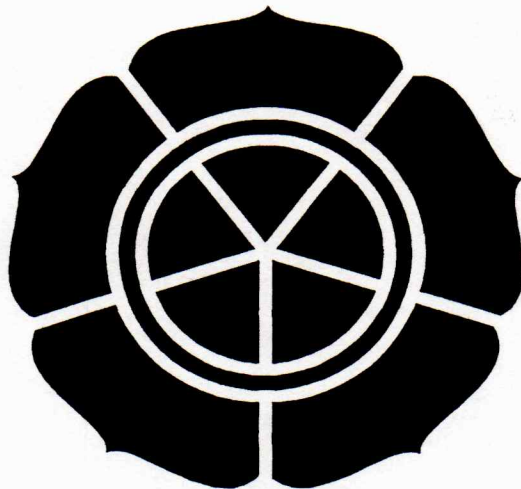


**ANALISIS SISTEM KEAMANAN JARINGAN NIRKABEL (Studi Kasus
Pada Jaringan Hot-Spot PT. XYZ yang Menerapkan WEP dan WPA-PSK)**

Skripsi



oleh:

Satrya Darmawan (04.11.0560)

**TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
"AMIKOM"
YOGYAKARTA
2008**

HALAMAN PENGESAHAN

**"ANALISIS SISTEM KEAMANAN JARINGAN NIRKABEL (Studi Kasus
pada Jaringan Hot-Spot PT. XYZ yang Menerapkan WEP dan WPA-PSK)"**

Skripsi

Disusun sebagai persyaratan untuk memperoleh gelar Sarjana Komputer

Jurusan Teknik Informatika

Sekolah Tinggi Manajemen Informatika dan Komputer

AMIKOM Yogyakarta

Disetujui dan disahkan oleh :

Ketua STMIK AMIKOM Yogyakarta



(Dr. M. Suyanto, MM)

Dosen Pembimbing

(Abas Ali Pangera, MKom)

HALAMAN BERITA ACARA

"ANALISIS SISTEM KEAMANAN JARINGAN NIRKABEL (Studi Kasus pada Jaringan Hot-Spot PT. XYZ yang Menerapkan WEP dan WPA-PSK)"

Laporan ini telah dipertahankan dan diajukan oleh **Satrya Darmawan** didepan Tim Penguji Jurusan Teknik Informatika sebagai syarat kelulusan Strata 1 Teknik Informatika STMIK AMIKOM Yogyakarta, pada:

Hari/Tanggal : Senin/26 Mei 2008

Jam : 08.30 WIB

Tempat : Ruang Pixel

Tim Penguji

Penguji I

(Sudarmawan, MT)

Penguji II

(Melwin Syafrizal, S.Kom)

Penguji III

(Armadyah Amborowati, S.Kom)



HALAMAN PERSEMBAHAN

Segala puji hanya bagi Alloh Subhanahu wata'ala yang Maha Pemurah lagi Maha Berkuasa atas segala sesuatu. Segala puji hanya bagi Alloh Subhanahu wata'ala yang Maha Mendengar doa para hamba-Nya. Segala puji hanya bagi Alloh Subhanahu wata'ala atas segala nikmat yang diberikan kepada seluruh makhluk-Nya. Shalawat dan salam semoga tetap terlimpah pada nabi Muhammad Shalallohu alaihi wa salam, para keluarga, para sahabat dan para pengikut beliau yang senantiasa mengikuti sunnah-sunnahnya hingga akhir zaman.

Tidak lupa penulis ucapkan terima kasih pada:

- Bapak dan ibu yang selalu mendoakan, memberikan dukungan baik dana maupun moril kepada penulis, serta adiku Neneng yang mudah-mudahan Alloh senantiasa menjaga mereka semua.
- Dosen pembimbingku yang sudah sangat membantu penyelesaian tugas akhir ini ditengah kesibukannya yang sangat banyak bapak Abas Ali Pangera, MKom.
- Teman-temanku, Hakim yang telah banyak memberikan bantuan pada penulis sekaligus tempat curhat, Praja, Andi, Azis, Mas Nana, Yogi, Dimas yang telah banyak memberikan bantuan dan nasehat pada penulis serta teman-temanku yang lain yang tidak dapat disebutkan satu persatu. (Terima kasih atas support dan doanya).

KATA PENGANTAR

Assalamu 'alaikum warohmatullohi wabarokatuh

Dengan menyebut nama Allah Subhana Wata'ala Yang Maha Pengasih lagi Maha Penyayang, puji syukur kehadiran Allah Subhana Wata'ala yang telah melimpahkan rahmat, taufiq dan hidayah-Nya kepada hamba-hamba-Nya. Semoga sholawat dan salam selalu dilimpahkan kepada Nabi Muhammad Sholallohu 'Alaihi Wassalam, keluarganya, sahabat dan pengikut beliau yang beriman sampai hari kiamat.

