

**ANALISA KEAMANAN WIRELESS NETWORK DI WARNET
JAVATECHNO**



SKRIPSI

Disusun sebagai salah satu syarat menyelesaikan Program Studi Strata I pada
Jurusan Teknik Informatika Fakultas Komunikasi dan Informatika
Universitas Muhammadiyah Surakarta

Diajukan Oleh :

CITRA MAYANGSARI ADANINGGAR

L200080071

**PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS
KOMUNIKASI DAN INFORMATIKA UNIVERSITAS
MUHAMMADIYAH SURAKARTA**

2012

HALAMAN PERSETUJUAN

Skripsi dengan judul

“ANALISA KEAMANAN WIRELESS NETWORK DI WARNET JAVA TECHNO”

Ini telah diperiksa, disetujui, dan disahkan pada :

Hari :

Tanggal :

Pembimbing I

Pembimbing II

(Fajar Suryawan, S.T., M.Eng.Sc., Ph.D)

NIK : 924

(Muhammad Kusban, S.T., M.T)

NIK : 663

HALAMAN PENGESAHAN

ANALISA KEAMANAN WIRELESS NETWORK DI WARNET

JAVATECHNO

dipersiapkan dan disusun oleh

Citra Mayangsari Adaninggar

NIM : L200080071

telah dipertahankan di depan Dewan Penguji

pada tanggal

Susunan Dewan Penguji

Pembimbing I

Anggota Dewan Penguji Lain

Fajar Suryawan, S.T., M.Eng.Sc., Ph.D

NIK : 924

Pembimbing II

Jan Wantoro, S.T

NIK : 200.1304

Muhammad Kusban, S.T., M.T

NIK : 663

Dedi Ary Prasetya, S.T

Nik : 982

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar sarjana

Tanggal

Dekan
Fakultas Komunikasi dan Informatika

Ketua Program Studi
Teknik Informatika

Husni Thamrin, S.T, MT., Ph.D.
NIK : 706

Aris Rakhmadi, ST., M.Eng.
NIK : 983

MOTTO

✚ *“Sesungguhnya, Allah tidak akan merubah keadaan suatu kaum sehingga mereka mengubah keadaan diri mereka sendiri”*

(Q.S Ar Ra'd :11)

✚ *“Dan barang siapa yang bertakwa kepada Allah, niscaya Allah menjadikan baginya kemudahan dalam urusannya”*

(Q.S Ath Thalaq : 4)

✚ *“Jalani sesuatu dengan senyuman ☺”*

(Citra Mayangsari A.)

PERSEMBAHAN

Hanya ini yang bisa aku berikan, jerih payah selama ini tak terasa telah menuai hasil karya yang sederhana ini. Kupersembahkan karya tulis yang sederhana ini untuk:

- Bapak dan Ibu tercinta. Kasih sayangmu, perjuanganmu, pengorbananmu, serta doamu abadi sepanjang masa. Karya sederhanaku ini kupersembahkan sebagai bukti keseriusanku dan hasil perjuangan mu selama ini
- Wahyu Prehantoro, adikku tersayang yang telah berkorban untukku, dan selalu memberikan dukungan serta kasih sayangnya
- Fajar Kurniawan, yang telah menemaniku menyelesaikan Tugas Akhir ini, dan tidak bosan – bosannya menyemangatiku, serta selalu kurepotkan
- Teman – temanku, yang selalu bersama dalam suka maupun duka
- Almamaterku Universitas Muhammadiyah Surakarta

KONTRIBUSI

Puji syukur kepada Allah SWT, atas karunia rahmat dan ridho-Nya sehingga penulis dapat menyelesaikan penelitian ini. Dengan ini saya menyatakan bahwa skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi.

Berikut saya sampaikan daftar kontribusi dalam penyusunan skripsi :

1. Saya melakukan beberapa jenis serangan untuk mengetahui celah keamanan yang masih terdapat di Warnet Javatechno
2. Saya mendapat bantuan dari teman saya Mas Surya dan Adefian dalam mengetahui bahwa network adapter laptop saya tidak support untuk melakukan serangan
3. Saya melakukan penelitian di Warnet Javatechno
4. Saya menemukan celah keamanan pada system wireless Warnet Javatechno, dan saya mencoba untuk memberikan saran berupa penerapan system tambahan guna mengatasi celah keamanan yang masih ada
5. Saya mencoba menerapkan system tambahan yang saya ajukan dengan bantuan teman saya

Demikian pernyataan dan daftar kontribusi ini saya buat dengan sejujurnya. Saya bertanggung jawab atas isi dan kebenaran daftar di atas.

