First Laboratory Experience for Cyber Engineering and Cybersecurity Students

Fong Mak[1]
[1]Gannon University. Erie
Pennsylvania
USA
mak001@gannon.edu

***ABSTRACT*: *This paper outlines the lab exercises designed as the first hands-on experiences for Cyber Engineering and Cybersecurity students. The lab exercises allow students to gain hands-on experience to support their understanding of networking technologies with security concerns in using network components and software applications. This one-credit lab experience course effectively covers the additional topics in the first-year course in Introduction to Networks to fully cover the foundational knowledge units needed to prepare students in other cyber courses in the curriculum. The designed hands-on exercises aim to enhance students' experience in PC technologies, FTP, Telnet, SSH, network building, switches, routers, VLAN, and network traffic analysis.*

Keywords: Cybersecurity, Cyber Engineering, Network Security Laboratory, Cyber Lab, Fcar, Evaltools

Received: 3 June 2021, Revised 20 October 2021, Accepted 1 November 2021

DOI: 10.6025/isej/2021/8/2/39-64

1. Introduction

The Dean of Engineering and Business appointed the author in 2018 to lead a faculty team from both the *Electrical and Computer Engineering* (ECE) and *Computer and Information Science* (CIS) to prepare an academic proposal to create two new programs in response to the market needs in cyber engineering and cybersecurity. The two new programs are (1) Cyber Engineering and (2) Cybersecurity. The Cyber Engineering program builds on the existing Computer Engineering curriculum among the two new programs. The current Computer Engineering option will be replaced if the new Cyber Engineering program is approved, effective in the 2019-2020 academic year. The school administrators so well received the proposal that Gannon has decided to invest resources for a new building designated as *Institute for Health and Cyber Knowledge*, I-HACK, Center. To support the programs, the author led the effort to design and develop the curriculums that consist of four designated physical labs for the Cybersecurity program and one for the Cyber Engineering program. The four physical labs for cybersecurity are Hacking Lab, Defense Lab, Cyber Teaching Lab, and Cyber Innovation Lab.

One of the goals in developing these two programs is to nurture synergized activities and potential entrepreneur development between these two groups of students. Each program's curriculum independently meets its *Accreditation Board for Engineering and Technology* (ABET) requirements in student outcomes and necessary subject matters [1,2] in *Engineering Accreditation*

Commission (EAC) and *Computing Accreditation Commission* (CAC), respectively. Hence, curricula of both programs share some essential topics in their first and second years; in particular, the following courses are considered common core to both programs: CIS290 Introduction to Networks, CIS219 Linux Programming, CYBER210 IT Security, ECE228 Circuits 1, and ECE111 Introduction to C/C++.

The two programs were first inaugurated in fall 2019. The author first taught *CIS290* in fall 2019 and adopted the book: *CompTIA Network+ Certification* by Meyers [3]. The author soon realized that students could not fully appreciate the concept covered in CIS290 because they lacked hands-on experience with computer and software usage. The author then developed *CYSEC 101 Network Security Lab* as the first laboratory experience added to the common core to both programs. The lab course was in place the following semester (spring 2020) to gain the needed experience before students move on to the rest of the curriculum.

1.1 Are there First-Year Laboratories Available?

Cybersecurity is a hot new discipline. There are quite a few resources [4, 8] geared toward penetration testing, wireless networks, computer security, or internet security for upper-level students in their junior or senior year. There are also *National Science Foundation*, NSF,-sponsored projects for resources that make available for the educators, such as GENI, *Global Environment for Network Innovations*. GENI provides virtual laboratory networking and distributed innovations in network science, security, services, and applications [9]. GENI provides a good infrastructure, but not the lab exercises. SEED labs, another NSF-sponsored project to develop hands-on laboratory exercises for computer and information security education and help instructors adopt these labs [10]. SEED labs are also more appropriate for upper-level students. Another popular platform for building and sharing free cybersecurity curricula is the *Cybersecurity Labs and Resource Knowledge-based* (CLARK), an *National Security Agency* (NSA)-sponsored project [11]. In CLARK, there are nanomodule, i.e., two or three lab exercises in network security, and a complete set of lab exercises in wireless network security labs for upper-level students.

Many university groups explored methods of teaching information security, designing and setting up laboratory infrastructures to support learning and teaching reported in [12-18]. Ref [12] documents how Georgia Tech establishes a hands-on network security laboratory that allows students to apply defensive and offensive strategies in the network. Ref [13] presents a cloud-based virtual laboratory education platform called V-lab that facilitates building a private network system from introductory to advanced levels for a progressive curriculum. Ref [14] presents a laboratory-based course on internet security that aims at senior undergraduates. Micco and Rossman [15] establish a laboratory where students learn penetration testing techniques and hardening networks against attacks. Frank and Wells explain in [16] laboratory exercises specific for a computer security course. Ref [17] documents SEED labs for students to learn the principles of security vulnerabilities, attacks, and countermeasures. Ref [18] expands SEED labs to include vulnerability scanning tools, analyzing malware, and so on. However, the various laboratories setup reported in [12-18] is not designed for the first-year experience that the author aims to provide. There is commercial software that supports topics in CIS290 and prepares students for the Network+ certification, but commercial resources are not an option to us. The author developed this first-year lab mainly because the author could not identify any relevant developed published lab exercises suitable for first-year students.

2. Overview of Paper and Design Methodology

The following sections of the paper cover the rationale for the topics and methodology for teaching and delivery strategy for the lab. The intent is not to cover every detail of instructions for the lab exercises but instead on the design philosophy and approach so that readers can add or remove details should they decide to implement some of the topics in their program.

The author adopted the concept of Quality Function Deployment, QFD, in designing the lab activities for CYSEC01. QFD is a widely used approach in engineering product design. QFD identifies the intended outcomes for students (customers), translates results into measurable design targets, and drives the design activities to meet the needs and expectations. QFD design approach aligns with the best practice of backward design for academic courses to identify desired results, determine acceptable evidence, and plan learning experiences and instructions [19,20]. In addition, since the programs adopt *Faculty Course Assessment Report*, FCAR, methodology [21] to collect student artifacts as objective evidence to support the preparation for ABET accreditation, FCAR methodology is deployed throughout the entire curriculum. FCAR presents a streamlined method that allows instructors to write assessment reports in a concise, standardized format conducive to course and student outcomes assessment. The central idea of FACR, instructors plan ahead of the learning experience and supporting evidence for each targeted learning outcome, compile course portfolio in delivering the teaching, evaluate the learning at the end of the semester. FCAR approach uses a performance vector that classifies student learning performance into four categories: Excellent (E), Adequate (A), Minimal (M), and Unsatisfactory (U), which form the EAMU performance vector. The results are flagged with different colors according to heuristic rules which indicate the academic status. Ref [21] gives a detailed report on the FCAR methodology for performance vectors and heuristic rules and the variations of FCAR deployment in three universities. We further explain in more detail how FCAR is used in CYSEC 101 in Section 2.3.

The following section examines the motivation for creating the first lab experience needed for both programs. Next, we discuss the CIS290 course content that led to the design of the first lab experience. Section 3 focuses on the lab design methodologies, supporting resources, and description of each lab exercise. Finally, we review the assessment data in Section 4 and finish by concluding remarks on what was accomplished in Section 5.

2.1 The Rationale for the First Lab Experience

One of the goals of the cybersecurity program is to prepare students for related professional certification before they graduate from the program. The first logical choice of a certification exam is the CompTIA Network+ Certification. Hence, we cover relevant topics in CIS290 and provide students a way to be familiar with the examination format and hands-on experience to support the understanding of key concepts covered in CIS290. Here we first review the contents to be covered in CIS290.

The contents covered in the adopted text for CIS290 are extensive as follows, Table 1:

1	Network Models	2	Cabling and Topology
3	Ethernet Basics	4	Modern Ethernet
5	Installing a Physical Network	6	TCP/IP Basics
7	Routing	8	TCP/IP Application
9	Network Naming	10	Securing TCP/IP
11	Advanced Networking Devices	12	IPv6
13	Remote Connectivity	14	Wireless Networking
15	Virtualization and Cloud Computing	16	Mobile Networking
17	Building a Real-World Network	18	Managing Risk
19	Protecting Your Network	20	Network Monitoring
21	Network Troubleshooting		

Table 1. Content Topics of CIS290

Everyone who has taken this subject matter in the past will find out the current network course CIS290 contains many more topics. There is no way to cover all these topics in one semester. Hence, we often opt to deliver this course as a theoretical course, perhaps, with one or two hands-on assignments to keep students interested in the class. In our case, we target to cover the first twelve topics in CIS290. The assignments mimic those quantitative questions in an actual Network+ Certification Examination and qualitative questions to further focus on issues that can be better served with an explanation or description. There are many good resources on practice tests that give samples of Network+ Certification, and the author uses relevant samples from Ref [22] as a resource for assignments for the class. The CSEC2017 [23] guideline is a good reference source for the qualitative questions.

However, topics 13 to 21 are equally important and need to be covered to provide a complete overview of essential foundational network knowledge as a basis for the other classes. In addition, there are minimal existing lab exercises for first-year students. Therefore, the author decided to develop the first lab experience for cyber students to achieve the following goals:

1. Gain knowledge in topics of 13 and 21

2. Gain hands-on experience and be familiar with PC technologies, including hands-on experience in disassembling and assembling a computer.

3. Ability to source the right parts of a computer to meet specific criteria

4. Ability to install Operating Systems or Server applications

5. Investigate case studies of cybersecurity

6. Use of resources that are not restricted to the physical lab

2.2 Delivery format and topics

This CYSEC101 course focuses on hands-on experience for students to expand and deepen their knowledge gained in networking, be familiar with essential tools used in cybersecurity, and give students some experience with crucial network analysis tools.

The course outcomes (CO) are:

- CO1: Design a basic network architecture given a specific need and set of hosts/clients.
- CO2: Track and identify the packets involved in a simple TCP connection (or a trace of such a connection)
- CO3: Use network monitoring tools (e.g., a network protocol analyzer like WireShark) to observe the flow of packets
- CO4: Perform network mapping (enumeration and identification of network components) (e.g., Nmap, a network mapping tool)
- CO5: Describe the hardware components of modern computing environments and their functions.

