ANALISIS KEAMANAN FASILITAS JARINGAN *(WI-FI)* TERHADAP SERANGAN PACKET SNIFFING PADA PROTOCOL HTTP DAN HTTPS

SKRIPSI

Diajukan Oleh :

HALIM HUZAIRI
NIM. 170212015

Bidang Peminatan : Teknik Komputer dan Jaringan
Mahasiswa Fakultas Tarbiyah dan Keguruan
Program Studi Pendidikan Teknologi Informasi

UNIVERSITAS ISLAM NEGERI AR-RANIRY

FAKULTAS TARBIYYAH DAN KEGURUAN

PROGRAM STUDI PENDIDIKAN TEKNOLOGI INFORMASI

2023 M/1445 H

SKRIPSI

ANALISIS KEAMANAN FASILITAS JARINGAN *(WI-FI)* TERHADAP SERANGAN PACKET SNIFFING PADA PROTOCOL HTTP DAN HTTPS

Oleh:

HALIM HUZAIRI
NIM. 170212015

Bidang Peminatan : Teknik Komputer dan Jaringan
Mahasiswa Fakultas Tarbiyah dan Keguruan
Program Studi Pendidikan Teknologi Informasi

Bidang Peminatan: Teknik Komputer Jaringan

Disetujui Oleh:

Pembimbing 1	Pembimbing 2
Ridwan, M.T	**Firmansyah, S.Kom., M.T**
NIP. 198402242019031004	**NIP. 198704212015031002**

ANALISIS KEAMANAN FASILITAS JARINGAN *(WI-FI)* TERHADAP SERANGAN PACKET SNIFFING PADA PROTOCOL HTTP DAN HTTPS

SKRIPSI

Telah diuji oleh Panitia Ujian Munaqasyah Skripsi Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry Banda Aceh dan Dinyatakan Lulus serta diterima sebagai salah satu beban studi Program Sarjana (S-1) dalam Pendidikan Teknologi Informasi

Pada :

Rabu, 20 Desember 2023
07 Jumadil Akhir 1445 H

Darussalam – Banda Aceh
Panitia Ujian Munaqasyah Skripsi

Ketua	Sekretaris
Ridwan, M.T	**Firmansyah, S.Kom., M.T**
NIP. 198402242019031004	NIP. 198704212015031002
Penguji 1	Penguji 2
Aulia Syarif Aziz, S.Kom., M.Sc	**Sarini Vita Dewi, S.T., M.Eng**
NIP. 199305212022031001	NIP. 197312222022032001

Mengetahui,
Dekan Fakultas Tarbiyah Dan Keguruan UIN Ar-Raniry
Darussalam, Banda Aceh

Prof. Safrul Muluk, S.Ag., M.A., M.Ed., P.Hd
NIP. 197301021997031003

LEMBAR PERNYATAAN KEASLIAN KARYA ILMIAH

Yang bertanda tangan dibawah ini:

Nama : Halim Huzairi
NIM : 170212015
Program Studi : Pendidikan Teknologi Informasi
Fakultas : Tarbiyah dan Keguruan
Judul Skripsi : ANALISIS KEAMANAN FASILITAS JARINGAN (*WI-FI)* TERHADAP SERANGAN SNIFIING PADA PROTOCOL HTTP DAN HTTPS

Dengan ini menyatakan bahwa dalam penulisan Skripsi ini, saya:

1. Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan mempertanggung jawabkan.
2. Tidak melakukan plagiat terhadap Naskah karya orang lain
3. Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya
4. Tidak memanipulasi dan memalsukan data
5. Mengerjakan sendiri karya ini dan mampu bertanggung jawab atas karya ini

Bila di kemudian hari ada tuntutan dari pihak lain atas karya saya dan telah melalui pembuktian yang dapat dipertanggung jawabkan dan ternyata memang ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap dikenai sanksi berdasarkan aturan yang berlaku di Fakultas Tarbiyah dan Keguruan UIN Ar-Raniry Banda Aceh

Demikian Pernyataan ini saya buat dengan sesungguhnya.

Banda Aceh, 5 Desember 2023
Yang Menyatakan

Halim Huzairi

ABSTRAK

Nama : Halim Huzairi
NIM : 170212015
Fakultas/Prodi : Tarbiyah dan Keguruan/Pendidikan Teknologi Informasi

Judul : Analisis Keamanan Fasilitas Jaringan (*wi-fi*) Terhadap Serangan Packet Sniffing Pada Protocol HTTP dan HTTPS

Bidang Peminatan : Teknik Komputer Jaringan (TKJ)
Pembimbing I : Ridwan, M.T
Pembimbing II : Firmansyah, S.Kom, M.T
Kata Kunci : HTTP, HTTPS, Sniffing, Wireshark, Burpsuite

Jaringan *computer* bukanlah sesuatu yang baru saat ini, hampir disetiap tempat banyak terdapat jaringan komputer untuk memperlancar arus informasi pada tempat tersebut. Di dalam sebuah jaringan *computer* banyak sekali paket data yang berlalu lalang pada kabel jaringan, baik itu paket data yang mengandung informasi-informasi penting yang bersifat pribadi yaitu nama dan *password*, alamat dari sebuah situs, ip anddres user dan lain – lain. Dengan tingkat keamanan yang dilengkapi keamanan tambahan ialah *Secure Socket Layer (SSL)* atau *Transport Layer Security (TLS).* Pada *Secure Socket Layer (SSL)* berguna untuk mengkripsi proses-proses autentifikasi yang terjadi pada weib browser. Bagaimana bentuk penyerangan sniffing pada web yang di security dan web yang tidak di security dan bagaimana perbandingan antara ke 2 kondisi tersebut. Metode penelitian deskriptif adalah salah satu metode yang digunakan pada penelitian yang bertujuan menjelaskan suatu kejadian, atau suatu metode dalam penelitian status sekelompok manusia, suatu objek, suatu set kondisi, suatu system pemikiran apapun suatu kelas peristiwa pada masa sekarang. Kedua *tools* yang digunakan mampu menjalankan fungsinya masing – masing pada kedua protocol yang di serang oleh packet sniffing. Kondisi dari website dengan protocol HTTP dan HTTPS saat terkena serangan packet sniffing, yaitu tools burpsuite dapat merekam jejak dari aktivitas target saat mengakses website yang sudah terenkripsi sertifikat CA yang mana tools ini dapat melihat dan membaca pesan request dan response antara web browser dan web server yang terjadi dalam internet. Pada penyerangan website HTTP tools wireshark juga mampu merekam serta menampilkan username dan password dikarenkan tidak adanya enkripsi saat web browser dan web server melakukan komunikasi.

KATA PENGANTAR

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

Segala puji beserta syukur kita ucapkan atas kehadirat Allah SWT. dengan segala rahmat dan hidayah-Nya sehingga kita dapat meraskaan nikmatnya Iman dan Islam dalam kehidupan saat ini, tak lupa pula shalawat beriring salam kepada Baginda Rasulullah Muhammad SAW yang menjadi penerang dalam kehidupan, menjadi purnama yang hangat ditengah sejuknya malam, dan menjadi suri tauladan sebagai sebaik-baik tauladan bagi umat manusia, sehingga penulis dapat menyelesaikan Skripsi yang berjudul **"Analisis Keamanan Fasilitas Jaringan (*wi-fi*) Terhadap Serangan Packet Sniffing Pada Protocol HTTP dan HTTPS"** dengan sebaik-baiknya.

Penulisan skripsi ini merupakan salah satu syarat penting yang harus diselesaikan untuk mendapatkan gelar sarjana oleh setiap mahasiswa Program Studi Pendidikan Teknologi Informasi Fakultas Tarbiyah dan Keguruan Universitas Islam Negeri Ar-Raniry Banda Aceh. Dengan segala upaya yang telah dilakukan dalam menyelesaikan skripsi ini, penulis juga menyadari sepenuhnya bahwa masih terdapat beberapa kekurangan baik dari hal penyusunan dan aspek lainnya. Dalam proses penulisan skripsi ini, tentunya terdapat banyak kesulitan dan tantangan yang dihadapi, baik dari segi penulisan, ekstraksi file, penyusunan data dan proses analisis data yang memakan waktu lama. Berkaitan hal tersebut,

proses penulisan skripsi ini juga adanya dukungan dan bantuan dari dari berbagai pihak.

Berkenaan dengan hal tersebut, maka penulis menyampaikan ucapan terima kasih kepada:

1. Kedua orang tua beserta keluarga yang selalu memberikan dukungan serta senantiasa mendoakan yang terbaik.
2. Rektor UIN Ar-Raniry Banda Aceh, Bapak Prof. Dr. Mujiburrahman, M.Ag.
3. Dekan Fakultas Tarbiyah dan Keguruan Universitas Islam Negeri Ar-Raniry Banda Aceh, Bapak Safrul Muluk, S.Ag., M.A., M.Ed., PhD.
4. Ketua Program Studi Pendidikan Teknologi Informasi Ibu Mira Maisura, M.Sc.
5. Sekretaris Program Studi Pendidikan Teknologi Informasi Bapak Ridwan, M.T.
6. Pembimbing 1 yaitu Bapak Ridwan, M.T dan juga Pembimbing 2 yaitu Bapak Firmansyah, S.Kom., yang telah meluangkan waktu dan memberikan saran serta motivasinya dan membimbing penulis dalam menyelesaikan penulisan skripsi ini.
7. Penguji 1 Bapak Aulia Syarif Aziz, S.Kom., M.Sc., serta Penguji 2 Ibu Sarini Vita Dewi, S.T., M.Eng. yang telah memberikan banyak masukan dan saran demi tercapainya kesempurnaan skripsi ini.

8. Staf Program Studi Pendidikan Teknologi Informasi yang telah membantu proses pelaksanaan penelitian untuk penulisan skripsi ini.
9. Dan semua pihak, secara langsung maupun tidak langsung, yang tidak dapat disebutkan di sini. Atas bantuan dan perhatiannya selama penyusunan Skripsi ini.

Berbagai upaya yang telah dilakukan dalam menyelesaikan skripsi ini, penulis menyadari sepenuhnya dalam penulisan skripsi ini masih banyak terdapat kekurangan baik dalam penulisan maupun isi.

Oleh karena itu, penulis mengharapkan kritik dan saran yang bersifat membangun agar dapat dijadikan masukan dan referensi untuk perbaikan skripsi lanjutan di masa berikutnya. Semoga Allah SWT meridhai segala penulisan skripsi ini dan dapat bermanfaat bagi kita semua. Aamiin

Banda Aceh, 5 Desember 2023

Penulis,

Halim Huzairi

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABLE

BAB I

PENDAHULUAN

1.1.Latar Belakang

Jaringan *computer* bukanlah sesuatu yang baru saat ini, hampir disetiap tempat banyak terdapat jaringan *computer* untuk memperlancar arus informasi pada tempat tersebut. Di dalam sebuah jaringan *computer* banyak sekali paket data yang berlalu lalang pada kabel jaringan, baik itu paket data yang mengandung informasi-informasi penting yang bersifat pribadi yaitu nama dan *password*, alamat dari sebuah situs, *ip anddres* user dan lain – lain. Pada umumnya setiap jaringan yang terhubung memalui internet tingkat keamanannya masih rendah dan tidak selalu aman masih dapat diekplotasi oleh para *hacker*. Dalam pembangunan sebuah perancangan system keamanan jaringan *WI-FI* yang telah terhubung ke internet haruslah diteliti dan dipelajari sehingga dapat dipahami oleh penguna agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan oleh seorang *hacker* yag tidak bertanggung jawab [1].

Dengan meningkatnya kejahatan yang terjadi melalui lalu lintas jaringan yang bersifat bolak-balik, maka telah banyak pada saat ini sebuah *web browser* menggunakan lalu lintas jaringan yang terenkripsi. Setiap *web browser* membutuhkan sebuah *protocol* dalam melakukan transaksi pertukaran data.

Dengan tingkat keamanan yang dilengkapi keamanan tambahan ialah *Secure Socket Layer (SSL)* atau *Transport Layer Security (TLS).* Pada *Secure Socket Layer (SSL)* berguna untuk mengkripsi proses-proses autentifikasi yang terjadi pada *web browser*. Sedangkan *Transport Layer Security (TLS)* untuk mengamankan HTTP menjadi HTTPS [1].

Pada saat ini telah banyak terdapat beberapa teknik penyerangan terhadap *system* keamanan jaringan yaitu memaksa masuk dengan menyerang database *password,* mengirim paket data dalam jumlah yang sangat besar terhadap suatu server, serangan ke amanan jaringan dalam bentuk *smurf attack,* serangan dengan *Spoofing,* Serangan dengan *Man In the midlle,* Serangan dengan *Sniffer,* serangan dengan *cracker,* dan serangan dengan *Spamming* [15].

Untuk mengetahui paket data dan mengontrol pengguna pada jaringan LAN terutama pada saat penggunaan terkoneksi dengan jaringan *wi-fi* yang akan mengakses internet menggunakan *web browser*. Maka dibutuhkan suatu analisis jaringan menggunakan *tools* pihak ketiga oleh *network analyzer* dengan tujuan menganalisa jaringan dengan melakukan pengawasan terhadap pengguna sehingga administrator dapat dengan mudah memonitoring aktivitas – aktivitas yang dilakukan oleh pengguna [15].

