ANALISA KEAMANAN JARINGAN WIRELESS DI UNIVERSITAS KRISTEN DUTA WACANA

Skripsi

oleh

STEVANUS TJANDRA

71130101

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS KRISTEN DUTA WACANA

2018

ANALISA KEAMANAN JARINGAN WIRELESS DI UNIVERSITA KRISTEN DUTA WACANA

Skripsi

Diajukan kepada Program Studi Informatika Fakultas Teknologi Informasi

Universitas Kristen Duta Wacana

Sebagai Salah Satu Syarat dalam Memperoleh Gelar

Sarjana Komputer

Disusun oleh

STEVANUS TJANDRA

71130101

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI

UNIVERSITAS KRISTEN DUTA WACANA

2018

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

ANALISA KEAMANAN JARINGAN WIRELESS DI UNIVERSITAS KRISTEN DUTA WACANA

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 8 Januari 2018

STEVANUS TJANDRA
71130101

HALAMAN PERSETUJUAN

Judul Skripsi	:	ANALISA KEAMANAN JARINGAN WIRELESS DI UNIVERSITAS KRISTEN DUTA WACANA
Nama Mahasiswa	:	STEVANUS TJANDRA
NIM	:	71130101
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Gasal
Tahun Akademik	:	2017/2018

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 8 Januari 2018

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, S.Kom.,M.Cs.	Budi Susanto, SKom.,M.T.

HALAMAN PENGESAHAN

ANALISA KEAMANAN JARINGAN WIRELESS DI UNIVERSITAS KRISTEN DUTA WACANA

Oleh: STEVANUS TJANDRA / 71130101

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 13 Desember 2017

Yogyakarta, 8 Januari 2018
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
2. Budi Susanto, SKom.,M.T.
3. Gani Indriyanta, Ir. M.T.
4. Hendro Setiadi, M.Eng

Dekan	Ketua Program Studi
(Budi Susanto, S.Kom., M.T.)	(Gloria Virginia, Ph.D.)

UCAPAN TERIMA KASIH

Puji syukur penulis ucapkan kehadirat Tuhan Yang Maha Esa karena telah memberi berkah dan perlindunganNya sehingga penulis dapat menyelesaikan laporan penelitian Analisis Keamanan Jaringan *Wireless* di Universitas Kristen Duta Wacana. Penulisan skripsi ini diajukan untuk memenuhi salah satu syarat kelulusan jenjang perkuliahan Strata I Universitas Kristen Duta Wacana.

Dalam penulisan skripsi ini tentunya masih banyak kekurangan, baik dari aspek kualitas maupun kuantitas materi penelitian yang disajikan. Penulis menyadari bahwa skripsi ini jauh dari kata sempurna sehingga penulis membutuhkan kritik dan saran yang bersifat membangun untuk perkembangan penulis di masa mendatang.

Pada kesempatan ini penulis dengan tulus hati mengucapkan terima kasih untuk orang-orang yang telah banyak mendukung dalam penulisan ini, kepada :

1. Bapak **Willy Sudiarto Raharjo, S.Kom, M.Cs** selaku Dosen Pembimbing I.
2. Bapak **Budi Susanto, S.Kom, M.T.** selaku Dosen Pembimbing II.
3. Pihak PUSPINDIKA yang telah memberikan dukungan data saat pengerjaan skripsi.
4. Orang tua penulis yang telah banyak membantu dan memberikan dukungan.
5. Teman-teman seperjuangan Claverence, Samuel, Ryan Daniel, Jordan, Wyllson dan Mada yang telah membantu dan memberikan dukungan juga.
6. Teman-teman kuliah Yudha, Yosafat, Ester, Aditya, Kosa dan Aryo yang telah membantu penulis dalam proses penyelesaian skripsi ini.
7. Seluruh teman-teman Informatika angkatan 2013 yang telah menjadi teman seperjuangan dalam menjalani proses perkuliahan dan tugas akhir.
8. Seluruh pihak yang telah terlibat yang tidak dapat disebutkan satu persatu dalam proses perkuliahan dan penyelesaian skripsi.

