SimSecLab (SSL)

A simulated environment for learning security, building trust, fostering privacy, and providing openness in e-Society

Final report
August 1, 2013
DSV, Stockholm University

Prologue

CS2Lab (Cyber Systems Security Lab) is part of the Systems Sciences and Security (SAS) unit at DSV. The lab was formally established in March 2010 with the introduction of courses in Digital and Cyber Forensics, which were later supplemented with another course in Network Security.

The vision of the CS2Lab is the establishment of an education and research profile of the modern cyber infrastructure as an enabler and foundation of e-Society, which is among other things, an aggregation of various digital services, and where various security threats are major obstacles for the generation of trust, responsibility and accountability among the cyber citizens. One of the initial steps in developing the potential of the CS2Lab has been the application for and the implementation of the Future Learn project, the details of are provided below.

System Architecture and Implementation

One of our project's main goals was the provisioning of a simulated e-environment for students and researchers that enables experimentation and training on digital security and forensics issues. A platform that could support such a simulated e-environment should be capable of both system as well as network simulation. A list of requirements that we have compiled in the start of the project is presented below.

Requirement	Description	Explanation
RA-1	The platform should allow the simulation of realistic network topologies	A common SMB network topology may follow a hierarchical switched and routed model combined with a so-called "three-part" firewall system that provides isolation and filtering between business internal systems, publicly offered services and the rest of the world.
RA-2	The platform should allow the simulation of various network services	There is a set of common network services that are fundamental to the proper functioning of the network. Network services like DHCP for automated configuration of network clients, DNS for communicating with systems using human-friendly domain names and

		SNMP for managing and monitoring network devices are important and their secure configuration and operation a challenging task.
RA-3	The platform should allow the simulation of various e-services	There is a plethora of electronic services that an e-environment may be called to provide. Common e-services may include web services for distribution of static or dynamic content, file transferring, e-mail, multimedia streaming etc. Each e-service comes with its own security requirements and challenges.
RA-4	The platform should enable exposure to information and communication security technologies and protocols.	Strengthening the security of a network or e-service is a complex task involving the integration and cooperation of multiple specialized tools and technologies. Security appliances such as firewalls, virtual private networks (VPN), intrusion detection systems (IDS) and security and event management (SIEM) are indispensable technologies for protecting the security of modern networks.
RA-5	The platform should enable exposure to digital forensic tools and techniques	Digital forensics deal with the recovery and interpretation of electronic data of potentially evidentiary value. Specialized methods and tools need to be employed in order to extract, analyze and present such data in a forensically sound manner. Digital storage systems, traces of network communications and computer-generated logs may need to be examined using a combination of commercial and open-source tools (e.g. EnCase and FTK)
RA-6	The platform should be remotely accessible	A student or a researcher should be able to access the platform anytime of the day using a device with Internet access.
RA-7	The platform should be configurable on-demand	The platform should be flexible enough to allow configuration changes so as to serve different educational or research activities.

After an initial survey of current technologies and products that could support some of the suggested requirements, we selected the software **GNS3** (www.gns3.net), which is an open source programming and development package that allows the simulation of networks of

varying complexity. GNS3 comes pre-packaged with emulation capabilities for specialized networking equipment such as routing devices. The software is accompanied by a graphical interface that allows the user to design and simulate arbitrary complex topologies as Figure 1 shows. GNS3 has integration capabilities with VirtualBox mentioned below, which enables the virtualization of network hosts and integration to the specified network topology.