Berdasarkan uraian di atas, penulis tertarik untuk mempelajari cara untuk mengamankan jaringan internet untuk judul skripsi “Analisis Kemanan Fasilitas

Jaringan (*WI-FI)* Terhadapat Serangan *Packet Sniffing* Pada *Protocol* HTTP dan HTTPS"

1.2.Identifikasi Masalah

Adapun identifikasi masalah yang dapat di ambil dari latar belakang tersebut adalah sebagai berikut:

1. Kurangnya pemahaman tentang keamanan data di jaringan *computer* oleh administrator dan pengguna computer secara umum, khususnya ancaman terhadap pencurian data pada jaringan *wi-fi* seperti username dan *password.*
2. Kurangnya pemahaman tentang pencegahan bagaimana mengatasi penyadapan terhadap jaringan *wi-fi*
3. Kuranganya pengawasan terhadapa aspek keamanan dalam komunikasi melalui jaringan *computer* karena telah banyak aktivitas pertukaran informasi rahasia internet.

1.3. Rumusan Masalah

Berdasarkan latar belakang yang telah disebutkan, maka permasalahan pada penelitian ini dapat diambil sebuah rumusan masalah yaitu : "

1. Bagaimana bentuk penyerangan sniffing pada web yang di amankan (HTTPS) dan web yang tidak di amankan (HTTP)
2. Bagaimana perbandingan antara web HTTP dan HTTPS tersebut?"

1.4.Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Untuk menguji cara kerja *protocol* yang menggunakan *Secure Socket Layer* (SSL) data dilundungi sebelun dikirim ketujuan maupun sebelum menggunakan *Secure Socket Layer* (SSL) yang pengiriman data nya dalam bentuk *plaint-text* tanpa perlindungan lebih.
2. Untuk membandingkan 2 kondisi bagaimana penyerangan terhadapat web yang di*secure* dan yang tidak di*secure*
3. Untuk menguji seberapa jauh keamanan jaringan *wi-fi* yang terkoneksi dengan internet baik yang menggunakan *Secure Socket Layer* (SSL) maupun yang tidak menggunakan *Secure Socket Layer* (SSL)

1.5.Penelitian Terdahulu

1. Keamanan HTTP dan HTTPS Berbasis Web Menggunakan system Operasi *Kali Linux*

   Menurut Adzan Abdul Zabar (2015), pada penelitian dengan judul keamanan HTTP dan HTTPS Berbasis Web Menggunakan Sistem Operasi *Kali Linux* yang menjelaskan bahwa Aspek kemanan dalam komunikasi melalui jaringan *computer* menjadi semakin penting terutama karena banyaknya aktivitas pertukaran informasi rahasia melalui internet. Untuk menghindari penyadapan atau tindak kejahatan

lainnya. Oleh karena itu, penelitian ini akan membahas beberapa kelemahan yang ada pada internet khususnya pada website melakukan perbandingkan keamanan antara http dan https.

Perbedaan dengan penelitian yang ingin dilakukan oleh penulis ialah penulis tidak hanya melakukan perbandingan keamanan dari kedua *protocol* saja melainkan penulis ingin melakukan perbandingan dengan analisa bagaimana sebuah bentuk atau kondisi penyerangan sniffing terhadapat *protocol* yang di*secure* dan tidak di*secure*.

2. Pemanfaatan Betterceap Sebagai Teknik Snifffing pada paket Traffic Jaringan *Wi-fi*

Penelitian Dian Kurnia (2019) dengan judul Pemanfaatan *Betterceap* Sebagai Teknik *Snifffing* pada paket *Traffic* Jaringan *Wi-fi* ialah adanya perancangan suatu jaringan *wi-fi public* yang terhubung ke internet melalui modem. Jaringan yang telah dibangun dilakukan analisi *traffic* jaringan, *protocol* jaringan dengan teknik – teknik *sniffing*. *Sniffing* difokuskan pada pencarian *username* dan *password* untuk login web dan mencoba mengetahui lebih paket data keluar ketika *user login* pada *page login web* dan keseluruhan aktifitas user dalam mengakses url di *browser*.

Perbedaan keamanan jaringan yang akan penulis kerjakan ialah

penyerang melakukan koneksi dengan *Acces point* dengan melakukan suatu koneksi internet dan penyerang mulai melakukan *scanning user* yang aktif.

3. Analisis Sniffing Password Menggunakan Aplikasi *Cain dan Abel* pada Jaringan *Wi-fi* Universitas Semarang

   Penelitian Susanto (2018) tentang Analisis *Sniffing Password* Menggunakan Aplikasi *Cain dan Abel* pada Jaringan *Wi-fi* Universitas Semarang ialah saat ini Universitas Semarang telah menerapkan jaringan computer kabel maupun nirkabel sebagai media pertukaran data atau informasi pelayanan umum maupun akademik dan informasi penting lainnya. Universitas Semarang juga memiliki jaringan *wi-fi* yang tidak menutup kemungkinan terjadinya serangan pada jaringan tersebut. Sedikit celah dapat dimanfaatkan oleh *hacker* dan *cracker* untuk menembus suatu jaringan. Oleh karena itu peneliti merasa perlu untuk meneliti dan menganalisis serangan *packet* dan *sniffing*.

   Perbedaan serangan jaringan yang penulis kerjakan ialah adanya analisa dalam keamanan jaringan *wireless*. Yang mana jarinagn *wireless* hanya sebagai gerbangnya saja dan data yang akan dicuri ada pada web.

BAB II

LANDASAN TEORI

2.1 Dasar Teori

2.1.1 Konsep Kemanan Jaringan

Penulis memiliki acuan penelitian Noviyanto yang berjudul analisis keamanan *wireless* di universitas Muhamidayah Surakarta yaitu pada saat ini suatu keamanan jaringan sangat penting dan patut di perhatikan, terutama untuk jaringan yang terhubung dengan internet atau *wi-fi* dan memiliki dasar tidak selalu aman dari penyadapan, baik dari jaringan wired LAN maupun *wireless* LAN. Pada pembangunan sebuah *system* keamanan jaringan internet haruslah direncanakan dan dipahami agar dapat melindungi pengguna dan meminimalisir terjadi serangan oleh orang yang tidak bertanggung jawab [2].

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* kemanan jaringan.

2.1.2 Ancaman

Pada dasarnya, ancaman datang dari seseorang yang menpunyai keinginan memperoleh akses illegal ke dalam suatu jaringan *computer*. Oleh karena itu, harus ditentukan siapa saja yang memperoleh mempunyai akses legal ke dalam *system*, dan ancaman-ancaman yang dapat mereka timbulkan. Ada beberapa

tujuan yang ingin dicapai oleh penyusup dan, sangat berguna apabila dapat membedakan tujuan tujuan tersebut pada saat merencanakan system keamanan jaringan computer. Beberapa tujuan para penyusup adalah:

a) Pada dasarnya hanya ingin tahu system dan data yang ada pada suatu jaringan komouter yang dijadikan sasaran. Penyusup yang bertujuan seperti ini sering disebut *the curius.*
b) Membuat *system* jaringan menjadi *down*, atau mengubah tampilan situs web. Penyusup yang mempunyai tujuan seperti ini sering disebut sebagai *the malicious.*
c) Berusaha untuk menggunakan sumber daya di dalam system jaringan *computer* untuk memperoleh popularitas. Penyusup seperti ini sering disebut sebagai *the high-profile intruder.*
d) Ingin tahu data apa saja yang ada di dalam jaringan *computer* untuk selanjutnya dimanfaatkan untuk mendapatkan uang. Penyusup seperti ini sering disebut sebagai *the competition.*

2.1.3 Kelemahan

Kelemahan mengambarkan seberapa kuat *system* keamanan suatu jaringan *computer* terhadap jarinagn *computer* lain, kemungkinan bagi seseorang untuk mendapat akses illegal ke dalamnya.

2.2 Jenis - Jenis Ancaman Kemanan Jaringan

2.2.1 Packet sniffer

Menurut Achmat Rizal Fauzi (2018), *Packet sniffer* ialah suatu teknik pemantauan setiap komunikasi dan transfer data yang melintas pada jaringan dan memonitor semua lalu lintas jaringan. *Packet sniffer* tidak sama dengan jaringan host standar yang hanya menerima dan mengirim lalu lintas khusus. Ancaman keamanan yang disajikan oleh penyadapan adalah kemanpuan mereka untuk menagkap semua lalu lintas masuk dan keluar. Termasuk *password* dan *username* atau bahan sensitive lainnya. Untuk dapat membaca dan menganalisa setiap *protocol* yang melintasi jaringan, diperlukan program yang bias membelokkan paket ke *computer* attacker. Biasa disebut serangan *spoofing*, attacker akan bertindak sebagai *Man-In-the-Middle* (Asrodia & Patel, 2012:1) [3]

2.2.2 ARP spoofing / ARP poisoning

Menurut Achmat Rizal Fauzi (2018), ARP (*Addres Resolution Protocol) poisoning* ini adalah suatu teknik pada jaringan *computer* local baik dengan media kabel atau *wireless,* yang memungkinkan penyerang bias mengendus frame data pada jaringan local dan melakukan modifikasi *traffic* atau bahkan menghentikan *traffic*. *ARP spoofing* merupakan konsep dari serangan penyadapan diantara terhadap dua mesdin yang sedang berkomunikasi atau yang disebut dengan *MITM (Man in The Middlle Attack)* [3].

Prinsip serangan *ARP poisoning* ini memanfaatkan kelamahan pada teknologi jaringan *computer* itu sendiri yang menggunakan *arp broadcast*. *ARP* berada pada layer 2, diamana pada layer dua adalah *MAC address*. Misalnya sebuah *host* (contoh: PC) yang terhubung pada sebuah ILAN ingin menghubungi *host* lain pada *LAN* tersebut, maka dia membutuhkan informasi *MAC address* dari *host* tuuan (Oktavianto, 2012) [4].

2.2.3 Probe

Menurut Rian Eka Fitriani (2019) Sebuah *probe* dapat dikenali dari adanya usaha – usaha yang tidak lazim untuk memperoleh akses ke dalam suatu *system* atau untuk menemukan informasi tentang *system* tersebut. Salah satu contohnya adalah usaha untuk login ke dalam sebuah account yang tidak digunakan. *Probing* dapat dianalogikan sebagai usaha untuk memasuki sebuah ruangan yang dengan mencoba – coba apakah pintunya terkunci apa tidak [4].

2.2.4 Scan

Menurut Rian Eka Fitriani (2019) 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 local maupun *host remote*, IP addrs yang aktif, bahkan bias untuk mengetahui system operasi yang digunakan pada host yang dituju [4].

2.2.5 Account compromise

Menurut Rian Eka Fitriani (2019) *Account compromise* adalah penggunaan *account* sebuah *computer* secara illegal oleh seseorang yang bukan pemilik account tersebut. *Account compromise* dapat mengakibatkan korban mengalami kehilangan atau kerusakan data. Sebuah insiden *Account compromise* dapat berakibat lebih lanjut, yitu terjadinya insiden *root compromise*, yang dapat menyebabkan kerusakan lebih besar [4].

2.2.6 Root compromise

Menurut Rian Eka Fitriani (2019) *Root compromise* mirip dengan *account compromise*, dengan perbedaan *account* yang digunakan secara ilegal adalah *account* yang mempunyai privilege sebagai administrator *system*. Istilah *root* diturunkan dari sebuah *account* pada *system* berbasis UNIX yang mempunyai privilege tidak terbatas. Penyusup yang berhasil melakukan *root compromise* dapat melakukan apa saja pada system yang menjadi korban, termasuk menjalankan program, mengibah kinerja *system*, dan menyembunyikan jejak penyusupan [4].

2.2.7 Denial of service (Dos)

Menurut (Ridwan Nur Wibowo, Parman Sukarno, Edwir Musthofa Jadied 2018).*Denial of service* (Dos) adalah salah satu jenis serangan dimana penyerang menghabiskan sumber daya jaringan *computer*. Dampak dari serangan Dos menyebabkan computer tidak dapat berfungsi dengan normal.

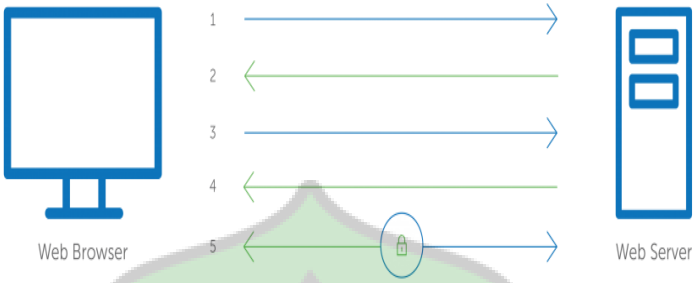
Sumber daya jaringan yang berharga antara lain *computer* dan database, serta pelayanan – pelayanan (service) yang disediakan oleh organisasi pemiliki jaringan. Kebanyakan user jaringan memanfaatkan pelayanan – pelayanan tersebut agar pekerjaan mereka menjadi efesien. Bila pelayanan ini tidak dapat dipergunakan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

a. Kemunginan jaringan menjadi tidak berfungsi karena kebanjiran *traffic*.
b. Kemungkinan ada virus yang menyebar dan menyebabkan *system computer* menjadi lamban atau bahkan lumpuh.
c. Kemungkinan device yang melindungi jaringan dirusak

2.3 Cara Kerja Secure Socket Layer (SSL)

Secure Socket Layer adalah suatu *protocol* yang diciptakan oleh *Netcape* untuk memastikan keamanan dalam bertransaksi di internet antara webserver dan *web browser* dari *client*. *Protocol* ini menggunakan sebuah badan yang biasa disebut CA (*Certificate Authority*) untuk mengidentifikasi memverifikasi pihak – pihak yang bertransaksi (Adzar Abdul Zabar, Fahmi Novianto, 2015). Skema diagram proses SSL *Handshake* dapat dilihat pada gamber 2.1 berikut [5].

