Implementation of Active Learning Techniques in an Online Information Security Graduate Laboratory Course

Carlos Velez
Polytechnic University of Puerto Rico
377 Ponce De Leon Avenue
San Juan, Puerto Rico 00918
velez_108679@students.pupr.edu

Alfredo Cruz, Ph.D.
Polytechnic University of Puerto Rico
377 Ponce De Leon Avenue
San Juan, Puerto Rico 00918
alcruz@pupr.edu

ABSTRACT

Hands-on online courses are being integrated as part of Information Security departmental curricula. The courses are implemented using blended learning approaches, virtual environments, and most recently Docker containers. This research focuses on the implementation of a virtual environment combined with modified “active learning” techniques. To do this, six laboratories designed within a virtual environment will be integrated into the online-taught Principles of Information Security course. As a complement, a Wordpress blog will be prepare to serve as an active learning technique for students to create and discuss a topic related to each laboratory. The intention is to create a virtual environment that consists of a network of several virtual machines with known vulnerabilities. A main Windows server with Hyper-V services will accommodate the environment. At the end of each laboratory, the student will be given an online assessment that will provide metrics, the instructor will have online real-time reports, and the student will get feedback on where to go look in the book for further input on any failed questions. The labs will focus on: basic commands, footprinting and reconnaissance, scanning and enumeration, cryptoanalysis, password cracking and network vulnerabilities. It is expected that a combination of a virtual environment and active learning positively impacts student’s learning of computer security.

Keywords

virtual environment, active learning, information security, teaching, cybersecurity

1. INTRODUCTION

Since the 1990s education about information technology has been moving into the online realm as seen in [2]. While traditional methods involving physical hardware can be used, their effectiveness is limited by the high cost of hardware and software in addition to the creation, configuration and maintenance of the laboratory environments [4].

Presently, students are being provided with the option to take hands-on online courses as part of departmental curriculum [6]. There have been several methods in which hands-on online courses and emergency trainings have been implemented, including blended learning approaches, virtual environments, and Docker containers [5, 7, 3].

This ongoing research focuses on the implementation of a virtual environment combined with modified “active learning” techniques [1]. In a classroom setting, these techniques provide one-on-one interaction between participants, and while online courses do not provide physical interaction, online blogs can be used to stimulate student discussions on assigned material.

2. VIRTUAL ENVIRONMENT METHODOLOGY

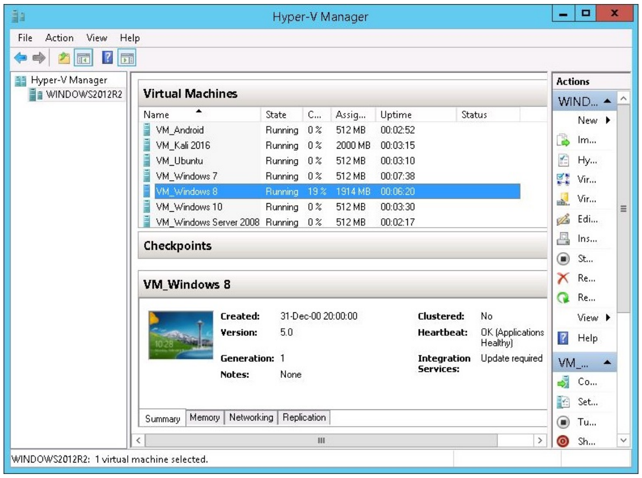
To integrate the laboratory component into the online-taught Principles of Information Security course, six laboratories will be designed within a virtual environment. As an active learning complement, a blog will be designed for students to create a topic related to each laboratory; offering students active interaction about each others selected topic.

The intention is to create a virtual environment that consists of a network of several virtual machines with known vulnerabilities (see Figure 1). A main Windows server with Hyper-V services will accommodate the environment. These laboratories will be designed using a metric that will calculate the student's grade based on how many questions were answered. At the end of each laboratory, the student will be given an online assessment that will provide metrics. At the same time, the assessment will provide the student with feedback on where to go look in the book for further input on any failed questions. The instructor will have online real-time reports of each student's progress. Laboratories will focus on basic commands, footprinting and reconnaissance, scanning and enumeration, cryptoanalysis, password cracking and vulnerabilities.