Traditionally, a lab is designated as a 3-hour long session and once a week for a one-credit lab. We schedule this lab course to be two-session per week and an hour and a half long each session. By doing so, students will have a better attention span for the lab session and have a breathing room to digest what they learned in the previous session for questions if needed. Depending on the topics covered, the author adopted a hybrid model of hands-on and lecture-oriented sessions for this lab. Besides topics 13 thru 21 covered in lecture-oriented sessions, we designed eight hands-on exercises to achieve the course outcomes. The lab exercises are:

1. Lab1: Familiarization with PC Technology

2. Lab2: Setting up a lab environment and commonly used tools

3. Lab3: Use of Wireshark for capturing and analyzing security in telnet/SSH traffic

4. Lab4: Port Forwarding

5. Lab5: Configure and investigate FTP traffic using Wireshark

6. Lab6: Packet tracer introduction

7. Lab7: Building a simple network

8. Lab8: VLAN implementation and security consideration

2.3 Course Assessment Methodology

For this paper, we focus only on assessing course outcomes, not the student outcomes associated with the program for ABET accreditation. To make life easier for instructors, we adopt EvalTools® [24] as our Outcomes Assessment System, OAS, in addition to our Learning Management System (LMS) for classroom teaching. Figure 1 shows the portion of the course syllabus that pertains to the course outcomes assessment. Figure 1 spells out the key assignment selected as evidence and its justification for each course outcome. Given Figure 1, it is clear which key assignments are selected and why and how they are used to assess how well we achieve our course outcomes. Each key assignment is graded against a score-based rubric vector, EAMU as described in Figure 1. One could use Excel to track the scores for each key assignment and compile the EAMU vector accordingly. However, EvalTools® offers FCAR as part of its assessment toolsets. After instructors uploaded the graded key assignments, EvalTools® composes the course portfolio for program review and compiles the data into EAMU with color-coded results for formative and summative evaluation of course outcomes. With EvalTools®, instructors focus on designing the key assignments and teaching instead of collecting and compiling data for later evaluation. More thorough coverage of constructing a well-form syllabus that includes selecting key assignments and their justification is reported in [25,26]. Ref [21] documents how the EAMU average is being computed. More complete applications and illustration of the EAMU vector and its

The course objectives and the corresponding student outcomes are assessed using the EAMU vectors. The construction of the EAMU vectors used for course assessment applies the following scoring in all cases: Excellent (E) is scoring 90 or better of the total points possible, Adequate (A) is 75 or better, Minimal (M) is 60 or better, and Unsatisfactory (U) is anything below 60.

• **CO1:** Design a basic network architecture given a specific need and set of hosts/clients.

Key Assignments: Lab 8: *VLAN implementation and security consideration*
Justification: Lab8: Question 1 and Question 6 requires students to design a network using Packet Tracer, implement security practices, and discuss the security issue to the switches involved. Hence it serves as a gauge of skills for CO1.

• **CO2:** Track and identify the packets involved in a simple TCP connection (or a trace of such a connection)

Key Assignments: Lab5: *Configure and investigate FTP traffic using Wireshark*
Justification: Lab5 Question 3 requires the student to use Wireshark to analyze and capture the vulnerability of transmission using FTP. Hence it is used as a gauge to measure skill in CO2.

• **CO3:** Use network monitoring tools to observe the flow of packets (e.g., WireShark)

Key Assignments: Lab 3: *Use of Wireshark for capturing and analyzing security in telnet/SSH traffic*
Justification: Lab3 Question 3 requires the student to address the issue they observed in the package flow for Telnet traffic vs. SSH traffic and identify/compare the security concern for both Telnet and SSH. Hence it serves as a gauge of skills in CO3.

• **CO4:** Perform network mapping (enumeration and identification of network components)

Key Assignments: Assignment 3: Host discovering with Nmap
Justification: Assignment 3: Question 6 is a non-hands-on exercise that requires students to apply Nmap to perform a host discovery, i.e., to enumerate open ports in a network and discuss the use of Nmap for network monitoring. Hence it serves as a gauge of skills in CO4.

• **CO5:** Describe the hardware components of modern computing environments and their functions.

Key Assignments: Lab 8: VLAN design
Justification: Lab 8: Question 1 requires students to design a VLAN and discuss each component's functionalities in that network. Hence it serves as a gauge of skills in CO5.

Key Assignments: Lab 1: PC Technology
Justification: Lab 1: Question 6 requires students to identify and summarize the function of the key components in a PC. Hence it serves as a gauge of skills in CO5.

Figure 1. Course assessment portion of the syllabus

roll-up to form a PVT, Performance Vector Table, of FCAR methodology applied to program assessment in addition to course assessment, is reported in [27]. We examine the FCAR results in Section 4.

We should note that cybersecurity is a fast-moving field regarding its technologies and software development. With the adoption or creation of IoT, the Internet of Things, devices, even more topics will be added to the list to be covered as foundational knowledge. Hackers will continue to develop better hacking software, so do we, as cybersecurity defenders. As a result, a more advanced version of software or equivalent will likely replace whatever software is used in the implemented lab exercises.

However, what is new here is that we implemented a hybrid model that mixes lectures with lab exercises in one credit-hour lab course that provides an alternative to the traditional long three-hour lab. The assessment methodology and topics selected will likely be applicable for the foreseeable future.

3. Hands-on Exercises

We cover the eight hands-on exercises in detail in this section.

3.1. Lab1: Familiarization with PC Technology

This exercise allows students to get familiar with PC technology and physical handling with a PC. It is common to observe that most cyber first-year students have little or no hands-on experience with PC technology. Most students have experience with Microsoft Office in their high school, but few know the PC technology. We use old PCs from the ECE lab for this lab exercise, and all the old PCs are functional. Before students began the disassembling, we went thru a short video clip on "How to disassemble a PC?" We introduced essential PC components like CPU, memory, motherboard, hard drives, power supply, connector types, and general lab safety measures in dealing with IC components. The following are the objectives and instructions provided to students:

Objectives:

- Identify essential components of a PC

- Techniques to disassemble and assemble a PC

- Source the right parts for a PC

Lab instructions:

- Identify the PC manufacturer and download the corresponding manual from the website.

- Be familiar with the PC disassembling process from the manual

- Pay attention to the power switch and static charge throughout the physical handling of the PC case

- Take a photo of the original wiring layout, connections, and component configuration so that you know of the expected end-result

- Identify essential components and take a snapshot of them for submission

- Keep your tool neat, organized, and next to you.

- After removing the parts, take a snapshot of each and submit the image to EvalTools [24].

- Put the parts back in reverse order

- Power on to see if the PC's OS comes back alive. If it is, your reassembling and assembling process is successful.

We use EvalTools as our LMS for this class. Students submit their work to EvalTools so that EvalTools can compile course portfolios for faculty that we can use later for program assessment. The following are the questionnaires for this lab exercise:

Q1. Upload the image of a motherboard

Q2. Upload the image of the CPU, and describe the model number and type

Q3. Upload the image of memory, and describe the model number and type

Q4. Upload the image of the power supply, and spell out the wattage rating

Q5. Upload the image of the hard drive, and describe the type and capacity

Q6. What other parts that are not uploaded as images, CPU cooler, video card, something else you found

Q7. Please use pcpartpicker.com to help you put a PC together: You are given a budget of 1000 dollars and must use AMD Ryzen 5 3600 as the CPU. Please complete the selection of components for a PC.

Question 7 requires students to source the right parts of a PC with the aid of the site: www.pcpartpicker.com [28]. Ref [28] is a good source for picking PC parts as the site provides a warning message if a student chooses an incompatible part. Also, by this time, students already have some ideas of PC parts, but to learn more on the compatibility issues among PC parts. For example, not all motherboards will work for the selected CPU once a CPU is selected. The following are general concepts discussed in class for this Question 7:

- Number of cores vs CPU speed

- The form factor of a mother and its case selection

- Memory type and its sizing

- Hard storage and its sizing

- Compatible video card and its speed

3.2 Lab2: Setting up a lab environment and commonly used network monitoring tool

Wireshark Setup: We introduce WireShark [29], a network protocol analyzer, as the first software toolset before setting the virtual lab environment. A sequence of WireShark [30] videos is a good resource for students. The author walked thru the following topics in one session using PowerPoint and walk-thru activities.

- Installation

- Overview of Wireshark environment

- Caption options

- Toolbar icons

- Filters

- More interface controls

- What is a packet

- TCP 3-way handshake as example

WireShark is available for download at www.wireshark.org. Setting up WireShark and later lab environment is a walk-thru activity with students as some students lack experience in software installation. A live walk-thru of downloading and installing Wireshark and pausing at each step is necessary to ensure all students are at the same pace.

VirtualBox Setup: We decided to use VirtualBox. VirtualBox is a general-purpose virtualization tool targeted at servers and desktops that allows users to run multiple guest operating systems on a single host efficiently. VirtualBox is freely available. Installing a VirtualBox is relatively straightforward by following the instructions during installation. Students can install it as many times as they wish on their PCs or laptops. VirtualBox is available for download at www.virtualbox.org [31].

Ubuntu Server Setup: We chose to use Ubuntu, the most widely used open-source operating system on Linux for the server, and simply go to Ubuntu.com [32] to download the latest stable long-term release (LTS) version of Ubuntu Server, such as the 20.04 LTS iso file. We opted to have students download directly from the source as part of the exercises. Students need to know where the source of the software we used in the lab. We also ask students to create a folder: Resource to keep all their downloads. Most students are likely to install a server for the first time, and installing a server is more involved than a computer OS.

1. Create a virtual instance – We make students aware that this process is the same as setting up physical server hardware that includes defining memory size, hard disk, hard-disk file type, and storage size.

2. Install the Server OS – at this step, we make students aware that they are to load the iso image via an external disk much the same as the physical loading an iso disk for OS installation. For this lab, we stayed with the default setting for the network, i.e., NAT (Network Address Translation) network.

As students power up the instance with the iso imaged loaded, students follow online instructions for installation. Students also install SSH as part of the process.

Telnet setup: activate the Ubuntu server instance, then execute the following commands in a command terminal to install telnet service on the Ubuntu Server.

• *sudo apt-get update* — update the server first

• *sudo apt-get upgrade* – update packages first

• *sudo apt-get install telentd –y* (install telnet server)

• *sudo systemctl status inetd* (start internet superserver)

• *sudo apt install net-tools* (you need it to use ifconfig command)

• *ifconfi*g (your ip address should be 10.0.2.x)

Test out Telnet and SSH connection

Students install PuTTy [33] from www.putty.org. For the host PC to make a connection to the VM instance via Telnet or SSH, students set the network connection of the VM to “Host-only Adapter” (Settings -> Network -> Adapter 1, then choose Host-only Adapter).

• With PuTTy running, navigate to Session -> choose Telnet for the connection type. PuTTy indicates port 23 for Telnet and 22 for SSH. Students should be aware of the default port for Telnet and SSH. With Telnet selected, enter the IP address of the VM. Use the command “ifconfig” on the VM; the corresponding IP should be 192.168.56.x. We make students aware that the VM is now on the same domain as the host. When Telnet into the Ubuntu server, we enter the user name and password. To exit, use “Ctl-C.”

• Repeat the process with SSH connection using PuTTy. The only difference is that students may be asked to accept the certificate initially to connect to the server.

· Students are to capture screenshots for submission to verify that they successfully connect the Telnet and SSH connection.

3.3 Lab3: Use of Wireshark for capturing and analyzing security in Telnet/SSH traffic

This exercise allows students to get familiar with investigating network traffic using Wireshark and identifying the security in Telnet protocol. Students are to address the critical Question 3 below by first capturing the network traffic in Telnet and SSH and better understanding the differences in these two protocols.

Q1. Please capture the steps with proper screenshots when you engage a Telnet connection and use Wireshark to capture the corresponding traffic in connection

Q2. Please capture the steps with proper screenshots when you engage an SSH connection and use Wireshark to capture the corresponding traffic in the connection

Q3. Explain why transmission attacks can often be viewed as connection attacks on network components. Please give a specific example or case study to support your claim

Capture Telnet traffic

- Set the Network adapter to “Host-only Adapter” so that it can communicate directly with the host.

- Activate the Ubuntu server and identify its ip address: (1) *ifconfig* — to identify Ubuntu server ip address.

- Activate Wireshark and select the proper connection to monitor its traffic on the host to the virtual Ubuntu server.

