MONITORING KOMPETISI PERTAHANAN SIBER

Albert Sagala
Teknik Komputer, Fakultas Teknik Informatika dan Elektro, Institut Teknologi Del
Jl.Sisimangaraja Desa Sitoluama Kec.Laguboti, Toba Samosir, 22381
Telp : (0632) 331234, Fax : (0632) 331116
E-mail : albert@del.ac.id

Abstrak

Saat ini, kompetisi keamanan jaringan di Indonesia sudah marak diselenggarakan oleh berbagai lembaga swasta atau tingkat universitas. Namun, penyelenggaraan model kompetisi yang ada saat ini sering terkendala dalam penentuan pemenang diakhir lomba. Perhitungan secara manual menjadi salah satu kendala utama. Juga, belum ada suatu model yang dapat menjadi acuan bagi seluruh pihak yang terlibat dalam pelaksanaan kompetisi. Pada penelitian ini dirumuskan sebuah model kompetisi dibidang keamanan jaringan yang mengutamakan keadilan (fairness) dalam penentuan pemenang kompetisi. Model kompetisi yang dirumuskan adalah Death Match Tournament, peserta diwajibkan memiliki kemampuan dasar, yaitu konfigurasi server yang aman.

Kata Kunci: *kompetisi keamanan, monitoring aplikasi, aplikasi penilaian, kompetisi death match*

Abstract

Currently, the network security competition is rife in Indonesia organized by private institutions or university level. However, the implementation of the current model of competition is often constrained in determining the winner at the end of the race. Manual calculation to be one of the main obstacles. Also, there is no one model that can be a reference for all parties involved in the implementation of the competition. In this study formulated a model of competition in the field of network security that promotes justice (fairness) in determining the winner of the competition. Competition model is formulated Death Match Tournament, participants are required to have basic skills, namely the configuration of a secure server.

Key words: *security competition, application monitoring, application scoring,death match tournament*

1. PENDAHULUAN

Pengamanan jaringan [1] merupakan hal yang sangat penting dilakukan untuk mencegah penyalahgunaan sumber daya jaringan. Keamanan jaringan memiliki beberapa aspek keamanan yang didefenisikan sebagai *confidentiality, integrity, authentication. Confidentiality* adalah usaha untuk menjaga informasi dari orang yang tidak berhak atau tidak memiliki izin. *Integrity* mensyaratkan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. *Authentication* adalah aspek yang berhubungan dengan metoda untuk menyatakan bahwa informasi diakses oleh orang yang benar.

1.1. Rumusan Masalah

Kebutuhan tenaga *hacker* yang professional di Indonesia sangat tinggi, namun tidak dibarengi dengan kurikulum IT yang mengarah ke bidang security. Saat ini masih sangat jarang sekali Program Studi yang membuka kurikulum ke arah konsentrasi keamanan jaringan. Bahkan kalau ditinjau kurikulum IT masih dominan ke administrasi jaringan dengan konten yang masih minim yang terkait keamanan jaringan. Namun, walaupun demikian, pada level kompetisi, saat ini telah banyak diselenggarakan kompetisi siber oleh organisasi, universitas, ataupun instansi [2][3]. Adanya kompetisi tentu mampu menumbuhkan minat dari para partisipan untuk mendalami keamanan jaringan. Semakin maraknya kompetisi ini, khususnya di Indonesia, sehingga perlu diulas model kompetisi yang baik dan benar, terkait pengawasan pada saat berjalannya kompetisi. Sehingga pemenang pada kompetisi dapat diperoleh secara adil dan transparan.

1.2. Tujuan Penelitian

Terdapat tiga hasil akhir yang dihasilkan pada penelitian ini (1) Mengembangkan sebuah model jenis kompetisi keamanan jaringan serta topologi jaringannya di tingkat universitas dengan biaya yang murah, (2) Membuat sebuah aplikasi untuk penilaian otomatis, pengumpulan laporan, dan pemonitoran untuk kompetisi keamanan jaringan dan (3) Menyusun aturan dan panduan bagi peserta kompetisi.