2.1 Commands for Linux and Windows Lab

To solidify the student's knowledge of basic commands, this laboratory will focus on reviewing and applying the utilization of commands from routine tasks such as navigation, file and folder creation, deletion and naming to more advanced commands that allow network debugging, identification of the computer's IP address, DNS and trace routes in both Linux and Windows systems. Students will be trained on the following tasks for Linux and Windows operating systems:

1. In this task the student will learn how to use the Linux **man, ls, cd, mkdir, rmdir** and **cat** commands. Students will need to *access* the General Commands Manual to learn how each command functions. They will then be able to use the commands to *navigate* between directories, *create* and *delete* folders and *display* file content. In Windows, to access information about a specific command, the student needs to type “/?” after the command. It is important to note that not



Virtual Machines

Name	State	C...	Assig...	Uptime	Status
VM_Android	Running	0 %	512 MB	00:02:52	
VM_Kali 2016	Running	0 %	2000 MB	00:03:15	
VM_Ubuntu	Running	0 %	512 MB	00:03:10	
VM_Windows 7	Running	0 %	512 MB	00:07:38	
VM_Windows 8	Running	19 %	1914 MB	00:06:20	
VM_Windows 10	Running	0 %	512 MB	00:03:30	
VM_Windows Server 2008	Running	0 %	512 MB	00:02:17	

Checkpoints

VM_Windows 8

Created:	31-Dec-00 20:00:00	Clustered:	No
Version:	5.0	Heartbeat:	OK (Applications Healthy)
Generation:	1	Integration Services:	Update required
Notes:	None		

WINDOWS2012R2: 1 virtual machine selected.

Figure 1: Physical server with a virtual environment consisting of seven virtual machines.

all commands in Windows have a manual assigned to them. Commands used to navigate files and folders include **cd, dir, mkdir**, and **rd /s /q**. The command type is very similar to the **cat** command in Linux.

2. The second task focuses on *manipulation* of files and folders through the use of **find, locate, grep, sort**, and **uniq** Linux commands while in Windows the commands are **find, findstr** and **sort**. These will allow the student to *peruse* strings in multiple files; ideal for log manipulation.

3. Linux network commands such as **ifconfig, ping, netstat, traceroute, nslookup** and **route** allow the student to *troubleshoot* and *identify* network parameters. In Windows the commands used are **ipconfig, ping, tracert, netstat**, and **nslookup**. This new information further permits an administrator to determine how secure is the network to carry out communications with other systems.

4. This task aims to teach the students how to *connect* to remote systems and services through the use of Linux **telnet, ssh** and **ftp** commands. In Windows, only the **ftp** command is available while Putty (an open source software) will be used for ssh and ftp connections. A successful connection would, in the case of **telnet** and **ssh**, provide full access to a remote system. In the case of **ftp**, files can be transferred securely over the network.

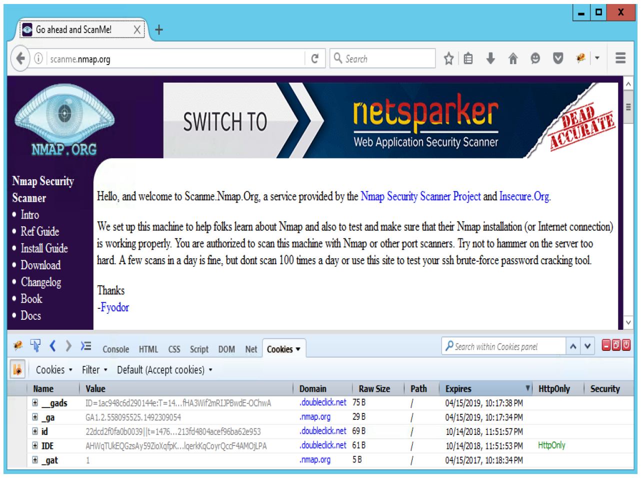
2.2 Footprinting Lab

Students will learn how to scan the source code of a website in search for content written in JavaScript, CSS, and HTML to obtain web cookies. This will be done by using an add-on tool for Mozilla Firefox called Firebug (see Figure 2).

To do this, students will perform the following tasks:

1. Install the Firebug add-on to Mozilla Firefox.

2. Open the provided website address and scan the source code to retrieve the cookies.



Hello, and welcome to Scanme.Nmap.Org, a service provided by the Nmap Security Scanner Project and Insecure.Org.

