SmallWorld: A Test and Training System for the Cyber-Security

Angelo Furfaro
Antonio Piccolo
Domenico Saccà
DIMES, University of Calabria, Rende (CS), Italy

Abstract

Powerful malware infects millions of computers every day and data breaches continue to increase. Cyber-Security incidents grow in frequency, the costs of managing and mitigating breaches also are rising. This situation demands for a suitable number of information security specialists to adequately handling issues arising in such a complex domain. This paper describes SmallWorld, a scalable software platform designed to reproduce realistic scenarios achieved by the immersion of real systems into a virtual environment with a fully integrated support for teaching with the aim to provide a venue for practical education in the learning and usage of all tools, techniques, and best practices employed to protect the confidentiality, integrity, authenticity, and availability of a designated information service. This software can be successfully adopted during high school, university and specific training to improve the quality and the results of the courses.

Keywords: Cyber-security, teaching, training

Introduction

Cyber security issues have an ever increasing social-economical impact both for citizens and enterprises, then the availability of tools allowing to improve the awareness of cyber-space threats, to learn how handle them and to assess the effectiveness of prevention and defense solutions is critical for the safeness of IT services. Traditionally, security assessment and penetration testing activities are performed on real networks while the training of security specialists is made on insulated and static virtualized systems. This paper proposes *SmallWorld*, a software platform enabling the assessment, teaching and learning of security-related aspects in different areas and for various purposes.

One of the main features of *SmallWorld* is the support for designing and building complex scenarios which are dynamic and reactive and where a

number of autonomous software agents can be deployed. Agents are able to reproduce the behaviors of human users and/or malicious applications into a scenario making it a more realistic training and testing environment.

SmallWorld can deliver to student the three types of learning outcomes defined in Computer Science Curricula 2013 document [1]:

- Familiarity, indicates the student theoretical comprehension of the proposed concepts. This is achieved via books and lectures available in the Content-Management-System of *SmallWorld*.
- Usage, indicates the student conceptual comprehension, he can apply it correctly when it's required. A mix of lectures and practical laboratory exercises usually achieves this.
- Assessment, indicates that the student can correctly recognize the given concept in practice, and correctly apply it as solution to some related problem. This is usually achieved via the training virtual environments and the Learning-Management-System available in *SmallWorld.*

Every content deployed in *SmallWorld* adhere to the NIST Cyber-Security Framework [2] created through collaboration between industry and government. The Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure.

Related Works

Most of the existing cyber security assessment tools act on real systems and virtual laboratories support only pre-built scenarios by developers or domain experts and do not allow for inclusion of real entities and traffic generation. A list of the main active projects on this subject is reported in the following

The main related work to SMALLWORLD is the **DeterLab** test bed [3], it offers scientific computing facilities for cyber security researchers engaged in research, development, discovery, experimentation, and testing of cyber security technology. DeterLab allows configuring user and group accounts with assorted permissions. Each group can have its own pre-configured experimental environments made of physical machines running Linux, BSD, Windows, or other operating systems. Users running DeterLab experiments have full control of real hardware and networks running pre-built software packages.

eLearningSecurity [4] offers certification, virtual labs and courses on cyber security;

The Hacker Accademy [5] has a web-based platform for experiencing, and teaching information security from the hackers perspective;

PENTESTIT [6] allows to emulate IT infrastructures of real companies, created for legal penetration-testing and for empowering

penetrating skills. Laboratories are always unique and contain the most recent and known vulnerabilities.

Pentest laboratory [7] offers a testing lab environment that includes all of the hosts, network infrastructure, tools, and targets necessary to practice penetration testing. However this solution is limited to a single scenario with four hosts, two networks and a firewall. In addition it is tied to GNU/Linux platforms.

The above solutions compared to SmallWorld have many limitations. In general they are not cloud oriented, so they are not scalable and it lacks the possibility to reproduce certain kinds of attacks, like user oriented attacks, because it would need the user interaction. SmallWorld overcomes to these difficulties introducing smart Agents provided with different behaviors allowing them to act as real users inside a scenario.

SmallWorld Architecture

SMALLWORLD has been developed with the main objective to be extensible and hypervisor-independent. To achieve these goals, it has been designed as multiple layers system, where the components of each layer cooperate among them to implement higher abstraction level services by exploiting the underlying tiers. A schema of the resulting architecture is reported in Fig. 1.

The five layers of the SMALLWORLD architecture are briefly described in details by the following subsections.

