ANALISIS VULNERABILITAS BERBASIS GRAF SERANGAN TERHADAP KEAMANAN *E-VOTING*

Teguh Nurhadi Suharsono
Program Studi Teknik Informatika
Universitas Sangga Buana YPKP Bandung
teguhns21@gmail.com

Abstrak

Dengan semakin banyak dan luasnya persebaran pemilih, semakin kompleksnya aspek kehidupan sosial, dan kebutuhan untuk mengelola proses pemungutan suara dengan efisien dan penetapan hasil dengan lebih cepat, pemungutan suara berbasis elektronik (e-voting) menjadi pilihan yang lebih menjanjikan. Sistem e-Voting membutuhkan perhatian yang tinggi terhadap persyaratan keamanan, baik keamanan informasi maupun jaringan. Pada penelitian ini dikembangkan framework untuk analisa keamanan e-Voting dan Algoritma untuk keamanan jaringan berbasis graf serangan. Dalam penelitian ini juga digunakan metode untuk menghasilkan graf yang mempertimbangkan kinerja jaringan dan privilege attacker pada setiap host dan dapat dipakai sebagai alat untuk menganalisis vulnerabilitas jaringan. Algoritma yang diusulkan untuk menghasilkan graf status, graf host dan graf vulnerabilitas. Framework untuk mengevaluasi dan meningkatkan keamanan jaringan e-Voting.

Kata Kunci: *e-voting, persyaratan keamanan, framework evaluasi analisa vulnerabilitas, graf serangan, algoritma graf serangan*

I. PENDAHULUAN

Pemungutan suara telah menjadi bagian penting dari sistem demokrasi, baik untuk menentukan pilihan terkait kebijakan, memilih wakil yang akan duduk dalam majelis perwakilan, maupun untuk memilih pemimpin. Perkembangan teknologi terutama yang berbasis elektornik yang mendukung terhadap sistem pemilihan umum semakin berkembang, seperti Marksense (menggunakan teknik *optical scan*) mulai digunakan pada pemilihan presiden Amerika tahun 1996, dan beragam perangkat Direct Recording Electronic (DRE) [1].

Dengan semakin banyak dan luasnya persebaran pemilih, semakin kompleksnya aspek kehidupan sosial, dan kebutuhan untuk mengelola proses pemungutan suara dengan efisien dan penetapan hasil dengan lebih cepat, pemungutan suara berbasis elektronik (*e-voting*) menjadi pilihan yang lebih menjanjikan. *E-voting* adalah suatu sistem pemilihan dimana data dicatat, disimpan, dan diproses dalam bentuk informasi digital [2]. Centinkaya dan Centinkaya menambahkan bahwa e-voting adalah penggunaan perlengkapan komputer atau proses komputerisasi *voting* untuk kartu suara pada pemungutan suara [3]. Jadi *e-voting* pada hakekatnya adalah pelaksanaan pemungutan suara yang dilakukan secara elektronik (*digital*) mulai dari proses pendaftaran pemilih, pelaksanaan pemilihan, penghitungan suara, dan pengiriman hasil suara.

Penerapan e-voting diharapkan dapat mengatasi permasalahan yang timbul dari pemilu yang diadakan secara konvensional, yaitu [4] [5].

1. Lebih mempercepat dalam penghitungan suara.
2. Akuratnya hasil penghitungan suara.
3. Bahan cetakan untuk kertas suara.
4. Biaya pengiriman kertas suara lebih hemat.
5. Bagi kaum yang mempunyai keterbatasan fisik (cacat) dapat menyediakan akses yang lebih baik.
6. Bagi masyarakat yang mempunyai keterbatasan waktu untuk mendatangi tempat pemilihan suara (TPS) lebih terakomodasi.

7. Kertas suara dapat dibuat ke dalam berbagai versi bahasa.
8. Akses informasi yang lebih banyak berkaitan dengan pilihan suara.
9. Dapat mengendalikan pihak yang tidak berhak untuk memilih.

E-voting mempunyai prospek yang baik jika diterapkan pada suatu negara karena [6]:

1. Kpercayaan banyak negara bahwa *e-voting* akan dijumpai pada masa yang akan datang.
2. Kenyamanan dalam *e-voting* dapat memuaskan pemilih.
3. *M*emenuhi kebutuhan khusus bagi masyarakat yang mempunyai keterbatasan fisik (cacat).
4. Untuk skala kecil banyak negara yang akhir-akhir ini sudah menerapkan *e-voting*.
5. Banyak negara yang bermaksud mengganti sistem pemilihan umumnya menemui kesulitan berkenaan dengan terbatasnya pilihan-pilihan yang tersedia.
6. Banyak negara yang tertarik pada sistem *e-voting* layar sentuh.

