Addressing resource challenges of educational institutes when teaching cyber security

Masudur Rahman[1], Alexios Mylonas[2], Tomasz Bosakowski[1], Vasilios Katos[2]
[1] Faculty of Computing, Engineering and Science, Staffordshire University, Beaconside, Stafford, ST18 0AD

Email address: masudur.rahman@staffs.ac.uk
[2] Bournemouth University, Poole, BH12 5BB
Email address: amylonas@bournemouth.ac.uk

Abstract

Nowadays cyber security is one of the biggest concerns for governments and the industry due to the increased use of ICT in our day-to-day life, coupled with the emergence of cyber crime. The IT security sector is facing difficulties because of a shortage of people with the necessary skills. Recent reports suggest that this shortage will be significantly higher within the next few years, which may impair the ability of organisations to protect their assets and to ensure the security and privacy of customer's data. In this context, governments from different countries have taken steps to ensure that cyber security skills are developed among students, who aim to work in this sector. However, one of the major difficulties in teaching cyber security is the lack of adequate resources that help students to build their expertise without compromising – knowingly or unknowingly - the security of their organisation or other organisations. This paper examines the need for cyber security skills in the education sector and the challenges faced. It proposes as a solution an IT infrastructure that enables teaching cyber security and digital forensics, which is cost effective, easy to maintain and sustainable.

Keywords:

1.0 Introduction

Cyber security is one of the biggest concerns for IT infrastructures today. All organisations, including private and public companies, are working to have effective mechanisms

2.0 Recent survey about the information security workforce around the world.

The seventh annual global workforce survey revealed a number of interesting facts regarding cyber security issues and available skill sets to tackle those challenges [3]. The survey comprised almost 14000 information security professionals from different sized organisations from around the world. According to this survey, there will be a shortage of 1.5 million information security professionals worldwide by 2020. Because of lack of security professionals, almost half of the participant organisations said they might take up to several days to correct any severe security incident within the organisation. Moreover, almost one fourth of the participants claimed they might take up to three weeks to correct a severe information security incident. According to this survey, the reasons behind the lack of security experts are differ considerably. Almost half of the participants believed the lack of insufficiently qualified personnel was the main reason behind this situation. However, the other half of the participants claimed that their organisation did not have the policy or procedure in place to tackle the security issues. Some other interesting findings from this survey are listed below:

- Vulnerabilities in applications

learning styles and to adopt a suitable teaching style for Cyber Security training in HE institutes

3. Cyber Security in Higher Education: How the Students Learn Better?

In recent years, governments from different countries have taken a number of different steps to encourage educational institutes to promote courses for cyber security and digital forensics to (r)-2(ag)8(e)-22[<4ETd [(d)eng

to an isolated network. There are three servers dedicated to these security provision only. One of these is used for the ethical hacking module for distance learning students via virtual machines (VM) and two others are used for the regular students.

Within this Cyber Security lab, there is one standard computer for per student. This standard image includes some basic software including Microsoft Office. Each of these machines also has the VMWare, which allows individual student to run Virtual Machines within local host machine. There are different Virtual Machine images in VMWare that includes Windows 8 and Kali Linux. Kali Linux are used for Ethical Hacking related modules while the Windows image has been used for Digital Forensics. The Windows image includes EnCase, XRY and other forensic software. Furthermore, these VMs are not stored in local machines but in a server within the faculty. VM's activate by using a start-up script, what runs on the standard lab PC on the time of booting. Students have administrative access for the VM's where they can run different software. As the VM's are not connected to the Internet, the only way of obtaining files from the Internet is to use a memory stick by downloading the required files from the Internet and then connecting the memory stick with the VM. Moreover, there is a shared drive within the VM, which can be used by the students to save their work. Figure 1 shows the lab infrastructure at Staffordshire University for Ethical Hacking and Digital Forensics modules.

Figure 1 – Present setup for the workstations in Cyber Security lab

With this infrastructure, lecturers are facing numerous challenges to deliver the practical sessions. Some of which are explained below:

- Virtual Machines, which loads on lab computers by running a start-up script, does not always run as it supposed to. The reason behind this issue is unknown. Restarting the computer normally runs the script and the VMs start working. But restarting a computer takes valuable time from tutorial session and students fall behind other students when this problem happens.
- Student user accounts are limited for using the malicious tools, even for malware analysis, when they are using the lab computers. This is due to the security settings within the network. This disadvantages the individual when studying the latest security threats.
- VMs are not connected to the Internet; therefore students require downloading tools in the lab PC and when transferring them to the VMs. This process is time consuming and on many occasions complicated.
- There are few target VMs within the network, which has a standard image. However, students do not have the opportunity to work on any network level security issues. They can only target one individual VM for penetration testing or limited ethical hacking.

- The target VMs are stored within one physical server, which does not have any virtual network defined for individual students. These target machines have general vulnerabilities and the IP addresses are manually given to the students where anyone can target any of these VMs. There is no subnetwork or predefined network within this VM environment (Figure 2).

Figure 2: VMware ESXi Based Infrastructure for Target Virtual Machines

- Present IT in

Figure 3: Workstation for the students with Zero Client and Desktop PC sharing same I/O devices by using KVM switch.

Servers will be built on VMware ESXi, where operating systems of the virtual machine will be chosen according to the need. For the Ethical Hacking module, individual students will have their own set of VMs, which they will be accessing by using zero clients. For each student, there will be an allocated virtual network,

Figure 4 –vCloud Director based virtual network for individual student.

7.0 Potential Benefits of using Zero Client - Hypervisor Based Infrastructure.

Successful implementation of such infrastructure will allow students to have greaterflexibility and administrativeaccess rights to explore the vulnerabilities,

have greater control and security over user's data and an effective mechanism in place against the malware infection or other cyber attack

8.0 Plan for future development

As a result of a successful bid for a research grant, necessary funds have been secured to create a model for such infrastructure for teaching and learning Cyber Security. Three zero clients from

9.0 References

1. Geer, Dan. A new Cyber Security Research Agenda, 2011, https://threatpost.com/new-cybersecurity-research-agenda-three-minutes-or-less-110711/75854/
2. 6. Sean Brandes, The newest warfighting domain: Cyberspace. http://www.synesisjournal.com/vol4_g/Brandes_2013_4-990.pdf
3. ISC2. (2015). Global Information Security Workforce Study 2015: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2Global-Information-Security-Workforce-Study-2015.pdf
4. Dale C. Rowe, Barry M. Lunt and Joseph J. Ekstrom; October 2011, The Role of Cyber-Security in Information Technology Education.
5. Martin Mink & Felix C. Freiling, September 2006, Is Attack Better Than Defense? Teaching Information Security the Right Way.
6. Anzai and Simon (1978-1979), The Theory of Learning by Doing
7. Bonwell, J.A. Eison and C.C, 1991, Active Learning: Creating Excitement in Classroom.
8. Kolb's Learning Theory, University of Leicester, http://www2.le.ac.uk/departments/gradschool/training/eresources/teaching/theories/kolb
9. Jan Kallberg & Bhavani Thuraisingham, 2012, Towards Cyber Operations, The New Role of Academic Cyber Security Research and Education.
10. Michael J. Assante and David H. Tobey, January 2011, Enhancing the Cybersecurity Workforce
11. Khaled Salah, Mohammad Hammoud & Sherali Zeadally, NOVEMBER 2014, Teaching Cybersecurity using the Cloud
12. RT Abler, D Contis, J B Grizzard, and Henry L Owen Georgia tech information security center hands-on network security laboratory.