evil Twin merely detect seizure activity and there has been no further discussion related to digital forensics, this is caused because there is a lack of SOP (standard operational procedure) in handling this case. This research was conducted with the aim to create a model based on the phases of forensic analysis in the case of MITM based Evil Twin.

The process in the investigation of MITM based Evil Twin performed using user-based live forensic side, then split into two, namely research focus, process analysis Wifi scanning to investigate Evil Twin attacks by analyzing the attribute or activity suspicious-activity of others. MITM attacks investigative analysis is done by analyzing network traffic in the area of Evil Twin.

The results of forensic investigations in research, produce a model investigation ENFGP (Extendend NFGP) which is divided into 10 stages and consists of 30 steps - steps completion, which is obtained through the process of testing and implenmentasi method in case of a MITM attack Based Evil Twin and further testing by some forensic previous models.

***Keywords**: Wifi, Evil Twin, Live, forensics, MITM*

iii

Pernyataan keaslian tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak ciptayang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Untuk material yang membutuhkan izin, saya juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan material tersebut dalam tesis ini.

Yogyakarta, 14 januari 2017

Muhammad Sabri Ahmad.,S.Kom

Publikasi selama masa studi

Tidak ada publikasi yang menjadi bagian dari tesis

Kontribusi yang diberikan oleh pihak lain dalam tesis ini

Tidak ada kontribusi dari pihak lain

Halaman Persembahan

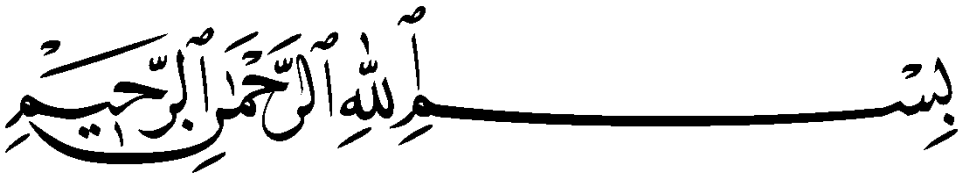
Alhamdulillah atas segala rahmat, hidayah, berkah dan kasih sayang Allah SWT yang selalu menemani disetiap langkah dan kondisi penulis..

Alhamdulillah atas kehadiran Baginda Rosulullah SAW yang menjadi pelita dalam ilmu pengetahuan..

Terima kasih kepada Bapak, Mama, dan kakak serta keluarga besar dan Teman-teman angkatan X forensik Digital yang telah mensupport penulis dalam setiap proses memperbaiki diri, salah satunya dengan medmberikan kesempatan untuk mengenyam pendidikan hingga saat ini.. terima kasih atas segala upaya yang dicurahkan disetiap waktu..

Terima kasih kepada teman dan sahabat yang telah bersedia berbagi ilmu, pengalaman dan kisah serta dukungan yang membangun..

Kata Pengantar



Assalamu'alaikum Wr. Wb.

Alhamdulillah segala puji bagi Allah SWT atas segala rahmat, hidayah, dan kehadirat-Nya, sehingga penulisan laporan tesis sebagai salah satu syarat memperoleh gelar Pascasarjana Magister Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia yang berjudul "Investigasi Live Forensik Dari Sisi Pengguna Untuk Menganalisa Serangan Man In The Middle Attack Berbasis Evil Twin" dapat diselesaikan dengan baik. Shalawat serta salam semoga senantiasa tercurah atas Nabi Muhammad SAW, para sahabat, serta pengikutnya.

Penyusunan tesis ini tidak lepas dari bimbingan, dukungan, dan bantuan dari berbagai pihak. Oleh Karena itu dalam kesempatan ini dan segala kerendahan hati, ucapan terima kasih diucapkan dengan setulus-tulusnya kepada:

1. Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis selalu diberkan kesehatan dan kemudahan selama masa pengerjaan tesis ini.
2. Bapak, Ibu, kakak, beserta keluarga besar yang telah mendoakan dan memberikan restu dan semangatnya.
3. Bapak Rektor dan seluruh jajaran rektorat Universitas Islam Indonesia.
4. Dr. R. Teduh Dirgahayu, ST., M.Sc selaku direktur Program Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia.
5. Dr. Imam Riadi, M.Kom dan Yudi Prayudi, S.Si.,M.Kom selaku dosen pembimbing yang telah memberikan pengarahan, bimbingan, masukan, serta dorongan semangat selama pengerjaan tesis ini.
6. Dosen-dosen Magister Teknik Informatika dan seluruh jajaran staf program Pascasarjana. Terima kasih atas semua ilmu pengetahuan, saran, motivasi, serta bantuannya.

7. Rekan-rekan Forensik Digital UII Angkatan X. terima kasih atas semua dukungan dan kerja samanya selama ini.
8. Keluarga besar Magister Teknik Informatika UII.
9. Rekan-Rekan Collayers, Rekan-Rekan Kosan Degolan, terima kasih atas semua dukungan dan kerja samanya selama ini
10. Terimakasih kepada kekasih tercinta yang jauh di malang, terimakasih atas dukunganya.
11. Sahabat-sahabat yang jauh disana dan selalu mendoakan, terima kasih.
12. Semua pihak yang telah memberikan bantuan dan dorongan yang tidak dapat disebutkan satu-persatu.

Saya menyadari bahwa dalam penulisan dan penyusunan laporan tesis ini masih banyak terdapat kekurangan. Untuk itu saya sampaikan permohonan maaf serta sangat mengharapkan kritik dan saran yang membangun untuk penyempurnaan di masa yang akan datang.

Yogyakarta, 2016

Muhammad Sabri Ahmad