E-voting berbasis *online* dapat dilaksanakan dalam beberapa metode [6]:

1. Sistem pemindaian optik. Sistem ini dilakukan dengan cara kertas diberikan kepada para pemilih kemudian hasilnya direkam dan dihitung secara elektronik. Metode ini harus menyediakan surat suara yang dapat dipindai dengan optik dan membutuhkan rancangan yang rumit dan biaya mahal. Di samping itu, tanda yang melewati batas kotak marka suara dapat menyebabkan kesalahan penghitungan oleh mesin pemindai. Sistem ini biasa disebut sebagai *e-counting*.
2. Sistem Direct Recording Electronic (DRE). Metode ini para pemilih memberikan hak suaranya melalui komputer atau layar sentuh atau panel/papan suara elektronik. Kemudian hasil pemungutan suara disimpan di dalam memori di TPS dan dapat dikirimkan baik melalui jaringan maupun *offline* ke pusat penghitungan suara nasional. Para pemilih masih diwajibkan untuk datang ke TPS namun data penghitungan suara sudah dapat disimpan dan diproses secara *realtime* dan *online*.
3. *Internet voting*. Pemilih dapat memberikan hak suaranya dari mana saja secara *online* melalui komputer yang terhubung dengan jaringan di mana pemungutan suara di TPS langsung direkam secara terpusat. Metode ini membutuhkan jaringan komunikasi data yang berpita lebar dan keamanan yang handal.

Tipe *e-voting* yang manapun yang dipilih untuk digunakan tetap mensyaratkan adanya perhatian yang serius terhadap aspek keamanannya. Keamanan adalah suatu proses menyediakan *confidentiality* (kerahasiaan), integritas dan *availability* (ketersediaan) terhadap suatu entitas berdasarkan suatu *policy* (kebijakan) [7]. Secara garis besar, persyaratan keamanan untuk *e-voting* dapat dibagi menjadi tiga bagian besar, yakni: persyaratan umum, persyaratan khusus, dan persyaratan tambahan. Persyaratan umum adalah persyaratan yang berlaku untuk semua sistem berbasis teknologi informasi dan komunikasi. Persyaratan khusus adalah persyaratan yang secara khusus muncul dalam konteks *e-voting*. Sedangkan persyaratan tambahan adalah meskipun bukan merupakan persyaratan yang secara langsung terkait dengan keamanan, namun akan dapat membantu kemudahan pengelolaan, menaikkan tingkat keikutsertaan dalam pemungutan suara, dan sedikit banyak akan mempengaruhi upaya penjaminan keamanan sistem e-voting secara keseluruhan.

Keamanan berkaitan erat dengan ancaman dan vulnerabilitas [8]. Pengertian ancaman dan vulnerabilitas adalah:

Ancaman adalah suatu kondisi lingkungan yang mempunyai potensi menyebabkan kehilangan atau kemacetan.

Jenis ancaman dapat dibedakan menjadi:

1. Ancaman fisik (misalnya kebakaran, banjir, kegagalan bangunan atau kegagalan daya).
2. Ancaman peralatan (misalnya CPU, jaringan, atau kegagalan media penyimpanan).
3. Ancaman manusia (misalnya kesalahan operator atau desain, pencurian sumber daya).

Vulnerabilitas adalah pengaruh kemungkinan suatu ancaman menjadi kenyataan dan berhubungan dengan kelemahan

pada sistem yang mungkin tereksploitasi dan menyebabkan kehilangan atau kemacetan.

Sejalan dengan berkembangnya lingkungan jaringan, ancaman internal dan eksternal juga akan muncul. Proses evaluasi terhadap keamanan perangkat keras dan perangkat lunak jaringan dan prosesnya serta melakukan penyesuaian untuk meningkatkan security jaringan disebut network hardening. *Network hardening* merupakan proses yang ditujukan untuk meningkatkan keamanan jaringan komputer dengan menerapkan *countermeasure* misalnya dengan mengimplementasikan software patch, memperkenalkan sistem *security* baru dan mengadopsi konfigurasi dan kebijakan operasi yang lebih baik. Hal utama dalam konsep *network hardening* adalah konsisten dalam mengevaluasi layout dan konfigurasi jaringan. Ancaman keamanan selalu mengarah pada pengeksploitasian vulnerabilitas pada lingkungan dengan perangkat keras, perangkat lunak dan protokol keamanan yang usang (*out-of-date*). Pemahaman tentang letak lubang keamanan pada jaringan merupakan langkah esensial yang pertama menuju *network hardening*. Masalah pertama adalah mengidentifikasi bahwa lubang keamanan itu ada. Tentu saja bukan hal yang bijak menunggu sampai jaringan kita ditembus oleh penyusup [9].

