ANALISIS PENYADAPAN TRANSMISI PAKET DATA JARINGAN KOMPUTER MENGGUNAKAN WIRESHARK (STUDI KASUS: UPT-IT UM-PALEMBANG)

SKRIPSI

Diajukan Sebagai Syarat ujian Skripsi Pada Program Studi Teknologi Informasi
Fakultas Teknik Universitas Muhammadiyah Palembang

Oleh:

ANGGI SAFITRI

162018083

PROGRAM STUDI TEKNOLOGI INFORMASI

FAKULTAS TEKNIK UNIVERSITAS MUHAMMADIYAH PALEMBANG

2022

HALAMAN PENGESAHAN

ANALISIS PENYADAPAN TRANSMISI PAKET DATA JARINGAN KOMPUTER MENGGUNAKAN WIRESHARK (STUDI KASUS : UPT-IT UM – PALEMBANG)

Oleh

ANGGI SAFITRI

162018083

Telah di terima sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom) pada program studi Teknologi Informasi

Pembimbing Utama	Pembimbing Pendamping
Apriansyah, S.Kom., M.Kom	**Dedi Haryanto, S.Kom., M.Kom**
NIDN/NBM : 0204049001/1339399	**NIDN/NBM : 0201089001/1337459**

Disetujui,

Dekan Fakultas Teknik,	Program Studi Teknologi Informasi, Ketua Program Studi,
Dr. Ir. Kgs. Ahmad Roni, M.T, IPM	**Karnadi, S.Kom., M.Kom**
NBM/NIDN : 763049/0227077004	**NBM/NIDN : 1088893/0210038202**

ii

HALAMAN PERSETUJUAN

Skripsi yang berjudul **"ANALISIS PENYADAPAN TRANSMISI PAKET DATA JARINGAN KOMPUTER MENGGUNAKAN WIRESHARK (STUDI KASUS: UPT-IT UM-PALEMBANG).** Oleh " Anggi Safitri" telah dipertahankan didepan komisi Penguji Pada hari Senin 08 Agustus 2022

Komisi Penguji

1. Apriansyah, S.Kom.,M.Kom (Ketua) (.....)
2. Dedi Haryanto, S.Kom.,M.Kom (Sekretaris) (.....)
3. Jimmie, S.Kom.,M.Kom (Anggota) (.....)
4. Meilyana Winda P, S.Kom.,M.Kom (Anggota) (.....)

Mengetahui,

Program Studi Teknologi Informasi

Ketua Program Studi,

Karnadi, S.Kom.,M.Kom
NBM/NIDN. 1088893/0210038202

HALAMAN PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama : Anggi Safitri

NIM : 162018083

Dengan ini menyatakan bahwa:

1. Karya tulis (Skripsi) yang saya buat ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik baik (Sarjana) di Universitas Muhammadiyah Palembang atau perguruan lain;
2. Karya tulis ini murni gagasan, rumusan, dan penilaian saya sendiri arahan dosen Pembimbing;
3. Karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dikutip dengan mencantumkan nama pengarang dan memasukan kedalam rujukan;
4. Saya Bersedia, Skripsi yang saya hasilkan dicek keasliannya menggunakan plagiarism checjer serta diunggah ke internet, sehingga dapat di akses publik secara daring;
5. Surat pernyataan ini saya tulis dengan sungguh-sungguh dan apabila terbukti melakukan penyimpangan atau ketidak benaran dalam pernyataan ini, maka saya bersedia menerima sanksi sesuai peraturan dan perundang-undangan yang berlaku.

Demikian surat pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, September 2022

Yang membuat pernyataan

Anggi Safitri

iv

MOTTO DAN PERSEMBAHAN

Motto:

"Jangan bersedih atas apa yang telah berlalu, kecuali itu bisa membuatmu bekerja lebih keras untuk apa yang akan datang," - Umar bin Khattab-

Persembahan:

Tidak bisa dipungkuri telah banyak yang membantu penulis selama menyelesaikan skripsi ini, maka dari itu izinkan penulis untuk mempersembahkan skripsi ini kepada orang-orang tersebut.