Skripsi yang berjudul "ANALISIS SISTEM KEAMANAN JARINGAN NIRKABEL (Studi Kasus pada Jaringan Hot-Spot PT. XYZ yang Menerapkan WEP dan WPA-PSK)" ini semoga dapat bermanfaat bagi siapapun dan bagi yang ingin mengembangkan lebih lanjut. Semoga dengan adanya penelitian ini dapat lebih bermanfaat bagi para administrator maupun pengguna jaringan nirkabel dalam menanggapi isu keamanan.

Semoga ilmu yang telah diperoleh dapat bermanfaat baik bagi penulis maupun bagi pembaca.

Jogjakarta, Mei 2008

Satrya Darmawan

DAFTAR ISI

| | |
|---------------------------------------|------------|
| HALAMAN JUDUL | i |
| HALAMAN PENGESAHAN | ii |
| HALAMAN BERITA ACARA | iii |
| HALAMAN PERSEMBAHAN | iv |
| KATA PENGANTAR..... | v |
| DAFTAR ISI | vi |
| DAFTAR GAMBAR..... | xi |
| DAFTAR TABEL | xiv |
| BAB I PENDAHULUAN | 1 |
| 1. Latar Belakang Masalah | 1 |
| 2. Perumusan Masalah | 3 |
| 3. Batasan Masalah | 3 |
| 4. Maksud dan Tujuan | 5 |
| 5. Metode Penelitian | 6 |
| 6. Sistematika Penulisan | 7 |
| 7. Jadwal Penelitian | 9 |
| BAB II LANDASAN TEORI..... | 10 |
| 1. Pengertian Jaringan Nirkabel | 10 |
| 1. 1. Wi-Fi (Wireless Fidelity) | 10 |

| | |
|---|----|
| 1.1.1. Ad Hoc | 11 |
| 1.1.2. Infrastructure dan Access Point | 12 |
| 1.2. LAN Nirkabel | 13 |
| 1.2.1. Standard 802.11a | 14 |
| 1.2.2. Standard 802.11b | 15 |
| 1.2.3. Standard 802.11g | 16 |
| 2. Wired Equivalent Privacy (WEP) | 17 |
| 2.1. Initialization Vector (IV) | 21 |
| 2.2. CRC 32 | 22 |
| 3. WPA (Wi-Fi Protected Access) | 22 |
| 4. WPA-PSK | 24 |
| 5. Manfaat Audit Jaringan Nirkabel | 25 |
| 6. Fitur Keamanan Dasar Jaringan Nirkabel | 27 |
| 6.1. Service Set Identifier (SSID) | 27 |
| 6.2. Wired Equivalent Privacy (WEP) | 27 |
| 6.3. Pemfilteran MAC Address | 28 |
| 7. Ancaman Jaringan Nirkabel | 28 |
| 7.1. Sniffing dan Eavesdrop | 28 |
| 7.2. Brute Force Attack | 28 |
| 7.3. Man-in-the-middle Attack | 29 |
| 7.4. Denial of Service Attack | 29 |
| 7.5. Packet Injection | 29 |

| | |
|--|-----------|
| BAB III RANCANGAN DAN KONFIGURASI | 30 |
| 1. Objek Penelitian | 30 |
| 2. Alat Penelitian | 31 |
| 2.1. Infrastruktur Komputer | 31 |
| 2.1.1. Komputer Penyerang (hacker) | 31 |
| 2.1.2. Komputer Client (target) | 32 |
| 2.2. Infrastruktur Jaringan | 32 |
| 2.3. Infrastruktur Perangkat Lunak | 33 |
| 2.3.1. Sistem Operasi | 33 |
| 2.3.2. Madwifi Driver | 34 |
| 2.3.3. Wireless Tools | 34 |
| 2.3.4. Kismet | 35 |
| 2.3.5. Aircrack-ng | 35 |
| 2.3.6. Aircrack-ptw | 36 |
| 3. Langkah-langkah Penelitian | 36 |
| 3.1. Access Point (AP) Target | 36 |
| 3.2. Komputer Client Target | 39 |
| 3.3. Komputer Penyerang (Hacker) | 42 |
| 3.3.1. Madwifi Driver | 44 |
| 3.3.2. Kismet | 45 |
| 3.3.3. Airodump-ng | 48 |
| 3.4. Langkah-Langkah Pengujian | 51 |