Gambar 1 : Gambar proses handshake pada SSL



a. Pada Proses Pertama *client* mengirim pesan ‘Hello’ kepada website yang sudah diamankan dengan *Secure Socket Layer* (SSL). Maka *client* ingin meminta kepada web server untuk melakukan proses identifikasi kepadanya.
b. Pada Proses Kedua kemudian web server akan merespon pesan ‘Hello’ dengan mengirimkan salinan sertifikat *Secure Socket Layer* (SSL), termasuj didalamnya adalah Public key server.
c. Klien melakukan verifikasi sertifikat *Secure Socket Layer* (SSL) server kepada *Certificate Authority*(CA) dan memastikan *Secure Socket Layer* (SSL) tersebut valid, jika proses ini berhasil maka akan dilakukan enkripsi dan dikirimkan kembali dengan *symmetric session key* menggunakan public *key* server.
d. Server kemudian melakukan dekripsi *syimmetric session key* dengan

public key dan mengirimkan kembali kepda klien dengan *session key* untuk memulai *encryption session*

1. Transport Layer Securty (TLS)

Protocol *TLS/SSLI* memiliki dua bagian yang pertama adalah *handshaking protocol*,yang kedua *record protocol*. *Handshaking protocol* menegosiasi *suite cipher*, mengotentikasi *server* dan secara opsional mengotentifikasi klien dan menetapkan *session keys*. Sedangkan *record protocol* mengamankan data aplikasi dengan *session keys* yang dibuat pada *record protocol* dan meverifikasi keaslian dan integritas aplikasi (Turner, 2014) [6].

2. Hipotesis

Hipotesis merupakan jawaban sementara terhadap rumusan masalah penelitian, dimana rumusan masalah penelitian telah dinyatakan dalam bentuk pernyataan. Hipotesis dirumuskan atas dasar kerangka piker yang merupakan jawaban sementara atas masalah yang dirumuskan. Berdasarkan kajian teori dan kerangka berfikir diatas maka dapat dirumuskan hipotesis yaitu dengan adanya sebuah bentuk penyerangan terhadapat protocol yang di*secure* dengan yang tidak di*secure* ini maka orang-orang awam dapat memahami secara terperinci dalam menguji tingkat keamanan sebuah jaringan local *wlan* serta mengetahui bagaimana bentuk atau kondisi sebuah *sniffer* melakukan serangan *sniffing* terhadap website yang memiliki keamanan lebih seperti protocol https dan website yang tidak memiliki keamanan seperti *protocol* http.

BAB III

METODOLOGI PENELITIAN

3.1 Metodologi Penelitian

Metode yang digunakan dalam penelitian ini adalah metode deskriptif. Metode penelitian deskriptif adalah salah satu metode yang banyak digunakan pada penelitian yang bertujuan menjelaskan suatu kejadian. Seperti yang dikemukakan oleh Moh. Nzir (2003) bahwa "Penelitian deskriptif adalah suatu metode dalam penelitian status sekelompok manusia, suatu objek, suatu set kondisi, suatu system pemikiran apapun suatu kelas peristiwa pada masa sekarang".

Pada metode ini juga menjelaskan bagaimana pengujian sebuah *protocol* HTTP dan HTTPS, pengujian ini dilakukan beberapa kali untuk memastikan serangan dengan teknik *Man in the middle attack* ini berhasil mengetahui dan melihat *username* dan *password* korban. Pada saat simulasi penyerangan ini berjalan nantinya menulis akan menganalisa setiap paket data dan juga mengamati setiap perubahan yang terjadi pada *protocol* http dan https yang lewat pada jaringan local *wi-fi*. Paket data yang penulis amati terdapat beberapa komponen, berikut 5 komponen dari paket data :

a. Time

   Menjelaskan format waktu packet yang tertangkap

b. Source

   Merupakan IP sumber dari suatu packet data.

c. Destination

   Merupakan IP tujuan kemana suatu packet data akan diteruskan.

d. Protocol

   Merupakan jenis *protocol* apa yang digunakan.

e. Packet Length

   Merupakan panjang dari suatu packet data yang digunakan .

f. Info

   Merupakan info lebih lanjut mengenai suatu packet.

3.2 Alat Analisis

Menurut Rahadi (2010), Tujuan pokok suatu penelitian adalah untuk menjawab pertanyaan dan hipotesis. Untuk itu peneliti merumuskan hipotesis, mengumpulkan data, memproses data, membuat analisisdan interpretasi. Analisis data ini belum dapat menjawab pertanyaan penelitian. Setelah data dianalisis dan diperoleh informasi yang lebeih sederhana, hasil analisis tersebut harus diinterpretasi untuk mencari makna dan implikasi dari hasil analisis tersebut.

Analisa data adalah mengelompokkan, membuat suatu urutan, memanipulasi serta meningkatkan data sehingga mudah untuk dibaca. Setelah itu langkah seta meningkatkan data sehingga mudah untuk dibaca. Setelah itu langkah pertama yaitu mencari kesimpulan dari dua *protocol* HTTP dan HTTPS bagaimana tingkat keamanan dari kerentanan website oleh eksplotasi informasi yang dilakukan penyerang seperti *username* dan *password* korban. Alat analisis yang penulis gunakan untuk mengekplotasi informasi dan mencari kerentanan dari sebuah website yang menggunkan protocol HTTP dan HTTPS sebagai berikut:

a. *Burpsuite*

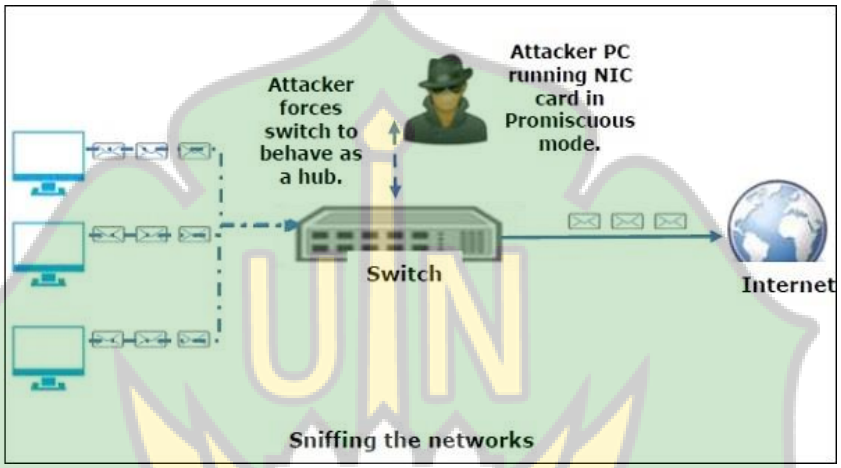
Merupakan aplikasi yang digunkan untuk mencari kerentanan dari aplikasi web. Tujuan dari *Burpsuite* ini adalah untuk mencari celah terhadap website HTTPS yaitu Portal UIN Ar-Raniry. Karena pada burpsuite memiliki sertifikat yang sudah ditandatangani sendriri yaitu setifikat *Certificate* Authority(CA) yang dikeluarkan oleh pengembang aplikasi burpsuite ini. Dan memungkinkan tools ini dapat melihat dan membaca jalur lalu lintas protocol HTTPS yang dimiliki keamanan lebih.

b. Wireshark

Merupakan sebuah *networkpacket analyzer* yang digunakan untuk membaca dan menganalisa paket – paket data serta menampilkan isi paket dengan sedetail mungkin dari memfilter packet, menampilkan packet list

yang sudah terurut secara numeric dan menganalisa jumlah byte dari setiap packet. *Tools* ini merupakan *tools* yang sangat popular pada saat ini karena dapat menangkap packet data secara real time[11].

Gambar 2 : Gambar Model Penyerangan Man in The Middle Attack



Pada gambar dijelaskan bahwa klien akan melakukan transaksi terhadap server https. Antara klien dan server nantinya akan bertukar data jaringan, sedangkan penyerang bertindak sebagai gate away dalam aliran lalu lintas. Penyerang tersebut ialah *MITM (Man The Middle Attcak)* yang bertujuan untuk memotong lalu lintas antara client dan server. Sehingga dapat mengubah pesan dan menyisipkan pesan baru sebelum lalu lintas dari sumber diteruskan ke tujuannya. Sehingga tindakan tersebut tidak disadari sama sekali[7].

1. Bahan dan Alat Penelitian

Adapun bahan dan alat yang digunakan dalam penelitian ini ialah peneliti menggunakan beberapa *software* dan *hardware* sebagai literature penelitian. Untuk spesifikasi kebutuhan *software* dan *hardware* sebagai berikut : [8]

1. Spesifikasi kebutuhan hardware dan system operasi..
    a. Leptop LENOVO *Computer* Inc, *Procesor* AMD12, memori (RAM) 8 GB.
    b. *System* Operasi *KALI LINUX*
2. Spesifikasi kebutuhan software
    a. Software *Wireshark* (untuk serangan Packet sniffing)
    b. Software *Burpsuite* (untuk menghambat lalu lintas https menggunakan proxy yang disetting pada firefox)

3.3 Flowchart Alur Penelitian

Untuk dapat memahami maka penulis menjabarkan alur penelitian menggunakan metode yang digunakan dalam flowcart alur penelitian

Pada gambar dijelaskan bahwa penelitian ini terbagi menjadi beberapa tahapan alur penelitian. Tahapan alur penelitian sebagai berikut :

a. Sebelum penulis melakukan tahap awal penelitian, penulis menyiapkan semua ketersediaan referensi sebagai literature seperti jurnal, buku, artikel dengan tujuan penunjang pelaksanaan penelitian.

b. Penulis menyiapkan kebutuhan *software* dan *hardware* yang dibutuhkan dalam pelaksanaan penelitian.
c. Penulis mengaktifkan jaringan *wi-fi* pada laptop dan siap untuk melakukan penyerangan guna untuk mendapatkan informasi penting tentang keamanan suatu *website* yang di*secure* dengan *protocol* https dan *website* yang tidak di*secure* dengan *protocol* http.
d. Setelah melakukan penyerangan penulis menganalis membandingkan dua kodisi dari masing – masing website yang di*secure* dan tidak di*secure*
e. Penulis dapat menarik kesimpulan dari perbedaan terhadap bentuk penyerangan dan nantinya dapat memberikan saran dalam mengamankan jaringan kabel LAN dan *wi-fi*

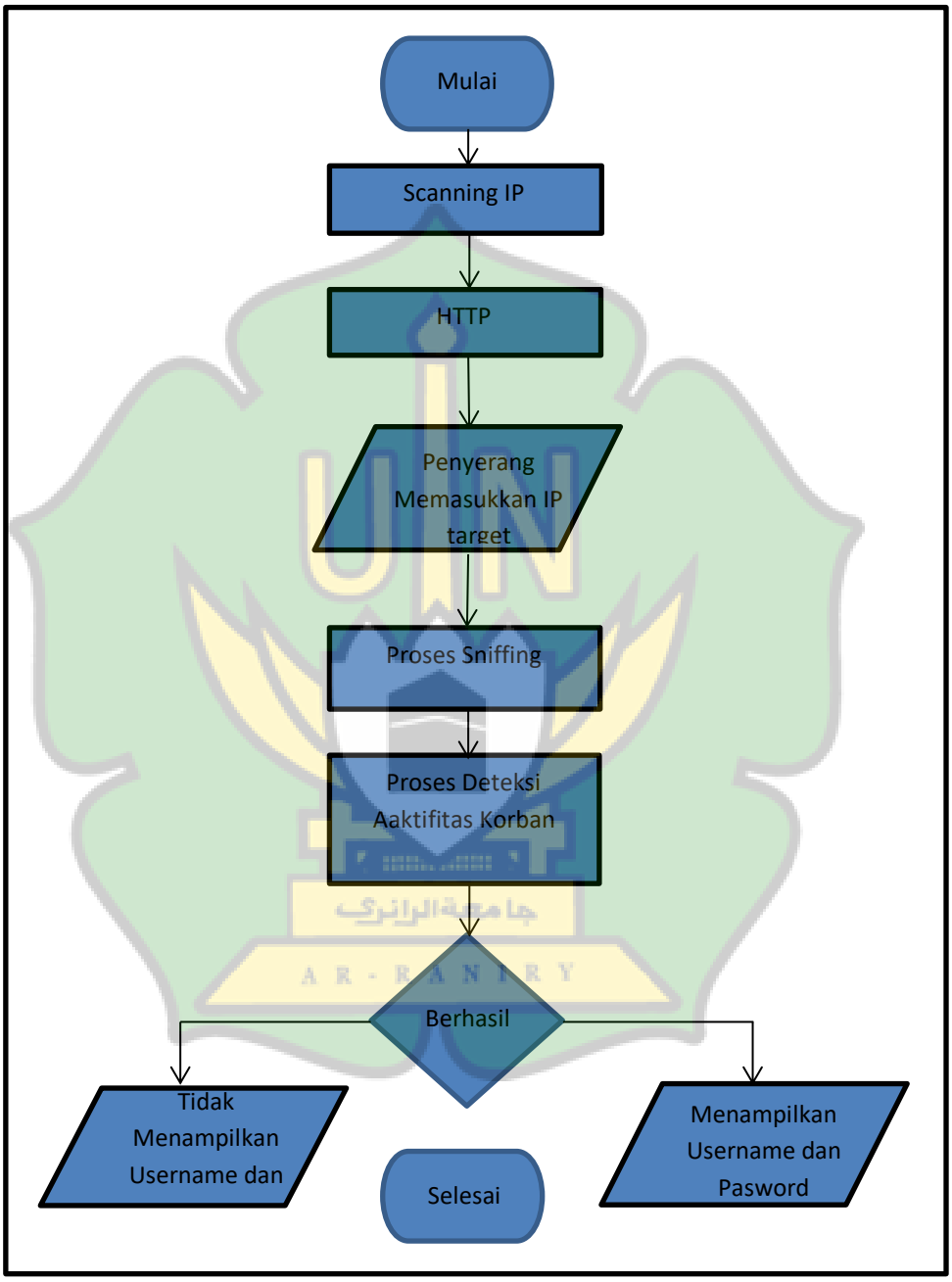
3.4 Tahapan Tahapan Penyerangan

1. Tahapan Penyerangan Protocol HTTP

Pada gambar merupakan tahapan dalam melakukan penyerangan menggunakan *tools wireshark*. Adapun tahapannya sebagai berikut :

