Critical Thinking Assignment 7: Labs Lessons 12

Alexander Ricciardi

Colorado State University Global

IT315-2: Introduction to Networks

Dr. Sheryl Drake

February 2, 2025

Critical Thinking Assignment 6: Labs Lessons 12

This documentation is part of the Critical Thinking 7 Assignment from ITS315: Introduction to Networks at Colorado State University Global.

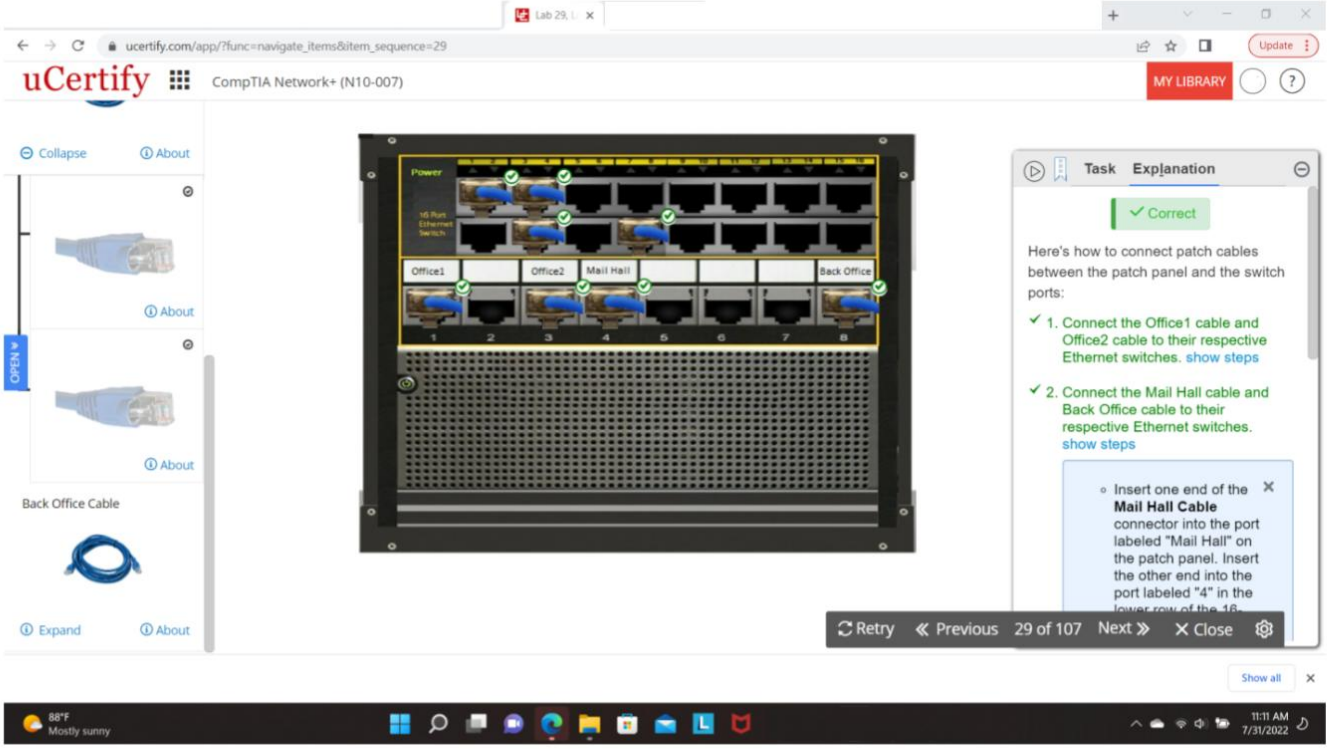
The Assignment Direction:

Module #6: uCertify Lab Simulations
For this assignment, you will complete multiple lab simulations. Activities include identifying network connection types, connecting networks to the internet, configuring routers, etc. You will take a screenshot upon completion of each lab and include the screenshots in the submitted assignment.

