SKRIPSI

MENDETEKSI *COVERT CHANNEL ATTACK* DALAM *ROGUE ACCESS POINT*

Disusun dan diajukan oleh:

AL AZHAR DP
D121 17 1525

PROGRAM STUDI SARJANA TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS HASANUDDIN
GOWA
2024

LEMBAR PENGESAHAN SKRIPSI

MENDETEKSI *COVERT CHANNEL ATTACK* DALAM *ROGUE ACCESS POINT*

Disusun dan diajukan oleh

AL AZHAR DP
D121 17 1525

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Program Studi Teknik Informatika
Fakultas Teknik Universitas Hasanuddin
Pada tanggal 15 Agustus 2024
dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama,

Dr-Eng. Ady Wahyudi Paundu, S.T., M.T
NIP. 19750313 200912 1 003

Pembimbing Pendamping,

Adnan, S.T, M. T, Ph. D
NIP. 19740426 200501 1 002

Ketua Program Studi,

Prof. Dr. Ir. Indrabayu, ST, MT, M. Bus. Sys., IPM, ASEAN. Eng
NIP. 19750716 200212 1 004

PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini ;

Nama	:	Al Azhar DP
NIM	:	D121171525
Program Studi	:	Teknik Informatika
Jenjang	:	S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul

MENDETEKSI *COVERT CHANNEL ATTACK* DALAM *ROGUE ACCESS POINT*

Adalah karya tulisan saya sendiri dan bukan merupakan pengambilan alihan tulisan orang lain dan bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri.

Semua informasi yang ditulis dalam skripsi yang berasal dari penulis lain telah diberi penghargaan, yakni dengan mengutip sumber dan tahun penerbitannya. Oleh karena itu semua tulisan dalam skripsi ini sepenuhnya menjadi tanggung jawab penulis. Apabila ada pihak manapun yang merasa ada kesamaan judul dan atau hasil temuan dalam skripsi ini, maka penulis siap untuk diklarifikasi dan mempertanggungjawabkan segala resiko.

Segala data dan informasi yang diperoleh selama proses pembuatan skripsi, yang akan dipublikasi oleh Penulis di masa depan harus mendapat persetujuan dari Dosen Pembimbing.

Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan isi skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Gowa, 15 Agustus 2024

Yang Menyatakan

AL AZHAR DP

NIM. D121 17 1525

ABSTRAK

AL AZHAR DP *Mendeteksi Covert Channel Attack Dalam Rogue access point* (dibimbing oleh Ady Wahyudi Paundu dan Adnan)

Access Point semakin ramai digunakan dan hampir ditemukan di setiap tempat ramai karena menyediakan konektivitas terhadap internet, akan tetapi terdapat masalah keamanan yang dapat menjadi hal serius jika tidak berhati-hati yaitu *Rogue Access Point* yang dapat mengambil data penting dari pengguna yang terhubung.

Penelitian ini memiliki tujuan membangun sebuah sistem pendeteksi *covert channel* dalam RAP. Sistem ini diharapan mampu mendeteksi *covert channel* dalam RAP yang terhubung dengan AP yang telah terlegimitasi keberadaannya. Sistem akan membaca lalulintas data yang menggunakan AP tersebut, apabila ditemukan *covert message* maka server analisis akan menampilkan *covert message* tersebut.

Sistem pendeteksian *covert channel* pada penelitian ini dibangun menggunakan Virtualbox agar dapat membuat *virtual machine*. Menginstal program server analisis pada salah satu *virtual machine* dan satu *virtual machine* lagi untuk pembuatan RAP, tools yang digunakan untuk membuat RAP adalah Hostapd dan *interface* yang digunakan adalah wifi adapter Atheros AR9271. RAP yang telah dibuat akan disimulasikan untuk mengirimkan *covert message* kepada penyerang yang berisi informasi dari pengguna yang terhubung, kemudian server analisis yang telah dibuat akan membaca *covert data* dari RAP yang dikirimkan kepada penyerang.

Hasil penelitian ini menunjukkan sistem pendeteksi *covert channel* berhasil mendeteksi *covert data* yang berada dalam RAP, server analisis berhasil membaca *covert message* dari RAP melalui AP yang terhubung.

