EVALUASI KEAMANAN JARINGAN WIRELESS HOTSPOT MENGGUNAKAN METODE SQUARE (STUDI KASUS WARNET MEDIANET SUMEDANG)

Yopi Hidayatul Akbar
Jurusan Teknik Informatika Dosen STMIK Sumedang
Email : yopi@stmik-sumedang.ac.id

ABSTRAK

Perkembangan teknologi infornasi pada saat ini sudah semakin maju, hal tersebut terbukti dengan banyaknya bermunculan software dan hardware mutakhir yang dapat menunjang kinerja kita sehari-hari. Sejalan dengan perkembangan teknologi informasi tersebut ada hal yang bersifat positif dan negatif dalam kegiatan teknologi informasi, dari sudut pandang negatif banyak penyalahgunaan teknologi informasi yang dapat menyebabkan kerugian bagi orang lain, sedangkan dari sudut pandang positif teknologi informasi mampu membantu pekerjaan kita dan mempercepat akses informasi yang kita perlukan. Penelitian ini bertujuan untuk mengevaluasi masalah persyaratan keamanan menggunakan metodologi Security Quality Requirements Engineering (SQUARE) berkaitan dengan risiko penyalahgunaan akses pada jaringan warnet khususnya jaringan wireless, dan bagaimana langkah untuk menanggulangi kondisi tersebut. Penelitian ini membahas evaluasi keamanan wireless hotspot menggunakan SQUARE sebagai suatu metodologi persyaratan keamanan untuk sarana teknologi informasi yang dapat digunakan untuk mengelola infrastruktur jaringan internet khususnya wireless agar lebih baik dan terhindar dari segala bentuk risiko, ancaman dan kerentanan yang dapat terjadi. Dengan Metodologi SQUARE diharapkan dapat menghindari dan meminimalisasi risiko dari penyalahgunaan akses sehingga tidak mengganggu proses bisnis yang dijalankan.

Kata Kunci : Evaluasi Keamanan, Wireless, SQUARE

PENDAHULUAN

a. Latar Belakang

Perkembangan teknologi informasi pada saat sekarang ini telah meningkat begitu cepat, seiring dengan perkembangan tersebut banyak bermunculan aplikasi, *gadget* dan *framework* terbaru yang mendukung kemajuan teknologi informasi. Namun di satu sisi dengan pekembangan teknologi informasi ada hal baik dan buruknya, jika dipandang dari sisi baiknya teknologi informasi telah banyak membantu kinerja perusahaan, dan di sisi buruknya teknologi informasi banyak yang disalahgunakan.Beberapa kasus yang terjadi akibat kemajuan teknologi informasi tersebut yaitu dapat melakukan peretasan terhadap situs, mencuri hak akses pengguna yang legal, mencuri data dan informasi yang bersifat penting, melakukan *deface* atau mengubah tampilan situs resmidengan tujuan untuk melakukan penipuan yang dapat mengakibatkan kerugian beberapa pihak.

Salah satu kemajuan teknologi informasi dalam hal jaringan internet yaitu *wireless*, atau sering juga disebut dengan *Wi-Fi*. Seperti kita ketahui *wireless* merupakan media/sarana untuk melakukan koneksi internet tanpa menggunakan kabel, banyak sekali perusahaan-perusahaan, universitas maupun dinas pemerintahan pada saat sekarang ini menggunakan *wireless hotspot* untuk jaringan internetnya, namun tidak dapat dipungkiri banyak sekali penyalahgunaan pada sistem jaringan *wireless**hotspot*misalnya pencurian informasi dan data maupun proses *hacking*melalui teknologi *wireless* tersebut.Aksi yang dilakukan pengguna illegal dalam jaringan wireless biasanya mencuri data *login* pengguna legal dengan menggunakan *tools*khusus, mengacak login pengguna bahkan masuk ke jaringan *wireless*

dengan cara illegal. Dengan kondisi tersebut maka sudah sepantasnya kita melakukan evaluasi dan merencanakan keamanan jaringan *wireless*sesuai dengan persyaratan keamanan yang berlaku agar terhindar dari aksi-aksi yang tidak diinginkan yaitu dengan cara memperbaiki infrastruktur jaringan internet dalam hal ini *wireless hotspot* dapat berjalan sesuai dengan yang diharapkan.

Warnet Medianet merupakan warnet yang sudah lama berkiprah dan cukup terkenal di wilayah angkrek Sumedang, warnet Medianet tersebut menyediakan beberapa klien dengan jaringan kabel dan ada diantaranya ruang khusus untuk wartawan yang ingin mengupload berita ke kantor pusat di Jakata untuk kepentingan publikasi dan terdapat juga sekitar ± 35 user yang berlangganan *internet* melalui jaringan *wireless hotspot.*Pada proses kinerja warnet medianet tersebut sering kali terjadi beberapa kasus berkaitan dengan penyalahgunaan hak akses dalam hal ini pencurian data pengguna yang sedang login melalui *wireless* sehingga pengguna yang legal menjadi terblokir, kemudian hal yang lain yaitu adanya penyadapan informasi dengan sebuah *tools* melalui jaringan LAN *(Local Area Network)*oleh pengguna warnet yang lain, selanjutnya sering terjadi proses acak login yang dilakukan pengguna illegal yang ingin mengakses jaringan *wireless* dengan menggunakan teknik *SQL injection* terhadap halaman menu *login* wifi.Kondisi tersebut dapat menyebabkanpengelola warnet medianet merasa dirugikan dan tidak nyaman dalam menjalankan usahanya sehingga pemilik warnet menginginkan dibuatnya suatu perencanaan infrastuktur serta mendefinisikan persyaratankeamanan yang dapat diterapkan dalam proses bisnis warnet agar dapat berjalan sesuai dengan yang diharapkan.

