IJIE (Indonesian Journal of Informatics Education)

Research Paper ISSN: 2549-0389

Leveraging Virtualization Technology in Teaching Cyber Security Courses in Sub-Saharan Africa

Clement Amone Keyamo[1*], Patrick Ogholuwarami Ejeh[2], Daniel Osamwonyi Iyoha[3]

[1*]Department of Cyber Security, Dennis Osadabay University, Nigeria
[2]Department of Computer Science, Dennis Osadabay University, Nigeria
[3] Department of Business Education, Madonna University, Nigeria

Corresponding Email: clement.keyamo@dou.edu.ng

Abstract:

Teaching and learning can be effective and enjoyable if the course is well-packaged and presented. This was the experience of students and teachers participating in our hands-on Cyber Security course. Effective teaching of Cyber Security requires practical demonstration of attack patterns and their related countermeasures. This implies that outstanding and modern laboratories must be in place to teach and learn the necessary principles and practices effectively. Unfortunately, newly established universities in Sub-Saharan Africa need more funds for establishing and maintaining such laboratories. However, several researchers have shown that virtualization technology (VT) can enhance available but limited physical computing laboratories as an alternative to complex physical laboratories with huge procurement costs. This paper proposes an ad hoc and mobile laboratory for teaching practical principles in Cyber Security. The report aims to demonstrate the effectiveness of virtualization technology in teaching Cyber Security in newly established universities in Sub-Saharan Africa with zero to minimal computer laboratory infrastructure.

Keywords: *Cyber Security, Education, Teaching-learning Process, Virtualization Technology, Virtual Machine.*

IJIE (Indonesian Journal of Informatics Education)
Vol 7 Issue 1 2023
DOI: https://doi.org/10.20961/ijie.v7i1.74983
Received: 14/06/23 Accepted: 28/07/23 Online: 7/08/23

Introduction

Teaching and learning in the world today is enhanced by the use of Information Technology (IT). In the case of IT-based programs like Cyber Security, students need to be provided with Laboratories for hands-on practice of principles taught since having well-designed hands-on practical exercises can improve students' understanding and retention of theoretical concepts (James et al, 2020). This creates a challenge since many of these laboratories have huge cost implications (Ogunyemi &Johnston, 2010).

The huge cost of establishing complex IT laboratories is not easily met by governments in Sub Saharan countries like Nigeria. It has been directly observed that newly established universities in sub-Saharan countries like Nigeria have challenges providing advanced laboratories necessary for the teaching of practical-oriented courses. The paucity of funds and the need to efficiently manage what is available to satisfy the diverse pressing needs of the infant institutions are among the reasons for the limitations in laboratory development.

Notwithstanding the limited capacity of laboratories available, teaching and learning must continue in these new institutions. The challenge is to meet the set learning objectives, including the practical objectives set for each course available in such institutions. Several researchers have recommended Visualization Technology (VT) as a panacea to the diverse challenges posed by the lack of or limitations in physical laboratories in universities.

Bližňák et al. (2008) proposed using VT as a practice tool in a parallel programming course, operating systems course, and a training kit in the industry for non-IT-based courses.Misevicïene et al. (2012) studied the use of virtualization technology for teaching and learning theoretical and practical courses at Kaunas University, United States of America. They outlined its advantages, including providing cost-effective on-demand, 24/7 access to teaching and learning aids (including laboratories). Czajkowski (2012) described VT and its application in IT education, concluding that VT increases available time to conduct classes as it makes laboratories available 19 to 24 hours a day, allows the use of obsolete and unsupported software for research, reduces the cost of electricity and Lab spaces, and generally makes lab classes more portable. Perez et al (2016) proposed a tool they called NETinVM based on nested virtualization where several computers and networks exist in a single virtual machine in a nested architecture. NETinVM was then used in a different teaching environment and was analyzed and evaluated to determine its efficacy. They concluded that the tool was useful in performing labs and practical exercises that are unfeasible with available physical systems while having the additional advantage of being feasible.

Also, Fernandez et al (2016) described the implementation of a developed virtualization-based networking lab model. The essence of the developed model was to ameliorate the effort and cost invested in creating physical networked labs. They based their research on the premise that creating virtual labs instead of physical ones contributes to simplifying the lab management tasks and affords more realistic and complex scenarios to be available for students' practice. They then used a survey-based assessment to demonstrate the effectiveness of their model. Eliot et al (2016) proposed a flexible lab environment for teaching cybersecurity courses using VT. The aim was to afford students to learn security principles using an off-campus network lab with a dedicated connection to the Internet. This approach was intended to protect the university network from the risks involved in teaching network security courses where the students need to be handed full control of physical services and equipment. They conclude that their method offers a low-cost alternative to teaching and learning Cyber Security practical courses, especially for the networked system.

Furthermore, Haag et al. (2019) developed an engaging virtual classroom for cybersecurity education. The virtual classroom, which was developed progressively, consists of a Virtual Computer Lab (VCL), made up of two nested software virtualization layers, that can be installed on students' computers; a Distributed Virtual Computer Lab (DVCL) that enables a peer-to-peer link between students via the internet; a central authority(CA) that controls the interworking between nodes in the DVCL; and finally, an intelligent tutoring system (ITS): a computer system used to provide feedback to learners, with little intervention from a human Advisor. They concluded that their virtual classroom allows students to conduct educational activities just as in an on-campus classroom.

In addition, James et al. (2020) proposed a VT hands-on learning approach for teaching Cyber Security courses. They described details of their Raspberry Pi-based lab architecture and provided example lab tasks that can be carried out with their architecture. They assessed their method using participating teachers' and students' responses and comparisons with previous courses taken without their solution. They conclude that their approach affords improved performance of students. Usman (2021) highlighted the benefits of using VT in teaching Cyber Security courses and described examples of practice environments for the practical labs. The benefits, as itemized by Usman (2021), include: Students could create more virtual hosts than the number of physical computers available in the laboratory; they can create complex scenarios involving several hosts; No restrictions on the number of network interfaces in each host; they have full control as they can act as the administrators of their virtual hosts; they can reproduce the experiments at home.