We set up this machine to help folks learn about Nmap and also to test and make sure that their Nmap installation (or Internet connection) is working properly. You are authorized to scan this machine with Nmap or other port scanners. Try not to hammer on the server too hard. A few scans in a day is fine, but dont scan 100 times a day or use this site to test your ssh brute-force password cracking tool.

Thanks
-Fyodor

Name	Value	Domain	Raw Size	Path	Expires	HttpOnly	Security
__gads	ID=1ac948c6d290144e:T=14...fHA3Wif2mRIJPBwdE-OChwA	.doubleclick.net	75 B	/	04/15/2019, 10:17:38 PM		
_ga	GA1.2.558095525.1492309054	.nmap.org	29 B	/	04/15/2019, 10:17:34 PM		
id	22dcd2f0fa0b0039||t=1476...213fd4804acef96ba62e953	.doubleclick.net	69 B	/	10/14/2018, 11:51:57 PM		
IDE	AHWqTUkEQGzsAy59ZioXqfpK...lqerkKqCoyrQccF4AMOjLPA	.doubleclick.net	61 B	/	10/14/2018, 11:51:53 PM	HttpOnly	
_gat	1	.nmap.org	5 B	/	04/15/2017, 10:18:34 PM		

Figure 2: Firebug tool (lower part) showing retrieved web cookies from the website http://scanme.nmap.org/ (upper part).

3. Provide specific information about the cookies (e.g., content, amount, and size).

Students will also *extract* meta tags, emails, phone numbers, faxes and URLs from company web-pages using the Web Data Extractor tool. This information can then be used by students to *impersonate* someone from one of the company websites. Students will also learn how hackers *duplicate* entire websites using the HTTrack tool. In addition, the Path Analyzer Pro tool will be used to *obtain* trace routes, DNS and other routing information and registries from websites that are not well configured.

To do this, students will perform the following tasks:

1. Install Web Data Extractor, HTTrack and the Path Analyzer Pro tools.

2. Scan a specific website using all the tools.

3. In a new file, save the output from the Web Data Extractor.

4. Duplicate the entire website using the HTTrack tool.

5. Recover the output provided by the Path Analyzer Pro tool.

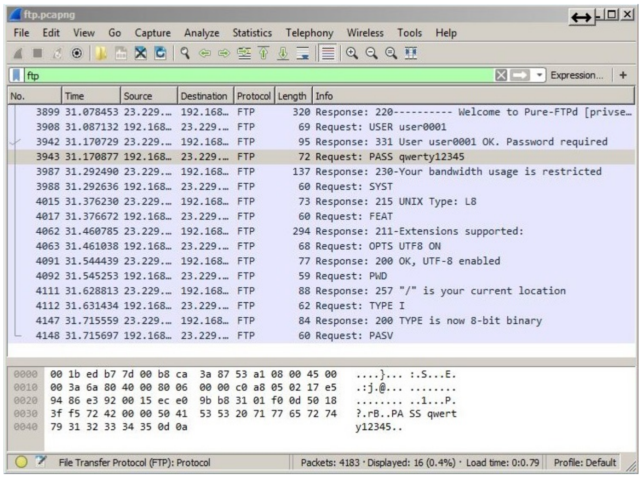
2.3 Scanning and Enumeration Lab

This lab teaches how to *monitor* data traffic (.pcap file) within a network using the Wireshark packet analyzer (Figure 3). In addition, students will perform Nmap scans on both Windows and Linux machines to spot open ports and identify operating systems in the network. Other scans will include Xmas Scans, ACK Flag Scans, UDP Scans, and IDLE Scans.