b. Ruang Lingkup

Berdasarkan latar belakang yang telah dikemukakan maka lingkup permasalahan yang akan dibahas adalah sebagai berikut :

1) Merencanakan infrastruktur jaringan internet khususnya wireless hotspot di warnet medianet.
2) Melakukan evaluasi terhadap persyaratan keamananmenggunakan metodologi SQUARE.

c. Tujuan Penelitian

Maksud dilakukannya penelitian ini adalah untuk mengumpulkan data yang relevan dengan mengidentifikasi masalah sehingga dapat dianalisis dan ditarik kesimpulannya, adapun tujuan penelitian ini adalah :

1) Membuat perencanaan berkaitan dengan infrastruktur jaringan internet khususnya wireless hotspot di warnet medianet Sumedang.
2) Melakukan evaluasi terhadap persyaratan keamananmenggunakan metodologi SQUARE.agar dapat diketahui faktor apa saja yang dapat mengganggu proses bisnis yang dijalankan agar dapat ditanggulangi secara tepat.

d. Metode Penelitian

Pada penelitian ini penulis menggunakan beberapa metode untuk menyelesaikan masalah antara lain meliputi :

1) Studi Pustaka, pada tahap ini penulis melakukan studi pembelajaran yang terkait dengan metodologi SQUARE dengan menggunakan media berupa Ebook, atau mencari bahan-bahan lainnya dari berbagai forum dan artikel online terkait evaluasi keamanan teknologi informasi.
2) Melakukan observasi dan wawancara, dimana penulis melakukan pengamatan langsung ke tempat atau objek yaitu Warnet Medianet Sumedang yang memiliki bisnis dalam menyebarluaskan akses internet menggunakan wireless hotspot. Wawancara dilakukan kepadaPengelola dan Administrator warnet.

PEMBAHASAN

a. SQUARE

SQUARE merupakan suatu model yang dikembangkan untuk memprediksi suatu proses persyaratan teknik,yang disesuaikan secara khusus untuk mengidentifikasi masalah persyaratan keamanan. SQUARE merupakan suatu sarana untuk memunculkan, mengkategorikan persyaratan keamanan yang diprioritaskan untuk sarana dan prasarana teknologi informasi dan aplikasi,banyak metode yang dapat digambarkan dengan baik melalui metode SQUARE dalam hal ini mengenai suatu kasus penyalahgunaan dalam suatu sistem. Berikut adalah tahapan metode SQUARE, antara lain :

1) Step 1 : *Agree on Definitions*(Mendefinisikan kebutuhan sistem)
   Menjamin komunikasi yang efektif dan jelas antara seorang *engineering* dengan *stakeholder* terkait dengan kebutuhan sistem yang akan dijalankan, dalam hal ini, *stakeholder*dapat mengetahui akses kontrol sebagai seperangkat kebijakan yang dapat dikelola
2) Step 2 : *Identify Security Goals*(Mengidentifikasi tujuan keamanan)
   Menyetujui serangkaian prioritas keamanan yang akan diterapkan, hal tersebut menjadi tanggung jawab sebagai relevansi persyaratan keamanan yang akan dihasilkan.
3) Step 3 : *Develop Artifacts*(Pengembangan Artefak)
   Tim *engineering* dan *stakeholder* dapat menghasilkan seperangkat persyaratan keamanan, tim harus mengumpulkan satu set lengkap artefak dari sistem.
   Berikut ini adalah jenis artefak yang harus dikumpulkan:
   a) Diagram arsitektur
   b) Diagram *use case*
   c) Diagram *Misuse Case*
   d) Attack Tree
   e) Template standar
4) Step 4 : *Perform Risk Assesment* (Penilaian resiko)
   Tujuan dari langkah ini adalah untuk mengidentifikasi kerentanan dan ancaman terhadap sistem yang berpotensi dapat terjadi, serta bagaimana cara penanggulangan terhadap permasalahan yang terjadi disertai dengan alasan yang logis.
5) Step 5 : *Select Elicitation Technique* (Memilih teknik elisitasi)
   Memilih teknik elisitasi yang cocok untuk melakukan penanganan terhadappekerjaan yang dilakukan.
6) Step 6 : *ElicitSecurity Requirements* (Permintaaan persyaratan keamanan)
   Elisitasi persyaratan keamananuntuk menyediakan pedoman rinci bagaimana melakukan elisitasi keamanan yang baik.
7) Step 7 : *Categorize Requirement* (Kategori kebutuhan)
   Mengklasifikasikan persyaratan sebagai hal yang penting, berkaitan dengansystem dan perangkat lunak.
8) Step 8 : *Prioritize Requirements* (Prioritas kebutuhan)
   Memprioritaskan kebutuhan keamanan sehingga para *stakeholder* dapat memilih untuk menerapkan prioritas kebutuhan yang sederhana dan fleksibel
9) Step 9 : *Requirements Inspection* (Kebutuhan penilaian)
   Menciptakan persyaratan keamanan yang akurat dan dapat diverifikasi. Pemeriksaan dapat dilakukan pada berbagai tingkat formalitas, Tujuan dari setiap metode adalah untuk menemukan kelemahan.

b. Temuan Masalah

Pada pembahasan penelitian ini, penulis mengambil referensi berdasarkan metodologi SQUARE yang telah dijelaskan pada poin sebelumnya. Untuk mengetahui faktor penyalahgunaan maka dilakukan pembagian kategori ancaman. Berikut ini merupakanpengkategorian ancaman yang terjadi antara lain sebagai berikut :