Approaches that utilize VT to teach Cyber Security courses have been classified into two broad areas by James et al. (2020). The classification better assist in identifying the weaknesses in the different approaches. The first group is those that base their work on virtual labs that run on individual machines-either personal PC of students or PC owned by concerned universities. The second group is those who base their system on virtual host infrastructure, that is, cases where universities make use of online hosted labs. A third group is added here. This group includes approaches that involve institutions purchasing relatively cheap computer systems for students and installing VT software to separate systems used for teaching Cyber Security hands-on from existing institutional infrastructure, as in the case of James et al. (2020).

For the first group, the challenge is the availability and reliability of the students' systems used. Also, where the students' systems are connected to the university infrastructure via the Internet, security issues arise since the students need to be given some administrative privileges. Furthermore, system maintenance costs and security issues are some limitations when university PCs are involved.

For the second group, identified limitations by James et al (2020) include high cost and maintenance issues that are beyond the reach of poorly funded institutions. This also mirrors the case of the third group which relatively is considered cheaper by James et al (2020), the creators of the approach.

In this research work, we consider the case where the university is a new one and challenged in availability of funds, with computer laboratories infrastructure at the range of between zero to minimal. This presents a problem of how to teach courses in cyber security with practical modules without having to wait till such a time as basic equipment is made available. Previous Approaches based on using students' PC cannot be directly applied in our case without some major modifications, as they are often founded on the premise of supporting IT infrastructure with reliable connectivity. There is a need to experiment with more basic systems that can meet the needs of institutions with zero and above IT lab environments.

Here, we propose an ad hoc and mobile lab for teaching practical principles in Cyber Security and aim to demonstrate the effectiveness of using VT in teaching Cyber Security in newly established universities in Sub-Saharan Africa having zero to minimal computer lab infrastructure.

Research Methods

Here, we apply major modifications to previous approaches that use student PC for hands-on practice as classified by James et al (2020). We introduce a distinct but simple tool that is not used in previous works: 2014 32' Samsung LED Television-set volunteered by one of the teachers. The television is connected to a laptop using a VGA to HDMI adaptor. The purpose of introducing the television set is to have a basic means of demonstrating hands-on practical skills to the students at little or no cost. Also, nine laptop computers of diverse brands were volunteered by 9 of the 39 students that enrolled in the course selected for the demonstration. Unlike some previous works that used students' systems for their demonstrations as classified by James et al. (2020), the volunteered laptops have no physical connection with each other or with the school's IT infrastructure. Each of the nine laptops, plus that of the instructor, and their respective specification is shown in Table 1.

Table 1. Volunteered PC Specifications

SN	PC Brand	Specification
1	HP (instructor's)	Intel(R)Core (TM)i3-4000MCPU@2.40GHz2.40GHz,4.00GBRAM,64-bitoperatingsystem,x64-basedprocessor
2	DELL	Intel(R)Core (TM)i5-4300MCPU@2.60GHz2.60GHz8.00GBRAM,64-bitOperatingsystem,x64-basedprocessor
3	DELL	Intel(R)Pentium(R)CPU2117U@1.80GHz1.8GHz,4.00GBRAM64-bitOperatingsystem,x64-basedprocessor
4	HP	
5		Intel(R)core (TM)i5-4310UCPU@2.00GHz2.60GHz4.00GBRAM,64-bitoperatingsystem,x64-basedprocessor.
6	HP	AMDA6-7310APUwithAMDRadeonR4Graphics@2.00GHz2.00GHz,6.00GBRAM,64-bitOperatingsystem,x64-basedprocessor
7	HP	Intel(R) Core (TM) i5-7300U CPU @ 2.60GHz 2.71 GHz 8.00GB RAM
8	HP	64-bit operating system, x64-based processor
9	HP	Intel® Core™ i7-8750H CPU @ 2.20GHz,16.0 GB RAM,64-bit operating system, x64-based processor
20	DELL	Intel(R) Core (TM)i5-2520M CPU @ 2.50GHz 2.50 Ghz

A 'virtual lab' made up of free virtualization software and Virtual Machines, in this case, a VMware player 17 and two virtual machines: Kali Linux and Windows XP SP2, is installed in each system. The virtual machines are connected in a local network using the host-only setting selection. Figure 1 illustrates the 'virtual Laboratory' installed in the computers. The details and the setting for each virtual machine is rendered in Figure 2.

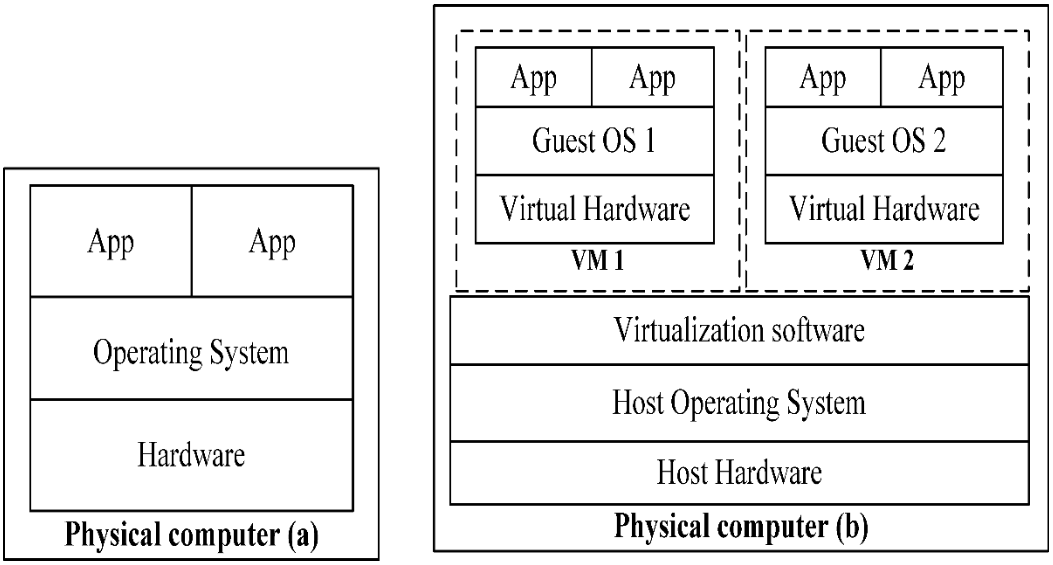


Figure 1. (a) systems without virtualization (b) systems with lab installed (image source: Miseviciene et al (2012)

