YAYASAN LEMBAGA PENDIDIKAN ISLAM DAERAH RIAU UNIVERSITAS ISLAM RIAU FAKULTAS TEKNIK



153510706

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNIK UNIVERSITAS ISLAM RIAU PEKANBARU 2019

LEMBAR PENGESAHAN PEMBIMBING SKRIPSI

Nama NPM

Teknik Laformatika

Strata Satu ()

Jenjang Pendidikan

Judul Skripsi

Program Studi

Analisis Keama MIEI/Terhadap UNIVERSITAS ISLAM RIAU Pekanbaru

Format sistematika dan pembahasan materi pada masing-masing bab dan sub bab dalam skripsi ini telah dipelajari dan dinilai relatif relah memenuhi ketentuan-ketentuan dan kriteria, kriteria dalam metode penuhsan ilmiah. Oleh karena itu, skripsi ini dinilai lavak dapat disetujui untuk disidangkan dalam ujian komprehensif. ekanburu 06 Desember 2019

Dosea Pembimbing

EKANBARU

Disetujui

Disahkan Oleh :

Dekon Fahultas Teknik NL MT.MS., TR 8 03 02 098

Ketua Prodi Teknik Informatika CHI SC EDTORA

AUSE LABELLAPANSA, ST., M.Cs., M.Kom

LEMBAR PENGESAHAN TIM PENGUJI UJIAN SKRIPSI

Muhammad Denny Sanjaya

NPM : 15351070

lurusan 🔅 Teknik

Program Studi

Nama

njang Pendidikan : Strata Satu (S1)

Judul Skripsi

Analisis Keamanan Jaringan Pada Fasilitos Internet (WIFI) Terhadap Serangan Peckel soft Tog Pada Kartos Indosat Doredo Rekanbara

Skripsi ini secara kescluruhan dinitat telah memenuhi ketertuan-ketentuan dan kaidah-kaulah dalam penyerengan penelulah di Angera telah dini dan dapat dipertahankan dihadapan tum pengui. Oleh karena nu Tim Penguji Ujian Skripsi Fakultas Teknik Universitas Islam Riau menyatakan bahwa mahasiswa yang bersangkutan dinyatakan Telah Lulus Mengikuti Ujian Komprehensif Pada Tanggal 66 Desember 2019 dan disetupat serta diretima untuk memenuhi salah satu syarat guna memperoleh gelar Sariana Strate Satu Bidang Ilmu Teknik Informatika.

1. Ir. Hj Des Suryani 2. Yudhi Arta, ST. M Sebagar Tini Penguji I Sebagar Tini Penguji I SEKANBARU

Dosen Pembimbing

Disetujui Oleh

Pekanharu, 66 Desember 2019

ABDUL SYUKUR, S.Kom., M.Kom

Disahkan Oleh :

an Enkultas Tekpik AINI, MT., MS., TR NPK : 88 03 02 098

Ketua Prodi Teknik Informatika AU SEUPINA

AUSE LABELLAPANSA, ST., M.Cs., M.Kom

LEMBAR PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini:

Nama: Muhammad Denny SanjayaTempat/Tgl Lahir: Pekanbaru, 25 Mei 1997Alamat: Jalan Muslim Kelurahan Tanjung Palas Kota Dumai.Adalah mahasiswa Universitas Islam Riau yang terdaftar pada:Fakultas: Teknip STAS ISLAM RIAUProgram StudiWeknik InformatikaJenjang Pendidikan: Strata-1 (S1)

Dengan ini menyatakan dengan sesungguhnya balawa skripsi yang saya tulis adalah benar dan asli hasil dari penelitian yang telah saya lakukan dengan judul"Analisis Keamanan Jaringan Pada Pasilitas (*Wifi*) Terhadap Serangan *Packet Sniffing* Pada Kantor Indosat Ooredoo Pekanbaru.".

Apa bila dikemudian hari ada yang merasa dirugikan atau menuntut karena penelitian ini menggunakan sebagian hasil tulisan atau karya orang lain tanpa mencantumkan nama penda yang bersangkutan atau terbukti karya ilmiah ini bukan karya saya sendiri atau plagiar nasil karya orang lain maka saya bersedia menerima sanksi sesuai dengan peraturan perundangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya untuk dapat digunakan sebagai mana mestinya.

Pekanbaru, 13 Desember 2019 Yang membuat pernyataan.

ERAI 58AHF14484824 00

(Muhammad Denny Sanjaya)

KATA PENGANTAR

Dengan menyebut nama Allah SWT yang Maha Pengasih lagi Maha Panyayang, Penulis ucapkan puji syukur atas kehadirat-Nya, yang telah melimpahkan rahmat, hidayah, dan inayah-Nya kepada kami, sehingga penulis dapat menyelesaikan proposal skripsi yang berjudul "Analisis Keamanan Jaringan Pada Fasilitas Internet (*Wifi*) Terhadap Serangan *Packet Sniffing* Di Kantor Indosat Ooredoo Pekanbaru" ini tepat pada waktunya.

Proposal skripsi ini telah penulis susun dengan maksimal dan mendapatkan bantuan dari berbagai pihak sehingga dapat memperlancar pembuatan proposal skripsi ini. Untuk itu penulis menyampaikan banyak terima kasih kepada semua pihak yang telah berkontribusi dalam pembuatan proposal skripsi ini.

Terlepas dari semua itu, penulis menyadari sepenuhnya bahwa masih ada kekurangan baik dari segi susunan kalimat maupun tata bahasanya. Oleh karena itu dengan tangan terbuka penulis menerima segala saran dan kritik agar penulis dapat menyempurnakan laporan ini.

Akhir kata penulis berharap semoga proposal ini dapat memberikan manfaat, inpirasi, dan dapat dipergunakan oleh instansi terkait.

i

Pekanbaru, 20 September 2019

Dokumen ini adalah Arsip Milik : Perpustakaan Universitas Islam Riau

Penulis

DAFTAR ISI

KATA PENGANTAR

DAFTAR IS	I
DAFTAR TA	BEL
DAFTAR GA	MBARv
BAB I	LEOSTAS ISLAN
PENDAHUL	UAN
1.1 Latar l	Belakang
1.2 Identif	ikasi Masalah
1.3 Rumus	an Masalah
1.4 Batasa	n Masalah
1.5 Tujuar	Penelitian
1.6 Manfa	at Penelitian
BAB II	
LANDASA	TEORI
2.1 Stu	di Kepustakaan 5
2.2 Das	sar Teori
2.2.1	Konsep Kemanan Jaringan7
2.2.2	Ancaman
2.2.3	Kelemahan
2.3 Jenis –	Jenis Ancaman Keamanan Jaringan
2.3.1	Packet Sniffer
2.3.2	ARP Spoofing / ARP Poisoning
2.3.3	<i>Probe</i>
2.3.4	<i>Scan</i>
2.3.5 Ac	count Compromise
2.3.6	Root Compromise
2.3.7	Denial of Service (Dos)
2.3.8	Flowchart
BAB III	

METODOLOGI PENELITIAN	
3.1 Metode Penelitian	
3.1.1 Bahan dan Alat Penelitian	
3.2 Flowchart Alur Penelitian	
3.3 Tahapan-tahapan Instalasi dan Konfigurasi Software	
3.4 Tahapan – Tahapan Penyerangan	29
BAB IV	
4.1. Analisis Hasil Peneletian ASITAS ISLA	
4.2 Solusi Untuk Mencegah Serangan Packet Sniffing	
BAB V	
5.1 Kesimpulan	
5.2 Saran	
DAFTAR PUS <mark>TAKA</mark>	



DAFTAR TABEL



DAFTAR GAMBAR

Gambar 3. 1 <i>Flowchart</i> Alur Penelitian
Gambar 3. 2 <i>software netstumbler</i>
Gambar 3. 3 Tampilan software inSSIDer pada windows 10 21
Gambar 3. 4 Penginstalan <i>Wireshark</i> Tahap Pertama
Gambar 3. 5 Penginstalan <i>Wireshark</i> Tahap Kedua
Gambar 3. 6 Penginstalan <i>Wireshark</i> Tahap Ketiga
Gambar 3. 7 Penginstalan <i>Wireshark</i> Tahap Keempat
Gambar 3. 8 Penginstalan Wireshark Tahap Kelima
Gambar 3. 9 Penginstalan Wireshark Tahap Keenam
Gambar 3. 10 Pengistalan <i>Wireshark</i> Tahap Ketujuh
Gambar 3. 11 Penginstalan Wireshark SELESAI
Gambar 3. 12 <i>Flowchart</i> Tahapan Penyerangan
Gambar 3. 13 Posisi tempat/lokasi penyerangan yang diizinkan pada gedung
kantor PT Indosat
Gambar 3. 14 Posisi tempat/lokasi penyerangan yang diizinkan pada gedung baru
Kantor PT Indosat
Gambar 3. 15 Tampilan software inSSIDer saat identifikasi <i>wifi</i>
Gambar 4. 1 Pukul 10.00 W.I.B – 11.00 W.I.B
Gambar 4. 2 Pukul 11.00 W.I.B – 12.00 W.I.B
Gambar 4. 3 Pukul 13.00 W.I.B s/d 14.00 W.I.B
Gambar 4. 4 Pukul 14.00 W.I.B s/d 15.00 W.I.B

Gambar 4. 5 Tahap Penyerangan Pertama Identifikasi Jaringan <i>Wifi</i>	38
Gambar 4. 6 Aktifitas Jaringan Wifi Pada Aplikasi Wireshark	39
Gambar 4. 7 Website Yang Tidak Memiliki Sistem Terenkripsi	40
Gambar 4. 8 Aktifitas Website Pada Aplikasi Wireshark	41
Gambar 4. 9 Hasil Pencarian IP Website Pada Command Prompt	42
Gambar 4. 10 Aktifitas Website Yang Sedang Berjalan	43
Gambar 4. 11 Cara Melihat Aktifitas Login Website	44
Gambar 4. 12 Pencarian Aktifitas Login Melalui Find Text	45
Gambar 4, 13 Perbedaan jaringan internet <i>wifi</i> kantor dan umum	46



BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada saat ini keamanan jaringan sangat penting dan harus diperhatikan terutama pada jaringan yang terhubung dengan internet atau suatu *wifi*, karena pada dasarnya jaringan tidak selalu aman dan selalu ada orang yang ingin mengekploitasi jaringan tersebut, baik dari jaringan *wired LAN* maupun *wireless LAN*. Dalam pembangunan sebuah perancangan system keamanan yang telah terhubung ke suatu internet haruslah direncanakan dan daoat dipahami oleh pengguna agar dapat melindungi sumber daya yang berada di dalam jaringan tersebut dan bisa dapat meminimalisir serangan yang terjadi oleh seseorang yang tidak bertanggung jawab.

Wireshark adalah aplikasi *packet sniffer* yang berguna untuk melakukan sebuah analisa protocol keamanan jaringan. Aplikasi ini dapat memblokir lalu lintas pada jaringan *LAN*, mencuri password, dan melakukan penyadapan aktif terhadap protokol-protokol umum.

Sedangkan Netstumbler adalah tools wifi hacking yang digunakan untuk mendeteksi dan mengidentifikasi sinyal wireless yang terbuka dan menyusup ke dalam jaringan.

Indosat didirikan sebagai perusahaan penanaman modal asing pertama di Indonesia yang menyediakan layanan telekomunikasi internasional melalui satelit internasional. Saat ini Kantor Indosat Ooredoo Pekanbaru telah menerapkan jaringan komputer kabel maupun nirkabel sebagai media pertukaran data/informasi pelayanan umum, kepegawaian dan informasi penting lainnya. Terdapat jaringan yang terpasang dalam lingkup Kantor Indosat Ooredoo Pekanbaru yaitu terinstall pada gedung yang didalamnya terdapat ruang customer service dan ruangan teknisi dengan menerapkan jaringan kabel.

Berdasarkan uraian diatas, penulis tertarik untuk mempelajari cara untuk mengamankan suatu jaringan. Oleh karena itu, penulis mengambil bahan mengenai keamanan jaringan internet untuk judul skripsi "Analisis Keamanan Jaringan Pada Fasilitas Internet (*Wifi*) Terhadap Serangan *Packet Sniffing*". 1.2 Identifikasi Masalah

Adapun identifikasi masalah yang dapat diambil dari penjelasan latar belakang tersebut adalah sebagai berikut "Kantor Indosat Ooredoo Pekanbaru perlu mempunyai pengawasan tentang bahaya nya jaringan komputer kantor dan umum dalam 1 jaringan yang berada di lingkungan Kantor Indosat Ooredoo Pekanbaru".

1.3 Rumusan Masalah

Berdasarkan latar belakang masalah dan hubungan dengan pemilihan judul tersebut, maka penulis merumuskan pokok permasalahan yaitu Evaluasi keamanan fasilitas internet (*wifi*) di Kantor Indosat Ooredoo Pekanbaru.

1.4 Batasan Masalah

Dalam pembuatan skripsi penulis membatasi masalah yang akan dikerjakan yaitu:

- 1. Penggunaan aplikasi Wireshark dalam melakukan simulasi penyerangan.
- 2. Penggunaan aplikasi *Wireshark*, dan *inSSIDer* untuk menganalisa keamanan jaringan di Kantor Indosat Ooredoo Pekanbaru.
- 3. Dalam skripsi penulis tidak melakukan implementasi peningkatan keamanan jaringan yang sudah ada, hanya memberikan solusi yang sebaiknya dilakukan untuk mengantisipasi terjadinya serangan seperti yang dilakukan penulis.
- 4. Untuk penelitian dilakukan percobaan beberapa hari dikantor untuk memahami konsep yang sedang berjalan dan membuat kembali simulasi dirumah jalan karya 1 gang miduk 1 yang memiliki koneksi internet.

