APLIKASI POHON DALAM PENCARIAN CELAH KEAMANAN SUATU JARINGAN

Aldo Suwandi

NIM : 13509025

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung,
Jl. Ganesha 10 Bandung 40132, Indonesia

Email : 13509025@std.stei.itb.ac.id

***Abstrak*—Makalah ini membahas tentang aplikasi pohon dalam pencarian celah keamanan suatu jaringan. Celah keamanan adalah suatu kesalahan dalam suatu jaringan yang dapat memungkinkan penurunan peforma dalam suatu suatu jaringan. Pencarian celah ini sebenarnya dapat dilakukan dengan berbagai banyak cara, namun tidak semua cara memiliki hasil yang efektif. Ada 7 cara yang dapat dilakukan untuk pencarian celah ini, namun kita tidak tahu harus memulai dengan cara yang mana terlebih dahulu. Penggunaan graf dapat dilakukan untuk membantu meringankan pemilihan metode pencarian celah keamanan suatu sistem yang efektif dan cepat**.

***Kata kunci*—jaringan, sistem, pohon, keamanan.**

I. PENDAHULUAN

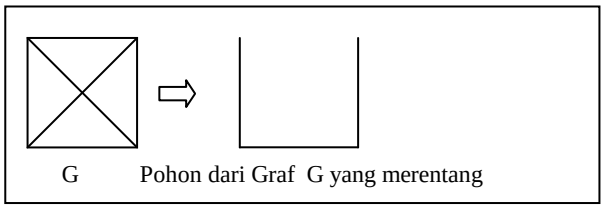
I.I Pengertian Pohon

Pohon dapat didefinisikan sebagai Graf yang tidak memiliki sebuah sirkuit. Graf adalah suatu pasangan himpunan yang membentuk simpul dan salah satu himpunan dari pasangan himpunan tersebut tidak boleh kosong, sehingga dimungkinkan suatu graf tidak memiliki sisi satu buahpun, tetapi simpulnya harus ada.

Graf memiliki berbagai macam jenis. Graf terdiri dari dari graf sederhanan, graf tak sederhana, graf berarah, dan graf tak berarah. Graf sederhana adalah graf yang tidak mengandung gelang maupun sisi ganda. Graf tak sederhana adalah graf yang mengandung sisi ganda atau gelang. Graf berarah adalah graf yang memiliki orientasi arah. Lalu graf tak berarah adalah graf yang tidak memiliki orientasi arah.

Melihat definisi dari graf sebelumnya, dapat diartikan bahwa pohon adalah suatu bagian dari graf yang tidak memiliki arah dan tidak mengandung sebuah sirkuit di dalamnya. Pohon memiliki sifat bahwa setiap pasang simpul dalam suatu pohon terhubung dengan lintasan tunggal, pohon terhubung dan memiliki m = n -1 buah sisi, pohon tidak mengandung sirkuit dan penambahan satu sisi pada graf akan membuat hanya satu sirkuit, pohon terhubung dan semua sisinya adalah jembatan (jembatan adalah sisi yang bila dihapus menyebabkan graf terpecah menjadi dua komponen).

Bila G adalah sebuah graf yang membentuk sebuah sirkuit maka bila sisi G dihapus, G akan membentuk sebuah pohon yang merentang.



Gambar 1 Contoh Pohon yang merentang

Jika G adalah graf yang berbobot maka bobot pohon merentang dari G didefinisikan sebagai jumlah bobot semua sisi di pohon. Dalam pembentukan pohon merentang dapat dicari bentuk perentangan yang paling minimum bobotnya. Algoritma yang digunakan adalah algortima Prim dan algortima Kruskal.

Algoritma Prim bekerja dengan cara membentuk pohon merentang minimum dengan langkah per langkah. Pada setiap langkah kita mengambil sisi yang minimum bobotnya dan bersisian dengan simpul-simpul di dalam pohon tersebut tanpa membentuk suatu sirkuit.

Algortima Kruskal bekerja dengan cara pengurutan terlebih dahulu sisi dari graf dengan pengurutan dengan bobot terurut membesar. Sisi yang dimasukan ke dalam pohon adalah sisi yang dapat membentuk pohon dengan bobot terkecil tanpa membentuk suatu sirkuit.