Tabel 1 Kategori Ancaman

No	Kategori Ancaman	Kondisi	Dampak	Kategori
1.	SQL Injection	Melakukan acak login pada menu utama login klien	Kehilangan data pengguna dalam hal ini user dan password pengguna legal	**Medium**
2.	Data Sniffing	Melakukan sniffing terhadap data yang ada dalam jaringan	Penyerang dapat mengetahui data secara jelas dalam jaringan	**High**
3.	Mac Address Spoofing	Mengambil mac address yang ada dalam jaringan	Penyerang dapat mendapatkan informasi yang disediakan untuk pengguna legal	**Medium**
4.	Spyware dan Trojans	Melakukan perusakan, penyalinan dan/atau pengintipan aktifitas sebuah komputer	Dapat memantau aktivitas klien, mengendalikan komputer serta dapat melakukan copy terhadap data user	**Low**
5.	Denial of Services (DoS)	Mengirim paket data dalam jumlah yang sangat bersar terhadap server dimana server tersebut tidak bisa memproses semuanya.	Membuat jaringan menjadi padat, sehingga tidak bisa diakses dan tidak merespon terhadap permintaan layanan	**Medium**

c. Merencanakan Infrastuktur Jaringan Wireless

Pada proses perencanaan infrastruktur jaringan wireless pada warnet medianet Sumedang menggunakan metodologi SQUARE, langkah yang dilakukan yaitu dengan mendefinisikan persyaratan keamanan berdasarkan metodologi SQUARE tersebut, dengan tahapan antara lain :

1. Mendefinisikan Kebutuhan Sistem *(Agree on Definitions)*
   Dalam mendefinisikan kebutuhan sistem warnet medianet langkah pertama yaitu mengumpulkan beberapa data dan informasi yang diperoleh guna memudahkan perencanaan dalam menerapkan sistem keamanan.
2. Mengidentifikasi Tujuan Keamanan (*Identify Security Goals)*
   Tujuan keamanan harus mempunyai dukungan yang jelas secara keseluruhan, beberapa persyaratan yang perlu dilakukan antara lain

Tabel 2.Tujuan Bisnis (*Business Goal*)

No.	Tujuan Bisnis
1.	Jaringan wireless dibangun untuk keperluan masyarakat yang memerlukan koneksi internetuntuk mendapatkan informasi yang dibutuhkan oleh pengguna.
2.	Jaringan wirelessdibangun untuk melayani masyarakat yang ingin memerlukan internet dengan sarana hotspot yang dikelola oleh administrator jaringansehingga masyarakat tidak perlu dating ke warnet cukup hanya mempunyai laptop/sejenisnya untuk dapat terkoneksi ke jaringan wireless.
3.	Jaringan wireless dapat menjaga privasi user, dalam hal ini pelanggan hotspotdan administrator yang berfungsi sebagai pengelola jaringan dan memperbaiki kesalahan jika dibutuhkan.
4.	Dengan adanya jaringan wireless dapat membantu masyarakat untuk dapat menikmati sarana internet dan memungkinkan pengguna untuk mengakses sumber daya jaringan dari hampir semua lokasi dimana pengguna tersebut berada dalam jangkauan wireless.

Tabel 3.Tujuan Keamanan (*Security Goals*)

Goals		Tujuan Keamanan
G-01	Kerahasiaan (*Confidentiality*)	Data admin, data user, informasi user, harus terjaga kerahasiaanya dari akses pengguna illegal yang tidak berwenang sampai suatu batas waktu yang ditentukan. Tujuannya agar pihak lain yang tidak berwenang/pengguna illegal tidak mengetahui data otentifikasi user.
G-02	Integritas Data (*Data Integrity*)	Data admin, data user, informasi user, harus terjaga keasliannya dari akses pihak luar yang tidak berwenang. Tujuannya agar user yang akan melakukan konektivitas dapat menjalankan semua aplikasi sesuai dengan prosedur yang ditentukan.
G-03	Ketersediaan (*Availability*)	Seluruh data dan informasi harus tersedia didalam sistem terutama ketika data tersebut dibutuhkan dan akan digunakan oleh user.
G-04	Kontrol Akses (*Access Control*)	1. Hanya administrator yang berwenang yang dapat melakukan menambah, mengubah atau penghapusan data user pada system 2. Adanya pengaturan (kontrol akses) terhadap para pengguna dan komponen sistem
G-05	Penggunaan (*Application*)	1. Keamanan harus terkelola secara terstruktur dan terencana, serta tidak menghambat proses bisnis 2. Menghindari resiko dari aktifitas yang merugikan system

3. Membangun Artefak (*Develop Artifacts*)

Dalam mengembangkan serangkaian artefak berfungsi sebagai hal yang sangat penting dalam menempatkan langkah-langkah berikutnya. Artefak termasuk diagram arsitektur sistem, penggunaan / penyalahgunaan kasus, pohon serangan, dan penilaian aset dan layanan pentin