1. penyerang melakukan *scanning* ip yang tertangkap untuk mengetahui ip target
2. langkah selanjutnya memasukkan ip target untuk melakukan metode *sniffing*
3. proses selanjutnya yaitu proses mengetahui aktifitas korban dengan menganalisa apakah korban melakukan proses login pada web browser
4. jika benar maka *tools wireshark* akan mencapture *username* dan *password*, untuk lebih jelasnya dapat dilihat pada gambar

Gambar 3 : Gambar Tahapan Penyerangan Protocol HTTP

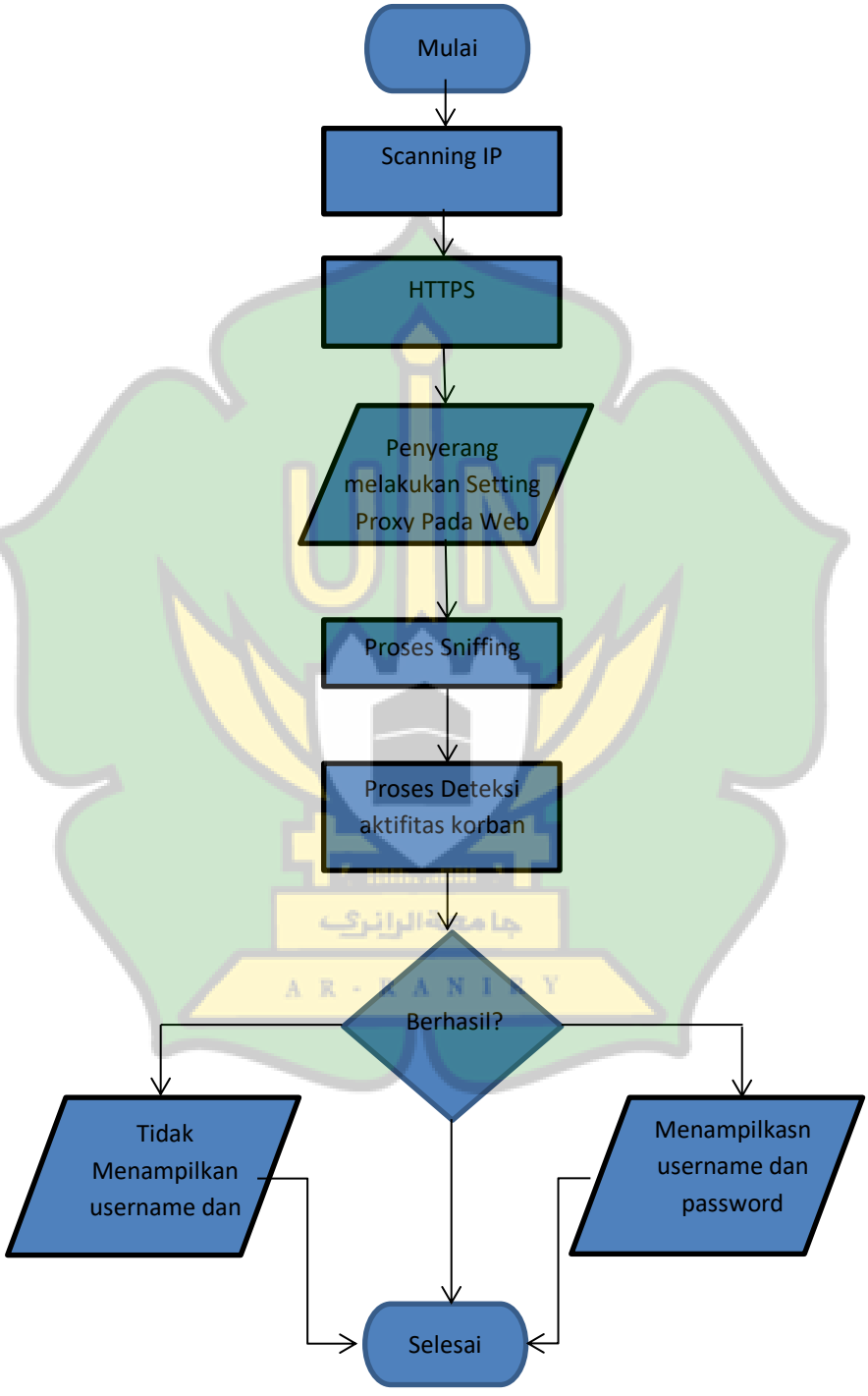


2. Tahapan Penyerangan Protocol HTTPS

Berikut merupakan tahapan dalam metode penyerangan terhadap *protocol* https yang memiliki keamanan data yang sangat aman. Adapun tahapannya sebagai berikut :

1. pertama melakukan *scanning* ip guna untuk mengetahui ip target yang akan di*sniffing*
2. selanjutnya memasukkan ip target tadi kedalam tools yang penulis pakai, untuk melakukan *sniffing*
3. proses selanjutnya yaitu proses untuk mengetahui aktifitas korban dengan menganalisa apakah korban melakukan proses *login* pada web browser.
4. Jika tidak berhasil maka akan mencoba melakukan beberapa kali pengujian.
5. Penulis mengatur settingan pada web browser yaitu firefox dengan membuat proxy menjadi *localhost*
6. Selanjutnya akan mencoba menggunakan aplikasi *Burpsuite* yang mana dengan aplikasi ini dapat membaca celah dari kerentanan dari sebuah website karena burpsuite ini memiliki sertifikat yang sudah ditandatangani sendiri yaitu sertifikat CA(*Certificate Authority*). Dengan adanya sertifikat itu dapat melihat serta membaca lalu lintas jaringan yang menggunakan *protocol* HTTPS. Untuk lebih jelasnya dapat dilihat Gambar berikut.

Gambar 4 : Gambar Tahapan Penyerangan Protocol HTTPS



BAB IV

HASIL DAN PEMBAHASAN

Analisis ini perlu dilakukan untuk mengetahui bagaimana bentuk dari sebuah penyerangan packet *sniffing* terhadap *protocol-protocol* jaringan yaitu HTTP dan HTTPS. Pada umumnya tingkat keamanan buka berasal dari *software* maupun *hardware* yang ada melainkan ada peran penting dari pengguna/manusia yang melakukan koneksi terhadap suatu perancangan jaringan tersebut

Keamanan dari jaringan *wi-fi* yang terkoneksi ke internet pada umumnya rentan terhadap ancaman. Maka dari itu perlu mengevaluasi kembali bagaimana tingkat keamanan *website* terhadap serangan *packet sniffing*.

4.1. Analisis Hasil Penelitian

4.1.1 Mengkoneksikan Komputer Pada Jaringan *Wi-fi*

Pada Simulasi ini penulis melakukan koneksi terhadap jaringan local *wi-f*, penulis melakukan koneksi menggunakan jaringan *wi-fi indihome*, sehingga *computer* terkoneksi dengan *wi-fi*. Hal ini dapat memudahkan penulis dalam menggunakan computer sendiri

4.1.2 Analisis Jaringan *Wi-fi*

Percobaan analisis ini dilakukan untuk memastikan aktivitas korban dalam membuka website, apakah *website* tersebut menggunakan keamanan atau tidak.

Hal ini berguna untuk perbandingan bagaimanan response terhadap website yang terkena *packet sniffing* baik dengan Protocol HTTP maupun HTTPS

4.1.3 Packet Sniffing

Penelitian ini dilakukan guna untuk mengetahui suatu informasi penting seperi *account username*, *password*, akses DNS yang akan dituju dan informasi lainnya. Pada penelitian ini penulis ingin memberikan gambaran bagaimana siumulasi dari penyerangan *website* yang menggunakan keamanan maupun tidak. Dan hal ini dilakukan agar penyerang dapat melakukan akses internet secara tidak sah untuk memberikan keuntungan pribadi tetapi dapat merugikan bagi orang lain karena sama – sama terhubung pada jaringan local *wi-fi*.

Pada penelitian ini penyerangn berhasil mendapatkan *username* dan *password* korban. Percobaan kali ini *wi-fi* itu hanya sebagai gerbangnya saja, penulis akan melakukan penyadapan terhadap computer yang terkoneksi internet yang kebetulan melakukan *autentifikasi* login pada suatua *website* yang menggunakan *protocol* HTTP dan HTTPS. Dengan demikian penulis mendapatkan suatu pernyataan bagaimana kondisi dari *website* tanpa keamanan yang menerima serangan *packet sniffing* dan kondisi dari *website* dengan keamanan yang menerima serangan *packet sniffing* sniffing.

4.1.4 Kali Linux

Pada penelitian ini penulis memilih menggunakan system operasi *kali linux* karena untuk melakukan serangan terhadap website dan situs – situs lainnya dan

keperluan dalam *penetration test.* Sangan dibutuhkan system operasi yang dapat memuat semua aplikasi dalam melakukan teknik hacking. Pada *kali linux* banyak terdapat aplikasi security yang terkenal yaitu *Nmap, Aircrack-ng, kismet, wireshark, metasploit framework, burp suit, john the ripper, social engineering toolkit, maltego, ettercap, OWASP ZAP*

4.1.5 *Certificate Authority* (CA)

Pada *Secure Socket Layer* (SSL) tentunya memiliki peranan yang sangat penting salah satunya adalah melakukan *validasi* terhadap identitas *server* dan memastikan *client* melakukan komunikasi pertukaran data dengan *server* yang benar. Agar *server* tidak dipalsukan maka dibutuhkan *Certificate Authority (CA)* yang memberikan client jaminan bahwa gembok (*public key*) memiliki *certificate* dari pihak ketiga.

4.2 Scenario Penyerangan Sniffing

Scenario *penyerangan* dalam melakukan penyerangan *packet sniffing* yaitu dengan membagi 2 target. Target pertama yaitu website yang tidak menggunakan *security* (HTTP) dan target kedua website yang menggunakan *security* (HTTPS). Penulis akan melakukan penyerangan terhadap 2 *protocol* yaitu HTTP dan HTTPS lalu membandingkan dua kondisi bagaimana *responden* terhadap serangan *packet sniffing* yang penulis lakukan

4.2.1. Penyerangan Sniffing Website HTTP

4.2.1.1. Berikut langkah – langkah terhadap target 1 yaitu *protocol* HTTP dari scenario yang dilakukan :

a. Penyerang memastikan target berada dalam satu jaringan yang sama dengan penyerang
b. Penyerang mencari suatu website tanpa keamanan yang menggunakan protocol HTTP yang sama tidak memiliki system keamanan yang terenkripsi.
c. Selanjutnya melakukan proses *login* pada *system* website tersebut
d. Proses *login* yang dicoba yaitu menggunakan *username* dan *password* yang salah karena ingin mengetahui tingkat keamanan terhadap website tersebut.
e. Penyerang berhasil mengetahui aktivitas dari target dan software *wireshark* dapat merekam beberapa *packet list* yang masuk.

4.2.1.2. Berdasarkan website HTTP yang akan diserang, ada beberapa website tampa keamanan yang penulis ingin coba. Dapat dilihat pada tabel sebagai berikut :

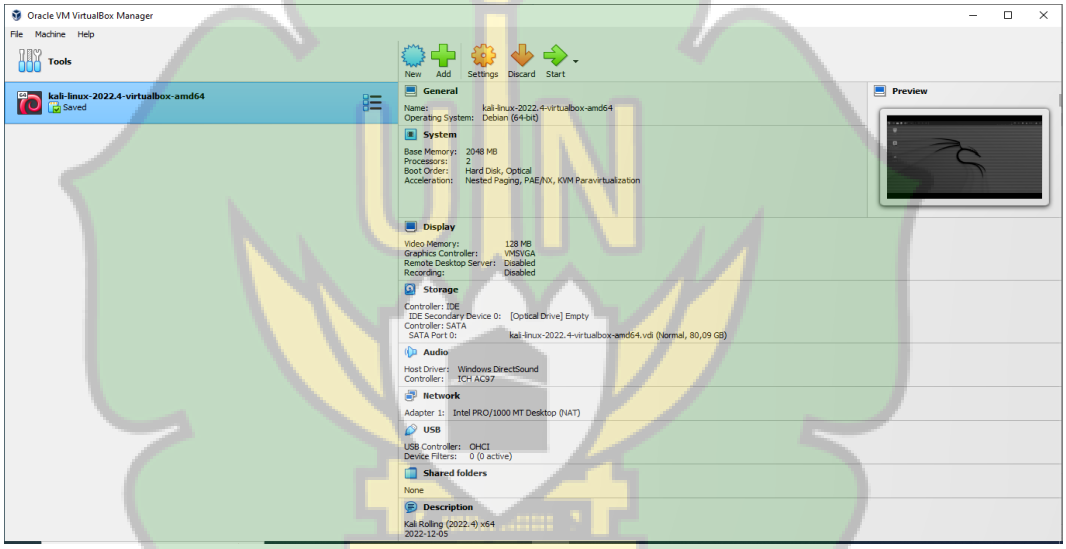
Table 1 : Tabel Penyerangan HTTP

No	Nama Website	Link Website
1	Penmaru UMSU	http://penmaru.umsu.ac.id/
2	website resmi desa condong campur	http://condongcampur-banjarnegara.desa.id/
3	RSUD TEGAR KOTA MALANG	http://rsudtidar.magelangkota.go.id/
4	UNIVERSITAS PGRI Semarang	https://pmb.upgris.ac.id/

4.2.1.3. Scenario penyerangan dari website HTTP

a. Pada penelitian ini penulis menggunakan *kali linux* dengan *virtualbox*. Sebelumnya penulis sudah melakukan instalasi *kali linux*, setelah berhasil barulah *kali linux* dapat dioperasikan pada gambar ini.

