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 Sciences, 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 risks. 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 or to ensure the security and privacy of customers' 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: Cyber Security Education, Cyber Security in HE Institutes, Infrastructure for Cyber Security Training, Virtualization.

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 in place to ensure the security of their infrastructure. Moreover, the utility infrastructures, which depend on IT in many ways, are also vulnerable to different types of cyber attacks. Developments in innovative security technologies are helping to fight against the threats, but lack of skills and expertise are a challenge in the fight against the cyber threats.

Research in Cyber Security is also challenging because of the lack of available resources. Dan Geer, CISO of In-Q-Tel, suggested that solving known problems is not research for cyber security but what the future problems would be – that the research for this sector [1]. Even though this statement is valid for all the researchers, it is critical for Cyber Security research. The US is considering Cyber as war fighting domain along with land, sea, space and air, as are many other nations across the world since this domain can dominate all other war fighting domains [2]. This also shows the importance of research in this area. Thousands of organisations across the world are becoming victims of the cyber attacks, identity theft and industrial espionage; yet critics argue this area lacks in research compared to the others.

Different researchers showed that the lack of resources is one of the key reasons behind many organisations becoming a victim of cyber threats while most of them are struggling to get the right skill sets to protect the organisation from them. With regards to the available infrastructure to train people, who can work in this sector, research has showed significant shortcomings as well. Firstly, not many experts are entering the teaching and training area for cyber security. Secondly, it is complicated to teach cyber security within the organisation's traditional IT infrastructure without risking the available services, as training requires the investigation of different exploitation mechanisms and identifying the potential solutions to secure the network.

This paper has investigated two surveys in relation to the lack of skilled people and adequate infrastructure for cyber security training. Findings of this research indicate the importance of adequate resources for cyber security training in Higher Education and how academia can play significant role to prepare students. This research has furthermore investigated the different styles of learning and the suitable style that can ensure the equal opportunity to learn in cyber security. It is crucial to have effective and efficient resources for all individuals to learn actively. We will propose an IT infrastructure to face these challenges, which could deliver cost effective, sustainable and effective solution for the University to teach Cyber Security and digital forensics.

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 seven 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, malware and mistakes in the configuration are three most important security concerns among the participants or the organisation. These also indicate mostly the lack of security experts within the organisation.
- In answer to the question about security readiness of the organisation compared to the previous three years, more than half of the participants responded that their organisation did not improve their ability in terms of readiness for security incidents, discovering security breach or recovery from potential security breach. This finding also raised the question "why", without having any clear answer to this.
- Even though the investment in security tools has increased compared to recent years, investment in training and education remains the same, which is still a huge challenge for this sector.
- Across the board, salaries for information security professional have been increased dramatically according to skills and expertise. Some experts suggested this as a direct result of skill shortage and an increased demand in this sector.
- Use of cloud computing has increased significantly and more than half of the participants were concerned about data security over the cloud. However, no evidence has been found about the majority of the organisation whether they have arranged any expertise to look after the security issues in cloud or not.

Information provided by this survey clarifies the shortage of and need of security experts, where implementing suitable teaching and learning strategy for security related modules would be able to contribute to deal with this issue worldwide. In the next section, we will be exploring different aspects of teaching, different

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 deal with the growing needs of security experts [4]. Emphasis has been given in all aspects of cyber security training, that includes developing skills for vulnerability analysis, threat analysis, penetration testing, network security, ethical hacking or digital forensics. Each of these topics requires a high degree of practical activities along with the traditional lectures to provide a better learning experience for the individual student. Some academics suggested that a traditional lecture session with a demonstration of an activity could be more effective for students' learning instead of having a traditional lecture session only. For example, while teaching botnet for Cyber Security, creating an infrastructure for a bot network along with an explanation of different components and effectiveness would have a better impact on an individual's learning rather than explaining botnet alone.