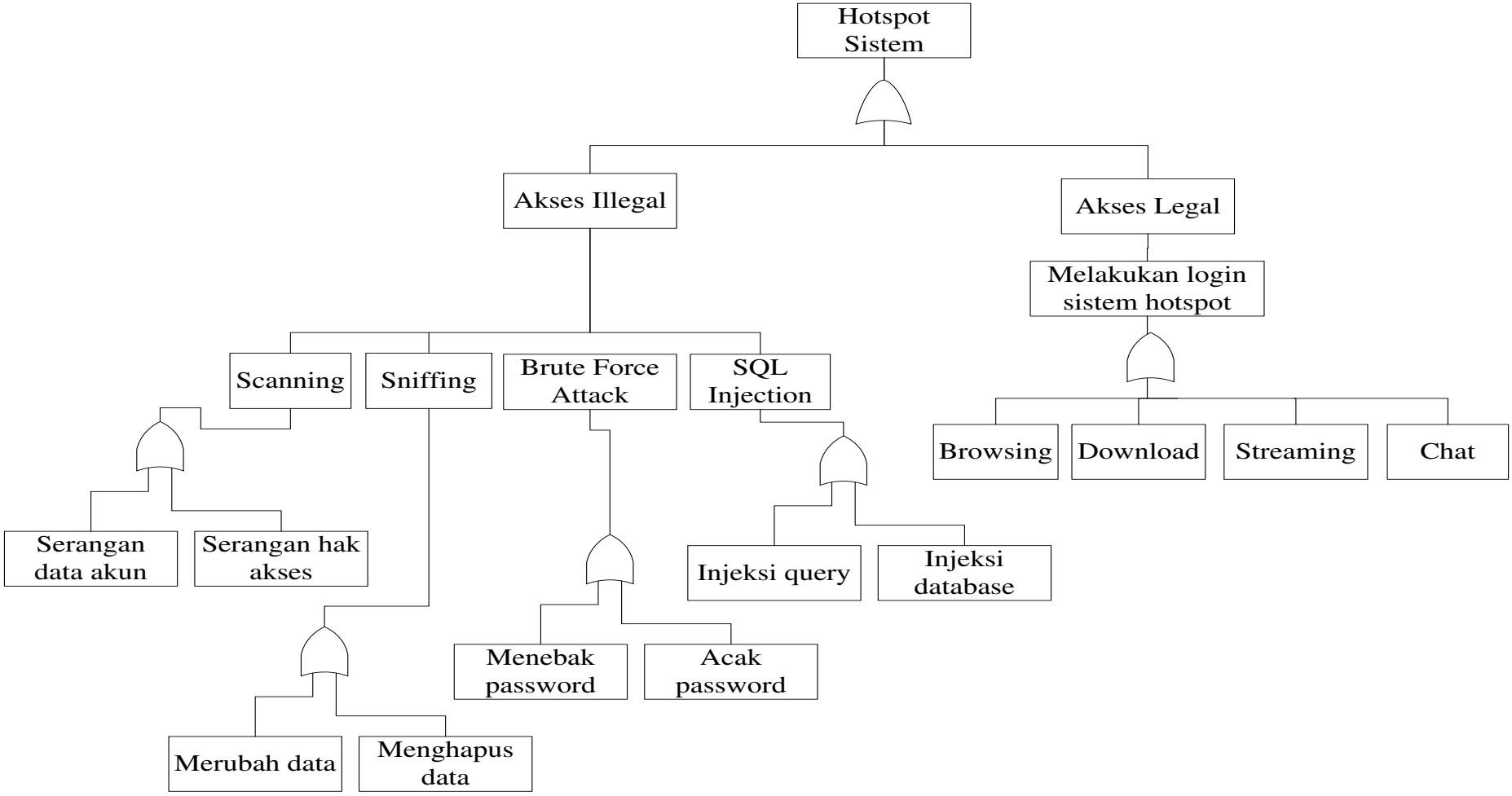
a. Arsitektur Sistem Jaringan Wireless

Pada proses perencanaan artefak maka langkah ini membutuhkan suatu arsitektur system jaringan yang menggambarkan kinerja system atau proses bisnis yang dilakukan, berikut ini merupakan arsitektur jaringan wireless warnet medianet

b. Pohon Serangan (Attack Tree)

Pohon serangan menyediakan, cara hirarki formal yang menggambarkan ancaman keamanan untuk sistem berdasarkan jenis serangan yang bisa terjadi dan bagaimana mereka dapat direalisasikan. Berikut ini akan digambarkan mengenai pohon serangan yang terjadi pada proses bisnis warnet medianet diantaranya :

1. Pohon serangan *scanning* (MC-01)
2. Pohon serangan *sniffing* (MC-02)
3. Pohon serangan *brute force authentication* (MC-03
4. Pohon serangan *SQL Injection* (MC-04)