- *Kepada Bapak Agunawan dan Ibu Joti Yartika selaku orang tua saya yang selalu memberikan doa, kasih sayang, nasehat serta dukungan yang tiada henti baik moral maupun material.*
- *Kepada adik-adik saya Lendy dian varega, Dian ageisha putri, M. Afgan Tegar dan M. Arhan serta keluarga tercinta Kakek Asman Ali, Nenek Nunija, Nenek Atma dan seluruh keluarga besar yang selalu memberikan semangat*
- *Kepada Dosen Teknologi Informasi yang telah membimbing, Terutama dosen pembimbing saya Bapak Apriansyah, S.kom.,M.kom dan Bapak Dedi Haryanto, S.kom.,M.kom yang telah membantu dan memberikan kritik dan saran.*
- *Serta teman-temanku, Intan, deva, riska, ayundha, rita, oca, vera, erni, ice, dan bagas pramana putra yang telah memberikan semangat dan motivasi dalam mengerjakan skripsi.*

ABSTRAK

Dalam penelitian ini, penulis melakukan proses penyadapan *(sniffing)* untuk mendapatkan informasi seperti akses browser, username dan password, menggunakan perangkat lunak WireShark. Wireshark merupakan sebuah aplikasi analisis jaringan yang bisa melakukan proses capture data pada interface wireless, kemudian mengamati hasil capture-an yang berisikan data POST yang berisikan username dan password pada HTTP. Dalam penelitian ini menggunakan metode tindakan (action research). Keamanan jaringan yang ada pada ruang lingkup Universitas Muhammadiyah Palembang sudah bisa dikatakan aman karena disetiap ruangan dosen dan pegawai ada wifi yang sudah memiliki keamanan , akan tetapi ada beberapa wifi yang tidak memiliki keamanan yang bisa bebas dipakai oleh semua mahasiswa, sehingga bisa membahayakan user pada saat menggunakan wifi tersebut, karena masih banyak mahasiswa yang awam tentang keamanan jaringan. Melakukan penyadapan atau pengendusan data dan melakukan capture data secara langsung pada sebuah interface menggunakan wireshark, mampu menampilkan informasi yang sangat detail seperti alamat ip pengguna, perangkat pengguna dan juga username dan password serta informasi akses browser pada protokol http. Melakukan capture paket data menggunakan wireshark memudahkan administrator jaringan untuk melakukan monitoring jaringan.

Kata Kunci: Keamanan Informasi, *Sniffing*, *Wireshark,* Metode Penelitian

ABSTRACT

In this study, the authors carried out the process of tapping (sniffing) to obtain information such as browser access, username and password, using WireShark software. Wireshark is a network analysis application that can capture data on a wireless interface, then observe the results of the capture containing POST data containing the HTTP username and password. In this study using the method of action (action research). Network security that is within the scope of the Muhammadiyah University of Palembang can be said to be safe because in every room of lecturers and employees there is wifi that already has security, but there are some wifi that do not have security that can be freely used by all students, so that it can endanger the user at any time. use the wifi, because there are still many students who are unfamiliar with network security. Performing wiretapping or data sniffing and capturing data directly on an interface using wireshark, capable of displaying very detailed information such as the user's ip address, the user's device as well as the username and password as well as browser access information on the http protocol. Capturing data packets using wireshark makes it easier for network administrators to monitor network.

Keyword: *Information Security, Sniffing, Wireshark research methods.*

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT, yang telah melimpahkan rahmat dan karunianya, sehingga penulis dapat menyelesaikan Skripsi ini, penulis telah melibatkan beberapa pihak, Oleh karena itu penulis mengucapkan terima kasih kepada :

1. Bapak Dr. Abid Djazuli, S.E.,M.M selaku Rektor Universitas Muhammadiyah Palembang
2. Bapak Dr. Ir, Kiagus Ahmad Roni, MT, IPM selaku Dekan Fakultas Teknik Universitas Muhammadiyah Palembang
3. Bapak Karnadi, S.Kom.,M.Kom selaku Kaprodi Teknologi Informasi
4. Bapak Apriansyah, S.Kom., M.Kom Selaku Pembimbing 1 dan Bapak Dedi Haryanto, S.Kom., M.Kom selaku Pembimbing II yang telah banyak memberikan saran dan kritik selama proses penulisan skripsi ini.
5. Bapak dan Ibu Dosen Program Studi Teknologi Informasi Universitas Muhammadiyah Palembang
6. Orang Tua tercinta yaitu ayah dan ibu dan adik-adik saya, yang selalu mendukung, mendoakan, dan memberikan bantuan.
7. Serta Teman-teman seperjuangan yang telah memberikan banyak semangat dan motivasi yang baik

Saran dan kritik yang sifatnya membangun sangat penulis harapkan. Semoga karya ilmiah ini bermanfaat dan dapat memberikan sumbangan yang berarti bagi pihak yang membutuhkan.