To do this, student will perform the following tasks:

1. Install Nmap and Wireshark packet analyzers.

2. Scan single and multiple IP addresses, perform fast scans and detect remote operating systems using Nmap.


ftp.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp
Expression...
+

```
No.     Time      Source     Destination Protocol Length Info
   3899 31.078453 23.229...  192.168...  FTP         320 Response: 220---------- Welcome to Pure-FTPd [privse...
   3908 31.087132 192.168... 23.229...   FTP          69 Request: USER user0001
   3942 31.170729 23.229...  192.168...  FTP          95 Response: 331 User user0001 OK. Password required
   3943 31.170877 192.168... 23.229...   FTP          72 Request: PASS qwerty12345
   3987 31.292490 23.229...  192.168...  FTP         137 Response: 230-Your bandwidth usage is restricted
   3988 31.292636 192.168... 23.229...   FTP          60 Request: SYST
   4015 31.376230 23.229...  192.168...  FTP          73 Response: 215 UNIX Type: L8
   4017 31.376672 192.168... 23.229...   FTP          60 Request: FEAT
   4062 31.460785 23.229...  192.168...  FTP         294 Response: 211-Extensions supported:
   4063 31.461038 192.168... 23.229...   FTP          68 Request: OPTS UTF8 ON
   4091 31.544439 23.229...  192.168...  FTP          77 Response: 200 OK, UTF-8 enabled
   4092 31.545253 192.168... 23.229...   FTP          59 Request: PWD
   4111 31.628813 23.229...  192.168...  FTP          88 Response: 257 "/" is your current location
   4112 31.631434 192.168... 23.229...   FTP          62 Request: TYPE I
   4147 31.715559 23.229...  192.168...  FTP          84 Response: 200 TYPE is now 8-bit binary
   4148 31.715697 192.168... 23.229...   FTP          60 Request: PASV

0000  00 1b ed b7 7d 00 b8 ca  3a 87 53 a1 08 00 45 00   ....}... :.S...E.
0010  00 3a 6a 80 40 00 80 06  00 00 c0 a8 05 02 17 e5   .:j.@... ........
0020  94 86 e3 92 00 15 ec e0  9b b8 31 01 f0 0d 50 18   ........ ..1...P.
0030  3f f5 72 42 00 00 50 41  53 53 20 71 77 65 72 74   ?.rB..PA SS qwert
0040  79 31 32 33 34 35 0d 0a                            y12345..

File Transfer Protocol (FTP): Protocol    Packets: 4183 · Displayed: 16 (0.4%) · Load time: 0:0.79    Profile: Default
```

Figure 3: Wireshark capturing FTP traffic.

3. Analyze a .pcap file to provide host and destination IP addresses, sequence numbers, header length and window size using Wireshark.

4. Duplicate the entire website using the HTTrack tool.

5. Specific to the FTP protocol, the student will analyze a .pcap file for FTP traffic like username, password, names of files transferred and destination folder using Wireshark.

2.4 Encryption Lab

Students will learn basic encryption processes like Caesar, Vigenère and Playfair ciphers (Figure 4). These processes serve as the base for more advanced techniques such as Blowfish and Gost encryption algorithms. In this lab, students will *apply* CryptoForge to solve highly advanced algorithms. A very important part of this lab is the usage of a web application that shows a step by step encryption/decryption process of the DES algorithm. As a result, students will be able to identify weak encryption keys. Hashes allow students to learn how to detect files that have been modified or corrupted. During a second part of this lab, students will learn how to calculate hash values of files. To accomplish this, on Windows machines they will use the HashCalc tool, while on Linux, they will use built-in commands.

To do this, student will perform the following tasks:

1. Students will access the Caesar, VigenÃÍre and Playfair ciphers online and will answer questions related to this in the assessment.

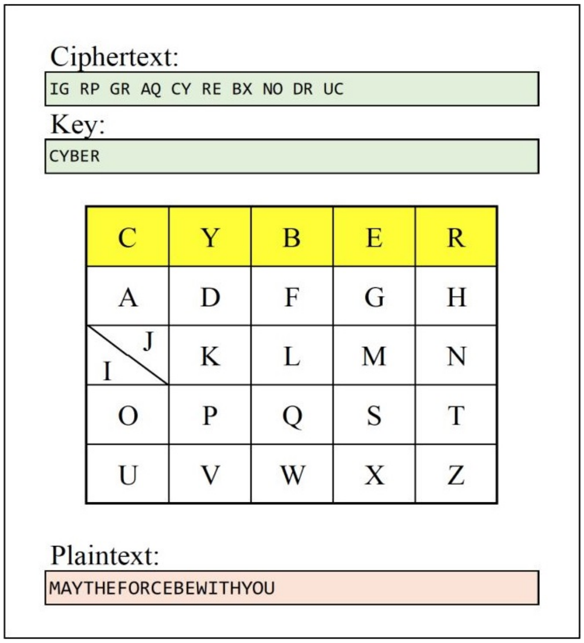
2. Install the CryptoForge tool.

