VOL. 10, NO. 2, FEBRUARY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

DEVELOPING A SMALL SCALE CYBER DEFENSE COMPETITION

Albert Sagala, Deni P. Lumbantoruan
Cyber Security Research Centre (CSRC), Faculty of Electrical and Informatics Engineering, Del Institute of Technology, North Sumatra, Indonesia
E-Mail: albert@del.ac.id

ABSTRACT

The growth of cyber security competition is increase in Indonesia; it is organized by private institutions or university level. This cyber competition will encourage students and community to increase their level of knowledge in protecting the infrastructure by cracker. However, most institution do not prepare the insfrastruture as an internship for students to learn ethical hacking. So, sometimes hacking activity will make the operational disturbed. Institution need to have an isolated network as an arena for study ethical hacking. In this paper, we design a lab for making lab simulation so that red team and blue team can join together in one network. The network topology model which we provide also support scoring automatic for judging the cyber competition. This scoring system will help the white team to control and monitor the competition.

Keywords: security competition, application monitoring, application scoring, death match tournament.

INTRODUCTION

Knowledge of computer network security (Jhon, 2001) is very important to prevent the misuse of network resources from third party. Network security has some security aspects are defined as confidentiality, integrity, and authentication. Confidentiality is an attempt to keep information from people who are not eligible or do not have permission. Integrity requires that the information must not be altered without permission from the owner. Authentication is the aspect relates to a method for stating that the information accessed by the right people and also sending by the right people.

A need of security professional hackers in Indonesia is so high. Universities should equip students with technical capabilities in the field of ethical-hacking. While, today this is still very rare Studies Program curriculum which opens towards the concentration of network security. So that students learn network security by autodidact, and this often affects the disruption of the infrastructure that is being operated (Lance, 2005). Even in IT Curriculum that learn about network administration, students only have time to learn how to activate the service but lack of skill and knowledge on how to protecting the client when using the service.

The need of security professional hacker in Indonesia, there are so many cyber defense competitions so that it become popular and attract the student to learn about security. Some competition that run regulary in Indonesia are Cyber Defense Competition by Defense of Ministry, National Cyber Jawara by ID SIRTI (Indonesia Security Incident Responses Team on Internet Infrastructure), Gemastik (National Student Exhibition of Information and Communication Technology) by DIKTI (General Higher Education), and Indonesian Cyber Army by Menkominfo and APTIKOM.

In the learning network security, very necessary to provide an isolated lab to operational networks. To implement this, often constrained by limited funds held by institutions.

In this paper, we will explain step and methodology to make a small scale cyber defense competition with a limited budget or infrastructure. We also provide the system with scoring automatic so that a winner of the competition can be obtained in a fair and transparent. Competition model supplied is capable models to test the ability of each participant in the network security. So at the end of the competition can be seen that the winner is actually does have skills.

Related research and contribution

National Collegiate Cyber Defense Competition (NCCDC) was develop an application for monitoring of network competition by dividing actor competition into the Blue Team, Red Team, White Team, Gold Team, Chief Judge, and Green Team. The competition is carried out using the Internet infrastructure. Each participant will be given a Public IP and Private IP (NCCDC, 2013). Each service would be checked by the engine every three minutes. A successful check was recorded if the service provided the expected response as designated by the grey team (IOWA, 2013).

Our contribution in this paper is to develop application for the cyber defense competition so that white team (judge) will easier to grade the participant. Service will be checking every seconds and the scoring will be add to the system. We also provide a guideline for small scale cyber competition lab environment. In this small scale cyber competition, students need to familiar with setup and manage the server, hardening the server so secure from the attacker.

NETWORK SECURITY COMPETITION MODEL

Cyber security Competition (VICTOR, 2005), (Lance, 2005) is a competition that aims to test the ability of participant in terms of network administration, information systems security, software security holes in the system, in a limited time to familiarize themselves with the everyday life of the network security and a

security system server. There are several types of security models are often contested competition, such as Death Match Tournament, Digital Forensic Investigation, Face to Face Competition, Cyber Security Challenge, Cyber Quests / Security Quiz, Cyber Grand Challenge, Pwn2Own, Discover and Embedded System Security Vulnerabilities (Mike, 2012).

