

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.

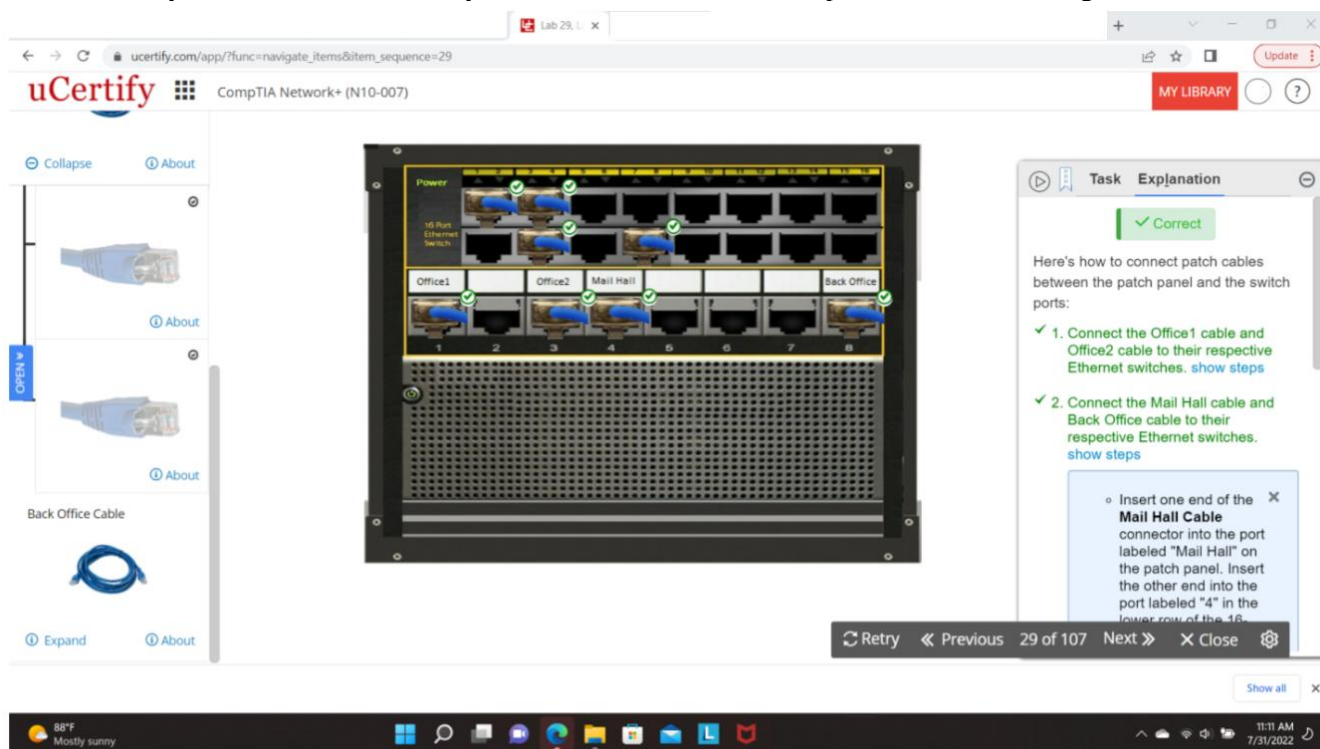
Access uCertify and login, go to Labs, and complete the tasks in the following lab simulations:

- 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 connection

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.



Screenshots

Figure 1
12.2.9 Identifying network attacks

The screenshot shows a web browser window displaying a quiz on the uCertify platform. The URL is `seu-csuglobal.ucertify.com/app/?func=navigate_items&item_sequence=88`. The quiz is titled "12.2.9 Identifying network attacks".

The main content area displays a matching exercise with two columns:

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

Arrows indicate the correct matches: 1 to D, 2 to C, 3 to A, 4 to E, and 5 to B. The "Correct Answer" button is highlighted.

On the right side, the "Explanation" tab is active, showing a "Correct" status and a list of network attack types:

- ✓ **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

The bottom of the screen shows a Windows 10 taskbar with the time 4:30 PM on 2/2/2025.

Figure 2
12.3.7 Scanning using nmap

The screenshot shows a web browser window displaying a quiz on the uCertify platform. The URL is `seu-csuglobal.ucertify.com/app/?func=navigate_items&item_sequence=89`. The quiz is titled "12.3.7 Scanning using nmap".

The main content area displays a video player with the title "Scanning using nmap". The video player shows the uCertify logo and the text "Scanning using nmap".

On the right side, the "Explanation" tab is active, showing a "Correct" status and a list of steps for scanning using nmap:

- ✓ **Scan using nmap, show steps**

The bottom of the screen shows a Windows 10 taskbar with the time 4:34 PM on 2/2/2025.