Palembang, Agustus 2022

Anggi Safitri
162018083

DAFTAR ISI

BAB II TINJAUAN PUSTAKA

BAB III METODE PENELITIAN

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan Teknologi Informasi khususnya di bidang jaringan komputer memungkinkan pertukaran informasi lebih cepat dan lebih kompleks dan data yang dipertukarkan dapat bervariasi. Pengguna internet dan penyedia jaringan nirkabel internet, memungkinkan mengakses apapun dan dari manapun yang mereka mau, yang menyebabkan keamanan informasi menjadi penting. Proses penyadapan informasi (*Sniffing)* pada jaringan komputer menjadi semakin biasa dilakukan, baik untuk kegunaan yang positif maupun negatif. Jaringan komputer bukanlah sesuatu yang baru saat ini, hampir di setiap tempat ada sebuah jaringan komputer guna untuk memperlancar arus informasi di tempat tersebut. Didalam sebuah jaringan komputer terdapat banyak sekali paket data yang berlalu lalang pada kabel jaringan, baik itu paket data yang mengandung informasi penting seperti password, alamat sebuah situs, user name, ip user dan lain-lain.

Sniffing merupakan proses pengendusan paket data pada sistem jaringan komputer, yang diantaranya dapat monitor dan menangkap semua lalu lintas jaringan yang lewat tanpa peduli kepada siapa paket itu dikirimkan. Dampak positif sniffing adalah admin dapat menganalisa paket data yang lewat pada jaringan untuk keperluan optimasi jaringan, seperti dengan melakukan analisa paket data, agar dapat diketahui membahayakan performa jaringan atau tidak, dan dapat mengetahui apa ada penyusup atau tidak[1]. Contoh dampak negatif sniffing adalah seseorang bisa melihat paket data informasi penting seperti username dan

password yang lewat pada jaringan komputer, username dan password yang dikirimkan bisa di salah gunakan oleh sniffer (penyadap). Hal ini mengakibatkan hilangnya salah satu sifat keamanan yaitu privasi. Untuk mengetahui paket data yang melintas pada suatu jaringan dibutuhkan sebuah aplikasi monitoring, yang bertujuan untuk mendapatkan informasi seperti Wireshark. Wireshark adalah sebuah *software* penganalisa jaringan yang paling dikenal. Software ini sangat berguna dalam menyediakan jaringan dan protokol serta memberikan informasi tentang data yang tertangkap pada jaringan. Wireshark bisa menganalisa transmisi paket data dalam jaringan, proses koneksi dan transmisi data antar komputer. Dapat mengumpamakan sebuah *Network Packet Analyzer* sebagai alat untuk memeriksa apa yang sebenarnya sedang terjadi di dalam kabel jaringan[2]. Dan aplikasi ini berguna untuk memeriksa keamanan jaringan dan bisa digunakan sebagai pengendus data-data privasi yang ada pada jaringan. Serta bisa menangkap paket-paket data atau informasi yang bertebaran pada jaringan.

Universitas Muhammadiyah Palembang merupakan salah satu perguruan tinggi swasta yang ada di bawah naungan persyarikatan Muhammadiyah yang berdiri sejak 15 juni 1979. Yang memiliki 7 fakultas Strata satu (1) dan 4 Program studi pascasarjana dua (S2) dan mempunyai layanan, salah satunya adalah UPT IT. UPT IT adalah Unit Pelaksanaan Teknis Teknologi Informasi yang menyediakan berbagai macam layanan teknologi informasi, untuk menunjang agar layanan administrasi tertata secara baik dan rapi dan UPT IT Memiliki jaringan yang terkoneksi satu sama lain, maka dari itu diperlukan Tools jaringan untuk memonitoring lalu lintas jaringan, yang berguna untuk mengetahui aktivitas yang

dilakukan pengguna jaringan dengan akses internet disana dan sniffing guna untuk mengecek keamanan jaringan.

Dalam Penelitian ini, proses sniffing (penyadapan) digunakan untuk mendapatkan informasi username dan password. Proses sniffing dilakukan menggunakan perangkat lunak Wireshark. Wireshark melakukan proses capturing data pada interface wireless, lalu mengamati hasil capture-an yang berisikan data POST yang berisi username dan password pada HTTP. Selama data tersebut tidak penting seperti berkomunikasi data menggunakan email, facebook, tidak masalah menggunkan koneksi HTTP. Karena mungkin dampak yang terjadi apabila ada yang mengintipnya tidak akan berpengaruh. Namun bagaimana jika data yang dikirimkan tersebut adalah password email, komunikasi bisnis yang sifatnya sangat rahasia, maka akibatnya sangat berisiko.