Aplikasi yang dapat digunakan dengan pohon ada bermacam-macan seperti pohon m-ary ,pohon biner, pohon ekspresi, pohon keputusan, kode awalan, kode huffman, dan pohon pencarian. Pada makalah ini akan menggunakan pohon pencarian, maka akan dijelaskan tentang pohon pencarian saja.

Pohon pencarian biner adalah pohon biner yang paling penting. Simpul pada pohon pencarian dapat berupa kunci pada data. Kunci adalah nilai yang membedakan setiap simpul dengan simpul yang lainnya. Kunci haruslah unik. Pohon pencarian biner adalah pohon biner yang setiap kuncinya diatur dalam suatu urutan tertentu.

I.II Metode Pencarian Celah Keamanan

Metode yang digunakan untuk pencarian celah keamanan menurut sertifikasi CEH harus dilakukan dengan tahapan, yaitu dengan mencari sistem yang aktif, mencari port yang terbuka, mengidentifikasi service, OS fingerprinting, vulneralbility scanning, menggambarkan diagram network dari host yang bermasalah, dan menyiapkan proxy.

Mencari sistem yang aktif adalah cara termudah untuk mencari komputer, banyak cara yang dapat dilakukan diantaranya yang termudah adalah dengan perintah ping, namun belakangan ini perintah ping sudah banyak ditolak oleh beberapa host besar, diantaranya seperti microsoft. Hal ini disebabkan karena adanya celah dalam proses pengiriman paket dari program ping ini.

Mencari port yang terbuka adalah cara dimana melakukan pencarian ibarat sebuah pintu masuk untuk masuk ke dalam suatu komputer. Dalam komputer ada 65,535 port, tidak mungkin kita mengaksesnya 1 per satu, maka diperlukan software yang efektif dalam proses pencarian ini.

Mengidentifikasi service adalah untuk mengetahui servis apa yang berjalan pada komputer. Cara ini memiliki hubungan yang sangat erat dengan cara mencari port yang terbuka. Dengan mengetahui port mana yang terbuka, kita dapat menembak service apa saja yang ada pada komputer.

OS fingerprinting adalah proses dimana pencari tahuan OS yang digunakan oleh komputer. Bila seseorang mengetahui OS yang digunakan oleh suatu komputer, maka orang tersebut akan dengan mudah mengetahui apa saja kelemahan yang ada pada OS yang digunakan.

Vulneralbility scanning adalah cara yang paling unik, cara ini mungkin digunakan bila ada data mengenai kelamahan-kelemahan suatu sistem, sehingga orang sudah tahu tentang kelemahan sistem tersebut dan langsung memanfaatkan tanpa perlu kerja yang keras.

Menggambarkan diagram network dari host yang bermasalah adalah cara dimana melakukan pemetaan terhadap host yang sudah diketahui permasalahannya, maka dengan memetakan secara visual, seseorang dapat lebih mudah memahami bagian mana yang terdapat celah keamanannya.

Menyiapkan proxy adalah langkah yang sebenarnya wajib dari setiap cara di atas. Setiap cara di atas haruslah diakhiri dengan mempersiapkan proxy server. Proxy ini bertujuan untuk menyembukin identitas seseorang contohnya untuk identitas yang paling penting adalah IP address.

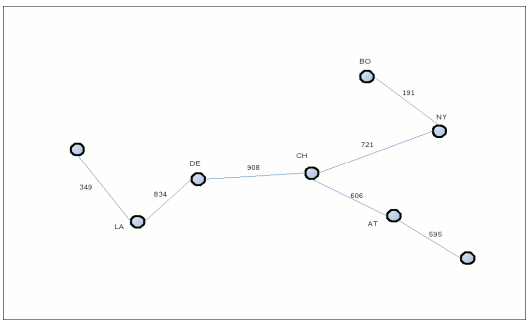
II. PENCARIAN CELAH KEAMANAN

Masalah keamanan dalam suatu jaringan sangatlah menjadi masalah yang sangat penting pada era teknologi masa kini. Penyimpanan data menggunakan teknologi digital juga bukan hal yang asing lagi pada zaman sekarang ini. Apa jadinya bila sistem yang kita gunakan untuk menyimpan, mengolah, dan memproses data dapat dimanipulasi dan dicuri oleh orang dari luar.

Makalah ini dibuat untuk mengkaji bagaimana proses penulusuran celah keamanan dan cara mana yang tersingkat untuk menuju celah tersebut. Bila dalam suatu sistem yang kecil, maka tentu kita dapat melakukan brute force, yaitu dengan mencoba satu-satu cara yang ada. Tapi bagaimana jadinya bila sistem yang ingin kita uji coba terdiri dari ribuan komputer?