In this study, we review a model of competition called the Death Match Tournament. This model was chosen because it will test the ability of participants, ranging from server configuration correctly, to try to carry out attacks to servers maintained by other participants.

Death Match Tournament Competition Model required participant to have three (3) different abilities, attack other blue team server, defending from other blue team and red team attacking, and hardening servers so that can run well.

Blue team will responsible to maintain one server with 5 service installed and minimum 15 vulnerability. Default port will be assign to each services so that it can access by other blue team or red team.

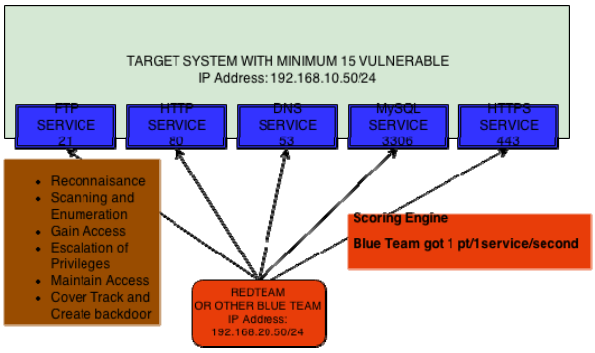

Figure-1. Assessment by Red Team to Blue Team server.

As shown in Figure-1, the red team will run ethical hacking step, start from reconnaissance, scanning, enumeration, gain access, escalation privileges, maintaining access and cover the tracks and create backdoor. The blue team needs to patch the existed vulnerability. On death match tournament, the attacking also can coming from another blue team. During competition, the scoring engine will run and give one point for each service per second.

In developing the model of the Death Match Tournament competition, there are some components that are need to define and prepare, such as:

a) Actors who participate in network security competitions are divided into 3 (three) types, i.e. participants who competed (Blue Team), a jury competition (White Team), and a Red Team as a Security Professional.
b) The competition is using a dashboard application that is displayed on a monitor screen which is located in front of all the participants in the competition. The dashboard will display the information of each service status.
c) Rules and guidelines are made to avoid some cheating, and as a guide for participants to get score and also guideline to scoring manually.
d) Network topology which is designed for competition, consist of 2 subnets, the first subnet is for the participants or Blue Team. The second subnet is for the Red Team and the White Team.
e) Red Team attack will attack each blue team server. If blue team did not patch the vulnerable system then red team will easy to attack by running the script that already prepared by committee.
f) Servers supplied for the Blue Team was attacked by others blue team and Red Team has vulnerabilities that must be configured (hardening) by the Blue Team for an hour since the competition began.
g) Committee, they are work together with white team and red team to asses the competition.

Score competition

Assessment becomes an important thing that should be formulated during the competition; it would lead to the successful implementation of the competition. In the competition model that we propose, assessment was divided into two major parts, namely (1) Automatic Scoring and (2) Manual Scoring. For fairness, we give the weight from automatic is 70% and 30% for manual. This weighting can be change variably based on the competition condition.

Automatic scoring is counting directly by the application when the servers are ready, when the server was stop then the scoring will automatically stop for the team. Participant need to maintain their server during the competition, scoring engine will run and give score for each service. To handle some hacking activity that cannot monitor by the score engine application, participant need to submit their report to the application server. They need to submit the report when they are succeeding to attack the system and also submit the report when they are succeeding to defend against the attacker.

In the manual assessment, the assessment procedure is divided into several levels, depending on the type of attack or defense undertaken by each participant of the competition. Guideline to give scoring is based on Table-1.

Table-1. Manual scoring for White Team.