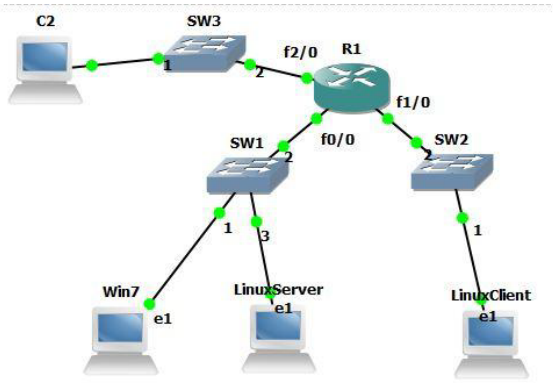

Figure 1: GNS3 Graphical Network Simulator

VirtualBox (www.virtualbox.org) – VirtualBox is open-source desktop virtualization software that allows running in parallel multiple guest operating systems such as Windows and Linux in along with emulated hardware forming a logical abstraction called virtual machine as shown in Figure 2. Sophisticated virtualization software such as VirtualBox provide a number of features that are considerably advantageous for educational or research purposes. The software allows the creation of pre-built virtual machines that can be used as a template for further multiple instantiation. Depending on the scenario, such a pre-built virtual machine can contain a specific operating system type and version, certain installed applications and configurations, e.g. an intentionally insecure and misconfigured Windows system for vulnerability assessment purposes. Virtual machines can be created either by the user, imported from publicly available VM repositories or reuse existing ones from our locally maintained VM template library. Additionally, VirtualBox provides the feature of snapshots, a copy of a system's current state in which the user can later on revert to. This is a feature commonly used when dealing with malicious or potentially destructive software (e.g. computer viruses) that allows isolation of the contaminated system or easy restoration to its normal state.

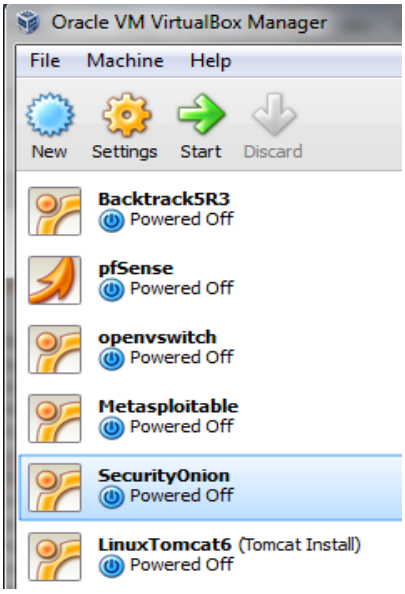

Figure 2: VirtualBox manager interface

Openvswitch (http://openvswitch.org/**) –** Open vSwitch is virtualization software that allows the simulation of network switches thus enabling communication between virtual machines. Contrary to common simplistic network switches, Open vSwitch supports a series of features commonly used in enterprise-grade networking equipment and important for advanced security needs such as network traffic monitoring and policing schemes.

Windows Server 2012 Hyper-V & Remote Desktop Services – Windows Server 2012 is the latest installment in the server operating systems developed by Microsoft. Hyper-V is a native hypervisor that enables the parallel execution of multiple workloads in the form of virtual machines by directly accessing the hardware in an optimized manner. Remote Desktop Services is another feature that allows users to remotely access, using Remote Desktop Connection, such virtual machines in a dynamic and personalized manner. This feature can be configured so as to establish the so-called Virtual Desktop Infrastructure, where the user can be assigned a personalized instance of a certain pre-built VM template, persist her work as well as consume server resources dynamically only when needed.

The first three software packages have been integrated so as to support educational and research activities in the premises of our laboratory, located in the DSV Forum building but also combined with the latest server component to allow remote access to users over the Internet. The platform utilizes 1 physical machine that acts as the main virtualization server along with other 2 dedicated systems for supporting services such as Active Directory for authentication and authorization purposes and Remote Desktop Gateway for remote connectivity purposes. An overview of the system architecture is provided in Figure 3.