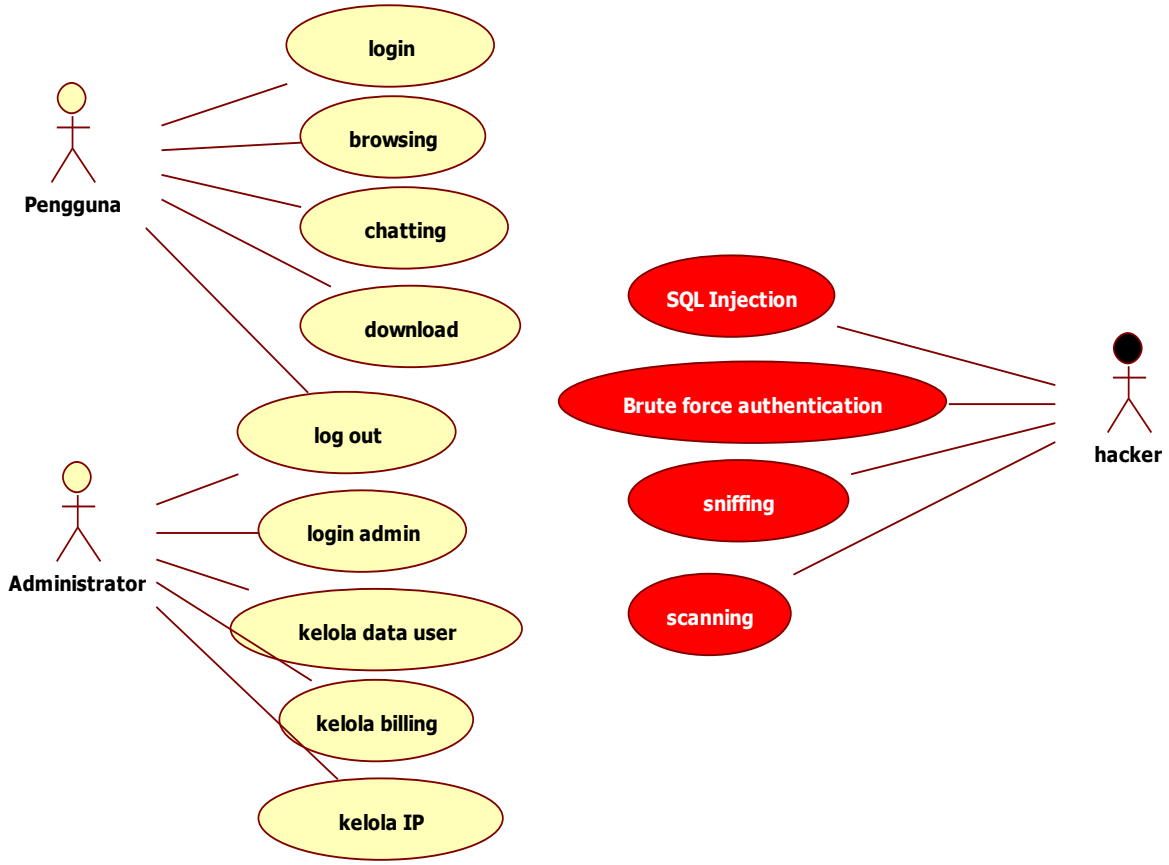
Gambar 1 Pohon Serangan

c. Use case

Use case merupakan scenario artefak yang memaksa para pemangku kepentingan untuk menjawab aktivitas yang dilakukan dalam proses bisnis, dengan menyediakan konteks untuk operasi, pemangku kepentingan dan tim rekayasa dapat memperoleh pemahaman yang mendalam tentang interaksi dari komponen sistem

d. Misuse Case

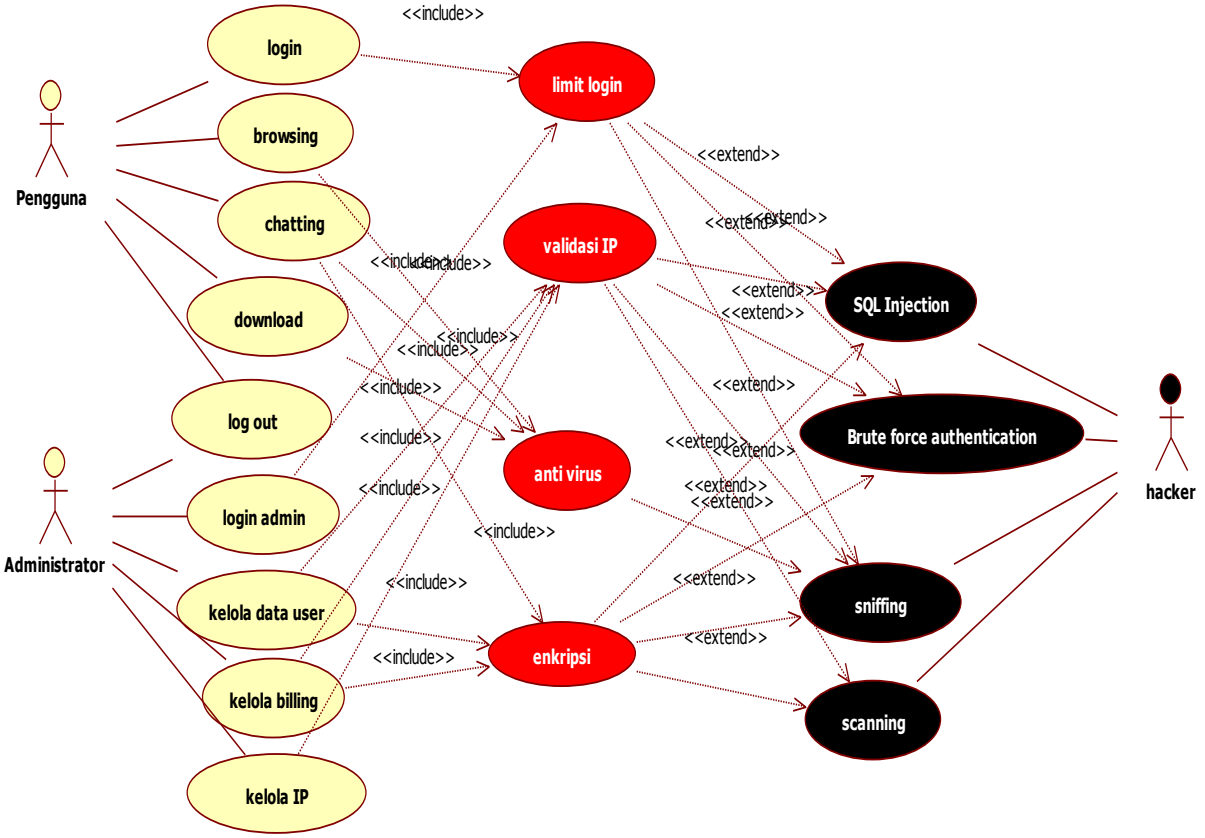
Misuse cases merupakan aktivitas serangan yang terjadai pada suatu system, dalam hal ini seorang pengguna illegal yang berusaha untuk masuk kedalam system dengan menggunakan langkah-langkah atau metode yang bersifat illegal