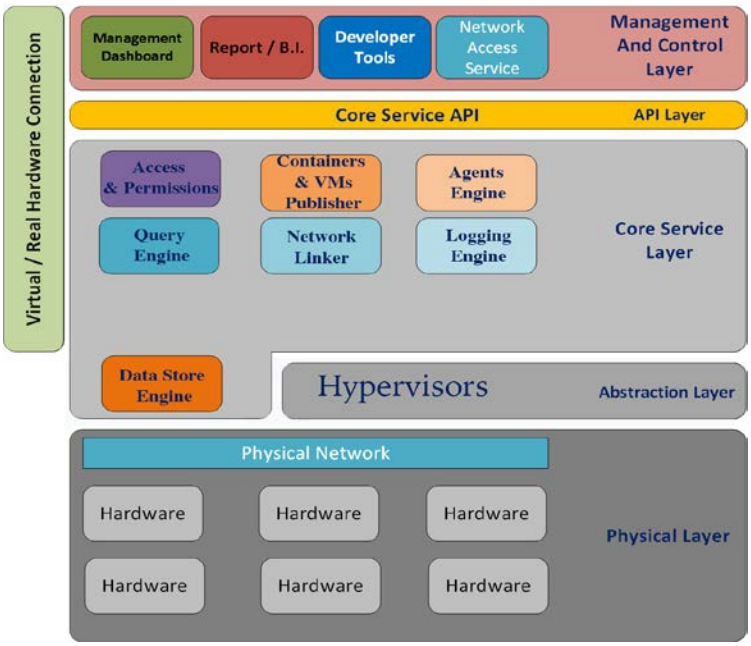

Figure 1

The Physical Layer hosts computational, storage and networking hardware configured in a suitable way in order to offer fault tolerance, business continuity and data replication mechanisms services for proper and scalable operation of the hypervisors. The above hypervisor layer abstracts and hides bare metal details that can then be easily changed for scalability purposes without impacting on the overall system operations.

The Abstraction Layer hosts the virtual machine monitor and the network hypervisor, which respectively enable to define via software the virtual computational nodes, along with the above operating systems and software layers and the virtual network infrastructure. There exists many hypervisors solutions that offer these features, OpenStack [8] is currently in use.

The Core Service Layer hosts the main software component that implements the core SmallWorld features, which are in turn, exposed by the above API layer. These components exploits the hardware abstractions offered by the hypervisors.

The API Layer is used for the implementation of the applications of the Management and Control Layer and is the key to implement the SmallWorld scenarios design and development toolkit independently from the software technologies used in the underlying layers.

The Management and Control Layer introduces the following facilities:

- A Dashboard, from where is possible to manage the scenarios, agents and virtual machines. It also allows to display system usage and statics, set scenario parameters, handle students access and account management.
- A Report tool, which provides statistical data about the running scenarios and the results of the exercises.
- A set of Development Tools that include an agent development tool, a scenario development tool and a virtual-system development tool.

Users can use these tools to easily build a new laboratory or load a preconfigured scenario. One of the SmallWorld main strength is the rich catalog of vulnerable software, operating systems, network templates and agent behaviors delivered with the platform.

A Case Study

In this section we present a case studies implemented in SmallWorld, figure 2, and that will be used during the cyber-security course at the University Of Calabria and and training laboratory during the second Cyber-Security Master course organized by Poste Italiane in collaboration with the PosteCERT and the University of Calabria.

