Achieving Sustainable Delivery of Web Application Security Virtual Laboratory Resources for Distance Learning

OWASP
The Open Web Application Security Project

Adrian Winckles & Ibrahim Jeries
Anglia Ruskin University

12th July 2012

About Me

OWASP
The Open Web Application Security Project

- About Me
  - Adrian Winckles BEng MSc CEng CITP
  - Senior Lecturer in Computing & Technology
  - Department of Computing
  - Anglia Ruskin University
  - Cambridge, UK

  - Telephone Number (Office): +44 845 196 2440
  - Email: Adrian.Winckles@anglia.ac.uk
  - Skype: adrianwinckles

Anglia Ruskin University
Cambridge & Chelmsford

- **Before we start!!**
- Has anyone used virtualisation technology or have an idea what it is….

Virtual Desktops

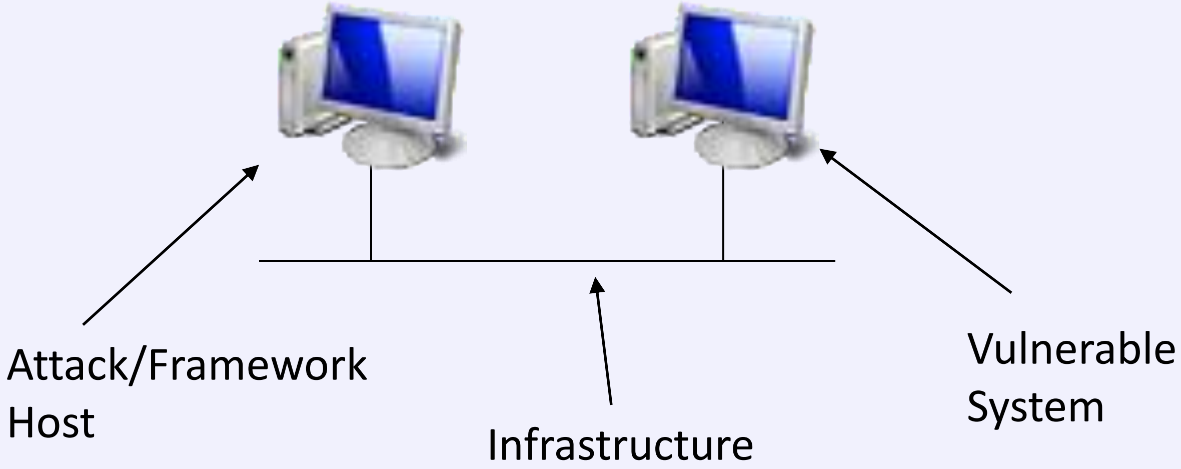
“Ability to access a traditional computer desktop from anywhere regardless of the type of computing platform being used…”

Penetration Testing Labs

- Conventional methods of teaching/learning ethical hacking/penetration testing
  - Using two or more physical computers.
  - Setting up virtual based lab on own/local computing platform.

Minimum Lab Model

- Essentially two/three parts
  - Vulnerable Systems
  - Penetration Testing Frameworks and Tools
  - Possible infrastructure components



Attack/Framework Host

Infrastructure

Vulnerable System

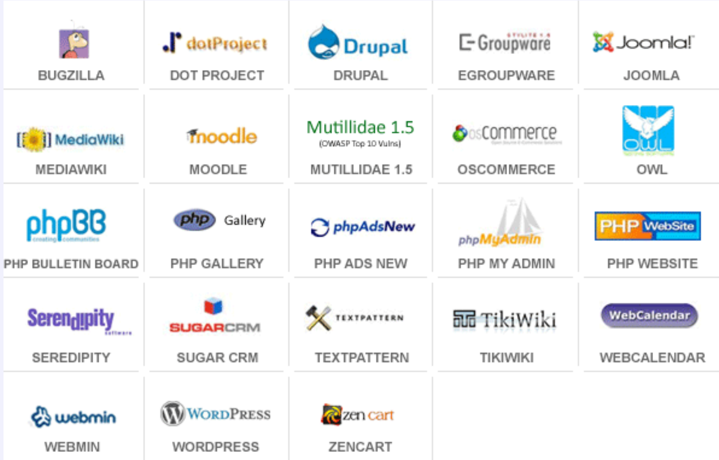
Vulnerable Systems

OWASP
The Open Web Application Security Project

- To name but a few
  - Metasploitable VM
  - UltimateLAMP VM
  - DVWA
  - Mutillidae
  - Moth VM
  - WebGoat
  - Hacme Series
    - Hacme Bank
    - Hacme Books
    - Hacme Casino
    - Hacme Travel
    - Hacme Shipping

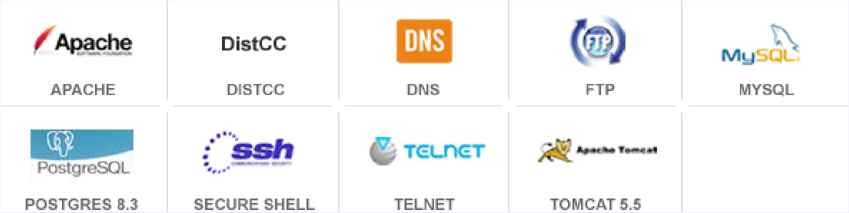
Typical Vulnerable Applications

OWASP
The Open Web Application Security Project



BUGZILLA	DOT PROJECT	DRUPAL	EGROUPWARE	JOOMLA
MEDIAWIKI	MOODLE	MUTILLIDAE 1.5	OSCOMMERCE	OWL
PHP BULLETIN BOARD	PHP GALLERY	PHP ADS NEW	PHP MY ADMIN	PHP WEBSITE
SEREDIPITY	SUGAR CRM	TEXTPATTERN	TIKIWIKI	WEBCALENDAR
WEBMIN	WORDPRESS	ZENCART		

- Typical applications vulnerable systems may use.
- Older versions often utilised due to inherent vulnerabilities



APACHE	DISTCC	DNS	FTP	MYSQL
POSTGRES 8.3	SECURE SHELL	TELNET	TOMCAT 5.5	

Attack Testing & Frameworks

- Backtrack v4, 5 etc
- WTF Samurai Framework
- Metasploit Framework
- DIY Toolset on a VM (or multiple VM’s)
  - Choose your own tools/toolset (mix & match)
    - Nessus
    - Cain & Abel
    - etc