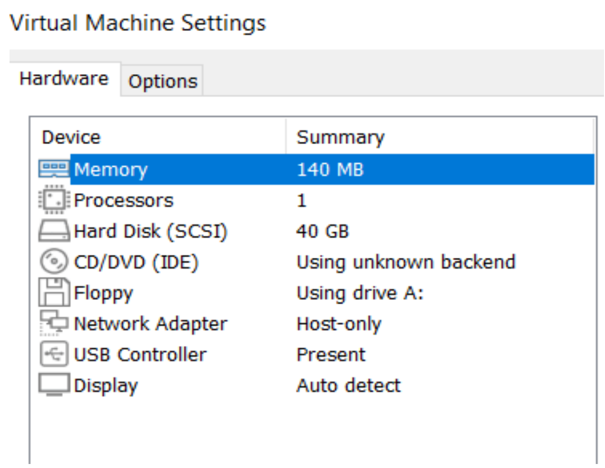
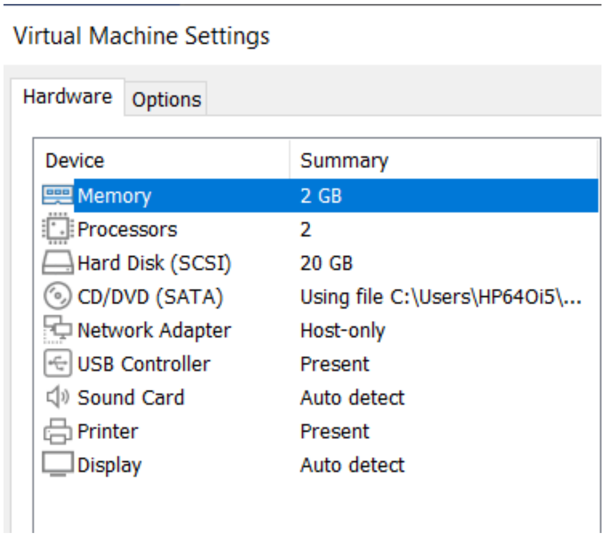
Windows XP SP2 virtual machine settings (VM1)	Kali Linux vitual machine settings (VM2)
 Virtual Machine Settings Hardware Options Device — Summary Memory — 140 MB Processors — 1 Hard Disk (SCSI) — 40 GB CD/DVD (IDE) — Using unknown backend Floppy — Using drive A: Network Adapter — Host-only USB Controller — Present Display — Auto detect	 Virtual Machine Settings Hardware Options Device — Summary Memory — 2 GB Processors — 2 Hard Disk (SCSI) — 20 GB CD/DVD (SATA) — Using file C:\Users\HP64Oi5\... Network Adapter — Host-only USB Controller — Present Sound Card — Auto detect Printer — Present Display — Auto detect

Figure 2. Virtual machines settings

For the demonstration proper, we select the Cyber course: CYB 213 (Threats, Attacks and Countermeasures, being taught to first semester 200-level Cyber security undergraduates in our institution.) The course is an introductory course to Ethical Hacking and covers the fundamental topics including concepts definitions, basics of networking, Ethical hacking Methodology, Hacking tools and software defense tools and software, and so on. The Denial of Service (DoS) Attacks is selected as a significant Cyber-attack pattern to illustrate hacking principles throughout the course.

The presentation of the course is straightforward. We divide lecture periods of 2 hours into 2 sessions of 1 hour each.In the first session, We teach the theoretical concepts as highlighted above,while in the second session, we carry out guided hands-on practical work using the television connected to the instructor’s PC to display the procedure to the students. Each student is allowed to take turns in the available computers in an approximate 4 students to 1 PC-rotation order. The course content, objectives of the guided lab (Denial of Service Lab only) and the step-by-step procedure are listed in subsections 2.1, 2.2, and 2.3 respectively.

Finally, the students are assessed at the end of the course. The assessment comprises written and hands-on examinations. The hands-on assessment was structured in such a way that the students must meet the full objectives of the lab to get full marks. In the case of the DoS hands-on, the grading of the lab assessment was carried out in a progressive manner in line with the objectives of the lab. This is achieved thus: Completing steps 1 and 2 in the guided lab itemized in section 2.3 gives a student 30 marks (that is 15 marks each), completing steps 3 and 4 gives 20 marks (that is ten marks each), steps 5 and 6 gives 20 marks (10 marks each), and steps 7 gives ten marks. This gives 100 marks to a student that successfully completes all steps in section 2.3 during the assessment. The general weighting for the course assessment is 30% for Continuous Assessment (CA), where the hands-on carries a huge chunk and 70% for the final written exam.

Course Content

Table 2 shows the general course content taught for the course

Table 2. Course content

Week	Hours	Topics to cover
1	2	Introduction of Concepts (network and host security concepts and mechanisms, vulnerabilities, Threats, Risks, Damage, Exploits, Countermeasures, etc.)
2	2	Introduction to Hacking (: footprinting, Enumeration, Reconnaissance, Fingerprinting, Scanning, etc
3	2	Hacking: software tools and Exploits
4	2	Hacking: software tools and countermeasures
5	2	Denial of Service Attacks: Concepts and Principles
6	2	Denial of Service Attacks; Exploits and software tools
7	2	Denial of Service Attacks; Countermeasures and software tools
8	2	Mid-semester Assessment (CA1)
9	2	Man in the middle attacks: concepts and principles
10	2	Man in the middle attacks: Exploits and Software Tools
11	2	Man in the middle attacks: Countermeasures and Software Tools
12	2	Introduction to Malware: Attacks and Countermeasures
13	2	Revision
14	2	Final assessment

DoS Course Content

DoS course content taught for the demonstration is listed below:

- Denial of Service Attacks: Concepts and Principles
- Categories of DoS Attacks: DOS and Distributed DoS Attack
- Variants of DoS/DDoS Attacks: Ping of Death Attack (also called ICMP flood attack), Smurf Attack, and SYN Attack (also TCP flooding)
- DoS/DDoS Attack Tools
- DoS/DDoS Countermeasures