1.5 Tujuan Penelitian

Tujuan yang hendak dicapai dalam penelitian ini adalah :

- Meningkatkan keamanan jaringan *Wifi* pada Kantor Indosat Ooredoo Pekanbaru.
- 2. Jaringan *wifi* dikantor Indosat Ooredoo Pekanbaru dapat lebih diperhatikan terhadap penyadapan orang yang tidak bertanggung jawab.

1.6 Manfaat Penelitian

Penelitian ini bermanfaat untuk :

- 1. Memberikan solusi terbaik untuk keamanan jaringan wifi.
- 2. Membantu pihak IT Kantor untuk mengontrol keamanan jaringan wifi.
- 3. Pihak kantor dapat merasa aman terhadap serangan *sniffing*.
- 4. Sebagai pengetahuan bagi pengguna layanan / fasilitas internet (*wifi*) khususnya bagi pengguna yang awam terhadap bahaya jaringan *Wifi* tanpa







BAB II

LANDASAN TEORI

2.1 Studi Kepustakaan

Menurut Lalu Delsi Samsumar (2017), Penelitian yang ingin dilakukan oleh penulis ialah penulis tidak dapat menghasilkan suatu model untuk hasil dari penelitian yang dapat digunakan sebagai referensi pengembagan atau meningkatkan keamanan akses jaringan *Wired LAN* pada jaringan Kantor Indosat Ooredoo Pekanbaru. Penggunaan teknologi internet semakin banyak dan tidak terkontrol, hal ini disebabkan karena banyaknya oengguna internet di dunia dan hamper semua lapisan masyarakat mengetahui tentang adanya internet.

Perbedaan dengan Penelitian yang ingin dilakukan oleh penulis ialah penulis tidak menghasilkan sebuah model sebagai hasil dari penilaian yang dapat digunakan sebagai referensi untuk mengembangkan dan meningkatkan keamanan akses jaringan komputer nirkabel pada jaringan pada kantor PT.Indosat Ooredo Pekanbaru. Penelitian Aji Supriyanto (2006) ialaah adanya batasan jangkauan radio dan interferensi menyebabkan ketersediaan servis menjadi terbatas. DoS attack dapat dilakukan dengan menginjeksikan *traffic* palsu. Pemakaian perangkat berbasis wlan pada saaat ini sudah begitu banyak, baik dugunkanan untuk komunikasi suara maupun data. Karena banyak teknologi komunikasi lainnya meggunakaan operator yang memberikan layanan komunikasi. Kelemahan jaringan wlan secara umum dapat dibagi menjadi 2 jenis yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Secara garis besar, celah oada jaringan wlan terbentang atas empat laye dimana keempat lapis layer tersebut sebenarnya merupakan proses dari terjadinya komunikasi pada data media wlan.

Perbedaan dengan penelitian yang akan penulis bahas ialah adanya batasan jangkauan radio dan interferensi menyebabkan ketersediaan servis menjadi terbatas. DoS attack dapat dilakukan dengan menginjeksikan *traffic* palsu.

Menurut Hendri Noviyanto (2011) yang berjudul analisis keamanan wireless di universitas muhammadiyah Surakarta berisi tentang pengguna access point sangat mudah dan dapat dipakai di tempat yang terjangkau sinyal wireless tanpa harus berada di tempat tertentu. Seorang penyerang dapat melakukan koneksi dengan access point dengan melakukan satu koneksi dan seorang penyerang itu mulai melakukan sccaning untuk pengguna yang sedang aktif. Perbedaan keamanan jaringan yang akan penulis kerjakan ialah penyerang melakukan koneksi dengan Access point dengan melakukan suatu koneksi internet dan penyerang mulai melakukan scanning user yang aktif.

2.2 Dasar Teori

2.2.1 Konsep Kemanan Jaringan

Penulis memiliki acuan pada penelitian Noviyanto yang berjudul analisis keamamanan wireless di universitas Muhammaddiyah Surakarta yaitu pada saat ini suatu keamanan jaringan sangat penting dan patut di perhatikan, terutama untuk jaringan yang terhubung dengan internet atau *wifi* dan memiliki dasar tidak selalu aman dari penyadapan, baik dari jaringan wired LAN maupun wireless LAN. Pada pembangunan sebuah system keamanan jaringa internet haruslah di rencanakan dan dipahami agar dapat melindungi pengguna dan meminimalisir terjadi serangan oleh orang yang tidak bertanggung jawab.

Apabila ingin mengamankan suatu jaringan maka harus ditentukan terlebih dahulu tingkat ancaman yang harus diatasi, dan resiko yang harus diambil maupun yang harus dihindari. Berikut ini akan dibahas mengenai ancaman , kelemahan, dan *policy* keamanan jaringan.

2.2.2 Ancaman

Pada dasarnya, ancaman datang dari seseorang yang mempunyai keinginan memperoleh akses ilegal ke dalam suatu jaringan komputer. Bagaimana tidak banyak ancaman-ancaman yang terjadi pada sistem informasi yang akan merugikan banyak pihak, baik individu, masyarkat, dan lain sebagainya. Oleh karena itu untuk mencegah ancaman-ancaman terhadap sistem informasi yaitu perlu adanya keamanan yang sangat canggih agar dapat mendeteksi atau membenarkan dari sebagian sistem yang rusak akibat gangguan pada sistem informasi. Ada beberapa tujuan yang ingin dicapai oleh penyusup dan, sangat berguna apabila dapat membedakan tujuantujuan tersebut pada saat merencanakan sistem keamanan jaringan komputer. Beberapa tujuan para penyusup adalah:

- a. Setiap penyusup hanya ingin tau susunan sistem dan data yang ada pada suatu jaringan komputer yang dijadikan sasaran. Penyusup yang bertujuan seperti ini disebut dengan *the curius*.
- b. Hanya ingin membuat sebuah sistem jaringan menjadi *down*, atau mengubah tampilan situs web. Penyusup yang mempunyai tujuan seperti ini disebut sebagai *the malicious*.
- c. Penyusup hanya berusaha untuk menggunakan sumber daya di dalam sistem jaringan komputer untuk memperoleh popularitas.
 Penyusup seperti ini disebut sebagai *the high-profile intruder*.
- d. Penyusup hanya ingin tau susunan data apa saja yang ada di dalam jaringan komputer dan selanjutnya dimanfaatkan untuk mendapatkan uang. Penyusup seperti ini disebut sebagai *the competition*.

2.2.3 Kelemahan

Kelemahan menggambarkan seberapa kuat sistem keamanan suatu jaringan komputer terhadap jaringan komputer yang lain, dan kemungkinan bagi seseorang untuk mendapat akses ilegal ke dalamnya.

2.3 Jenis – Jenis Ancaman Keamanan Jaringan

2.3.1 Packet Sniffer

Menurut Achmad Rizal Fauzi (2018), Packet sniffer ialah suatu teknik pemantauan setiap komunikasi dan transfer data yang lintas pada jaringan dan memonitor semua lalu lintas jaringan. Packet sniffer tidak sama dengan jaringan host standar yang hanya menerima dan mengirim lalulintas khusus. Ancaman keamanan yang disajikan oleh penyadapan adalah kemampuan mereka untuk menangkap semua lalu lintas masuk dan keluar, termasuk password dan username atau bahan sensitif lainnya. Untuk dapat membaca dan menganalisa setiap protokol yang melintasi jaringan, diperlukan program yang bisa membelokkan paket ke komputer attacker. Biasa disebut serangan spoofing, attaker akan bertindak sebagai Man-In-the-Middle (Asrodia & Patel, 2012:1)

2.3.2 ARP Spoofing / ARP Poisoning BAR

Menurut Fauzan F dengan judul Perancangan dan Analisis Keamanan Jaringan Terhadap ARP Spoofing pada Hotspot ialah Arp spoofing adalah suatu teknik untuk melakukan penyerangan kepada jaringan internet local baik menggunakan media kabel maupun nirkabel, yang dapat memungkinkan penyerang dapat mengendus frames data pada jaringan local atau penyerang dapat memodifikasi traffic bahkan menghentikan traffic.

2.3.3 Probe

Sebuah *probe* dapat dikenali dari adanya usaha-usaha yang tidak lazim untuk memperoleh akses ke dalam suatu sistem atau untuk menemukan informasi tentang sistem tersebut. Salah satu contohnya adalah usaha untuk login ke dalam sebuah account yang tidak digunakan. *Probing* ini dapat dianalogikan sebagai usaha untuk memasuki sebuah ruangan yang dengan mencoba-coba apakah pintunya terkunci **apa tidak**.

2.3.4 Scan

Scan adalah kegiatan probe dalam jumlah yang besar dengan menggunakan tool secara otomatis. Tool tersebut secara otomatis dapat mengetahui port-port yang terbuka pada host lokal maupun host remote, IP address yang aktif, bahkan bisa untuk mengetahui sistem operasi yang digunakan pada host yang dituju.

2.3.5 Account Compromise

Account compromise adalah penggunaan account sebuah komputer secara ilegal oleh seseorang yang bukan pemilik acoount tersebut. Account compromise dapat mengakibatkan korban mengalami kehilangan atau kerusakan data. Sebuah insiden account compromise dapat berakibat lebih lanjut, yaitu terjadinya insiden root compromise, yang dapat menyebabkan kerusakan lebih besar.

2.3.6 Root Compromise

Root compromise mirip dengan account compromise, dengan perbedaan account yang digunakan secara ilegal adalah account yang mempunyai privilege sebagai administrator sistem. Istilah root diturunkan dari sebuah account pada sistem berbasis UNIX yang mempunyai privelege tidak terbatas. Penyusup yang berhasil melakukan root compromise dapat melakukan apa saja pada sistem yang menjadi korban, termasuk menjalankan program, mengubah kinerja sistem, dan menyembunyikan jejak penyusupan.

2.3.7 Denial of Service (Dos)

Sumber daya jaringan yang berharga antara lain komputer dan database, serta pelayanan-pelayanan (service) yang disediakan oleh organisasi pemilik jaringan. Kebanyakan user jaringan memanfaatkan pelayanan-pelayanan tersebut agar pekerjaan mereka menjadi efisien. Bila pelayanan ini tidak dapat dipergunakan karena sebab-sebab tertentu, maka tentu saja akann menyebabkan kehilangan produktivitas. Sulit untuk memperkirakan penyebab *denial of service*. Berikut ini adalah contoh penyebab terjadinya *denial of service*:

- a. Kemungkinan jaringan menjadi tidak berfungsi karena kebanjiran traffic.
- b. Kemungkinan ada virus yang menyebar dan menyebabkan sisten komputer menjadi lamban atau bahkan lumpuh.
- c. Kemungkinan device yang melindungi jaringan dirusak.

2.3.8 Flowchart

Flowchart adalah bagan-bagan yang mempunyai arus yang menggambarkan langkah-langkah penyelesaian suatu masalah. *Flowchart* merupakan cara penyajian dari suatu algoritma. Simbol *flowchart* dan fungsinya dapat dilihat pada tabel sebagai berikut (Ladjamudin, 2006:265) :

Tabel 2. 1 Simbol dan Fungsi Flowchart

No	Simbol	Nama	Fungsi					

Dokumen ini adalah Arsip Milik : Perpustakaan Universitas Islam Riau



Dokumen ini adalah Arsip Milik : Perpustakaan Universitas Islam Riau







BAB III

METODOLOGI PENELITIAN

3.1 Metode Penelitian

Pada simulasi ini menggambarkan suatu *mode* kecil topologi jaringan internet Kantor Indosat Ooredoo Pekanbaru yang dalam jaringan *wifi* nya digunakan oleh pihak Kantor dan Umum (pengunjung), dan tidak memisahkan penggunaan nya antara jaringan *wifi* kantor dengan *wifi* untuk umum (pengunjung). Hingga perlu adanya pengawasan tentang bahaya nya jaringan *wifi* terhadap penyadapan data. Berikut langkah-langkah metode simulasi yang harus dilakukan.

Pada simulasi penelitian ini menggambarkan suatu *mode* kecil topologi jaringan internet Kantor Indosat Ooredoo Pekanbaru yang dalam jaringan *wifi* nya digunakan oleh pihak Kantor dan Umum (pengunjung), dan tidak memisahkan penggunaan nya antara jaringan *wifi* kantor dengan *wifi* untuk umum (pengunjung). Hingga perlu adanya pengawasan tentang bahaya nya jaringan *wifi* terhadap penyadapan data. Berikut langkah-langkah metode simulasi yang harus dilakukan.

3.1.1 Bahan dan Alat Penelitian

Pada saat melakukan penelitian ini Penulis menggunakan beberapa *software* dan *hardware* sebagai penunjang penelitian yang akan dilakukan oleh penulis. Untuk spesifikasi alat yang digunakan penelitian adalah sebagai berikut:

- 1. Kebutuhan perangkat keras dan sistem operasi.
 - a. Laptop Asus X441N, *Processor intel 2Core* 2,4 Ghz, Memori

2 GB

- b. Sistem operasi Windows 10.
- 2. Kebutuhan perangkat lunak.
 - a. Software Wireshark (untuk serangan Packet sniffing).

b. Software *Netstumbler* versi 0.4.0 (untuk melihat keberadaan *wifi*)

Software inSSIDer

3.2 Flowchart Alur Penelitian

c.