Infrastructure Components

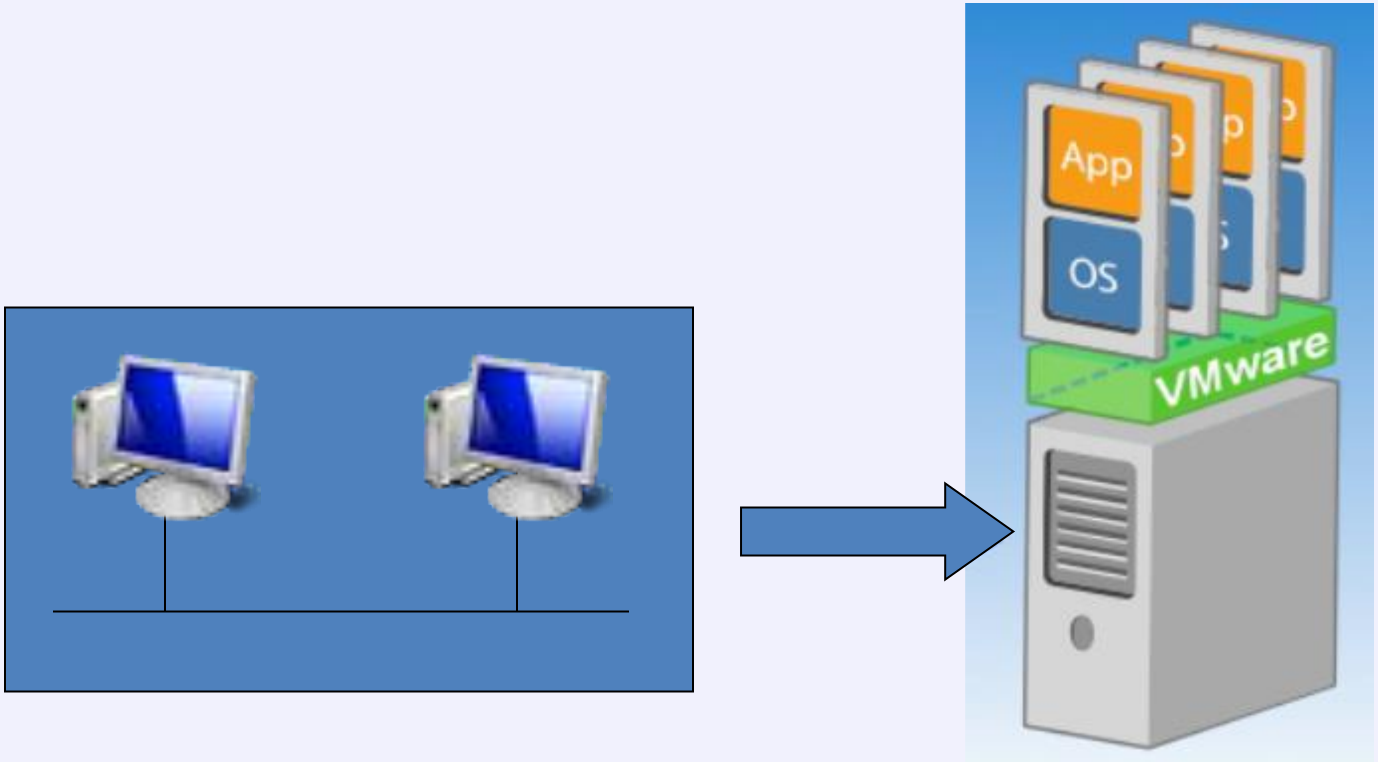
OWASP
The Open Web Application Security Project

- Physical Infrastructure
  - Cables/Switch/Hub (virtual or physical)
- Active Infrastructure
  - Firewalls/Router (including NAT fuctions)
  - IDS/IPS
  - Security Appliances

Physical Problems

- Physical Implementations unsustainable
  - Too many physical computing components for complex models
  - Space for multiple computing platforms
  - Additional administration if configurations need to change
  - Power consumption
- To overcome these limitations consider virtual implementation

Simplistic Virtualised Lab

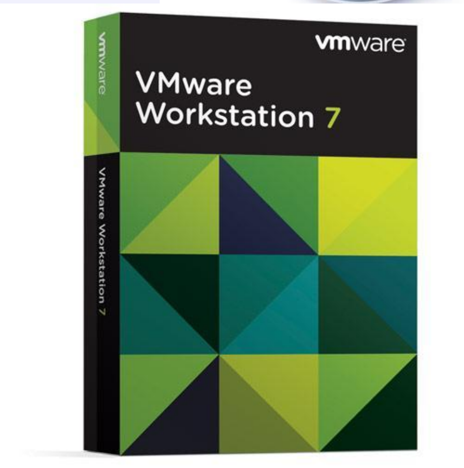


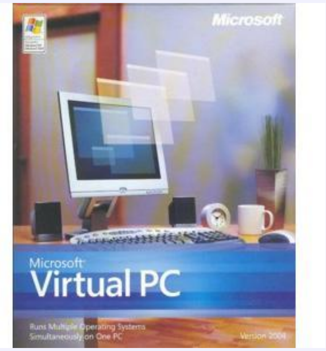
Use virtual networks between VM’s

Assigning each VM to the relevant subnets (VMnet) (essentially VLAN’s)