Lab Objectives

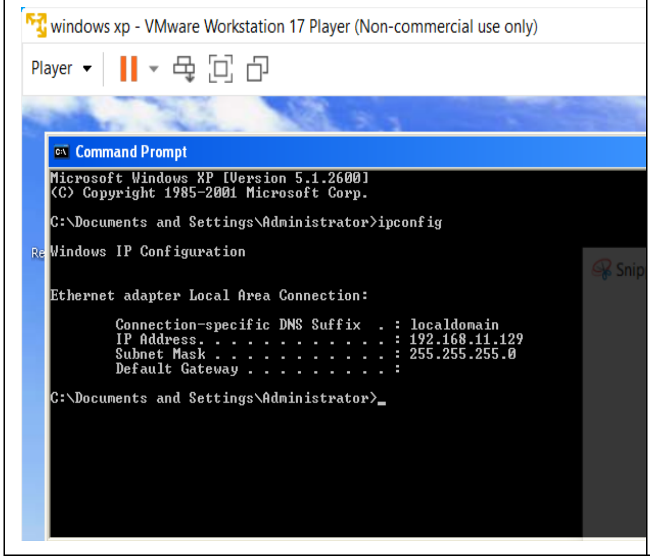
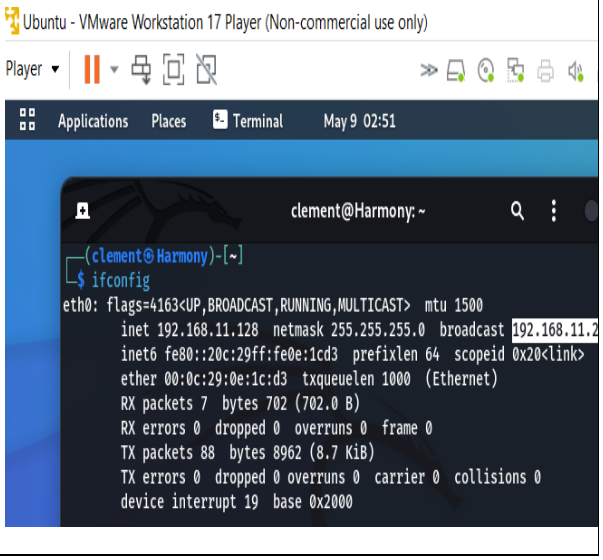
The objectives for the guided lab for the demonstrated DoS attack were listed as:

- Students should be able to set up Target and Attack machines on their PC using Virtualization software.
- Establish a Local network between the virtual machines installed on it.
- Check for connectivity between the attack and target machines using the ping utility tool

- Confirm that the firewall is active or inactive in the target machine
- Enable and disable the firewall on the target machine (the objective is to know how and why, and it is carried out from the target itself)
- Carry out port scanning using Nmap or HPing3 tools
- Use the Hping3 tool to carry out DoS Attacks as described in the theoretical part of the course
- Verify the effectiveness of the attack by using the WXP system Performance Monitoring Utility
- Write a report on the Lab practice.

Procedure for Guided Lab

We followed the under-listed steps to demonstrate the DoS attack. The lab practice was structured to help students better understand the concepts learned in the theory part of the course, including techniques. Hackers use to carry out DoS attacks so they can better defend against them.

Windows XP(VM1)	Kali Linux (VM2)
	

windows xp - VMware Workstation 17 Player (Non-commercial use only)
Player
Command Prompt

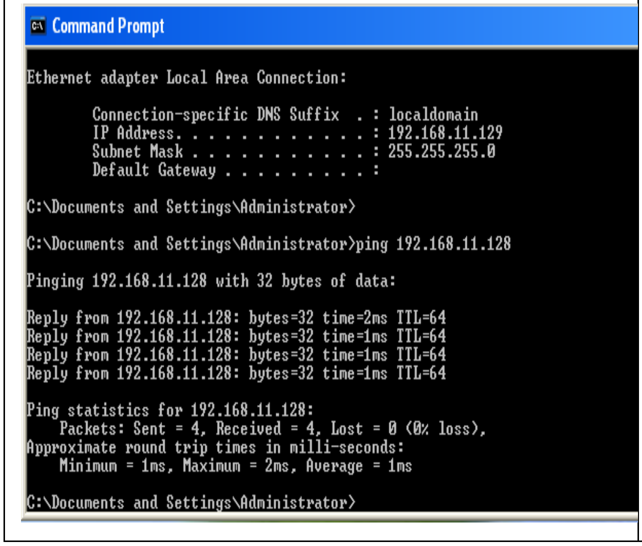
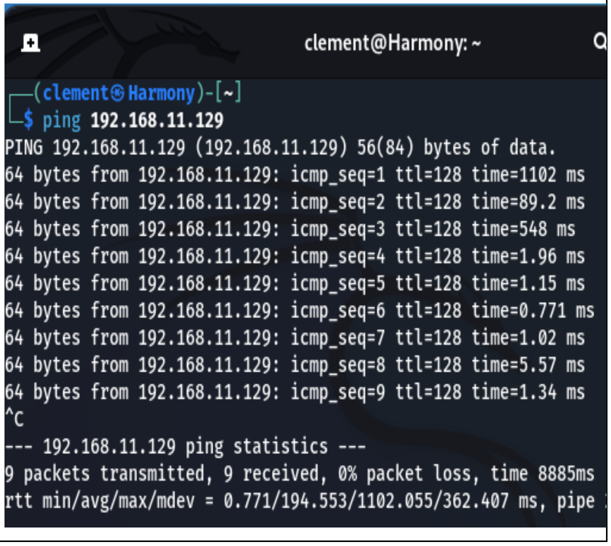
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.11.129
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\Administrator>_
```

Ubuntu - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Terminal
May 9 02:51
clement@Harmony: ~