Kata Kunci: AP, RAP, Covert Channel

ABSTRACT

AL AZHAR DP. *Datecting Covert Channel Attack in Rogue Access Points* (supervised by Ady Wahyudi Paundu and Adnan)

Access Points are increasingly widely used and are found in almost every crowded place because they provide connectivity to the internet, but there are security issues that can be serious if not careful, namely Rogue Access Points that can take important data from connected users.

This research aims to build a covert channel detection system in RAP. This system is expected to be able to detect covert channels in RAP that are connected to AP that have been legitimated. The system will read the data traffic that uses the AP, if a covert message is found, the analysis server will display the covert message.

The covert channel detection system in this study was built using Virtualbox to create a virtual machine. Install the analysis server program on one of the virtual machines and another virtual machine for creating RAP, the tools used to create RAP are Hostapd and the interface used is the Atheros AR9271 wifi adapter. The RAP that has been created will be simulated to send a covert message to the attacker containing information from the connected user, then the analysis server that has been created will read the covert data from the RAP sent to the attacker.

The results of this study indicate that the covert channel detection system successfully detected covert data in the RAP, the analysis server successfully read the covert message from the RAP via the connected AP.

Keywords: AP, RAP, Covert Channel

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR SINGKATAN DAN ARTI SIMBOL

Lambang/Singkatan	Arti dan Keterangan
WLAN	*Wireless Local Area Network*
RAP	*Rogue access point*
AP	*Access Point*
MITM	*Man In The Middle*
WPA-PSK	*Wi-Fi Protected Access Pre-Shared Key*
WEP	*Wired Equivalent Privacy*
RTT	*Round Trip Time*
IEEE	*Institute of Electrical and Electronic Engineers*
EAP	*Extensible Authentication Protocol*
RADIUS	*Remote Authentication Dial-In User Service*
MIMO	*Multiple Input Multiple Output*
REPL	*Read Evaluate Print Loop*
OS	*Operating System*

DAFTAR LAMPIRAN

KATA PENGANTAR

Assalamu'Alaikum Warahmatullahi Wabarakatuh.
Alhamdulillah, puji dan syukur kita panjatkan kepada Allah Subhanahu Wata'ala, tidak ada sembahan yang benar dan berhak untuk disembah kecuali hanya Ia semata., yang telah memberikan rahmat dan karunia-Nya kepada penulis untuk menyelesaikan tugas akhir dengan judul "Mendeteksi *Covert Channel Attack* dalam *Rogue Access Point*".

Dalam penyusunan penelitian ini, penulis menyajikan hasil penelitian terkait dengan judul yang telah diangkat dan telah melalui proses pencarian dari berbagai sumber baik itu jurnal penelitian, prosiding pada seminar internasional, buku, maupun situs-situs dari internet.

Shalawat dan salam kepada Rasulullah Shallallahu Alaihi Wasallam yang senantiasa menjadi sumber inspirasi dan teladan terbaik untuk umat manusia. Skripsi ini tidak lepas dari bantuan dan dukungan dari berbagai pihak yang telah ikhlas membantu penulis dalam melakukan penelitian dan penyusunan skripsinya sebagai syarat untuk memperoleh gelar Sarjanah (S1). Oleh karena itu, sudah sepantasnya penulis dengan penuh hormat mengucapkan terimakasih yang sebesar-besarnya kepada :

1. Allah Subhanahu wata'ala, atas segala rahmat, karunia, dan bantuan-Nya yang diberikan kepada penulis hingga saat ini.
2. Kedua orang tua penulis, Bapak Deppungeng dan Ibu Saddiah, yang selalu memberikan dukungan, doa, dan semangat kepada penulis yang masih berlangsung hingga saat ini.
3. Bapak Dr. Eng. Ady Wahyudi Paundu, S.T., M.T., dan Bapak Adnan, S.T, M. T, Ph. D., selaku pembimbing yang senantiasa menyediakan waktu, tenaga, pikiran, dan perhatian yang luar biasa dalam mengarahkan penulis dalam menyelesaikan tugas akhir ini dengan sabar.
4. Bapak Prof. Dr. Ir. Indrabayu, S.T., M.T., M.Bus.Sys., IPM, Asean. Eng., selaku Ketua Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin atas segala bimbingan, motivasi, dan dukungan selama masa perkuliahan.
5. Segenap Dosen dan Staf Deparetmen Teknik Informatika, Fakultas Teknik Universitas Hasanuddin, yang telah banyak memberikan ilmu, pengalaman, serta bantuan kepada penulis selama menuntut ilmu di kampus Universitas Hasanuddin ini.
6. Sahabat-sahabat penulis, Saphira Noer S., Nurina Rahayu, Herlina Anwar, Devy Noviani, Irma Jufri, Bishram, Andar Sugianto, Achmad Asjar, Wahyudi Sumara, Wahyu Faisal dan Abduh yang selalu mendukung dan membantu penulis selama proses pengerjaan tugas akhir ini, serta menghibur penulis agar tetap semangat dalam menyelesaikan tugas akhir ini.

