Teaching and Learning Cybersecurity courses with Virtualization Technology

Aminu Usman, PhD, HEA
Department of Computer Science
York St John

Presented at YHIoT Tech Seminar, 2021
Outline

• VT - Enabling students beyond the classroom
• Virtualization Technology ?
• Teaching With VT
• Examples - Environment Setup for the Experiments
• VT-Based Assessment Methods
• Samples of experiment
• VM Vs Containers
• Instructors and Students Observations/Feedback
## Enabling students beyond the classroom

<table>
<thead>
<tr>
<th>Category</th>
<th>Questions/considerations</th>
</tr>
</thead>
</table>
| Achieving accurate learning outcomes and assessments that reflect | - the practical elements of the courses learning objectives  
- students' expectations,  
- Industry's changing requirements |
| Time & Logistics                | - How many hours do students have access to the laboratory infrastructures?                 |
| Safe Environment for Students Work | - Can the students have access to their practical learning platforms at their comfort and at any time?  
- Would the students be able to practice their learning in a safe environment with all the computer and network access privileges |
| Scalability                     | - Would they be able to scale their work with adequate resources to enable them to demonstrate their learning from anywhere? |
Student-focused/expectations

- Students are looking for
  - Job related topics

- Some topics are difficult to be taught theoretically
- Most of the subjects requires students to build a network

Cybersecurity Pre-course Survey

What topics would you like to focus on through the semester? You are to choose your best five.

- Penetration Testing (66.7%)
- Web Security (73.3%)
- Network Security - Packet Sniffing & Spoofing attacks and countermeasures (73.3%)
- Applied Cryptography (46.7%)
- DNS and Attacks (40%)
- Building Virtual Private Network (53.3%)
- The General Data Protection Regulation (GDPR) (26.7%)
- IT Security Audit and Control (33.3%)
- Digital Forensic (33.3%)
- Cybercrime: Ethics and Responsibilities (86.7%)

Multi answer: Percentage of respondents who selected each answer option (e.g. 100% would represent that all this question’s respondents chose that option)
Student-focused/expectations (2)

- Students are looking for hands-on experiences/learning.

Cybersecurity Pre-course Survey
### Student-focused/expectations (3)

<table>
<thead>
<tr>
<th>Why do you want to attend this course?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Security interests me and would be a good consideration for a career</td>
</tr>
<tr>
<td>Out of interest and importance of cyber security.</td>
</tr>
<tr>
<td>Interested in the topic</td>
</tr>
<tr>
<td>To get to know how to prevent cybercrime and look into possible job opportunities using this module</td>
</tr>
<tr>
<td>I find cyber security interesting. Would like to expand upon my existing knowledge.</td>
</tr>
<tr>
<td>I believe it is a good module for future work places. Lots of areas to work on in cyber crime.</td>
</tr>
<tr>
<td>I thought it would be good experience for the professional world.</td>
</tr>
<tr>
<td>Hopefully turn it into a career</td>
</tr>
<tr>
<td>Sounds interesting, different to all the other modules</td>
</tr>
<tr>
<td>Cybercrime and security is a very large business sector so it seems like a wise investment of my time</td>
</tr>
<tr>
<td>To learn about cybercrime!</td>
</tr>
<tr>
<td>I have an interest in Cyber Security</td>
</tr>
<tr>
<td>To finish my degree</td>
</tr>
</tbody>
</table>

Career, Interest, work placement, experience, to finish a degree.
ILOs and constructive alignment with L&T and Assessment Method

• At the heart of curriculum design are three key processes:
  • establishing appropriate ILOs;
  • designing appropriate learning and teaching activities that enable learners to meet those outcomes;
  • designing appropriate assessment methods through which learners can demonstrate that they have met the outcomes.
Teaching Cybersecurity courses

Theory – lectures
   Explain/describe ideas and the meanings of terms

Case studies
   Evaluate/discuss/ the strength and weaknesses of security systems

Simulators/Emulators/Model Checkers
   Illustrate events/incidences with limitations & approximations

Mathematics
   Demonstrate ideas with approximations. NOT the actual events

Virtualization Technology
   Practice
**Virtualization Technology?**

**Virtualization**

- Virtualization is the creation of a virtual version computer, including virtual computer hardware platforms, storage devices, etc.

- A VM is a software implementation of a computer that executes programs like a physical machine.

- Hypervisors (VMM) - a software program that manages multiple OSes

- Types  
  - Application Server Virtualization  
  - Application Virtualization  
  - Network Virtualization  
  - Storage Virtualization  
  - Desktop Virtualization  
  - Full Virtualization

**Virtualization Concepts**

- **Bare-Metal Hypervisor (Type 1)**  
  - VMware vSphere/ESXi  
  - Microsoft Hyper-V  
  - Citrix XenServer

- **Hosted Hypervisor (Type 2)**  
  - VMware Workstation/Fusion  
  - Oracle VirtualBox  
  - Parallels (Mac)
Students can create more virtual hosts than the number of physical computers available in the laboratory.