Access uCertify and login, go to Labs, and complete the tasks in the following lab simulations:

12.2.9 Identifying network attacks
12.3.7 Scanning using nmap
12.3.8 Running the Nessus vulnerability scan
12.5.3 Identifying types of firewall
12.6.1 Creating a remote access VPN connectionr

After completing the task, click Submit >> Evaluate >> Record my answer to record your answer. Take a screenshot of each of the labs and paste the screenshot into a Word document. The document should have a title page that includes your name, date, school name, section, course name, and instructor name.
Submit the assignment in Canvas.
Please ensure your screenshot includes your name, date, and timestamp as shown in the image below.



✓ Correct

Here's how to connect patch cables between the patch panel and the switch ports:

✓ 1. Connect the Office1 cable and Office2 cable to their respective Ethernet switches. show steps

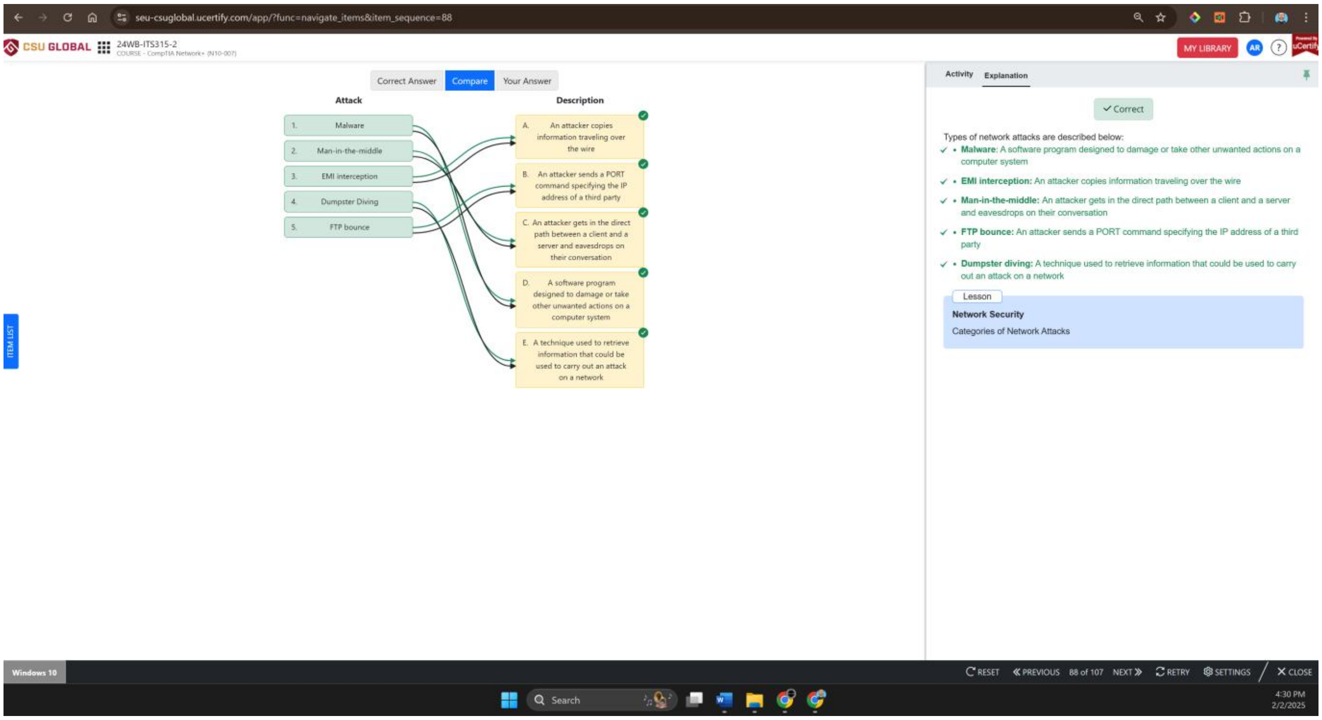
✓ 2. Connect the Mail Hall cable and Back Office cable to their respective Ethernet switches. show steps

- Insert one end of the **Mail Hall Cable** connector into the port labeled "Mail Hall" on the patch panel. Insert the other end into the port labeled "4" in the lower row of the 16-