Akhir kata, semoga penelitian ini dapat berguna bagi kemajuan pendidikan dan kepentingan masyarakat umum.

Yogyakarta, 27 November 2017

Penulis

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas berkat dan kasih karunia-Nya sehingga penulis dapat menyelesaikan pembuatan sistem dan laporan tugas akhir dengan judul "*Analisis Keamanan Jaringan Wireless di Universitas Kristen Duta Wacana*" dengan baik.

Penulisan laporan tugas akhir ini diajukan sebagai salah satu syarat guna mencapai gelar Sarjana Strata Satu (S1) di Fakultas Teknologi Informasi Program Studi Teknik Informatika Universitas Kristen Duta Wacana Yogyakarta.

Dalam pembuatan laporan ini, penulis menyadari bahwa masih ada kekurangan, baik dari materi maupun teknik penyajiannya. Oleh karena itu, penulis sangat mengharapkan adanya kritik dan saran dari pembaca. Akhir kata penulis memohon maaf apabila dalam penulisan laporan ini, ada kalimat yang kurang berkenan. Semoga hasil dari pengerjaan tugas akhir ini dapat berguna dan bermanfaat bagi banyak pihak.

Yogyakarta, 27 November 2017

Penulis

INTISARI

Analisis Keamanan Jaringan *Wireless* di Universitas Kristen Duta Wacana

Man in The Middle (MiTm) adalah metode penyerangan yang digunakan oleh attacker untuk memanipulasi komunikasi antara *user* dan *access point* pada jaringan *wireless.* Serangan *MiTM* memiliki kelemahan 2 inti aspek keamanan yaitu *Confidentiality* dan *Integrity.* Pada jaringan *wireless* sangat diperlukan keamanan untuk komunikasi *user* di dalamnya. Namun, keamanan tidak bisa dilakukan sepenuhnya dari sisi *access point, client* juga harus mencegah terjadinya proses *Mitm* oleh *attacker.*

Penelitian ini menganalisis keamanan jaringan *wireless* di Universitas Kristen Duta Wacana berdasarkan aspek *Confidentiality* dan *Integrity.* Jaringan *wireless* di Universitas Kristen Duta Wacana tidak sepenuhnya aman.

Dari hasil analisis terhadap percobaan di gedung Agape dan gedung Didaktos, masih ditemukan celah keamanan jaringan *wireless* terhadap serangan *ARP poisoning* dan *DNS spoofing* didapatkan beberapa log *username* dan *password user* secara *plain text*. Dari hasil analisis peneliti menyarakan beberapa tools untuk pencegahan *ARP spoofing* dari segi *client*.

Kata kunci: *Man in The Middle, access point, user,* jaringan *wireless.*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Analisis Keamanan Jaringan *Wireless* di Universitas Kristen Duta Wacana

Man in The Middle (MiTm) adalah metode penyerangan yang digunakan oleh attacker untuk memanipulasi komunikasi antara *user* dan *access point* pada jaringan *wireless.* Serangan *MiTM* memiliki kelemahan 2 inti aspek keamanan yaitu *Confidentiality* dan *Integrity.* Pada jaringan *wireless* sangat diperlukan keamanan untuk komunikasi *user* di dalamnya. Namun, keamanan tidak bisa dilakukan sepenuhnya dari sisi *access point, client* juga harus mencegah terjadinya proses *Mitm* oleh *attacker.*

Penelitian ini menganalisis keamanan jaringan *wireless* di Universitas Kristen Duta Wacana berdasarkan aspek *Confidentiality* dan *Integrity.* Jaringan *wireless* di Universitas Kristen Duta Wacana tidak sepenuhnya aman.

Dari hasil analisis terhadap percobaan di gedung Agape dan gedung Didaktos, masih ditemukan celah keamanan jaringan *wireless* terhadap serangan *ARP poisoning* dan *DNS spoofing* didapatkan beberapa log *username* dan *password user* secara *plain text*. Dari hasil analisis peneliti menyarakan beberapa tools untuk pencegahan *ARP spoofing* dari segi *client*.