Student can create complex scenarios involving several hosts.

No restrictions of the number of network interfaces in each host.

Student are the administrators of their virtual hosts.

Students can reproduce the experiments at home.
Examples - Environment Setup for the Experiments

Web security - SQL Injection Attacks & countermeasures

Network Security - Use reverse SSH tunnelling to access an internal web server

Digital Forensics

Network Security - DNS Attacks & countermeasures
VMs Network settings

For more advanced networking needs, such as network simulations and running servers in a guest.

If all you want is to use the VM to browse the Web.

Internal network that allows outbound connections.

Visible to selected virtual machines.

This can be used to create a network containing the host and a set of virtual machines.

Rarely used modes which share the same generic network interface.
Creating the Hypervisor

Creating VMs

Installing OSs on VM

Configure the VM

Building a virtual network with VMs.

Build and configure other services (Server)

Installing Software Packages

Creating the virtual computer hardware
- define the hard-drive (HD) type and size
- RAM size, and other parameters

Linux
Windows
Mac OS
Android, etc

General Advanced Tab:
- Shared Clipboard: Bidirectional
- Drag'n'Drop: Bidirectional

System:
- Motherboard Tab:
- Base Memory: 2GB
- Extended Feature: Enable I/O APIC

Processor Tab:
- Processors(s): 2 CPU
- Extended Features: Enable PAE/Nx
- Acceleration Tab:
- Hardware Virtualization: Enable VT-x/AMD-V
- Enable Nested Paging

Network:
- Adapter 1:
  - Attached to: NAT Network
  - Advanced:
    - Promiscuous Mode: Allow All

MAC Address: (click generate new MAC)

VPN, DNS, DHCP, SSH, TELNET, Firewall, Mail Service, Web Server, etc.

Web Security
Network Security
Digital Forensics
Traffic Monitoring
Vulnerability exploitation
Applied Cryptography
Packet Crafting
Penetration testing

Installing VirtualBox
Or VMware
Cloud Hypervisor

Building the Lab Environment
Kali Linux – Advance Penetration Testing tool

- Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing
  - Hundreds of penetration tools...
  - Kali Linux can run on laptops, desktops or servers
  - Open source availability
  - Azure Penetration Testing
  - Building a customized Kali ISO is easy, fun, and rewarding
  - You can run Kali "Live" from a USB drive on standard Windows and Apple PCs
A hands-on laboratory exercises (called SEED labs) for computer and information security education

- Software Security Labs
- Network Security Labs
- Web Security Labs
- System Security Labs
- Cryptography Labs
- Mobile Security Labs

Cloud-ready: You can now create a SEED VM on the cloud

The SEED project is now fully open sourced: https://github.com/seed-labs.
Virtual Labs Environment

• Among the popular virtual security labs
  • DeterLab (cyber DEfense Technology Experimental Researc) – Terry Benzel, University of Southern California.
  • Tele-Lab IT – a web-based training system, University of Trier, Germany
  • NETinVM – Comprises several computers and networks, in a single virtual machine using nested virtualization

• These virtual labs can facilitate cybersecurity experiments, whereby students can configure a number of networked virtual machines and embark on security offense and defense exercises
VT-Based Assessment Methods (1)

Example Screenshots (still pictures)
Settings, configurations, parameters, static outcomes, policies, codes or scripts

Example
Question – Detecting Cross-Site Scripting vulnerabilities in web applications.
Cross Site Scripting vulnerabilities allow attackers to spoof content, steal user cookies, and even execute malicious code on the user's browser. Many Web pen testers use the Nmap scripting engine to discover these vulnerabilities in web servers.

Your task is to use either Nmap scripts or any methods of your choice to scan a web server looking for file vulnerabilities to Cross-Site Scripting (XSS). You are required to use a free scan web server or develop your own.

Example - Assessment with Screenshots (still pictures)
VT-Based Assessment Methods (2)

- **Assessment With Screen Capture Video**
  - VT comes with a built-in screen video capturing function
  - Time in grading is reduced significantly
  - Short procedures, interactive outcomes

- **Virtual Hard Disk Files and Virtual Appliances**
  - The entire virtual hard disk file can be submitted for assessment
  - Using Save State - VM clears its memory when it is shut down