Melalui pohon dalam struktur diskrit ini, penulis akan mencoba mengaplikasikan pohon dengan proses pencarian celah keamanan ini.

Seperti dijelaskan pada bab sebelumnya, terdapat 7 tahapan untuk mencari celah keamanan, baik dalam suatu sistem ataupun suatu komputer. Dalam tiap masing-masing tahapan tersebut tentu memiliki bobot yang berbeda-beda. Bobot disini dapat diibaratkan sebagai bobot pada sisi pohon yang merentang.



Gambar 2 Contoh Pohon yang memiliki bobot

Dapat dilihat pada gambar bahwa pada setiap cabang pohon terdapat angka-angka yang menunjukan beban. Teradapat 2 algoritma yang dapat memilih pohon merentang mana yang bobotnya terkecil, sehingga dapat mempermudah dan mempercepat proses pencarian nanti.

```
Procedure Prim(input G : graf, output
    T : pohon)
{Membentuk pohon merentang minimum T
dari graf G. Masukan : graf berbobot
terhubung G = (V,E), yang mana |V| =
n. Keluaran : pohon rentang minimum T
= (V,E') }


KAMUS
    e : sisi

ALGORITMA
    T ← sisi e yang mempunyai
        bobot minimum
```

```
E ← E – e
for i ← 1 to n – 2 do
      e ← sisi yang punya bobot
           terkecil
      T ← T U e
      E ← E – e
endfor
```

Gambar 3 Algoritma Prim

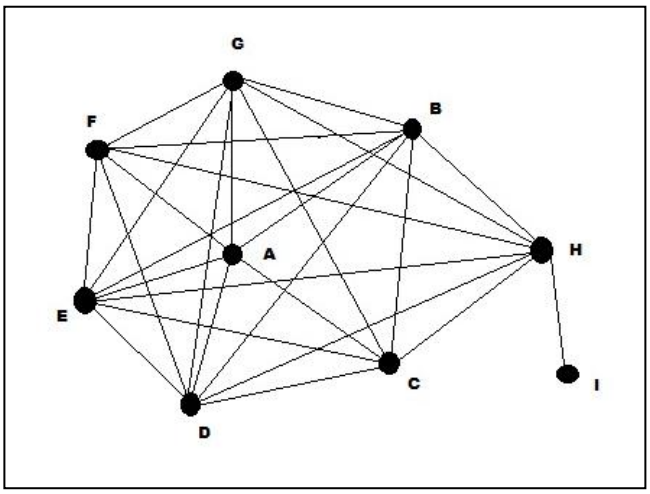
```
Procedure Kruskal(input G : graf,
    output T : pohon)
{Membentuk pohon merentang minimum T
dari graf G. Masukan : graf berbobot
terhubung G = (V,E), yang mana |V| =
n. Keluaran : pohon rentang minimum T
= (V,E') }

KAMUS
    i,p,q,u,v : integer

ALGORITMA
    T ← []
    while jumlah sisi T < n -1 do
          e ← sisi di dalam E yang
               bobot terkecil
          E ← E – e
          Iif e tidak membentuk
              sikulus di T then
              T ← T U e
          endif
    endwhile
```

Gambar 4 Algoritma Kruskal

Setelah mengetahui kedua algoritma di atas, maka kita dapat langsung mengaplikasikannya dengan pencarian celah keamanan di dalam suatu sistem. Dapat dimisalkan graf pencarian celah keamanan seperti gambar di bawah ini :



Gambar 5 Graf Sirkuler Pencarian Celah Keamanan

Dapat dilihat pada simpul A,B,C,D,E,F, dan G semuanya saling berhubungan. Lalu dari semua simpul tersebut akan menuju simpul H dan berujung pada simpul I.

Setiap simpul dari B,C,D,E,F, dan G dapat diwakilkan dengan 6 cara yang akan dilakukan dalam proses searching. A adalah sebagai akar utamanya dan H adalah proses penyiapan proxy di mana semua cara akan melalui cara tersebut. I pada graf adalah sebagai tujuan akhir, yaitu dimana I adalah kondisi saat celah keamanan sudah ditemukan.