7. Teman-teman, senior, maupun junior departemen informatika, terkhusus angkatan 2017 yang selalu mendukung dan memberi semangat kepada penulis.
8. Seluruh pihak yang tidak sempat disebutkan satu per satu, atas segala dukungan dan bantuan dalam menyelesaikan tugas akhir ini.

Akhir kata penulis menyadari masih terdapat kekurangan dalam penyusunan laporan tugas akhir ini baik dari segi isi maupun penyajiannya. Oleh karena itu, penulis meminta maaf sedalam-dalamnya atas kekurangan tersebut dan mengharapkan adanya saran serta masukan yang membangun kesempuranaan laporan ini. Penulis berharap semoga tugas akhir ini dapat bermanfaat bagi para pembaca dan dapat dijadikan sebagai referensi demi pengembangan ke arah yang lebih baik. Kebenaran datangnya dari Allah dan kesalahan datangnya dari diri penulis sendiri. Semoga Allah SWT senantiasa melimpakhan rahmat dan ridho-Nya kepada kita semua. Amin.

Wassalamu’alaikum Warahmatullahi Wabarakatuh

Makassar,2 Agustus 2024

Penulis
Al Azhar DP

BAB I
PENDAHULUAN

1.1 Latar Belakang

Wireless Local Area Networks (WLAN) semakin terintegrasi ke dalam kehidupan kita sehari-hari, di mana Access Points (AP) merupakan bagian integral dari infrastruktur WLAN, karena AP bertanggung jawab untuk mengoordinasikan pengguna nirkabel dan menghubungkan mereka ke jaringan berkabel dan akhirnya ke Internet. AP ditempatkan di mana-mana, mulai dari bandara hingga kafe dan rumah sakit, untuk menyediakan konektivitas Internet. Salah satu masalah keamanan paling serius yang dihadapi oleh pengguna WLAN adalah keberadaan *Rogue access point*s (RAP). Beberapa kategori dari RAP adalah *Evil-twin, Unauthorized, Compromised, dan Improperly Configured RAPs. Evil-twin* menggunakan AP berbasis perangkat lunak yang diinstal pada perangkat portabel. Dengan demikian, perangkat portabel dengan *external card* dan *tool* seperti *airbase-ng* sudah cukup untuk mengatur jenis RAP ini, *Unauthorized* merupakan RAP yang dipasang oleh karyawan atau pengguna tanpa izin administrator jaringan. *Compromised* adalah AP yang telah dimasuki oleh pengguna jahat yang memiliki *shared key* dari AP tersebut, dan *Improperly Configured RAPs* adalah AP yang tidak dikonfigurasikan dengan benar (Utama et al., 2020).

Internet pada jaringan Wifi banyak diminati masyarakat sebagai sarana untuk melakukan berbagai macam aktivitas seperti, bisnis, transaksi jual beli, aktivitas pembayaran dan berbagai macam hal lain, namun tanpa disadari hal ini amat beresiko bagi penggunanya, telah terjadi banyak kasus pencurian data melalui jaringan WLAN dimana para pelaku melakukan tindak kejahatan seperti membuat RAP untuk memantau lalu lintas data pada jaringan tersebut, kemudian menggunakan teknik serangan *Man In The Middle* (MITM) pada jaringan kemudian menggali data maupun informasi penting milik pengguna jaringan. Berdasarkan dalam ilmu kriptografi dan keamanan PC serangan MITM adalah serangan di mana penyerang diam-diam mentransfer dan mungkin mengubah korespondensi antara dua pihak yang meyakini bahwa mereka sedang berkomunikasi secara langsung satu sama lain (Mallik, 2018).