Gambar 2. Misuse Cases

e. Use case Mitigasi

Use case mitigasi merupakan aktivitas yang berfungsi untuk melakukan pencegahan terhadap penyalahgunaan akses illegal yang terjadi pada system. Berikut ini merupakan use case mitigasi pada warnet medianet



Gambar 3. Use Case Mitigasi

4. Melakukan penilaian risiko (Perform Risk Assessment)
   Dalam melakukan analisis, ada beberapa metodologi penilaian risiko yang dianalisis untuk menentukan yang cocok untuk elisitasi persyaratan keamanan. Hasil dari analisis ini dapat disajikan dalam bagian ini sebagai contoh teknik yang tersedia, serta kekuatan dan kelemahan sistem
   a) The Government Accountability Office's (GAO) model [GAO 99]
   b) National Institute of Standards and Technology (NIST) model [Stoneburner 02]
   c) NSA's INFOSEC Assessment Methodology [NSA 05]
   d) Butler's Security Attribute Evaluation Method (SAEM) [Butler 02]
   e) CMU's "V-RATE" method [Lipson 01]
   f) Yacov Haimes's RFRM model [Haimes 04]
   g) CMU's Survivable Systems Analysis method [CERT/CC 02]
   h) Martin Feather's DDP model [Cornford 04]

Tabel 4. Hasil Penilaian Resiko Studi Literatur

	Untuk organisasi kecil	jangka waktu singkat	Pengumpulan data	persyaratan	Rata-rata
GAO	2	4	2	2	2.50
NIST	**2**	**2**	**1**	**1**	**1.5**
NSA/IAM	3	3	2	2	2.50

SAEM	4	4	4	4	4.00
V-RATE	3	4	4	4	3.75
Haimes	**2**	**2**	**2**	**2**	**2.00**
SSA	2	2	2	4	2.50
DDP	3	4	2	4	3.25

Berkaitan dengan hasil penilaian resiko tersebut diatas, selanjutnya kita membuat penilaian resiko terhadap sistem yang kita rencanakan dalam keamanan jaringan warnet/wireless

Tabel 5. Penilaian Resiko

Level	**Identifikasi**	**Aksi**	**Karakter Resiko**
1.	Pengguna dalam kategori illegal melakukan penyalahgunaan hak akses yaitu dengan mencuri data dan informasi user yang sah, dalam hal ini berkaitan dengan username dan password. Selanjutnya penyerang melakukan pencurian atau pengubahan terhadap data dan informasi user yang sah yang terdaftar dalam jaringan.	Pengguna illegal menggunakan tools atau aplikasi untuk dapat masuk kedalam sistem kemudian melakukan pencurian terhadap data user, dan informasi user, atau melakukan manipulasi data user yang terdaftar dalam jaringan	**Very High**
2.	Pengguna illegal melakukan aksi penyalahgunaan terhadap sistem jaringan wireless melalui form login di browser . Pengguna illegal melakukan aksi penyerangan dengan mengacak alamat IP yang dimiliki oleh pengguna yang sah supaya dapat masuk ke dalam sistem	Pengguna luar menggunakan sistem yang illegal dengan menyadap akun user. Penyerang menggunakan aplikasi seperti *hide ip* untuk dapat masuk kedalam sistem melalui akun user	**High**
3.	Pengguna illegalmengirim tools berbahaya seperti virus, trojan, spyware, malware pada jaringan aktif yang dapat menghentikan pelayanan	Penyerang mencuri username dan password pengguna dan admin agar dapat masuk kedalam system	**High**
4.	Pengguna illegal melakukan aksi scanning dengan menggunakan tools sehingga dapat mengetahui celah keamanan yang lemah	Pengguna illegal melakukan penyerangan terhadap database sistem yang berisi informasiusername dan password pengguna yang sah dan melakukan manipulasi data / informasi yang dapat mengakibatkan kerugian bagi pengguna yang.	**High**

5. Memilih Teknik Elisitasi (select elicitation technique)

Tabel 6. Matriks Perbandingan

	Misuse cases	**SSM**	**QFD**	**CORE**	**IBIS**	**JAD**	**FODA**	**CDA**	**ARM**
Adaptasi	3	1	3	2	2	3	2	1	2
Case Tools	1	2	1	1	3	2	1	1	1
Persetujuan klien	2	2	2	2	3	2	1	3	3
Kompleksitas	2	2	1	2	3	2	1	1	2
Laporan gambar	2	2	1	1	2	1	2	2	3
Waktu penerapan	2	2	1	1	2	1	2	2	3
Kurva pembelajaran	3	1	2	1	3	2	1	1	1
Kematangan	2	3	3	3	2	3	2	2	1
Skalabilitas	1	3	3	3	2	3	2	1	2

Skala : 3 = sangat baik, 2 = lemah, 1 = buruk.

6. Mendapatkan persyaratan keamanan *(Elicit Security Requirements)*

Tim yang melakukan analisis terhadap system tidak menggunakan teknik elisitasi terstruktur untuk mengembangkan kembali persyaratan dengan para pemangku kepentingan. Namun pada langkah ini tim memanfaatkan metode wawancara terstruktu berkaitan dengan persyaratan keamanan

Tabel 7. Persyaratan Keamanan

R-01	Sistem ini diperlukan untuk menentukan langkah-langkah otentikasi pada gateway. Yaitu dengan cara membatasi hanya komputer dengan Hak akses IP Address tertentu yang telah didaftarkan pada komputer server yang dapat melakukan manipulasi data user	G-04 G-05
R-02	Sistem ini diperlukan untuk menentukan mekanisme kontrol akses berbasis peran yang mengatur unsur-unsur sistem (data, fungsi, dll) pengguna dapat melihat, memodifikasi, dan / atau berinteraksi dengan system. Karakter yang ditentukan hanya memperbolehkan huruf a – z, A – Z atau angka 0 – 9 dan melarang karakter unik seperti @, %, ^, &, * , /, \, “, ‘ atau symbol	G-02 G-04 G-05
R-03	System ini diperlukan untuk kelangsungan rencana operasi untuk memastikan ketersediaan sistem. Setiap user diharuskan menggunakan username dan kode pengamanan (*password*) berupa kombinasi karakter, misalnya antara angka, huruf besar atau kecil, karakter tententu.	G-01 G-02 G-03 G-05