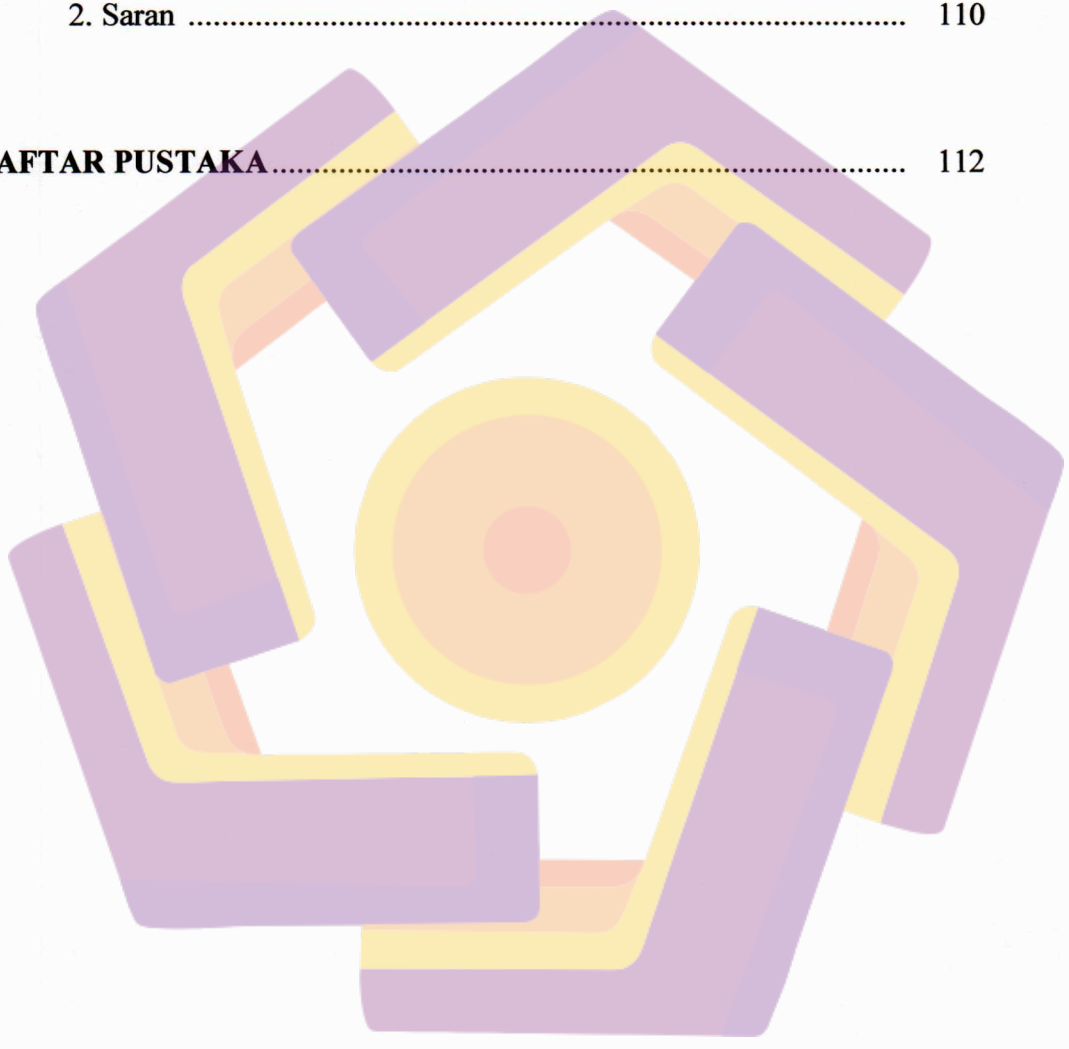
| | |
|--|-----------|
| BAB IV HASIL PENGUJIAN DAN PEMBAHASAN | 54 |
| 1. Cracking WEP Keys | 54 |
| 1.1. Footprinting | 59 |
| 1.2. Sniffing Packet | 63 |
| 1.3. Packet Injection | 65 |
| 1.4. Crack WEP Keys | 72 |
| 2. Cracking WPA Keys | 78 |
| 2.1. Analisa Paket WPA (koneksi yang sukses) | 81 |
| 2.2. Analisa Paket WPA (koneksi dengan passphrase salah) ... | 92 |
| 2.3. Footprinting | 96 |
| 2.4. Sniffing Paket Handshake | 97 |
| 2.5. Deauthentication | 99 |
| 2.6. Crack WPA-PSK | 102 |
| 3. Solusi Keamanan Jaringan Nirkabel | 103 |
| 3.1. Mengaktifkan enkripsi WPA-PSK dengan password rumit | 104 |
| 3.2. Filtering MAC Address | 105 |
| 3.3. Matikan Broadcast SSID | 105 |
| 3.4. Berikan Alamat IP statis pada perangkat nirkabel | 105 |
| 3.5. Menjalankan Fungsi Logging | 106 |
| 3.6. Meletakkan Access Point pada lokasi yang aman | 106 |
| 3.7. Matikan jaringan nirkabel yang tidak digunakan | 107 |
| 3.8. Captive Portal | 107 |