Berdasarkan latar belakang diatas, maka dibutuhkan suatu tools untuk menganalisa dan melakukan penyadapan (sniffing) trasnmisi paket data jaringan komputer yang ada di sana. Salah satu perangkat yang dapat digunakan untuk menganalisa dan melakukan penyadapan adalah wireshark. Maka dari itu penulis mengambil judul Tugas Akhir **"Analisis Penyadapan Transmisi Paket Data Jaringan Komputer Menggunakan Wireshark"** pada UPT IT UM-Palembang.

1.2 Rumusan Masalah

Berdasarkan penjelasan latar belakang diatas maka rumusan masalah adalah " Bagaimana cara melakukan analisis penyadapan transmisi paket data jaringan komputer menggunakan wireshark pada UPT IT UM-Palembang?"

1.3 Batasan Masalah

Untuk menghindari terjadinya pembahasan yang meluas maka penulis akan membatasi masalah yang akan di analisis sebagai berikut:

1. Penulis hanya melakukan Analisis paket data pada jaringan komputer menggunakan aplikasi wireshark
2. Melakukan analisis dari hasil capturing paket data protokol jaringan yaitu HTTP *(HyperText Transfer Protocol)* yang berisi informasi penting seperti username dan password serta alamat sebuah situs, dan lain-lain.

1.4 Manfaat Penelitian

Adapun manfaat dari penilitian ini terbagi menjadi 3 bagian sebagai berikut:

1.4.1 Bagi Mahasiswa

Adapun Manfaat penilitian ini bagi mahasiwa sebagi berikut:

1. Penulis dapat mengetahui cara melakukan analisis transmisi paket data
2. Penelitian ini dapat digunakan mengembangkan ilmu pengetahuan yang diperoleh selama perkuliah dan menambah wawasan

1.4.2 Bagi Universitas

Adapun manfaat penelitian ini bagi Universitas sebagai berikut:

1. Dapat menjadi tolak ukur pencapaian kinerja universitas dan program studi dalam mengevaluasi hasil pembelajaran oleh instasi tempat mahasiswa melakukan penelitian

2. Sebagai referensi tambahan bagi perpustakaan universitas muhammadiyah palembang.

1.4.3 Bagi Instansi

Berikut ini manfaat penelitian bagi perusahan instansi tempat mahasiswa melakukan penelitian sebagai berikut:

1. Memudahkan admin untuk memeriksa serta meningkatkan keamanan jaringan dan bisa melakukan analisa jaringan yang lalu lintas pada jaringan komputer.
2. Dengan menggunakan wireshark untuk menganalisa jaringan memudahkan proses capture paket data secara langsung dari sebuah *network interface* dan mampu menampilkan informasi yang detail.

1.5 Tujuan Penelitian

Tujuan dari Penelitian ini adalah sebagai berikut:

1. Untuk melakukan analisa paket data supaya bisa melihat apakah bisa mempengaruhi performa jaringan atau tidak dan bisa mengetahui ada penyusup atau tidak.
2. Mengumpulkan informasi yang berguna seperti IP Address, riwayat situs-situs, username, dan password yang tercapture dari jaringan sehingga jaringan dapat diatur dan dikontrol oleh administrator. Dengan begitu diharapkan jika user jaringan mengakses website terlarang didalam jaringan akan cepat diketahui dan melakukan tindakan pemblokiran website terlarang tersebut, sehingga mahasiswa universitas muhammadiyah palembang tidak terganggu dalam belajar.

1.6 Sistematika Penulisan

Adapun sistematika penulisan tugas akhir ini untuk memberikan gambaran umum tentang penelitian, yang dijalankan dan menjelaskan mengenai uraian secara singkat isi setiap bab dalam penelitian, sebagai berikut:

BAB I PENDAHULUAN

Bab ini penulis menguraikan tentang latar belakang, rumusan masalah, batasan masalah, manfaat penelitian bagi mahasiswa, universitas, bagi perusahaan serta tujuan penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang landasan teori dasar yang mendukung pembahasan secara detail, dan berupa definisi-definisi yang berkaitan langsung dengan ilmu atau masalah yang diteliti, serta menjelaskan tentang penelitian sebelumnya.