Terdapat berbagai solusi yang ditawarkan untuk mendeteksi RAP pada sebuah jaringan. Solusi tersebut diklasifikasikan menjadi tiga jenis pendekatan berdasarkan letak di mana metode diaplikasikan yaitu *server-side, client-side,* dan *hybrid*. Pada pendekatan *client-side* terdapat dua jenis metode yang dapat diaplikasikan yaitu *Round Trip Time* (RTT), *Received Signal Strength and Sequence Hypothesis Method*. Kemudian, pendekatan *server-side* dibagi menjadi empat jenis metode yang terdiri dari *Temporal Characteristic*, *Hidden Markov Model, ClockSkew*, dan *Hybrid Framework.* Sedangkan untuk pendekatan *hybrid* terdiri dari dua jenis metode yaitu *Covert channel* dan *Multi-agent Sourcing*. Pada *Covert channel* proses deteksi akan dilakukan dengan mencocokan *authentication string* yang dikirimkan oleh AP pada perangkat pada pengguna. Ketika terdapat

kecocokan, maka perangkat akan terhubung dengan AP yang bersangkutan. Namun, ketika AP yang dimaksud tidak memiliki kecocokan, maka koneksi akan segera diputus (Anmulwar et al., 2015).

Covert channel dapat dibedakan menjadi dua jenis yaitu: timing channels dan storage channels. Storage *Covert channel* biasanya dibuat dengan mengubah header fields atau memanfaatkan padding fields yang tersedia pada protokol jaringan yang digunakan. Sedangkan Timming *Covert channel* memiliki metode yang lebih rumit dariapada Storage *Covert channel*. Secara umum, mereka mengeksploitasi parameter yang berbeda dari timming relations selama transmisi data. *Covert data* ditransmisikan dengan memilih backoff time value yang tepat, biasanya digunakan untuk mengaktifkan Collision Avoidance dalam kontrol media akses (Sawicki et al., 2021). Dalam artikel (Bodhe et al., 2020) menggunakan *fuzzy logic tool* untuk menemukan RAP yang ada disekitar. Terdapat perbandingan hasil analisis dari beberapa metode dalam mendeteksi RAP yang telah ada dengan metode *fuzzy logic tool.* Sayangnya tidak ditemukan nilai perbandingan untuk metode *Covert channel* dalam tabel perbandingannya dengan catatan keterbatasan dalam pemasangan *Covert channel*. Maka dari itu, penulis mengusulkan judul "Mendeteksi *Covert Channel Attack* dalam *Rogue Access Point*" untuk mencoba membuat sebuah sistem yang dapat mendeteksi *Covert Channel* dalam RAP. Diharapkan penelitian ini dapat memberikan sebuah sistem pendeteksi *Covert Channel* pada RAP.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan pada poin sebelumnya, maka rumusan masalah pada penelitian adalah bagaimana cara membangun sistem pendeteksi *Covert Channel* yang terdapat pada RAP?

1.3 Tujuan Penelitian

Tujuan akhir dari penelitian ini yakni membangun sistem pendeteksi *Covert Channel* yang terdapat pada RAP.

1.4 Manfaat Penelitian

Manfaat yang akan didapatkan pada penelitian ini yaitu memperoleh sistem yang dapat mendeteksi *Covert channel* dalam RAP. Penulis mengharapkan agar penelitian ini dapat menjadi referensi bagi penelitian-penelitian lain dengan tema *Rogue access point* dan *Covert channel*.

