ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Simulation on Cyber War in Cloud Computing

Arul Selvam. P[1], Jeevanantham. G[2]

Dept. of Computer Science and Engineering, Nehru Institute of Engineering and Technology, Coimbatore, India[1, 2]

ABSTRACT: To secure confidential data we have developed this paper. Our proposal uses the idea of an isolated simulated environment with real world threats to instruct the participating teams even more effectively. Implementation of this paper facilitates the scalability and the ease to access the system from anywhere. Thus the players can attend the training from different centers, and the cloud computing approach satisfies these requisites. In our paper, we have shown simulator on cyber war in one cloud based environment and also other simulations involving cloud computing and multi-agent based systems uses intelligent agents to manage the interaction between the attacker machines and the player machines. This simulation not only depends on IT professionals, but also the top decision makers of the institution. Thus, the top decision maker could measure the consequences of a resolution before it happens in real world.

KEYWORDS: Cloud computing; cyber war simulation; Multi-agent-based system; real-time attacks

I. INTRODUCTION

In the World Wide Web, cyber threats can materialize in the worst ways in the case of malwares, DDoS, phishing, trapdoors, logic bombs and others; bring concerns from the public and private organizations to ordinary users.The simulator is based on cloud computing due to its various advantages such as availability and scalability in addition to the cost of the infrastructure be vastly reduced.The paper is organized as follows: section 2 presents the work related to simulation of cyber-attacks. In session 3, it showed details about the model of the system architecture. Session 4 provides details about the model of the system design. The section 5 presents the conclusion of this article and shows the objectives and benefits of the proposed model.

II. RELATED WORKS

Several researches about simulations are being carried out. We quote Ariel Futoransk et al. [2009], which proposes the ”Insight”, a framework that is centered on the point of view of the attacker and is based on a probabilistic model of attacks and using this model of attacks the simulator does not become so realistic.

Our model focus on two sides of the simulation, the attacker and the defense, it alsomakes use of a multi-agents based system, using intelligent agents to simulate the attackers, so it creates a real system, since agents can learn on each simulation, making it different and more challenging than the last.We are also going to link with simulations involving cloud computing and multi-agent based systems and show the result.

III. ARCHITECTURE MODEL

While developing this work, one of our main concern were that the simulator could be accessed from anywhere, allowing different centers to participate on the same exercise, making it more realistic. Having this in mind we built all the virtual machines on a private cloud server. The architecture is specified in Figure 2.

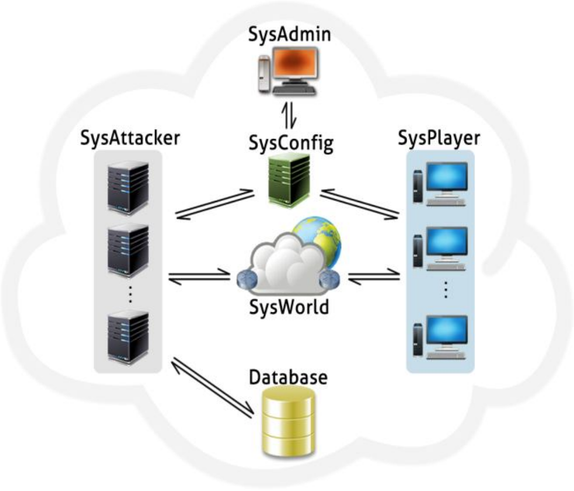

Figure 2: Cloud Architecture

The main subsystem is the SysAdmin. It is used to manage all the exercise, choosing the training scenarios, numbers of players and attackers, time and etc. This machine is also responsible for generating and show the live reports (explained in details later) using the logs received from SysConfig.SysAttacker machine will simulate an attacker and the numbers of machines will be chosen by the Administrator on the configuration section. This system will act like a real attacker, simulating all the steps for a successful penetration, since the reconnaissance until the real exploitation,using real vulnerabilities. This subsystem connects directly to the database where the exploits are.