Figure 3**12.3.8 Running the Nessus vulnerability scan**

The screenshot shows a uCertify quiz page. The main content area displays a Windows 10 desktop background. On the right, the quiz interface includes a 'Correct' status, a list of steps to run a Nessus scan, and a video player titled 'Running the Nessus vulnerability scan'. The video player shows the uCertify logo and a play button. Below the video is a 'Transcript' section with a 'Lesson' tab selected. The bottom of the screen shows a Windows taskbar with the search bar and several icons.

Activity **Explanation** **Answer**

✓ **Correct**

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

Transcript

Lesson

Network Security
Defending Against Attacks

RESET PREVIOUS 90 of 107 NEXT RETRY SETTINGS CLOSE

4:44 PM 2/2/2025

Figure 4**12.5.3 Identifying types of firewall**

The screenshot shows a uCertify quiz page. The main content area displays a matching exercise where descriptions of firewall types are matched to their names. The descriptions are: 1. Inspects traffic to identify unique sessions, 2. Inspects traffic leaving the inside network as it goes out to the Internet, 3. Inspects traffic based solely on a packet's header, and 4. Filters traffic based on ACL-like rules, however, lacks flexibility. The firewall types are: A. Packet-filtering and B. Stateful. The correct matches are: 1 to B, 2 to B, 3 to A, and 4 to A. The bottom of the screen shows a Windows taskbar with the search bar and several icons.

Correct Answer **Your Answer**

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

A. Packet-filtering B. Stateful

Activity **Explanation**

✓ **Correct**

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.

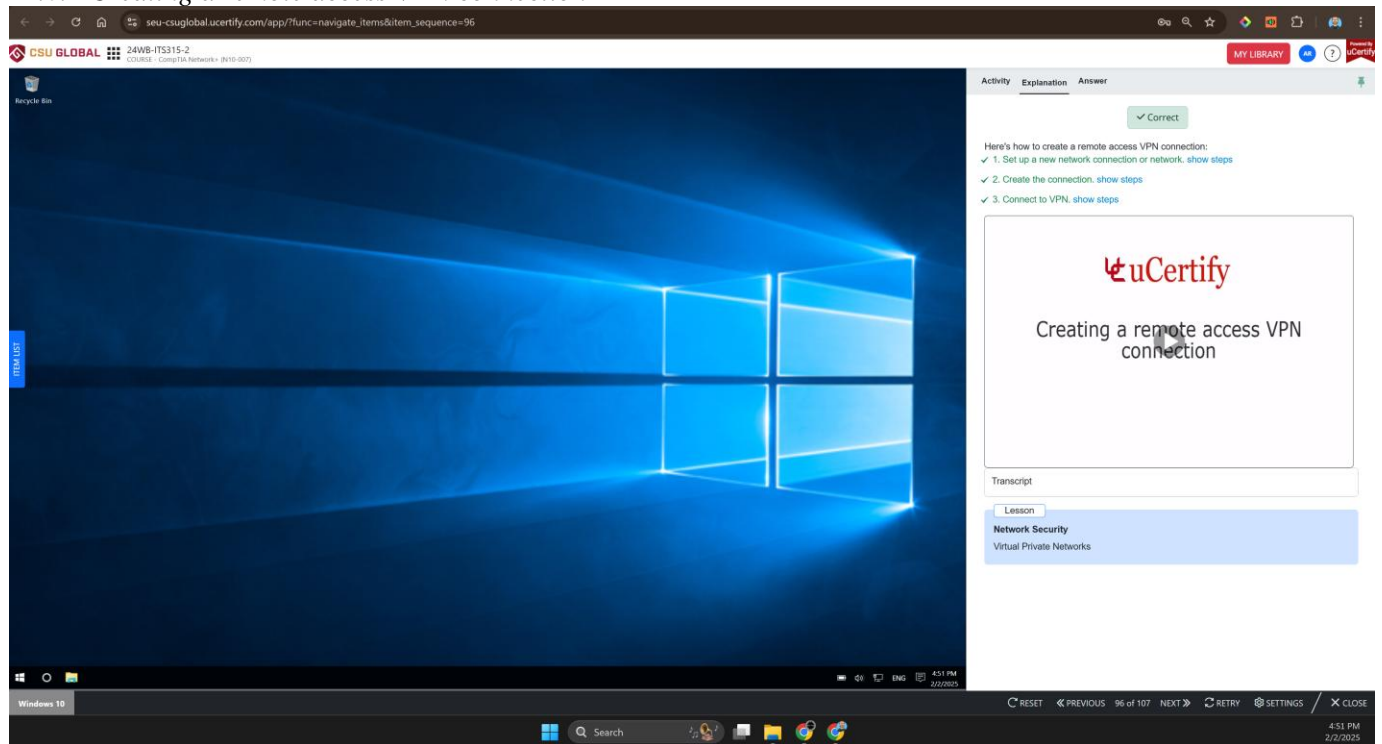
Lesson

Network Security
Firewalls

RESET PREVIOUS 92 of 107 NEXT RETRY SETTINGS CLOSE

4:45 PM 2/2/2025

Figure 5
12.6.1 Creating a remote access VPN connection



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