Gambar 5 : Tampilan VirtualBox

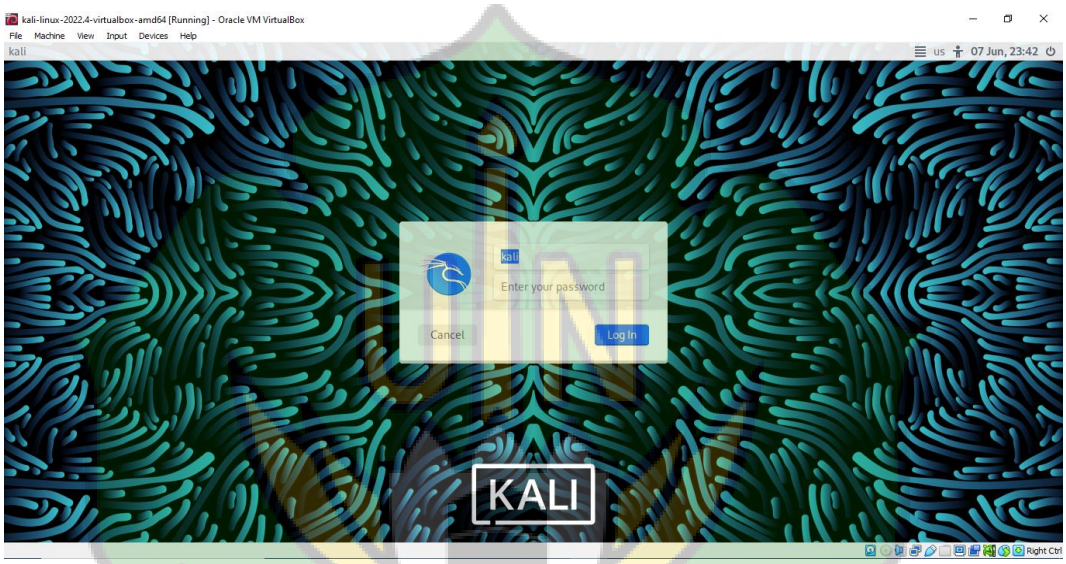


b. Penulis membuat virtual *machine* dengan nama *kali-linux-2022.4-virtualbox-amd* lalu mengkonfirigurasikan *Operating System (OS) Kali Linux*

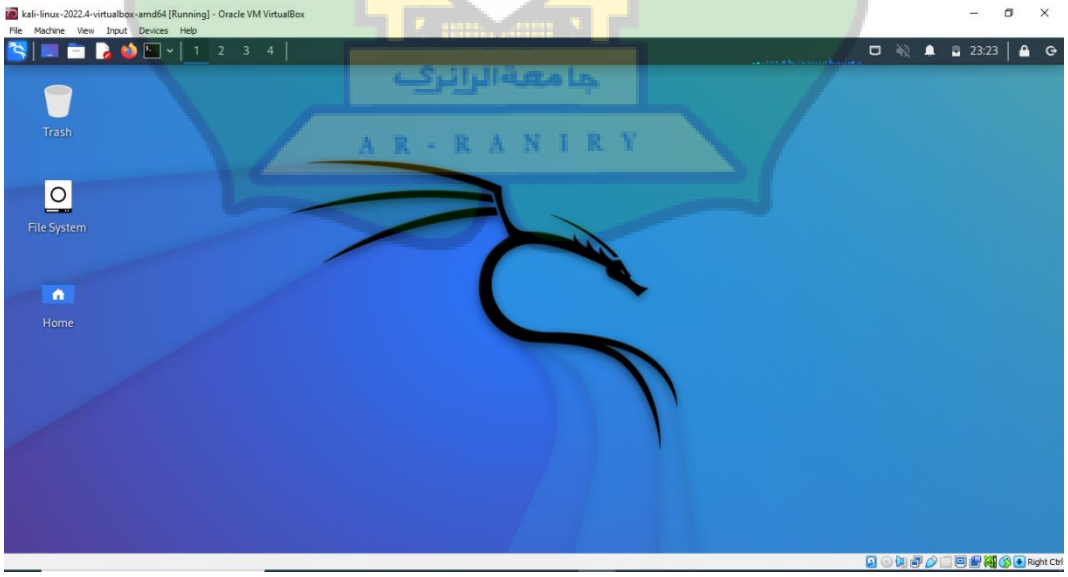
c. Selanjutnya penulis menekan tombol *Star* untuk menjalankan *Operating System (OS) Kali Linux.* Seperti Gambar

d. Penulis memasukkan *username* dan *password* kali, sesuai dengan yang di setel pada saaat menginstalasi *Operating System kali linux* pada gambar

Gambar 6 : Tampilan *Login Kali Linux*

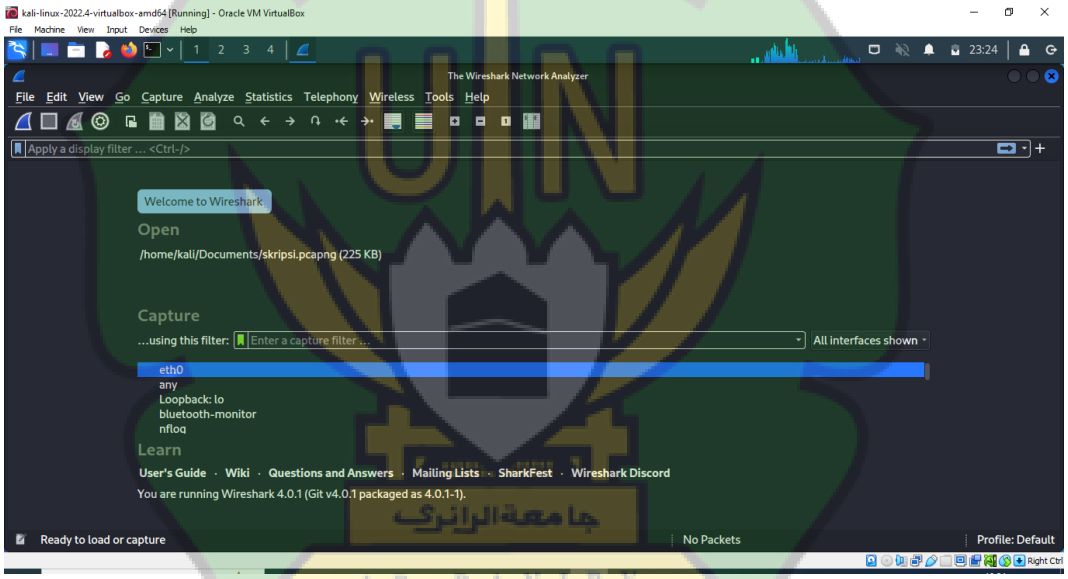


Gambar 7 : Tampilan *Deskop Kali Linux*



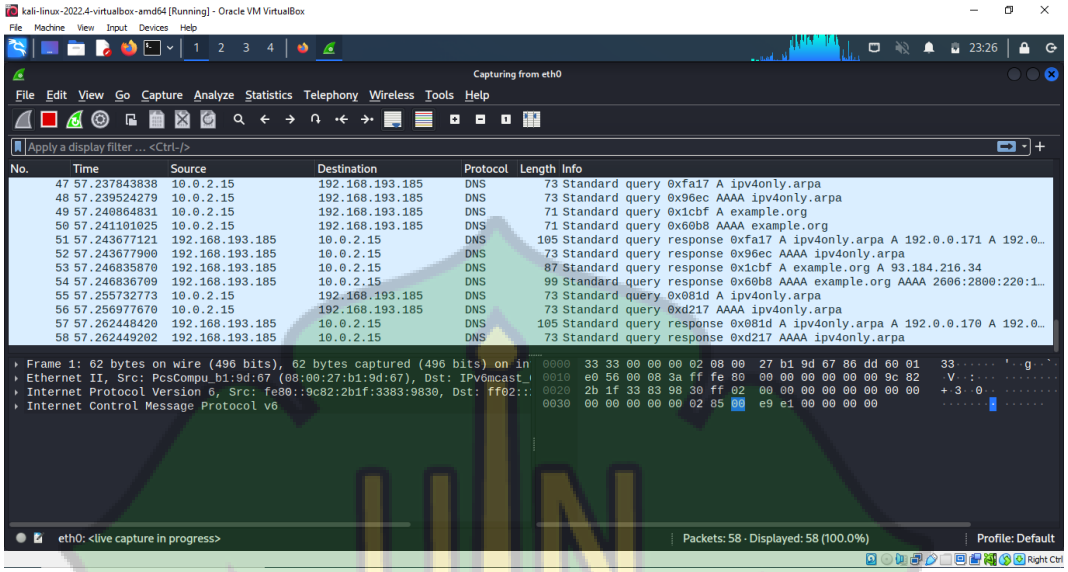
e. Selanjutnya penulis membuka *software wireshark.* Langkah pertama penyerangan adalah pilih *interface* jaringan yang diinginkan. Terdapat beberapa *interface* yang bertugas untuk meng *capture packet*. Pada tahap ini penulis memeilih *interfaxe eth0.* Seperti gambar

Gambar 8 : Tampilan *Interface* pada *Wireshark*



f. Setelah melakukan start pada *interface* yang sudah dipilih tadi, maka dengan otomatis tools pada *wireshark* berjalan dan menangkap hasil *capture packet* dari *web browser* yang telah dibuka. Seperti pada gambar

Gambar 9 : Proses *Capture* pada *interface eth0*

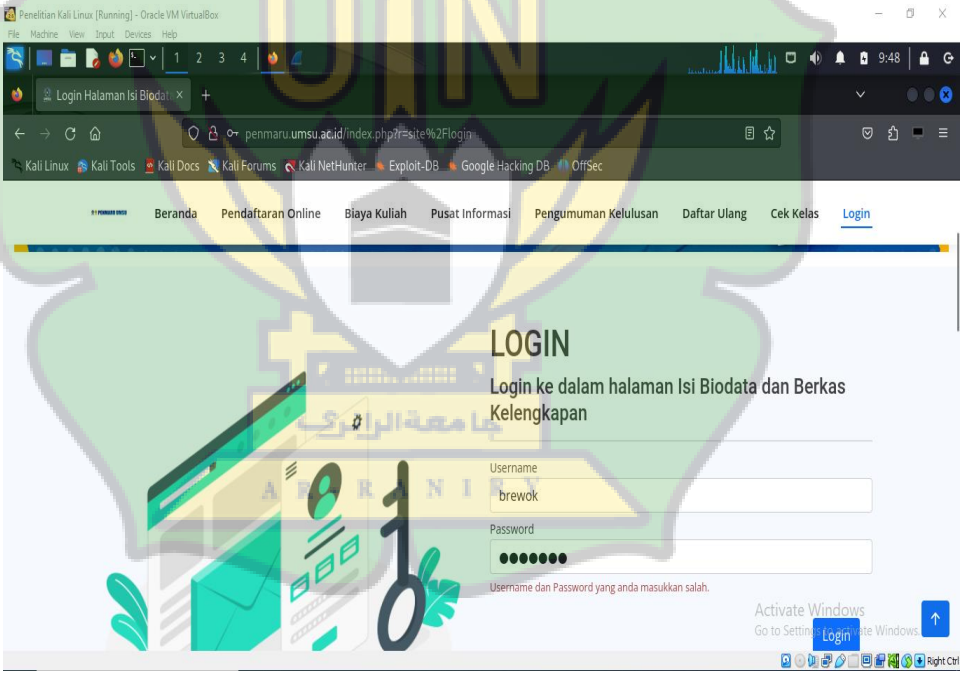


g. Dari beberapa *website* HTTP yang ingin dilakukan simulasi percobaan penyerangan *packet sniffing* pada tabel .. maka penulis hanya memilih datu *website* yang akan ditapilkan dalam laporan. *Website* HTTP yang akan dijelaskan dalam pembahasan kali ini yaitu *website* teknokrat Penmaru UMSU

4.2.1.4. Penyerangan Website Penmaru UMSU

4.1 Pada tampilan *login website* Penmaru UMSU, penyerangan mencoba melakukan serangan *packet sniffing* terhadap website Universitas Muhamadiyah Sumatra Utara. Pada tahap ini penyerang melakukan proses *login* mengimput *username* dan *password* yang salah dengan tujuan ingin mencoba kerentanan terhadap website tersebut. Seperti pada gambar berikut