```
┌──(clement㉿Harmony)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.11.128  netmask 255.255.255.0  broadcast 192.168.11.2
        inet6 fe80::20c:29ff:fe0e:1cd3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:0e:1c:d3  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 702 (702.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 88  bytes 8962 (8.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000
```

Figure 3. Determining the IP address of the VMs

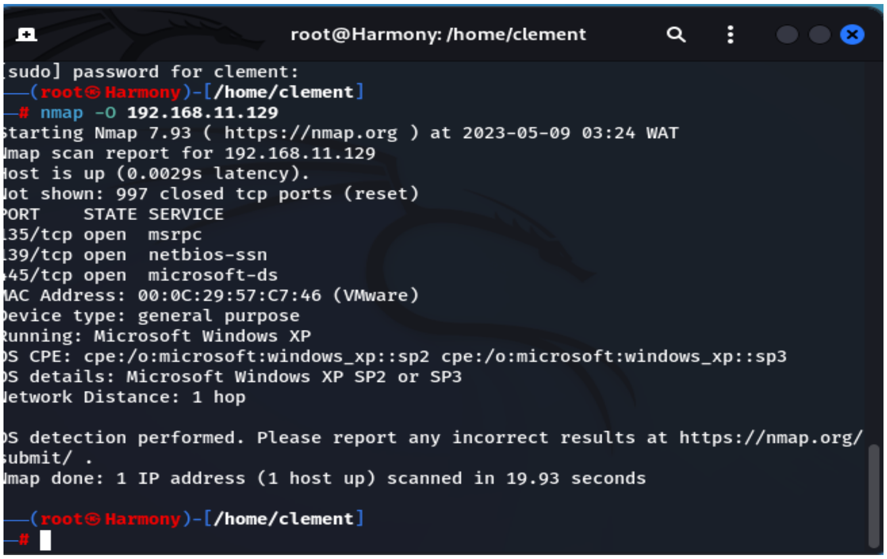
- Set up two Visual Machines on your system. Kali Linux and Windows XP (WXP).
- Configure the machines as shown in Figure 2 for Kali and WXP, respectively
- Open each device on separate windows and get the IP address by typing the command ipconfig for WXP and ifconfig for Kali. This is shown in Figure 3.
- Ping each machine from the command line and terminal using ping <IP address> to ensure they are connected and can communicate with each other: Figure 4 illustrates the step.
- Turn on and off the WXP firewall and selected ports and see the effect on pinging the target machine
- Scan the target machine (WXP) using Nmap. Carry out OS enumeration to detect open ports/ other vulnerabilities. Figure 5 illustrates this step.
- To be able to monitor the effectiveness of the DoS attack, turn on the system performance monitoring utility in the target machine. The performance of the system before the attack is noted in Figure 6.

Windows XP(VM1) :pinging Kali	Kali Linux (VM2):pinging WXP
	

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.11.129
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\Administrator>

C:\Documents and Settings\Administrator>ping 192.168.11.128

Pinging 192.168.11.128 with 32 bytes of data:

Reply from 192.168.11.128: bytes=32 time=2ms TTL=64
Reply from 192.168.11.128: bytes=32 time=1ms TTL=64
Reply from 192.168.11.128: bytes=32 time=1ms TTL=64
Reply from 192.168.11.128: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.11.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Documents and Settings\Administrator>
```

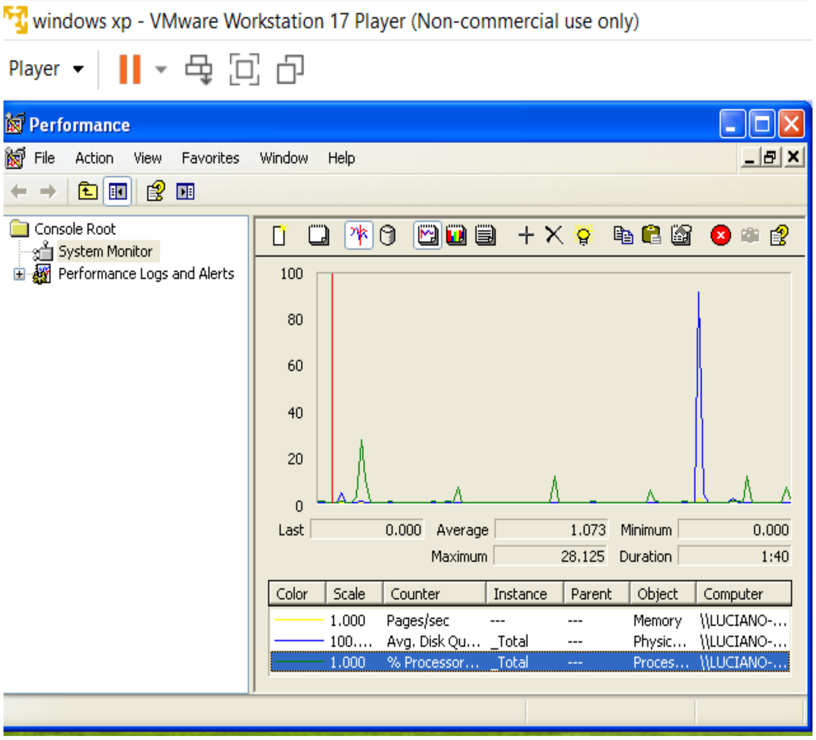
```
┌──(clement㉿Harmony)-[~]
└─$ ping 192.168.11.129
PING 192.168.11.129 (192.168.11.129) 56(84) bytes of data.
64 bytes from 192.168.11.129: icmp_seq=1 ttl=128 time=1102 ms
64 bytes from 192.168.11.129: icmp_seq=2 ttl=128 time=89.2 ms
64 bytes from 192.168.11.129: icmp_seq=3 ttl=128 time=548 ms
64 bytes from 192.168.11.129: icmp_seq=4 ttl=128 time=1.96 ms
64 bytes from 192.168.11.129: icmp_seq=5 ttl=128 time=1.15 ms
64 bytes from 192.168.11.129: icmp_seq=6 ttl=128 time=0.771 ms
64 bytes from 192.168.11.129: icmp_seq=7 ttl=128 time=1.02 ms
64 bytes from 192.168.11.129: icmp_seq=8 ttl=128 time=5.57 ms
64 bytes from 192.168.11.129: icmp_seq=9 ttl=128 time=1.34 ms
^C
--- 192.168.11.129 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8885ms
rtt min/avg/max/mdev = 0.771/194.553/1102.055/362.407 ms, pipe
```