Surakarta, Januari 2012

Citra Mayangsari Adaninggar

Mengetahui,

Dosen Pembimbing I

Dosen Pembimbing II

(Fajar Suryawan, S.T., M.Eng.Sc., Ph.D.) **(Muhammad Kusban, S.T., M.T.)**

NIK : 924

NIK : 663

KATA PENGANTAR



Assalamu 'alaikum WR.WB

Segala puja dan puji syukur Alhamdulillah kami panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat, hidayah, serta karunia kepada kita selaku hamba yang dicintai dan disayangi di alam semesta. Shalawat dan salam terlimpahkan kepada manusia pilihan Allah SWT yaitu Nabi Muhammad SAW yang dengan penuh perjuangan telah mengantarkan kita menjadi umat pilihan dan mendapat Ridho-Nya.

Hanya karena Allah SWT akhirnya penulis bias melewati kendala dan tantangan dalam menyelesaikan dan menyusun laporan tugas tugas akhir ini. Tugas akhir ini disusun dan diajukan sebagai syarat untuk kelulusan dan mendapatkan gelar Sarjana Komputer di jurusan Teknik Informatika Universitas Muhammadiyah Surakarta. Adapun judul tugas akhir yang penulis ajukan : “ANALISA KEAMANAN WIRELESS NETWORK DI WARNET JAVATECHNO”.

Selama penyusunan tugas akhir ini penulis mendapatkan dukungan, pembinaan, dan saran dari pembimbing dan pihak – pihak lain yang terlibat secara langsung maupun tidak langsung dalam tugas akhir ini. Maka tiada kata yang lebih bagi penulis yang hanya terucap dan bisa mengucapkan terima kasih kepada :

1. Bapak Husni Tamrin, S.T., M.T., Ph.D. selaku Dekan Fakultas Komunikasi dan Informatika Universitas Muhammadiyah Surakarta
2. Bapak Aris Rakhmadi, S.T., M.Eng. selaku Ketua Jurusan Teknik Informatika Universitas Muhammadiyah Surakarta
3. Bapak Fajar Suryawan, S.T., M.Eng.Sc., Ph.D. selaku pembimbing pertama dalam penyusunan tugas akhir ini (terima kasih atas bimbingan, referensi, dan waktu yang telah diberikan)
4. Bapak Muhammad Kusban, S.T., M.T. selaku pembimbing kedua dalam penyusunan tugas akhir ini (terima kasih atas bimbingan, referensi, dan waktu yang telah diberikan)
5. Bapak dan ibu dosen yang telah memberikan ilmu dan pengetahuan selama menempuh pendidikan di Teknik Informatika UMS
6. Seluruh Staf Tata Usaha, Staf Akademik maupun non Akademik, yang telah banyak membantu dan memberikan kemudahan kepada penulis selama menempuh studi di Fakultas Komunikasi dan Informatika jurusan Teknik Informatika Universitas Muhammadiyah Surakarta
7. Mas Five selaku pengelola Warnet Javatechno yang telah berkenan memberikan izin untuk penelitian
8. Seluruh Staf administrator Warnet Javatechno yang tidak dapat saya sebutkan satu per satu yang telah memberikan bantuan dan dukungan dalam penyusunan tugas akhir ini
9. Bapak dan Ibuku yang selalu member kasih sayang, perhatian, motivasi, biaya, dan tak lupa do'anya

10. Adikku Wahyu Prehantoro yang selalu menyayangi dan menyemangatiku
11. Nenekku atas dukungan dan kasih sayangnya
12. Saudara – saudaraku yang selalu memberi bantuan dikala kesulitanku
13. Fajar Kurniawan yang selalu membantu dan menyemangatiku,selalu aku repotkan, hanya ucapan terima kasih atas kebersamaan dan bantuannya selama ini
14. Sahabatku, Iris Diana yang selalu menemaniku walaupun jauh di sana
15. Pak Wuri dan Mas Ihsan, terima kasih untuk ilmunya yang sangat membantu
16. Gilang dan Surya (Amikom Yogyakarta) yang telah memberiku referensi mengenai serangan wireless
17. Teman – teman kosku yang selalu memberi warna dan menemaniku dalam proses penyelesaian tugas akhir ini, khususnya Iin Sofiyani, Eti Rohani, dan Umi yang selalu meminjamkanku laptop ketika membutuhkan laptop tambahan
18. Seluruh rekan – rekan di Teknik Informatika yang tidak bisa disebutkan semuanya, terima kasih atas persahabatan dan persaudaraannya selama kuliah di UMS
19. Ucapan terima kasih kepada semua pihak yang telah membantu penyelesaian tugas akhir ini, yang tidak bisa saya sebutkan satu – per satu

Selalu penulis sadari bahwa laporan tugas akhir ini tidaklah sempurna yang diharapkan karena keterbatasan kemampuan penulis dalam penyusunan, oleh sebab itu saran dan kritik yang bersifat membangun akan selalu penulis terima untuk kesempurnaan diwaktu mendatang.