A 6th Century BC Chinese philosopher, Lao Tzus said, " If you tell me, I will listen. If you show me, I will see. If you let me experience, I will learn"; which has been proved in many years for students who have different learning styles. Cyber security is an applied field, where practical activities will allow the students to learn theories and to explore the applied techniques that are used by the attackers. Martin and Felix [5] argued that using "offensive techniques" for teaching cyber security in combination with "defensive techniques" might provide the best opportunity for the learners to gain valuable skill sets, which is required for the information security sector. By offensive technique, the author means to give the learner an opportunity to attack target machines by using different tools and techniques. At the same time, the author suggested allowing individuals to implement protective mechanisms to protect the IT infrastructures against the attacks, which are known as defensive technique". Furthermore, educational experts have suggested adopting suitable teaching and learning approaches based on individual needs, which offer positive engagement for individual student.

Anzai and Simon [6] explained that learning takes place when students are actively engaged in "doing things", which is also known as "active learning". Many educational researches have shown that having the opportunity to interact with and experience something increased the effectiveness of teaching and learning sessions to develop the individual's skills [7]. Kolb's famous learning theory also was based on "learner's experience", which is one of the most popular learning theories in the modern era [8]. Having the opportunities to be engaged with the learning process encourages the individual learner to take the responsibility of learning, to think critically to solve a given problem by developing skills.

It is important to engage the individual learner in the learning process and to do so it is also important to have an efficient infrastructure in place, which will not be a risk to the organisation's security. Research in Cyber Security is also important for teaching and learning. A recent survey was conducted on 48 Centres of Academic Excellence (CAE) in U.S.A by focusing on the ability of those research centres to adopt the changes towards cyber operation. Among the other criteria for this research, one of the key criteria was to identify "if there is research on offensive and responding cyber defence, if the research conducted steers towards counter attacks, including psychological and information operations" [9]. In response to this question, only 10.4% centres answered positively. This information could be vital for progressing Cyber Security in Higher Education sector as many experts believe the offensive techniques are the best way of delivering cyber security training and not many institutes have the efficient IT infrastructure to deliver this. However, it is important to note that this particular survey was limited in regards to the research progress, knowledge production and publication records [9]. But still this research can be used as an indication about the situation of many Higher Education Institutes as far as the cyber security courses are concerned.

4.0 Resource issues in HE institutes for Cyber Security training.

The education sector in the UK is facing challenges in regards to the funding and increased pressure of delivering effective outcomes with limited resources. Delivering courses related to cyber security, cyber warfare, ethical hacking, digital forensic or cloud computing security requires a significant amount of resources for effective teaching and learning, which can met the demand of growing needs of security professionals. Many institutes in the UK and other parts of the world have a limited ability for teaching cyber security or researching in this area because of a lack of resources. The common issues HE institutes are facing in this regards include the followings:

Security Issues: Security is one of the main concerns for using attacking tools and techniques within the organisation, which can be classed as malware. Teaching cyber security or penetration testing demands of allowing learners to use tools and techniques which hackers might use to attack a real system. Without knowing these tools and techniques, learners will not be able to develop their skills or expertise, which will be invaluable to work in the IT security industry. However, allowing students to use many of these tools and techniques within the institute's own network can cause serious concerns about the security of the IT infrastructure. It is crucial for the institutes to make a justified balance between providing adequate teaching and learning resources by ensuring the security of the IT infrastructure.

Infrastructure: Expensive IT infrastructure is required in order to create a positive learning environment, where individual learners can explore the opportunities and challenges of IT security and digital forensics. Traditionally, client-server network

has been used within educational institutes with strong access control for student's accounts. However, most HE institutes that teach IT security, have developed an isolated network for their security provision, giving greater control of doing practical activities within the organisation's IT infrastructure. Building an isolated network and relevant infrastructure is expensive considering the cost of the equipment, maintenance, electricity cost etc.

Cloud Computing Environment: Cloud computing is one of the most popular technologies of this century, which is growing fast and strong. Not only the cloud computing becoming popular with the normal users, but it has been used by many organisations because of the efficiency and cost effectiveness. Furthermore, the infrastructure of cloud computing has been used by the attackers for attacking different targets. Learning the Cloud Computing infrastructure, security vulnerabilities associated with this technology and the techniques to make cloud more secure is a vital skill that learners need to gain. Traditionally Cloud Computing infrastructure is complex in nature, as this involves many different networking devices and relevant software. Providing an infrastructure similar to the Cloud Computing environment for learners will offer greater opportunity to understand the security issues and protective mechanisms for the cloud environment. Having virtualisation and Cloud environment in place can also be used for the modules related to forensic investigation in Cloud or Virtualised IT environment.