BAB III METODE PENELITIAN

Bab ini menjelaskan tentang sejarah singkat perusahaan, struktur organisai, waktu dan tempat penelitian, jadwal peneliti, serta menjelaskan tentang kerangka penelitian, metode pengumpulan data, sumber data, teknik analisis data, metode penelitian, gambaran sistem yang sedang berjalan.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi tentang hasil dan pembahasan hasil analisis paket data jaringan komputer pada UPT-IT UM-Palembang, yang diperoleh dari teori-teori dan hasil penelitian terdahulu.

BAB V PENUTUP

Pada bab ini berisi kesimpulan yang telah dikerjarkan dan saran yang akan menjadi masukan bagi perkembangan jaringan yang akan dikembangkan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

[1] M. F. Adriant and I. Mardianto, "Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan," *Semin. Nas. Cendekiawan*, pp. 224–228, 2015, [Online]. Available: https://www.trijurnal.lemlit.trisakti.ac.id/semnas/article/download/139/138.

[2] D. Irawan, "Analisis dan Penyadapan Transmisi Paket Data Jaringan Komputer Menggunakan Wireshark," *Anal. dan Penyadapan Transm. Paket Data Jar. Komput. Menggunakan Wireshark*, vol. 7, no. 1, pp. 1–5, 2017.

[3] R. Tianingrum and H. N. Sopiany, "Analisis Kemampuan Pemahaman Matematis Siswa SMP pada Materi Bangun Ruang Sisi Datar," *Pros. Semin. Nas. Mat. dan Pendidik. Mat.*, pp. 440–446, 2017, [Online]. Available: http://pmat-unsika.eu5.org/Prosiding/64RisnaTianingrum-SESIOMADIKA-2017.pdf.

[4] M. Barrimi *et al.*, "Konsep Analisis," *Encephale*, vol. 53, no. 1, pp. 59–65, 2013, [Online]. Available: http://dx.doi.org/10.1016/j.encep.2012.03.001.

[5] K. Zonggonau and H. Sajati, "Membangun Sistem Keamanan Arp Spoofing Memanfaatkan Arpwatch Dan Addons Firefox," *Compiler*, vol. 4, no. 1, pp. 49–58, 2015, doi: 10.28989/compiler.v4i1.87.

[6] Santo Faskafri, "Bab 1 pendahuluan," *Pelayanan Kesehat.*, no. 2015, pp. 3–13, 2020, [Online]. Available: http://repository.usu.ac.id/bitstream/123456789/23790/4/Chapter I.pdf.

[7] D. Kurnia, "Pemanfaatan Bettercap Sebagai Teknik Sniffing Pada Paket Trafik Jaringan Wifi," *Semin. Nas. Tek. UISU*, vol. 2, no. 1, pp. 83–85, 2019, [Online]. Available: www.olx.co.

[8] E. R. Onainor, "**済無**No Title No Title No Title," vol. 1, pp. 105–112, 2019.

[9] M. J. N. Yudianto, "Jaringan Komputer dan Pengertiannya," *Ilmukomputer.Com*, vol. Vol.1, pp. 1–10, 2014.

[10] U. D. R. Zaky Maula Luthfansa, "Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet," vol. 05, pp. 34–39, 2021.

[11] U. B. Darma *et al.*, "Analisis Dan Monitoring Sniffing Paket Data Jaringan Lokal Bps Sumsel Dengan Network," pp. 102–109.

[12] R. Tri, I. Gunawan, I. Marleni, O. Gregarius, and M. Nanda, "Analisis Keamanan Wifi Menggunakan Wireshark," *JES (J. Elektro Smart)*, vol. 1, no. 1, pp. 1–3, 2021.

[13] M. H. Nasution, K. Nasution, and O. K. Sulaiman, "Implementasi Aplikasi

Cain and Abel Dalam Penyadapan Paket Data Pada Jaringan Wifi," 2021.

[14] A. A. Zabar and F. Novianto, "Keamanan Http Dan Https Berbasis Web Menggunakan Sistem Operasi Kali Linux," *Komputa J. Ilm. Komput. dan Inform.*, vol. 4, no. 2, pp. 69–74, 2015, doi: 10.34010/komputa.v4i2.2427.

[15] D. Susianto and A. Rachmawati, "Implementasi dan Analisis Jaringan Menggunakan Wireshark, Cain and Abels, Network Minner (Studi Kasus: AMIK Dian Cipta Cendikia)," *J. Cendikia*, vol. XVI, pp. 120–125, 2018.

[16] "Sniffing Jaringan Menggunakan Wireshark." .