Figure 4. Determining the connection of the VMs



```
[sudo] password for clement:
┌──(root㉿Harmony)-[/home/clement]
└─# nmap -O 192.168.11.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 03:24 WAT
Nmap scan report for 192.168.11.129
Host is up (0.0029s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:57:C7:46 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.93 seconds

┌──(root㉿Harmony)-[/home/clement]
└─#
```

Figure 5. Scanning the target VM using Nmap

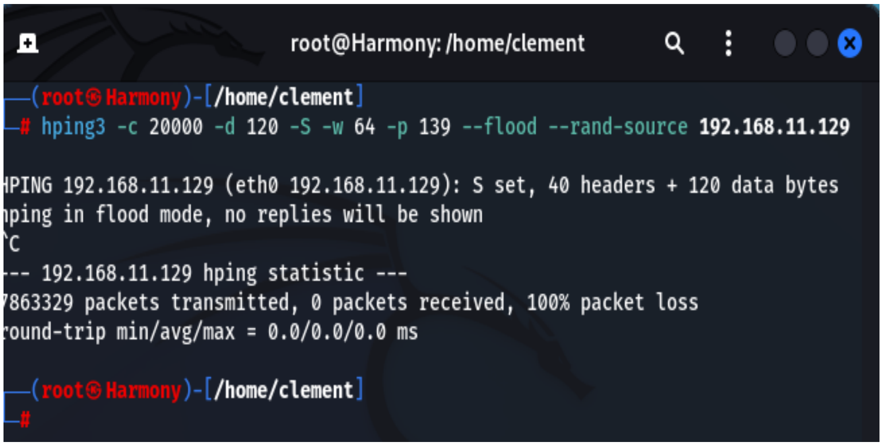

windows xp - VMware Workstation 17 Player (Non-commercial use only)
Player
Performance
File Action View Favorites Window Help
Console Root
System Monitor
Performance Logs and Alerts
100
80
60
40
20
0

Last	0.000	Average	1.073	Minimum	0.000
		Maximum	28.125	Duration	1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
🟨	1.000	Pages/sec	---	---	Memory	\\LUCIANO-...
🟦	100....	Avg. Disk Qu...	_Total	---	Physic...	\\LUCIANO-...
🟩	1.000	% Processor...	_Total	---	Proces...	\\LUCIANO-...

Figure 6. System performance of WXP before an attack

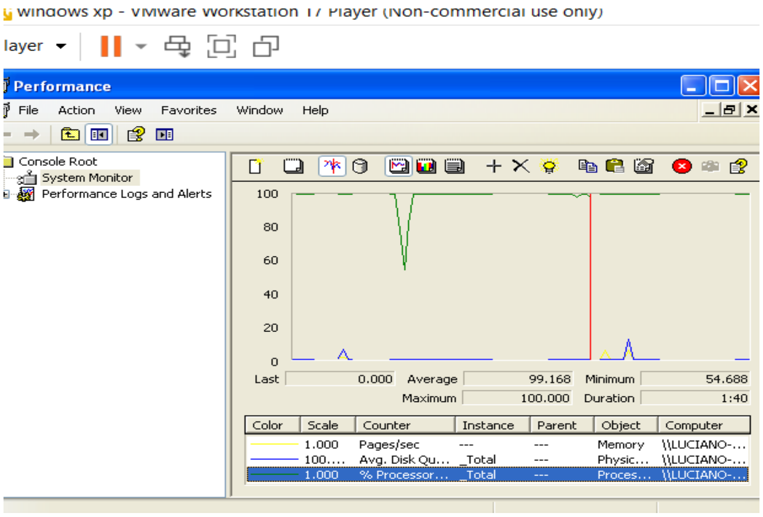
- Next, attack the target machine, using the free Hping3 tool taking advantage of the open port 139 and randomizing source IP to evade detection. Flood the target with 20,000 packets, as shown in Figure 7.



```
┌──(root㉿Harmony)-[/home/clement]
└─# hping3 -c 20000 -d 120 -S -w 64 -p 139 --flood --rand-source 192.168.11.129

HPING 192.168.11.129 (eth0 192.168.11.129): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.11.129 hping statistic ---
7863329 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(root㉿Harmony)-[/home/clement]
└─#
```

Figure 7. DoS attack on target VM

- Confirm the effectiveness of the attack using the system performance monitoring utility of WXP. The performance utility shows a spike in CPU usage to an average of 99% as against 28% before the attack. This shows the attack is effective. Figure 8 illustrates this.


windows xp - VMware Workstation 17 Player (Non-commercial use only)
layer
Performance
File
Action
View
Favorites
Window
Help
Console Root
System Monitor
Performance Logs and Alerts
100
80
60
40
20
0

Last 0.000 Average 99.168 Minimum 54.688
Maximum 100.000 Duration 1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
🟨	1.000	Pages/sec	---	---	Memory	\\LUCIANO-...
🟦	100....	Avg. Disk Qu...	_Total	---	Physic...	\\LUCIANO-...
🟩	1.000	% Processor...	_Total	---	Proces...	\\LUCIANO-...

Figure 8. System performance of WXP after attack

Results and Analysis

Here we combine feedback from students' performance in the term examinations and participating students' opinions of the demonstration to determine the effectiveness of the approach (James et al, 2020) . In our case, we do not have records of students who took this course previously as this is the first set of students enrolled in the university. instead, we use records from previous courses taken by the same students in the previous two consecutive semesters and records of two related courses taken by the same set of students at the current level to determine the effectiveness of our method.

Result from Assessment

Table 3 displays the performance of the same students in the current course, CYB213, compared with their performances in previous introductory courses in Cyber Security. The earlier courses had zero hands-on sessions.

Table 3. Student performance compared over three semesters

Score range	CYB213 (3rd semester)	CYB121 (2nd semester)	CYB111 (1st semester)
0--39 (fail)	10.3%	20%	30.9%
40-49 (Fair)	30.8%	28.9%	30.9%
50---59(Good)	10.3%	17.8%	16.7%
60--69(Very Good)	10.3%	15.6%	11.9%
70--100 (excellent)	38.5%	17.8%g	9.5%

In addition, Table 4 compares the students' performance in related courses in the same semester. The other two courses had zero hands-on sessions.