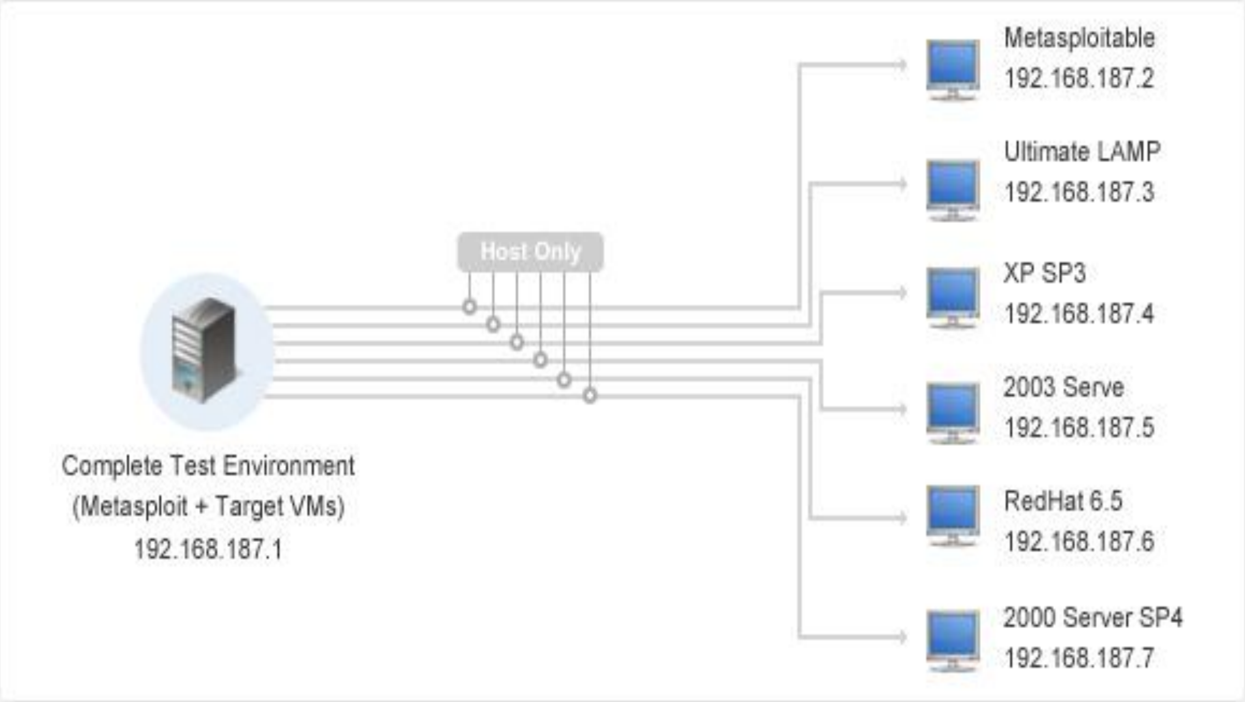
Hosted Hypervisor’s

- Hosted Hypervisor Virtualisation Platforms
  - VMWare Workstation/Fusion
  - Citrix
  - Microsoft Virtual PC
  - Virtual Box
  - Amongst others





More Complex Virtualised Example



- Metasploit‘s Suggested Virtual Pen Test Lab

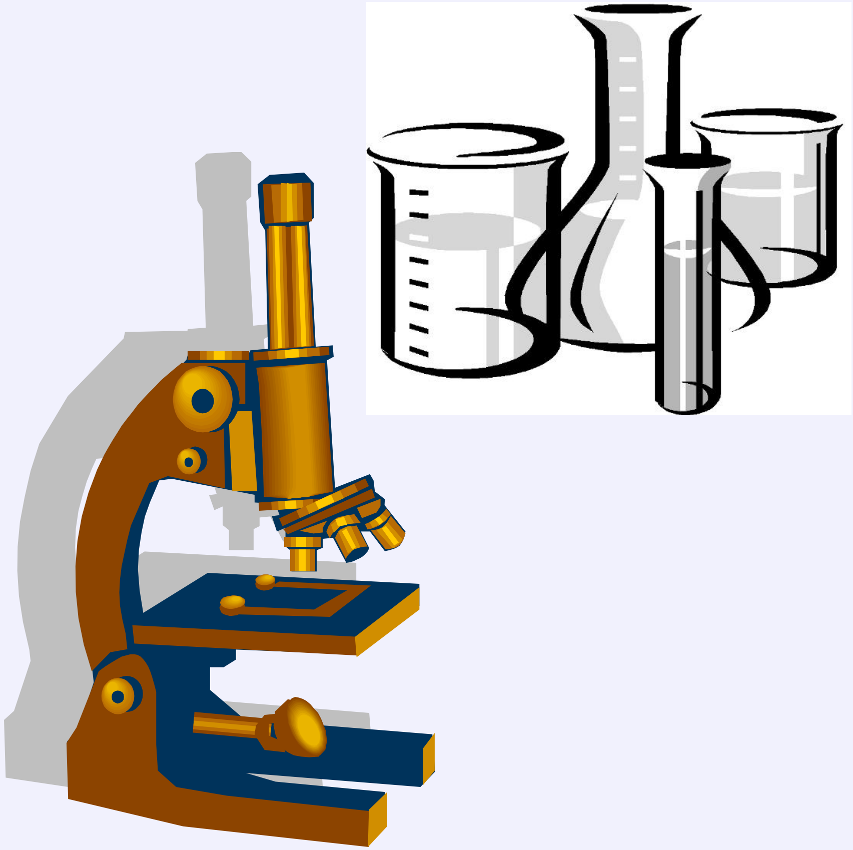
- Problems – fine for personal use but
  - Requires dedicated personal machine
  - Lots of memory, multi cored processor
  - Hosted hypervisor (although this can/should be free), competing with resources with more conventional applications and main OS.
  - Biggest problem could be licensing
    - E.g. If Windows VM's are required, would require multiple personal licenses.

Larger Scale Teaching

- Personal VM solutions fine but not always scalable If delivering training provision
  - How do you keep track of students progress
  - Ho do you stop the students “knowing what’s there”
  - Reverting back to snapshot
  - Keep the environment secure
  - IT Departments are especially paranoid about students/learners running penetration tools in any form connected to corporate or university networks.

What is a “Laboratory”?

- Maybe some formof Lab Solution is the answer?
- Oxford English Dictionary definition:
  - *“A laboratory is “a room or building for scientific experiments, research, or teaching, or for the manufacture of drugs or chemicals”.*