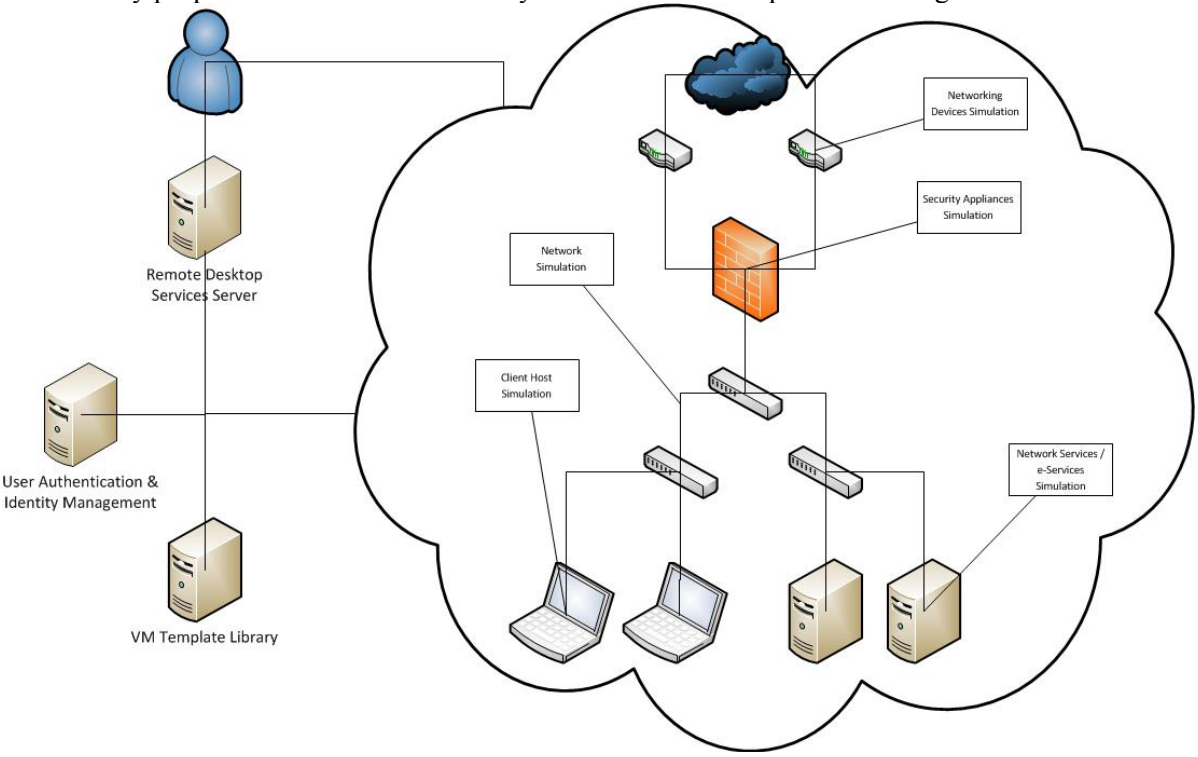

Figure 3: SSL Platform Architecture

Use Cases

Education in Network Security

One of the courses that our lab conducts is NETSEC – Network Security. The course's goal is to teach students fundamentals concepts of modern computer networks and network security

technologies along with practical aspects of relevant security tools and implementations. Some of the topics covered during the course are cryptographic protocols and systems for secure network communication (e.g. SSL and Public Key Infrastructure), malicious use of network communication protocols and countermeasures applicable by networking devices (e.g. switches and routers) as well as network access control and security monitoring mechanisms (e.g. firewalls and intrusion detection systems).

Designing and enforcing a network security policy is not an easy task that requires good knowledge of computer networks, a good understanding of offensive techniques as well as practical challenges in the implementation and integration of the different security functions and components. Practical experience with such security technologies is important not only in order to better understand the theory but also to identify and counter emergent security properties that derive from improper configuration or the complex multi-component nature of modern computer networks.

During VT2012, we have employed our developed platform in order to conduct a set of 3 practical lab exercises that involved a series of tasks and problems for the students relevant to the covered topics. During the first lab, each student group simulated a basic network consisting of a set of network hosts along with routing and switching network devices, similar to the one depicted in Figure 1. The students were asked to establish and monitor communication channels between the hosts thus observe network communication protocols and networking devices in action. The students were also asked to setup core network services required for the proper functioning of the network. Each student group was given physical access to a PC appropriately pre-configured with the simulation software and template VMs representing the network hosts. In the final step, each student group was called to configure appropriately its simulated network so as to connect with other teams' simulated networks thus forming an inter-network. The students were also asked to perform 'erroneous' actions that could cause the network to malfunction and later attempt to resolve the issues in a proper way.