Telah dijelaskan bahwa setiap cara memiliki bobot yang berbeda-beda, hal ini ditentukan dengan bagaimana cara yang dilakukan untuk menempuh ke dalam cara tersebut. Ada sistem jaringan yang hanya cukup dengan 1 cara saja sudah dapat dicari bagian celah keamanannya, tapi ada juga yang harus melalui seluruh cara untuk sampai ke bagian I (penemuan celah keamanan).

III. Aplikasi Pohon

Untuk mendapatkan hasil yang tercepat dan tersingkat dalam metode pencarian celah keamanan, dapat digunakan pohon.

Awalnya terbentuk sebuah graf yang menggambarkan 7 cara untuk cara pencarian celah keamanan. Lalu akan dibentuk pohon yang merentang berdasarkan graf sirkuler tersebut. Namun sebelum kita membentuk pohon yang merentang, kita harus menentukan bobot-bobot yang ada pada cabang setiap graf tersebut.

Dalam pendapatan nilai bobot pada cabang akan ditentukan sesuai dengan tingkat kesulitan tiap cara.

Cara pertama (B) yaitu hanya dengan mencari sistem yang aktif. Biasanya hanya dengan menggunakan program ping, bobot untuk cara ini mungkin adalah bobot paling ringan, namun kemungkinan untuk suskesnya sangat kecil.

Cara kedua (C) yaitu mencari port yang terbuka, cara ini cukup rumit, di mana pengguna harus menggunakan berbagai macam kombinasi TCP scan untuk benar-benar dapat menemukan port yang terbuka.

Cara ketiga (D) yaitu dengan mengidentifikasi services, cara mempunyai hubungan yang cukup erat dengan cara kedua, namun tak menghapus kemungkinan bahwa cara ketiga ini akan dijalankan tanpa melalui cara kedua.

Cara keempat(E) yaitu OS Fingerprinting. Cara ini dapat dibilang tergolong mudah, karena pada cara ini, kita hanya menemukan apa tipe sistem operasi yang digunakan pada komputer jaringan, sangat kecil kemungkinan dengan bermodalkan cara ini untuk mendapatkan celah keamanan, kecuali bila celah keamananya sudah diumumkan ke umum, dan admin dari jaringan tersebut belum memperbaharui sistemnya dengan patch terbaru.

Cara kelima (F) yaitu dengan vulneralbility scanning. Cara ini mungkin tergolong mudah, bila vulneralbility (celah keamanan) didapat dengan menggunakan bantuan software khusus yang menyediakan jasa untuk mencari celah-celah keamanan pada sistem. Namun, bila software

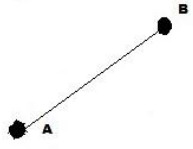
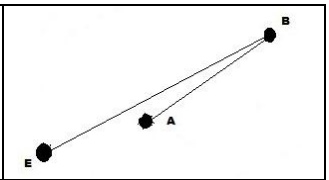
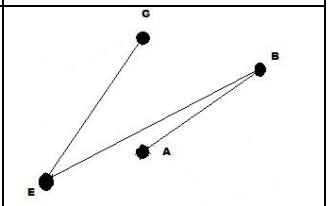
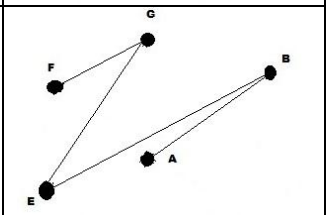
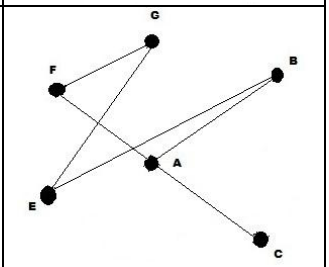
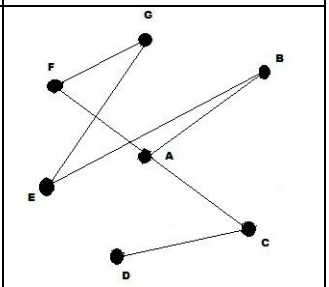
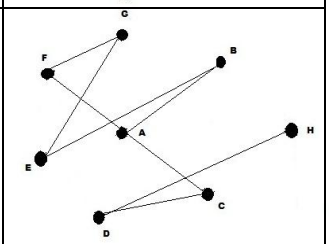
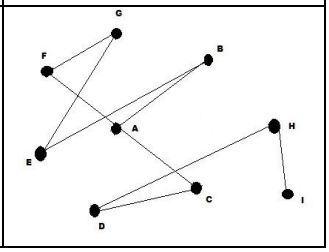
tersebut tidak dapat bekerja dengan baik, maka akan sangat sulit bila menelusuri satu-satu bagian mana yang ada kesalahan mungkin dari source code, atau dari algoritma sistem yang ada.