Pada jaringan komputer terdapat vulnerabilitas yang ada pada *host* di jaringan. Vulnerabilitas ini memungkinkan penyusup untuk masuk ke dalam jaringan komputer. Urutan vulnerabilitas yang dilalui oleh penyusup dapat digambarkan menjadi suatu graf serangan. Graf serangan merupakan sebuah abstraksi yang menggambarkan cara penyerang melanggar kebijakan keamanan dengan cara memanfaatkan saling ketergantungan di antara berbagai vulnerabilitas yang ada [9].

II. PERSYARATAN KEAMANAN E-VOTING

Secara garis besar, persyaratan keamanan untuk e-voting dapat dibagi menjadi tiga bagian besar, yakni: persyaratan umum, persyaratan khusus, dan persyaratan tambahan. Dengan memperhatikan hal-hal yang disebutkan oleh Fujioka dkk. [10], Cranor dan Cytron [11], Salini dan Kanmani [12], Wu dkk. [13], dan Adeshina dan Ojo [14] dapat dituliskan daftar persyaratan sebagai berikut:

A. Persyaratan Umum

Berupa persyaratan yang berlaku untuk semua sistem berbasis teknologi informasi dan komunikasi, yakni:

1. Kerahasiaan (*confidentiality*). Semua data yang disimpan, diolah, dan dipertukarkan melalui jaringan komunikasi harus dijamin agar hanya bisa diakses oleh pihak yang berhak, misalnya: detil informasi tentang data diri pemilih harus dijamin tidak terbuka untuk publik.
2. Integritas (*integrity*). Semua data harus dijamin tidak mengalami perubahan yang tidak sah, misal: basis data yang berisi hasil pemungutan suara harus dijaga agar tidak termodifikasi oleh siapapun secara tidak sah.
3. Autentikasi (*authentication*). Sistem harus bisa dan memberikan fasilitas kepada semua pihak terkait untuk membuktikan kebenaran klaim identitasnya, misal: semua pihak (pemilih, kandidat, petugas pemilihan, saksi dll.) harus terlebih dahulu dapat menunjukkan bukti identitasnya sebelum berinteraksi dengan sistem.
4. Ketersediaan (*availability*). Sistem harus dijamin dalam kondisi yang baik dan menyediakan layanan sebagaimana dijanjikan dengan derajat ketersediaan tertentu, misal: harus diupayakan dan dijamin bahwa sistem *e-voting* akan tersedia dan dapat diakses dalam 99,9999% dari seluruh waktu pemilihan yang telah ditetapkan.

B. Persyaratan Khusus

Berupa persyaratan yang secara khusus muncul dalam konteks *e-voting*, yaitu:

1. *Eligibility*: hanya orang yang ada dalam daftar pemilih sah yang dapat mengikuti pemungutan suara dan setiap pemilih yang sah hanya boleh sekali menggunakan hak pilihnya (memasukkan suara).
2. *Anonymity*: tidak ada siapapun (atau apapun) yang dapat merunut hubungan antara pilihan (suara) dengan pemilih yang memasukkannya.
3. *Privacy*: tidak ada pemilih yang memiliki cukup bukti tentang isi pilihannya dan dapat menunjukkannya kepada pihak lain.
4. *Accuracy*: tidak ada siapapun (atau apapun) yang dapat mengubah, menghapus, atau menduplikasi suara yang sah.

5. *Verifiability*: setiap pemilih harus dapat memeriksa apakah pilihannya telah tercatat dengan benar dan system dapat menunjukkan bahwa semua suara sah telah dihitung dengan benar.
6. *Fairness*: semua suara (pilihan) yang telah masuk ke sistem dan jumlah perolehan suara sementara tiap kandidat tidak dapat diketahui oleh siapapun sebelum pengumuman hasil akhir resminya.
7. *Dispute-freeness*: sistem harus menyediakan mekanisme dan artefak yang dibutuhkan untuk menyelesaikan sengketa yang mungkin muncul di semua tahapan.
8. *Auditability*: sistem harus dapat diaudit untuk menjamin semua prosesnya sesuai dengan spesifikasi dan semua ketidaksesuaian dapat ditangani dengan benar.