Computing Labs

OWASP
The Open Web Application Security Project

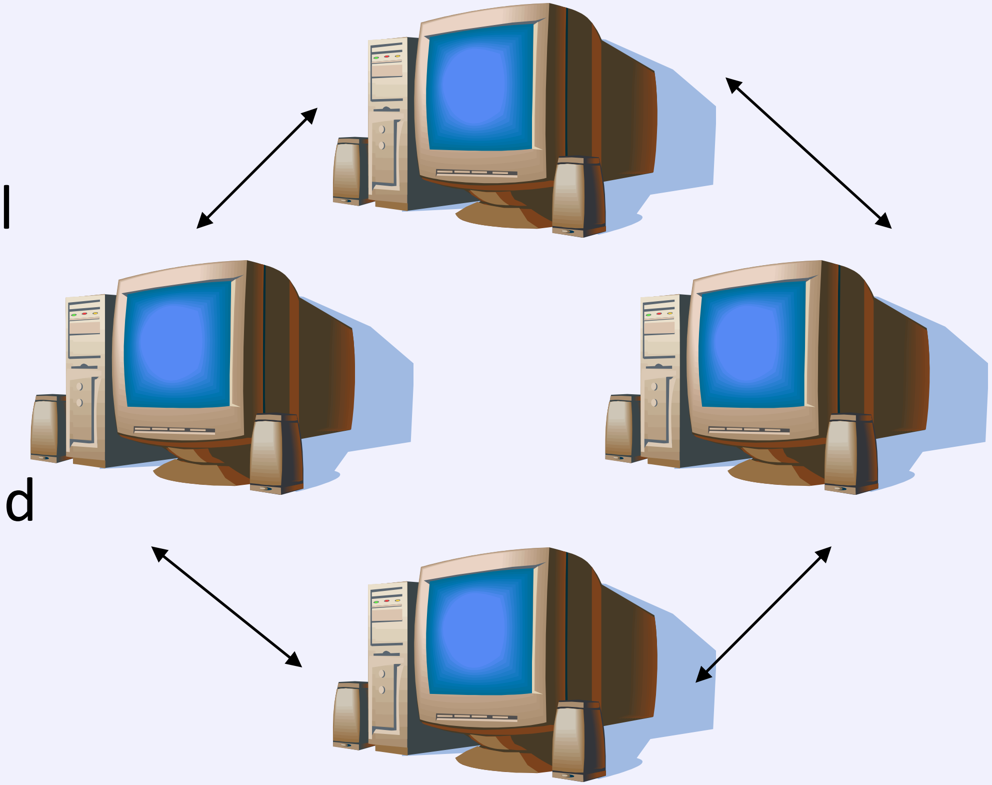
- According to (Machotka, J., Nedic, Z., Gol, O., 2007).
  - *Computer Science labs require students to have access to equipment like networked computers, servers, routers, switches and specific software applications so that the teaching process can be as productive, fruitful and realistic as possible*

Limitations of Traditional Computing Labs

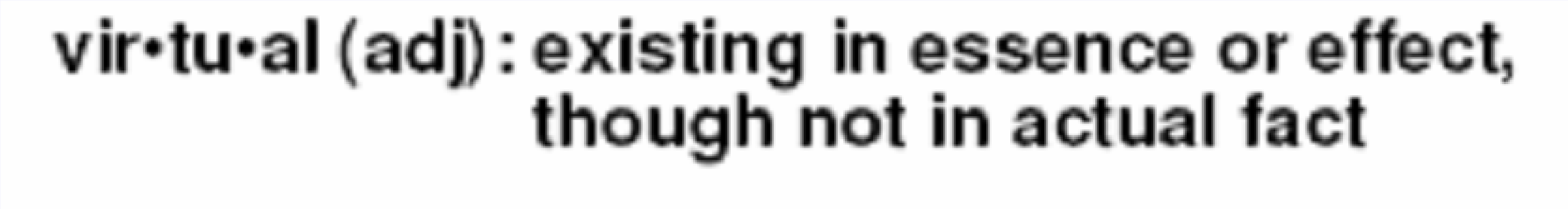
- Traditionally was the ONLY way to teach practical IT security issues
- Limitations included:-
  - Time and space restrictions
  - Supervision required
  - High maintenance costs
  - Scheduling activities common to many colleges/univeristies

Complex IT Laboratories

- In a physical lab to set up many of these configurations, lots of physical machines are needed (space and physical storage requirements considerable)
- In a physical computer lab with virtualisation, can build the scenarios but the problem is with storing the data.



The Virtual Laboratory



vir•tu•al (adj): existing in essence or effect, though not in actual fact

- Often badged with “remote” labs but has a definition all of its own
  - *“any local computer hosting a simulation” is considered a virtual lab”*
    - Leitner & Cane (2005)

- Term can be extended further to include
  - *a computational grid, used for solving computational problems with geographically distant resources.*

Growth of Virtualization for Labs

- Virtualization is most popular choice for delivering quality distance teaching.
- Many different implementations and technologies
- Often used to teach
  - Different operating system concepts and application configuration
  - Integrating diverse systems
  - Configuring network
  - IT Security (application, network ...)
- Key issues – can help to enforce sandbox approaches
  - Happy IT Departments
- All without being on campus……

Virtualization - Definition

- Encourages portability
- Definitions
  - *to create abstract computer resources which are only virtual software versions of something rather than really existent* (Michocka, D., Shwartsman, S., 2008).
  - *"virtualization enables one server or computer to act as many".* (Robb, D., 2008)
  - *Instead of keeping your important programs on separate servers so that if one application or server fails, the other applications aren't affected, virtualization software lets you run many applications on the same server."* (Robb, D. 2008)

Complex Laboratories

- In essence this means more than one usable virtual machine or virtual desktop
- Needs to have a minimum of 2 networked together to provide some form of IT Security scenario function. Likely to be much more complicated.
- Aim is to provide functionality to offer this as a remote distance learning tool in the most beneficial way for the students learning experience whilst maintaining “state of the art” equipment/software and the use of relevant scenarios.

Virtual Lab Solution

- Virtual Laboratories
  - Also termed in the new cloud paradigm
  - “Lab as a Service” - LaaS
- Offering remote access to virtual resources which can be created/deleted as required. VM’s only active for learner session thus preserving scarce resources.
- Virtual images could be stored for student progression or reverted to previously stored states.

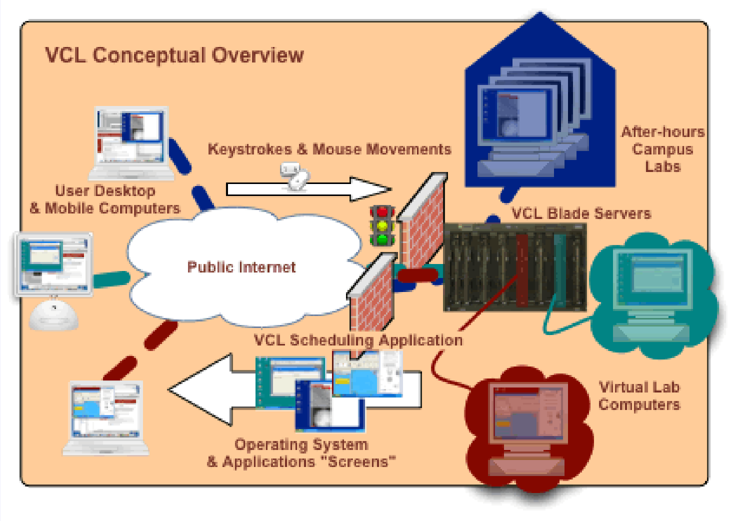
Virtual Lab Approaches

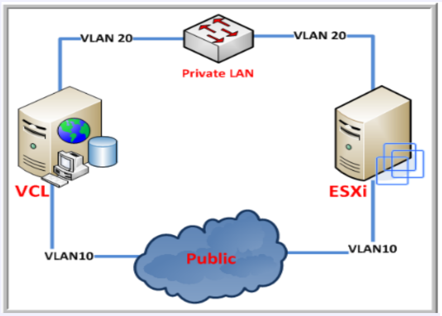
OWASP
The Open Web Application Security Project