Kata kunci: *Man in The Middle, access point, user,* jaringan *wireless.*

BAB 1
PENDAHULUAN

1.1. Latar Belakang Masalah

Peningkatan penggunaan jaringan *wireless* telah meningkat pesat. Jaringan *wireless* hampir dapat ditemukan di berbagai fasilitas umum. Salah satunya adalah Universitas Kristen Duta Wacana.

Jaringan *wireless* memiliki banyak celah keamanan dibandingkan dengan jaringan kabel. Jaringan *wireless* secara umum memiliki 3 aspek celah keamanan. Aspek keamanan tersebut adalah *Confidentiality, Integrity, Avaibality*.(Scarfone dkk,2008). Seluruh aspek kelemahan ini disebabkan cara kerja jaringan *wireless* ataupun media yang dimiliki jaringan *wireless.*

Maka dari itu proses perencanaan, implementasi, pemilihan dan pengolahan jaringan *wireless* membutuhkan kompetensi yang cukup, mengingat berbagai celah keamanan yang ada. Serangan yang sering terjadi di dalam jaringan *wireless* antara lain: *Sniffing, Spoofing* dan *Hijacking*. Jenis serangan-serangan tersebut lebih mudah dilakukan oleh para *attacker* karena jaringan *wireless* menggunakan udara sebagai media pengiriman dan menyebabkan para *attacker* mudah untuk melihat aktivitas *internet* dan paket yang dikirim yang dilakukan oleh *user*. Aktivitas *internet user* yang telah berhasil di *sniffing* oleh *attacker* membuat kredibilitas dari layanan jaringan *wireless* tersebut menjadi berkurang. Para *attacker* memiliki kemungkinan untuk mengetahui segala aktivitas *Internet* yang dilakukan oleh *user* dalam jaringan *wireless*. Kemungkinan lain yang mungkin terjadi adalah seluruh aktivitas *Internet user* telah dipalsukan oleh *attacker*. Seluruh paket yang dikirim ke *user* lain, bisa diubah oleh *attacker* tanpa mengetahui isi paket sesungguhnya.

Peneliti menganalisis seluruh masalah keamanan jaringan *wireless* di UniversitasKristen Duta Wacana dan memberikan solusi ataupun perbaikan terhadap masalah keamanan jaringan untuk meningkatkan keamanan jaringan *wireless* di Universitas Kristen Duta Wacana.

1.2. Rumusan Masalah

Seberapa baik tingkat keamanan jaringan *wireless* di Universitas Kristen Duta Wacana dengan uji penetrasi menggunakan *tools Ettercap* dan *Aircrack*.

1.3. Batasan Masalah

1. Ruang lingkup dalam tugas akhir untuk mengoptimalkan keamanan jaringan *wireless* pada Universitas Kristen Duta Wacana untuk pencegahan serangan keamanan jaringan *wireless*.
2. Penelitian dilakukan dengan mengambil sampel dari gedung Agape dan gedung Didaktos di Universitas Kristen Duta Wacana.
3. Penelitian dilakukan di hari libur atau diluar jam operasional perkuliahan untuk mengurangi dampak serangan terhadap jaringan *wireless.*
4. Aspek pengujian keamanan yang dinilai menggunakan *tools Ettercap* dan *Aircrack* lebih di fokuskan pada aspek *confidentiality* dan *Integrity*.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengidentifikasi dan mengevaluasi jaringan *wireless* di Universitas Kristen Duta Wacana melalui uji penetrasi yang dilakukan oleh peneliti.

1.5. Metode Penelitian

Metodologi yang digunakan dalam penelitian untuk mengevaluasi keamanan jaringan *wireless* di Universitas Kristen Duta Wacana sebagai berikut:

1) Studi Pustaka

   Studi pustaka, mempelajari, mencari, dan mengumpulkan data yang berkaitan dengan keamanan jaringan *wireless*. Cara melakukan evaluasi keamanan jaringan, melalui beberapa buku, jurnal, artikel, dan bahan lain yang mendukung penelitian ini baik melalu *internet* maupun buku tercetak.