Type of scoring	Low	Medium	High
Attacking scoring	Max (25)	Max (50)	Max (100)
Defending scoring	Max (25)	Max (50)	Max (100)
Hardening scoring	Max (25)	Max (50)	Max (100)

In Table-1, there are three major components for scoring, they are Attacking, Defending and hardening Scoring. Hardening score is an assessment provided by the

white team for the improvements made by the blue team on vulnerable server image on competition participants.

BLUE TEAM SERVER

Servers were given to the Blue Team. The server is vulnerable; the committee already makes at least 15 vulnerability with category low, middle and high. Participants need to be able to detect the vulnerability and make patching or repair the system.

On red team side, they already prepare script for attacking. The attack used were at least 15 (fifteen) attack techniques with three (3) levels per service level by attacking 5 (five) service on each server the Blue Team. Some attack techniques generated in this study can be seen in the table below.

Hardening session is allocated for one hour. After hardening session, among blue team can attack each other. Also red team will participate in compromise the blue team server.

As in Figure-2 blue Team A can carry out attacks against security holes found in five service in Blue Team B and C, as well as the Blue Team B can perform attacks on the Blue Team C and A. All team will run ethical hacking process and the committee (white team) will monitor the traffic through port mirroring on the switch. If committee found that the participant do activity illegally, such as DoS, Flooding, etc then they will get the warning from the committee.

Scenario attack by red team

Attacking by Red Team is the scenario that is expected to act fairly and run using the same techniques to all the participants. It is run sequence and prepared by committee. There are two (2) types of attacks for the Red Team, which is semi-automatic and ¬step-by-step. This model is based on the vulnerability that already exist in the system.

This action is directed to attack all blue team, and also use the same technique to all participants. In this mode, we also propose the rule for the red team, such as:

- Red team will not attack in hardening sessions.
- Red team allows attack the blue team after the hardening session was finish.
- Committee already prepares auto-exploit file that easy to compromise the blue team server. The script will run from low, middle and high category.
- When all file auto-exploit in all categories have been completed executed, Red team can re-run any auto-exploit.

Scoring by white team

White Team acts as the judge that will provide assessment through reporting applications of network competition. Reports received in advance should be assessed first. White Team was not allowed to conduct random assessment.

SMALL SCALE CYBER DEFENSE COMPETITION INFRASTRUCTURE

At cyber defense competition model that we develop, total of time allocated are five hours. It is divide to two sessions. First session, one hour for hardening session, participant need to assess the image server which will be give by committee and then make some configuration so that it will difficult to attack by other team. During the hardening process, traffic is limited by the white team / red team to avoid attacking between participants. The second session, four hours later, all participants carried out the attack on other participants servers. Competition rules prohibit participants carry out attacks against to the competition infrastructure, hardware and software. Network topology designed competition, consisting of two subnets, which is for the committee, Red Team, application and white. The second subnet is for participant (blue team).

As Figure-2, network for blue team and red team will be separated. Two networks are connected by one Router Board 433, firewall is activated to filter the traffic that allow/disallow from blue team to server application and white team/ red team. In case of blue team or red team cannot connect the wired network, we also provide the Access Point. This access point can only accessed by permission from the committee.

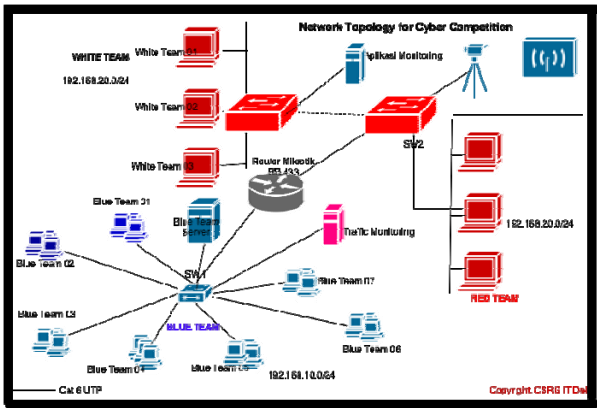

Figure-2. Competition topology network.