Lack of Experienced Trainers / Researchers in Higher Education Sector: As mentioned earlier in the survey, Cyber Security is one of those areas, which is offering high salary and excellent career opportunities. On the other hand, working in the education sector is always challenging because of work pressure and comparatively low wages. Working as a lecturer requires many hours of preparation before each session. This profession also requires having additional time for preparing assessments, providing feedback on each assessment and other day-to-day responsibilities. Furthermore, lack of resources to deliver the teaching and learning sessions in an effective way, is a common frustration among many academics, who have industry experience of cyber security and would like to deliver the best for their students. Because of this complex nature of teaching profession, there is a shortage of experts who are passionate about working in the education sector to share their Cyber Security related experiences and expertise to prepare the next generation of workforce for this sector.

The next section will explain the IT infrastructure used by Staffordshire University and limitations of using such infrastructure for Cyber Security provision.

5.0 IT Infrastructure for Teaching Cyber Security or Digital Forensics at Staffordshire University

Staffordshire University does have one dedicated IT lab to be used for cyber security and digital forensics modules. This lab comprises 21 computers connected

to an isolated network. There are three servers, dedicated to the 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 EnCasse, 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 scrip, 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.

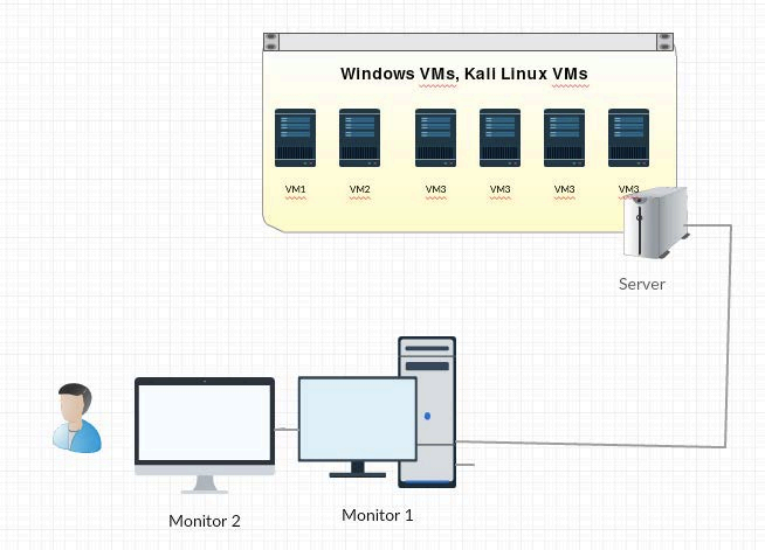

Figure 1 – Present setup for the workstations in Cyber Security lab.

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 the 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 normally given to the students where anyone can target any of these VMs. There is no sub-network or predefined network within this VM environment (Figure 2).