The SysWorld is a virtual machine responsible for simulating all the communications, i.e., real world routes, email, telephony, etcetera. It can be configured for different kinds of exercises, since attackers on the same network as the players, until attackers on the other side of the world, simulating the use of proxies, tunnels passing through internet providers, firewalls and all the sort of network devices. This part of the simulation is useful when training how to protect from internal threats or how to trace the origin of the attacks.

The SysPlayer are vulnerable operational systems controlled by the teams. The vulnerabilities are dynamic, chosen by the Administrator through the SysAdmin. The players must fix the vulnerabilities before the Attackers exploit them. As the simulator is built on the cloud, teams can access it from different training centers around the country through the internet.

SysConfig machine handle the configuration files generated by the SysAdmin and do all the communication between both SysAttacker and SysPlayer, setting the configurations and also querying for new information for state updates.

IV. DESIGN MODEL

A. Agents

A Multi-agent system is used to control the exercise, setting up the configuration on each virtual machine. This task is accomplished using a multi-agent system (MAS), in formal definition, it is a system composed of multiple interacting intelligent agents within an environment [WEISS 1999]. An agent is a computer system that is situated in an environment and is capable of autonomous actions in this environment in order to accomplish its design objectives [Wooldridge 2002].The synchronization of the agents is fundamental for the simulator itself and for a better learning of the agents. Each machine has many intelligent agents, in particular one that controls the other agents and its own machine. Among others functions, the agents must control and monitor.

1) Control and Action: The Control Agents set up the machines that are involved in the simulation.

On the Administrator's machine, these agents have the function to send beginning or ending signals of the simulation, besides the function of managing the initial set up configurations. In fact, these settings can be changed at any time, thus the Administrator can set the difficulty level of the training.

On configuration machine, Control Agents delegates the actions that the agents on another machines conduct since the beginning of the simulation until the end of that, but the initial set up of the exercise is dictated only by the Administrator, while during the simulation, besides the Administrator interference in the actions, the agents analyzes the state, i.e., signals sent by other agents, and delegate the tasks to be performed.

In defense machines, the agents configure which vulnerabilities are enabled and which are disabled, and also monitor if the integrity of the defense machines is maintained, i.e., if the enabled services by the agents are still working and vulnerable, whether they are disabled, etc., thereby sending signals of the machine state where it is situated to the configuration machine that delegates what action should be taken.

On each attacker machine, this agents configure which attacks are made, for how long and at what intensity they occur, which exploits are used, which others attacks machines is assisting during an attack, originating, thus, a distributed attack.

This machine also have Attacker Actions Agent who will be responsible for making the attack on the stipulated targets using the information collected by the monitoring agents, these intelligent agents adapt to the environment and thus, they can choose the best strategy to efficiently dominate the target, if successful, its implements these backdoors or logic bombs; and contain Defense Actions Agent that are able to prevent attacks on the Attackers machine to succeed, making decisions on how to proceed in case an attack against them is occurring.

2) Monitoring: The Monitoring Agents will make the analysis of the activities, such as network traffic, which occur on each machine during simulation to generate reports and logs, and populate the memory of all agents.

On SysAttacker machines such agents monitor attacks indicating the final result, whether the attack was successful or failure. In case of success, how long it took to reach the goal, how much computational effort was required to make the attack and if the attacker machine had been compromised. In case of failure, a simple report about what had been done.

In the SysPlayer machine, the agents will monitor the activity of the machine player, i.e., how much time was required to detect a current attack, how many vulnerable services were exploited, which services are active and secured and how long it took to fix them, which tools were used to block the attack and which were these.

In the SysConfig machine, these agents will gather and organize all the information passed by the Monitoring Agent of the other machines tobuild the graphics and pictures of the activities that will be displayed on the monitor of the Administrator.

3) Report/Logs: A variety of graphics and reports are generated during and after the simulations.

Live reports show what is happening during the exercises and is used by the Administrators so they can evaluate how the teams are handling the attacks and doing their defenses.Among the information's available on this report is possible to verify the network traffic, which teams were attacked, which services are still vulnerable. For this will be used an evaluation system, explained later.

The post-simulation reports, is used for the Administrators so they can statistically evaluate what happened during the simulation. Information's about what kind of attacks were the most efficient, possible damage caused, what threats were easily defended and a parallel with the previous exercises to see if the teams are going better. The Administrator can also see traffic patterns and which actions were taken to solve a problem. Thus the weaknesses can be improved.