BAB V KESIMPULAN DAN SARAN 108

 1. Kesimpulan 108

 2. Saran 110

DAFTAR PUSTAKA 112

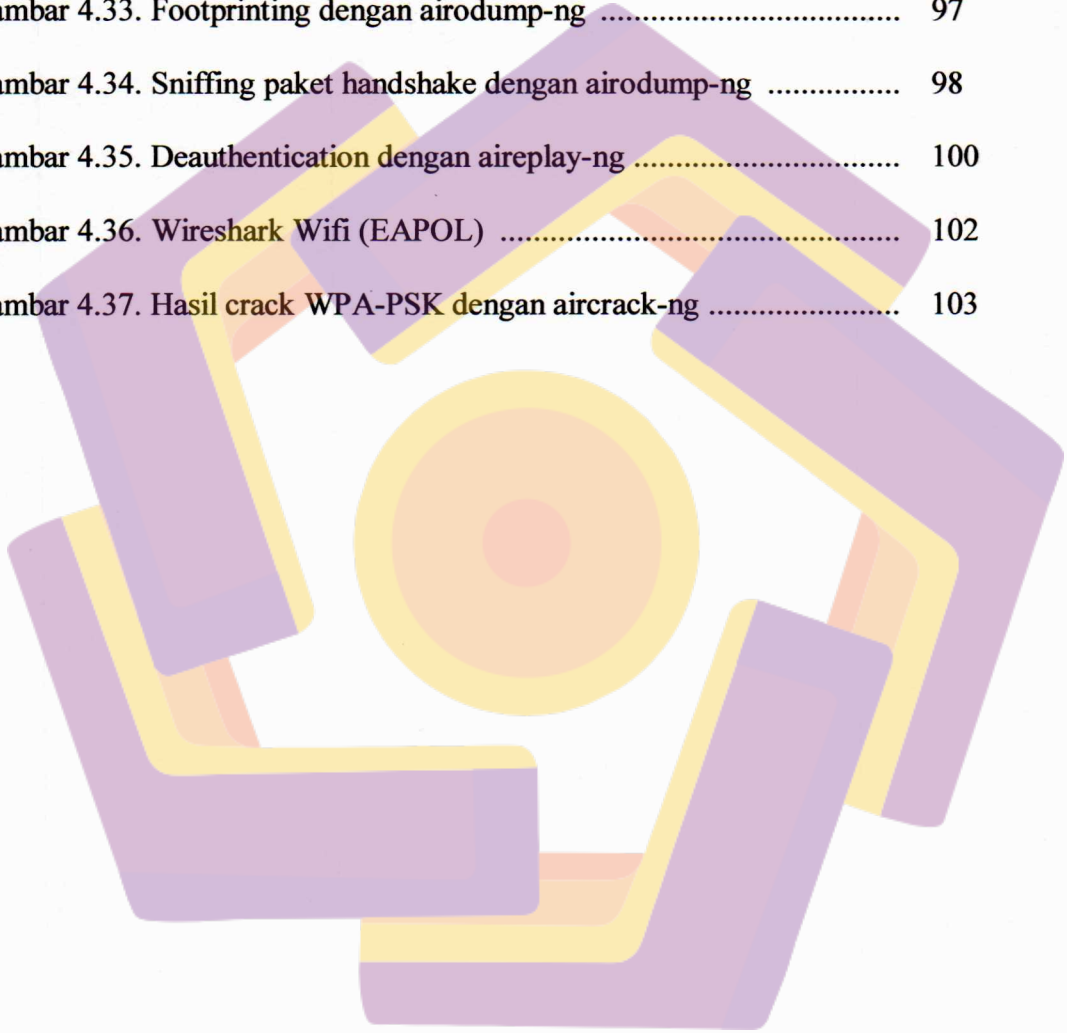


DAFTAR GAMBAR

| | |
|---|----|
| Gambar 2.1. Jaringan Ad Hoc | 12 |
| Gambar 2.2. Jaringan Infrastruktur | 13 |
| Gambar 2.3. Enkripsi WEP | 22 |
| Gambar 2.4. Komponen WPA | 23 |
| Gambar 3.1. Login ke AP | 37 |
| Gambar 3.2. Masuk ke dalam menu AP | 37 |
| Gambar 3.3. Setting Administrator | 38 |
| Gambar 3.4. Konfigurasi AP | 38 |
| Gambar 3.5. Konfigurasi server DHCP | 39 |
| Gambar 3.6. Melihat jaringan nirkabel yang terdeteksi | 40 |
| Gambar 3.7. Setting Wireless Network pada client | 41 |
| Gambar 3.8. Setting DHCP client | 42 |
| Gambar 3.9. Tampilan awal Backtrack | 44 |
| Gambar 3.10. Kismet | 46 |
| Gambar 3.11. iwconfig | 49 |
| Gambar 3.12. airodump-ng | 50 |
| Gambar 4.1. Setting keamanan WEP-64 bit | 59 |
| Gambar 4.2. Footprinting dengan airodump-ng | 62 |
| Gambar 4.3. Sniffing paket dengan airodump-ng | 64 |
| Gambar 4.4. Packet injection dengan aireplay-ng | 67 |
| Gambar 4.5. Deauthentication dengan aireplay-ng | 69 |

| | |
|--|----|
| Gambar 4.6. Paket deauthentication | 70 |
| Gambar 4.7. Paket ARP | 72 |
| Gambar 4.8. Cracking WEP-64bit dengan aircrack-ng (Percobaan 1) | 73 |
| Gambar 4.9. Cracking WEP-64bit dengan aircrack-ptw (Percobaan 1) ... | 74 |
| Gambar 4.10. Cracking WEP-64bit dengan aircrack-ng (Percobaan 2) .. | 75 |
| Gambar 4.11. Cracking WEP-64bit dengan aircrack-ptw (Percobaan 2) . | 75 |
| Gambar 4.12. Setting keamanan WEP-128 bit | 76 |
| Gambar 4.13. Cracking WEP-128 bit dengan aircrack-ng | 77 |
| Gambar 4.14. Cracking WEP-128 bit dengan aircrack-ptw | 77 |