1.5 Ruang Lingkup

Berdasarkan beberapa hal yang dicantumkan pada rumusan masalah, maka ruang lingkup dari penelitian ini yakni :

1. RAP yang digunakan terhubung dengan AP yang sah.
2. laptop yang dapat mengoperasikan VirtualBox.
3. Wireless adapter dengan chip Atheros 9k sebagai *interface* RAP dan *tools Hostapd* untuk pembuatan RAP.
4. Menggunakan VirtualBox untuk membuat beberapa *Guest OS*

BAB II
TINJAUAN PUSTAKA

2.1 *Rogue access point*

Rogue access point (RAP) adalah sebuah Accesss Point (AP) yang terhubung ke perangkat nirkabel yang diatur pada jaringan yang aman dan terlindungi tanpa memiliki izin dari admin jaringan, ini dapat dipasangkan oleh pekerja itu sendiri atau seorang yang memiliki niat untuk menyerang. Apabila penyerang atau pekerja tersebut memasang AP pada jaringan yang aman, mereka dapat dengan mudah mengeksekusi berbagai macam pemindaian kerentanan terhadap jaringan yang aman tersebut tanpa harus secara fisik berada di dekat sumber jaringan, mereka dapat menyerang dari jarak jauh pada jaringan nirkabel(Bodhe et al., 2020). Perangkat yang beroperasi sebagai RAP diatur sedemikian rupa sehingga perangkat pengguna tidak dapat membedakan antara AP yang aman dan RAP. Akibatnya, perangkat klien akan terhubung ke RAP yang dapat menangkap data data yang dikirim oleh pengguna seperti password dan nomor kartu kredit (Sawicki & Piotrowski, 2012).

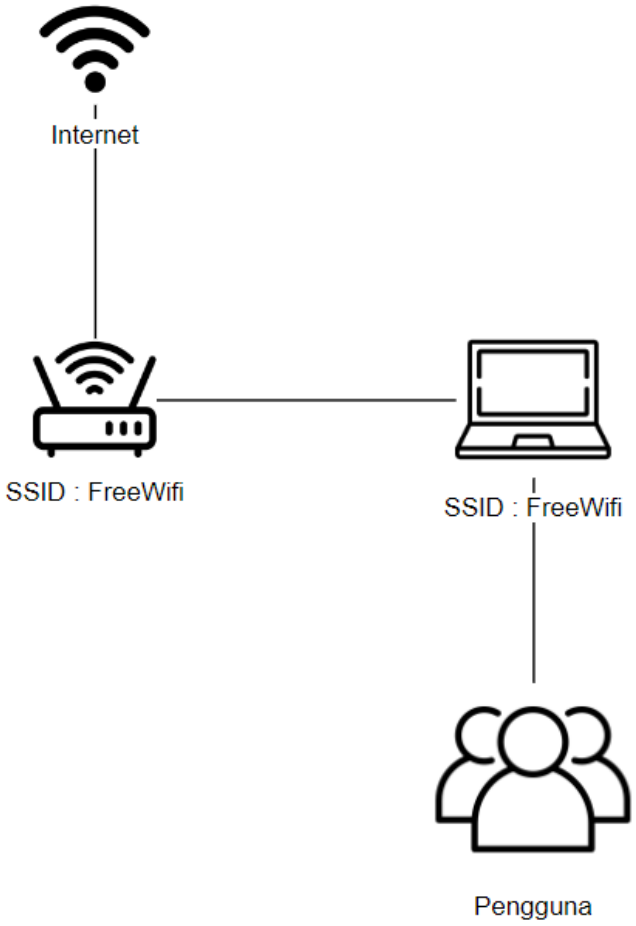
RAP diklasifikasikan kedalam empat kategori yaitu : *Evil-Twin, Improperly Configured, Unauthorized,* dan *Compromised*(Alotaibi & Elleithy, 2016).

2.1.1 *Evil-twin*

Evil-twin AP menggunakan AP berbasis perangkat lunak yang diinstal pada perangkat portabel. Oleh karena itu, perangkat portabel dengan *wireless card* eksternal dan alat seperti *airbase-ng* (sebuah *tool* untuk menyerang pengguna dan AP) sudah cukup untuk menyiapkan RAP jenis ini. Terdapat dua *identifier* dalam standar IEEE 802.11 yang dapat mengotentikasi AP ke pengguna, yaitu SSID dan MAC *address*(BSSID) dari AP tersebut. Karena *identifier* ini dapat dengan mudah ditipu, AP dapat dibuat-buat oleh orang luar dan tidak dapat dibedakan bagi pengguna nirkabel. AP *evil-twin* memiliki dua bentuk :

1. *Coexistence* : AP yang sah berdampingan dengan *Evil-twin* dalam lokasi yang sama. *Evil-twin* membajak SSID dan MAC *address* dari AP yang sah dan meningkatkan kekuatan sinyalnya agar memaksa pengguna untuk terhubung, kemudian meneruskan paket data melalui AP yang sah.