C. Persyaratan Tambahan

Meskipun bukan merupakan persyaratan yang secara langsung terkait dengan keamanan, namun hal-hal di bawah ini akan dapat membantu kemudahan pengelolaan, menaikkan tingkat keikutsertaan dalam pemungutan suara, dan sedikit banyak akan mempengaruhi upaya penjaminan keamanan sistem *e-voting* secara keseluruhan:

1. Kenyamanan (*convenience*). Pemilih akan merasa nyaman jika dapat memasukkan pilihan atau suaranya melalui satu sesi pemungutan suara dengan cepat dan mudah, tanpa membutuhkan perangkat dan ketrampilan khusus.
2. Efisiensi (*efficiency*). Penyelenggara pemungutan suara akan terbantu jika sistem *e-voting* dirancang untuk beroperasi dengan kebutuhan sumber daya komputasi dan waktu proses seminimal mungkin.
3. Fleksibilitas (*flexibility*). Dengan adanya bermacam kebutuhan untuk meminta pendapat, sistem *e-voting* perlu dirancang untuk dapat menerima bermacam format kartu suara (misal: pilihan tunggal, pilihan jamak, pemberian nilai untuk tiap kandidat, penetapan urutan kandidat, penulisan jawaban terbuka dll.).
4. Mobilitas (*mobility*). Partisipasi pemilih diharapkan akan meningkat jika sistem *e-voting* memberikan keleluasaan kepada pemilih untuk dapat memasukkan suaranya di berbagai lokasi atau melalui beragam media yang tersedia dan dapat diakses dengan mudah oleh pemilih.

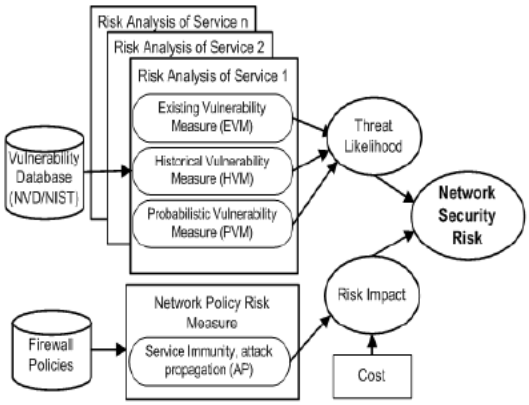
Properti-properti ini adalah salah satu faktor yang memberikan kontribusi besar dalam memperumit masalah keamanan pada sistem *e-voting*.

III. PENDEKATAN UNTUK MENGANALISA VULNERABILITAS TERHADAP KEAMANAN

Beberapa *framework* dapat digunakan untuk menganalisa vulnerabilitas terhadap keamanan:

A. Framework Pengukuran Risiko Jaringan

Dalam [15] Ahmed dkk mengajukan kerangka kerja metrik keamanan yang mengidentifikasi dan mengkuantifikasi faktor risiko keamanan yang paling signifikan secara obyektif seperti pada gambar 1 di bawah ini.

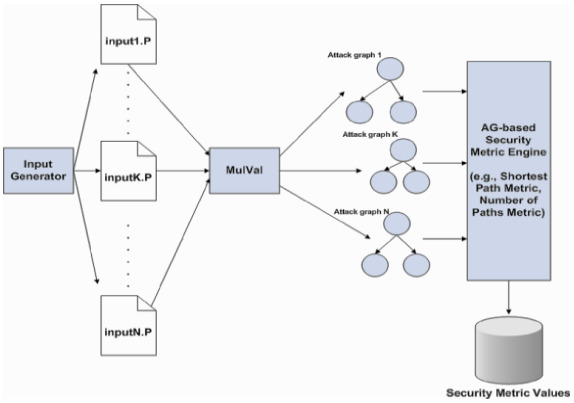


Gambar 1 : Framework Pengukuran Risiko Jaringan[15]

Faktor-faktor ini mencakup vulnerabilitas yang ada, kecenderungan historis vulnerabilitas dari layanan yang bisa diakses secara *remote*, prediksi vulnerabilitas potensial untuk layanan jaringan umum, hingga ketahanan kebijakan terhadap rambatan serangan pada jaringan. Selanjutnya dibahas percobaan validasi secara menyeluruh menggunakan data vulnerabilitas dari National Vulnerability Database (NVD) untuk menunjukkan akurasi yang baik dari metrik yang diajukan. Beberapa penelitian terdahulu meninjau vulnerabilitas menggunakan analisis kode.

Bagaimana pun, penelitian ini adalah yang pertama kali menggunakan informasi vulnerabilitas dan konfigurasi kebijakan keamanan publik.
Pada framework ini meneliti untuk satu jaringan. Penerapan network hardening belum optimal karena tidak mengukur kinerja jaringan.