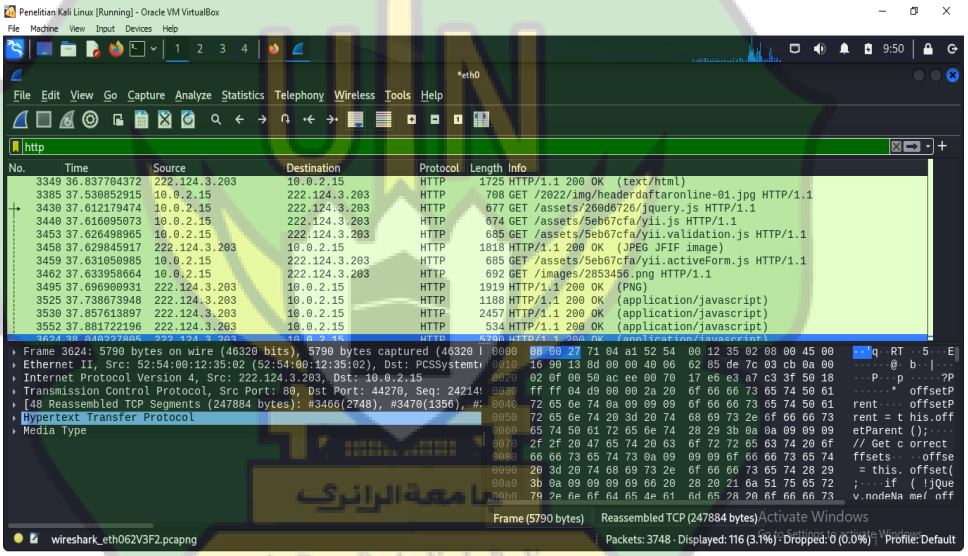
Gambar 10 : Tampilan *Login Website* Universitas Muhamadiyah Sumatra Utara



4.2 Selanjutnya proses capture *packet* akan terjadi, lalu penyerangan menekan *stop* untuk menghentikan proses *capturing packet*. Pada tampilan *capturing packet* dapat dilihat beberapa informasi seperti

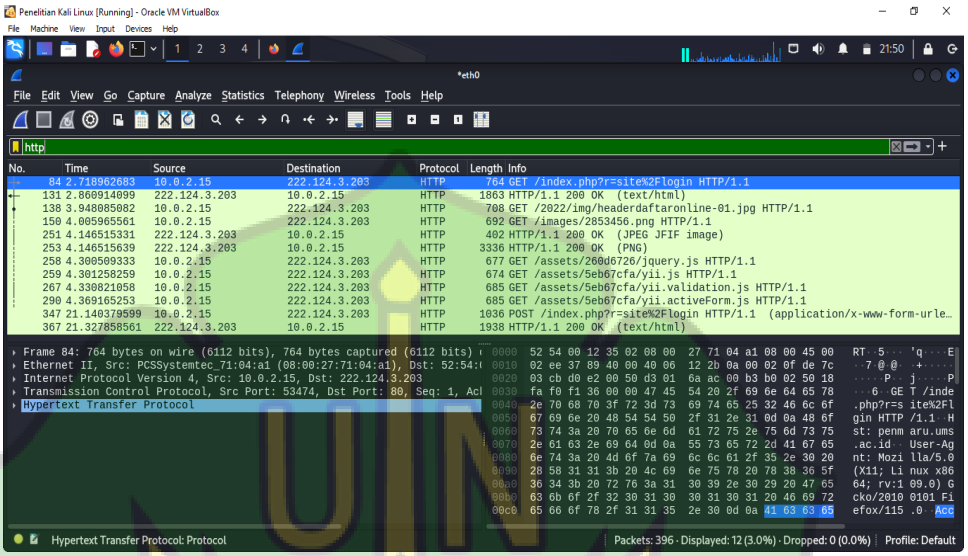
packet list dan *packet byte*. Pada *packet list* dilihat beberapa infromasi packet yang terurut secara numeric informasi dari *packet list* yaitu waktu, sumber paket, ip tujuan, protocol yang digunakan , panjang paket dan informasi lebih lanjut tentang paket sedangkan pada packet byte hasil paket ditampilkan dalam bilangn Hexadecimal dan ASCII, seperti pada gambar ini

Gambar 11 : Proses *Stop Capture Packet*



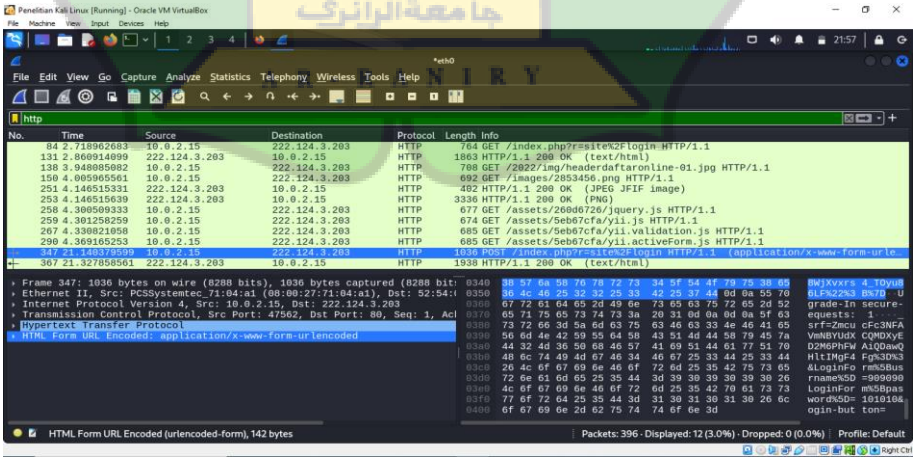
4.3 Kemudian tuliskan kata HTTP di kolom pencarian *wireshark* agar menampilkan protocol HTTP saja seperti gambar berikut :

Gambar 12 : Proses pencarian HTTP



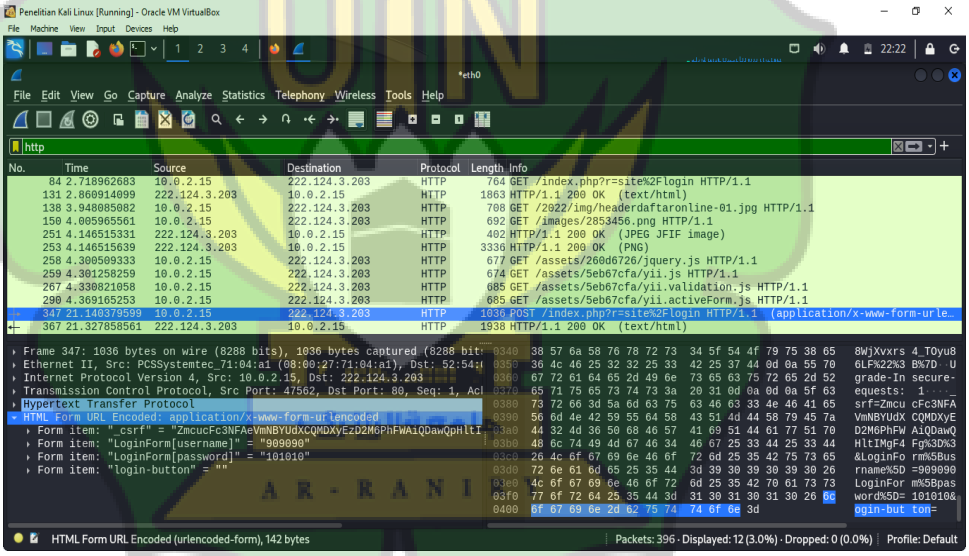
4.4 Selanjutnya setelah menampilkan http yang kita inginkan maka sekarang kita mencari kata *POST* di antara bagian info seperti gambar berikut

Gambar 13 : Tampilan pencarian kata *POST*



4.5 Kemudian setelah menemukan kata post maka kita ke bagian HTML, selanjutnya klik HTML untuk menampilkan username dan password. Dan dapat disimpulkan bahwa penyerangan *website* terhadap keamanan HTTP dapat dengan mudah terbaca oleh *wiresahark*. Hasil penyerangan berhasil, dan *wireshark* mampu menampilkan username 909090 dan password 101010. Seperti gambar berikut

Gambar 14 : Hasil Penyerangan pada HTTP



4.2.1.5. Scenario penyerangan website HTTPS

a. Berikut langkah-langkah terhadap target 2 yaitu protocol HTTPS dari scenario yang dilakukan:

a) Penyerang menyiapkan beberapa website dengan protocol HTTPS guna untuk menguji bagaiman respon website

terhadap penyerangan *sniffing*, guna menguji keamanan dari website

b) Selanjutnya penyerangan membuka aplikasi *burpsuite*, pada tahap ini penyerang mengatur proxy pada settingan di *browser* guna untuk membuat *burpsuite* bertindak sebagai proxy

c) Pada *tools burpsuite* penyerang mematikan intercept is on menjadi of sehingga website dapat dibuka pada *browser* penyerang akan melakukan serangan untuk mencari kerentanan dari suatu website

d) Penyerang melakukan proses *login* terhadap website.

e) Aplikasi *burpsuite* memonitoring setiap *request* maupun *response* dari *web browser* dengan server

f) Penyerang berhasil menemukan *username* dan *password* target

b. Berikut beberapa website HTTPS yang penyerang ingin mencari kerentanan dari tingkat keamanan website:

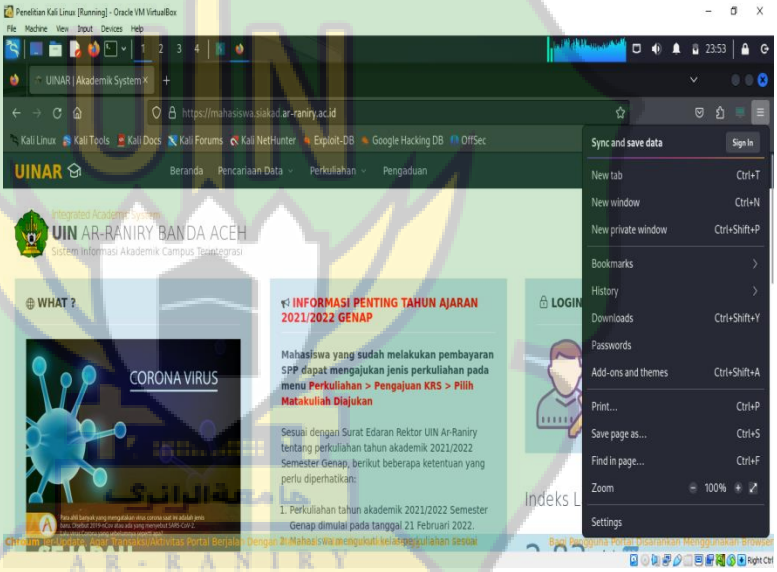
Table 2 : Tabel Penyerangan HTTPS

No	Nama Website	Link Website
1	UINAR Akademik System - UIN Ar-Raniry	https://mahasiswa.siakad.ar-raniry.ac.id/
2	LDC UIN Ar-Raniry	https://pusatbahasa.ar-raniry.ac.id/
3	Instagram	https://www.instagram.com/accounts/login/
4	Facebook	https://id-id.facebook.com/
5	Portal USU (Universitas Sumatra Utara)	https://portal.usu.ac.id/
6	Portal Akademik Universitas Malikussalaeh	http://portal.unimal.ac.id/

c. Hasil skenario penyerangan website HTTPS

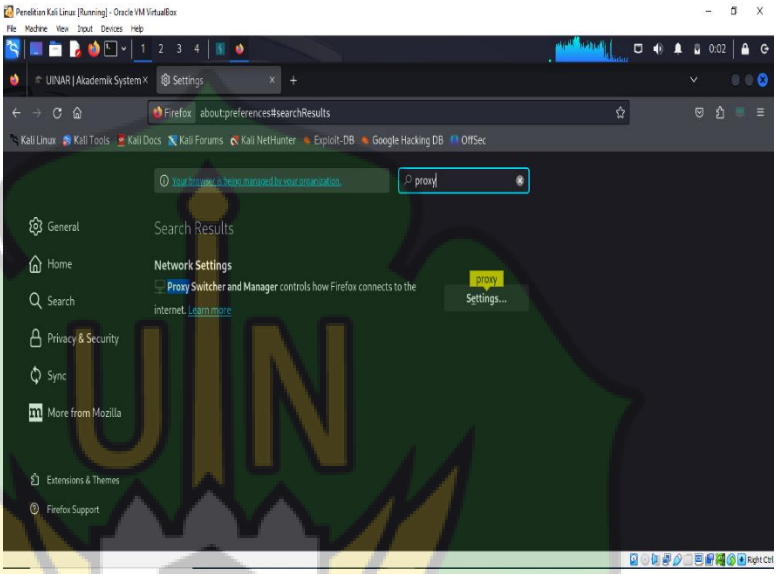
a) Pertama sebelum penyerang membuka aplikasi burpsuite, penyerang mengatur proxy yang tersedia pada browser guna membuat *burpsuite* bertindak sebagai proxy. Pada tahap ini pilih settingan pada browser pilih Setting. Seperti gambar