Cara keenam (G) yaitu dengan menggambar diagram network. Cara ini adalah cara yang tergolong dengan bobot yang kecil, karena pada tahap ini kita diasumsikan sudah mengetahui diagram jaringan dengan baik, maka kita dapat memvisualisasikannya dengan baik, dan dapat kita telaah lebih lanjut.

Berikut adalah tabel dari bobot graf sistem jaringan pada gambar 5.

Titik Awal	Titik Akhir	Bobot
A	B	4
A	C	10
A	D	5
A	E	6
A	F	12
A	G	5
B	C	11
B	D	8
B	E	6
B	F	9
B	G	16
B	H	20
C	D	8
C	E	36
C	F	9
C	G	10
C	H	58
D	E	14
D	F	1.3
D	G	21
D	H	8
E	F	9
E	G	3
E	H	8
F	G	7
F	H	19
G	H	2
H	I	2

Dengan melihat tabel di atas, maka dapat dibuat sebuah pohon yang merentang dengan algoritma Prim, yaitu dengan tabel sbb :

Langkah	Sisi	Bobot	Pohon
1	A,B	4	
2	B,E	6	
3	E,G	3	
4	G,F	7	
5	F,C	9	
6	C,D	8	
7	D,H	8	
8	H,I	2	

Gambar 6 Tabel Pohon Merentang Minimum dari Graf Sistem Jaringan dengan Algoritma Prim

Dapat dilihat pada gambar, hasil yang diperoleh dengan menggunakan algoritma Prim, pohon merentang minimum yang berasal dari graf suatu pencarian sistem keamanan.

Melalui pohon yang dibuat di atas, kita dapat mengetahui tahapan langkah-langkah mana saja yang harus di ambil dalam pencarian celah keamanan pada sistem jaringan tersebut.

Masalah yang dialami pada saat ini adalah, kebanyakan orang tidak tahu harus memulai dari mana, dan kebanyakan orang harus secara brute force mencob satu-satu cara tersebut, semoga dengan dibuatnya pohon merentang ini, dapat menjawab masalah yang ada.

Tabel di atas hanya merupakan salah satu contoh penyelesaian masalah. Penulis tidak dapat memastikan dengan benar bobot yang sesuai untuk masing-masing tahap. Hal ini dikarenakan, untuk mendapatkan bobot yang benar-benar pas, penulis harus benar-benar mencoba cara tersebut satu per satu untuk memastikan kebenaran dari bobot tersebut.

V. Kesimpulan

Dalam dunia sekarang ini, semakin maju sebuah teknologi, maka semakin banyak juga masalah baru yang ditemukan. Untuk mengatasi hal itu, kita perlu berpikir kreatif dan inovatif dalam menyelesaikan masalah-masalah yang bermunculan.

Penyelesaian masalah, tidaklah perlu dengan menggunakan hal-hal yang kompleks, tetapi cukup dengan memanfaatkan apa yang sudah ada, dan masalah dapat dengan mudah teratasi.

Menyangkut hal di atas, penulis berusaha untuk mengaplikasikan materi kuliah sutruktur diskrit terutama dalam bagian graf dan pohon.

Dengan memanfaatkan graf dan pohon, masalah dalam pencarian celah keamanan dalam suatu sistem dapat teratasi, karena graf dan pohon membentuk suatu bagian yang dapat mempermudah alur dan tahap pencarian dalam hal mepersingkat waktu dan mengefektifkan kinerja.

Maka, bila kita hendak membuat suatu software pencari celah keamanan, ataupun kita ingin secara manual untuk mecari celah keamanan dari suatu sistem, kita dapat menerapkan graf dan pohon untuk mempermudah kerja kita.

DAFTAR PUSTAKA

[1] Munir, Rinaldi, Matematika Diskrit. Ed.3, Bandung : Informatika Bandung, 2007

[2] S'To, C.E.H (Certified Ethical Hacker) Ed.1, Jakarta : Jasakom, 2009

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 15 Desember 2010

ttd

Aldo Suwandi
13509025