B. Framework Percobaan Idika
Pada Gambar 2 dibawah ini dapat dilihat kerangka kerja percobaan (*experiment framework*) yang dilakukan pada penelitian disertasi Idika [16].



Gambar 2 : Framework Percobaan Idika [16]

Pembangkit masukan (*Input Generator*) menghasilkan file masukan untuk Mulval. Tiap masukan yang dihasilkan yaitu input1.P, input2.P, input3.P,...,inputK.P, input(K+1).P, input(K+2).P, ..., input(N-1).P, inputN.P masing-masing dimasukkan ke MulVal untuk dibuatkan graf serangan yang bersesuaian. Pembangkit masukan ini melakukan *generate* vulnerabilitas pada tiap *host* di jaringan. Setiap graf serangan diukur menggunakan metrik keamanan jaringan berbasis graf. Metrik keamanan berbasis graf ini dihitung oleh AG-based Security Metric Engine. Untuk setiap graf serangan, nilai metrik keamanan berbasis graf disimpan dalam *database*.
Pada framework Idika, asumsi yang digunakan menggunakan jenis vulnerabilitas *remote*, tidak melibatkan vulnerabilitas lokal. Jaringan yang diteliti dua buah jaringan. Belum menerapkan network hardening pada invidual host.

C. Framework Model Oriented Security Requirements Engineering(MOSRE)
Salini dkk [12] menjelaskan tentang Framework Model Oriented Security Requirements Engineering(MOSRE), dengan tahapan sebagai berikut:

1. Mengidentifikasi Tujuan dari Aplikasi Web
2. Identifikasi *Stakeholder*
3. Identifikasi Aset
4. Pilih Teknik elisitasi
5. Hasilkan level tinggi dari Diagram Arsitektur untuk Aplikasi Web
6. Buat Tujuan dan Kebutuhan Non-Keamanan
7. Generate Use Case Diagram untuk Aplikasi Web
8. Identifikasi Tujuan Keamanan / Sasaran Keamanan
9. Mengidentifikasi ancaman dan kerentanan
10. Lakukan Penilaian Risiko
11. Kategorikan dan Prioritaskan Ancaman dan Kerentanan untuk mitigasi
12. Menghasilkan Misuse Cases Diagram untuk Aplikasi Web
13. Mengidentifikasi Persyaratan Keamanan
14. Menghasilkan Use Case Diagram untuk Aplikasi Web dengan mempertimbangkan Kebutuhan Keamanan
15. Menghasilkan model Analisis Struktural
16. Kembangkan diagram Unified Modeling Language (UML)

Pada *framework* ini tidak dihasilkan suatu pengukuran keamanan terhadap *e-voting*, terutama untuk beberapa persyaratan keamanan *e-voting* serta belum menerapkan *network hardening*. Jaringan yang diteliti hanya satu jaringan.

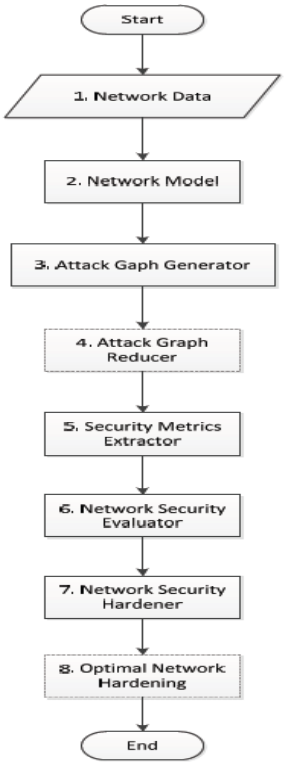
D. *Framework* Evaluasi dan Peningkatan Keamanan Jaringan
Dalam penelitian [9] telah dihasilkan suatu *framework* untuk mengevaluasi dan meningkatkan keamanan jaringan komputer yang lebih komprehensif. *Framework* ini tidak hanya menganalisis langkah-langkah

serangan oleh penyusup pada suatu jaringan komputer dan menghasilkan grafnya saja. Namun juga menganalisis berbagai konfigurasi *countermeasure* yang akan diterapkan dengan menghitung risiko dan biaya total dari penerapan konfigurasi *countermeasure*. Konfigurasi *countermeasure* ini dipilih berdasarkan kebutuhan pengguna.

Framework penelitian yang dihasilkan didasarkan pada *reasoning* sebagai berikut. *Threat* adalah sesuatu yang dapat terjadi atau hasil dari serangan terhadap satu atau lebih aset. Vulnerabilitas adalah karakteristik dari aset yang dituju yang membuat aset tersebut lebih rentan diserang oleh *threat* atau membuat suatu serangan lebih berpeluang untuk berhasil atau memiliki dampak. *Threat* mengeksploitasi vulnerabilitas yang menyebabkan terekspos nya suatu aset.