Dalam menjelaskan sebuah permasalahan alur penelitian dibuat untuk mempermudah pemahaman dalam penelitian tersebut. Metode tersebut dibuat dalam *flowchart* alur penelitian.



Gambar 3.1 Flowchart Alur Penelitian.

Sesuai dengan *flowchart* alur penelitian pada gambar 3.1 penelitian ini dilakukan dalam beberapa tahapan.

- a. Sebelum memulai penelitian penulis menyiapkan semua literatur, buku, ebook dan artikel untuk membantu menunjang penelitian.
- b. Penulis harus memenuhi persyaratan/prosedur perizinan penelitian yang diberikan oleh pihak Kantor PT.Indosat Ooredoo Pekanbaru, karena tidak semua tempat/lokasi boleh masuk kecuali karyawan tertentu yang berhak.
- c. Penulis mencari informasi data yang ada, konfigurasi jaringan *wifi* yang terpasang di seluruh ruangan Kantor PT.Indosat Ooredoo Pekanbaru meliputi tempat, SSID, BSSID, enkripsi yang digunakan.
- d. Penulis menyiapkan *hardware* dan *software* yang dibutuhkkan untuk mendukung pelaksanaan penelitian.
- e. Penulis melangkah untuk melakukan sebuah percobaan penyerangan kepada jaringan *wifi* untuk mendapatkan informasi tentang keamanannya.
- f. Penulis bisa menarik kesimpulan untuk memutuskan sebuah saran yang bisa digunakan untuk mengamankan jaringan kabel *LAN* dan *wifi* melihat dari sisi pengguna.

3.3 Tahapan-tahapan Instalasi dan Konfigurasi Software

- 1. Instalasi software Netstumbler pada windows 10
 - a. Klik 2x pada file netstumblerinstaller_0_4_0.exe untuk instalasi, kemudian ikuti perintah selanjutnya dengan klik *i agree, next* dan *install* sampai selesai.

 Konfigurasi *device network* yang terhubung dengan laptop pada netstumbler dengan cara meng-klik pilihan device, seperti pada gambar 3.2. berikut :



Gambar 3. 2 software netstumbler.

c. Setelah melihat gambar 3.2 ternyata *device network adaptor* yang terhubung dengan laptop penulis tidak *support*, karena *software netstumbler* hanya dapat berjalan sempurna pada *windows XP* dan tidak dapat berjalan sempurna pada *windows 10*. Kemudian penulis menggantinya dengan software *inSSIDer* sebagai alternatif *software netstumbler* untuk *windows 10*.

inSSIDer Lite							-	o ×
File View Settings Wi-Fi Help								
							Unlock with <u>inS</u>	SIDer Plus
SSID	CHANNELS	SIGNAL (dBm)	# RADIOS	PHY TYPE	SECURITY	MIN BASIC RATE	MAX DATA	RATE
INDOSAT FREE WIFI	8 11	-28	1	b, g, n	1	1.0		72.2
HUAWEI-udF4	10	-47	1	b, g, n	-	1.0		130.0
@wifi.id	1, 11	-55	2	b, g, n	1	1.0		144.4
ANNISA	1	-76	1	b, g, n	A	1.0		144.4
KOST ANNISA	1*	-84	1	b, g, n	<u> </u>	1.0		300.0
IndiSchool@wifi.id	11	-90	1	b, g, n	1	1.0		144.4
2.4 GHz	UNIVERSI		AM	HAU				-30 -40 -50 -60
-70 -80 -90		iSchool@wifi.id	2		0			-70 -80 -90
1 2 3 4	5 6 / 8 9 1	0 11 12 13	36	44 52 60	1	00 108 116 124 132	2 140 149 15	/ 165

Gambar 3. 3 Tampilan software inSSIDer pada windows 10.

- 2. Instalasi software Wireshark pada Windows 10
 - a. Klik 2 kali pada file *wireshark-win640-3.0.5* yang telah di download sebelum nya untuk memulai install aplikasi *wireshark*.
 - b. Selanjut nya akan muncul seperti gambar 3.4 dan klik Next yang

akan melanjutkan kehalaman selanjutnya



Gambar 3. 5 Penginstalan Wireshark Tahap Kedua

d. Selanjut nya ceklis semua pilihan lalu tekan Next perhatikan digambar 3.6

🚄 Wireshark 3.0.5 64-bit Setup			_		\times
Choose Components Choose which features of Wires	shark 3.0.5 64-bit you want	to install.			
The following components are a Select components to install:	Wailable for installation.	15			
Space required: 193.9 MB	Description Position your mouse over description,	a componen	at to see it	S	
SIME	< Back	Next	t >	Car	ncel

Gambar 3. 6 Penginstalan Wireshark Tahap Ketiga

e. Selanjutnya ceklis kolom yang tersedia agar aplikasi wireshark berada di

10

desktop dan tombol start lalu tekan next, perhatikan gambar 3.7



f. Selanjutnya pilih tempat penyimpanan yang diinginkan dengan menekan *browser* untuk memilih tempat penyimpanan lalu tekan *next* untuk menuju tahap selanjutnya, perhatikan gambar 3.8



25

Gambar 3.8 Penginstalan Wireshark Tahap Kelima

g. Selanjutnya tekan install untuk memulai penginstalan seperti gambar

3.9



Gambar 3.9 Penginstalan Wireshark Tahap Keenam

h. Selanjutnya tunggu penginstalan hingga selesai tekan next setelah penginstalan selesai, perhatikan gambar 3.10



Gambar 3. 10 Pengistalan Wireshark Tahap Ketujuh

- i. Selesai dalam melakakukan penginstalan aplikasi *Wireshark* dan siap digunakan tekan *finish* untuk menutup penginstalan, perhatikan gambar
 - 3.11





Gambar 3. 11 Penginstalan Wireshark SELESAI

EKANBARU



3.4 Tahapan – Tahapan Penyerangan

Gambar 3. 12 Flowchart Tahapan Penyerangan

Sesuai dengan *flowchart* tahapan penyerangan diatas, penyerangan ini dilakukan dalam beberapa tahapan.

1. Penulis mencari posisi tempat penyerangan yang diizinkan.



Gambar 3. 13 Posisi tempat/lokasi penyerangan yang diizinkan pada gedung kantor PT Indosat.

Gambar 3.7 adalah denah lokasi dimana penulis melakukan penelitian pada gedung kantor PT Indosat Ooredoo Pekanbaru, angka – angka yang tertulis diatas merupakan perwakilan dari beberapa ruangan, berikut penjelasannya :

- a. Ruang 1 terdapat Ruang Karyawan Pelayanan Customer.
- b. Ruang 2 terdapat Ruang Karyawan Administrasi Keuangan, dan Kasir.
- c. Ruang 3 terdapat Ruang Supervisor Operasi & Teknik.
- d. Ruang 4 terdapat Ruang Karyawan Kebersihan & Peralatan.
- e. Ruang 5 adalah Ruang Rapat yang penulis gunakan sebagai tempat penelitian, yang didalam ruangan tersebut terdapat *switch* dan modem ADSL Provider.



Gambar 3. 14 Posisi tempat/lokasi penyerangan yang diizinkan pada gedung baru Kantor PT Indosat.

Gambar 3.8 adalah denah lokasi dimana penulis melakukan penelitian pada gedung kantor PT Indosat Ooredoo Pekanbaru, angka – angka yang tertulis diatas merupakan perwakilan dari beberapa ruangan, berikut penjelasannya:

- a. Ruang 1 adalah ruangan server.
- b. Ruang 2 adalah ruang karyawan PT Indosat Ooredoo.
- c. Ruang 3 adalah ruang supervisor PT Indosat Ooredoo.
- d. Ruang 4 adalah ruang tunggu.
- e. Ruang 5 adalah ruang monitoring jaringan komputer yang penulis gunakan sebagai tempat penelitian.
- f. Ruang 6 adalah Gudang.

2. Pengidentifikasian keamanan Wifi menggunakan software inSSIDer

Penulis menjalankan software inSSIDer pada windows 10 dan secara otomatis akan menampilkan informasi tentang keberadaan wifi dengan lengkap dengan nama SSID, *mac address*, *vendor, channel* yang dipakai, *network type* dan *security* atau keamanan yang digunakan.



Gambar 3. 15 Tampilan software inSSIDer saat identifikasi wifi.

BAB IV

HASIL DAN PEMBAHASAN

Analisis ini perlu dilakukan agar dapat mengetahui seberapa aman tingkat keamanan yang ada dalam sebuah jaringan *wireless* pada PT.Indosat Ooredoo Pekanbaru. Seperti pada umumnya tingkat keamanan bukan berasal dari *hardware* dan *software* yang sudah ada namun terdapat peran penting dari manusia/pengguna jaringan yang melakukan kontak atau koneksi dari perancangan jaringan itu sendiri.

Keamanan jaringan komputer yang terpasang di area PT.Indosat Ooredoo Pekanbaru pada umumnya masih perlu peningkatan kemanan, terbukti pada *wifi* yang terpasang tidak menggunakan keamanan atau terbuka. Disamping itu masih banyak pegawai dan konsumen yang masih awam tentang keamanan jaringan *wifi*.

4.1. Analisis Hasil Peneletian a. Mengindetifikasi Wifi

Percobaan ini penulis lakukan untuk mengidentifikasi keberadaan *wifi* dalam berbentuk informasi lengkap dengan nama SSID, *mac address*, RSSI, *vendor, channel* yang memakai *network type* dan *security* atau keamanan yang digunakan. Hal ini hanya untuk memudahkan penulis melakukan penyerangan untuk mendapatkan koneksi dengan jaringan *wifi* yang ada. Dalam mengidentifikasi ini penulis mendapatkan jaringan *wifi* tanpa pengaman atau terbuka yang berada di area PT.Indosat Ooredoo Pekanbaru.

b. Analisis jaringan wifi

Percobaan analisis ini dilakukan untuk memastikan website yang sering di kunjungi pihak kantor PT. Indosat Pekanbaru, dan untuk memastikan bahwa website tersebut bebas dari serangan *packet sniffing*. Hal ini dapat memudahkan penulis untuk memastikan website yang dapat terbebas dari serangan dan tidak, agar pihak kantor tidak perlu khawatir menggunakan jaringan *wifi* yang berada di wilayah kerja kantor PT.Indosat Ooredoo Pekanbaru.

Analisis ini dilakukan beberapa kali dalam keadaan jam kerja,berikut contoh analisis yang dilakukan :