Table 4. Student performance in CYB213 compared with their performance in two related courses in the same semester

Score range	CYB213	CYB 212	CYB 211
0--39 (fail)	10.3%	28.6	17.9
40-49 (Fair)	30.8%	28.6	28.9
50---59(Good)	10.3%	15.6	10.3

61--69(Very Good)	10.3%	10.4	15.4
70--100 (excellent)	38.5%	15.6	28.9

Analysis of Results

In the case of the progression of the students from earlier semesters to the current semester where the hands-on exercises are implemented, there is observable improvement in the performance of the students, as can be seen from Table 3. In studying the raw scores for the students for all three semesters, it was observed that a few students progressed from the failure range (0-39%), where they had remained in the two previous semesters, to a lower fair coverage (40-49%). Also, those who previously were in the fair, good (50-59%), and very good (60-69%) ranges in both previous semesters had better performance in the third-semester course where the hands-on was used for teaching. Overall, there was an upward migration of students in terms of performance in the hands-on course as against previous semester courses where no hands-on exercises took place. However, it was noted that some students remained stagnant in all three semesters. For those that remained in the failure group in all three semesters it was observed by the instructors to be students who consistently missed classes.

In the second case, where the performance of the students that took the hands-on supported course was compared with their performance in courses taken at the same level but had no practical augmentation, it was observed that the students performed better with the course with the hands-on than with those without hands-on. Like with the cases when the comparison was with the courses taken in the earlier semester that had no hands-on augmentation, there was marked upward migration in the performance of students as shown in Table 4.

We observed that the improvement in performance was because of better interest in the course and better comprehension by students as in the case of James et al. (2020) due to the approach implemented. This was confirmed by the students' responses to questions asked in interviews carried out to determine their satisfaction levels with the approach. The responses of students are considered in the next section.

Feedback from Students

Participating students were interviewed to elicit their views on the effectiveness of the demonstration. Figure 8 displays the questions asked and the response from one student typical to most of the students.

In response to questions 1 and 2, many students interviewed praised the effort of the instructors in putting together the practice sessions. Most of the students claimed that the hands-on lab helped them better understand the principles taught in the theoretical part of the course and that the manner of presenting the course made the teaching an enjoyable experience. This, they claimed, made them focus better while the demonstration continued.

On the challenges encountered during the course, as solicited from question 3, students mostly complained that the approach was rigorous and slow. The limited number of PC for the demonstration was the major contributing reason for the above challenge. Also, during the lab assessment, the students had to spend less than ten minutes each to complete their assessment. In some cases, a lack of familiarity with the assigned system hindered some students' performance. Power and poor power fittings also affected the efficiency of the demonstration. In some lecture periods, classes had to be shifted to a more conducive environment due to poor facilities. This greatly reduced the time-on system for many students.

One notable response by a student to question 3 was that 'Practical for now is still on the superficial level and could use more time and dedication. It's like learning a new programming language, and it takes more self-practice than class-based work.' We believe the student was concerned about the limited time frame for the practice sessions as a result of the limited PCs and time for each student to take turns. Some of the students collaborated with this as they complained of their lack of satisfaction in watching others use the system in most of the practice time than they had time to use the system themselves. Again, this is not new, as researchers have identified this challenge as common with using student systems for lab exercises.

On ways to improve the approach as solicited from question 4, most of the students wanted the university to provide the PCs. We thought this was due to the challenge of sharing available systems rather than the problem of lack of familiarity with borrowed systems since none of the students directly hinted at a lack of understanding being an issue. One student suggests that more time be given to each student for practice and that a projector be provided in place of the television. This we believe is due to the limited size of the available 32-inch TV used for the demonstration. We observed that students had to sit very close to the TV set for a better view of the procedure. This caused some crowding in areas of the class, resulting in further discomfort for the students.

Table 8. Typical Student interview response

SN	Question	Free flow response (not yes and no, please)
1	What's your general opinion of the Practical in CYB213?	In my own opinion, CYB213 was the only course I understood at least 99% of this semester.
2	Do you think it assisted you in understanding the course better? No, yes, and no response, please. State your reasons as briefly as you can.	Of course, yes, the practical helped a lot in understanding the course. If I were to be asked, I feel Cyber security as a whole is a practical course. It's not something we come to and always take notes on because we're dealing with real-world activities, unlike other classes.
3	Identify the challenges you personally encountered with the practical	Personal challenges during the course were mainly the availability of good and enough laptops. I believe this should be a general problem as well because this made assimilation and the classes as well very slow. Also, it is better to operate it myself than look at someone else's laptop. That way, I can get to identify some problems while I do it than watching someone else do it and assume I can perform it myself.
4	Suggest ways you think we can improve the practical session	The ways I can identify is to improve facilities for practical sessions. Saying this I don't mean just laptops, it dies down to the hall we make use of too, it is ideal we have at least a big computer lab with constant electricity, powerful laptops and if possible, a big screen where the lecturer can project his own system. This would help faster learning for those who don't have their laptops and those who have theirs but aren't following due to laptop issues or related problems.
5	Do you think it is possible to teach practical this way when facilities are not available?	It is possible for practical to be taught this way without facilities, but it's not close to being the best, looking at what I have listed above. So, it could be a lot better and help in faster assimilation when good enough facilities are provided.

Finally, the majority seemed undecided on whether it was possible to teach a practical approach if no Facility was made available. Some students were happy for what was available but wanted something better. One student put it this way, 'when facilities are not available, it would be slightly difficult' another student thought that 'it could make the institution not to get better infrastructure...'and did not want that to happen. One said, 'it could only be acceptable if all students had their own PC' One student was philosophical in his response, claiming that half dough (of bread) is better than none; it's better to have this kind of hands-on practice, than nothing at all. In fact, most of the student requested that more of their courses be designed and presented in a similar manner, despite the challenges encountered during the hands-on sessions.

We suspect that the exposure of the approach gave the students ideas of the immense benefits of hands-on in learning and they simply desired more. A student's response to question 3 emphasizes this point, '...the practical helped a lot in understanding the course. If I were to be asked, I feel Cyber security is a practical course, it's not something we come and always take notes because we're dealing with real world activities unlike other courses.