2. *Replacement* : *Evil-twin* akan mematikan AP yang sah kemudian menggantikannya. Jenis RAP ini memiliki koneksi internet tersendiri.



Gambar 1 *Evil-twin* RAP

2.1.2 *Improperly Configured*

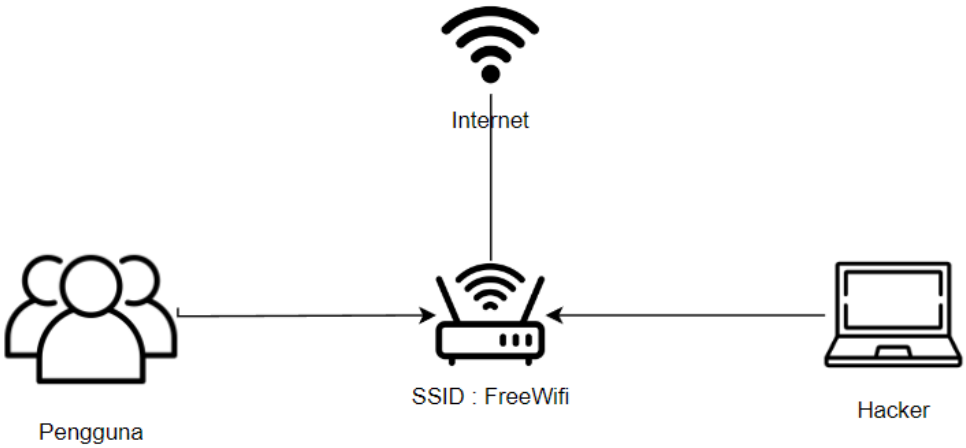
Jenis RAP ini tidak ditempatkan oleh individu berbahaya, RAP ada di WLAN karena AP tidak dikonfigurasi dengan benar. Ada banyak situasi di mana AP dapat salah dikonfigurasi. Administrator yang tidak memiliki latar belakang keamanan yang memadai mungkin memilih pengaturan autentikasi atau enkripsi yang tidak cukup kuat. Contoh lain terjadi ketika driver AP tidak berfungsi atau seluruh perangkat lunak rusak. Selain itu, AP mungkin menjadi rentan setelah pembaruan perangkat lunak (misalnya, firmware dengan enkripsi yang diaktifkan menggunakan WPA-PSK atau WEP mungkin menyebabkan AP dilanjutkan tanpa enkripsi). Hal ini dapat membuka *backdoor* untuk melewati autentikasi, sehingga memungkinkan pengguna yang tidak sah untuk berbagi sumber daya jaringan. Ini adalah RAP berbasis perangkat keras yang dicolokkan ke switch atau router, dan tidak ada niat jahat di balik keberadaannya.

2.1.3 *Unauthorized*

Jenis RAP ini diinstal oleh karyawan atau pengguna naif tanpa izin administrator jaringan. Meskipun, AP ini tidak dipasang oleh administrator jaringan, namun dianggap sebagai bagian dari WLAN karena terhubung melalui kabel sama seperti AP yang sah. Dengan demikian, AP yang tidak sah menerima dan mengirimkan data secara nirkabel dari pengguna nirkabel ke sisi jaringan kabel begitupun sebaliknya. RAP ini dapat diatur untuk tujuan kenyamanan, terutama di organisasi besar, untuk memungkinkan karyawan mendapatkan akses ke sumber daya jaringan. AP yang tidak sah juga dapat diatur untuk tujuan yang jahat seperti menciptakan kerentanan dalam keamanan organisasi, sehingga memungkinkan pihak luar untuk mengeksploitasi kelemahan ini. Dengan demikian, pengguna tidak sah yang menggunakan RAP ini berbagi media dengan pengguna yang berwenang, menguping lalu lintas pengguna yang berwenang, dan melancarkan serangan terhadap sumber daya jaringan. Ini adalah RAP berbasis perangkat keras lainnya.