3. Encrypt and decrypt files by using any of the following algorithms found in CryptoForge: Blowfish, Rijndael, TripleDES or Gost.

4. Identify the weak keys for the DES algorithm using the web application.

5. Install the HashCalc tool.

6. Calculate the ADLER32, MD5, SHA-1 and SHA-512 hashes of a given file using the HashCalc on a Windows machine.



Ciphertext:

IG RP GR AQ CY RE BX NO DR UC

Key:

CYBER

C	Y	B	E	R
A	D	F	G	H
J I	K	L	M	N
O	P	Q	S	T
U	V	W	X	Z

Plaintext:

MAYTHEFORCEBEWITHYOU

Figure 4: Playfair Cipher decryption process.

7. Calculate the MD5, SHA-1, SHA-256, SHA-512 hashes of a given file on a Linux machine using commands.

2.5 Password Cracking Lab-Windows only

The objective of this lab is for students to use the ophcrack tool to determine what is the password used by a specific username in a Windows machine. To do this the students will need to complete two steps: *extract* the Security Account Manager (SAM) database file from the user's Windows machine using the pwdump7 tool and *decrypt* hashes from the SAM into readable passwords.

To do this, students will perform the following tasks:

1. Install the pwdump7 tool.

2. Extract the SAM using the pwdump7 tool.

3. Install the ophcrack tool.

4. Load the rainbow table and the SAM file to the ophcrack tool.

5. Run the ophcrack tool (crack) to obtain the possible plaintext passwords for that username.

2.6 Web Server Vulnerabilities Lab

This lab covers the use of Wpscan and Metasploit tools to find vulnerabilities placed in a local web server. Furthermore, the student will learn how to *patch* these vulnerabilities until the web server is secured.

To do this, students will perform the following tasks:

1. Launch Wpscan from a Kali machine.

2. Using the Wpscan tool, scan the Wordpress website located inside the local web server to find the PHP and the Wordpress version numbers, installed plugins and usernames.

3. Launch Metasploit and select the “wordpress-login-enum” auxiliary module.
4. Load the PasswordList.txt file to perform a dictionary attack.
5. Login to the Wordpress website using the obtained credentials.

3. EXPECTED RESULTS

It is expected that a combination of a virtual environment and active learning will positively impact student’s learning of a computer security introductory course. In addition, this course design will allow students to interact and share their findings with other students by providing hands-on experience using real tools in a controlled environment.

4. REFERENCES

[1] J. Duffany. Active learning applied to introductory programming. In *Proceedings XIII Latin American and Caribbean Conference for Engineering and Technology*, July 2015.

[2] A. F. Smeaton. Using hypertext for computer based learning. *Computers Education*, 17(3):173–179, August 1991.

[3] J. C. Wang, W. F. Cheng, H. C. Chen, and H. L. Chien. Benefit of construct information security environment based on lightweight virtualization technology. In *2015 International Carnahan Conference on Security Technology (ICCST)*, pages 1–4. University of Texas, September 2015.

[4] C. Willems, W. Dawoud, T. Klingbeil, and C. Meinel. Security in tele-lab – protecting an online virtual lab for security training. In *2009 International Conference for Internet Technology and Secured Transactions, (ICITST)*, pages 1–7, November 2009.

[5] C. Willems, T. Klingbeil, L. Radvilavicius, A. Cenys, and C. Meinel. A distributed virtual laboratory architecture for cybersecurity training. In *2011 International Conference for Internet Technology and Secured Transactions*, pages 408–415, December 2011.

[6] D. Wu, J. Fulmer, and S. Johnson. Teaching information security with virtual laboratories. In *Innovative Practices in Teaching Information Sciences and Technology: Experience Reports and Reflections*, pages 179–192. Springer International Publishing, January 2014.

[7] T. Zlateva, L. Burstein, A. Temkin, A. MacNeil, and L. Chitkushev. Virtual laboratories for learning real world security. In *12th Colloquium for Information System Security Education.* University of Texas, June 2008.