1. Jam kerja pukul 10.00 W.I.B – 12.00 W.I.B

Gambar 4. 1 Pukul 10.00 W.I.B – 11.00 W.I.B

No.	Time	Source	Destination	Protocol	Length Info
696	671 1135.924812	13.107.4.50	10.126.75.175	HTTP	627 [TCP Previous segment not captured] Continuation
696	682 1136.064497	13.107.4.50	10.126.75.175	HTTP	1514 Continuation
696	685 1136,086861	13.107.4.50	10.126.75.175	HTTP	1514 Continuation
600	586 1136 086863	13 107 4 50	10 126 75 175	нттр	1514 Continuation
050	000 1100.0000000	20.00.000.115	10.120.75.175	UTTO	
090	095 1150.000072	50.09.220.115	10.120./5.1/5	nite	940 Continuation
690	594 1136.086873	36.89.220.115	10.126.75.175	HTTP	1514 Continuation
690	695 1136.086873	13.107.4.50	10.126.75.175	HTTP	1514 Continuation
696	697 1136.086874	13.107.4.50	10.126.75.175	HTTP	1514 Continuation
693	704 1136.087522	13.107.4.50	10.126.75.175	HTTP	1514 Continuation
693	713 1136.234935	13.107.4.50	10,126,75,175	HTTP	1514 Continuation
69	714 1136 234937	13 107 4 50	10 126 75 175	HTTP	1514 Continuation
607	716 1126 124020	26 00 220 115	10.126.75.175	UTTO	1514 Continuation
09	/15 1156.254956	30.09.220.115	10.120.75.175	ni ir	1514 Conclinuation
69.	/16 1136.23494/	36.89.220.115	10.126.75.175	HITP	1514 Continuation
69	/17 1136.234948	13.107.4.50	10.126.75.175	HTTP	1514 TCP Previous segment not captured Continuation
697	725 1136.656416	13.107.4.50	10.126.75.175	HTTP	1514 Continuation
691	726 1136.656419	13.107.4.50	10.126.75.175	HTTP	1514 Continuation
693	727 1136.656420	13.107.4.50	10.126.75.175	HTTP	1514 Continuation
69	728 1136.656422	36.89.220.115	10.126.75.175	HTTP	1514 [TCP Previous segment not captured] Continuation
69	729 1136,656423	36,89,220,115	10,126,75,175	HTTP	1514 Continuation
69	758 1137,166927	13,107,4,50	10.126.75.175	HTTP	1514 [TCP Previous segment not continued] Continuation
603	23 1130 210522	13 107 4 50	10 126 75 175	HTTP	151/ Continuation
603	015 1100.210022	26 90 220 115	10.126.75.175	UTTO	The Continuation of IOLA
090	525 1139.336560	30.05.220.113	10.120.75.175	A DOLLAR	134 Continuation
698	64/ 1140.240543	36.89.220.115	10.126./5.1/5	HITP	1514 Continuation
698	870 1140.435161	13.107.4.50	10.126.75.175	HTTP	1514 [TCP Previous segment not captured] Continuation
698	872 1140.438904	13.107.4.50	10.126.75.175	HTTP	1514 Continuation
698	876 1140.453525	36.89.220.115	10.126.75.175	HTTP	1514 [TCP Spurious Retransmission] Continuation
698	877 1140.453531	36.89.220.115	10.126.75.175	HTTP	1514 Continuation
698		36.89.220.115	10.126.75.175	HTTP	1514 [TCP Previous segment not captured] Continuation
		0	Gambar	• 4. 2	Pukul 11.00 W.I.B – 12.00 W.I.B
	2.	Jam ker	Gambar ja 13.00	• 4. 2 W.I.I	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B
	2.	Jam ker	Gambar ja 13.00	• 4. 2 W.I.I	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B
	2.	Jam ker	Gambar ja 13.00	• 4. 2 W.I.I	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B
No.	2. Time	Jam ker	Gambar ja 13.00	• 4. 2 W.I.]	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B
No.	2. Time 849 466.963384	Jam ker	Gambar ja 13.00 Destination 10.126.255.255	• 4. 2 W.I.I Protocol NBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B
No.	2. Time 849 466.963384 850 466.996693	Jam ker Source 10.126.168.230 10.126.168.230	Gambar ja 13.00 Destination 18.126.255.255 19.126.255.255	• 4. 2 W.I.I Protocol NBNS NBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B
No.	Time 849 466.963384 859 466.996693 851 467.102478	Source 10.126.168.230 10.126.168.239 10.126.168.331	Gambar ja 13.00 Destnaton 10.126.255.255 10.126.255.255 10.26.255.255	• 4. 2 W.I.I Protocol NBNS NBNS UDP	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B
No.	2. Time 649 466.963384 650 466.996693 051 467.102478 051 467.102478 052 467.103642	Source 10.126.168.230 10.126.168.230 10.126.183.152 10.126.111.234	Gambar ja 13.00 Destination 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255	• 4. 2 W.I.I Protocol NBNS NBNS UDP NBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B
No. 16(16(16(16(16(2. Time 049 466.963384 050 466.996693 051 467.102478 052 467.103642 053 467.249098	Surce 10.126.168.230 10.126.168.230 10.126.183.152 10.126.111.234 10.126.111.234	Gambar ja 13.00 ^{Destinaton} 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255	Yotocol W.I.I Protocol NBNS NBNS UDP NBNS NBNS NBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B
No. 161 161 161 161 161	2. Time 849 466.963384 859 466.996693 851 467.103642 853 467.24908 854 467.251987	Source 10.125.158.230 10.126.158.230 10.126.138.152 10.126.111.234 10.126.111.234 10.126.111.234	Gambar ja 13.00 ^{Destnaton} 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255	• 4. 2 W.I.] Protocol NBNS NBNS NBNS NBNS NBNS NBNS NBNS NBN	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B 92 Iane query IIB M3.ZABHCQ.IET.005 92 Iane query IIB M3.ZABHCQ.IET.005 93 Jane query IIB DESKT0P-GP4WG4Cle5 93 Name query IIB DESKT0P-GP4WG4Cle5 93 Name query IIB DESKT0P-GP4WG4Cle5 93 Name query IIB DESKT0P-GP4WG4Cle5 93 Salts - Salts Lenz63
No. 160 160 160 160 160	Time 849 466.966384 859 466.99663 951 467.182478 852 467.103642 853 467.249988 854 467.251967	Sure 10.126.156.230 10.126.166.230 10.126.163.230 10.126.11.234 10.126.11.234 10.126.11.234	Gambar ja 13.00 ^{Destination} 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255	 4.2 W.I.J Protocol NBNS NBNS NBNS NBNS NBNS NBNS NBNS NDP NBNS NDP NDP	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B
No. 16(16(16(16(16(16(16(16(16(Z. Tme 649 466.963384 650 466.996693 851 467.182478 852 467.183642 853 467.24998 854 467.251987 855 467.341088	Source 10.125.168.230 10.125.168.230 10.126.168.230 10.126.111.234 10.126.111.234 10.126.12.244 10.126.34.63 10.125.34.63	Gambar ja 13.00 0.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255	• 4. 2 W.I.I Protocol NBNS NBNS UDP IBNS NBNS UDP BROMKEPD	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B 2 Name query NB 08.7ABNAQ.NET(80) 305 54915 - 54915 Len-263 32 Name query NB 05XT0P-GP4UG4<12> 32 Name query NB 05XT0P-GP4UG4<12> 32 Name query NB 05XT0P-GP4UG4<12> 32 Name query NB 05XT0P-GP4UG4<12> 32 Name query NB 05XT0P-GP4UG4<12> 34 Name query NB 05XT0P-GP4UG4 35 Name query NB 05XT0P-GP4UG4 36 Name query NB 05XT0P-GP4UG4 37 Name query NB 05XT0P-GP4UG4 38 Name query
No. 16(16(16(16(16(16(16(16(16(16(2. Time 049 466, 96384 050 466, 996693 051 467, 102478 052 467, 103642 053 467, 249098 055 467, 249098 055 467, 461080 055 467, 461080	Source 19.126.156.239 10.126.156.239 10.126.156.239 10.126.111.234 10.126.111.234 10.126.21.224 10.126.21.245 10.126.21.254 10.126.51.259 10.126.51.56.129	Gambar ja 13.00 ^{Destination} 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255	Protocol NBNS NBNS UDP NBNS NBNS UDP BROWSER NBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B 27 Jane query H8 M8.748H0Q.HETG80 92 Jane query H8 M8.748H0Q.HETG80 93 State query H8 D5XT0PC GRAUGG412 93 Jane query H8 D5XT0PC GRAUGG412 94 Host Announcement HP-PC, Workstation, Server, Print Queue Server, HT Workstation 93 Jane query H8 D5XT0PC
No. 161 160 160 160 160 160 160 160	Time 649 466.963384 659 466.996693 651 467.102478 652 467.103642 653 467.249698 654 467.251987 655 467.364108 655 467.462046 657 467.462046 657 467.462046	Source 19.126.168.239 19.126.168.239 19.126.168.239 19.126.111.23 19.126.111.23 19.126.111.23 19.126.123.4.63 19.126.34.61 19.126.34.61	Gambar ja 13.00 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255	 4.2 W.I.I Protocol NBNS NBNS UDP NBNS UDP NBNS UDP NBNS UDP NBNS <li< th=""><th>Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B 20 Name query NB NS.74BH0Q.NET609 20 Name query NB NS.74BH0Q.NET609 20 Name query NB D5ST0P.6844064(1c) 20 Name query NB D5ST0P.68440(1c) 20 Name quer</th></li<>	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B 20 Name query NB NS.74BH0Q.NET609 20 Name query NB NS.74BH0Q.NET609 20 Name query NB D5ST0P.6844064(1c) 20 Name query NB D5ST0P.68440(1c) 20 Name quer
No. 166 166 166 166 166 166 166 166	2. Time 0499 466. 9963384 0499 466. 99633 051 467. 10342 053 467. 249988 054 467. 251967 055 467. 349488 056 467. 461008 056 467. 462046 058 467. 632711	Source 10.125.166.230 10.125.168.230 10.125.168.230 10.125.168.230 10.125.111.234 10.125.124 10.125.124 10.125.124 10.125.124 10.125.24.63 10.125.111.23 10.125.209.59	Gambar ja 13.00 0.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255	 4.2 W.I.I Protocol NBNS NBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B ergh Info 92 Name query NB V5.7ABNPQ.NETK00> 93 Name query NB V7.7ABNPQ.NETK00> 9365 54915 - 54915 Len-263 92 Name query NB USXT0P-GP4WG44(12) 93 Name query NB USXT0P-GP4WG44(12) 93 Name query NB USXT0P-GP4WG44(12) 93 Staf1 - 57621 Len-40 243 Host Announcement NP-PC, Workstation, Server, Print Queue Server, NT Workstation 93 Name query NB USXTAPC40> 93 Name query NB USXTAPC40> 93 Name query NB USXTAPC40>
No. 160 160 160 160 160 160 160 160 160 160	Time 249 466.963384 850 466.996693 851 467.102478 852 467.103472 853 467.249098 854 467.251987 855 467.34108 856 467.461088 857 467.33140 858 467.633240	Source 10.126.156.230 10.126.166.230 10.126.166.230 10.126.111.234 10.126.111.234 10.126.111.234 10.126.111.234 10.126.34.63 10.126.461.29 10.126.34.63 10.126.245.260 10.126.245.260	Gambar ja 13.00 Destination 10.126.255.255 10.126.255 10.126.255 10.126.255 10.126.255 10.126.255 10.126.255 10.126.255 10.126.255 10.126.255 10.126.255 10.126.255 10.126 10.126 10.126 10.126 10.126 10.126 10.126 10.1	+ 4, 2 W.I.I Protocol HBNS HBNS UDP HBNS UDP HBNS UDP BROWSER HBNS HBNS HBNS HBNS HBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B 21 Name query H8 M5.ZABHXQ0,HETK08> 32 Name query H8 M7.ZABHXQ0,HETK08> 32 Name query H8 D5XTR24BHXQ0,HETK08> 32 Name query H8 D5XTR24BHXQ0,HETK08> 32 Name query H8 D5XTR24BHXQ0 32 Name query H8 D5XTR24BHXQ0 34 Host Announcement H2-PC, Workstation, Server, Print Queue Server, HT Workstation 32 Name query H8 D5XTR24BHX 34 Host Announcement H2-PC, Workstation, Server, Print Queue Server, HT Workstation 32 Name query H8 D5XTR24BHX 34 Host Announcement H2-PC, Workstation, Server, Print Queue Server, HT Workstation 38 Name query H8 D5XTR24BHX 34 Host Announcement H2-PC, Workstation, Server, Print Queue Server, HT Workstation 39 Name query H8 D5XTR24BHX 34 Host Weith H2 H7 D5XTR24BHX 34 H5XTR24BHX 34 Host Weith H2 H7 D5XTR24BHX 34 H5XTR24BHX 34 H
No. 160 166 166 166 166 166 166 166 166 166	2. Time 49 466.963384 459 466.99663 951 467.102478 852 467.103642 853 467.24998 854 467.251987 855 467.461088 856 467.461088 858 467.632711 859 467.333440 868 467.63299	Source 10.126.168.230 10.126.168.230 10.126.168.230 10.126.111.234 10.126.111.234 10.126.12.244 10.126.72.181 10.126.12.244 10.126.72.181 10.126.181.129 10.126.181.299 10.126.24.25.200 10.126.25.200 10.126.25.200	Gambar ja 13.00 0.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255	+ 4. 2 W.I.I Protocol HBNS HBNS HBNS HBNS HBNS HBNS HBNS HBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B
No. 164 166 166 166 166 166 166 166 166 166	2. Time 049 465.963384 049 465.963384 059 465.996633 051 467.103642 053 467.249098 054 467.251987 055 467.324108 056 467.32111 059 467.633840 058 467.632711 059 467.633840 061 467.980413 051 467.980415 051 467.980415 051 467.980415 051 467.980415 051 467.980415 051 4	Source 19.125.166.230 10.125.166.230 10.125.166.230 10.125.166.230 10.126.163.152 10.126.101.234 10.126.12.234 10.126.111.234 10.126.234.53 10.126.166.129 10.125.245.200 10.125.245.200 10.126.245.200 10.126.245.200	Gambar ja 13.00 Destination 10.126.255.255 10.126.255 10.126.255 10.126.255 10.126 10.126 10.1265 10.126 10.126 10.126 10.126 10.	+ 4. 2 W.I.I Protocol NBNS NBNS UDP NBNS NBNS UDP BROWSER HBNS NBNS NBNS NBNS NBNS NBNS NBNS NBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B Event Info 92 Name query NB M3, ZABNQQ,NETK00> 9305 54915 - 54915 Len-263 92 Name query NB D5XTAP-C60+WU64(12) 9305 54915 - 54915 Len-263 92 Name query NB D5XTAP-C60 93 Total Announcem HP-PC, Workstation, Server, Print Queue Server, NT Workstation 93 Name query NB D5XTAP-C60 93 Name query NB D5XTAP-C60 92 Name query NB D5XTAP-C60 93 Name query NB D5XTAP-C60 93 Name query NB D5XTAP-C60 94 Name query NB D5XTAP-C60 94 Name query NB D5XTAP-C60 95 Name query NB D5XTAP-C60 95 Name query NB D5XTAP-C60 95 Name query NB D5XTAP-C60 96 Name query NB D5XTAP-C60 97 Name query NB D5XTAP-C60 97 Name query NB D5XTAP-C60 97 Name query NB D5XTAP-C60 97 Name query NB NS NAME-C017C42252E-C60 97 Name query NB NS NAME-C017C4225E-C60 97 Name query NB NS NAME-C017C425E-C60 97 Name query NB NS NAME-C017C4
No. 16(16(16(16(16(16(16(16(16(16(2. Time 649 466.963384 650 466.996633 651 467.102478 653 467.249098 854 467.249098 854 467.249098 855 467.34108 856 467.461088 857 467.34108 856 467.462046 614 67.980413 860 467.980413 862 467.981555	Source 10.126.156.239 10.126.156.239 10.126.156.239 10.126.156.239 10.126.111.234 10.126.211.234 10.126.211.234 10.126.245.209 10.126.245.209 10.126.245.209 10.126.245.209 10.126.168.239	Gambar ja 13.00 ^{Destnaton} 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255 18.126.255.255	+ 4. 2 W.I.I Protocol NBNS UDP NBNS NBNS NBNS NBNS NBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B C liane query HB M3.28BN00.HET.000 20 liane query HB M3.28BN00.HET.000 20 liane query HB M3.28BN00.HET.000 20 liane query HB M3.28BN00.HET.000 20 liane query HB D5XT0P.084U404120 20 liane query HB D5XT0P.084U404120 20 liane query HB SATAP.080 243 Host Announcement HP-PC, Workstation, Server, Print Queue Server, HT Workstation 20 liane query HB SATAP.080 243 Host Announcement HP-PC, Workstation, Server, Print Queue Server, HT Workstation 20 liane query HB SATAP.080 243 Host Announcement HP-PC, Workstation, Server, Print Queue Server, HT Workstation 20 liane query HB SATAP.080 243 Host Query HB SATAP.080 29 liane query HB SATAP.080 20 liane query HB JSATAP.080
No. 166 166 166 166 166 166 166 166 166 16	2. Time 1049 466.963384 4054 466.96633 851 467.103642 852 467.103642 853 467.24928 854 467.251967 855 467.34108 857 467.462846 858 467.32110 859 467.33340 868 467.636299 861 467.980413 862 467.981555 863 467.982683	Source 10.126.168.230 10.126.168.230 10.126.168.230 10.126.168.230 10.126.113.24 10.126.122.24 10.126.224 10.126.122.24 10.126.224 10.126.224 10.126.234.63 10.126.24.25.200 10.126.125.200 10.126.25.200	Gambar ja 13.00 0.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255 10.126.255.255	+ 4. 2 W.I.I Protocol NBNS UDP IBNUS UDP BROWSER NBNS NBNS NBNS NBNS NBNS NBNS NBNS NBN	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B B s/d 15.00 W.I.B 2 Name query NB N3.74BHXPQ.NETK00> 305 54915 - 54915 Len-263 29 Name query NB D5XTP-GP4V04K1c> 305 54915 - 54915 Len-263 325 54915 - 54915 Len-263 325 54915 - 54915 Len-263 325 54915 - 57621 Len-40 34 Host Annouement HP-PC, Workstation, Server, Print Queue Server, NT Workstation 92 Name query NB D5XTAPK00> 39 Name query NB D5XTAPK00> 39 Name query NB D5XTAPK00> 39 Name query NB NB.KTAPK00> 39 Name query NB NB.KTAPK00> 39 Name query NB NB.KTAPK00> 30 Name query NB NB