Semoga laporan Tugas Akhir ini dapat bermanfaat bagi penulis pada khususnya serta bermanfaat bagi pembaca pada umumnya dan dapat dijadikan referensi untuk menambah pengetahuan di bidang informatika dan untuk penelitian serupa di waktu mendatang, Amin.

Wassalamualaikum WR.WB

Surakarta, Januari 2012

Peneliti

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN MOTTO	v
HALAMAN PERSEMBAHAN	vi
HALAMAN KONTRIBUSI.....	vii
KATA PENGANTAR.....	ix
DAFTAR ISI.....	xiii
DAFTAR TABEL	xvi
DAFTAR GAMBAR.....	xvii
ABSTRAKSI.....	xx
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	5
1.6 Sistematika Penulisan	5
1.7 Mind Map	7
1.8 Metodologi Penelitian	7
BAB II TINJAUAN PUSTAKA	9
2.1 Telaah Penelitian	9

2.2 Landasan Teori	10
2.2.1 Internet	10
A. Local Area Network (LAN)	11
B. Metropolitan Area Network (MAN)	12
C. Wide Area Network (WAN)	12
2.2.2 Wireless LAN.....	15
A. Komponen Wireless LAN.....	19
B. Topologi Wireless LAN	25
C. Keamanan Wireless LAN.....	27
D. Handshaking Access Point	35
E. Autentikasi Wireless	36
2.2.3 Lapisan Protokol TCP/IP	37
A. Arsitektur Protokol TCP/IP.....	38
B. IP Address	44
C. MAC Address	51
2.2.4 Sistematika Perjalanan Paket ARP	54
BAB III METODE PENELITIAN	58
3.1 Waktu dan Tempat	58
3.2 Profil Warnet	58
3.3 Peralatan Utama dan Pendukung	59
3.3.1 Bahan Analisis dan Perancangan	59
3.3.2 Perlengkapan Pendukung.....	60
3.4 Tahap Analisis dan Perancangan.....	60

3.4.1 Study Literatur.....	60
3.4.2 Survey dan Pengambilan Data	61
3.4.3 Teknis Serangan	62
3.4.4 Proses Pelaksanaan Percobaan	62
3.4.5 Hasil/Keluaran yang Didapat dari Percobaan	81
BAB IV HASIL DAN PEMBAHASAN	83
4.1 Hasil Penelitian	83
4.2 Analisis Hasil Penelitian	83
4.3 Sistem Tambahan untuk Menangani Celah Keamanan yang Ada	86
BAB V KESIMPULAN DAN SARAN.....	92
5.1 Kesimpulan	92
5.2 Saran.....	93
DAFTAR PUSTAKA	94
LAMPIRAN.....	96

DAFTAR TABEL

Tabel 2.1 : Tabel Spesifikasi Wi-Fi	19
Tabel 2.2: Arsitektur TCP/IP	42
Tabel 2.3: Kelas IP Address.....	45

DAFTAR GAMBAR

Gambar 1.1 : Mind Map Skripsi.....	7
Gambar 2.1 : Alur Koneksi Internet	10
Gambar 2.2 : <i>Access Point</i> dari produk <i>Linksys, Symaster, Dlink</i> (repository.usu.ac.id : 2010).....	20
Gambar 2.3 1: Jaringan Menggunakan <i>Extension Point</i> (repository.usu.ac.id : 2010).....	22
Gambar 2.4 : Jangkauan Area Antena Omnidirectional (repository.usu.ac.id : 2010).....	24
Gambar 2.5 : Jangkauan Antena Directional (repository.usu.ac.id : 2010)....	24
Gambar 2.6 : Wireless LAN Card (repository.usu.ac.id : 2010).....	25
Gambar 2.7 : Topologi Ad Hoc (joss.staf.ugm.ac.id : 2005)	26
Gambar 2.8 : Topologi Infrastruktur (joss.staf.ugm.ac.id : 2005).....	27
Gambar 2.9 : Pembentukan dan Pemurusan Koneksi TCP	36
Gambar 2.10 : Proses Autentikasi Jaringan	37
Gambar 2.11 : Pergerakan Data dalam Layer TCP/IP	43
Gambar 2.12 : Perolehan Informasi ARP	57
Gambar 3.1 : Host yang Aktif beserta MAC Addressnya.....	63
Gambar 3.2 : Host yang Aktif beserta MAC Addressnya.....	63
Gambar 3.3 : IP Address dan MAC Address Device Penyerang.....	64
Gambar 3.4 : Program MAC Address Changer	65
Gambar 3.5 : Proses Pengubahan MAC Address Device Penyerang	66