- Activate PuTTY on the host; initiate Telnet session connection to Ubuntu server; and enter the proper credentials

- Stop Wireshark for capturing traffic.

- Analyze Telnet traffic. Be sure to use “follow TCP stream” to see the user name and password in the Telnet session.

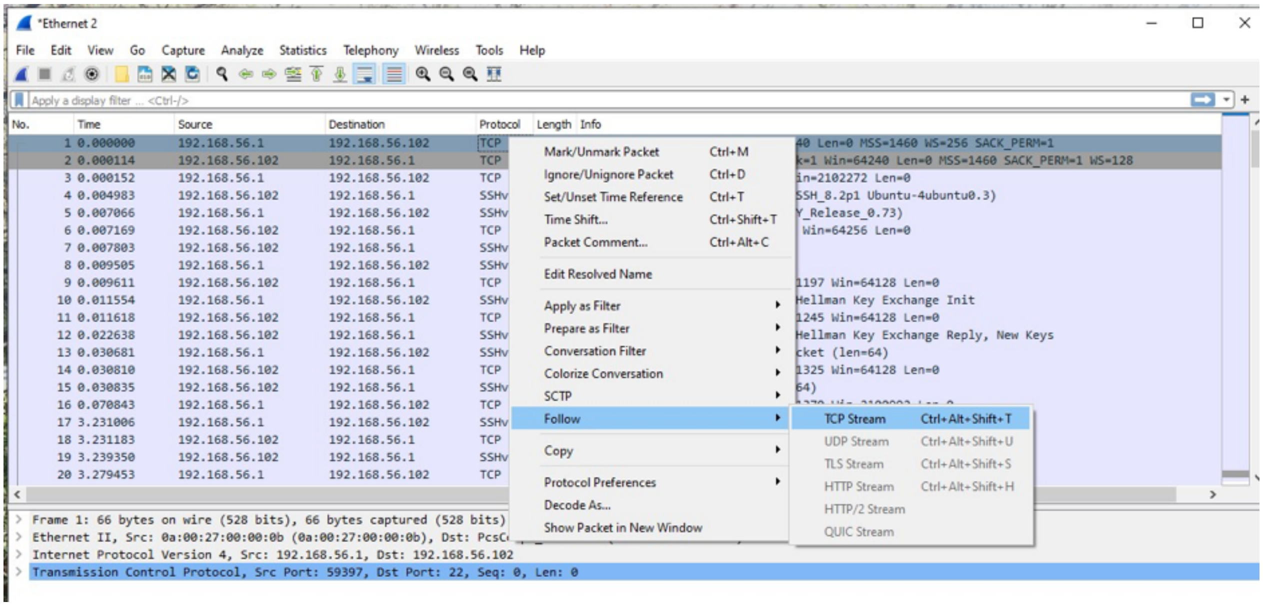
Figure 2 shows screenshots of the Telnet traffic in clear text captured by Wireshark. It is straightforward to identify the user credential, as indicated in Figure 2.

Capture SSH traffic

- Repeat the above but with SSH connection using PuTTY.

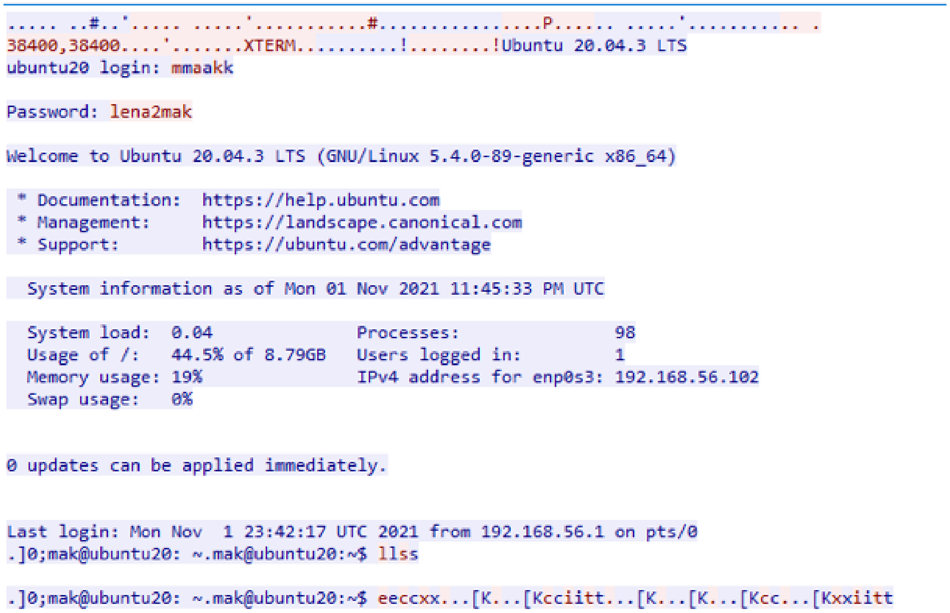
- Capture the relevant steps of an SSH session with Wireshark capture, and upload the results to EvalTools®.

The captured traffic is encrypted text with SSH, and the user credential is not identifiable. Students show excitement in class when they realize they can monitor network traffic to identify users’ credentials in Telnet but not in SSH.


*Ethernet 2
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.56.1	192.168.56.102	TCP		40 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000114	192.168.56.102	192.168.56.1	TCP		k=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
3	0.000152	192.168.56.1	192.168.56.102	TCP		in=2102272 Len=0
4	0.004983	192.168.56.102	192.168.56.1	SSHv		SSH_8.2p1 Ubuntu-4ubuntu0.3)
5	0.007066	192.168.56.1	192.168.56.102	SSHv		Y_Release_0.73)
6	0.007169	192.168.56.102	192.168.56.1	TCP		Win=64256 Len=0
7	0.007803	192.168.56.102	192.168.56.1	SSHv		
8	0.009505	192.168.56.1	192.168.56.102	SSHv		
9	0.009611	192.168.56.102	192.168.56.1	TCP		1197 Win=64128 Len=0
10	0.011554	192.168.56.1	192.168.56.102	SSHv		Hellman Key Exchange Init
11	0.011618	192.168.56.102	192.168.56.1	TCP		1245 Win=64128 Len=0
12	0.022638	192.168.56.102	192.168.56.1	SSHv		Hellman Key Exchange Reply, New Keys
13	0.030681	192.168.56.1	192.168.56.102	SSHv		cket (len=64)
14	0.030810	192.168.56.102	192.168.56.1	TCP		1325 Win=64128 Len=0
15	0.030835	192.168.56.102	192.168.56.1	SSHv		64)
16	0.070843	192.168.56.1	192.168.56.102	TCP		
17	3.231006	192.168.56.1	192.168.56.102	SSHv		
18	3.231183	192.168.56.102	192.168.56.1	TCP		
19	3.239350	192.168.56.102	192.168.56.1	SSHv		
20	3.279453	192.168.56.1	192.168.56.102	TCP		

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: 0a:00:27:00:00:0b (0a:00:27:00:00:0b), Dst: PcsC
> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.102
> Transmission Control Protocol, Src Port: 59397, Dst Port: 22, Seq: 0, Len: 0
```



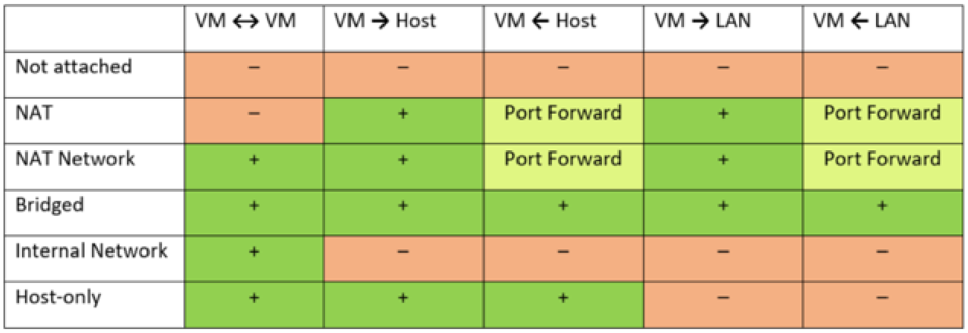
```
..... ..#..'..... .....'...........#................P...... .....'........... .
38400,38400....'.......XTERM..........!........!Ubuntu 20.04.3 LTS
ubuntu20 login: mmaakk

Password: lena2mak

Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon 01 Nov 2021 11:45:33 PM UTC

  System load:  0.04              Processes:               98
  Usage of /:   44.5% of 8.79GB   Users logged in:         1
  Memory usage: 19%               IPv4 address for enp0s3: 192.168.56.102
  Swap usage:   0%


0 updates can be applied immediately.


Last login: Mon Nov  1 23:42:17 UTC 2021 from 192.168.56.1 on pts/0
.]0;mak@ubuntu20: ~.mak@ubuntu20:~$ llss