2) Pengumpulan data

   Pada tahap pengumpulan data, peneliti mengambil data-data jaringan *wireless* UKDW dari pihak PUSPINDIKA. Data tersebut diambil atas izin resmi dengan pihak PUSPINDIKA. Selanjutnya kekurangan data yang diambil digabungkan dengan data hasil observasi langsung peneliti.

3) Perencanaan, identifikasi dan penyerangan untuk menguji keamanan jaringan *wireless*

   Pada tahap ini dilakukan beberapa proses untuk melakukan pengujian celah keamanan jaringan *wireless* Universitas Kristen Duta Wacana. Proses ini dibagi menjadi 3 tahapan untuk menguji celah keamanan yang ada.

   1. Tahap perencanaan

      Pada tahap perencaan, peneliti melakukan observasi dan menentukan lokasi serta target (*access point)* untuk dilakukan pengujian keamanan jaringan *wireless*.

   2. Tahap identifikasi

      Pada tahap identifikasi, peneliti mengumpulkan seluruh informasi mengenai target berupa network, port, service dan informasi lainnya yang digunakan untuk menemukan celah keamanan yang dapat dieksploitasi.

3. Tahap penyerangan

   Pada tahap penyerangan terdapat beberapa proses yang dilakukan oleh peneliti yaitu:

   - Mendapatkan akses: Setelah mengumpulkan informasi dari proses identifikasi, peneliti mencoba mendapatkan akses dari *access point* melalui celah keamanan yang ada.
   - Mendapatkan *privileges*: Jika pada tahap sebelumnya peneliti hanya mendapatkan akses sebagai user, peneliti berikutnya akan mencoba mendapatkan akses penuh sebagai *system administrator*.
   - Identifikasi kelemahan sistem: Pada tahap ini peneliti mengumpulkan informasi kembali dengan mengidentifikasi kelemahan sistem untuk mendapatkan akses tambahan dari sistem.
   - Penyerangan kedua: Pada tahap ini, peneliti melakukan serangan kembali menggunakan tools tambahan untuk mendapatkan informasi atau akses tambahan dengan memanfaatkan celah keamanan yang ada.Analisis hasil penelitian

4) Analisis hasil penelitian

   Membuat laporan dari hasil pengujian dan identifikasi jaringan *wireless.* Peneliti mencatat seluruh serangan dan celah keamanan yang ditemui dari hasil pengujian. Hasil pengujian akan dianalisis untuk menemukan solusi perbaikan kedepannya.

1.6. Sistematika Penulisan

BAB I PENDAHULUAN membahas tentang latar belakang, rumusan masalah, batasan masalah, hipotesis, tujuan penelitian, metode penelitian serta sistematika penulisan penelitian ini.

BAB II TINJAUAN PUSTAKA. membahas tinjauan pustaka yang berisi referensi mengenai keamanan jaringan *wireless* dan landasan teori yang menjadi dasar penelitian ini. Pada bab ini dijelaskan secara detail seluruh informasi dan studi pustaka yang diperoleh oleh peneliti berkatian dengan analisis keamanan jaringan *wireless.* Bab ini akan menjadi acuan peneliti untuk melakukan tahapan penelitian.

BAB III ANALISIS DAN PERANCANGAN PENELITIAN. Berisi rancangan jaringan *wireless* yang diimplementasikan standar keamanan jaringan Alur kerja sistem, hardware dan software yang dibutuhkan untuk mendukung penelitian.

BAB IV IMPLEMENTASI SISTEM DAN ANALISIS SISTEM. Berisi uraian detail implementasi sistem dan uraian detail hasil analisis sistem yang didapatkan dari hasil uji coba yang dilakukan.

BAB V SARAN DAN KESIMPULAN. Berisi kesimpulan dari hasil analisis yang didapat,saran dan rekomendasi yang dapat dilakukan untuk penelitian lebih lanjut.