No. 166 166 166 166 166 166 166 166 166 16	Time 49 466.963384 850 466.996693 851 467.102478 852 467.102478 853 467.249098 854 467.249098 854 467.331408 856 467.461088 856 467.461088 867 467.462046 868 467.633249 860 467.636299 861 467.980413 862 467.981555 863 467.981555	Soure 10.126.156.239 10.126.156.239 10.126.166.239 10.126.161.234 10.126.111.234 10.126.111.234 10.126.111.234 10.126.34.33 10.126.34.33 10.126.34.39 10.126.245.239 10.126.162.37 10.126.156.23 10.126.135.23 10.126.237.230	Gambar Ja 13.00 Destination 10.126.255.255 10.126.255 10.126.255.255 10.126.255 10.126.255.255 10.126.2	+ 4. 2 Protocol IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B Vierge uery H8 M5.288000,HET(80) 22 Hane query H8 M7.288000,HET(80) 23 Hane query H8 M7.288000,HET(80) 24 Hane query H8 DStTAP(80) 25 Mane query H8 DStTAP(80) 24 Host Announcement HP-PC, Workstation, Server, Print Queue Server, HT Workstation 28 Hane query H8 DStTAP(80) 29 Hane query H8 DStTAP(80)
No. 661 166 166 166 166 166 166 166 166 16	2. Time 9466.963384 859 466.996633 851 467.102478 852 467.103642 853 467.24998 854 467.251987 855 467.461088 858 467.632711 859 467.333840 868 467.632293 861 467.980413 862 467.981555 863 467.98253	Soure 10.126.168.230 10.126.168.230 10.126.168.230 10.126.168.230 10.126.111.234 10.126.12.244 10.126.72.161 10.126.12.244 10.126.224 10.126.209.99 10.126.168.230 10.126.168.230 10.126.158.230 10.126.158.230 10.126.155.23 10.126.155.23	Gambar ja 13.00 10.126.25.25	+ 4. 2 W.I.I Protocol NBNS UDP NBNS UDP UDP NBNS NBNS BROWSER	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B B s/d 15.00 W.I.B S s/d 15.00 W.I.B P lane query NB N5.74BNQ.NET(00) 20 lane query NB N5.74BNQ.NET(00) 20 lane query NB N5.74BNQ.NET(00) 20 lane query NB D5.74P.(00) 20 lane query NB N5.74P.(00) 20 lane query NB N5.74P.(00) 20 lane query NB N5.74P.(00) 20 lane query NB N5.74P.(00) 20 lane query NB D5.74P.(00) 20 lane query NB D5.74P.(00)
No. 166 166 166 166 166 166 166 166 166 16	2. Time 849 466.96384 859 466.96384 859 467.182478 852 467.18342 853 467.24938 854 467.251967 855 467.461088 857 467.462046 858 467.32711 859 467.63284 859 467.63284 859 467.63284 859 467.63284 859 467.83285 864 467.985155 863 467.982633 864 467.98375 865 467.983155	Surce 10.125.166.230 10.125.168.230 10.125.168.230 10.125.168.230 10.125.113.234 10.125.12.244 10.125.12.244 10.125.12.244 10.125.12.244 10.125.12.245.200 10.125.13.234 10.125.135 10.125.134 10.125.135 10.125.134 10.125.135 10.125.1	Gambar ja 13.00 0.126.255.255 10.126.255 10.126.255.255 10.126.255.255 10.126.255	Protocol NBNS NBNS NBNS NBNS NBNS NBNS NBNS NBN	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B S/d 15.00 W.I.B 2 Name query NB N5.7ABHXPQ.NET(80) 305 54915 - 54915 Len-263 9 Name query NB D5XTXP-GR0 305 54915 - 54915 Len-263 8 2 5621 - 57621 Len-40 24 Host Announcement HP-R, korkstation, Server, Print Queue Server, NT Workstation 9 Name query NB D5XTAP-GR0 30 Name query NB D5XTAP-GR0 30 Name query NB NS.TAP-GR0 30 Name query NB NB.TAP-GR0 30 Name query NB NB.TAP-GR0 30 Name query NB NB.TAP-GR0 30 Name query NB D5XTAP-GR0 30 Name query NB D5XTAP-GR0 30 Name query NB D5XTAP-GR0 30 Name query NB D5XTAP-GR0 31 Name query NB D5XTAP-GR0 32 Name query NB D5XTAP-GR0 32 Name query NB D5XTAP-GR0 33 Host Announcement AERKU-PC, Workstation, Server, NT Workstation, Potential Browser 65 (TO RETRANSISTION 705 - 1618 (GN) Server, NT Workstation, Potential Browser
No. 1661 1661 1661 1661 1661 1661 1661 16	2. Time 49 466. 963384 450 466. 996693 851 467. 1202478 852 467. 1202478 853 467. 249098 854 467. 249098 854 467. 249098 856 467. 461088 857 467. 348178 859 467. 633849 866 467. 980413 862 467. 981555 863 467. 982643 864 467. 983757 865 467. 986125 865 463. 983757 865 467. 986125 865 465. 983757 865 467. 986125 865 465. 983757 865 467. 986125 865 465. 983757 865 467. 986125 865 465. 983311	Source 10.126.166.239 10.126.166.239 10.126.166.239 10.126.168.239 10.126.111.234 10.126.111.234 10.126.212.224 10.126.211.123 10.126.211.123 10.126.201.99 10.126.245.209 10.126.237.239 10.126.156.23 10.126.155.23 10.126.255.65 10.126.224 10.126.255.65	Gambar ja 13.00 Destination 18.126.255.255 10.126.255.255	+ 4. 2 Protocol INBNS NBNS NBNS NBNS NBNS NBNS NBNS NBNS NBNS NBNS BRONSER TCP UDP	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B B s/d 15.00 W.I.B 9 Name query NB M5.28BNCQ.NETC09 92 Name query NB M5.24BNCQ.NETC09 93 Name query NB D5XTR260 94 Name query NB D5XTR260 95 Name query NB D5XTR260 92 Name query NB D5XTR260 93 Name query NB D5XTR260 94 Name query NB D5XTR260 94 Name query NB D5XTR260 92 Name query NB D5XTR260 92 Name query NB SATA260 93 Name query NB SATA260 94 Name query NB SATA260 94 Name query NB SATA260 95 Name query NB SATA260 95 Name query NB SATA260 94 Name query NB SATA260 94 Name query NB SATA260
No. 166 166 166 166 166 166 166 166 166 16	2. Time 49 466.963384 859 465.996633 851 467.102478 852 467.103642 853 467.249088 854 467.251987 855 467.461088 857 467.462046 856 467.461088 859 467.33340 866 467.636299 861 467.980413 866 467.983555 863 467.983555 863 467.983575 865 467.981555 865 467.981555 865 468.983575 865 468.983575 865 468.983575 865 468.108331 867 468.108331 868 468.20800 868 468.208000 868 468.208000 868 468.208000 868 468.208000 868 468.208000 868 468.2080000000 868 468.208000000000000000000000000000	Source 10.126.168.230 10.126.168.230 10.126.168.230 10.126.168.230 10.126.108.231 10.126.111.234 10.126.12.243 10.126.12.243 10.126.123 10.126.123 10.126.123 10.126.123 10.126.123 10.126.123 10.126.123 10.126.523 10.126.5.55 10.126.12.244 10.126.5.55 10.126.12.245 10.126.5.55 10.126.12.245 10.126.5.55 10.126.12.245 10.126.5.23 10.126.12.245 10.126.5.55 10.126.12.245 10.126.7.2181 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.7.2181 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.12.245 10.126.125.25 10.126.12.245 10.126.12.245 10.126.125.25 10.126.12.245 10.126.125.25 10.126.12.245 10.126.125.25 10.126.125.25 10.126.125.25 10.126.125.25 10.126.12.245 10.126.125.25 10.126.125.25 10.126.125.25 10.126.125.25 10.126.125.25 10.126.125.25 10.126.12.245 10.126.125.25 10.125.25 10.126.125.25 10.125.25 10.125	Gambar ja 13.00 Desthaton 10.126.255.255 10.126 10.126 10.126 10.126 10	+ 4. 2 Protocol NBNS UDP NBNS UDP NBNS NBNS NBNS NBNS BROWSER TCP UDP NBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B B s/d 15.00 W.I.B S s/d 10.00 W.I.B S s/d 15.00 W.I.
No. 166 166 166 166 166 166 166 166 166 16	2. Time 449 466.963384 450 466.996633 451 467.182478 452 467.182478 453 467.249098 454 467.451987 455 467.331408 456 467.451988 456 467.45198 456 467.45198 456 457.45289 464 467.981555 463 467.982633 464 467.981357 465 468.98433 465 468.98433 465 468.98457 465 468.28648 465 468 467	Soure 10.126.156.230 10.126.166.230 10.126.166.230 10.126.166.230 10.126.111.234 10.126.111.234 10.126.111.234 10.126.111.234 10.126.245.200 10.126.111.234 10.126.245.200 10.126.111.234 10.126.237.230 10.126.112.234 10.126.237.230 10.126.112.244 10.126.237.245 10.126.237.245 10.126.237.245 10.126.237.245 10.126.237.245	Gambar ja 13.00 18.126.25.25 10	+ 4. 2 Protocol IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS IBNS BROWSER TOP IBNS BROWSER TOP IBNS BROWSER TOP IBNS ICHS ICHS IBNS ICH	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B C State St
No. 164 164 164 164 164 164 164 164 164 164	2 Time 49 466.963384 659 466.996633 651 467.102478 652 467.102478 653 467.24998 654 467.51987 655 467.461084 658 467.632911 658 467.632418 658 467.632418 659 467.33340 660 467.980413 661 467.980413 663 467.981555 663 467.982603 663 467.982603 664 465.983757 865 467.98155 865 468.248824 667 468.148331 868 468.226606 899 468.248825 809 468.248855 809 468.248855 809 468.248855 809 468.248855 809 468.248855 809 468.248855 809 468.	Source 10.126.168.239 10.126.168.239 10.126.168.239 10.126.168.239 10.126.111.234 10.126.122.24 10.126.122.24 10.126.122.24 10.126.237.451 10.126.237.239 10.126.156.239 10.126.156.239 10.126.155.23 10.126.155.23 10.126.155.23 10.126.155.23 10.126.155.23 10.126.155.23 10.126.155.23 10.126.155.23 10.126.152.24 10.126.237.431 10.126.73.63 10.126.75.75 10.126.75.75 10.126.75.75 10.126.75.75 10.126.75.75 10.1	Gambar Ja 13.00 Destination 10.126.255.255 10.255 10.255 10.255 10.255	+ 4. 2 Protocol Protocol NBNS UDP BROWSER NBNS UDP BROWSER NBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B B s/d 15.00 W.I.B S s/d 15.00 W.I.B P lane query HB M3.280x00.HET603 20 lane query HB M3.280x00.HET603 20 lane query HB M3.7280x00.HET603 20 lane query HB D5XTAP.600 20 lane query HB M5.7280 20 lane query HB M5.7780 20 la
No. 166 166 166 166 166 166 166 166 166 16	2. Time 9466.963384 659 466.996633 951 467.182478 952 467.183428 954 467.251987 955 467.34108 954 467.45294 956 467.461089 957 467.462846 959 467.333440 960 467.632291 961 467.980413 962 467.981555 963 467.981555 963 468.981555 963 468.981555 964 468.48153312 965 468.193311 967 468.193312 966 468.248422 970 468.355129 971 458.355129 971 458	Sure 19.126.168.230 19.126.168.230 19.126.168.230 19.126.168.230 19.126.168.230 19.126.128.125 19.126.122.24 19.126.122.24 19.126.122.24 19.126.121.123 19.126.234.63 19.126.234.63 19.126.234.63 19.126.234.63 19.126.235.200 19.126.156.23 19.126.25.65 19.126.25.65 19.126.21.244 19.126.25.65 19.126.21.244 19.126.25.65	Gambar ja 13.00 Desthaton 10.126.255.255 10	+ 4. 2 Protocol NBNS NBNS NBNS NBNS NBNS NBNS NBNS NBNS NBNS NBNS NBNS NBNS BRONSER TCP UDP NBNS BRONSER TCP UDP NBNS BRONSER TCP UDP NBNS NBN	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B B s/d 15.00 W.I.B S s/d1 5.00 W.I.
No. 166 166 166 166 166 166 166 166 166 16	2. Time 49 466.963384 850 466.996693 851 467.102478 852 467.102478 853 467.249098 854 467.249098 854 467.351987 855 467.34108 855 467.34108 856 467.45108 856 467.452046 857 467.452046 864 467.981555 863 467.981255 863 468.220609 869 468.220809 869 468.220809 869 468.220809 869 468.220809 869 468.220809 869 468.235129 870 468.355129 871 4714	Source 10.126.156.239 10.126.156.239 10.126.156.239 10.126.164.239 10.126.111.234 10.126.111.234 10.126.111.234 10.126.211.234 10.126.245.209 10.126.245.209 10.126.245.209 10.126.255.65 10.126.257.3181 10.126.257.3181 10.126.257.3181 10.126.27.3181 10.276.27.3181 10.126.27.3181 10.1	Gambar ja 13.00 Destination 10.126.255.255	+ 4. 2 Protocol IBNS HBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B B s/d 15.00 W.I.B V Image query NB M5.288x00,NET(00) 22 Name query NB M5.288x00,NET(00) 23 Name query NB M5.2784x00,NET(00) 24 Name query NB D5XTR-060 25 Name query NB D5XTR-060 24 Host Announcement NP-PC, Workstation, Server, Print Queue Server, NT Workstation 29 Name query NB D5XTR-060 29 Name query NB D5XTR-060 29 Name query NB D5XTR-060 20 Name query NB D5XTR-060 20 Name query NB D5XTR-060 20 Name query NB D5XTR-060 20 Name query NB D5XTR-060 24 Host Announcement ACERU-PC, Workstation, Server, NT Workstation, Potential Browser 26 TGF4 Retransistory 50075 - 4.056 (SYN) Sequel Nim-66440 Leneo N5551460 (IS=256 SAU, PENIIS 29 Name query NB D5XTR-060 24 Name query NB D5XTR-060 24 Name query NB D5XTR-060 25 Name servery NB D5XTR-060 20 Name query NB NB NSTR-060 20 Name qu
No. 166 166 166 166 166 166 166 166 166 16	Time 1000 400 400 400 400 400 400 401 401 401 402 401 401 401 401 401 401 401 401 401 401 401 401 401 401 401 401 401 401 401 402 403 404 401 401 401 401 401 402 403 404 404 404 405 401 402 403 404 404 404	Source 10.126.168.230 10.126.168.230 10.126.168.230 10.126.168.230 10.126.108.132 10.126.111.234 10.126.112.244 10.126.7.2.181 10.126.128.209.99 10.126.168.230 10.126.158.230 10.126.158.230 10.126.158.23 10.126.255.65 10.126.255.65 10.126.255.65 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181 10.126.27.181	Gambar Ja 13.00 Destination 10.126.255.255	+ 4. 2 Protocol HBNS UDP HBNS UDP HBNS HBNS HBNS HBNS BROWSER TCP UDP HBNS HBNS BROWSER TCP UDP HBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B S s/d 15.00 W.I.
No. 1661 1666 1666 1666 1666 1666 1666 16	2. Time 449 466.963384 450 466.996633 451 467.102478 452 467.103472 453 467.249098 454 467.451088 457 467.461088 457 467.461088 456 467.451088 456 467.451088 456 467.451088 456 467.981555 463 467.981555 463 467.981555 463 467.981555 463 467.981555 465 468.48574 467 468.19331 468 468.29606 468.355129 471 468.355129 471 468.355129 472 468.353129 473 468.355129 473 473 473 473 473 473 473 473 473 473	Source 10.126.126.230 10.126.126.230 10.126.126.230 10.126.126.230 10.126.111.234 10.126.111.234 10.126.111.234 10.126.111.234 10.126.237.230 10.126.111.234 10.126.247.200 10.126.111.234 10.126.237.230 10.126.111.234 10.126.237.230 10.126.111.234 10.126.237.230 10.126.112.244 10.126.237.230 10.126.112.244 10.126.237.33 10.126.112.244 10.126.237.33 10.126.112.245 10.126.237.33 10.126.12.145 10.126.237.33 10.126.12.145 10.126.237.33 10.126.12.145 10.126.237.33	Gambar Ja 13.00 Destination 10.126.255.255	+ 4. 2 Protocol IBNS HBNS HBNS UDP BROKSER HBNS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B C Solar State St
No. 1661 1661 1661 1661 1661 1661 1661 16	2. Time 449 466.963384 459 466.996633 451 467.102478 452 467.102478 452 467.103642 453 467.24998 454 467.251987 455 467.34198 456 467.46108 457 467.462046 47.462046 47.462046 47.462046 47.462046	Source 10.126.166.239 10.126.166.239 10.126.166.239 10.126.166.239 10.126.161.234 10.126.111.234 10.126.212.224 10.126.212.244 10.126.201.293 10.126.201.293 10.126.201.293 10.126.201.293 10.126.201.293 10.126.212.244 10.126.237.238 10.126.212.244 10.126.237.238 10.126.212.244 10.126.237.238 10.126.212.244 10.126.277.431 10.126.27.363 10.126.27.363 10.126.237.394 10.126.2	Gambar Ja 13.00 Destination 10.126.255.255	+ 4. 2 Protocol INBIS NENS	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B B s/d 15.00 W.I.B 20 Imme query NB NS.ZBRNCO.NET.080 20 Imme query NB DS.TAP.080 20 Imme query NB DS.TAP.080 20 Imme query NB STAP.080 20 Imme query NB ISTAP.080
No. 166 166 166 166 166 166 166 166 166 16	2. Tme 484 466.963384 489 466.963384 489 466.996633 851 467.102478 852 467.103642 853 467.24908 854 467.42946 854 467.451987 855 467.34108 858 467.462046 858 467.462046 858 467.34108 859 467.33340 960 467.45299 961 467.980413 966 467.45299 961 467.981555 963 467.982603 964 468.103331 965 467.981555 963 468.103351 965 468.488.20600 969 468.248422 970 468.355129 971 468.355135 872 468.558373 873 468.559726 975 468.558373 873 468.559726 975 468.558328	Soure 10.126.168.230 10.126.168.230 10.126.168.230 10.126.168.230 10.126.168.230 10.126.112.34 10.126.122.24 10.126.122.24 10.126.122.24 10.126.123.20 10.126.111.234 10.126.209.99 10.126.25.25 10.126.25 10.126	Gambar ja 13.00 Destination 10.126.255.255	+ 4. 2 Protocol Hotosol Hot	Pukul 11.00 W.I.B – 12.00 W.I.B B s/d 15.00 W.I.B S s/d 10.00 W.I.B S s/d 15.00 W.I.