.]0;mak@ubuntu20: ~.mak@ubuntu20:~$ eeccxx...[K...[Kcciitt...[K...[K...[Kcc...[Kxxiitt
```

Figure 2. Telnet traffic captured screenshots

3.4. Lab4: Port Forwarding

This exercise follows after a lecture-oriented virtualization technologies session on the bare-metal hypervisor, a type 1 hypervisor that runs directly on the host machine's physical hardware, and a Type2 hypervisor that runs on top of an operating system. VirtualBox is an excellent example of a Type 2 Hypervisor. Ref [34] gives a rather thorough description of each network adapter. Table 2 summarizes the network modes supported by VirtualBox and how the VM relates to the host and the local area network (LAN). We use only a NAT network adapter to keep activities simple for this lab.

Students learn to create a forwarding rule that allows traffic to be forwarded to the virtual machine (VM) Server from the host machine on port 8022 instead of port 22. In NAT mode, the host or other machines in the network cannot access the VM. Hence, we use NAT to illustrate the concept of port forwarding. The exercise further supports port forwarding to access particular network services hidden behind the NAT from external networks.



	VM ↔ VM	VM → Host	VM ← Host	VM → LAN	VM ← LAN
Not attached	–	–	–	–	–
NAT	–	+	Port Forward	+	Port Forward
NAT Network	+	+	Port Forward	+	Port Forward
Bridged	+	+	+	+	+
Internal Network	+	–	–	–	–
Host-only	+	+	+	–	–

Table 2. VirtualBox network modes

With the VM Server powered off, students can configure the forwarding rule by

- Navigating to Settings -> Network -> Adapter 1, choosing **NAT** for network mode, (2) clicking on **Advanced,** (3) clicking on "Port Forwarding. illustrates the interface for this step. (4) create a rule with the following information:

a. Name: Ubuntu-SSH

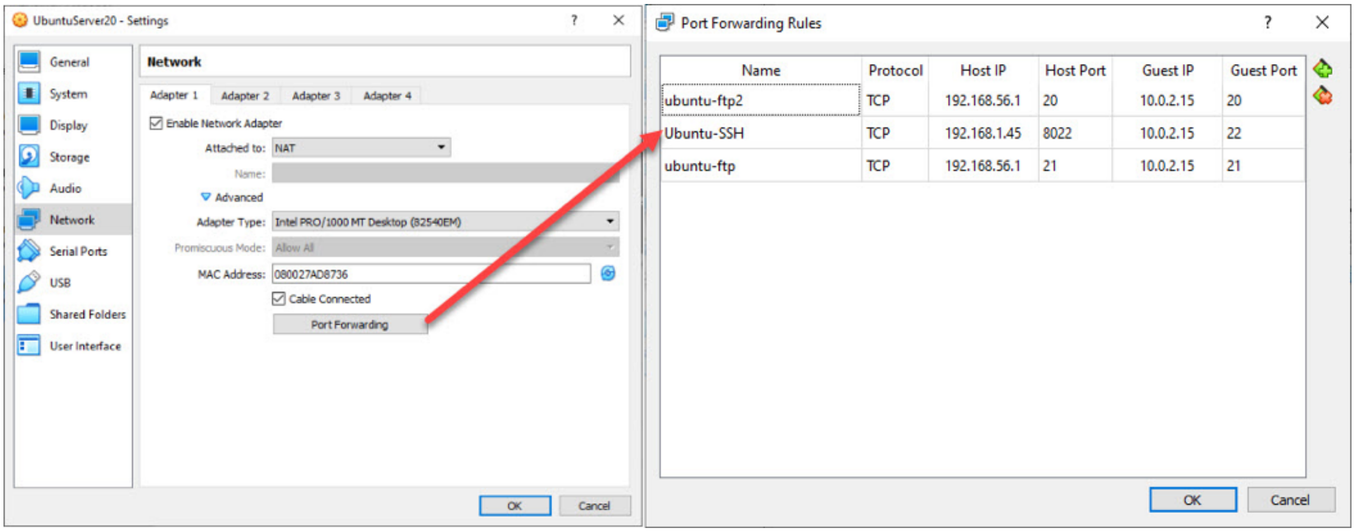
b. Protocol: TCP

c. Host IP: 127.0.0.1

d. Host Port: 8022

e. Guest IP: 10.0.2.15

f. Guest Port: 22



☑ Enable Network Adapter

Attached to: NAT

Name:

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Allow All

MAC Address: 080027AD8736

☑ Cable Connected

Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
ubuntu-ftp2	TCP	192.168.56.1	20	10.0.2.15	20
Ubuntu-SSH	TCP	192.168.1.45	8022	10.0.2.15	22
ubuntu-ftp	TCP	192.168.56.1	21	10.0.2.15	21

Figure 3. Forwarding rule

With the forwarding rule defined in Figure 3, students open an SSH client using PuTTy and connect to 127.0.0.1 on port 8022. Students then find the regular SSH login session seen before in Lab 3. Students can certainly use the host IP instead of the 127.0.0.1 address. The following are required for submission:

Q1. Please capture an image of your port-forwarding settings with 127.0.0.1. Please capture a picture of a successful PuTTy session with SSH from your host to your Ubuntu Server.

Q2. Repeat the above with the host IP setting

Q3. Explain how a port forwarding work

3.5. Lab5: Configure and investigate FTP traffic using Wireshark

This exercise allows students to get familiar with analyzing network traffic using Wireshark and further identifying the security in File Transfer Protocol (FTP). FTP is selected because FTP uses two ports, 20 and 21, for its connection in active mode. Students analyze the network traffic with Wireshark to determine the security issue with FTP if a secure FTP is not configured. Secure FTP configuration is not part of the exercises as it requires Secure Socket Layer, SSL/TLS, certificate configuration, which may be too much for a freshmen's lab experience.

FTP installation and configuration – run Ubuntu server VM in NAT and perform the following (only key instructions are shown here)

- *sudo apt install vsftpd* (install FTP package)

- Configure FTP settings:

- *sudo nano /etc/vsftpd.conf* (edit FTP configuration file)

- change the settings: Anonymous_enable = YES

- *sudo systemctl restart vsftpd* (restart FTP server)

- *sudo systemctl status vsftpd* (check FTP status)

- change directory to */srv/ftp* folder

- create a new directory: share_yourUsername (share_mak, for example)

FTP client and anonymous login – install an FTP client [35] on your host PC.

- We download the FileZilla, an FTP client, from [35]

- Set two port forwarding rules according to Table 3 by navigating to *Settings -> Network -> Adapter 1*, choosing **NAT** for network mode, (2) clicking on **Advanced,** (3) clicking on "Port Forwarding." Add the following to the rules table:

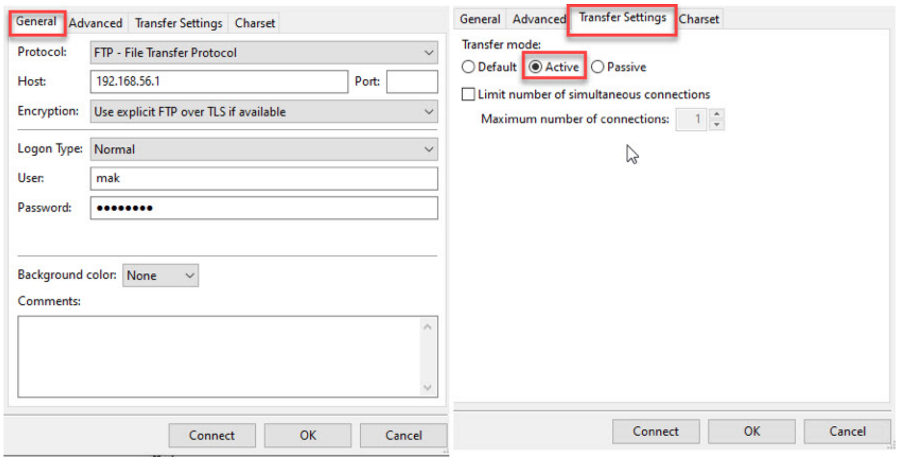
Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
Ubuntu-FTP	TCP	192.168.56.1	20	10.0.2.15	20
Ubuntu-FTP	TCP	192.168.56.1	21	10.0.2.15	21

Table 3. Forwarding rules for FTP

- The host IP should be the one that corresponds to VirtualBox Host-Only Ethernet Adapter.

- Open FTP client as illustrated in Figure 4, click on **File** on the top-left corner.

- Click on "Site Manager" to get to the following screen, click on "new site," and enter the info as shown in Figure 4.



Protocol: FTP - File Transfer Protocol
Host: 192.168.56.1 Port:
Encryption: Use explicit FTP over TLS if available
Logon Type: Normal
User: mak
Password: ••••••••
Background color: None
Comments:

Transfer mode:
○ Default ● Active ○ Passive
□ Limit number of simultaneous connections
Maximum number of connections: 1

Figure 4. Settings For Ftp Active Mode

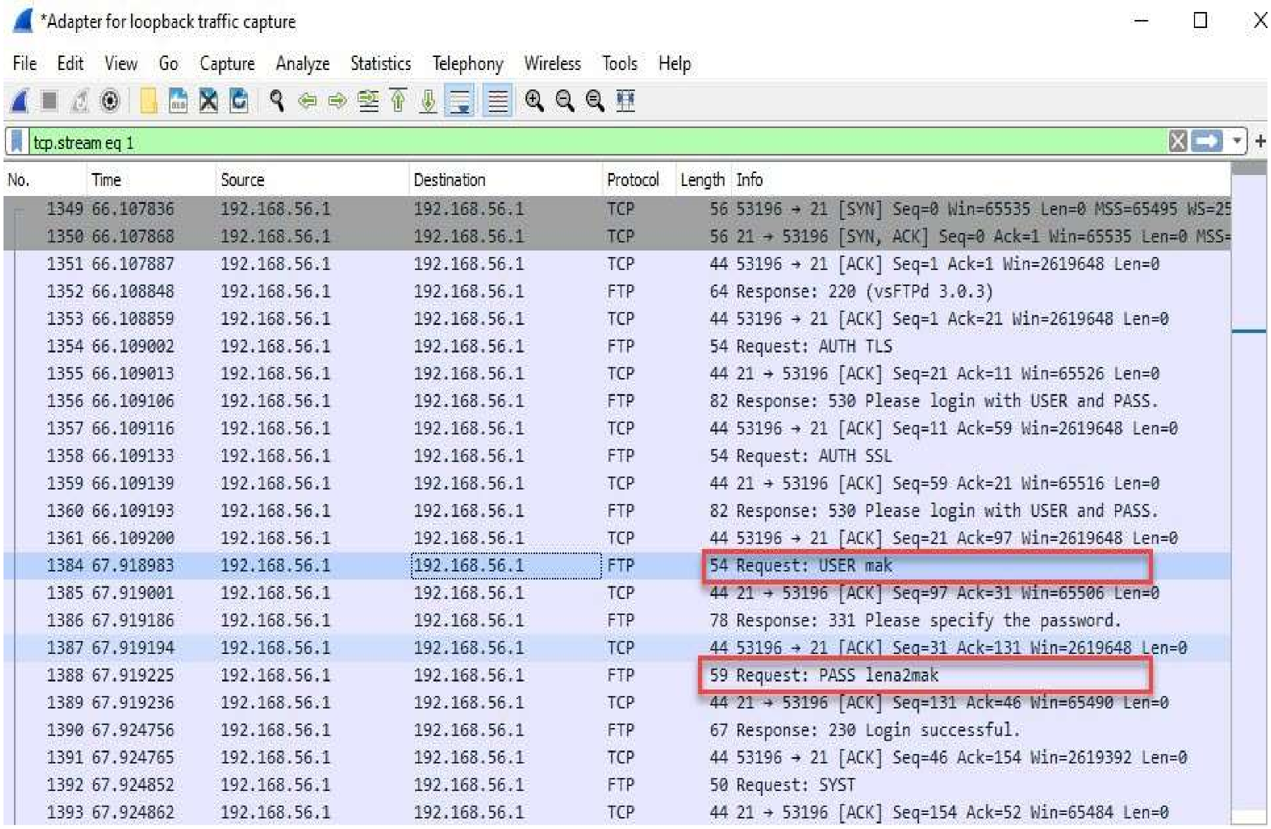
- If successfully connected to the FTP server, students should see the folder they created, share_mak, for example.

FTP with Credential Login – Students configure the FTP to use the credential for login.

- *sudo nano /etc/vsftpd.conf* (edit FTP configuration file)
- Change the settings: Anonymous_enable = NO
- *sudo adduser mak2* (create an FTP user account)
- Enter a password for the user and fill in all the required details when prompted by the creation process

Capture FTP Traffic

- Activate Wireshark and select the proper connection adapter.
- Activate FTP client on the host; initiate FTP session connection to Ubuntu server, and enter the proper credentials
- Stop Wireshark for capturing traffic.
- Analyze FTP traffic. Students should see the user's credential displayed as clear text in the network traffic, as shown in Figure 5.


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 1

No.	Time	Source	Destination	Protocol	Length	Info
1349	66.107836	192.168.56.1	192.168.56.1	TCP	56	53196 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=25
1350	66.107868	192.168.56.1	192.168.56.1	TCP	56	21 → 53196 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=
1351	66.107887	192.168.56.1	192.168.56.1	TCP	44	53196 → 21 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
1352	66.108848	192.168.56.1	192.168.56.1	FTP	64	Response: 220 (vsFTPd 3.0.3)
1353	66.108859	192.168.56.1	192.168.56.1	TCP	44	53196 → 21 [ACK] Seq=1 Ack=21 Win=2619648 Len=0
1354	66.109002	192.168.56.1	192.168.56.1	FTP	54	Request: AUTH TLS
1355	66.109013	192.168.56.1	192.168.56.1	TCP	44	21 → 53196 [ACK] Seq=21 Ack=11 Win=65526 Len=0
1356	66.109106	192.168.56.1	192.168.56.1	FTP	82	Response: 530 Please login with USER and PASS.
1357	66.109116	192.168.56.1	192.168.56.1	TCP	44	53196 → 21 [ACK] Seq=11 Ack=59 Win=2619648 Len=0
1358	66.109133	192.168.56.1	192.168.56.1	FTP	54	Request: AUTH SSL
1359	66.109139	192.168.56.1	192.168.56.1	TCP	44	21 → 53196 [ACK] Seq=59 Ack=21 Win=65516 Len=0
1360	66.109193	192.168.56.1	192.168.56.1	FTP	82	Response: 530 Please login with USER and PASS.
1361	66.109200	192.168.56.1	192.168.56.1	TCP	44	53196 → 21 [ACK] Seq=21 Ack=97 Win=2619648 Len=0
1384	67.918983	192.168.56.1	192.168.56.1	FTP	54	Request: USER mak
1385	67.919001	192.168.56.1	192.168.56.1	TCP	44	21 → 53196 [ACK] Seq=97 Ack=31 Win=65506 Len=0
1386	67.919186	192.168.56.1	192.168.56.1	FTP	78	Response: 331 Please specify the password.
1387	67.919194	192.168.56.1	192.168.56.1	TCP	44	53196 → 21 [ACK] Seq=31 Ack=131 Win=2619648 Len=0
1388	67.919225	192.168.56.1	192.168.56.1	FTP	59	Request: PASS lena2mak
1389	67.919236	192.168.56.1	192.168.56.1	TCP	44	21 → 53196 [ACK] Seq=131 Ack=46 Win=65490 Len=0
1390	67.924756	192.168.56.1	192.168.56.1	FTP	67	Response: 230 Login successful.
1391	67.924765	192.168.56.1	192.168.56.1	TCP	44	53196 → 21 [ACK] Seq=46 Ack=154 Win=2619392 Len=0
1392	67.924852	192.168.56.1	192.168.56.1	FTP	50	Request: SYST
1393	67.924862	192.168.56.1	192.168.56.1	TCP	44	21 → 53196 [ACK] Seq=154 Ack=52 Win=65484 Len=0

Figure 5. FTP network traffic

Students are to address the following questions:

Q1. Document steps for an FTP session with credential-based login using FileZilla that includes the forwarding rules configuration on the VirtualBox VM. Explain how ports 20 and 21 work in FTP active mode.

Q2. Please capture a screenshot of each step of the FTP session and the relevant Wireshark captured images. Highlight the user name and password caught.

Q3. Please comment on the security threat of using FTP.

3.6. Lab6: Packet Tracer Introduction

Packet Tracer Setup: Students can download a version of Packet Tracer from www.netacad.com [36], but students must also enroll in an accessible Introduction to Packet Tracer course offered by Cisco as part of the requirements to gain access to Packet Tracer download. The Introduction course is a good resource for getting familiar with Packet Tracer. We select Packet Tracer for its rich resources, and students can understand better the function of a switch, a router, and how all these components are put together in a network. We cover Lab 6 in a week. We introduce Packet Tracer by walking through downloading, installing, identifying the available videos for self-learning, and briefly explaining the menu's functionality in the Packet Tracer's interface. The second session is to construct the following simple network. We do not find it helpful to cover the details of Packet Tracer in one session. Instead, we introduce the relevant functionalities of Packet Tracer as we move forward with the construction of more complex examples in several labs.

3.6.1. Simple network

In this exercise, students build a simple network with two PC hosts and two switches, as shown in Figure 6.

You could include more PCs per switch. The objective is for students to use the *ping* command to see the other computer connected with a switch. Students learn to configure basic settings, including hostname, local passwords, and login banner. Students also use *show* commands to display the running configuration, IOS version, and interface status. Table 4 gives the necessary addressing for the network.

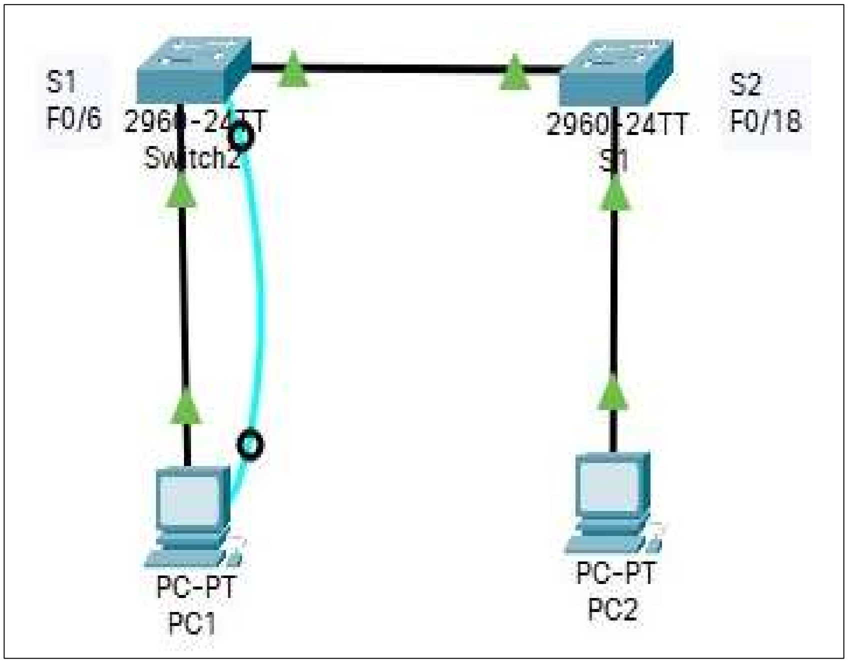


Figure 6. A simple network

Device	Interface	IP Address	Subnet Mask	PC to switch	Switch to Switch
PC1	NIC	192.168.1.10	255.255.255.0	PC1:F0 -> S1: F0/6	S1:F0/1 -> S2:F0/1
PC2	NIC	192.168.1.11	255.255.255.0	PC2:F0 -> S2: F0/18	

Table 4. Addressing of PCs and connection

The required resources from Packet Tracer's component list are:

- 2 switches (CISCO 2960)
- 2 PCs (Windows 7 or 8)
- Console cables to configure the CISCO IOS devices using the console ports

Network Connection – This exercise is a walk-thru activity with students to drag and drop network components from Packet Tracer's component list and get them familiar with the basic set of commands for configuring the switches and PC's address. For example, PC1 is connected via a straight-through cable from its fastEthernet0 (F0) to the F0/6 of switch 1 (S1). Students made the rest of the connections according to Table 3.

PC Configuration – students double click on the PC1 icon, and a pop-up window then shows options of Physical, Config, Desktop, Programming, and Attributes. Students click on Desktop, and they will see a list of icons such as Terminal, IP Configuration, etc. Students click on IP configuration to enter the PC address for PC1, according to Table 3. In this exercise, students enter IPv4: 192.168.1.10 and a Subnet Mask: 255.255.255.0 for PC1 and leave blank for Default Gateway and DNS, *Domain Name System*, Server. Students repeat the PC configuration for PC2, but with IPv4: 192.168.1.11.

Switch Configuration – Students connect from PC1's RS232 to S1's console port using a console cable, as shown in Figure 6, just the same as they would do in real life to configure a switch via the RS232 connection using a laptop. The following is a sequence of commands to use for configuring the switch.