Gambar 15 : Tahap Pertama Mengatur Proxy



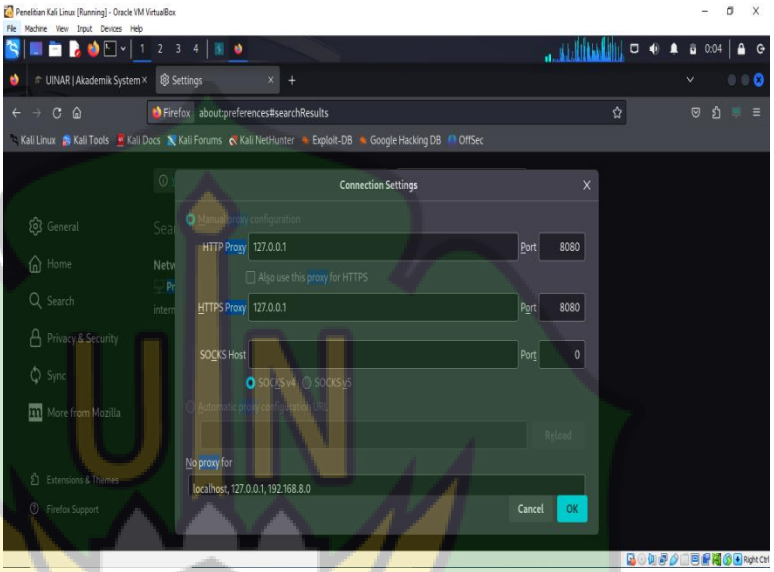
b) Selanjutnya memilih proxy dengan mengetik proxy pada kolom pencarian. Seperti gambar

Gambar 16 : Tahap Kedua Mengatur Proxy



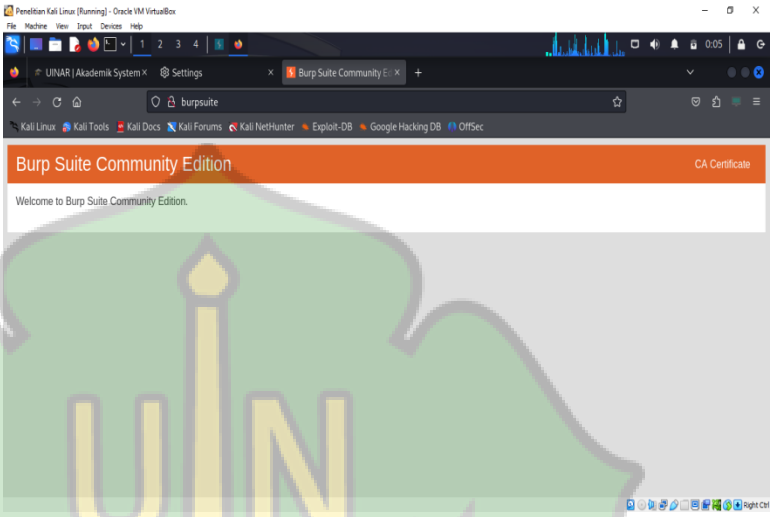
c) Pada tahap ketiga penyerang memilih konfigurasi proxy secara manual dengan mengimputkan HTTP Proxy 127.0.0.1 dengan port 8080 dan juga bias mengatur HTTP proxy menjadi localhost tetapi penyerang memilih HTTP proxy 127.0.0.1 supaya proxy berjalan dengan lancar. Seperti gambar

Gambar 17 : Tahap Ketiga Mengatur Proxy



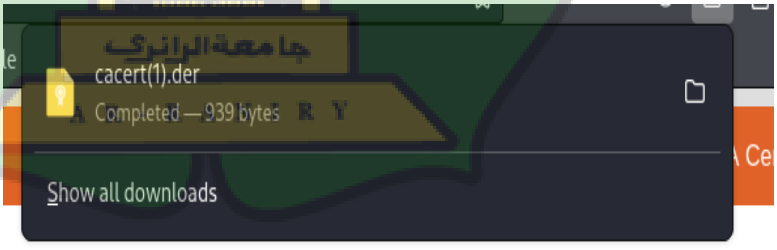
d) Dan apabila proxy tidak berjalan maka langkah selanjutnya dengan mendownload kembali sertifikat CA *(Certificate Authority)* yang telah disediakan oleh *tools burpsuite* ini. Ketikkan http://burpsuite pada url browser. Seperti gambar

Gambar 18 : Tahap Pertama Mengatur CA Certificate



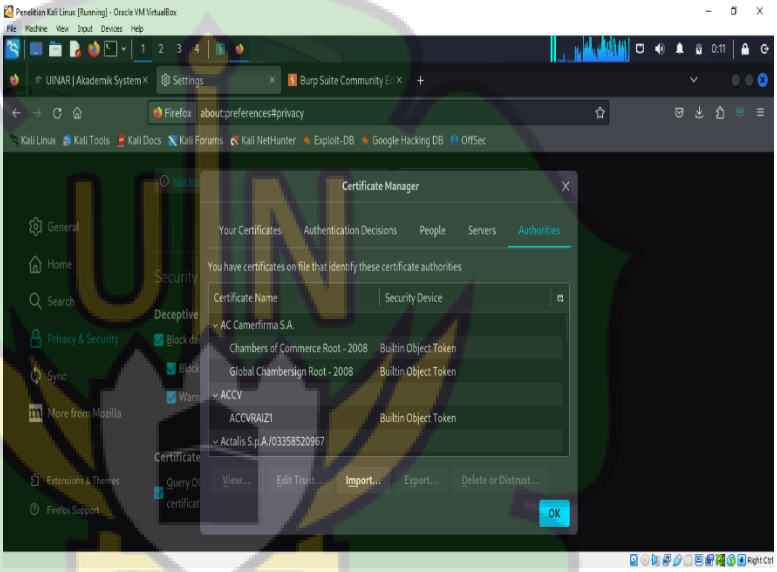
e) Selanjutnya pilih CA(*Certificate Authority)* Certificate di pojok kanan maka akan muncul tampilan download cacert.der lalu pilih *save file*. Seperti gambar

Gambar 19 : Tahap Kedua Mengatur CA Certificate



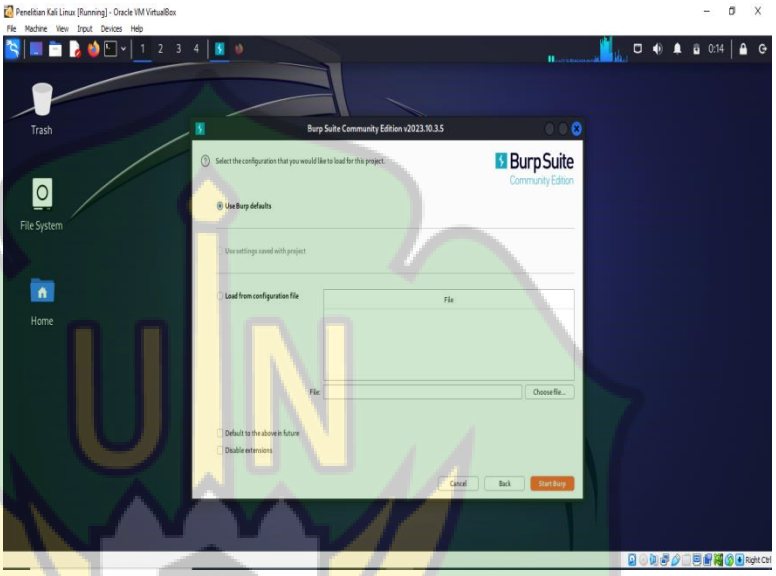
f) Selanjutnya setelah download selesai, tahap selanjutnya ialah melakukan *inport certificate* yang telah *didownload* dengan cara pilih *preferences-certificate* pada pengaturan browser lalu pilih inport. Seperti gambar

Gambar 20 : Tahap Ketiga Mengatur CA Certificate



g) Jika sudah melakukan *inport Certifikacte* maka langsung saja menjalankan *burpsuite* dengan cara klik *start burpsuite*

Gambar 21 : Menjalankan Burpsuite



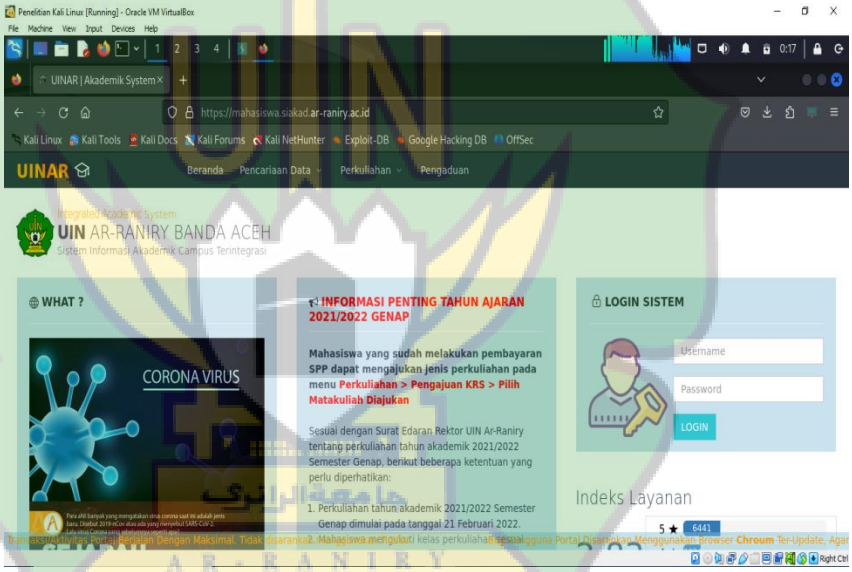
h) Dari berbagai website HTTPS yang akan penyerang lakukan, penyerang hanya memilih satu website yang akan ditampilkan pada laporan yaitu website siakad UIN AR RANIRY

d. Penyerangan Website system informasi Akademik Siakad (SIAKAD) UIN AR RANIRY

Pada target pertama dalam penyerangan website HTTPS, penyerang melakukan penyerangan terhadap website yang sudah terenkripsi dan mencoba apakah dapat menembus keamanan yang

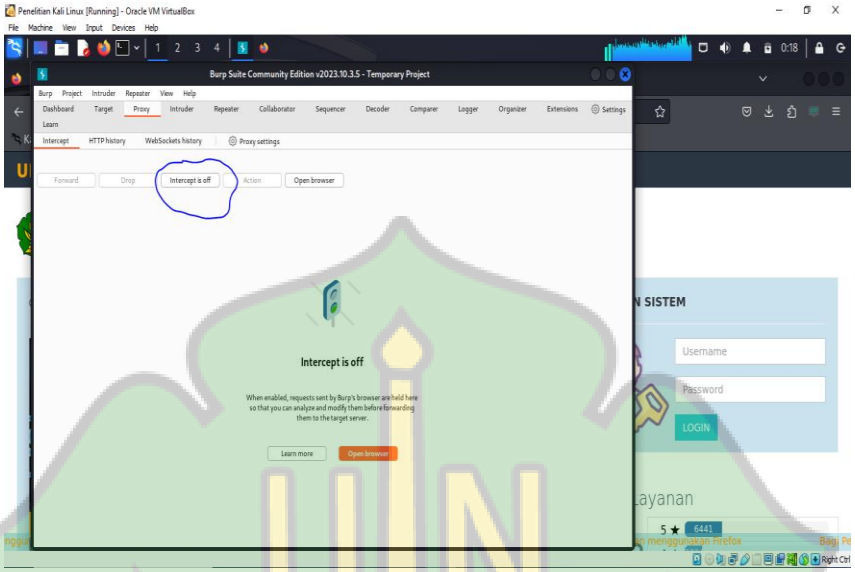
dimiliki website tersebut dan apakah terdapat kerentanan sehingga pesan *request* dan *respons* dari browser dan server dapat diketahui oleh aplikasi *burpsuite* ini. Pada tahap ini penyerang melakukan proses login dengan memasukkan *account* palsu untuk melakukan *testing* apakah *burpsuite* dapat mendapatkan celah dari website terenkripsi tersebut.

Gambar 22 : Proses Login Website Siakad



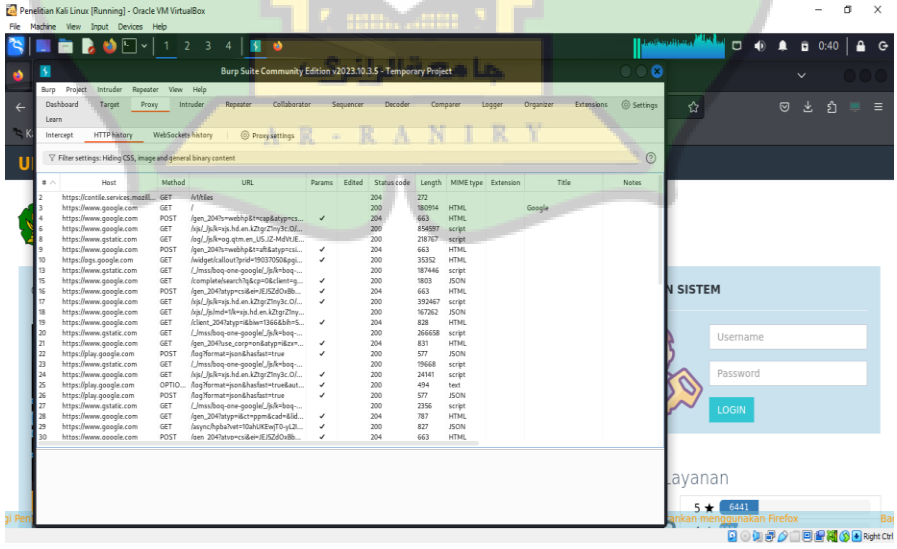
Selanjutnya apabila *intercept* pada menu proxy ini dalam status *on* maka perlu kita ubah dulu ke status *off*, karena apabila *intercept* dalam status *on* maka browser tidak bisa berjalan, jadi di perlukan ubah ke status *off* agar browser bisa berjalan dengan lancar. Seperti gambar