2.1.4 *Compromised*

Metode keamanan seperti WPA-PSK dan WEP menggunakan *shared keys* untuk mengamankan komunikasi antara AP dan pengguna nirkabel. Jika pengguna nakal mendapatkan *shared keys* yang digunakan oleh AP maka AP itu akan berubah menjadi RAP, sehingga memungkinkan peretas melancarkan serangan dan mendapatkan akses ke informasi sensitif. Peretas dapat menggunakan perangkat lunak sederhana menggunakan sistem operasi berbasis Linux seperti BackTrack atau Kali menyediakan banyak alat bagi peretas untuk memecahkan *shared keys*, seperti *Aircrack-ng*.



Gambar 2 *Compromised* RAP

2.2 *Covert channel*

Covert channel mengacu pada transmisi informasi secara rahasia (yaitu tidak terlihat oleh *end user*s) melalui saluran komunikasi yang tidak dimaksudkan untuk komunikasi dan melanggar kebijakan keamanan. *Covert channel* tidak hanya digunakan oleh peretas untuk mengirimkan dan mencuri informasi tetapi juga digunakan oleh pihak tepercaya untuk membagikan *secret keys*. Selain itu, ini juga digunakan untuk otentikasi jaringan, perlindungan hak cipta, dan bukti *cybercrimes*. Hal ini juga menambah banyak tantangan keamanan karena peretas mencari pendekatan yang lebih kuat untuk menyembunyikan keberadaan *Covert channel*. Terlebih lagi, ia menggunakan sebagian besar saluran bandwidth untuk mengirimkan informasi dalam jumlah kecil sekalipun. *Covert channel* berbeda dengan kriptografi karena tujuan utamanya adalah untuk menyembunyikan keberadaan transmisi sedangkan kriptografi tidak menyembunyikan keberadaan pesan tetapi mengubahnya sedemikian rupa sehingga tidak dalam bentuk yang dapat dibaca. Selain itu, bentuk *Covert channel* sebelumnya adalah steganografi yang digunakan untuk menyembunyikan keberadaan pesan dalam file teks atau multimedia berukuran besar. *Covert channel* diklasifikasikan menjadi dua kategori besar yaitu *network timing Covert channel* dan *storage covert chanel*(Goher et al., 2012).

2.2.1 *Timing Covert channel*

Timing Covert channel berfokus pada penyampaian pesan melalui pola kedatangan paket daripada isi pesan. Selain itu, *timing Covert channel* tidak menggunakan *packet header* atau muatan untuk *encode covert messages*. *Timing covert chanel* dibagi menjadi dua *channels*: *packet sorting channels* dan *timing channels* dimana informasi disampaikan berdasarkan urutan kedatangan paket dalam saluran penyortiran paket. Di sisi lain informasi melalui saluran waktu disampaikan oleh ada atau tidaknya paket dalam interval waktu tertentu(Cabuk et al., 2004).

2.2.2 *Storage Covert channel*

Dalam *storage Covert channel*, salah satu proses secara langsung atau tidak langsung *writes* ke lokasi penyimpanan tertentu sedangkan proses lainnya *reads* dari lokasi penyimpanan tertentu. Sejumlah alat menggunakan protokol TCP, IP, ICMP, dan HTTP untuk membangun saluran penyimpanan rahasia. Dalam protokol ini, bidang yang tidak digunakan digunakan untuk mengirimkan informasi karena bidang ini umumnya tidak terdeteksi oleh *intrusion detection system* dan *firewall*.

2.3 *Hostapd*

*Host*apd adalah *user space daemon* untuk AP dan server otentikasi di WLAN. Ini mengimplementasikan fungsi manajemen AP, otentikasi dan enkripsi

IEEE802.11. Bagian keamanan mencakup Otentikator IEEE802.1X/WPA/WPA2/EAP, klien RADIUS, server EAP, dan server otentikasi RADIUS. Selain itu, *host*apd mengimplementasikan sekelompok antarmuka pemrograman untuk *console* dan *graphic applicaiton*. Antarmuka ini dapat dieksplorasi oleh programmer lain untuk membangun aplikasi dengan antarmuka pengguna yang ramah(He & Guo, 2010).