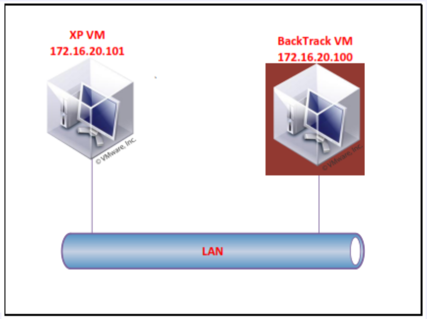
- Essentially 3 different models
  - Simple Virtual Lab (single VM’s)
  - Hybrid Virtual Lab (nested VM’s)
  - Complex Virtual Lab (multiple interconnected VM’s)

"Simple" Virtual Laboratories

- Simple Remote Lab could offer differing virtual machines
- Could create two instances of different virtual desktops and have them interact together.
- Requires user to maintain connectivity and interactions


VCL Conceptual Overview
Keystrokes & Mouse Movements
After-hours Campus Labs
User Desktop & Mobile Computers
VCL Blade Servers
Public Internet
VCL Scheduling Application
Virtual Lab Computers
Operating System & Applications "Screens"



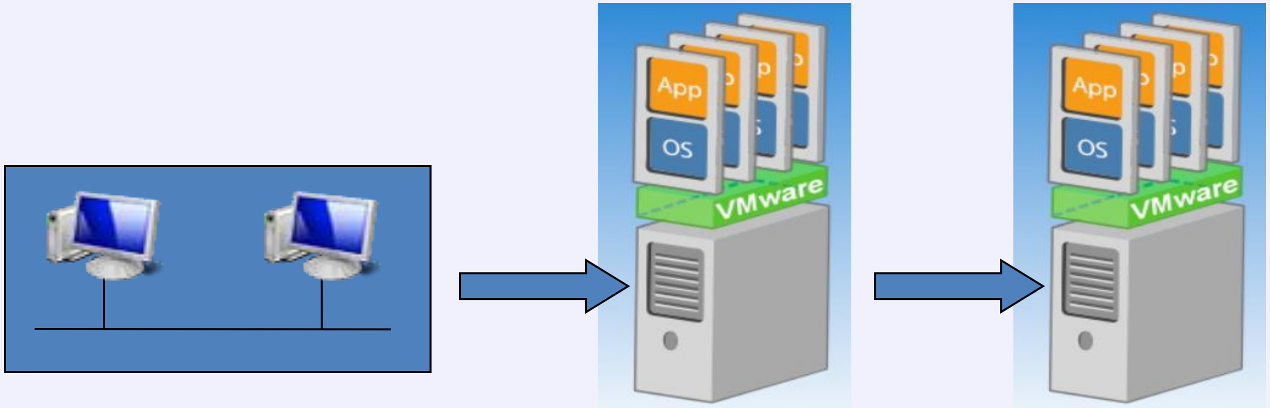


Virtual Computer Lab (VCL)

(Open Source Apache Foundation)

Hybrid Solution

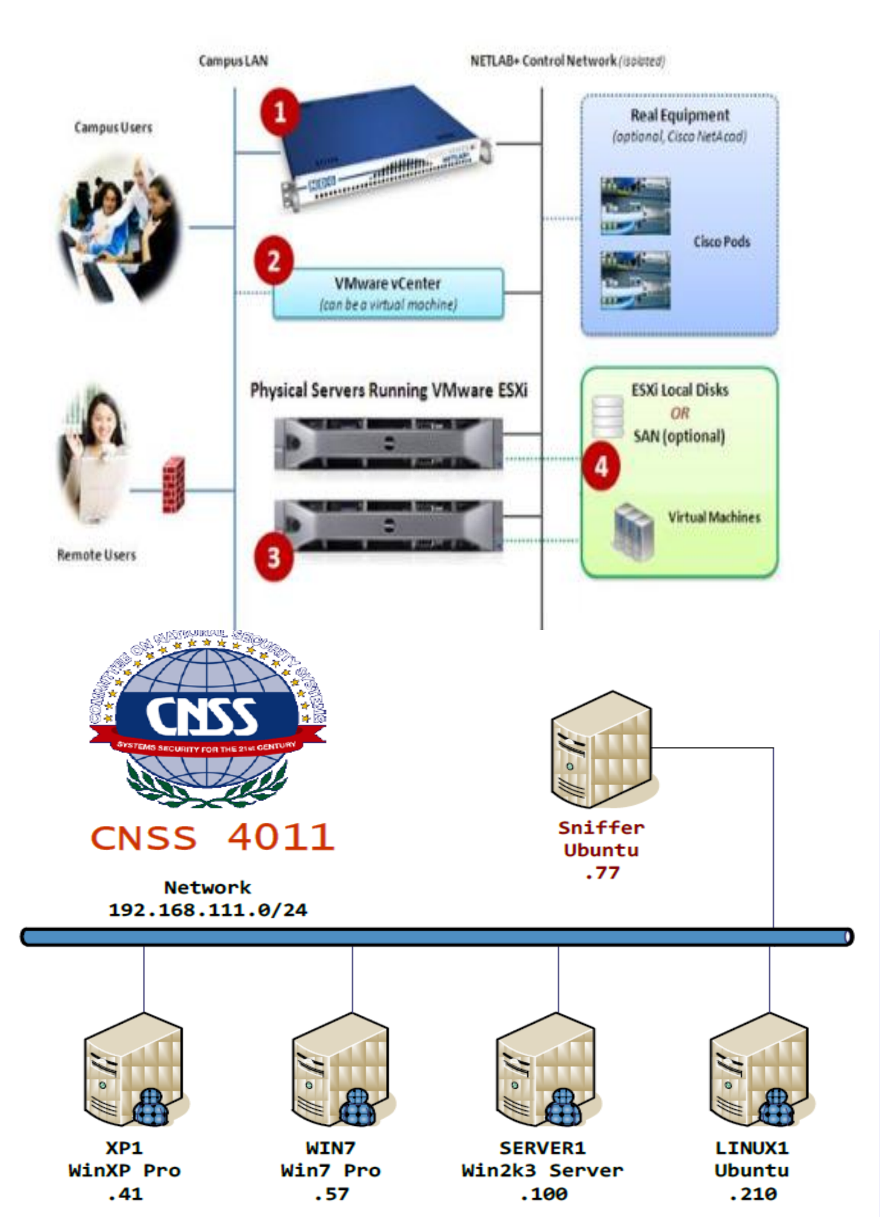
- Team of virtual machines available on a desktop platform (which is then virtualised itself and offered as one vm) (aka Nesting)
- Performance issues as everything has been virtualised twice.
- Other issues with maintaining state are similar having to remember where/how to access the nested VM's.
- Cold easily be offered by VCL to overcome its short comings but does not offer user friendly interface or other requirements.