1.3. Related Work

Collegiate Cyber Defense Competition mengembangkan sebuah aplikasi untuk pemonitoran kompetisi jaringan dengan membagi aktor kompetisi menjadi *Blue Team*, *Red Team*, *White Team*, *Gold Team*, *Chief Judge*, dan *Green Team*. Kompetisi yang dilaksanakan mempergunakan infrastruktur Internet. Setiap peserta akan diberikan IP Public dan IP Private. [3]

National Cyber Defense Competition mengembangkan sebuah model kompetisi dengan melakukan scanning terhadap suatu service setiap 5- 10 menit. Service yang dikompetisikan adalah *Web Server (HTTP +content)*, *Shell Server (SSH)*, *Remote Desktop Server (RDP)*, *Mail Server (SMTP+IMAP+HTTPS)* dan *Domain Controller (Kerberos+LDAP)* [4][7].

Model kompetisi yang dikembangkan pada penelitian ini adalah penyederhanaan dari model kompetisi yang dikembangkan oleh *Collegiate Cyber Defense* dengan pengecekan service pada **HTTP**, **HTTPS**, **SSH**, **FTP** dan **DNS**. Pengecekan *service* dilakukan setiap detik, sehingga nilai service dapat dilihat pada dashboard secara *realtime*.

2. MODEL KOMPETISI KEAMANAN JARINGAN

Kompetisi keamananan jaringan [5][6] adalah sebuah kompetisi yang bertujuan untuk menguji kemampuan pengguna komputer dalam hal administrasi jaringan, keamanan sistem informasi, celah keamanan *software* pada sistem, dalam waktu yang terbatas untuk membiasakan diri dengan kehidupan sehari-hari mengenai keamanan jaringan dan sistem keamanan *server*. Ada beberapa jenis model kompetisi keamanan yang sering dilombakan, misalnya *Death Match Tournament, Death Match Tournament, Digital Forensic Investigation, Face to Face Competition, Cyber Security Challenge, Cyber Quests / Security Quiz, Cyber Grand Challenge,* Pwn2Own, dan *Embedded System Security Discover Vulnerabilities*[4].

Pada penelitian ini, akan diulas suatu model kompetisi yang disebut dengan Deatch Match Tournament. Model ini dipilih karena akan menguji kemampuan dari peserta, mulai dari konfigurasi server dengan benar, sampai mencoba melakukan serangan ke server yang dikelola oleh peserta lain.

2.1. Model Kompetisi *Death Match Tournament*

Pada penelitian ini dipilih model kompetisi *Death Match Tournament*, karena dalam model kompetisi ini peserta dituntut untuk memiliki 3 (tiga) kemampuan yang berbeda, yaitu menyerang (*hacking*), bertahan (*defense)*, dan *hardening server* (*patching*). Dalam pengembangan model kompetisi *Death Match Tournament*, ada beberapa komponen yang dimiliki oleh sistem, yaitu:

a. Aktor yang ikut dalam kompetisi keamanan jaringan terbagi menjadi 3 (tiga) jenis, yaitu peserta yang berkompetisi (*Blue Team*), Tim yang menjadi juri kompetisi (*White Team*), dan Tim yang menjadi Tim penguji atau penyerang peserta lain (*Red Team*).
b. Menggunakan sebuah aplikasi *dashboard* yang ditampilkan pada sebuah layar monitor yang berada di depan seluruh peserta kompetisi pada saat kompetisi berlangsung. *Dashboard* tersebut menampilkan informasi perolehan nilai, status *service server* yang dimiliki oleh peserta.
c. Aturan dan panduan yang dibuat untuk menghindari beberapa kecurangan, menghindari ketidakadilan untuk seluruh peserta, dan sebagai panduan bagi peserta kompetisi atau Tim juri untuk menilai secara manual laporan dari peserta kompetisi dan Tim penyerang.
d. Topologi jaringan kompetisi yang dirancang, terbagi atas 3 *subnet,* yaitu *subnet* yang pertama adalah untuk peserta Blue Team. *Subnet* kedua adalah untuk Red Team dan White Team. Dan *subnet* yang terakhir adalah aplikasi *dashboard* untuk penilaian, pemonitoran, dan mengunggah laporan peserta kompetisi.
e. *Red Team* menggunakan *script* penyerangan ke peserta *Blue Team* yang telah disiapkan dan *Blue Team* harus siap untuk diserang oleh *Red Team*.
f. *Server Blue Team* yang disediakan untuk diserang oleh *Blue Team* lain dan *Red Team* memiliki celah keamanan yang harus dikonfigurasi (*hardening*) oleh *Blue Team* selama satu jam sejak kompetisi dimulai.