Conclusion

In this paper, our aim was to demonstrate the effectiveness of using VT in situations where new institutions, specifically found in sub Saharan Africa, had zero or minimal IT lab infrastructure available for teaching IT-based courses such as Cyber Security courses. Previous works where mostly based on the availability of Virtual Host infrastructure , availability of institutional PCs with supporting IT infrastructure or financial capacity to implement some novel solutions to a discovered challenge. We proposed an ad hoc, mobile VT lab, introducing a simple but important modification to approaches based on the use of student PC.

We evaluated the the effectiveness of our approach by combining two yardsticks: 1. comparing the results of assessments on students who participated in our demonstration with results they obtained in similar course they took that did not follow the approach and 2. the response of participating students to questions in interviews designed to solicit their level of satisfaction with our approach.

Our results show that students who took part in our approach had better performance in our course than in other courses, that lacked hands-on augmentations, that they also participated in. There was significant upward movement of students from lower score ranges to higher ones. As much as 10% of students who had previously remained in the failed range migrated to the lower pass levels. Similarly, about 10% of students where observed to have moved from the good and very good score range of 50-59% and 60-69%, in previous semesters and in courses that had no hands-on, to the excellent range of 70%-100% in the course where our approach was implemented.

The improved performance in assessments and the high levels of satisfaction of the students that participated in our course, suggests that the students had better understanding and where better focused and interested as against courses that did not have hands-on augmentations. We conclude here that the significant improvement in performance by students in our course over related courses they took that had no hands-on practices, was a confirmation that, " having well designed hands-on practical experiences improves understanding and retention of theoretical content." This is an indication that our approach is effective and that using VT technology in our described setting is not only feasible but an enjoyable experience for teachers and students.

References

Ahmed, B. T. (2020). Virtualization Mechanisms and Tools: A Comprehensive Survey. Use retrieves from: Bakhan Tofiq Ahmed / *International Journal of Computer Science Engineering* (IJCSE), 9(4), pp. 346-255. https://doi.org/10.21817/ijcsenet/2020/v9i4/200904022

BouSaba, C., Burton, L., & Fatehi, F. (2010). Using virtualization technology to improve education. In EDULEARN10 Proceedings (pp. 201-206). IATED.

Czajkowski, A.(2012) Virtualization as a Support Tool for Teaching of The Information Technologies at Higher Education Level.

Deng, Y., Lu, D., Chung, C. J., Huang, D., & Zeng, Z. (2018, October). Personalized learning in a virtual hands-on lab platform for computer science education. In 2018 IEEE frontiers in education conference (FIE) (pp. 1-8). IEEE. https://doi.org/10.1109/FIE.2018.8659291

Wu, D., Fulmer, J., & Johnson, S. (2014). Teaching information security with virtual laboratories. *Innovative Practices in Teaching Information Sciences and Technology: Experience Reports and Reflections*, 179-192 https://doi.org/10.1007/978-3-319-03656-4

Eliot, N., Kendall, D., & Brockway, M. (2018). A flexible laboratory environment supporting honeypot deployment for teaching real-world cybersecurity skills. IEEE Access, 6, 34884-34895. https://doi.org/10.1109/ACCESS.2018.2850839

Fernández, D., Ruiz, F. J., Bellido, L., Pastor, E., Llorente, O. W., & Mateos, V. (2016). Enhancing learning experience in computer networking through a virtualization-based laboratory model. *The International Journal of Engineering Education, 32*(6), 2569-2584. ISSN-e 0949-149X

García, J., & Entrialgo, J. (2015). Using computer virtualization and software tools to implement a low cost laboratory for the teaching of storage area networks. *Computer applications in engineering education*, *23*(5), 715-723. https://doi.org/10.1002/cae.21644

Haag, J., Vranken, H., & van Eekelen, M. (2019). A virtual classroom for cybersecurity education. Transactions on

Edutainment XV, 173-208. https://doi.org/10.1007/978-3-662-59351-6_13

James, P., Powell, L., O'reilly, L., & Moller, F. (2020, June). Hands-on security testing in a university lab environment. In Proceedings of the 2020 ACM Conference on Innovation and Technology in Computer Science Education (pp. 68-74). https://doi.org/10.1145/3341525.3387366

Klement, M., & Gregar, J. (2016). Options of Integration Virtualization Technologies into Education. In 3rd International Multidisciplinary Scientific Conference on Social Sciences and Arts SGEM 2016 (pp. 713-722).

Lemus-Zúñiga, L. G., Benlloch-Dualde, J. V., Montañana, J. M., Pla, M. A. M., & Pons, J. (2015, June). Teaching computer networks using virtual machines. In 2015 International Conference on Information Technology Based Higher Education and Training (ITHET) (pp. 1-6). IEEE.

Miseviciene, R., Ambraziene, D., Tuminauskas, R., & Pazereckas, N. (2012). Educational infrastructure using virtualization technologies: Experience at kaunas university of technology. *Informatics in Education, 11*(2), 227-240. https://doi.org/10.15388/infedu.2012.12

Ogunyemi, A., & Johnston, K. (2010). The use of virtual machines to support hands-on learning experiences in undergraduate systems-oriented courses. In Proceedings of the 4th International Conference on Dynamic Informatics.

Pérez, C., Orduña, J. M., & Soriano, F. R. (2016). A Nested Virtualization Tool for Information Technology Practical Education. *SpringerPlus, 5,* 1-9. https://doi.org/10.1186/s40064-016-2041-8

Usman, A. B. (2021). Teaching and Learning Cybersecurity courses with Virtualization Technology.

Vojtěšek, J., Bližňák, M., Matušů, R., & Dulík, T. (2009). *Virtualization as a Teaching Tool for IT-based Courses. WSEAS Transactions on Advances in Engineering Education.6* (1), 265-274 http://www.wseas.us/e-library/transactions/education/2009/29-098.pdf

Du, W., Jayaraman, K., & Gaubatz., N.B. (2010, June). Enhancing security education with hands-on laboratory exercises. In proceedings of 5th Annual Symposium on Information Assurance (ASIA ’10) (pp.156-61)

Xie, X., & Chu, J. (2022). Data collection and Visualization Application of VMware Workstation Virtualization Technology` in college Teaching Management. Mathematical Problems in Engineering, 2022. https://doi.org/10.1155/2022/6984353