Countermeasure didesain untuk mencegah suatu *threat* terjadi atau mengurangi dampak dari suatu *threat* jika *threat* itu terjadi. Aset merupakan target dari suatu *threat* untuk diekspos. Aset merupakan penerima dari suatu *countermeasure*. Aset adalah sesuatu yang harus dilindungi.

Framework evaluasi dan peningkatan keamanan jaringan yang dapat dilihat pada Gambar 3.



Gambar 3 : Framework Evaluasi dan Peningkatan Keamanan Jaringan [9]

Data masukan pada bagian pertama *framework* berupa data topologi jaringan, data vulnerabilitas jaringan, data konektivitas *host*, data aset dan data *firewall rules*. Masing-masing data jaringan memiliki representasi yang diimplementasikan pada blok ke-2 framework.

Pada blok ke-2 framework yaitu model jaringan direpresentasikan dalam bentuk matriks konektivitas yang menggambarkan topologi jaringan. Vulnerabilitas dinyatakan dalam bentuk himpunan vulnerabilitas yang ada di setiap *host*.

Pada blok ke-3 *framework* yaitu *attack graph generator* dihasilkan suatu graf status keamanan, graf *host* dan graf vulnerabilitas. Pada bagian 3 ini diajukan satu perbaikan algoritma untuk menghasilkan status keamanan jaringan.

Attack graph reducer pada bagian ke-4 *framework* ditujukan untuk mereduksi ukuran graf yang dihasilkan. *Attack graph reducer* ini belum diimplementasikan dalam penelitian ini.

Pada bagian ke-5 *framework* yaitu *Security Metrics Extractor* dihasilkan metrik keamanan jaringan dan nilainya. Metrik keamanan jaringan yang dihasilkan ada 2 jenis yaitu metrik keamanan berbasis graf dan metrik keamanan tidak berbasis graf.

Bagian ke-6 *framework* yaitu *Network Security Evaluator* berfungsi untuk mengevaluasi keamanan jaringan yang sedang ditinjau. Evaluasi terhadap keamanan jaringan ini menggunakan metrik yang dihasilkan pada bagian 5 *framework* yaitu *security metrics extractor*.

Bagian ke-7 *framework* yaitu *network security hardener* diimplementasikan dengan cara menerapkan berbagai konfigurasi *countermeasure* terhadap vulnerabilitas yang ada pada jaringan. Setiap konfigurasi *countermeasure* yang diterapkan akan menimbulkan risiko dan biaya. Metode yang digunakan untuk menghitung risiko dan biaya dari penerapan konfigurasi *countermeasure* diadopsi dari [17].

Pada bagian ke-8 *framework* yaitu *optimal network hardening* dimaksudkan untuk memilih konfigurasi *countermeasure* yang memiliki risiko dan biaya yang paling kecil. Bagian ini merupakan bagian pelengkap pada penelitian ini.

Pada *framework* ini pemilihan konfigurasi *countermeasure* yang optimal belum dilakukan dalam penelitian ini. Pemilihan konfigurasi *countermeasure* dalam penelitian ini berdasarkan kebutuhan pengguna. *Optimal network hardening* belum dilakukan dalam penelitian ini. Jaringan yang diteliti masih skala kecil. Sudah dihasilkan pengukuran untuk keamanan.

Tabel 1.
Penelitian Framework Analisa Vulnerabilitas terhadap Keamanan

No	Peneliti/Tahun Penelitian	Nama Framework	Skala Jaringan	Optimal *Network hardening*
1	Ahmed dkk 2008 [32]	Framework Pengukuran Risiko Jaringan	Satu Jaringan	Network risk measurment framework (tidak mengukur kinerja jaringan)
2	Idika, 2010 [*2*]	Framework Percobaan Idika	Dua jaringan	Program Dinamis(belum untuk individual *host*, tidak mengukur kinerja jaringan)
3	Salini dkk 2012 [*3*]	Framework Model Oriented *Security* Requirements Engineering (MOSRE)	Satu jaringan	-
4	Purboyo, 2015 [9]	Framework Evaluasi dan Peningkatan Keamanan Jaringan	Satu jaringan	User Based Network Hardening (sesuai kebutuhan pengguna)

IV. PENDEKATAN KEAMANAN JARINGAN MEMAKAI GRAF SERANGAN

Attacker dapat menyusup ke dalam jaringan *internal* melalui vulnerabilitas yang berada pada *host* di jaringan yang ditinjau. Urutan vulnerabilitas yang dieksploitasi oleh attacker dapat digunakan untuk membangun *attack graph* [9]. Beberapa penelitian yang berkaitan dengan graf serangan dapat dilihat pada uraian berikut ini.