Gambar 4. 3 Pukul 13.00 W.I.B s/d 14.00 W.I.B

lo.	Time	Source	Destination	Protocol Length Info	^
1787	78 529.459661	10.126.33.56	10.126.255.255	BROWSER 243 Host Announcement DESKTOP-POT53IJ, Workstation, Server, NT Workstation, Potential B	rowser
1787	79 529.671701	10.126.245.200	10.126.255.255	NBNS 92 Name query NB BRWFC017C4B252E<00>	
1788	30 529.675647	10.126.162.73	10.126.255.255	NBNS 110 Registration NB WORKGROUP<00>	
1788	81 529.678173	10.126.145.249	10.126.255.255	NBNS 92 Name query NB ISATAP<00>	
1788	32 529.680600	10.126.8.229	10.126.255.255	NBNS 92 Name query NB WPAD<00>	
1788	83 529.714083	10.126.173.96	10.126.255.255	NBNS 92 Name query NB WPAD<00>	
1788	84 529.715169	10.126.173.96	10.126.255.255	NBNS 92 Name query NB WPAD<00>	
1788	85 529.716365	10.126.173.96	10.126.255.255	NBNS 92 Name query NB WPAD<00>	
1788	36 529.870324	10.126.193.111	10.126.255.255	BROWSER 243 Host Announcement ARYANDISCOUT24, Workstation, Server, NT Workstation, Potential Br	owser
1788	87 529.870934	10.126.12.146	192.168.1.255	TCP 66 [TCP Retransmission] 59079 → 1688 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_	PERM=1
1788	88 529.871224	10.126.208.105	10.126.255.255	NBNS 92 Name query NB 5ISOHU.COM<00>	
1788	39 530.080385	10.126.183.152	10.126.255.255	UDP 305 54915 → 54915 Len=263	
1789	0 530.083206	10.126.72.181	10.126.255.255	UDP 305 54915 → 54915 Len=263	
1789	91 530.183475	10.126.38.162	10.126.255.255	NBNS 92 Name query NB WPAD<00>	
1789	92 530.190550	10.126.127.233	10.126.255.255	BROWSER 240 Browser Election Request	
1789	93 530.191676	10.126.208.191	10.126.255.255	NBNS 92 Name query NB WPAD<00>	
1789	94 530.203908	10.126.93.57	10.126.255.255	UDP 1462 889 → 889 Len=1420	
1789	95 530.2880 35	10.126.8.214	10.126.255.255	NBNS 92 Name query NB WPAD<00>	
1789	96 530.289212	10.126.245.200	10.126.255.255	NBNS 92 Name query NB BRWFC017C4B252E<00>	
1789	97 530.335871	10.126.123.122	10.126.255.255	NBNS 92 Name query NB ISATAP<00>	
1789	98 530.337026	10.126.8.214	10.126.255.255	NBNS 92 Name query NB WPAD<00>	
1789	99 530.338222	10.126.8.214	10.126.255.255	NBNS 92 Name query NB WPAD<00>	
1790	00 530.402628	10.126.40.75	255.255.255.255	UDP 82 57621 → 57621 Len=40	/
1790	01 530.404952	10.126.173.96	10.126.255.255	NBNS 92 Name query NB WPAD<00>	
1790	02 530.406069	10.126.173.96	10.126.255.255	NBNS 92 Name query NB WPAD<00>	
1790	03 530.456067	10.126.162.168	10.126.255.255	NBNS 92 Name query NB 5ISOHU.COM<00>	
1790	04 530.604446	10.126.47.112	10.126.255.255	NBNS 92 Name query NB WORKGROUP<1c>	
1700	05 530,923013	10.126.8.229	10.126.255.255	NBNS 92 Name query NB WPAD<00>	

Gambar 4. 4 Pukul 14.00 W.I.B s/d 15.00 W.I.B

c. Packet Sniffing

Penelitian ini di lakukan untuk dapat melihat informasi penting seperti *acoount username, password,* akses DNS yang akan di tuju dan informasi lainnya. Penelitian ini dilakukan agar penyerang dapat melakukan akses internet secara tidak sah dan untuk menguntungkan diri sendiri tapi dapat merugikan bagi orang lain yang menggunakan jaringan yang sama dengan penyerang. Pada penelitian ini penyerang berhasil mendapatkan beberapa *username* dan *password* dari salah satu pengguna yang berada didala jaringan. Dengan demikian penulis dapat memberi pernyataan bahwa jaringan dapat terekam dengan mudah dan dapat dicuri yang hanya menguntungkan diri sendiri.

Skenario dimana penyerang sedang melakukan penyerangan dengan membagi kelompok target menjadi dua kelompok yaitu target 1 dan target 2 dimana target 1 atau target utama tidak merespon atau tidak melakukan aktifitas apapun maka penyerang akan langsung otomatis berpindah ke target 2 begitu pula sebaliknya hingga penyerang dapat merekam semua akses dan aktifitas yang berjalan pada target.