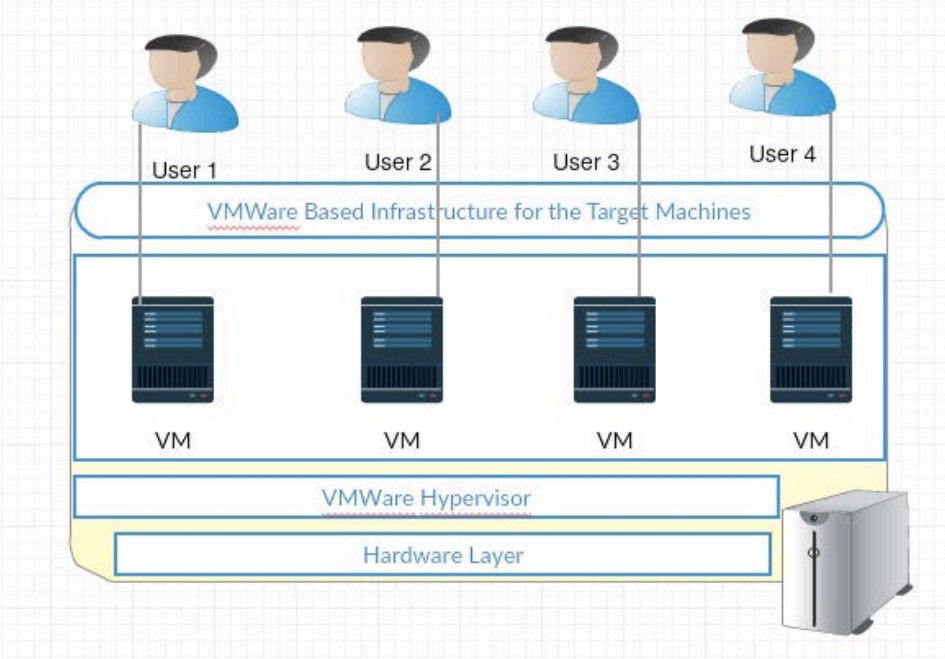

Figure 2: VMware ESXi Based Infrastructure for Target Virtual Machines

- Present IT infrastructure of this lab offers limited access rights for the students as they mainly use a desktop computer mainly, which is connected to the server. Even though the access control rules for the students are quite flexible compared to the other IT labs in the University, still this comes as an obstacle to conduct many different tests.
- Maintenance of lab PCs are time consuming as well such as setting up the lab for the first time. IT support use standard image for lab PCs. However, deploying that image on a computer takes time and it is often difficult to reimage the computer in a timely manner because of the packed scheduled time for classes.
- To use certain Forensic Investigation tools like EnCase, students require high processing power in lab PCs. A significant amount of capital investment is required to develop such a lab, which will only have a few years of lifetime with high electricity cost, maintenance cost and a considerable carbon footprint.

In the next section, we will propose a potential solution to overcome the issues addressed above for teaching cyber security.

6.0 Proposed System – Zero Client and Hypervisor Based IT Infrastructure

To provide a better learning experience for all individuals, we suggest using zero clients in the lab along with existing desktop terminals by using KVM switch. This KVM switch will allow the students to use two computers by sharing the same keyboard, mouse and monitors. Zero clients will be used as a terminal and will be using VMs for the Operating System. Actual data processing will take place within the Virtual Machine. The proposed system will have the zero client – virtual server based network, where students will be accessing their own virtual network within Hypervisor by using zero clients (figure 3).

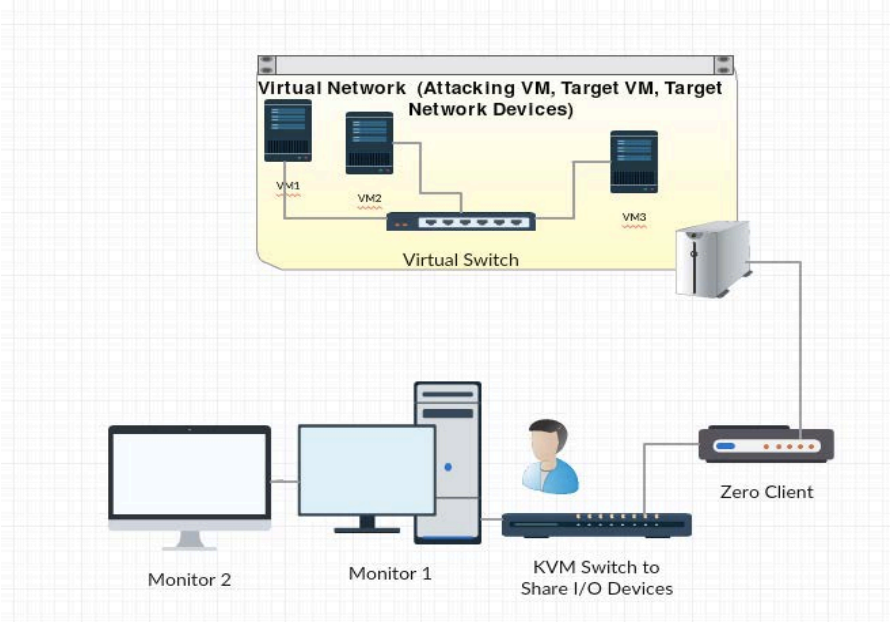

Figure 3: Workstation for the students with Zero Client and Desktop PC, sharing same I/O devices by using KVM switch.