During the second lab exercise, students were able to simulate an exchange of cryptographically-protected messages among a set of hosts. This simulation enabled to bring in reality a commonly presented theoretical model followed by most literature in the area of communication security where two normal users (Alice and Bob) attempt to communicate securely over a malicious third party (Eve). The students using the network simulation and system virtualization capabilities were able to better understand how cryptography is employed in the network communication context as well as how implementation deficiencies may constitute the communication insecure. Finally, the students were able to configure additional systems where digital certificates and digital signatures could be generated and employed. The latter formed the basis of a local public key infrastructure that was later used for securing common e-services like Web (SSL over HTTP) similar to how Web security is applied in the Internet.

Finally, during the third lab exercise, students were able to simulate even more complex network topologies consisting of firewalls, intrusion detection systems, multiple clients and various application servers, as depicted in Figure 4.

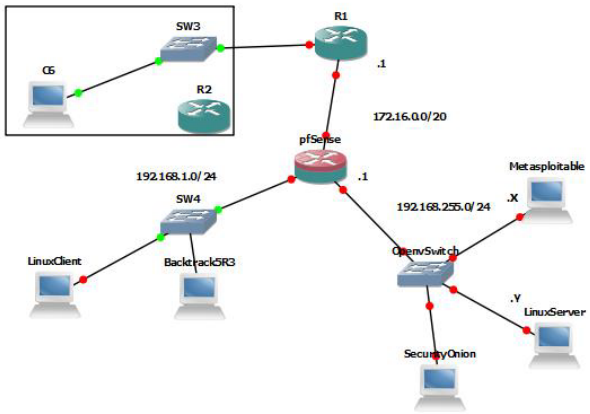

Figure 4: Simulated Network Topology

The students were asked to design a network security policy so as to form security zones depending on the security posture of each system. The students were later asked to configure given security appliances, in the form of VMs, so as to implement the specified security policy and later enforce it by monitoring for potential security violations. Each student group was able to employ more that 7-8 VMs and configure them properly so as to implement common network security solutions such as DMZ, NAT, Firewall, Access Control Lists, IDS and more.

Overall, the experiences gained from the use of such a simulation platform during the course were very beneficial. On the one hand, we have the educational and pedagogical aspects that enabled students to get a deeper understanding of theory and practice themselves in dealing with practical issues that arise in complex systems as well develop skills on designing and implementing appropriate solutions. The simulation platform enabled the teaching staff to reduce considerably the time needed to prepare and supervise such assignments. The use of virtualization features like virtual disks and snapshots allowed easy persistence of a certain group's work during the assignment's period, transfer among different physical PCs or even the student's personal workstations as well as almost instantaneous restoration to a previous good state in case of any potential halting issue.

Remote Desktop Virtualization for Digital Forensics Education and Research

Desktop Virtualization is a technology that allows the decoupling of the execution platform of a desktop environment and any application software running on it from the physical host accessing it. Digital Forensics is one of the main research areas of our laboratory and two courses (Digital Forensics, Cyber Forensics) also run each year. Our lab is equipped with specialized digital forensic commercial tools (e.g. Encase, FTK, Microsystemation XRY, IDA Pro) that are used for the forensic analysis of data carriers such as hard drives, USB sticks, RAM memory, smartphones, GPS devices, encrypted or malicious files etc.