Complex Virtual Lab

OWASP
The Open Web Application Security Project

- Each computing element is accessed via a web front end.
- Each component can only access others connected to its group.
- Completely secure (sandboxed) from other operational environments.
- Commercial solution such as NDG's Netlab (opposite)



Virtual Lab Model Summary

- Simple Virtual Labs requires learner to set up two different bookings and facilitate communication between at least two virtualised images. No sandboxed environment
- Hybrid Environment keeps all environment to one virtual machine but is slower due to nested VM's.
- Complex Virtual Lab provides some of the functionality required especially with relation to secure sandboxed environment, access to each node within the scenario.

Other Important Issues

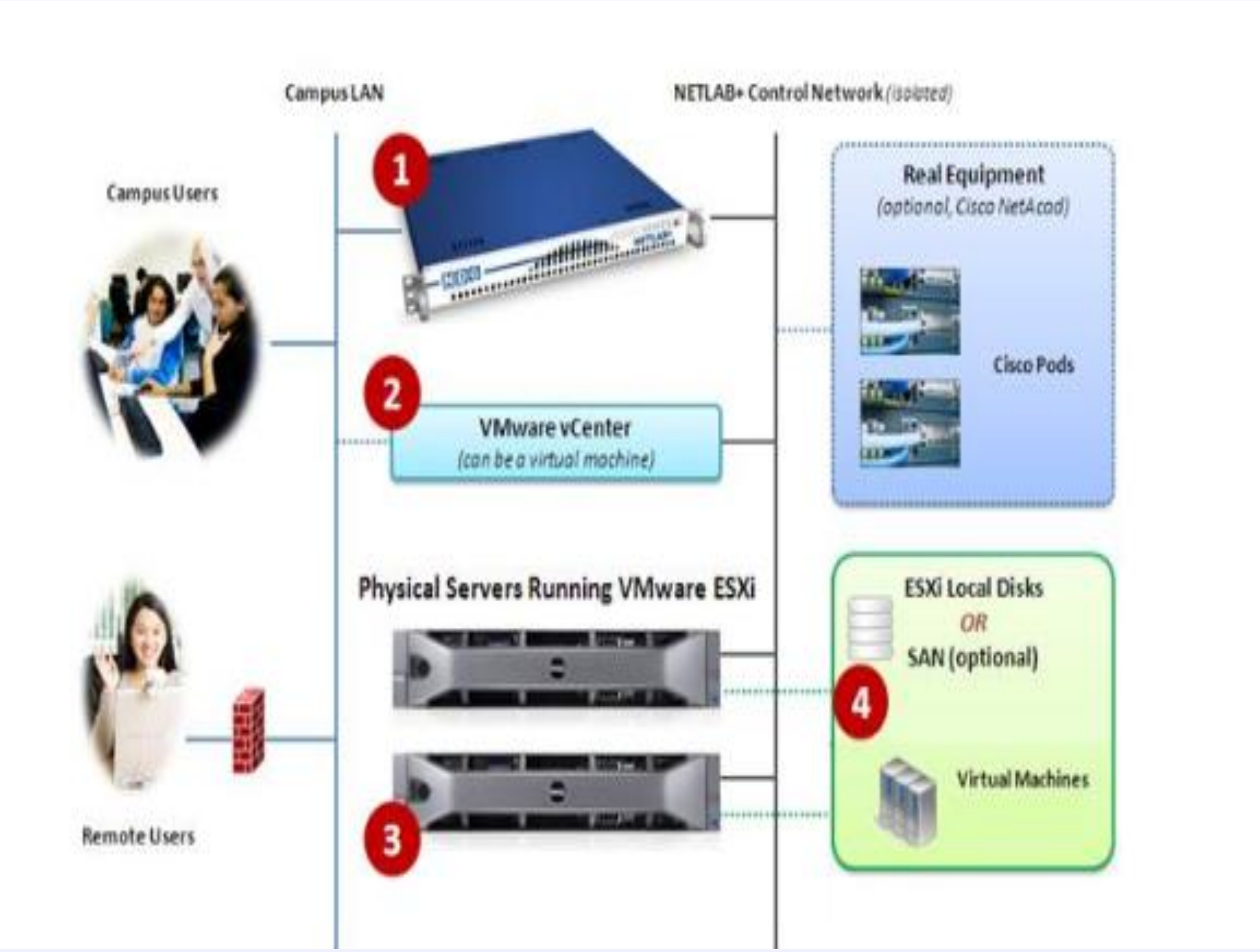
- **Persistence** – maintaining the state of the learners experience with the virtual laboratory i.e. letting the student carry on where they left off, saving the state.
- **Snap Shots** – the state of the laboratory is not saved, its reverts at the end of the session to a previous template.