*Example - Assessment With Screen Capture Video*
VT-Based Assessment Methods

• Anonymous marking
  • Customize Bash Prompt
    • Change PS1 in ~/.bashrc, and then restart terminal
    • PS1=" Student ID : 7869167 "

```
Student ID : 7869167 $ sudo nmap -vS -p - -script vuln 45.33.49.119
Starting Nmap 7.91 (https://nmap.org) at 2021-03-13 15:24 GMT
Nmap scan report for ack.nmap.org (45.33.49.119)
Host is up (0.00019s latency).
Not shown: 65530 filtered ports
PORT STATE SERVICE VERSION
22/tcp open tcpwrapped
http-vuln-cve2010-4344:
  The SMTP server is not Exim: NOT VULNERABLE
sslv2-drown:
80/tcp open tcpwrapped
  http-csrf: Couldn't find any CSRF vulnerabilities.
  http-dombased-xss: Couldn't find any DOM based XSS.
host: Reported with: Apache/2.4.6 (CentOS)
http-server-header: Apache/2.4.6 (CentOS)
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
http-trace: TRACE is enabled
113/tcp closed ident
443/tcp open tcpwrapped
  http-csrf: Couldn't find any CSRF vulnerabilities.
  http-dombased-xss: Couldn't find any DOM based XSS.
  http-server-header: Apache/2.4.6 (CentOS)
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
sslv2-drown:
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 1268.39 seconds
```
Building a Learning Portfolio With VT

• With VMs, students can easily save their hands-on learning activities by using a new VM for each assignment
  • each student would have an archive of virtual hard disk files
Sample practical experiments

Injecting data into a TCP/UDP connection
Sample practical experiments

**Idea:** To fill the queue storing the half-open connections so that there will be no space to store TCB for any new half-open connection, basically the server cannot accept any new SYN packets.

**Steps to achieve this:** Continuously send a lot of SYN packets to the server. This consumes the space in the queue by inserting the TCB record.

- Do not finish the 3rd step of handshake as it will dequeue the TCB record.

**Counter measures**
- Turn ON the SYN Cookie countermeasure:

![Diagram](image-url)
VM Vs Containers

• The industry standard today is to use Virtual Machines (VMs) to run software applications.

• Docker is a platform for developers and sysadmins to build, run, and share applications with containers.

Containers are:
- Lightweight
- Easy to start -- Only a few seconds
- Less OS maintenance
- Efficient
# Challenges – Teaching with Virtualisation Tech

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Backward compatibility</strong></td>
<td>Compatibility issues when using legacy system can be time-consuming and difficult to solve.</td>
</tr>
<tr>
<td></td>
<td>- A good and descent PC, Cloud</td>
</tr>
<tr>
<td><strong>Backup</strong></td>
<td>Frequent software updates can make it difficult to access backup at times.</td>
</tr>
<tr>
<td></td>
<td>- Snapshots</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Unlike some tech solutions, virtualization is not really a “set it and forget it” type of solution.</td>
</tr>
<tr>
<td></td>
<td>- Regular updates</td>
</tr>
<tr>
<td><strong>Learning curve</strong></td>
<td>A misconception exists that virtualization is difficult to learn.</td>
</tr>
<tr>
<td></td>
<td>- Training and practices</td>
</tr>
</tbody>
</table>
Instructor Observations

- VT solve the logistics problems associated with hands-on activities
- It also helped to improve interaction with students and enabled more content coverage during class
- More hands-on projects
- Assessments are more aligned ILOs and comprehensive
- Coverage of material increased
- More interaction between
  - students and instructors – students ask questions more frequently
  - students and instructors – problems solving
Students Feedback on using the VT in Cybersecurity class

1. Given your experience using VT, do you think it helps students learn and improve students' skills with the course?

- Strongly Agree: (75%)
- Agree: (25%)
- Neither Agree Nor Disagree: 0
- Disagree: 0
- Strongly Disagree: 0

1.a. Do you think using the VT gives you access to your practical learning platforms at your comfort and at any time?

- Strongly Agree: (62.5%)
- Agree: (37.5%)
- Neither Agree Nor Disagree: 0
- Disagree: 0
- Strongly Disagree: 0

1.a.i. Do you think using the VT increases your engagement/number of Hrs spent with your learning?

- Strongly Agree: (50%)
- Agree: (12.5%)
- Neither Agree Nor Disagree: (37.5%)
- Disagree: 0
- Strongly Disagree: 0
Students Feedback on using the VT in Cybersecurity class

1.a.i. Do you think using the VT enabled you to scale your work and demonstrate your learning from anywhere?

- Strongly Agree (25%)
- Agree (62.5%)
- Neither Agree Nor Disagree (12.5%)
- Disagree 0
- Strongly Disagree 0

1.a.iv. Please provide any comments on your overall experience of the use of VT

- the networking in the VMs is fiddly
- Initially getting my head round the VT was difficult however it has slowly become more clear. I believe some of the course will be useful in industry however for me personally I would prefer to pursue a career in web development.
- It’s great.
- used it before so it wasn’t a new concept to me however I had never created my own little network and played around with packet capture and hacking concepts in a realistic manner before so I have really enjoyed the use of VT

1.a.w. What advice would you give to another student taking this module regarding the use of VT?

- It’s tricky, but so worth doing.
- mess around with the settings in your own time to understand how it all works
- Make sure your environment is set up early to avoid further complication in future weeks.
References