| Gambar 4.15. Setting Keamanan WPA-PSK | 80 |
| Gambar 4.16. Beacon | 82 |
| Gambar 4.17. Probe Response | 83 |
| Gambar 4.18. Authentication Request | 84 |
| Gambar 4.19. Authentication Acceptance | 85 |
| Gambar 4.20. Association Request | 86 |
| Gambar 4.21. Association Response | 86 |
| Gambar 4.22. EAPOL Key 1 | 88 |
| Gambar 4.23. EAPOL Key 2 | 89 |
| Gambar 4.24. EAPOL Key 3 | 89 |
| Gambar 4.25. EAPOL Key 4 | 90 |
| Gambar 4.26. Paket Data 1 | 91 |
| Gambar 4.27. Paket Data 2 | 91 |
| Gambar 4.28. EAPOL key 1 | 93 |

| | |
|--|-----|
| Gambar 4.29. EAPOL key 2 | 93 |
| Gambar 4.30. EAPOL key 5 | 94 |
| Gambar 4.31. EAPOL key 6 | 95 |
| Gambar 4.32. Deauthentication dari AP | 96 |
| Gambar 4.33. Footprinting dengan airodump-ng | 97 |
| Gambar 4.34. Sniffing paket handshake dengan airodump-ng | 98 |
| Gambar 4.35. Deauthentication dengan aireplay-ng | 100 |
| Gambar 4.36. Wireshark Wifi (EAPOL) | 102 |
| Gambar 4.37. Hasil crack WPA-PSK dengan aircrack-ng | 103 |



DAFTAR TABEL

| | |
|---|----|
| Tabel 1-1. Rencana Kegiatan Penelitian | 9 |
| Tabel 2-1. Spesifikasi 3 Standard 802.11 | 16 |
| Tabel 3-1. Spesifikasi komputer penyerang (<i>hacker</i>) | 31 |
| Tabel 3-2. Spesifikasi komputer <i>client</i> target | 32 |
| Tabel 4-1. Chipertext “a” | 55 |
| Tabel 4-2. Chipertext “b” | 56 |
| Tabel 4-3. XOR Chipertext “a” dan “b” | 56 |
| Tabel 4-4. XOR Plaintext “a” dan “b” | 56 |
| Tabel 4-5. Hasil cracking pada keamanan WEP 64-bit (Percobaan 1) | 74 |
| Tabel 4-6. Hasil cracking pada keamanan WEP 64-bit (Percobaan 2) | 75 |
| Tabel 4-7. Hasil cracking pada keamanan WEP 128-bit | 77 |