The aforementioned tools are essential both for researchers conducting their research work as well as students during practical lab assignments in the context of the courses as well as further experimentation during courses' project work or bachelor and master thesis work. Previously, there were a number of practical limitations for using such tools remotely due to the fact that most of these tools required a specially configured OS environment to work on (e.g. most of the tools are Windows-based only) that not matching the ones the users had. Furthermore, users were required to perform considerable modifications on their personal systems (e.g. install additional software, apply specific settings). In addition to the former, such software requires the operation of certain licensing schemes (e.g. physical license dongles or network-based license servers) which for security reasons can only be offered in private and isolated systems and networks.

Our developed platform combines the benefits of virtualization with remote access capabilities in order to provide a full-featured Virtual Desktop Infrastructure. Researchers and students can authenticate through a webpage (https://cs2vdi.dsv.su.se/RDWeb), as depicted in Figure 4, and then be given remote access to preconfigured systems operating as virtual machines in our virtualization platform.

Figure 5: Selecting a Remote Desktop

The provided Virtual Machines are pre-built with a selection of relevant software solutions and properly configured according to each software's licensing and functional requirements. The user is given access to a central storage where datasets related to current research or laboratory activities can be found. The user can easily share data between her physical device and the remote infrastructure while keeping to a minimum any modifications on her own system.

Such a remote access service alleviates the problem of limited physical accessibility to such specialized hardware and software while saves considerable time and from potential frustration users from having to perform mundane tasks such as installation, configuration and troubleshooting of software problems. The platform is also optimized in such a way so as a user consumes datacenter's resources only when actually needed which allows for much more flexible and dynamic resource allocation from our datacenter as well as the ability to support several concurrent users (approximately 15 with our current hardware capacity). Such a capability, combined with the aforementioned use cases can pave the way for fully-featured remotely accessible labs simulated a number of scenarios in the digital security and forensics area while also better support current and future research activities.

National and international dimensions

As indicated in the project in the project proposal, and in line with the DSV and SU both national and internationalizations inclinations with respect to promoting state-of-the-art research and education, some of the features in the SSL facility were used to (1) test the C-PEPS implementation of the e-ID (with Sweden and DSV being part of the EU project STORK 2.0), and (2) the results were also part of the joint demo project for Vinnova (September 2012 – March 2013 along with the other units at DSV) for innovative e-services within the eGov lab. There is a preliminary decision that the new project for eGov services and their innovation will be supported by Vinnova on a long term basis where the SSL platform should play a key role in the dealing with security, privacy and interoperability issues.

Moreover, the educational and research affordances of the platform were presented in the key note lecture about education and research e-Infrastructures at the CEE-USER workshop as one of the work packages of the CEENGINE FP7 project on May 22, 2013, in Kiev, Ukraine, with the participation from more than twenty countries in EU, CEE, CA and Caucasus

regions, where there is a great interest to enroll in EU (SE) educational institutions, however due to economic and other social conditions the distance learning mode is the only possibility. The advantages of the SSL platform, in particular the capabilities for digital and cyber forensics labs were also presented to the Faculty of Computer Science and Engineering (Saints Cyril and Methodius University, Skopje, Macedonia) in April, 2013. They are very much interested, among other things, in joint educational programmes and the two institutions (DSV and FINKI) are in the process of signing MoU.

Finally, in the beginning of June 2013 during the two hour open lab demonstration for the representatives from Microsoft, Oracle and IBM, the SSL platform was presented as well. During the same month, it was used as one of the "tools" to evaluate the integrity of the pubic servers that offer e-services of the e-Government of Bhutan with respect to security vulnerabilities The platform could be used in the future for training and education on how to discover and remedy (if any) various kinds of security threats.

All of these activities clearly indicate the real possibilities for using the platform in the international educational context as one of the initial objectives the project in the very near future. Indeed, in many ways the capability and the diversity of the platform with respect to the problems coming from different areas provides unique opportunities for introducing the latest in technology enhanced learning to tackle the interesting and challenging issues and problems in interoperability, e-infra integrity, security, and cyber unwanted behavior and crime detection and prevention.

Information concerning the contact person:

Professor Oliver Popov
E-mail: popov@dsv.su.se
Phone: +46734618868