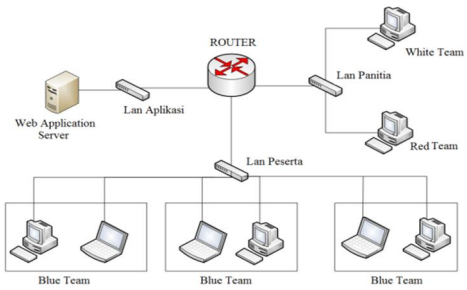
Pada kompetisi *Model Death Match Tournament*, alokasi waktu yang disediakan berdurasi 5 jam, dengan pembagian sesi adalah:

1. Sesi pertama, yaitu satu jam pertama, setiap peserta melakukan *hardening* terhadap *server* peserta tersebut. Selama proses *hardening*, *traffic* dibatasi oleh *white team/ red team* sehingga menghindari serangan antara peserta kompetisi.
2. Sesi kedua, yaitu empat jam berikutnya, seluruh peserta melakukan penyerangan hanya pada *server* peserta lainnya. Aturan kompetisi melarang peserta melakukan serangan terharap infrastruktur kompetisi, perangkat keras dan perangkat lunak.

3. TOPOLOGI JARINGAN KOMPETISI DEATH MATCH TOURNAMENT

Topologi jaringan dibagi menjadi 3 buah network, yaitu *network* panitia, *network server*, dan *network* peserta kompetisi (*Blue Team*). *Server* untuk aplikasi ditempatkan pada *subnet* yang berbeda dari *subnet* jaringan *Blue Team, Red Team,* dan *White Team* [3]. Sedangkan *Red Team* dan *White Team* ditempatkan satu *subnet* jaringan.

Pada Gambar 1 ditunjukkan aliran data pertama yang mengalir adalah dari komputer Blue Team yang akan mengirimkan status dari *server* Komputer Blue Team menuju ke *Server Web-Application* saat 4 (empat) jam berjalan setelah proses 1 (satu) jam *hardening* pada saat kompetisi berjalan. Aliran data yang kedua adalah dari komputer Red Team menuju ke komputer Blue Team saat proses penyerangan yang dilakukan menggunakan *script attacking* oleh Red Team ke *server* Blue Team.



Gambar 45Topologi Jaringan Kompetisi

3.1. Metode Penilaian Selama Kompetisi

Penilaian menjadi hal penting yang harus dirumuskan selama kompetisi, hal ini tentu berujung kepada suksesnya pelaksanaan kompetisi. Pada model kompetisi *Deatch Match Tournament*, penilaian terbagai menjadi dua bagian besar, yakni (1) **Penilaian Otomatis** dan (2) **Penilaian Manual**. Penilaian otomatis diberikan langsung oleh sistem komputer otomatis ketika peserta mampu mempertahankan semua layanan (*service*) bekerja secara optimal. Sedangkan, penilaian secara manual dilakukan langsung oleh *White Team* kepada aplikasi pelaporan selama kompetisi.

Metode penilaian yang dilakukan oleh aplikasi secara otomatis memeriksa status *service.* Sehingga diperoleh kondisi:

1. Saat status *service* Blue Team hidup maka Blue Team akan bertambah 1 poin setiap detik untuk setiap *service*
2. Saat status *service Blue Team* mati maka score Blue Team untuk service yang dimonitor tidak akan bertamabah. Scoring bertambah pada saat *Blue Team* berhasil menghidupkan kembali *service*.

Pada penilaian secara manual, prosedur penilaian dibagi menjadi beberapa level, tergantung dari jenis serangan atau pertahanan yang dilakukan oleh setiap peserta kompetisi. Blok penilaian seperti pada Tabel 1.