```
• Switch > enable  (enter privilege EXEC mode)
• Switch # configure terminal (Enter configuration mode)
• Switch(config)#  hostname S1 (give the switch a name)
• S1 (config)# no ip domain-lookup (prevent unwanted DNS lookup)
• S1 (config)# enable secret class  (prevent unauthorized access to the switch)
s1 (config)# line console 0
S1 (config-line)# password gannon  (use a standard password for the class)
S1 (config-line)# login
S1 (config-line)# exit

•  S1 (config)# banner motd #  (enter a login MOTD, Message Of The Day,  banner)
Enter Text message. End with the character '#'
unauthorized access is strictly prohibited and prosecuted to the full extent of the law. #
S1 (config)# exit

• S1 # copy running-config startup-config  (save the configuration)
Destination filename [startup-config]? [enter]
building configuration …
[OK]

• S1 # show running-config (display the current configuration)
Building configuration…
(pay attention to the details of the contents…)

• S1 # show IP interface brief (display the status of the connected interfaces of the switch)
(pay attention to the printout details)
```

Students repeat the switch configuration process to Switch 2 (S2). Students shall submit the following as evidence of work:

- Record the interface status for the following interfaces, and explain why some FastEthernet ports on the switches are up and others are down?

Interface	S1		S2	
	Status	Protocol	Status	Protocol
F0/1	UP? Down?			
F0/6				
F0/18				
VLAN1				

- What could prevent a ping from being sent between the PCs? Is firewall enabled?

Students are to address the following questions:

Q1. Please capture an image of your complete constructed network that includes two switches and two PCs.

Q2. Please capture an image of your successful *ping* from PC1 to PC2

Q3. Please export your complete configuration for SW1 as a text file. Your configuration file shall contain (1) password setting, (2) banner setting

Q4. Please submit the full table of records for the interface status in a pdf format

Q5. Discuss the security measures you have taken to secure the switches in this simple network setup.

3.7. Lab7: Building a simple network with a router

In this exercise, students expand the network built in Lab 6 to include a router (RTA) to connect two domains. Students then configure RTA with basic settings and configure the IP addresses on switches and their associated PCs as VLAN. Students then learn to use various *show* commands to verify the configuration and use the *ping* command to verify the connectivity between PCs. Table 5 shows the IP addresses assigned to each device. Figure 7 shows the network to be built. The essential resource is the same as Lab 6, but with one added router, RTA 1941.

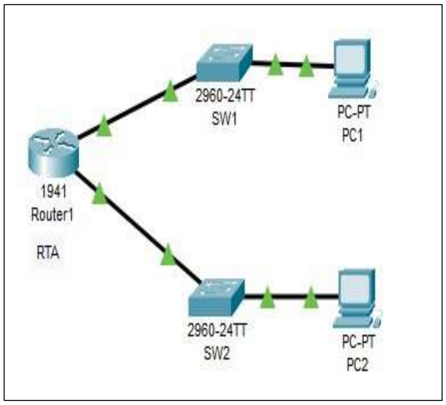


Figure 7. A simple network with a router

Device	Interface	IP Address	Subnet Mask	Default Gateway
RTA	G0/0	10.10.10.1	255.255.255.0	N/A
	G0/1	10.10.20.1	255.255.255.0	N/A
SW1	VLAN1	10.10.10.2	255.255.255.0	10.10.10.1
Sw2	VLAV2	10.10.20.2	255.255.255.0	10.10.20.1
PC1	NIC	10.10.10.10	255.255.255.0	10.10.10.1
PC2	NIC	10.10.20.10	255.255.255.0	10.10.20.1

Table 5. Addresses for each device

Router configuration – in this exercise, students configure the switch and router directly by doubling clicking on the router icon and click on the **CLI** of the options menu instead of using a console cable with a laptop. The following summarizes the commands used for router configuration.