Gambar 23 : Tahap Mengatur Intercept



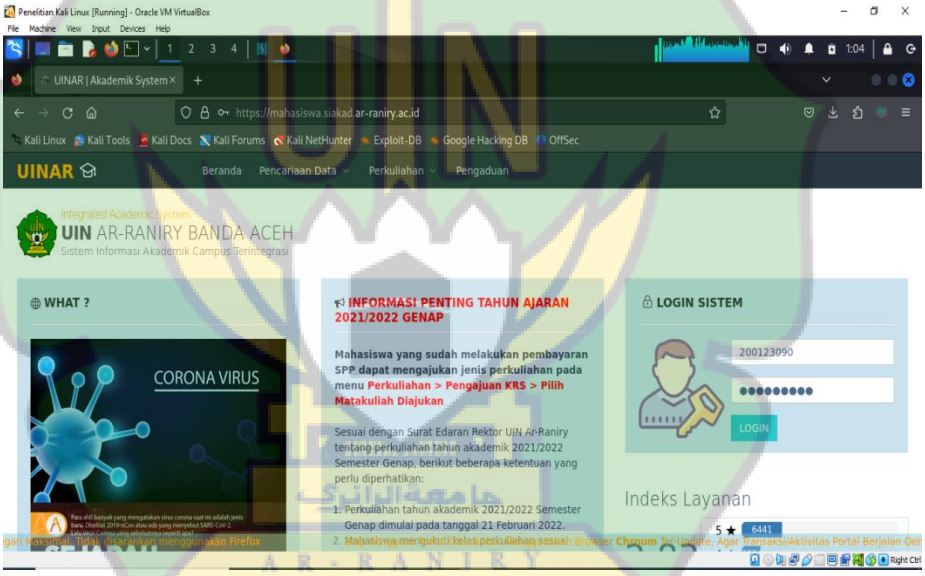
Pada tampilan *capture packet* pada http *history* dapat dilihat detail packet yang tertangkap dan beberapa situs website. Seperti gambar

Gambar 24 : Proses Capture Packet pada HTTP History



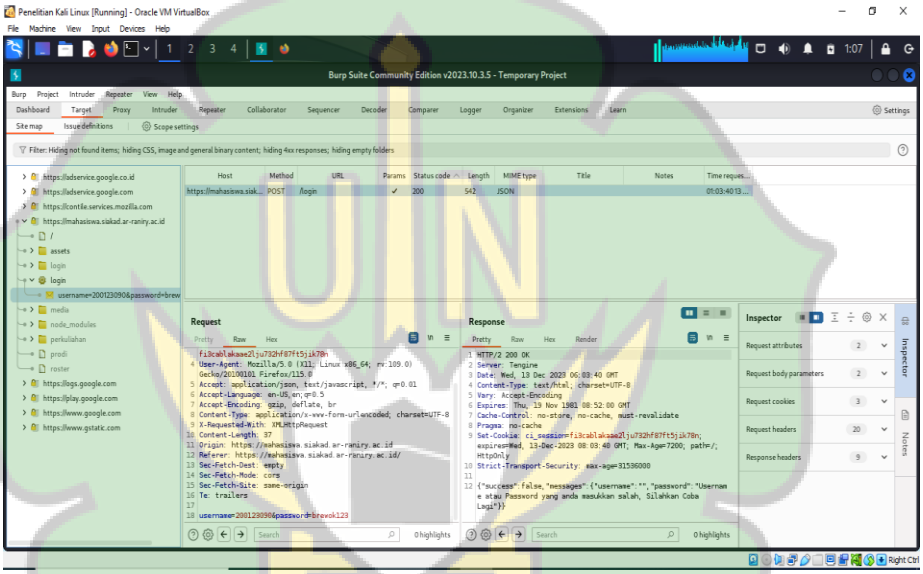
Pada tampilan login website Siakad UIN AR-RANIRY, penyerangan mencoba melakukan serangan *packet sniffing* terhadap website Universitas Islam Negeri Uin Ar-Raniry. Pada tahap ini penyerang melakukan proses *login* mengimput *username* dan *password* yang salah dengan tujuan ingin mencoba kerentanan terhadap website tersebut. Seperti pada gambar berikut

Gambar 25 : Tampilan Login Siakad Uin Ar-Raniry



Pada tahap ini tampilan site map juga dapat menampilkan beberapa website yang tertangkap juga dapat menampilkan arsitektur dari data API-nya sehingga didapatkan hasil token berupa *username* 200123090 dan *password* brewok12. Seperti gambar

Gambar 26 : Tampilan Site Map



Pada hasil site map *tools burpsuite* mampu menampilkan pesan *request* dari web browser. Tampilan site map dapat membaca data API nya yang terdiri dari hostnya adalah siakad.uin ar raniry.ac.id dan juga content-length 37.

Table 3 : Perbedaan penyerangan antara wireshark dan burpsuite

Wireshark	Burpsuite
Memilih interface pada menu capture interface yang mana akan mencapture paket yang lewat	Menyiapkan proxy yang mungkin penyerang menemukan celah arsitektur web
Setelah memilih maka pada tampilan *wireshark* akan menampilkan tangkapan paket yang lewat pada tampilan *wireshark* saat menangkap paket terbagi menjadi 3 bagian yaitu: bagia 1, terdapat detail infroamsi dari waktu mulai, *ip sourc, Ip Destination, Protocol* yang digunakan, panjang paket, dan informasi tentang paket secara umum. Bagian 2, pada bagian tengah menampilkan detail informasi yang terbagi menjadi 5 lapisan yaitu lapisan fisik, data link, *network, transport* dan aplikasi. Bagian 3, wireshark menampilkan paket dalam format hexadecimal	Melakukan monitoring pada menu proxy dan intercept apabila intercept dalam keadaan on maka setiap request dan response daripada data API nya akan terlihat jelas, serta penyerang dapat memanipulasi dan mengubah data *request* pada arsitektur web nya

4.3 Perbedaan analisis hasil capture antara protocol HTTP dan HTTPS

Pada dasarnya tingkat keamanan dalam mengamankan proses transimis packet data masih lebih aman HTTPS dikarenakan adanya proses enkripsi pesan yang diterima olehg tools *wireshark* dan kenapa pada *burpsuite* dapat membaca pesan *request* maupun *reponse* karena aplikasi burpsuite telah didukung dengan adanya CA(*Certificate Authority*) certificate yang bertindak sebagai pihak ketiga yang terpercaya yang memungkinkan dapat menadatangani sertificate yang digunakan *protocol* HTTPS.

4.4 Solusi dan tahap selanjutnya saat mengahadapi serangan packet sniffing

Setelah melakukan beberapa penyerangan dari scenario, langkah selanjutnya adalah meningkatkan keamanan website saat pengguna internet melakukan akses secara illegal. Adabeberapa solusi untuk mencegah dari serangan *packet sniffing* untuk dapat menganalisis suatu keamanan jaringan wi-fi sebagai berikut

4.4.1. Dengan mengganti protocol HTTP menjadi HTTPS

Untuk menghindari tindakan sniffing maka perlu menganti HTTP ke HTTPS, karena pada dasarnya HTTP dapat mengirim

paket data tampa adanya enkripsi sehingga dapat dengan mudah terkena tindakan sniffing maka dengan memakai HTTPS banyak memiliki kelebihan seperti keamanan dalam transmisi data serta keamanan data karena telah terenkripsi dan pada saat ini protocol HTTPS masih dipercaya

4.4.2. Gunakan keamanan WPA2-PSK (Wi-fi protected Acces-Pre Shared Key)

Dengan metode ini dapat mengamankan jaringan wi-fi karena merupakan security terbaru yang disediakan untuk jaringan wireless, jika ada yang ingin melakukan *cracking* akan memakan waktu yang cukup lama.

BAB V

KESIMPULAN DAN SARAN

1.1.Kesimpulan

Berdasarkan pembahasan yang sudah penulis lakukan dengan penelitian "Aanalisis Keamanan Fasilitas Jaringan *wi-fi* terhadap serangan *packet sniffing* pada protocol HTTP dan HTTPS, dengan menganalisis kedua protocol tersebut masih perlu adanya evaluasi dalam meningkatkan keamanan maka hasil penelitian ini dapat disesimpulkan sebagai berikut :

1. Penyerangan packet sniffing menggunakan metode MITM *(Man in the middla attack)* antara *web browser* dengan *web server* dapat memonitoring hasil aktivitas pertukaran data yang lewat dan dapat menampilkan *username* dan *password* saat melakukan autentifikasi *login* pada target, dengan menggunakan *tools* dalam mencari kerentanan bagaimana pesan *request* dan *response* dapat terbaca oleh *tools wireshark* dan *burpsuite*
2. Kondisi dari website dengan protocol HTTP dan HTTPS saat terkena serangan *packet sniffing*, yaitu *tools burpsuite* dapat merekam jejak dari aktivitas target saat mengakses website yang sudah terenkripsi sertifikat CA (*Certificate Authority*) yang mana *tools* ini dapat melihat dan membaca pesan *request* dan *response* antara web browser dan web server yang terjadi dalam internet. Pada penyerangan website HTTP *tools*

wireshark juga mampu merekam serta menampilkan *username* dan *password* dikarenkan tidak adanya enkripsi saat web browser dan web server melakukan komunikasi.

3. Perbedaan serangan antara *website* HTTPS dan *website* HTTP ialah terletak pada tingkat keamanan *website* tersebut. Jika memiliki keamanan yang lebih maka seperti *website* LDC pusat bahasa uin ar raniry penyerang tidak dapat menampilkan *username* dan *password* dikarenakan adanya *enkripsi* data menggunakan SSL (*Secure Socket Layer)* dan TLS(*Transport Layer Security)* yang memungkinkan *website* tersebut tidak dapat dibobol dengan mudah dan membutuhkan waktu yang cukup lama karena saat ini keamanan HTTPS masih aman sampai sekarang.

1.2.Saran

Simulasi yang penyerang lakukan jauh dari kata sempurna, masih banyak terdapat kekurangan-kekurangan. Maka dari itu dibutuhkan perkembangan lebih lanjut agar simulasi ini terlihat sempurna. Adapun saran-saran dari simulasi ini sebagai berikut :

1. Simulasi ini lebih baik dilakukan dengan menggunakan 2 PC atau 2 komputer untuk serangan *packet sniffing.* Pada simulasi ini penulis hanya menggunakan 1 PC dalam melakukan *sniffing* data dan menggambarkan bagaimana serangan seperti *packet sniffing* terjadi.

2. Agar dapat melakukan serangan *packet sniffing* menggunakan *wireshark*. Penulis harus terhubung pada jaringan *wi-fi* yang sama. Maka dari itu diperlukan keamanan terhadap jaringan *wi-fi* dengan menggunakan keamanan WPA2-PSK. Dengan ini dapat meminimalisir serangan *Packet sniffing*. Sedangkan serangan menggunakan *burpsuite* penyerang hanya terhubung kedalam jaringan yang dapat mengakses internet dan menjalankan *burpsuite* untuk bertindak sebagai *proxy*.

Daftar Pustaka :

[1] D. Susianto and A. Rachmawati, "Implementasi dan Analisis Jaringan Menggunakan Wireshark, Cain and Abels, Network Minner," *J. Cendikia*, vol. XVI, pp. 120–125, 2018.

[2] Hendri Noviyanto, "Analisis Keamanan Wireless di Universitas Muhammadiyah Surakarta," UNIVERSITAS MUHAMMADIYAH SURAKARTA, 2012.

[3] A. Rizal Fauzi and I. Made Suartana, "Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids," *J. Manaj. Inform.*, vol. 8, no. 2, p. 7, 2018.

[4] R. E. Fitriani, "MENDESAIN KEAMANAN SISTEM JARINGAN," 2015.

[5] 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.

[6] L. H. Turner, *PENGANTAR TEORI KOMUNIKASI : Analisis dan Aplikasi*. Jakarta : Salemba Humanika, 2017.

[7] H. E. Wahanani, "Uji Coba Serangan Man In The Middle Pada Keamanan SSL Protokol HTTP," *J. Sist. Inf. dan Bisnis Cerdas*, vol. 13, no. 1, pp. 21–26, 2020, doi: 10.33005/sibc.v13i1.1769.

[8] 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

[9] H. Pranata, L. A. Abdillah, and U. Ependi, “Analisis Keamanan Protokol Secure Socket Layer (SSL) Terhadap Proses Sniffing di Jaringan,” pp. 21–22, 2015, [Online]. Available: http://arxiv.org/abs/1508.05457

[10] I. G. P. K. Juliharta, “Bussiness Impact Analysis Aplikasi Jaringan Komputer Dengan Teknik Packet Sniffing,” *J. Sist. Dan Inform.*, vol. 10, no. 1, pp. 149–158, 2015.

[11] M. Ferdy Adriant and Is Mardianto, “Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan,” *Semin. Nas. Cendekiawan*, pp. 224–228, 2015.

[12] P. T. Mahmud, “Sniffing Jaringan Menggunakan Wireshark,” *J. Jar. Komput.*, pp. 5–8, 2020.

[13] T. Setiawan, “Internet Menggunakan Hping, Nmap, Nessus, Dan Ethereal,” Institut Teknologi Bandung, 2004.

[14] E. M. Putra, B. Tujni, and E. S. Negara, “Analisis Kemanan Jaringan Internet (Wifi) Dari Serangan Packet Data Sniffing Di Universitas Muhammadiyah Palembang,” *J. Ilm. Teknol. Inf.*, 2018.

[15] Reza Kurniawan, "Analiss Kemanan Fasilitas Jaringan (WI-FI) Terhadap Serangan Packet Sniffing Pada Protocol HTTP dan HTTPS. Riau. Universitas Islam Riau