Tabel 30 Penilaian Manual

Jenis Penilaian	***Level***			
	Low	***Medium***	***High***	***Critical***
Skor Menyerang	Max (25)	Max (50)	Max (100)	Max (200)
Skor Bertahan	Max (25)	Max (50)	Max (100)	Max (200)
Skor Hardening	Max (25)	Max (50)	Max (100)	Max (200)
Skor Bonus	Penilaian diberikan berdasarkan kecepatan mengakses *Root* dari Peserta lain			

Pada Tabel 1, terdapat empat komponen utama untuk penilaian yaitu Skor Menyerang, Skor Bertahan, *Hardening* dan Bonus Skor. Bonu skor ditambahkan bagi peserta yang berhasil melakukan exploitasi terhadap peserta lain dalam waktu yang singkat, yang ditentukan oleh Panitia. Sedangkan *hardening score* adalah penilaian yang diberikan oleh *white team* terhadap perbaikan yang telah dilakukan oleh *blue team* pada *image server* yang dibagikan pada peserta kompetisi.

4. PESERTA PADA KOMPETISI MODEL DEATH MATCH TOURNAMENT

4.1. Aturan dan panduan Kompetisi *Death Match Tournament*

Aturan yang dibuat untuk para peserta *Blue Team* adalah peraturan yang dapat menjamin seluruh peserta adil dan berkurangnya kecurangan yang dapat merugikan peserta lain yang sedang berkompetisi. Salah satu yang harus dipikirkan saat pembuatan aturan untuk peserta adalah keadilan (*fairness*) yang ditekankan untuk menjamin kepuasan dari para peserta Blue Team yang ikut berkompetisi.

Panduan untuk peserta kompetisi dan juri dibuat agar semua metode penilaian yang dilakukan tim juri bersifat adil bagi peserta kompetisi dan sebagai panduan untuk menghindari kebingungan yang dialami oleh peserta kompetisi. Pada penelitian ini dirancang beberapa peraturan dan panduan kompetisi untuk tim penyerang dan peserta kompetisi, yaitu:

1. Aturan bagi peserta kompetisi, Blue Team
   a. Jumlah maksimal dari peserta Blue Team adalah lima belas (15) tim
   b. Tiap tim, beranggotakan 2 – 3 orang

c. Tiap tim hanya dapat membawa maksimal dua (2) buah laptop dengan spesifikasi yang akan disyaratkan oleh Panitia.
d. Tim yang melakukan aktivitas mengganggu jaringan kompetisi, seperti *DDOS*, *DOS*, *Brute-force*, *flooding*, dan aktivitas yang dapat mengganggu peserta kompetisi lain akan diberikan peringatan keras.
e. Tim yang mendapat peringatan keras tiga (3) kali akan di-diskualifikasi dari kompetisi.

2. Panduan bagi Juri, White Team
   a. Juri harus menilai laporan melalui suatu aplikasi yang disediakan dari tiap peserta kompetisi berdasarkan panduan metode penilaian untuk proses penyerangan, *hardening*, dan bertahan oleh peserta kompetisi.
   b. Juri harus memberi nilai seadil – adilnya kepada peserta kompetisi.
   c. Penilaian dilakukan langsung terhadap laporan yang telah dikirimkan oleh terlebih dahulu.

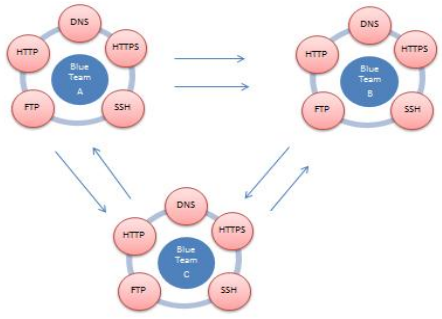
4.2. *Server* Blue Team Kompetisi *Death Match Tournament*

Server yang diberikan kepada peserta *Blue Team* telah terinstall 5 *service* yang sudah diberikan celah keamanan. Peserta harus dapat mendeteksi celah tersebut dan memperbaikinya pada periode waktu hardening.

Serangan yang digunakan berjumlah paling sedikit 15 (lima belas) teknik serangan dengan 3 (tiga) tingkatan level per *service* dengan menyerang 5 (lima) *service* pada setiap *server Blue Team*. Beberapa teknik serangan yang dihasilkan pada penelitian ini dapat di lihat pada tabel di bawah.