Dalam [23] Zhao dkk menjelaskan semua vulnerabilitas diasumsikan dapat dieksploitasi secara remote dan lokal. Graf Serangan yang dihasilkan Graf Status yang meninjau kinerja jaringan. Metode perhitungan menggunakan manual. Pada penelitian ini menggunakan algoritma AG_Generation(H,R, s0) yang berdasarkan Virtual Performance Node (VPN). VPN adalah *node* yang menyatakan status keamanan jaringan berdasarkan pada aspek-aspek khusus yang ditinjau. Dengan

mempertimbangkan *loss of performance* untuk mengukur *attack effect*.

Dalam [16] Idika menjelaskan semua vulnerabilitas diasumsikan dapat dieksploitasi secara *remote* sehingga tidak bersifat umum. Jenis graf serangan yang dihasilkan tidak meninjau kinerja jaringan. Metode perhitungan menggunakan komputer. Pada penelitian ini menggunakan algoritma Depth-first Search, dimana algoritma ini mengevaluasi dua buah jaringan menggunakan graf serangan sintesis.

Dalam [17] Viduto menjelaskan menjelaskan semua vulnerabilitas diasumsikan dapat dieksploitasi secara *remote* dan lokal. Jenis graf serangan yang dihasilkan tidak meninjau kinerja jaringan. Metode perhitungan menggunakan komputer. Pada penelitian ini tidak menghasilkan algoritma.

Dalam [9] Purboyo menjelaskan jenis graf serangan yang dihasilkan yaitu Graf Status yang meninjau kinerja jaringan, Graf Host, Graf Vulnerabilitas. Asumsi vulnerabilitas yang dapat dieksploitasi dapat secara *remote* dan lokal. Untuk simulasi menggunakan metode komputasi komputer dan manual. Salah satu kontribusi pada penelitian ini adalah algoritma untuk mengimplementasikan *attack rule* yang menghasilkan semua status keamanan jaringan.

Tabel 2.

Perbandingan Penelitian Graf Serangan

No	Peneliti/Tahun Penelitian	Jenis Graf Serangan	Asumsi Vulnera-bilitas	Metode Komputasi	Algoritma
1	Zhao dkk, 2009 [23]	Graf Status meninjau kinerja jaringan. Tidak dihasilkan Graf *Host* dan Graf Vulnerabi-litas	Vulnerabilitas *Remote* dan Vulnerabilitas Lokal	Metode Perhi-tungan manual	AG_Generation(H,R, s0) berbasis VPN
2	Idika, 2010 [16]	Tidak meninjau Kinerja Jaringan	Vulnerabilitas *Remote* dan Vulnerabilitas Lokal	Metode Perhitungan menggunakan komputer	Depth-first search
3	Viduto, 2012 [17]	Tidak meninjau Kinerja Jaringan	Vulnerabilitas *Remote* dan Vulnerabilitas Lokal	Metode Perhitungan menggunakan komputer	-
4	Purboyo, 2015 [9]	Graf Status meninjau kinerja jaringan, Graf *Host*, Graf Vulnerabilitas	Vulnerabilitas *Remote* dan Vulnerabilitas Lokal	Metode Komputasi Komputer dan Manual	Algoritma Graf Status Keamanan

V. KESIMPULAN

Berdasarkan dari uraian sebelumnya, maka dapat dilihat beberapa peluang untuk melakukan penelitian selanjutnya:

1. Dari beberapa *framework* untuk menganalisa vulnerabilitas, belum ada yang secara khusus membahas berdasarkan persyaratan keamanan *e-Voting* dan pengoptimalan *network hardening*. Berdasarkan hal tersebut dapat menjadi peluang penelitian untuk menghasilkan *framework* yang dapat mengevaluasi keamanan pada sistem *e-voting* berdasarkan persyaratan

keamanan *e-voting* dengan *network hardening* yang optimal secara dinamis.

2. Dari beberapa algoritma yang dihasilkan untuk mengkonstruksi graf serangan, belum terlihat yang dapat mengevaluasi kinerja jaringan dengan eksploitasi vulnerabilias *remote* dan lokal serta metode komputasi komputer. Untuk hal tersebut dapat menjadi peluang penelitian untuk membuat suatu algoritma yang menghasilkan Graf Status keamanan jaringan serta Graf *Host* dan Graf Vulnerabilitas pada *e-voting* dengan metode komputasi komputer serta asumsi vulnerabilitas yang dieksploitasi dapat secara *remote* dan lokal.