Monitoring application will monitor all service that available at each blue team server. It will be started after one hour hardening sessions. Monitoring application will check the status of every services (http, ssh, ftp, dns, mysql). Traffic monitoring will have a role as police the traffic from blue team to another blue team or from red team to blue team. Port mirroring which is integrated with IDPS (Intrusion Detection and Prevention System) will be implemented on that network, and the participant will get a warning when it is found make activity which is prohibited, such as DDoS activity, brute force and exploit the network infrastructure.

A competition can be run by simply installing the necessary virtual machines and deploying the blue team server. To minimize the cost for preparing the

competition, we use virtualization so that on one machine can deploy six virtual hosts. In our environment, one machine has 16 GB memory, so it can be use by six virtual servers for blue team. So, we only need three machines for 18 team to compete as a blue team. Restricting work solely to virtual machines reduces complexity means students do not experiment with hardware firewalls, routers, and switches.

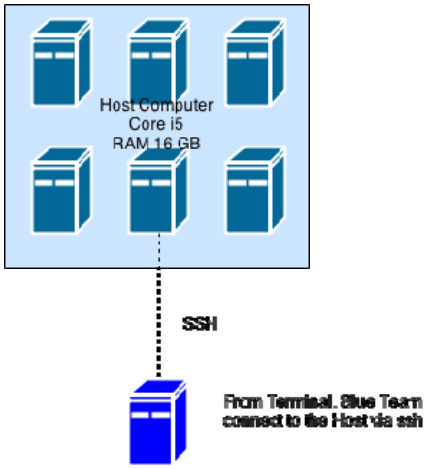

Figure-3. Communications from Blue Team to VMware.

Each blue team will be give the username and password to connect to the server. The server it self is already install web server, ftp server, ssh server, dns server and my sql server. Five server is vulnerable to attack, so that the blue team need to harden the server.

RESULT AND ANALYSIS

Network topology for cyber competition was implemented on Cyber Defense Competition on 22 August 2014 by Cyber Security Research Centre, Del Institut of Technology. Competition was divide into two batch. Batch I is online hacking, and batch II is Grand Final at Del Campus.

At first Batch, participant need to solve some cases that related with network security, and they submit the answer through online e-learning, www.edmodo.com. Problem case that need to be analysis by the team is networking traffic data from CSRC Lab, participant need to answer some question based on data analysis. Tools that can be use by participant are ettercap or wireshark.

At second batch, all participant which is success from batch I come to IT Del to compete each other. As network topology proposed, they only need to bring two laptop. These laptop can be use to attack another blue team and maintain their server remotely. Participant will got username and password to access their server.

All team will be provided with information of network topology, detil information as Table-2.

Table-2. Information for Blue Team.

No.	Team name	IP address server	Username	Password	Web admin	Password web
1	Raphita	192.168.10.130/24	root	****	admin	****
2	cyberX	192.168.10.135/24	root	****	admin	****
3	Cakue	192.168.10.140/24	root	****	admin	****
...	...	....	....	....	....	....
10	Mulajadi	192.168.10.175/24	root	****	****	****

When participant is given the server information, they will connect to ssh server using username and password given. Because all of their activity will be monitor for grading, they need to access the submission report, kompetisi2.csrg.net. For automatic scoring, they need to access kompetisi1.csrg.net. These two website will be online for 5 hours. And after 5 hours competition, the white team can find the winner based on two application that develop, manual report and automatics.

To accomodate 10 team that will be competed on CSRC competition, then we need to provide hardware as Table-3.

Table-3. Hardware specification.

No.	Hardware	Unit	Specification	Virtual Server
1	PC for Blue Team	2	Intel Core i3 RAM 16 GB	12 Units
2	PC for monitoring	1	Intel Core i3 RAM 4 GB	-
3	Switch 24 port	3	Port Mirroring Enable	
4	Router	1	RB 433 Mikrotik	
5	PC for application	1	Intel Core i3 RAM 4 GB	
6	Cat6 UTP	1	Gigabit	
7	Access point	1	Gigabit	

PC for blue team will be installed on virtual machine with 2GB RAM each. So that, with 16 GB RAM, it can allocated for maximum 6 teams. We still need to allocate 4GB for computer host. Two PC for monitoring and application also will be provided with hardware specification lower than PC for blue team.