Screenshots

Figure 1

12.2.9 Identifying network attacks



Attack	Description
1. Malware	A. An attacker copies information traveling over the wire
2. Man-in-the-middle	B. An attacker sends a PORT command specifying the IP address of a third party
3. EMI interception	C. An attacker gets in the direct path between a client and a server and eavesdrops on their conversation
4. Dumpster Diving	D. A software program designed to damage or take other unwanted actions on a computer system
5. FTP bounce	E. A technique used to retrieve information that could be used to carry out an attack on a network

✓ Correct

Types of network attacks are described below:

- ✓ **Malware:** A software program designed to damage or take other unwanted actions on a computer system
- ✓ **EMI interception:** An attacker copies information traveling over the wire
- ✓ **Man-in-the-middle:** An attacker gets in the direct path between a client and a server and eavesdrops on their conversation
- ✓ **FTP bounce:** An attacker sends a PORT command specifying the IP address of a third party
- ✓ **Dumpster diving:** A technique used to retrieve information that could be used to carry out an attack on a network

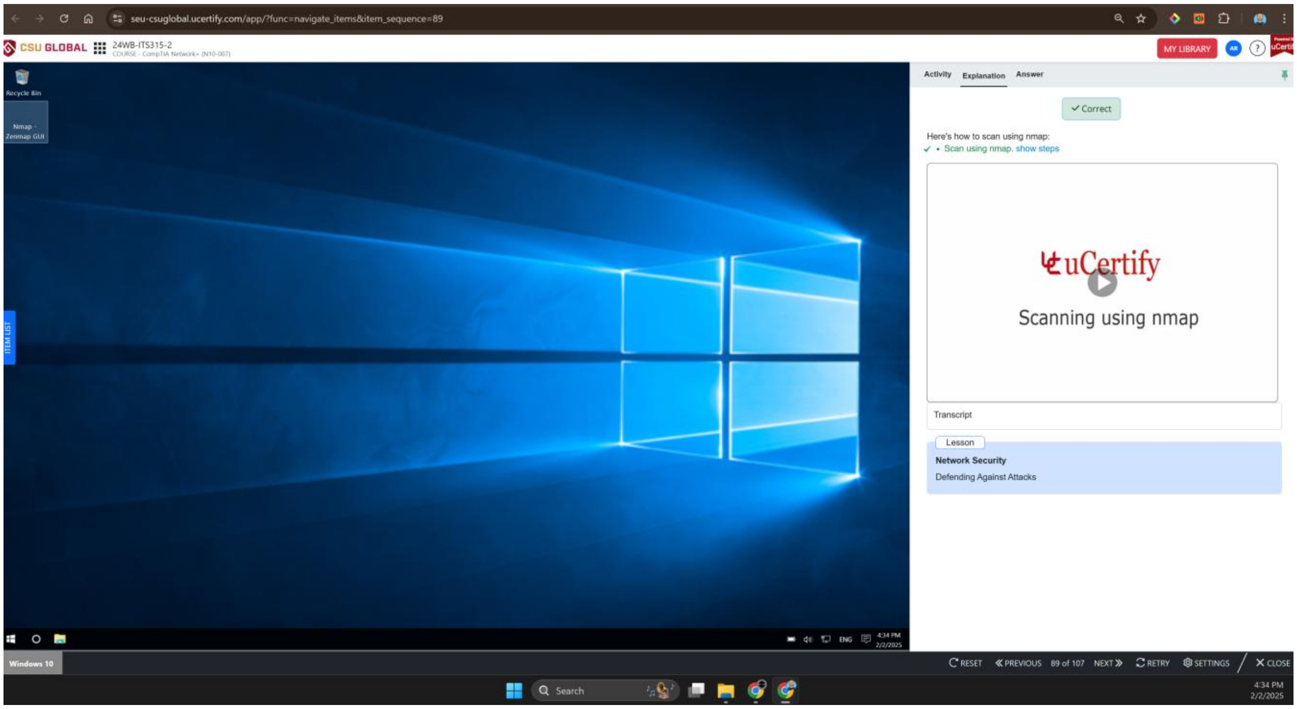
Lesson

Network Security

Categories of Network Attacks

Figure 2

12.3.7 Scanning using nmap



✓ Correct

Here's how to scan using nmap:

- ✓ Scan using nmap. show steps

Transcript

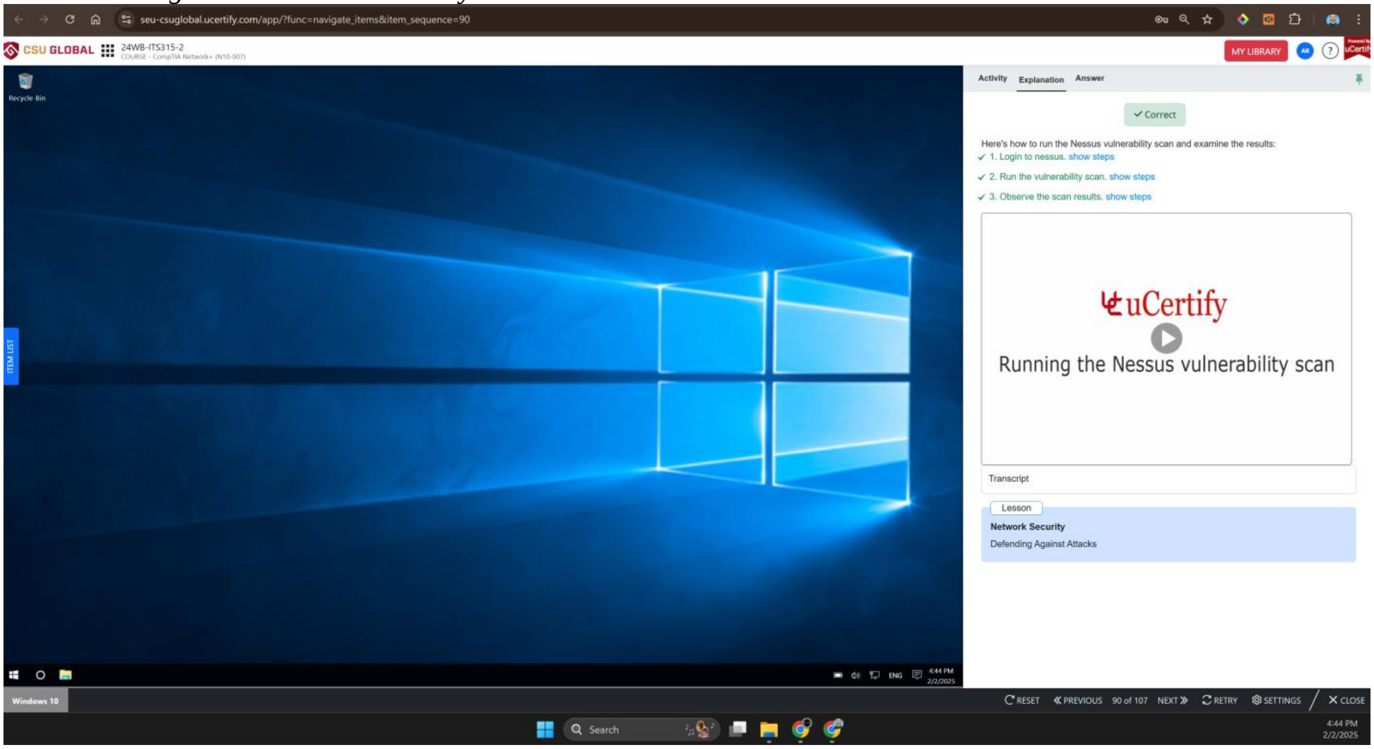
Lesson

Network Security

Defending Against Attacks

Figure 3

12.3.8 Running the Nessus vulnerability scan



Here's how to run the Nessus vulnerability scan and examine the results:

- ✓ 1. Login to nessus. show steps
- ✓ 2. Run the vulnerability scan. show steps
- ✓ 3. Observe the scan results. show steps