DAFTAR PUSTAKA

[1] M Bellis. (2015, Desember) The History of Voting Machines - History of the Voting. [Online]. http://inventors.about.com/library/weekly/aa111300b.htm

[2] VoteHere Inc, *Network Voting Systems Standards*.: Public Draft 2, April 2002.

[3] O Centinkaya and D Cetinkaya, "Verification and Validation Issues in Electronic Voting," *The Electronic Journal of e-Government*, vol. 5 (2), pp. 117 - 126, 2007.

[4] A Riera and P Brown , "Bringing Confidence to Electronic Voting," *Electronic Journal of e-Government*, vol. 1 (1), pp. 14-21, 2003.

[5] B de Vuyst and A Fairchild, "Experimenting with Electronic Voting Registration: the Case of Belgium," *The Electronic Journal of e-Government*, vol. 2 (2), pp. 87-90, 2005.

[6] D Gritzalis, *Secure Electronic Voting; New Trends New Threats*.. Athens: Dept. of Informatics Athens University of Economics & Business and Data Protection Commission of Greece., 2002.

[7] L Hayden, *IT Security Metrics*. New York: The McGraw-Hill Companies, 2010.

[8] S.M. Furnell, S. Katsikas, J. Lopez, and A. Patel, *Securing Information and Communications Systems: Principles, Technologies, and Applications*.: Artech House, Inc., 2008.

[9] T.W. Purboyo, *Pengembangan Metrik Keamanan Berbasis Graf*., 2016.

[10 A Fujioka, T Okamoto, and K Ohta, "A Practical Secret Voting Scheme," *Advances in Cryptology - AUSCRYPT '92*, 1992.

[11 L. F. Cranor and R. K. Cytron, "Sensus: A *Security*-Conscious Electronic," in *Proceedings of the Hawai`i International Conference on System Sciences*, 1997.

[12 P Salini and S Kanmani, "Application of Model Oriented *Security* Requirements Engineering Framework for secure E-Voting," in *2012 CSI Sixth International Conference on Software Engineering (CONSEG)*, 2012, pp. 1–6.

[13 Z. Y. Wu, J.-C. Wu, S.-C. Lin, and C Wang, "An electronic voting mechanism for fighting bribery and coercion," *J. Netw. Comput. Appl*, vol. 40, pp. 139–150, April 2014.

[14 S. A. Adeshina and A. Ojo, "Design imperatives for e-voting as a sociotechnical system," *2014 11th International Conference on Electronics, Computer and Computation (ICECCO)*, pp. 1–4, 2014.

[15 Ahmed, M. S., Al-Shaer, E., Khan, E., "A novel quantitative approach for measuring network *security*.," in *Proceedings of IEEE INFO COM 2008.*, 2008.

[16 Nwokedi C. Idika, "Characterizing and Aggregating Attack Graph-Based *Security* Metrics," Purdue University, West Lafayette, Indiana, PhD Dissertation 2010.

[17 Valentina Viduto , "A Risk Assessment and Optimisation Model for Minimising Network *Security* Risk and Cost," Bedfordshire: University of Bedfordshire, 2012.

[18 Kenneth H. Rosen, *Discrete Mathematics and Its Applications*, Seventh Edition ed.: The McGraw-Hill Companies,

Inc, 2012.

[19 Ravindra K. Ahuja, Thomas L. Magnanti, and James B. Orlin, *Network Flows Theory, Algorithms, and Applications*. New Jersey: PRENTICE HALL, 1993.

[20 I. N. Bronshtein, K. A. Semendyayev, G. Musiol, and H. Muehlig, *Handbook of Mathematics*, 5th ed. Verlag Berlin Heidelberg: Springer, 2007.

[21 Oleg Sheyner, Joshua Haines, Somesh Jha, Richard Lippmann, and Jeannette M. Wing, "Automated Generation and Analysis of Attack Graphs," in *IEEE Symposium on Security and Privacy*, 2002.

[22 P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph-based network vulnerability analysis," in *9th ACM conference on Computer and communications security*, 2002, pp. 217–224.

[23 Yiuan Zhao, Zulin Wang, Xudong Zhang, and Jing Zheng, "An Improved Algorithm for Generation of Attack Graph Based on Virtual Performance Node," in *International Conference on Multimedia Information Networking and Security*, Beijing: Beijing University of Aeronautics and Astronautics, 2009.