R-04	System diperlukan untuk petugas keamanan yang ditunjuk agar dapat mengaudit status dan penggunaan sumber daya sistem termasuk perangkat keamanan.	G-02
R-05	Petugas yang telah ditunjuk diminta untuk mengaudit status sumber daya sistem dan penggunaannya secara teratur.	G-02 G-05
R-06	System diperlukan untuk komunikasi system jaringan yang dilindungi dari informasi yang tidak sah, pengumpulan dan / atau menyadap dengan enkripsi dan teknik lain yang. Enkripsi perlu diterapkan pada keamanan jaringan, misalnya otentifikasi login. Hal tersebut untuk mencegah agar penyelundup yang telah menyadap atau memasuki sistem tidak dapat mengetahui akses login.	G-01 G-04
R-07	Ini merupakan persyaratan bahwa kedua proses inti untuk mencegah instalasi perangkat lunak atau perangkat tanpa izin sebelumnya.	G-02 G-05
R-08	Melindungi perangkat fisik agar dilindungi dari kehancuran, kerusakan, pencurian, sabotase, atau penggantian secara tidak diketahuiterkecuali kerusakan akibat vandalisme, sabotase, teroris, atau tindakan alam.	G-02 G-05
R-09	Menerapkan komponen perangkat lunak yang dirancang untuk memanfaatkan keamanan software terbaik.	G-03 G-05

Tabel 8. Teknik Elisitasi

	Misuse Cases	Accelerated Requirements Method (ARM)
Adaptability	3	3
CASE Tool	1	1
Client Acceptance	2	2
Complexity	2	1
Graphical Output	2	2
Implementation Duration	2	2
Learning Curve	3	2
Maturity	2	2
Scalability	1	2
Jumlah	18	17

Skala : 3 = very good, 2 = fair, 1 = poor

Dari tabel di atas dapat diketahui bahwa Misuse cases lebih mendominasi untuk dapat melakukan tahapan analisis kerentanan keamanan sistem dibandingkan dengan *Accelerated Requirements Method* (ARM). Oleh karena itu kami menggunakan misuse cases dalam melakukan langkah analisis keamanan sistem

7. Mengkategorikan Persyaratan (*Categorize Requirements*)

Setelah persyaratan awal yang dihasilkan oleh para pemangku kepentingan maka selanjutnyayaitu mengelompokan persyaratan keamanan yang dipilih dan menciptakan nama unik untuk setiap kelompok,dalam hal ini menggabungkan langkah-langkah pengelompokan, penamaan, dan kategorisasi bersama-sama

Tabel 9. Kategori Persyaratan

Group A : **Kerahasiaan**	Group B : **Akses Kontrol**
Klien atau pelanggan yang mengaksesinternet melalui LAN dan wireless harus terjaga secara rahasia berkaitan dengan data dan informasi pengguna yang sah dari akses pengguna yang illegal.	1. Pada kontrol sistem ditentukan hanya user yang terdaftar sajayang dapat melakukan akses. 2. Adanya pengaturan akses control terhadap keamanan jaringan LAN dan wireless.
Group C : **Integritas Data**	Group D : **Pengelolaan**
Harus dilakukan secara rutin mengenai setting terhadap data user, akses control agar terhindar dari serangan pengguna illegal.	Adanya proses manajemen hak akses yang dapat dipertanggungjawabkan atas kebenaran data yang ada. Melakukan log terhadap aktifitas yang terjadi pada system jaringan
Group E: **Penggunaan**	Group F : **Authentifikasi**
1. Menerapkan manajemen terhadap Sistem keamanan agar dapat dilakukan pengelolaan & tidak mengganggu terhadap kinerja sistem yang berjalan. 2. Sistem harus selalu tersedia untuk melakukan autentikasi terhadap akses user 3. Menghilangkan risiko terhadap aktifitas yang dapat merusak sistem.	Sistem harus dapat melakukan autentifikasi dengan baik sesuai dengan prosedur dan ketentuan

8. Melakukan Prioritas Persyaratan *(Prioritize Requirements)*
   Pada proses ini akan dilakukan pemilihan prioritas persyaratan yang berkaitan dengan sistem keamanan pada jaringan wireless dan LAN pada warnet medianet berdasarkan misusecases yang telah dibuat sebelumnya. Untuk melakukan prioritas terhadap serangan yang mungkin dapat terjadi dilakukan pemilihan berdasarkan ancaman mana yang lebih berbahaya, maka digunakan tabel priortitas ancaman yang diharapkan dapat menangulangi permasalahan tersebut

Tabel 10. Prioritas Keamanan

Tujuan	**Confidentiality, Integrity, dan Availability**
Kebutuhan	- Keamanan sistem login dan server - Kemanan pada alamat IP - Database yang terjaga kerahasiaannya
Kategori	- *Unauthorize Attack* - *Access Control* - *Privacy* - *Authentication*
Rekomendasi	- Pemasangan firewall pada server - Penggunaan tanda tangan digital untuk sistem login - Patching pada sistem aplikasi - Pemasangan anti virus - Menerapkan enkripsi pada system *database* - Perubahan password pengguna secara rutin