Karena dalam penyerangan ini selama beberapa jam kerja penyerang tidak menemukan aktifitas yang sedang mengakses seperti email dan password, maka penyerang melakukan 1 skenario lagi yaitu :

- a. Berikut langkah langkah dari skenario yang dilakukan:
 - 1. Penyerang memastikan target berada didalam satu jaringan yang sama dengan penyerang
 - 2. Penyerang mencari sebuah website yang tidak memiliki sistem keamanan yang terenkripsi
 - 3. Penyerang melakukan login pada sistem informasi tersebut.
 - 4. Akun yang di coba login adalah akun yang salah karena penyerang hanya mencoba sistem keamanan website tersebut.
 - 5. Penyerang berhasil merekam beberapa aktifitas dari target yang sudah masuk dengan menggunakan software *wireshark*.
- b. Hasil penyerangan skenario yang dilakukan penyerang
 - 1. Memastikan penyerang berada dalam jaringan yang sama dengan target pada aplikasi *wireshark*. Seperti gambar 4.5.



Gambar 4. 5 Tahap Penyerangan Pertama Identifikasi Jaringan Wifi

2. Setelah memilih jaringan yang ingin diiginkan penyerang dapat

melihat aktifitas jaringan tersebut seperti gambar 4.6.

🧧 Captu	ring from Wi-Fi					
<u>F</u> ile <u>E</u> dit	<u>V</u> iew <u>G</u> o <u>C</u>	apture <u>A</u> nalyze <u>S</u> tatistic	s Telephon <u>y W</u> ireless	<u>T</u> ools <u>H</u> elp		
🦾 🔳 🙋		٩ ⇔ ⇔ 🕾 آ	े 👲 📃 📃 🔍 Q, 🖲	Q 🖽		
Apply a	display filter <ctri< td=""><td>I-/></td><td></td><td></td><td> E</td><td>xpression +</td></ctri<>	I-/>			E	xpression +
No.	Time	Source	Destination	Protocol L	ength Info	1
153	18.281434	10.126.239.6	192.168.1.255	ТСР	66 [TCP	Retransmis
154	18.384127	10.126.51.128	255.255.255.255	UDP	82 57621	l → 57621 L
155	18.464001	45.56.90.99	10.126.239.6	TLSv1.2	406 Appli	ication Dat
156	18.465124	45.56.90.99	10.126.239.6	TLSv1.2	85 Encry	pted Alert
157	18.465126	45.56.90.99	10.126.239.6	TCP	54 445 -	> 50138 [FI
150	18 470838	10.126.239.6	45.56.90.99	тср	54 50130	$3 \rightarrow 443$ [AC
160	18.675106	45.56.90.99	10.126.239.6	тср	54 443 -	> 50138 [AC
1		MERSI	MO ISLAMD,		4	
<		INIVE	- MA	11-		
> Frame	1: 92 bytes of	n wire (736 bits), 92	bytes captured (736	bits) on i	nterface 0	
> Etherr	net II, Src: L:	iteonTe_0d:fa:09 (ac:	e0:10:0d:fa:09), Dst:	Broadcast	(ff:ff:ff	:ff:ff:ff)
> Interr	net Protocol V	ersion 4, Src: 10.126	.38.69, Dst: 10.126.2	55.255		
> NetBT(S Name Service	coi, Src Port: 137, D	st Port: 157			
/ Netbit	5 Name Service		(1) Y	-	1	
				~ 1		
					1	
			9100 2 2			
		AL 4 131	free and the second		-	
0000 ff	ff ff ff ff ff f	ff ac e0 10 0d fa 09	08 00 45 00	·····E·		
0010 00 0020 ff	ff 00 89 00 8	9 00 3a ac 75 cf 3e	01 10 00 01 ·····			
0030 00	00 00 00 00 00	00 20 45 4a 46 44 45	42 46 45 45	E JFDEBFEE		
0040 42	46 41 43 41 4	43 41 43 41 43 41 43	41 43 41 43 BFACAC	AC ACACACA		
0050 41	. 43 41 43 41 4	1 41 00 00 20 00 01	ACACAA	A		
				1	1	
		PEL	ARU		1	
		SKA	NBAD	~	1	
		1 70	Test Au	5	/	
		h				
		Oh.	1 P.C.	0		
		M h				

Gambar 4. 6 Aktifitas Jaringan Wifi Pada Aplikasi Wireshark

3. Setelah itu penyerang dapat mencari website yang tidak memiliki keamanan yang terenkripsi. Dan setelah penyerang dapat website yang tidak memiliki system keamanan terenkripsi penyerang dapat mengisi kolom *username* dan *password* yang salah karena system akan tetap membaca apapun yang terisi pada sistem yang akan diserang. Contoh website yang tidak terenkripsi dapat dilihat pada gambar 4.7.



Gambar 4. 7 Website Yang Tidak Memiliki Sistem Terenkripsi

4. Setelah itu penyerang dapat melihat aktifitas pada *website* pada aplikasi *wireshark*. Seperti gambar 4.8.

	*Wi-Fi												_		\times
<u>F</u> ile	<u>E</u> dit <u>V</u> iev	v <u>G</u> o	<u>C</u> aptu	re <u>A</u> i	nalyze	<u>S</u> tatisti	cs Tele	phony	<u>W</u> irele	ess <u>T</u> o	ols <u>F</u>	lelp			
		015	× C	9	⇔ ⇒	2 (F 🕹 🛛		⊕ ∈	e, e,) (
A	pply a display	filter <(Ctrl-/>									C	- E	expression	+
No.	Time		Sou	urce			Destin	ation		P	rotocol	Length	Info		^
	1135 83.60	00515	10	.126.2	239.6		36.91	.206.1	09	I	CMP	74	Echo	(ping)	
	1136 83.6	10630 35715	10	.91.20	184,122)	10.12	6.239.	255	N	BNS	92	Name	(ping) query	
	1138 84.60	3661	10	.126.1	175.150		10.12	26.255.	255	В	ROWSE	R 243	Host	Announ	
	1139 84.7	37638	36	.89.22	20.104		10.12	26.239.	6	Т	СР	62	[TCP	Retran	
	1140 84.73	37714	10	.126.2	239.6		36.89	220.1	04	T	CP	54	[TCP	Dup AC	=_
Ĺ	1142 85.02	24484	10	.126.3	38.69	OT	10.12	6,255.	255	N	BNS	92	Name	query	
<	4442 07 07		- 10		NE	1911	-	State	TH A	RIA.		7	-	>	Ť
> F	rame 1: 92	bytes	on wi	ire (7	36 bit	s), 92	2 bytes	captur	red (7	736 bit	ts) or	1 inter	face @)	
> E	thernet II	, Src:	Lited	onTe_0	d:fa:0	9 (ac:	e0:10:	0d:fa:0	09), C	Dst: Bi	roadca	ast (ff	:ff:ff	F:ff:ff	:ff)
> 1	internet Pr	otocol	Versi	ion 4,	Snc:	10.126	.38.69	, Dst:	10.12	26.255	. 255		11		
> U > N	lser Datagr letBTOS Nam	am Prot ne Servi	tocol, ice	, Src	Port:	137, 0	ost Por	t: 137				7			
		0				•	TTT				2	1			
							111								
				12	-11	12	210	5.5							
		0		116	1	13	311	63	2	5		0			
				-						-	-	1	-		
000	0 11 11 1 0 00 4e 3	f ff ff f 41 00	00 8	ic e0 0 11	10 0d	ta 09 0a 7e	26 45	45 00 0a 7e	N?	Α		E · N			
002	0 ff ff 0	0 89 00	89 0	0 3a	ac 75	cf 3e	01 10	00 01			·u·>·				
003	0 00 00 0 0 42 46 4	0 00 00	00 2	0 45	4a 46	44 45	42 46	45 45	BEA		JFDEB	BFEE			
005	0 41 43 4	1 43 41	41 4	1 00	00 20	00 01	- 17	41 45	ACA		· · · ·				
					10		MЦ								
					PF	EK I	A & 17	AN	2U						
			1			-rv	1/1	Shi	-		1				
							1.1.	20			~	-77			
							100					9			
				Ja.							4				
0	🛛 wiresha	rk Wi-Fi	20 19092	2809000	00 a0617	76.pcapn	q	Packet	ts: 114	3 • Displa	yed: 11	143 (100.0)%) F	Profile: De	fault
					100										