```
• Router> enable (enter privilege EXEC mode)
• Router# configure terminal (Enter configuration mode)
• Router (config)#  hostname RTA (give the router a name)
• RTA (config)#  banner motd &Warning… don’t mess with my router!&
• RTA (config)# line console 0 (protect your router)
RTA (config-line)# password gannon
RTA (config-line)# login
RTA (config-line)# exit
RTA (config)#  line vty 0 15
RTA (config-line)#  password gannon
RTA (config-line)# login
RTA (config-line)# exit
• RTA# configure terminal (get back into configuration mode)
RTA(config)# enable secret class
• RTA (config)#  interface gigabitEthernet 0/0 (assign IP to G0/0)
RTA (config-if)#  ip address 10.10.10.1 255.255.255.0
RTA (config-if)#  description GigabitEthernet0/0
RTA (config-if)#  no shutdown
• RTA (config-if)#  int gi 0/1 (assign IP to G0/1)
RTA (config-if)#  ip address 10.10.20.1 255.255.255.0
RTA (config-if)#  description GigabitEthernet0/1
RTA (config-if)#  no shutdown
RTA (config-if)#  exit
RTA #  copy running-config startup-config
```

Switch configuration – students configure the switch using the same process and command as those in Lab 6, except the following added commands for configuring VLAN:

```
• SW1# configure terminal
SW1 (config)# interface vlan1 (set up VLAN1)
SW1 (config-if)# ip address 10.10.10.2 255.255.255.0
SW1 (config-if)# no shutdown
SW1 (config-if)# exit
SW1 (config)# ip default-gateway 10.10.10.1
SW1 (config)# exit
SW1# copy running-config startup-config
```

As noted, the commands used for switch and router are similar. Students repeat the above steps for configuring S2, and assign VLAN2 to S2.

The following are commands that students practice on the network and gather information accordingly:

- Show ip interface brief
- Show interfaces
- Show ip interface
- Show ip route
- Show ip route connected

Students are to use *show* commands to gather information so that they can address the following questions:

- How many networks are known by the router based on the output of the *show ip route* command?
- What does the L at the beginning of the lines within the routing table represent?
- What does the /32 prefix listed in the router table indicate?
- On RTA, shut down the Gigabit Ethernet 0/0 interface and issue the *show ip route* command. How many networks are displayed in the routing table now?

- Attempt to ping PC1 from PC2. Was the ping successful?
- Issue the *show ip interface brief* command. What is the status of the Gigabit Ethernet 0/0 interface?
- Reactivate the Gigabit Ethernet 0/0 interface. Issue the *show ip route* command. Did the routing table repopulate?
- What can you infer about the interface status of routes that appear in the routing table?

3.8. Lab8: VLAN implementation and security consideration

In this exercise, students expand the network built in Lab 7 to include VLAN configuration. The objectives are:

- Explain how a VLAN traffic flow between PCs
- Know how to configure VLANs using *switchport* command
- Learn how to use Packet Tracer's simulation mode to observe packet flow.

Procedure – Students are to follow the instructions bellows accordingly.
Students are to (1) divide the network into three subnets with /26 subnet mask, (2) label the three VLANs as 10 (Engineering), 20 (HR), and 30 (Sales), (3) allocate two PCs to each department and connect each set of PCs with a switch and a router. Figure 8 shows the expected network layout.

Pre-Lab — Based on the subnet mask information students obtained from VLAN Lab 7 as a hint, students complete the following table for the IP address assignment for each PC and the associated switch and router. The VLANS needed with the assigned IPs for the three departments are (1) VLAN10: Engineering with 10.0.0.0/26, (2) VLAN20: HR with 10.0.0.64/26, and (3) VLAN30: Sales with 10.0.0.128/26. Students are to complete the IP assignments in Table 6:

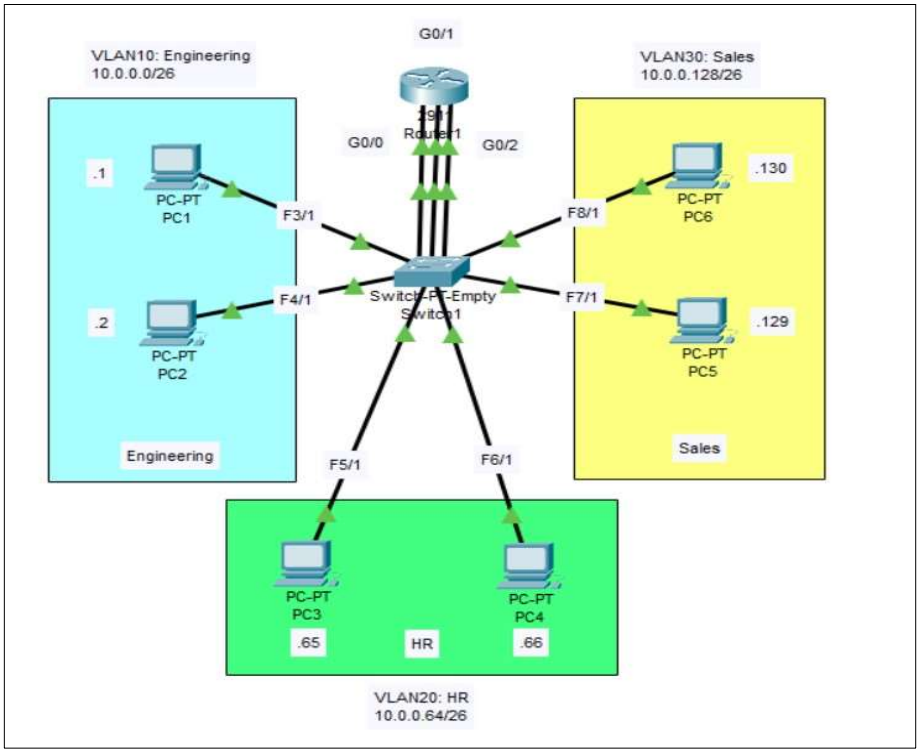


Figure 8. Network layout with VLAN

VLAN	PCs	SW1	Router	Gateway	Subnet mask
10	PC1: 10.0.0.1	F3/1	G0/1G0/1	G0/0	
	PC2:	F4/1			
20	PC3:	F5/1	G1/1	G0/1	
	PC4:	F6/1			
30	PC5:	F7/1	G2/1G2/1	G0/2	

Table 6. IP assignment for PCs used for the three departments

Resouces needed – Use Router 2911, and PT-Empty as the switch. PT-Empty is an empty switch that allows students to add connector modules. To add a connector module, students first turn off the switch, drag and drop the connectors they want. Students add (1) three PT-SWITCH-NM-ICGE (Gigabit Ethernet network module) to ports 0, 1, and 2, and (2) seven PT-SWITCH-NM-ICFE (Fast Ethernet network module) to ports 3 to 7. Students are to address: *Why use fast Ethernet to ports 3 to 7, but gigabit Ethernet to ports 0 to 2?*

The following are instructions for the rest of the setup:

- Configure the correct IP address/subnet mask on each PC. Set the gateway address as the Last Usable address of the subnet

- Make a connection between SW1 and all PCs of the three VLANs, according to Figure 8.
- Configure the router to have the three VLANs, set it up according to Table 6. Verify the setup by using the command: *show ip interface brief*. Commands that students may need are:

```
o Router> enable
o Router# configure terminal
o Router (config)# hostname R1
o R1 (config)#interface g0/0
o R1 (config-if)#ip address 10.0.0.62 255.255.255.192
o R1 (config-if)# no shutdown
```

- (do the same for G0/1 and G0/2 interfaces)
- R1 (config-if)# *do show ip interface brief* (to show what you set up thus far)
- Please remember to save your configuration into the startup-config.
- Configure the switch for the three VLANs, and capture your settings with proper naming for each VLAN. Commands that students may need:

```
o Switch> enable
o Switch# configure terminal
o Switch (config)# hostname SW1
o SW1 (config)#interface range  G0/1, F3/1, F4/1  (configure all together)
o SW1 (config-if-range)#switchport mode access  (this makes these ports access ports)
o SW1 (config-if-range)# switchport access vlan 10  (this create VLAN 10)
```

- (do the same for VLAN 20 and VLAN 30)
- SW1 (config-if-range)# *do show vlan brief*
- SW1 (config-if-range)# *vlan 10*
- SW1 (config-vlan)#*name Engineering*
- (change the names for vlan 20 and vlan 30 accordingly)
- SW1 (config-if-range)# *do show vlan brief* (capture the setting)
- Please remember to save your configuration into the startup-config.
- Verify your connectivity by using ping

o Use command windows from PC1 and *ping* to PC3. Is your ping successful? Capture your result.

o Repeat the *ping* to PC5.

o Use simulation mode to repeat the above Steps, step-thru each sequence of packet flow until a successful ping is made.

o Capture a sequence map of ping's flow pattern.

Students are to address the following questions:

Q1. You are to design a VLAN network for a company that has three departments: Engineering, HR, and Sales. (a) determine how many subnets can be created with /26 subnet mask, given the first IP is 10.0.0.0. (b) determine the last useable address for each subnet. (c) document your work in details of how you determine the usable ip range for each department.

Q2. Please define a table that has the proper assignments of IP address for each PC, switch, router, gateway, and subnet mask. (a) please submit a table that details the IP assignment for each VLAN with two PCs and the associated assignment of IP for switches and routers. (b) please capture a screenshot of your VLAN network with proper labels for all the components and connections among them.

Q3. Please capture the settings for the switch via *show vlan brief* in a pdf format

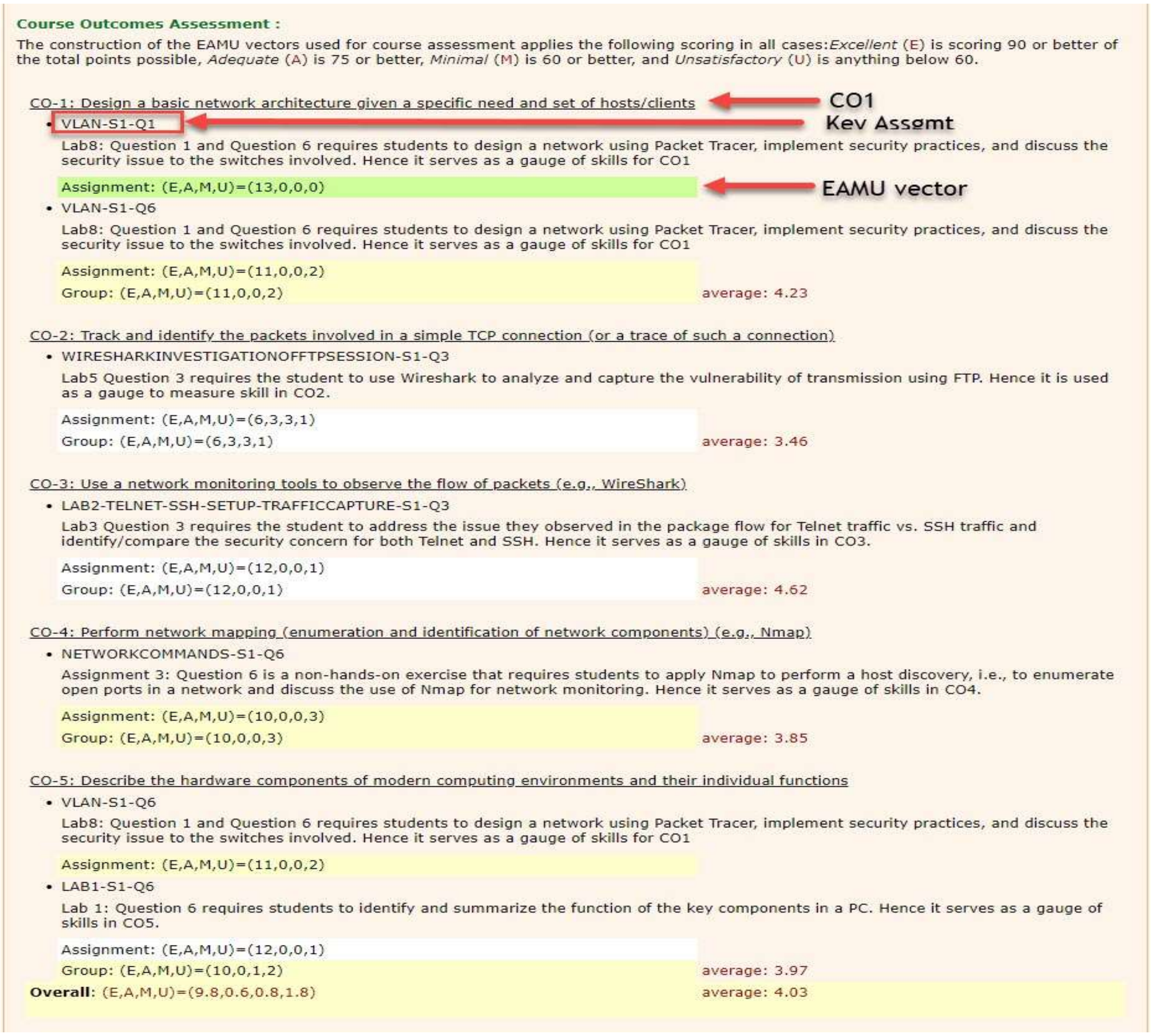
Q4. Please capture the settings for the router via *show ip interface brief* in a pdf format

Q5. Please capture a successful sequence map of a *ping* command's flow pattern

Q6. Please discuss how a VLAN configuration provides security in a company's segmentation of PCs in different zones.

4. Assessment

The assessment data is compiled once the key assignments are scored and uploaded to EvalTools®. Since the assessment data



Course Outcomes Assessment :

The construction of the EAMU vectors used for course assessment applies the following scoring in all cases:*Excellent* (E) is scoring 90 or better of the total points possible, *Adequate* (A) is 75 or better, *Minimal* (M) is 60 or better, and *Unsatisfactory* (U) is anything below 60.

CO-1: Design a basic network architecture given a specific need and set of hosts/clients

- VLAN-S1-Q1

  Lab8: Question 1 and Question 6 requires students to design a network using Packet Tracer, implement security practices, and discuss the security issue to the switches involved. Hence it serves as a gauge of skills for CO1

  Assignment: (E,A,M,U)=(13,0,0,0)

- VLAN-S1-Q6

  Lab8: Question 1 and Question 6 requires students to design a network using Packet Tracer, implement security practices, and discuss the security issue to the switches involved. Hence it serves as a gauge of skills for CO1

  Assignment: (E,A,M,U)=(11,0,0,2)

  Group: (E,A,M,U)=(11,0,0,2) average: 4.23

CO-2: Track and identify the packets involved in a simple TCP connection (or a trace of such a connection)

- WIRESHARKINVESTIGATIONOFFTPSESSION-S1-Q3

  Lab5 Question 3 requires the student to use Wireshark to analyze and capture the vulnerability of transmission using FTP. Hence it is used as a gauge to measure skill in CO2.

  Assignment: (E,A,M,U)=(6,3,3,1)

  Group: (E,A,M,U)=(6,3,3,1) average: 3.46

CO-3: Use a network monitoring tools to observe the flow of packets (e.g., WireShark)

- LAB2-TELNET-SSH-SETUP-TRAFFICCAPTURE-S1-Q3

  Lab3 Question 3 requires the student to address the issue they observed in the package flow for Telnet traffic vs. SSH traffic and identify/compare the security concern for both Telnet and SSH. Hence it serves as a gauge of skills in CO3.

  Assignment: (E,A,M,U)=(12,0,0,1)

  Group: (E,A,M,U)=(12,0,0,1) average: 4.62

CO-4: Perform network mapping (enumeration and identification of network components) (e.g., Nmap)

- NETWORKCOMMANDS-S1-Q6

  Assignment 3: Question 6 is a non-hands-on exercise that requires students to apply Nmap to perform a host discovery, i.e., to enumerate open ports in a network and discuss the use of Nmap for network monitoring. Hence it serves as a gauge of skills in CO4.

  Assignment: (E,A,M,U)=(10,0,0,3)

  Group: (E,A,M,U)=(10,0,0,3) average: 3.85

CO-5: Describe the hardware components of modern computing environments and their individual functions

- VLAN-S1-Q6

  Lab8: Question 1 and Question 6 requires students to design a network using Packet Tracer, implement security practices, and discuss the security issue to the switches involved. Hence it serves as a gauge of skills for CO1

  Assignment: (E,A,M,U)=(11,0,0,2)

- LAB1-S1-Q6

  Lab 1: Question 6 requires students to identify and summarize the function of the key components in a PC. Hence it serves as a gauge of skills in CO5.

  Assignment: (E,A,M,U)=(12,0,0,1)

  Group: (E,A,M,U)=(10,0,1,2) average: 3.97

Overall: (E,A,M,U)=(9.8,0.6,0.8,1.8) average: 4.03

Figure 9. FCAR data on course outcomes assessment

is readily available, FCAR can facilitate formative evaluation. In this example, we focus on summative assessment at the end of the semester. Before the adoption of EvalTools®, instructors have to provide the FCAR in Word format. This manual process is eliminated with the use of EvalTools® for this program. Figure 9 shows a portion of the self-generated FCAR by EvalTools® for the instructor to review. Let's examine the result on CO1. The key assignment is VLAN-S1-Q1 (Question 1 of VLAN assignment), with the justification for selecting this specific assignment. The EAMU vector is (13,0,0,0). There are 13 submissions with scores above 90% or better. Hence, the color code is green for exceeding expectations. The second key assignment, VLAN-S1-Q6, selected is Question 6 of the VLAN assignment. The corresponding EAMU indicates a yellow flag of potential concern area due to the two submissions rated Unsatisfactory, 60% or below. Table 7 shows the heuristic rule for the color flags.

Further examining the root cause for the two submissions that were rated Unsatisfactory, it was found that students did not submit or complete their assignments. All the "U" resulted from no submission or incomplete work in this example. In general, we want instructors to write a course reflection and suggest new action items for any yellow-flag or red-flag EAMU for improvement as part of the FCAR. If we exclude no submission and incomplete work, the EAMU will be green or white. We have achieved our course outcomes.

Category	**Description**
Red Flag	Any performance vector with an average below 3.3 (on a 5-point scale) AND a level of unsatisfactory performance that exceeds 10% in the U column.
Yellow Flag	Any performance vector with an average below 3.3 OR a level of unsatisfactory perfor mance (U) that exceeds 10%
Green Flag	Any performance vector with an average that is at least greater than 4.6 and no indication of unsatisfactory performance (U)
No Flag (white)	Any performance vector that does not fall into one of the above categories

Table 7. Heuristic rule for color flags

Ref [21] documents the computation of EAMU. For clarity, we illustrate the EAMU calculation here. Figure 10 shows the raw data of key assignments for CO1 and CO2. There is only one key assignment for CO2 (data enclosed in red box). The corresponding EAMU calculation is relatively straightforward for each student's score. Let's take student 1 denoted as S1, for example. His score is 40 out of 40 points, hence, 100%. Thus, his score belongs to the "E" category. But, for CO1, there are two key assignments (data enclosed in the green box). The aggregate averaged percentage of all key assignment scores for each student is used to determine the corresponding EAMU category. The formula is:

$$Average\ score = \frac{score1+score2}{full\ score1+full\ score2} X\ 100\% \qquad (1)$$

For example, the score-weighted average for Student 10 (S10) is:

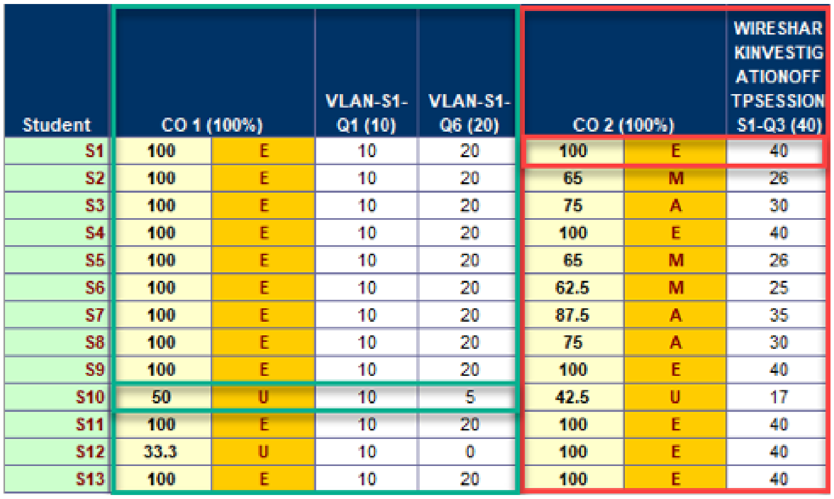
$$Average\ score = \frac{10+5}{10+20} X\ 100\% = 50 \qquad (2)$$

Hence, S10's score for CO1 belongs to the "U" category.

Equation (3) gives the calculation of the average of the EAMU vector.

$$EAMU\ average_3 = \frac{\#E*3+\#A*2+\#M*1+\#U*0}{\#E+\#A+\#M+\#U} \qquad (3)$$

The default scale for a base-3 EAMU is 3 for E, 2 for A, 1 for M, and 0 for U. The "#" indicates the total number of that category. Hence, #E means the total number of E. However, EvalTools® gives the option to scale the base-3 vector to a base-5 vector for ease of interpretation of the EAMU results and be consistent with the base scale for the survey instrument. Hence, for the base-5 vector, the average becomes:



Student	CO 1 (100%)		VLAN-S1-Q1 (10)	VLAN-S1-Q6 (20)	CO 2 (100%)		WIRESHARKINVESTIGATIONOFFTPSESSION S1-Q3 (40)
S1	100	E	10	20	100	E	40
S2	100	E	10	20	65	M	26
S3	100	E	10	20	75	A	30
S4	100	E	10	20	100	E	40
S5	100	E	10	20	65	M	26
S6	100	E	10	20	62.5	M	25
S7	100	E	10	20	87.5	A	35
S8	100	E	10	20	75	A	30
S9	100	E	10	20	100	E	40
S10	50	U	10	5	42.5	U	17
S11	100	E	10	20	100	E	40
S12	33.3	U	10	0	100	E	40
S13	100	E	10	20	100	E	40

Figure 10. Raw Data of EAMU computation for CO1 and CO2

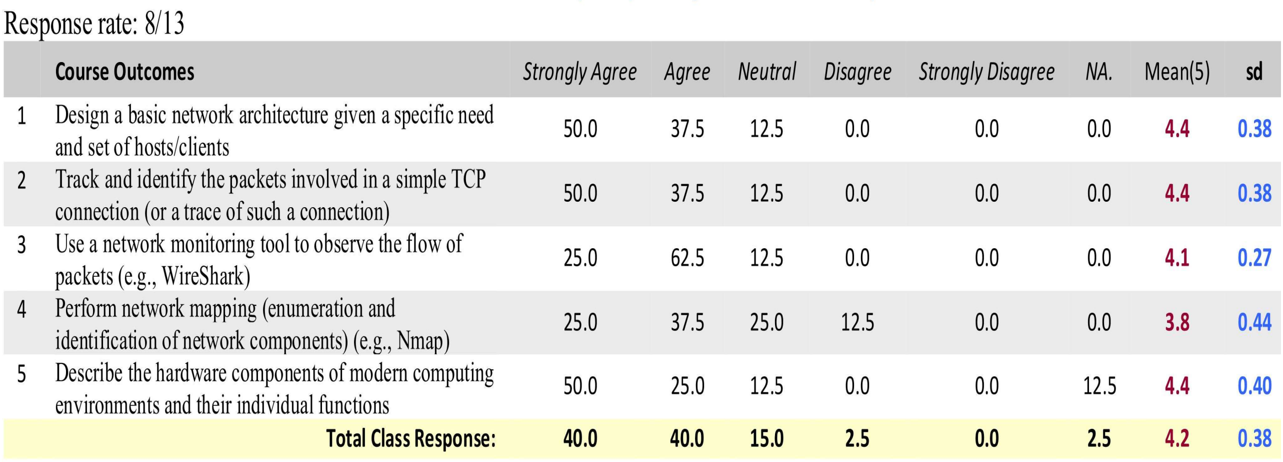
In this example, the base-5 scale is used. Hence, for CO1, with EAMU = (11, 0, 0, 2), the corresponding average is computed as follows:

$$EAMU\ average_5 = \frac{11*3+0*2+0*1+2*0}{11+0+0+2} * \left(\frac{5}{3}\right) = 4.23 \qquad (5)$$

Indirect Assessment:

How well does this lab achieve its course outcomes from students' perspectives? Table 8 summarizes the responses or perceptions from students at the end of the semester. The course outcomes section is automatically included in the end-of-term course-exit survey administrated by EvalTools®. The column fields "strongly agree" to "strongly disagree" are pre-set by the department and used consistently for this section of the questionnaire for all courses. Course outcomes always begin with a verb consistent with Bloom's taxonomy for suggested verbs for the cognitive domain. Bloom's cognitive domain [37] contains six categories of cognitive skills ranging from lower-order skills to higher-order skills. The six categories are knowledge, Comprehension, Application, Analysis, Synthesis, and Evaluation. Since CYSEC 101 is a freshmen-level course, we focus on the Knowledge category of cognitive skills. Hence, the verbs chosen for the course outcomes are mostly falling under the suggested word list of the Knowledge category. The students are accustomed to interpreting the course outcome statement with "the ability of" in front of each course outcome statement. The result from Table 8 shows that students have the least favorite of learning Nmap from the end-of-term survey responses. The author believes it has to do with Nmap being assigned as a regular dot-it-yourself assignment with instructions. To improve on the learning of Nmap, students would prefer a hands-on lab exercise. Concerning other course outcomes, students are mostly positive about the experience.

In general, students prefer a hands-on teaching approach, which also requires an instructor lot more effort to prepare. CYSEC101 is an intense and tight-schedule one-credit course. The preparation work requires the same amount of time or more effort as a three-credit teaching course for the instructor. It will be a challenge for a junior faculty to teach this course for the work and time involved. In addition, to facilitate a smooth class operation, the instructor needs a good teaching assistant to help students outside the lab schedule complete the lab exercises in time.



Response rate: 8/13

	Course Outcomes	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	NA.	Mean(5)	sd
1	Design a basic network architecture given a specific need and set of hosts/clients	50.0	37.5	12.5	0.0	0.0	0.0	4.4	0.38
2	Track and identify the packets involved in a simple TCP connection (or a trace of such a connection)	50.0	37.5	12.5	0.0	0.0	0.0	4.4	0.38
3	Use a network monitoring tool to observe the flow of packets (e.g., WireShark)	25.0	62.5	12.5	0.0	0.0	0.0	4.1	0.27
4	Perform network mapping (enumeration and identification of network components) (e.g., Nmap)	25.0	37.5	25.0	12.5	0.0	0.0	3.8	0.44
5	Describe the hardware components of modern computing environments and their individual functions	50.0	25.0	12.5	0.0	0.0	12.5	4.4	0.40
	Total Class Response:	**40.0**	**40.0**	**15.0**	**2.5**	**0.0**	**2.5**	**4.2**	**0.38**

Table 8. Students' perception of the course delivery

5. Conclusion

We have outlined a series of lab exercises that allow students to gain hands-on experience to support their understanding of networks with security concerns in using network components and software applications. This one-credit lab experience course effectively covers the additional topics in *CIS290 Introduction to Networks* with added hands-on exercises to enhance students' experience in PC technologies, FTP, Telnet, SSH, network building, switches, routers, VLAN, and network traffic analysis. With this added lab, we cover all the topics as essential building blocks of knowledge to support the rest of the curriculum courses in Cyber Engineering and Cybersecurity programs. More importantly, students are comfortable dealing with PC technologies, software applications and identifying online recourses. Students also learn to set up and build a lab environment using their resources, such as laptops or self-built PCs at home. We have achieved our initial targeted goals as follows:

- Gain knowledge in topics of 13 and 21

- Gain hands-on experience and be familiar with PC technologies, including hands-on experience in disassembling and assembling a computer.

- Ability to source the right parts of a computer to meet specific criteria

- Ability to install Operating Systems or Server applications

- Investigate case studies of cybersecurity

- Use of resources that are not restricted to the physical lab

References

[1] Criteria for Accrediting Engineering Programs, 2021-2022. https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-engineering-programs-2021-2022/

[2] Criteria for Accrediting Computing Programs, 2021-2022. https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2021-2022/

[3] Mike Meyers, *CompTIA Network+ Certification All-in-One Exam Guide*, Seventh Edition, 2018 McGraw-Hill Education

[4] Vyacheslav Fadyushin and Andrey Popov, *Building a Pentesting Lab for Wireless Networks*, 2016 Packt

[5] Kevin Cardwell, *Building Virtual Pentesting Labs for Advanced Penetration Testing*, Second Edition, August 2016, Packt

[6] Georgia Weidman, *Penetration Testing – A Hands-on Introduction to Hacking*, 2014, William Pollock

[7] Wenliang Du, *Computer Security – A Hands-on Approach, second Edition*, 2019, SEED labs, Syracuse University

[8] Wenliang Du, Internet Security – *A Hands-on Approach, second Edition*, 2019, SEED labs, Syracuse University

[9] GENI, information available at https://www.geni.net/about-geni/what-is-geni/

[10] Wenling Du, *SEED Labs - Instructor Manual*, 2018, Syracuse University

[11] CLARK, R. T. (). The Cybersecurity Labs and Resource Knowledge-base, information available at https://clark.center/home

[12] Abler, R., Contis, T. D., Grizzard, J. B., Owen, H. L. (2006). *Georgia Tech Information Security Center hands-on network security laboratory*, *IEEE Transactions on Education*, 49 (1) 82-87, Feb. 2006.

[13] Xu, L., Huang, D., Tsai, W. (2014). *Cloud-based virtual laboratory for network security education*, *IEEE Transactions on Education*, 57 (3) 145-150, August 2014.

[14] Mateti, P. (2003). *A laboratory-Based course on Internet security*," in Proc. 34th SIGCSE Tech. Symp. Computer Science Education, Reno, NV, Feburary, 252–256.

[15] Micco, M., Rossman, H. (2022). *Building a cyberwar lab: Lessons learned teaching cybersecurity principles to undergraduates*, *In*: Proceedings 33rd *SIGCSE Tech. Symp. Computer Science Education*, Northern Kentucky Convention Center, Feburary 2002, 18–22.

[16] Frank, C., Wells, G. (2002). *Laboratory exercises for a computer security course*," J. Comput. Sci. Colleges, vol. 17, no. 4, pp. 51–54, March.

[17] Wenliang, Du. (2011). *SEED: Hands-on lab exercises for computer security education*," IEEE Computer and Reliability Societies, September/October.

[18] Kwon, M., Kwak, G., Jun, S., Lee, H. (2017). *Enriching security education hands-on labs with practical exercises*," International Conference on Software Security and Assurance.

[19] Wiggins, Grant., McTighe, Jay. (2005). *Understanding by Design, 2nd Edition*. Alexandria, VA: Association for Supervision and Curriculum Development.

[20] Hansen, Edmund. (2011). *Idea-Based Learning – A Course Design Process to Promote Conceptual Understanding*, 2011, Sterling, VA: Stylus Publishing.

[21] Estell, John., Yoder, John., Morrison, Briana., Mak, Fong. (2012). Improving Upon Best Practices: FCAR 2.0," American Society for Engineering Education.

[22] Craig Zacker. (2018). *CompTIA Network+ Practice Tests*, 2018, John Willey & Sons.

[23] Cybersecurity Curricular Guidelines, CSEC 2017, available at: https://cybered.acm.org/

[24] EvalTools, a comprehensive online tool for learning management and outcomes assessment, information available at https://www.makteam.com

[25] Fong Mak, Steve Frezza, *Process to Identify Minimum Passing Criteria and Objective Evidence In Support of ABET EC2000 Criteria Fulfillment, In*: Proceedings of the 2004 American Society for Engineering Education Conference & Exposition, Salt Lake City, UT, June.

[26] Mak, Fong., Kelly, Jessica. (2010). *Systematic Means for Identifying and Justifying Key Assignments for Effective Rules-Based Program Evaluation*, 40th ASEE/IEEE Frontiers in Education Conference, Washington, DC, October 2010.

[27] Fong Mak, Ramakrishnna Sundaram. (2016). *Integrated FCAR model with Traditional Rubric-Based Model to Enhance Automation of Student Outcomes Evaluation Process*, *In*: Proceedings of the 2016 American Society for Engineering Education Conference & Exposition, New Orleans, LA, June.

[28] PC Part Picker, an online tool for integrating PC parts, info available at https://www.pcpartpicker.com

[29] WireShark, a network protocol analyzer, info available at https://www.wireshark.org/

[30] WireShark videos, https://www.youtube.com/watch?v=flDzURAm8wQ&list=PL6gx4Cwl9DGBI2ZFuyZOl5Q7sptR7PwYN

[31] VirtualBox, An virtualization tool, info available at https://www.virtualbox.org/

[32] Ubuntu server, instant Ubuntu VMs, info available at https://ubuntu.com/download.

[33] PuTTy, an SSH and telnet client, info available at https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

[34] VirtualBox guide, info available at https://www.nakivo.com/blog/virtualbox-network-setting-guide/

[35] FileZilla, an FTP client, info available at https://filezilla-project.org/download.php

[36] Packet Tracer, a network simulator, info available at https://www.netacad.com/zh-hant/courses/packet-tracer.

[37] Benjamin Bloom. (1989). *Taxonomy of Educational Objectives, Handbook 1: Cognitive Domain*, Allyn & Bacon, Incorporated, January.