Tabel 11. Kategori Prioritas

Misuse cases	A1	A2	A3	A4	Rata-rata	Prioritas
MC-01	8	9	9	9	8.75	Tinggi
MC-02	9	8	9	8	8.50	Tinggi
MC-03	6	7	7	6	6.50	Sedang
MC-04	8	7	7	7	7.25	Tinggi

9. Kebutuhan Penilaian *(Requirements Inspection)*

Proses selanjutnya yaitu requirements inspection yaitu bertujuan untuk melakukan penilaian terhadap perencanaan yang telah dilakukan. Metodologi ini memberikan tanggung jawab terhadap anggota tim inspeksi dan mengembangkan log yang memiliki peringkat masalah

Tabel 12. Rekafitulasi Hasil Penilaian Responden

No. Item	**Indikator Variabel**	**Total Skor**	**%**	**Kriteria**
1.	Perlu diterapkan keamanan jaringan pada warnet medianet agar terhindar dari penyalahgunaan	146	83,43	Baik
2.	Semua pengguna warnet dan pelanggan wireless harus dapat terjaga privasinya	141	80,57	Baik
3.	Manajemen password harus dilakukan secara rutin	144	82,29	Baik
4.	Melakukan pengamanan pada setiap PC dengan memasang antivirus	135	77,14	Baik
5.	Melakukan pengamanan pada mikrotik untuk mengatasi acak login	140	80,00	Baik
6.	Sistem harus dapat mendeteksi alamat IP yang mencurigakan	128	73,14	Baik
7.	Administrator wajib memblokir alamat IP yang mencurigakan	143	81,71	Baik
8.	Pengguna wajib mengikuti prosedur yang diterapkan oleh warnet medianet	135	77,14	Baik
9.	Sistem enkripsi wajib diterapkan untuk melindungi data dan informasi warnet	144	82,29	Baik
10.	Warnet medianet wajib mencabut kerjasama dengan pengguna yang berusaha masuk ke sistem pengguna yang lain	125	71,43	Baik
	Jumlah	**1381**		**Baik**

Data : Hasil Penelitian Tahun 2014

Nilai Ideal = 10 item x 35 orang x 5 = 1750

Hasil pengolahan data diatas menunjukan bahwa jumlah keseluruhan jawaban responden adalah sebesar 1381 dari nilai ideal 1750 dengan persentase sehingga dapat dikatakan secara keseluruhan pertanyaan yang berkaitan dengan keamaman jaringan internet pada warnet medianet Sumedang berada pada kategori **Baik,** meskipun masih ada beberapa celah keamanan yang belum dibahas dan belum dilakukan analisis keamanannya.

PENUTUP

a. Kesimpulan

1. Pada tahapan evaluasi keamanan jaringan internet menggunakan metode SQUARE pada warnet medianet diharapkan dapat memberikan kontribusi yang bermanfaat mengenai bagaimana melakukan pengamanan dan mitigasiterhadap segala bentuk penyalahgunaan hak akses yang dapat menimbulkan ancaman sehingga dapat merugikan pengelola warnet medianet.
2. Proses perencanaan infrastruktur keamanan jaringan internet pada warnet medianet dengan menggunakan metode SQUARE tentunya memerlukan alat ukur yang dapat memberikan solusi, gambaran sistem dan rekomendasi yang baik, dalam hal ini dengan menggunakan desain sistem UML agar kita dapat mengetahui kebutuhan dan persyaratan keamanan yang dapat dijadikan kebijakan yang lebih baik.
3. Berdasarkan hasil evaluasi terhadap keamanan jaringan internet warnet medianet sumedang khususnya wireless hotspot menunjukan hasil yang baik, dalam hal ini segala bentuk ancaman dan penyalahgunaan hak akses masih dapat ditangani meskipun belum optimal masih ada celah keamanan yang belum dilakukan analisis.

b. Saran

1. Untuk dapat meningkatkan sistem keamanan yang lebih baik, diharapkan untuk melakukan pengecekan secara rutin pada bagian kontrol akses agar data dan informasi yang berkaitan dengan pengguna yang sah dapat terjaga dan terhindar dari segala bentuk ancaman yang mungkin saja dapat terjadi diluar dugaan.
2. Untuk penelitian lebih lanjut diharapkan dapat menambah beberapa kebijakan dan prosedur keamanan jaringan yang lebih baik guna menjaga keberlangsungan bisnis warnet medianet agar lebih baik lagi agar dapat meminimalisir segala bentuk ancaman dan serangan baik yang disengaja maupun yang tidak disengaja yang dilakukan oleh pengguna atau pelanggan yang bekerjasama dengan pihak warnet medianet sumedang.

DAFTAR PUSTAKA

[1] Beck K (1999) *Extreme Programming Explained*. Addison-Wesley, Upper Saddle River

[2] Berander P, Wohlin C (2004) *Differences in Views between Development Roles in SoftwareProcess Improvement – A Quantitative Comparison*. Proceedings of the 8 th

[3] Berander P (2004) *Using Students as Subjects in Requirements Prioritization. Proceedings of the 2004 International Symposium on Empirical Software Engineering* (ISESE'04). EEE Computer Society, Los Alamitos, pp 167-176

[4] Fahmy, Syahrul, Haslinda Nurul, et.al. "*Evaluating the Quality of Software in e-Book Using the ISO 9126 Model*." International Journal of Control and Automation, vol. 5 (2012).

[5] Krutz,R.L. & Vines, R.D. The CISM Prep Guide : *Mastering the five domains of Information Security Management*, Wiley Publishing, Indianapolis,2003.

[6] Nancy R. Mead Eric D. Hough Theodore R. Stehney (2005) *II Security Quality Requirements Engineering (SQUARE) Methodology*