Tabel 31 *Vulnerable Server* [5]

TEKNIK	PENJELASAN	SOLUSI
Netcat	Serangan ini memaksa target untuk membuka port tertentu sehingga penyerang dapat masuk ke sistem target dan dapat mengeksekusi perintah sebagai super user/root melalui layanan MySQL, SSH, ataupun FTP	Admin harus memeriksa semua port yang melisten yang berjalan pada sistem dan memberhentikan yang mencurigakan
Handshake Public Key	Serangan yang dapat membuat penyerang dapat masuk ke sistem tanpa harus melakukan autentikasi terlebih dahulu melalui layanan SSH dan SFTP	Admin melakukan Generate Key secara berkala untuk memastikan key tidak dapat di copy oleh penyerang
Program Access Manipulation	Serangan yang memperbolehkan sebuah aplikasi untuk mengeksekusi seluruh perintah shell melalui layanan SSH	
Metasploit	Serangan eksploitasi dengan memanfaatkan celah keamanan pada target menggunakan *tools* dengan menggunakan library yang disediakan melalui layanan FTP, MySQL, HTTP, HTTPS	Admin harus melakukan *patching* atau menutupi celah keamanan pada sistem target
Directory Guessing	Halaman utama user admin (/users/admin) dapat dengan mudah ditebak.	Admin seharusnya, menciptakan file index.php sebagai redirect.
Command Execution	File backup tool freeping dapat disalahgunakan untuk menjalankan perintah ke server kernel.	Admin seharusnya menghapus file backup dari tools freeping.
CSRF	File backup tool admincontrolpanel dapat disalahgunakan untuk mengganti password admin.	Admin seharusnya menghapus file backup dari tools admin control panel.



Gambar *46Attack - Defense Blue Team*

Setelah melalui proses hardening selama satu jam, maka antar peserta *blue team* dapat melakukan saling serang.

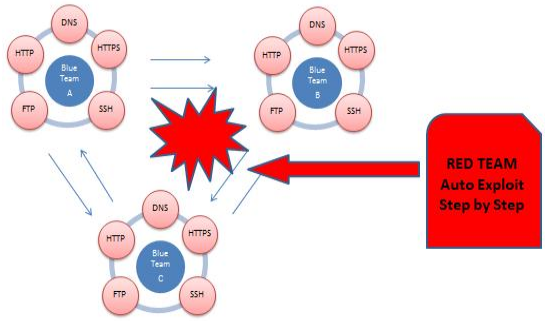
Seperti pada Gambat 2 *Blue Team A* dapat melakukan serangan terhadap celah kemanan yang terdapat pada lima layanan terhadap *Blue Team B* dan *Blue Team C*, demikian juga *Blue Team B* dapat melakukan serangan terhadap *Blue Team C* dan *Blue Team A*. Seluruh proses serang dan diserang akan langsung dimonitor oleh *White Team* dan *Red Team*. Ketika ditemukan ada team melakukan jenis serangan yang tidak diperbolehkan pada saat kompetisi, maka tim akan dikenai sanksi oleh Panitia.

4.3. Skenario Penyerangan Red Team Kompetisi *Death Match Tournament*

Skenario penyerangan oleh Red Team adalah skenario yang diharapkan bersifat adil dan berjalan menggunakan teknik yang sama kepada seluruh peserta kompetisi dan dilakukan secara berurutan dan bersamaan oleh tim penyerang (Red Team). Tindakan ini ditujukan untuk menyetarakan serangan dengan adil dan menggunakan

teknik yang sama ke seluruh peserta, sehingga peserta kompetisi tidak mendapatkan serangan yang berbeda dari tim penyerang saat kompetisi berlangsung. Aturan yang harus diikuti oleh Red Team adalah sebagai berikut:

1. Red Team tidak melakukan serangan pada proses hardening.
2. Setelah selesai sesi *hardening*, Red Team wajib menjalankan semua file *script* pada kategori rendah secara bersamaan berdasarkan kategori dan berdasarkan waktu ke seluruh peserta kompetisi.
3. File auto-exploit dijalankan mulai dari kategori rendah, menengah, sampai dengan high.
4. Ketika semua file *auto-exploit* pada semua kategori telah selesai dieksekusi, Red Team boleh kembali menjalankan file *auto-exploit* apapun dan sebanyak berapa kalipun secara bersamaan berdasarkan kategori dan berdasarkan waktu ke seluruh peserta kompetisi.



