



Arkansas Delta Information Systems and Cyber (DISC) Education Initiative



NSF Grant No. 1901877

Principal Investigator: Cindy Grove – cgrove@pccua.edu

Co-Principal Investigator: Arthur Gentry – agentry@pccua.edu

Co-Principal Investigator: Monica Quattlebaum – monica@pccua.edu

Cover Page

Virtualization Software Infosec Learning and Virtual Labs

Infosec Learning Labs are remote virtualization software that Instructors have implemented into the curriculum. Labs are developed for each course and specific curriculum components. These labs allow 24/7 access for students to complete assignments and it also allow students to practice skill sets in courses with high tech curriculum in Cybersecurity, Networking, Programming, and Servers. Other Virtual Labs and simulations are used to reinforce learning and allow students to practice skill sets.

Phillips Community College of the University of Arkansas
P.O. Box 785 | 1000 Campus Drive
Helena-West Helena, Arkansas 72342
Phone: (870) 338-6474 | Fax: (870) 338-7543

Infosec Learning Labs – Example Screen Shots

The screenshot shows a web browser window at lab.infoseclearning.com/labs. The page features a dark red header with the text "Infosec Learning" and buttons for "Edit Account" and "Log out". Below the header, the user is identified as "Hello Charlotte Purdy". The main content area is titled "Your Labs" and includes a "Link Course to Instructor" button. A list of labs is displayed, including "3.3.1 - 5-JRSS NETWORK ADMINISTRATOR" and "JBCE Router Delegated Administrator". A section titled "ETHICAL HACKING AND SYSTEMS DEFENSE" lists various topics such as "Performing Reconnaissance from the WAN", "Scanning the Network on the LAN", "Enumerating Hosts Using Wireshark, Windows, and Linux Commands", "Remote and Local Exploitation", "Crafting and Deploying Malware Using a Remote Access Trojan (RAT)", "Capturing and Analyzing Network Traffic Using a Sniffer", "Social Engineering Using SET", "Performing a Denial of Service Attack from the WAN", "Using Browser Exploitation to Take Over a Host's Computer", "Attacking Webservers from the WAN", "Exploiting a Vulnerable Web Application", "Breaking WEP and WPA and Decrypting the Traffic", "Attacking the Firewall and Stealing Data Over an Encrypted Channel", "Using Public Key Encryption to Secure Messages", and "Performing SQL Injection to Manipulate Tables in a Database". The Windows taskbar is visible at the bottom of the browser window.

The screenshot displays the "CentOS Server Linux Installation" lab page. The browser address bar shows lab.infoseclearning.com/lab/centos-server-linux-installation. The page has a dark red header with the lab title and a "STOP" button. A "Time remaining: 84:16" indicator is present. The main content area is divided into sections: "BEFORE YOU BEGIN" with a warning about browser compatibility, "LINKING TO INSTRUCTORS" with a numbered step, and "INTRODUCTION" with an overview. A large graphic on the right side of the page shows a server tower with the text "CentOS Server" and the IP address "192.168.1.2". A smaller inset window titled "Introduction to File Systems" is visible, showing a "Link Course to Instructor" button highlighted with a purple arrow. The Windows taskbar is also visible at the bottom.

Example of Blackboard Course – Module assignment page

Weekly Assignments > Module 6

Success: Desktop Virtualization - InfoSec Learning Lab edited.

Module 6

Build Content | Assessments | Tools | Partner Content

- Module 6 Discussion**
- Module 6 Reading**
Read "Troubleshooting Windows Startup."
- Lab 6-1: Rolling Back Device Drivers**
Software Simulation Powered by LabConnection.
- Lab 6-2: Using Windows Startup Repair**
Software Simulation Powered by LabConnection.
- Module 6 Test**
Test your understanding of the A+ exam objectives covered in this module with this multiple-choice practice exam.
- Desktop Virtualization - InfoSec Learning Lab**

COURSE MANAGEMENT

- Control Panel
- Content Collection
- Course Tools
- Evaluation