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, which will have an attacking machine, target machines and basic network infrastructure (Figure 4).

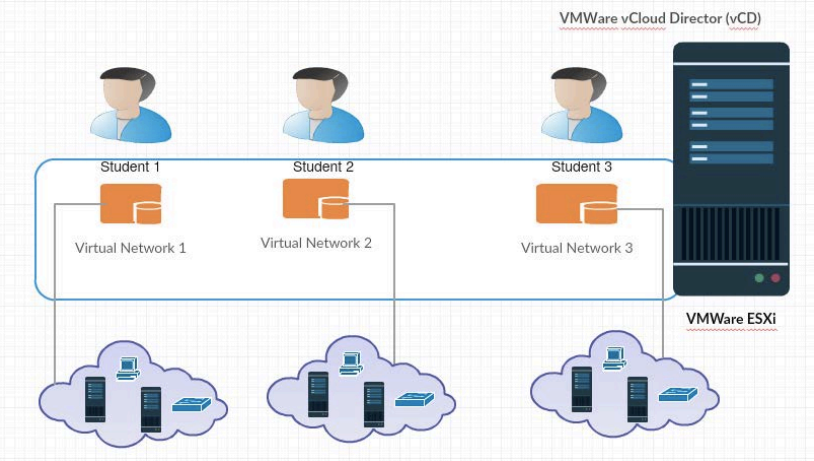

Figure 4 – vCloud Director based virtual network for individual student.

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

Successful implementation of such infrastructure will allow the students to have greater flexibility and administrative access rights to explore the vulnerabilities, ability of using attacking tools and techniques for penetration testing of different types of hosts including network devices. Should a student successfully penetrate the target machine and destroy the VM, an image of that VM can be deployed remotely just within a few minutes without interfering the teaching and learning sessions. This will also allow the individuals to learn how to harden the hosts to protect against different types of attacks and check the effectiveness of implemented security mechanisms. Not only will the Cyber Security modules benefit from such type of network but this can also be used extensively to allow students to participate in Cyber Warfare or Forensic Investigation related modules.

Initial lab setup cost will be reasonable because of less expensive zero clients and KVM switches, what can be setup alongside the existing network. There is evidence that shows different organisations have deployed zero clients and successfully reduced the maintenance cost of IT infrastructure and carbon footprint significantly. The proposed system also will be based on a typical environment for the Cloud Computing infrastructure by using VMWare ESXi and private cloud technology. Different organisations have adopted thin clients and cloud computing based networks in recent years because of the cost effectiveness and ability to offer additional security. In the long term, this project will allow us to explore the opportunities of using thin or zero clients in a wider context within HE institutes considering low carbon footprint, cost and energy efficiency, sustainability and less maintenance cost. Implementing this technology will also allow the institute to

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

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 IT infrastructure for teaching and learning Cyber Security. Three zero clients from different models have been received along with the KVM switches and other required items. One Dell PowerEdge server with VMware ESXi Hypervisor will be used for this research. This equipment will be used to create a model of the proposed network and will be used by the students. Initially this network will be entirely isolated and will not be connected to the Internet. Different learning activities will take place by using this virtual environment after implementing vCloud Director. Developed infrastructure will also be used for the assessment for Ethical Hacking modules where individual students need to submit a portfolio of penetration testing.

It is important to record and analyse the issues as well as the effectiveness of such a network on individuals learning; therefore different evaluation forms will be designed and developed which will be used to record the findings. Students will also be providing their opinion about using such networks for learning the tools and techniques for Cyber Security. Furthermore the electricity consumption will be recorded and compared with the traditional network used by present infrastructure to analyse the potential environmental impact of such infrastructure. It has also been planned to arrange a small scale "hackathon" by using this infrastructure once students are confident about their skills of penetration testing or securing a network. If implemented as planned, a hackathon will be suitable to do "stress testing" for such virtual environment. Such competition will also be used as "offensive techniques" for teaching the Cyber Security. Researchers, including myself, will be using this infrastructure to research the security issues of a private cloud network.

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_G90-95.pdf
3. ISC2. (2015). Global Information Security Workforce Study 2015: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-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. R T Abler, D Contis, J B Grizzard, and Henry L Owen. Georgia tech information security center hands-on network security laboratory.