Terdapat 2 (dua) jenis serangan bagi Red Team, yaitu *semi-automatic* dan *step-by-step*. Berikut ini adalah beberapa *file script* yang akan digunakan tim penyerang untuk menyerang *Server Blue Team* yang bersifat *semi-automatic* pada penelitian ini.

Gambar 47 Serangan Red Team

Tabel 32 *Semi Automatic Script*

Nama *Script File*	*Path File*	Teknik Serangan	Deskripsi
ssh-user.sh	/usr/attack/ssh/	Manipulasi akses *user*	Mengubah authorisasi dengan cara mengubah user ID dari user chkrootkit
ssh-root.sh	/usr/attack/ssh/	SSh-Key-Generate	Mengambil private key authorisasi untuk masuk sebagai root ke dalam *server*
ssh-nmap.sh	/usr/attack/ssh/	Application access manipulation	Mengubah akses dari penggunaan aplikasi NMAP yang memiliki fitur untuk mengeksekusi perintah shell dengan menggunakan sintaks –interactive.
ftp-deface.sh	/usr/attack/ftp/	Secure FTP	Menggunakan secure FTP untuk uploading file baru dan dapat overwriting index.html

4.4. Penilaian oleh White Team

White Team bertindak selaku juri yang akan memberikan penilaian melalui aplikasi pelaporan kompetisi jaringan. Laporan yang masuk terlebih dahulu harus dinilai terlebih dahulu. *White Team* tidak diizinkan melakukan penilaian secara acak.

Aplikasi *dashboard kompetisi jaringan* akan ditampilkan pada sebuah layar monitor yang berada di depan seluruh peserta kompetisi. *Dashboard* tersebut menampilkan informasi perolehan nilai dan status *service server* yang dimiliki oleh peserta. Tampilan aplikasi penilaian secara otomatis seperti pada Gambar 4.

Gambar 48 Tampilan Monitoring Kompetisi

5. SIMPULAN DAN SARAN

5.1. Simpulan

Aplikasi yang dibangun untuk penghitungan scoring secara otomatis pada jenis kompetisi model *death match tournament* memberikan kemudahan bagi peserta dan keadilan bagi seluruh peserta kompetisi. Penelitian ini dapat dijadikan kerangka untuk pelaksanaan model kompetisi jaringan di tingkat lokal universitas.

5.2. Saran

Beberapa saran yang perlu dilakukan untuk penelitian lanjut untuk meningkatkan kualitas kompetisi pada keamanan jaringan adalah:

- Mengembangan model kompetisi yang lebih luas cakupannya. Kompetisi dapat dilakukan melalui jaringan Internet.
- Mengembangkan aplikasi untuk jenis model kompetisi lain, sehingga dihasilkan kompetisi yang penilaiannya dapat transparan kepada seluruh peserta.
- Aliran data selama proses kompetisi perlu dilakukan analisis mendalam untuk melihat beban jaringan selama pelaksanakan kompetisi.

6. UCAPAN TERIMAKASIH

Terima kasih kami sampaikan Direktur Penelitian dan Pengabdian kepada Masyarakat DIKTI Tahun 2014 yang telah memberikan dukungan moril dan materil atas terselenggaranya penelitian ini.

7. DAFTAR RUJUKAN

[1] Jhon E.Canavan, Fundamentals of Network Security, Artech House INC, London, 2001
[2] Mike O'Leary, Small-Scale Cyber Security Competition, Proceedings of the 16th Colloquium for Information Systems Security Education, 2012. Lake Buena Vista, Florida
[3] State Collegiate Cyber Defense Competition, CSSIA 2013
[4] http://en.wikipedia.org/wiki/National_Collegiate_Cyber_Defense_Competition
[5] VICTOR-VALERIU PATRICIU, Guide for Designing Cyber Security Exercises, Computer Science Department Military Technical Academy
[6] Lance J. Hoffman, Daniel Ragsdale: *Exploring a National Cyber Security Exercise for Colleges and Universities*, IEEE Security and Privacy, Volume 3, Issue 5 (September 2005)
[7] IOWA State University Information Assurance Centre, National Cyber Defense Competition Guide, SPRING 2013.