B. Database

It contains two important types of information, what vulnerabilities exist and what their exploits. The first piece is important because it is from the Administrator chooses which kinds of vulnerabilities the teams have to defend, and the second contains the necessary information on how attackers exploit them.

1) Vulnerabilities:This database holds all the information necessary to create vulnerable environments. With this, Administrators can choose which type of attack the teams will have to protect from. The information about each vulnerability are: type (i.e., stack exploits, format string exploits, xss, phishing, etc.) and difficulty. The agents explained will be responsible for executing the appropriate attack.

2) Exploit:The exploits database will store the information necessary to perform the attacks. Based on intelligent analysis, the Attacker VM will discover the flaws in the players systems and use the correct exploit for that. The main information in this database is: which exploits work with a specific vulnerability.

C. Evaluation System

For a better analysis on the performance of teams during the exercises, the intelligent agents queries for different types of states on the SysPlayer machine. Depending on their states, a team scores or gets a penalty.

1) Services are active and vulnerable: The exercise starts with all chosen services active and vulnerable. This is the worst case, since the beginning, the teams must work on fixing all they can without compromised the services.

2) Services are active and not vulnerable:The best situation is when services are active but not vulnerable. It is considered ideal because the services are protected and available.

3) Services are not active: Disabling the attacked services is not the best way to protect the machine, because in this way the teams can avoid being attacked, on the other hand it fails to provide the services. A strategy must be used to analyze what causes the worst consequences.

V. CONCLUSIONS

Disabling the attacked services is not the best way to protect the machine, because in this way the teams can avoid being attacked, on the other hand it fails to provide the services. A strategy must be used to analyze what causes the worst consequences.As mentioned in the introduction of this paper, one of the requirements is that the simulator could add in one battle simulation, people across different training centers. The choice of implementation on a private cloud server was the best option among surveyed, as was shown in the architecture model session.

The use of a multi-agent system in based came naturally during development of the work, when the team realized it would be more real if the battles become harder over time. The implementation model can be seen in descriptions of the Control Agents, Monitoring Agents and Action Agents.

REFERENCES

1. BILLO, C., AND CHANG, W. 2004. CyberWarfare: An Analysis of the Means and Motivations of Selected Nation States. Dartmouth College.
2. BROWN, B., CUTTS, A., MCGRATH, D., NICOL, D. M., SMITH, T. P., AND TOFEL, B. 2003. Simulation of cyber attacks with applications in homeland defense training. SPIE 5071.
3. Como o exercitoprotege o espaco virtual brasileiro. http://info.abril.com.br/noticias/seguranca/ como-o-exercito-protege-o-espaco-virtual-brasileiro-shl.
4. CLARKE, R. A. 2010. Cyber War: The Next Threat to National Security and What to Do About It. Ecco, April.
5. CONSTANTINI, K. C. 2007. Development of a Cyber Attack Simulator for Network Modeling and Cyber Security Analysis. Master's thesis, Rochester Intitute of Technology.
6. Elbit unveils new cyber-war simulator. http://www.jpost.com/Defense/Article.aspx?id=272839.
7. FUTORANSKY, A., MIRANDA, F., ORLICKI, J., AND SARRAUTE, C. 2009. Simulating cyber-attacks for fun and profit. SIMUTools.
8. GEERS, K. 2010. Live fire execises: Preparing fo cyber war. Journal of Homeland Security and Emergency Management 7.
9. KOTENKO, I., KONOVALOV, A., AND SHOROV, A. 2010. Agentbased modeling and simulation of botnets and botnet defenses. CCD COE Tallin Estonia.
10. KOTENKO, I. 2007. Multi-agent modeling and simulation of cyberattacks and cyber-defense for homeland security. IEEE Internation Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Application (September).
11. 2012 norton cybercrime report. http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.
12. WEISS, G. 1999. Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence. The MIT Press.
13. WOOLDRIDGE, M. 2002. An Introduction to MultiAgent Systems. Wiley.