Gambar 4. 8 Aktifitas Website Pada Aplikasi Wireshark

5. Jika pada aktifitas *wireshark* penyerang tidak dapat melihat IP dari *Website* yang akan di serang maka penyerang bisa melihat IP *website* melalui *command prompt*, seperti gambar 4.9.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Users\Asus>ping portalmhs.stia-lk-dumai.ac.id
Pinging portalmhs.stia-lk-dumai.ac.id [36.91.206.109] with 32 bytes of data:
Reply from 36.91.206.109: bytes=32 time=7ms TTL=60
Reply from 36.91.206.109: bytes=32 time=10ms TTL=60
Reply from 36.91.206.109: bytes=32 time=10ms TTL=60
Ping statistics for 36.91.206.109:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds;
Minimum = 7ms, Maximum = 10ms, Average = 7ms
C:\Users\Asus>
```

Gambar 4. 9 Hasil Pencarian IP Website Pada Command Prompt

 Setelah penyerang mendapat IP Website penyerang dapat mencari aktifitas website tersebut di aplikasi wireshark seperti pada gambar 4.10.

																					_	
💻 *W	/i-Fi																			-		×
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	Cap	ture	<u>A</u> n	alyze	<u>S</u> ta	tistic	s T	Telep	hon	у	<u>W</u> irele	ss	[ools	He	elp				
	đ	۲	010		C	8	÷ =	. 🖻	1	J.				⊕ ∈		3 8						
ip.ds	st==3	6.91.2	06.109	&&htt	2						_		_					X		Ex	pression	+
e			Des	tinatio	n			Pro	tocol		enatł	n In	nfo									
26.239	.6		36.	.91.2	06.1	09		HT	TP	-	87	7 P	OST	/log	in Hi	TP/:	1.1	(ap	plica	atio	n/x-w	w-form
26.239	.6		36	91.2	06.1	89	-	HT	ТΡ		50	8 G	ET	/cdn-	cgi/	apps	/hea	d/gm	XC2gl	L9CE	15yG32	ZFrDP6
26.239	.6		36,	91.2	06.1	89		HT	ТΡ	_	47	3 G	ET	/js/s	crip	ts.j	s HT	TP/1	.1		Ĩ.	
26.239	.6		36.	91.2	06.1	39		HT	ТР		53	3 G	ET	/them	e/adı	nin/:	img/	whit	ey.jp	og H	ITTP/1.	1
26.239	.6		36.	91.2	06.1	09		HT	тр		47	3 G	ЕΤ	/js/s	crip	ts.j	s HT	TP/1	.1			
	1		1								75	5						O				
																		м	JA.			
		1	1				-	20	TT	AS	1 1	12	л									
<		127			-	-11	NE	100	111				14	MA	10	-		-	-	6.		>
		75. 6		-	1	744	/701	c. 1.4	+ - >						4	1010	l. d. a	-	-		0	
> Fra	ime 2	./5: 2	5// 0	ytes	on w	ire	(701)		τs),	, ŏ/	0.0	yte	5 0	aptur	ea (7016	DIT	(s) (10.1	teri	race 0	
> Eth	ierne	t 11,	Shc	: L10	eoni	e_2:	ca:	14 (100	220	19:2	5:C	a:1	14), U	st:	100	ssor	_20:	10:4	4 (8	00:00:0	50:20:1
> Int	erne	t Pro	toco	L ver	Deet	4,	Shc:	10.	126.	. 235	.0,	DS	τ: + Γ	36.91	. 200	.109	1	0	1			
	insmi	.5510r	Con		Prot	0001	L, SP	C PO	rt:	LAC	.42,	DS	τr	ort:	00,	seq:	1,	ACK	1,	Len	025	
> нтм	N Fo	icm III		coder	l· an	nlic	atio	o/v-		for	- m - 11	rle	nco	hah		-		-				
< mr				couer	ap	pric	acto	17	mm.	-101	m-u	1 10	nee	Jueu	-	-		1	1			
								100	<u> </u>				_									
								15	8.7	31	15	1							1			
			1		1.1	1.		12	5.8			5						~				
<			1			1		1000	2.00	1.	1/2		2	9				-				>
0000	00	30 88	20 1	10 a4	3c 1	95	09 23	ca	14	08	00	45 (00	· Ø ·	• • <	· ·#		E٠	71			~
0010	03	5f 31	8e 4	10 00	80 (86	d9 bo	l Øa	7e	ef	0 6 :	24	5b	·_1	· @ · ·		• • • •	\$[
0020	ce	6d c3	de (00 50	81	сс	9f 9d	1 30	25	6e	51	50	18	· m ·	••P•	(0%nQ	P٠				
0030	fa	f0 19	96 6	00 00	50 4	4f	53 54	1 20	2f	6c	6f (67	69		· · · P(D ST	/10	gi				
0040	6e	20 48	54 9	54 50	21 .	31	2e 31	L 0d	0a	48	6†	73	74	n H	TTP/:	1.1	··Ho	st				
0050	3a 2d	20 70 Go Gb	6T /	2 74	61 (5C 51	60 20	5 /3	2e	73	60	59	61 0d	: p	dum	L mn	s.st	la d.				
0000	2u Øa	55 73	65 7	72 2d	41	67	65 66	74	3a	20	4d 1	6f (7a	- IK	er-A	a i	ас.1 +• М	07				
0080	69	6c 6c	61	2f 35	2e	30	20 28	3 57	69	6e	64	6f	77	2 11	1/5.0	3 (1	Wind	ow				
0090	73	20 4e	54 2	20 31	30	2e	30 3b	20	57	69	6e :	36	34	s N	Г 10	. 0;	Win	64				
00a0	3b	20 78	36 3	34 3b	20	72	76 3a	36	39	2e	30	29	20	; x	54; i	r v:	69.0)				
00b0	47	65 63	6b (of 2f	32	30	31 30	30	31	30	31 3	20	46	Gec	ko/20	3 10	0101	F				
00c0	69	72 65	66 6	of 78	2f :	36	39 2e	30	Ød	Øa	41 (63 (63	ire	fox/	5 9.0	0 · · A	cc				
00d0	65	70 74	- 3a 2	20 74	65	78	74 21	68	74	6d	6C :	2C	61	ept	te:	x t∕	html	,a				
0000	70	70 60	69 6	5 61	74	09	0T 66	: 21	78	08	/4	od (0C	pp1	ICat:	L ON	/xnt	щт				~
02	Wi	reshar	Wi-Fi	201	.90000	a06	5176.pc	apn	Pac	kets:	: 114	3 · D)ispla	ayed: 5	(0.4%	6) • Dr	oppe	d: 0 ((0.0%)	Pr	ofile: De	fault

Gambar 4. 10 Aktifitas Website Yang Sedang Berjalan

7. Setelah dapat melihat aktifitas apa saja pada website penyerang bisa

dapat melihat aktifitas login website dengan cara seperti gambar 4.11.

- Wi-Fi		- 🗆 XL
<u>File Edit View Go</u> Capture Ana	lyze <u>S</u> tatistics Telephon <u>y</u> <u>W</u> ireless <u>T</u> ools <u>H</u> elp)
🚄 🔳 🖉 🛞 📙 🔜 🔀 🔄 🔍 <	⊨ ⇔ 🔨 🗿 🖢 📃 📃 🭳 Q, Q, II	
ip.dst==36.91.206.109&&http	1	Expression +
Destination	Protocol Length Info	
26.239.6 36.91.206.109	HTTP 877 POST /login HTTP/1 1	(annlication/x-www-form
26.239.6 36.91.206.109	HTTP 508 C Mark/Unmark Packet	Ctrl+M rDP6
26.239.6 36.91.206.109	HTTP 473 C Ignore/Unignore Pack	et Ctrl+D
26.239.6 36.91.206.109	HTTP 533 C Set/Upset Time Refere	inco Ctrl+T
26.239.6 36 .91.206.109	HTTP 473 C Set Offset time Refere	
	lime Shift	Ctrl+Shift+1
	Packet Comment	Ctrl+Alt+C
	ERSTAG TOLA	
< UN		
> Frame 275: 877 bytes on wire	(7016 bits), 877 byte Apply as Filter	
> Ethernet II, Src: LiteonTe_23	ca:14 (3c:95:09:23:0 Prepare a Filter	20:1
> Internet Protocol Version 4,	Snc: 10.126.239.6, D: Conversation Filter	
> Transmission Control Protocol	, Src Port: 50142, D: Conversation Title	
- Hypertext Transfer Protocol	Colorize Conversation	
> HTML Form URL Encoded: applic	ation/x-www-form-urle SCTP	
TCP Stream	Ctrl+Alt+Shift+T Follow	
UDP Stream	Ctrl+Alt+Shift+U	
TLS Stream	Ctrl+Alt+Shift+S	
HTTP Stream	m Ctrl+Alt+Shift+H Protocol Preferences	
0000 00 30 88 20	Decode As	<u>^</u>
0020 ce 6d c3 de 00 50 81 cc	of 9d 30 25 6e 51 50 Show Packet in New W	Vindow
0030 fa f0 19 96 00 00 50 4f	3 54 20 2f 6c 6f 67 09	1
0040 6e 20 48 54 54 50 2f 31	e 31 0d 0a 48 6f 73 74 n HTTP/1 .1 Host	t
0050 3a 20 70 6f 72 74 61 6c 0	d 68 73 2e 73 74 69 61 : portal mhs.stia	a
0000 20 0C 0D 20 04 75 00 01 0 0070 0a 55 73 65 72 2d 41 67	55 5e 74 3a 20 4d 6f 7a User-Ag ent: Mo	7
0080 69 6c 6c 61 2f 35 2e 30	20 28 57 69 6e 64 6f 77 illa/5.0 (Window	W
0090 73 20 4e 54 20 31 30 2e	30 3b 20 57 69 6e 36 34 s NT 10. 0; Win64	4
00a0 3b 20 78 36 34 3b 20 72	76 3a 36 39 2e 30 29 20 ; x64; r v:69.0)	
00b0 47 65 63 6b 6f 2f 32 30 3	31 30 30 31 30 31 20 46 Gecko/20 100101 F	
0010 09 72 05 00 0T 70 2T 30 3 0010 65 70 74 3a 20 74 65 78	74 2f 68 74 6d 6c 2c 61 ent: tev t/html	a
00e0 70 70 6c 69 63 61 74 69 0	of 6e 2f 78 68 74 6d 6c pplicati on/xhtml	1 🗸
wireshark Wi-Fi 201 90000 a061	76. pcapp Packets: 43 · Displayed: 5 (0, 4%) · Dropped:	0 (0.0%) Profile: Default
	orpegning reactor who bisplayed stor (78) bropped.	o (oro /o/) i romer o'erduit 🤐

Gambar 4. 11 Cara Melihat Aktifitas Login Website

8. Selanjutnya tampilan pencarian aktifitas login penyerang dapat mencari melalui *find text* seperti gambar 4.12.

 \wedge POST /login HTTP/1.1 Host: portalmhs.stia-lk-dumai.ac.id User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/ 20100101 Firefox/69.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/ *;q=0.8 Accept-Language: en-US, en; q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 251 Connection: keep-alive Referer: http://portalmhs.stia-lk-dumai.ac.id/logip Cookie: csrf cookie name=bc82a9176ecc98d8e3d47e4de4685f68; ci_session=c85q9jcd6q989318qcbkvmpu81kf7g81 Upgrade-Insecure-Requests: 1 ctoken=bc82a9176ecc98d8e3d47e4de4685f68&proses=6a4c3acdecbaf7ce61ca955 45923128a62fbca186fbed75d932a77a3f2e11712bb81c5dd3e8c58559d89f1d5fed2e a78f2e13d28714bec6bb7fe03940bbf278aTS90cwIurpevQzxSth6inINU6votQeLgDb0 RNEHLIp0%3D&username=denny&password=12345HTTP/1.1 200 OK Date: Sat, 28 Sep 2019 02:00:32 GMT Server: Apache Set-Cookie: csrf_cookie_name=bc82a9176ecc98d8e3d47e4de4685f68; expires=Sat, 28-Sep-2019 04:00:32 GMT; Max-Age=7200; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 1477 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8V.n.6.}.~...!...[W[...FS\$@.4m....Hb."U.Z{.~| G.....T....G.m]....+ce.....Ua.&K..c.|...'f.L.]. L.t6.%..V....D.5...:j0<H0...wV.. 1...o..K>.....U5D=1....*CU....#...A.......#....O.^.../.DHe.....& 2 client pkts, 3 server pkts, 3 turns, ✓ Stream 13 ≑ Show and save data as ASCII Entire conversation (4188 bytes) Find: denny Find Next Filter Out This Stream Print Save as... Back Close Help

Gambar 4. 12 Pencarian Aktifitas Login Melalui Find Text

 \times

4.2 Solusi Untuk Mencegah Serangan Packet Sniffing

Setelah melakukan beberapa penyerangan dan skenario penulis telah menyiapkan beberapa rekomendasi untuk meningkatkan keamanan sebuah jaringan pada wifi yang tanpa pengaman agar terhindar dari suatu serangan seperti yang dapat dilakukan oleh penulis. Untuk dapat menganalisis suatu keamanan jaringan *wifi* yang dapat diterapkan yaitu seperti :

1. Selalu bedakan antara jaringan *wifi* untuk pemakaian kantor dengan *wifi* untuk pengguna umum atau kostumer, karena ketika seorang penyerang atau orang yang tidak bertanggung jawab menggunakan teknik *packet sniffing* seperti yang di lakukan penulis tidak dapat menembus jaringan *wifi* kantor. Secara teknis solusi diatas dapat di lakukan dengan melakukan setting ulang *subnetting*, untuk jaringan *wifi* kantor misalnya dengan IP 192.168.2.1/25 dan untuk jaringan *wifi* umum dengan IP 192.168.3.1/26 untuk 64 host.



Gambar 4. 13 Perbedaan jaringan internet wifi kantor dan umum

Pada gambar 4.13 dijelaskan dengan membedak pemakaian antara jaringan *wifi* kantor dan umum maka serangan *packet sniffing* tidak dapat masuk kedalam jaringan kantor untuk menyadap lalu lintas data yang sedang berjalan, karena secara sistem *packet sniffing* berjalan di layer 2.

2. Binding IP dan Mac Address

Salah satu cara yang digunakan untuk mengatasi *ARP Spoofing* pada suatu jaringan adalah dengan *Binding* IP dan *Mac Address*. Metode ini dapat bekerja dengan cara mendaftarkan setiap pengguna yang terkoneksi dengan jaringan *gateway*. Setiap pengguna diikat IP *address* dan MAC addressnya sehingga *gateway* tidak salah dalam mengirimkan pesan atau paket kepada pengguna, maka *ARP Spoofing* dapat di hindari.

3. Selalu gunakan keamanan enkripsi WPA2-PSK dan radius yang hanya berada di dalam ruangan kantor, karena untuk mengamankan jaringan *wifi* kantor agar sinyal jaringan tidak dapat di jangkau oleh pengguna umum dan hanya karyawan yang mengetahui nya.





BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pembahasan yang sudah penulis lakukan dalam penelitian ini yang berjudul "Analisis Kemanan Jaringan *Wifi* Terhadap Penyerangan Packet Sniffing Pada Kantor PT Indosat Ooredoo Pekanbaru" masih perlu peningkatan keamanan , maka hasil penelitian ini dapat di simpulkan sebagai berikut :

- Penyerangan Packet Sniffing dapat merekam dan menampilkan username dan password target dengan menggunakan aplikasi Wireshark.
- Dengan melakukan penelitian ini pihak kantor PT Indosat Ooredoo Pekanbaru dapat mengetahui bahayanya penggunaan *wifi* tanpa pengaman dan yang berada dalam satu jaringan dengan pengguna umum.
- Pihak kantor PT Indosat Ooredoo Pekanbaru dapat meningkatkan keamanan wifi kantor dengan memisahkan pemakaian wifi kantor dan pengguna umum

5.2 Saran

Simulasi yang penulis lakukan ini sangat jauh dari kata sempurna banyak terdapat kekurangan. Untuk itu penulis sangat perlu pengembangan lebih lanjut agar simulasi isi terlihat sempurna, adapun saran-saran dari simulasi ini agar dapat dipertimbangkan untuk ke depannya adalah sebagai berikut :

- Simulasi ini hanya menggunakan 1 PC untuk menggunakan 2 PC harus menggunakan Operation System (OS) linux sedangkan penulis hanya memakai Operation System (OS) Windows 10.
- 2. Diperlukan pembagian jaringan untuk membedakan pemakaian wifi kantor dan pemakaian wifi umum agar tidak terjadi serangan yang dilakukan melalui jaringan wifi umum oleh pihak yang tidak bertanggung jawab untuk mendapatkan informasi penting demi keuntungan pribadi.
- Diperlukan nya pengamanan wifi berupa WPA2-PSK sebagai keamanan wifi awal untuk dapat meminimalisir terjadi nya packet sniffing.
- 4. Lakukan lah pergantian *password* secara berkala setelah login menggunakan *wifi* umum.
- 5. Lakukan pengecekan jaringan secara berkala untuk menghindari kesalahan/*eror* pada jaringan yang membuat kinerja jaringan menjadi lambat.

DAFTAR PUSTAKA

Rumalutur, Sonny. 2012. "Analisis Keamanan Jaringan Wireless Lan (WLAN) Pada PT.PLN(PERSERO) Wilayah P2B Area Sorong". Sorong : Politeknik Katolik Saint Paul Sorong.

Samsumar, Lalu Delsi. 2017. "Analisis dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (WLAN); Studi Kasus Di Kampus STMIK Mataram". Mataram : STMIK Mataram.

Supriyanto, Aji. 2006. "Analisis Kelemahan Keamanan Pada Jaringan Wireless". Semarang : Tugas Akhir Universitas Stikubank Semarang,

Setiawan, Thomas. 2004. "Analisis Keamanan Jaringan Internet

Menggunakan Hping, Nmap, Nessus, dan Ethereal". Bandung :

Tugas Akhir Institut Teknologi Bandung,

Noviyanto, Hendri. 2011. Analisis Keamanan Wireless di Universitas Muhammadiyah Surakarta. Surakarta : Tugas Akhir Universitas Muhammadiyah Surakarta.

Sinambela, Josua M. 2007. "Hacking Wifi "

Oktavianto, Digit. 2012. "Mencegah ARP Spoofing Dan ARP Poisoning Di Linux "

Fadillah, Fauzan. 2012. "Perancangan dan Analisis Keamanan Jaringan Terhadap ARP Spoofing pada Hotspot ",

Rumalutur, Sonny. 2012. "Analisis Keamanan Jaringan Wireless Lan (WLAN) Pada PT.PLN(PERSERO) Wilayah P2B Area Sorong". Sorong : Politeknik Katolik Saint Paul Sorong.