Gambar 3.6 : Memasukkan MAC Address Target untuk Melakukan Perubahan	67
Gambar 3.7 : Perubahan MAC Address pada Device Penyerang	68
Gambar 3.8 : Proses Merubah IP Address dan DNS Server	69
Gambar 3.9 : Perubahan IP Address Device Penyerang	69
Gambar 3.10 : Pengecekan Koneksi Internet dengan Command Prompt.....	70
Gambar 3.11 : Pengecekan Koneksi Internet dengan Web Browser	70
Gambar 3.12: <i>Traceroute</i> dan Ping Device Target Sebelum Login.....	71
Gambar 3.13 : <i>Traceroute</i> dan Ping Device Target Setelah Login.....	72
Gambar 3.14 : <i>Traceroute</i> dan Ping Device Penyerang.....	73
Gambar 3.15 : <i>Traceroute</i> Device Penyerang Setelah dilakukan Perubahan MAC Address dan IP Address	73
Gambar 3.16 : Ping Device Penyerang Setelah dilakukan Perubahan MAC Address dan IP Address.....	74
Gambar 3.17 : Interface Device Penyerang	75
Gambar 3.18 : Pengaktifan Interface	76
Gambar 3.19 : Membuat Interface Mode Monitor.....	76
Gambar 3.20 : Memonitor Jaringan	77
Gambar 3.21 : Program Wireshark	78
Gambar 3.22 : Option untuk Memilih Interface yang Ada	78
Gambar 3.23 : Hasil Pengelompokan Data Berdasarkan Protokol http.....	79
Gambar 3.24 : Hasil Sniffing Username dan Password.....	80
Gambar 3.25 : Keluaran Program SysAnalyzer.....	80

Gambar 3.26 : Hasil Program SysAnalyzer	81
Gambar 4.1 : Tampilan Comodo Firewall pada Proses Scanning oleh Client dengan Nmap	87
Gambar 4.2 : Tampilan DecaffeinatID ketika ada Perubahan MAC Address .	88
Gambar 4.3 : View Log pada DecaffeinatID	89
Gambar 4.4 : Penggantian Subnetmask Secara Manual Menjadi 255.255.255.255	91
Gambar 4.5 : Peringatan/Penolakan Penggantian Subnetmask Secara Manual	91

ABSTRAKSI

Jaringan nirkabel merupakan teknologi jaringan yang menggunakan udara sebagai medium transmisi data. Warnet Javatechno merupakan salah satu warnet yang mempunyai fasilitas jaringan nirkabel (wireless). Jaringan wireless sangat rentan terhadap ancaman serangan yang dilakukan oleh attacker, dikarenakan komunikasi yang terjadi bersifat terbuka. Diperlukan system pengamanan yang berlapis untuk dapat menjaga system wireless agar terhindar dari kerusakan yang disebabkan oleh orang-orang yang tidak bertanggung jawab.

System keamanan yang digunakan oleh Warnet Javatechno saat ini yaitu dengan Captive Portal yang merupakan metode Open System Authentication. Authentication pada metode ini tidak terjadi pada saat pengguna melakukan koneksi ke Access Point, melainkan terjadi ketika pengguna akan melakukan pengaksesan ke internet saat pertama kali. Hal ini belum bisa dijadikan sebagai patokan keamanan jaringan wireless, sehingga diperlukan beberapa percobaan untuk mengetahui celah keamanan yang masih ada. Beberapa jenis percobaan yang dilakukan antara lain MAC Address Spoofing, Man In The Middle Attack, Cracking Wireless, dan analisa keberadaan virus. Dari keempat percobaan yang telah dilakukan, MAC Address Spoofing berhasil dilakukan, sedangkan tiga percobaan yang lain tidak berhasil dilakukan. Hal ini menunjukkan bahwa masih terdapat celah keamanan pada system wireless Warnet Javatechno, yaitu dari sisi MAC Address Spoofing. Diperlukan system tambahan untuk dapat mencegah/menangani celah keamanan yang masih ada. Software decaffeinatID sebagai salah satu jenis IDS (Intrusion Detection Server) sederhana, serta Comodo Firewall sebagai salah satu software pertahanan dapat diterapkan untuk memonitor jaringan sehingga dapat mencegah/menangani celah keamanan yang masih ada. Pembagian network menjadi subnetwork pun dapat diterapkan untuk meminimalisir terjadinya MAC Address Spoofing.

Kata Kunci : *Wireless, Attacker, Keamanan Wireless*