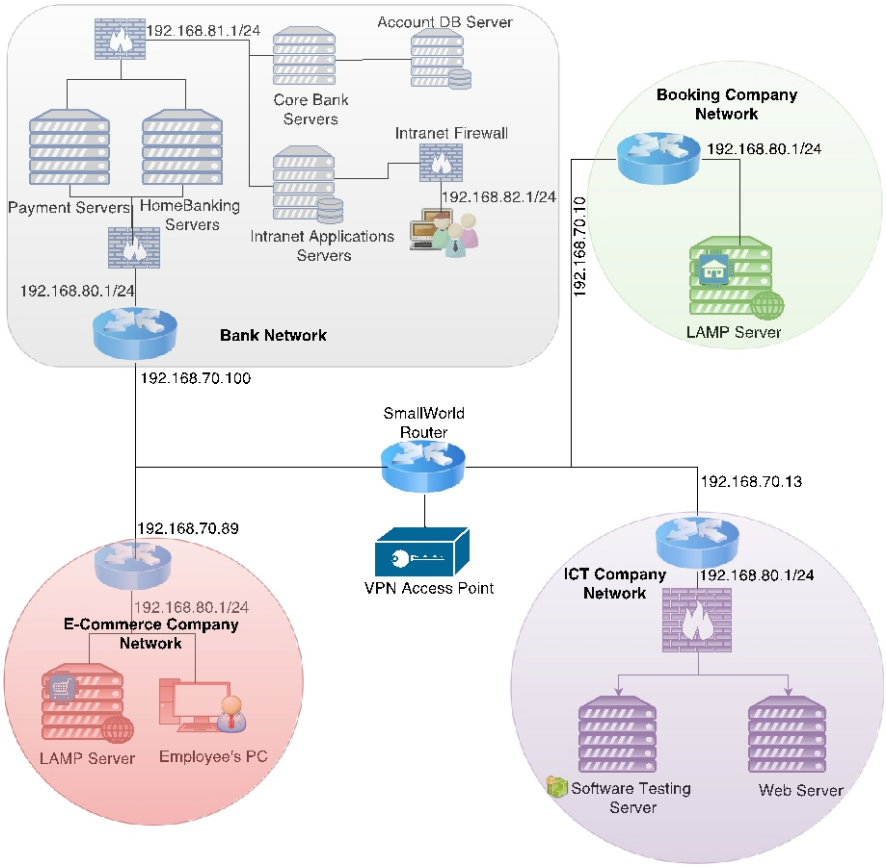

Figure 2

In this large computer network, many kinds of exploit and attacks techniques can be practiced. Each device and machine deployed is affected with al least one unique vulnerability with the purpose to allow students to “capture the flag” moving horizontally in the network from a start point to the end point, represented for example by an information contained in the servers of the bank.

Figure 3, shows as an hacker, in our case a student, can exploit a Stored XSS vulnerability in the E-Commerce system to stole the credentials of an employee or of the administrator. The malicious code is included as comment when the hacker place and order and it will be executed when the employee will check the new orders. At this point the cookies are stealthy stolen and sent to a server controlled by the hacker that now can impersonate the employee and have access to the back-end and to users and payments informations, furtheremore he can install a backdoor on the server and use it as a bot for future attacks.

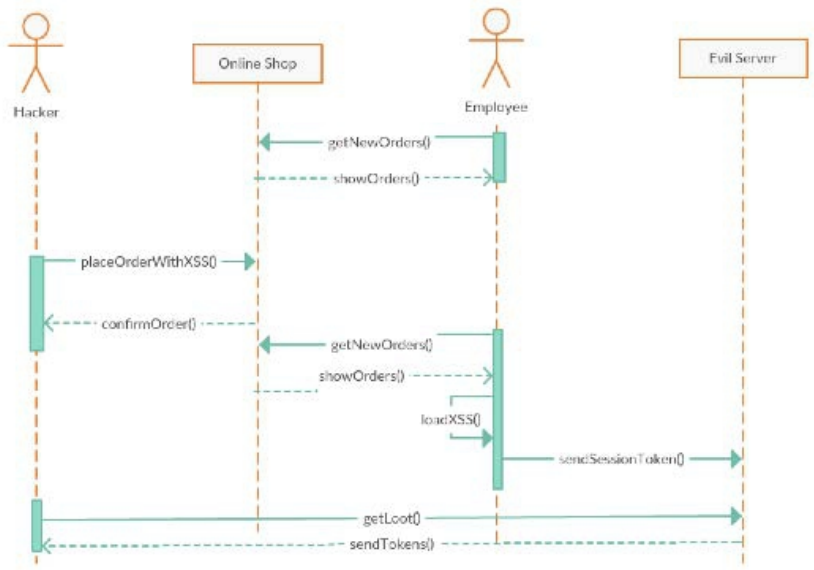

Figure 3

Unfortunately, we can't expose too many details about the vulnerabilities deployed in the scenario and how to exploit them because, as mentioned before, it will be soon officially used in two master courses.

Conclusion

Schools, University and also companies need a system to provide training courses, examples and laboratories built on top of real-like challenges and to configure them in an easy and quick way. Employees need to smoothly learn how to safely live in a cyber space by increasing their awareness of threats before exposing themselves to real risks. Researchers working in cyber-security need a great amount of real-like system logs, security environments to test new algorithms or to study malware propagation. Everyone can start soon to access the SmallWorld cloud and play with the preset content or customize the environment according to his needs.

References:

ACM/IEEE-CS JOINT TASK FORCE ON COMPUTING CUR- RICULA. Computer science curricula 2013. Tech. rep., ACM Press and IEEE Computer Society Press, December 2013.

http://www.nist.gov/cyberframework/

SCHWAB, S., WILSON, B., KO, C., AND HUSSAIN, A. Seer: A security experimentation environment for deter. In Proceedings of the DETER Community Workshop on Cyber Security Experi- mentation and Test on

DETER Community Workshop on Cyber Security Experimentation and Test 2007 (2007), USENIX Asso- ciation, pp. 2–2.
https://www.elearnsecurity.com/
http://hackeracademy.com
https://lab.pentestit.ru
http://pentestlab.org
SEFRAOUI, O., AISSAOUI, M., AND ELEULDJ, M. Article: Openstack: Toward an open-source solution for cloud computing. International Journal of Computer Applications 55, 3 (October 2012), 38–42.