Key Virtual Lab Requirements

OWASP
The Open Web Application Security Project

- Requirements
  - Web based front end providing proxy functions, seperated from virtual machine resources.
  - Scheduling function to book resources
  - Automated commissioning/decommissioning of virtual machines
  - Virtual switches & VLAN’s linking resources
  - Secure sandboxed environment
  - Method for remote access for KVM functionality (RDP, X-Windows, VNC etc)

Workings of a Virtual Lab

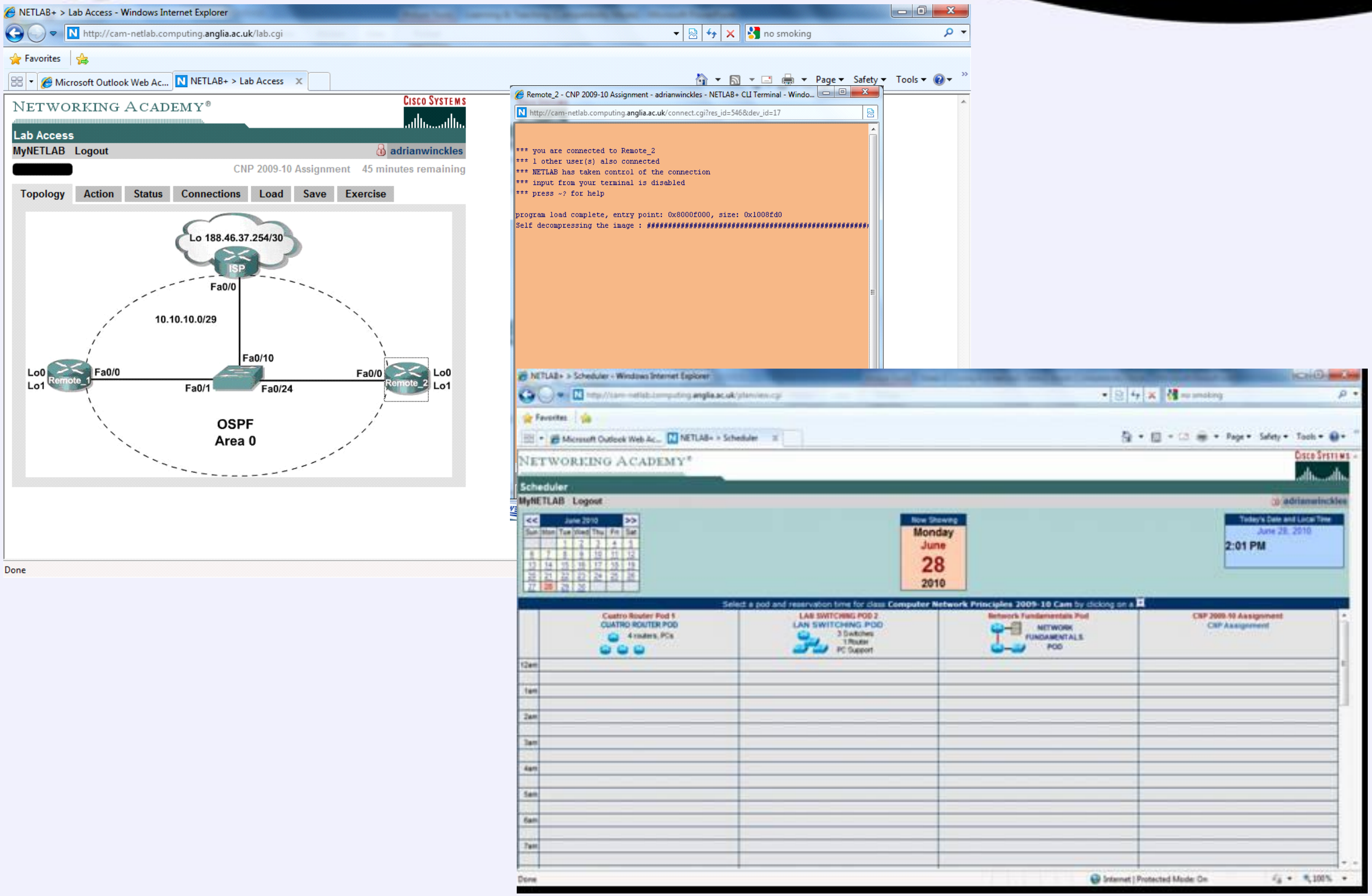


1. The NETLAB+ server provides the user interface for student and instructor access,an interface to manage virtual machines, and software features to automate scenario creation/removal.
2. VMware vCenter is used to manage your physical VMware ESXi servers, to create virtual machines, and to take snapshots of virtual machines. NETLAB+ communicates with vCenter to perform automated tasks and virtual machine management.
3. Physical VMware ESXi servers host the virtual machines for the security scenarios.
4. Typical security scenario consist of multiple virtual machines that reside on physical ESXi host server or reside on a Storage Area Network (SAN).

Typical Functionality

OWASP

The Open Web Application Security Project



NETLAB+ > Lab Access - Windows Internet Explorer

http://cam-netlab.computing.anglia.ac.uk/lab.cgi

NETWORKING ACADEMY®

Lab Access

MyNETLAB Logout adrianwinckles

[redacted]

CNP 2009-10 Assignment 45 minutes remaining

Remote_2 - CNP 2009-10 Assignment - adrianwinckles - NETLAB+ CLI Terminal - Windo...

http://cam-netlab.computing.anglia.ac.uk/connect.cgi?res_id=546&dev_id=17

```
*** you are connected to Remote_2
*** 1 other user(s) also connected
*** NETLAB has taken control of the connection
*** input from your terminal is disabled
*** press ~? for help

program load complete, entry point: 0x8000f000, size: 0x1008fd0
Self decompressing the image : ##################################################
```

NETLAB+ > Scheduler - Windows Internet Explorer

http://cam-netlab.computing.anglia.ac.uk/planview.cgi

NETWORKING ACADEMY®

Scheduler

MyNETLAB Logout adrianwinckles

Now Showing: Monday June 28 2010

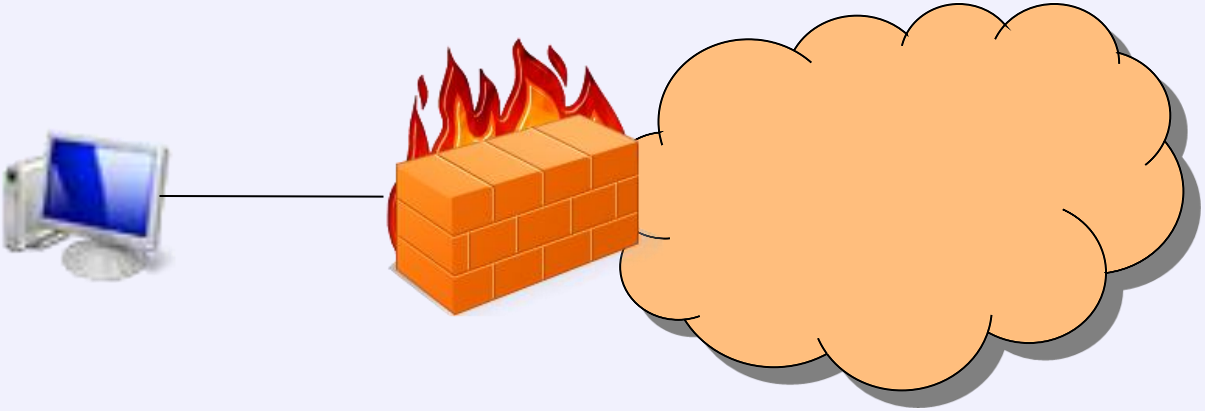
Today's Date and Local Time: June 28, 2010 2:01 PM