BAB 5
SARAN DAN KESIMPULAN

5.1. Kesimpulan

Berdasarkan dari hasil pengujian dan analisis yang telah dilakukan oleh peneliti pada bab sebelumnya, maka dapat disimpulkan bahwa:

1. Masih terdapat celah keamanan pada jaringan wireless UKDW berupa berhasilnya dilakukan serangan *ARP poisoning*.
2. Penyerangan *ARP poisoning* yang berhasil dilakukan membuat munculnya celah keamanan baru yang menyebabkan peneliti berhasil mendapatkan log *username* dan *password* hanya dengan terhubung ke jaringan *wireless* UKDW. Log *plain text* yang didapatkan sejumlah 33 buah, 31 buah melalui port 443 dan 2 buah melalui port 993.
3. Tingkat keamanan *wireless* di Universitas Kristen Duta Wacana belum cukup baik di karenakan kurangnya aspek keamanan *confidentiality* dan *integrity*.
4. Rekomendasi implementasi keamanan untuk pencegahan proses penyerangan dengan *ARP poisoning* dari segi client dengan menginstall aplikasi pendeteksi serangan *ARP* seperti : *ARP Guard* dan *Xarp.*

5.2 Saran

Beberapa saran yang dapat menjadi masukan untuk penelitian yang akan datang adalah:

1. Mencoba melakukan pengujian serangan kemanan dengan beberapa *tool* tambahan pada penelitian selanjutnya untuk menemukan celah keamanan lain yang mungkin terdapat pada jaringan *wireless* UKDW.

2. Menerapkan langsung hasil rekomendasi implementasi keamanan jaringan *wireless* yang diberikan oleh peneliti.
3. Memberikan informasi lebih lanjut kepada seluruh *user* jaringan *wireless* UKDW untuk meningkatkan tingkat kesadaran terhadap pengamanan saat menggunakan jaringan *wireless*.

DAFTAR PUSTAKA

.

Frankel, S., Eydt, B., Owens, L., & Scarfone, K. (2007). Establishing wireless robust security networks: a guide to IEEE 802.11 i. *National Institute of Standards and Technology*.

Scarfone, K., Dicoi, D., Sexton, M., & Tibbs, C. (2008). Guide to securing legacy IEEE 802.11 wireless networks. *NIST Special Publication*, *800*, 48.

Setyawan, B. K. A., & Syafrizal, M. (2012). ANALISIS KEAMANAN JARINGAN WIRELESS YANG MENGGUNAKAN CAPTIVE PORTAL (Studi Kasus: Warnet Fortran). *Data Manajemen dan Teknologi Informasi (DASI)*, *13*(3), 13.

Rumalutur, S. (2014). Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong. *Jurnal Ilmiah Teknologi dan Rekayasa*, *19*(3).

Sari, A., & Karay, M. (2015). Comparative Analysis of Wireless Security Protocols: WEP vs WPA. *International Journal of Communications, Network and System Sciences*, *8*(12), 483.

Bawiskar, A., & Meshram, B. B. (2013). Survey of Attacks on Wireless Network. *Int. J. Innov. Res. Comput. Commun. Eng.*, *1*.

Refaat, T. M., Abdelhamid, T. K., & Mohamed, A. F. M. (2016). Wireless Local Area Network Security Enhancement through Penetration

Testing. *International Journal of Computer Networks and Communications Security*, *4*(4), 114-129.

Kumar, U., & Gambhir, S. (2014). A literature review of security threats to wireless networks. *International Journal of Future Generation Communication and Networking*, *7*(4), 25-34.

Pavithran Muthu & Pavitharn.S (2015). Advanced Attack Against Wireless Networks Wep, Wpa/Wpa2-Personal And Wpa/Wpa2-Enterprise. International Journal of Scientific & Technology Research, 4(8).

M.Jain, V.Jain, & L.Borade (2016). A Surver on Man in the Middle Attack. International Journal of Science Technology & Engineering,2(9).