On competition that we have done, almost all participant connect to the system, only two team have a difficulty to access the server because the team can not access the server with domain name. And we are blocking access the server by ip address. For enhanced the infrastructure security we define some firewall rule on IDS server, router and application that we implemented. Rule that we implemented on IDS system are blocking illegal activity such as DoS, DDoS, Flooding, Bruteforce the infrastructure.

CONCLUSION AND SUGGESTIONS

A small scale cyber defense competition already develops and implemented on cyber competition that held by Cyber Security Research Group. The cost for the infrastructured is minimum with only one server to serve six blue team. This small scale cyber defense competition is also integrated with two applications which has a function for automatic and manual scoring by white team. This integrated system is well implemented and can be as a model for university or private institution to conduct the cyber competition.

With minimum hardware to implement the cyber competition then easy for the commitee to setup the environment and troubleshoot. Also, with automatic and manual scoring, committee with the help of white team is wasy to find the winner. In Traditionally, to decide the winner on cyber competition with death match model will need two hours minimum, but with the system that we develop, the winner can be decided right after the competition was finish.

After develop and implement the cyber competition, some suggestions that need to do for further research so that can improve the quality of competition in network security are:

1. In network topology, we can implement honeypot to make the network more complex, so that participant needs to run scanning first to identify the real victim on that competition. Also honeypot can be implemented by the commitee to protect the infrastructure from malicious activity.
2. In this research, we divide 70% for automatic and 30% for manual score. This weighting can be adjusted based on the model competition. So, it need to be reformulated to get the weighting.
3. Deep Packet Inspection during the competition is needed in implementing IDPS. From this inspecstion, can be integrated to give add or reduce the scoring.

ACKNOWLEDGEMENTS

We would like to say thank you to Directorate General of Higher Education (DIKTI) that has provided moral and material support for the implementation of this research.

REFERENCES

Christopher P. Lee. 2009. A. Selcuk Uluagac, Kevin D. Fairbanks, John A. Copeland. The Design of NetSecLab: A Small Competition-Based Network Security Lab. http://www.csc.gatech.edu/~copeland/6612/netseclab/Design%20of%20NetSecLab.pdf Accessed October 2014.

Chuan Yue. 2012. Weiying Zhu, Gregory Lynn Williams, Edward Chow Using Amazon EC2 in Computer and Network Security Lab Exercises: Design, Results, and Analysis, American Society for Engineering Education.

IOWA. 2013. State University Information Assurance Centre, National Cyber Defense Competition Guide, SPRING.

Jhon E. Canavan. 2001. Fundamentals of Network Security, Artech House INC, London, UK.

Mike O'Leary. 2012. Small-Scale Cyber Security Competition, Proceedings of the 16th Colloquium for

Information Systems Security Education. Lake Buena Vista, Florida.

Nicholas Childers .2009. Bryce Boe, Lorenzo Cavallaro, Ludovico Cavedon, Marco Cova, Manuel Egele, and Giovanni Vigna. Organizing Large Scale Hacking Competitions. https://seclab.cs.ucsb.edu/media/uploads/papers/2010-dimva-organizing_large_scale_hacking_competitions.pdf Accessed October 2014.

Lance J. Hoffman. 2005. Daniel Ragsdale: Exploring a National Cyber Security Exercise for Colleges and Universities, IEEE Security and Privacy. 3(5).

NCCDC. 2013. State Collegiate Cyber Defense Competition, CSSIA.

VICTOR-VALERIU. 2005. PATRICIU, Guide for Designing Cyber Security Exercises, Computer Science Department Military Technical Academy.