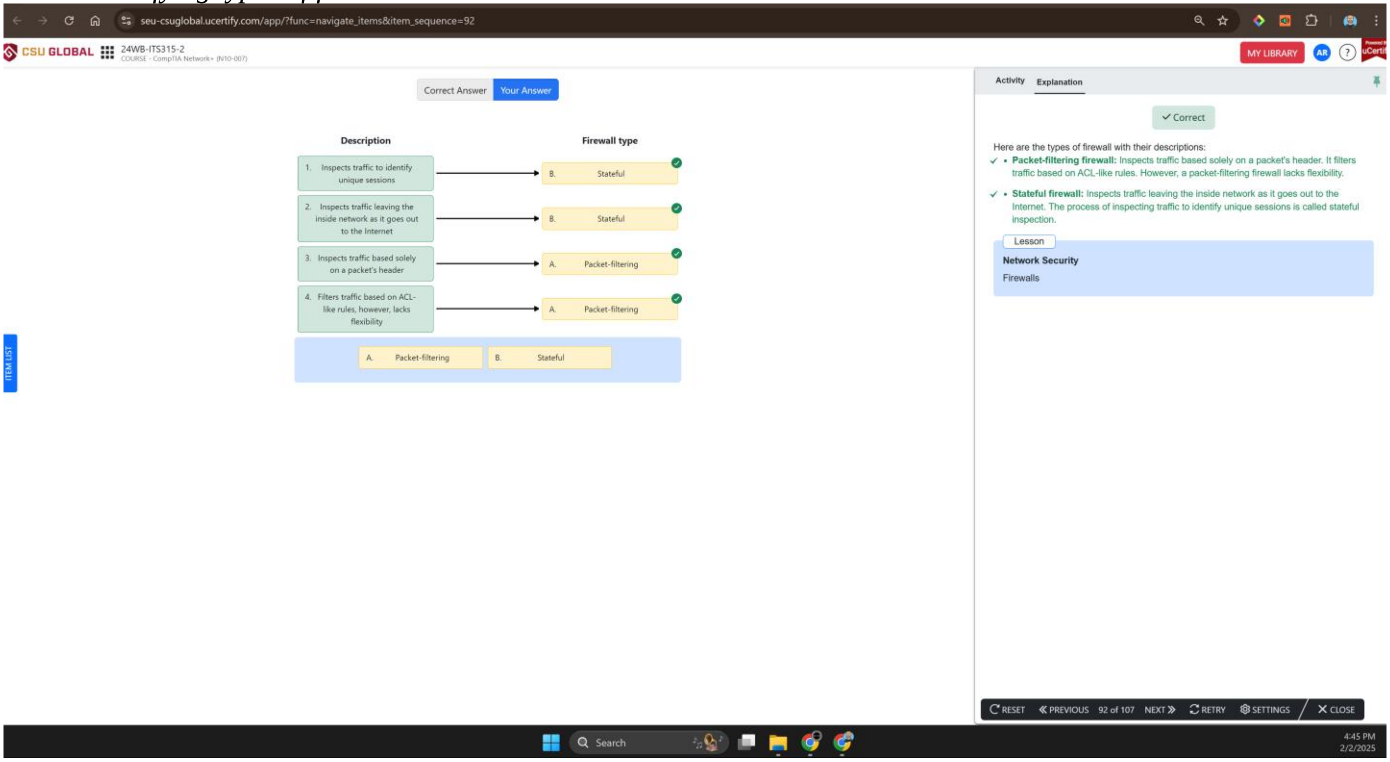
Running the Nessus vulnerability scan

Network Security

Defending Against Attacks

Figure 4

12.5.3 Identifying types of firewall



Description	Firewall type
1. Inspects traffic to identify unique sessions	B. Stateful ✓
2. Inspects traffic leaving the inside network as it goes out to the Internet	B. Stateful ✓
3. Inspects traffic based solely on a packet's header	A. Packet-filtering ✓
4. Filters traffic based on ACL-like rules, however, lacks flexibility	A. Packet-filtering ✓

Here are the types of firewall with their descriptions:

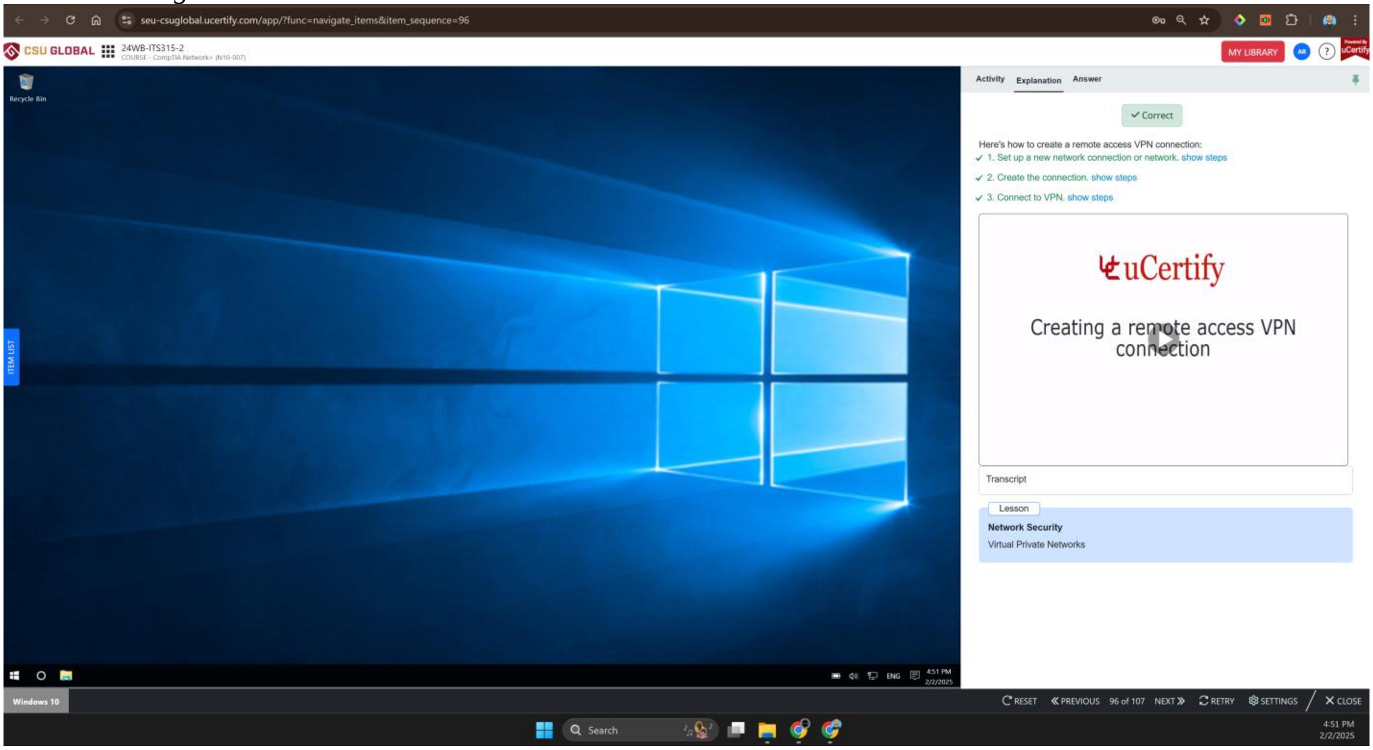
- ✓ **Packet-filtering firewall:** Inspects traffic based solely on a packet's header. It filters traffic based on ACL-like rules. However, a packet-filtering firewall lacks flexibility.
- ✓ **Stateful firewall:** Inspects traffic leaving the inside network as it goes out to the Internet. The process of inspecting traffic to identify unique sessions is called stateful inspection.

Network Security

Firewalls

Figure 5

12.6.1 Creating a remote access VPN connection



Here's how to create a remote access VPN connection:

- ✓ 1. Set up a new network connection or network. show steps
- ✓ 2. Create the connection. show steps
- ✓ 3. Connect to VPN. show steps

Figures 1 through 5 show that all the lab questions were answered correctly.