2.4 Atheros AR9271

Atheros AR9271 adalah chipset jaringan nirkabel yang dikembangkan oleh Qualcomm Atheros, anak perusahaan Qualcomm Inc. Chipset ini biasa digunakan di berbagai perangkat nirkabel untuk menyediakan konektivitas Wi-Fi. Chipset AR9271 mendukung standar nirkabel 802.11b/g/n, memungkinkan perangkat terhubung ke jaringan WiFi dan mengakses internet. Ini beroperasi pada rentang frekuensi 2,4 GHz dan menawarkan fitur seperti teknologi MIMO (Multiple Input Multiple Output) untuk meningkatkan kekuatan sinyal dan keluaran data. Chipset ini sering ditemukan di adaptor USB Wi-Fi, router, dan perangkat lainnya, menjadikannya pilihan populer untuk menambahkan konektivitas nirkabel ke berbagai produk.

Gambar 3 Wifi Adapter Atheros AR9271

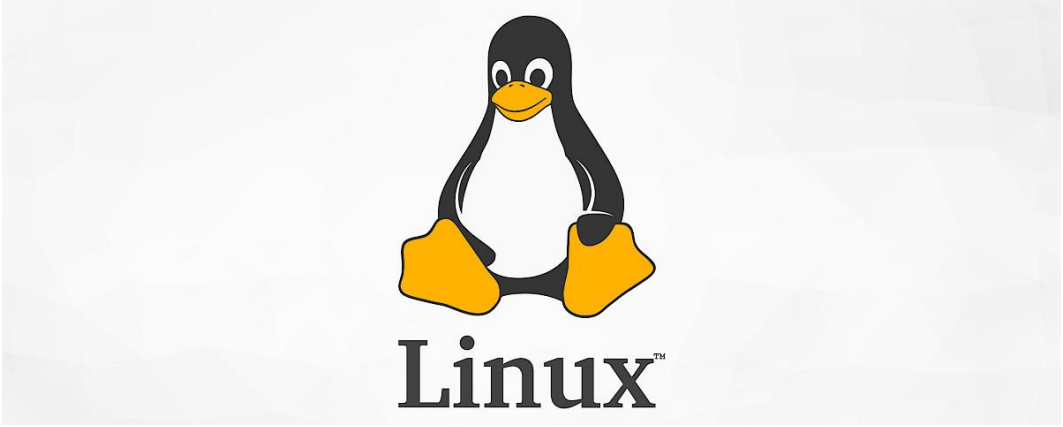
2.5 Scapy

Scapy adalah library paket interaktif yang ditulis dalam bahasa Python. Scapy mampu memalsukan atau mendekode paket dari sejumlah besar protokol, mengirimkannya melalui jaringan, menangkapnya, mencocokkan permintaan dan balasan, dan masih banyak lagi. Scapy dapat digunakan sebagai REPL atau sebagai library(Welcome to Scapy’s Documentation! — Scapy 2.6.0 Documentation, n.d.).

Gambar 4 Scapy Library

2.6 Linux

Sama seperti Windows, iOS, Mac OS, Linux juga merupakan sebuah sistem operasi yaitu perangkat lunak sistem yang mengatur sumber daya dari perangkat keras dan perangkat lunak, serta sebagai daemon untuk program komputer. Faktanya, salah satu platform paling populer di dunia saat ini, Android, didukung oleh sistem operasi linux. Sederhananya, sistem operasi mengelola komunikasi antara software dan hardware. Tanpa sistem operasi software tidak akan berfungsi sebagaimana mestinya (What Is Linux? - Linux.Com, n.d.).



Gambar 5 Linux OS

2.7 Python

Python adalah bahasa pemrograman tingkat tinggi dan serbaguna. Filosofi desainnya menekankan keterbacaan kode dengan penggunaan indentasi yang signifikan(Kuhlman, 2009). Python dibuat oleh Guido van Rossum dan pertamakali dirilis pada tahun 1991.

Gambar 6 Python Language

2.8 Nano

Nano adalah editor teks serbaguna yang utamanya digunakan untuk mengedit berkas secara langsung dari baris perintah sistem berbasis Unix. Antarmukanya yang mudah dipahami dan pintasan papan ketiknya menjadikannya alat yang praktis untuk tugas pengeditan teks cepat di lingkungan terminal.

Gambar 7 Nano Text Editor