Select a pod and reservation time for class **Computer Network Principles 2009-10 Cam** by clicking on a

	Cuatro Router Pod 1 CUATRO ROUTER POD 4 routers, PCs	LAB SWITCHING POD 2 LAN SWITCHING POD 3 Switches 1 Router PC Support	Network Fundamentals Pod NETWORK FUNDAMENTALS POD	CNP 2009-10 Assignment CNP Assignment
12am				
1am				
2am				
3am				
4am				
5am				
6am				
7am				

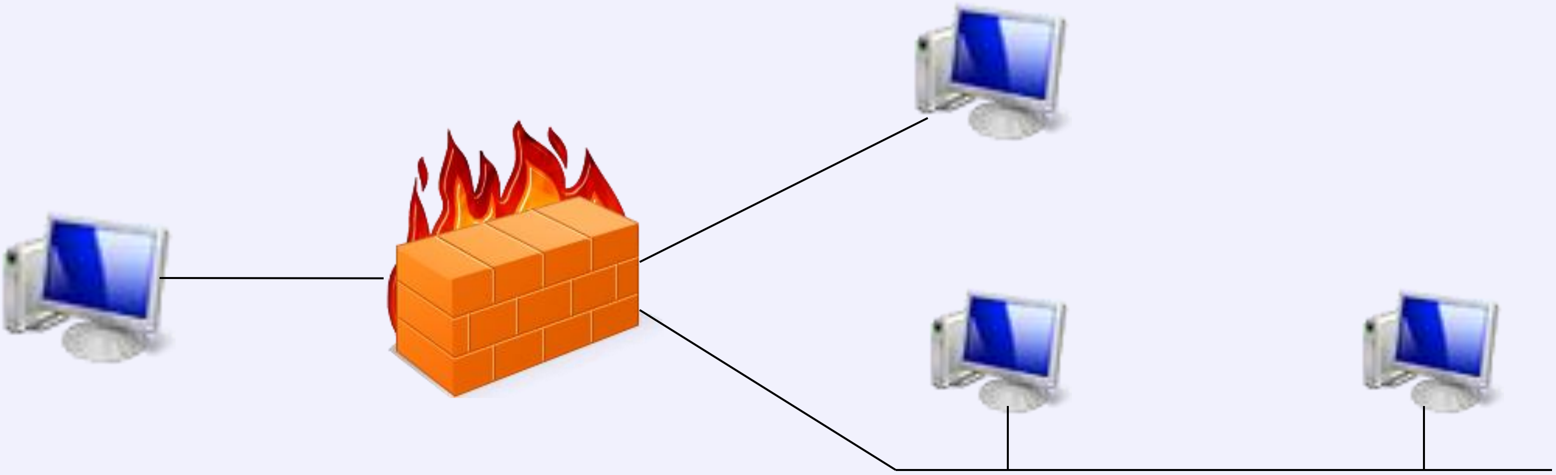
Other Scenario’s

- Hiding content, challenge the user to find whats behind the firewall/security appliance and break it
- “Capture the flag” competitions and other challenges



Other Scenario’s (revealed)

- Hiding content, challenge the user to find whats behind the firewall/security appliance and break it
- “Capture the flag” competitions and other challenges



Conclusions

- Both VCL and Netlab solutions are capable of delivering an automated and self-maintained virtualised remote computing environment to cater for students need with very little ongoing administration.
  - Whilst VCL provides a highly scalable, flexible and very cost effective solution, it is limited in the complexity of the solutions potentially offered.
  - Netlab provides a more managed solution better able to provide the complexity and flexibility that more advanced computer science courses may require. Volume License costing could be an issue.

Future Work

- Development of the open source model to offer persistent states.
- Development of external resources using cloud technologies

Future Work

- Development of open source VCL solution using secure groups for commissioning/decommissioning of multiple virtual machine.

Credits

OWASP

The Open Web Application Security Project

- Border, C. 2007. The development and deployment of a multi-user, remote access virtualization system for networking, security, and system administration classes. [internet] Available at: http://portal.acm.org/citation.cfm?id=1227310.1227501
- Fisher, K., Thacher, Cl., 2009, Virtualization: What does it mean for SAS®? [internet] Available at: http://support.sas.com/resources/papers/sgf09/347-2009.pdf
- Leitner, L. J. and Cane, J. W. 2005. A virtual laboratory environment for online IT education [internet] Available at: http://portal.acm.org/citation.cfm?id=1095714.1095780&coll=GUIDE&dl=GUIDE&CFID=84352268&CFTOKEN=88193923#
- Machotka, J., Nedic, Z., Gol, O., 2007, Collaborative Learning in the Remote Laboratory NetLab [internet] Available at: http://www.iiisci.org/journal/CV$/sci/pdfs/E147NH.pdf
- Mihocka, D., Shwartsman, S., 2008 Virtualization Without Direct Execution or Jitting: Designing a Portable Virtual Machine Infrastructure [internet] Available at: http://ivanlef0u.nibbles.fr/repo/todo/Virtualization_Without_Hardware_Final.pdf
- Nedic, Z., Machotka, J, Nafalski, A., 2003, Remote Laboratories Versus Virtual and Real Laboratories, [internet] Available at: http://ictt.insa-lyon.fr/ELabs/Bibliographie/documentation%20d%E9cembre%202005/IEEE/IEEE%20CNF/01263343.pdf
- Robb, D. 2008, What Virtualization Means for Small Business [internet] Available at: http://www.smallbusinesscomputing.com/news/article.php/3725081

Questions?

Feedback:
https://www.surveymonkey.com/s/Research12_Winckles_Jeries