Introduction to Wireshark lab quiz

Due 8 Feb at 23:59 | Points 5 | Questions 4 | Available until 23 Mar at 17:00
Time Limit None | Allowed Attempts 2

Take this lab quiz

Attempt	Time	Score
LATEST	1 minutes	5 out of 5

✓ Correct answers will be available 8 Feb at 23:59 . Sat at 17:00 .

Score for this attempt: 5 out of 5
Submitted 8 Feb at 23:59
This attempt took 1 minutes.

Last attempt details
Time: 1 minutes
Submitted: 8 Feb at 23:59
Current score: 5 out of 5
Final score: 5 out of 5

2 More Attempts available
Take this quiz again
Will keep the highest of all your scores

Attempt history

Page 1,of 3

In this course, we will be using the Wireshark network packet sniffer to study protocols in action. Wireshark is a free, open-source network packet sniffer. Download the latest version of Wireshark from www.wireshark.org/download/ .

We expect you to install a stable version of Wireshark and complete the process lab. Wireshark is a powerful tool that can be used to capture and analyze packets sent and received by your computer. Wireshark can be used to troubleshooting network problems, to detect malicious traffic, and to reverse engineer network protocols.

Feel free to explore around on your own. Wireshark is a very powerful, and very complex, tool.

Please proceed.

Since understanding of network protocols can often be greatly deepened by seeing them in action, we'll be using Wireshark throughout the course to explore the operation of various protocols, and to gain a deeper understanding of network protocols and network services. This will be done in a hands-on, "learn by doing" manner. Wireshark is a powerful network measurement and analysis tool, and it can be used for many purposes. We may also be able to use Wireshark to help us understand the operation of various network services. Wireshark is also a very powerful "learn by doing" tool for understanding how network protocols are implemented and operate. Wireshark can be used to capture packets sent and received by applications and network services running on your computer, for example, web browsers, email clients, and network services. Wireshark can also be used to capture packets sent and received by applications and network services running on other computers that are sent and received through applications and network services running on your computer. Wireshark can also be used to capture packets that are sent and received between two other computers, for example, between two web servers.

Figure 1 shows the network topology we will be using for our lab. In the rest of Figure 1, we see the various protocols and applications that we will be using in our lab exercises. We will be using the ping protocol, the DNS protocol, the HTTP protocol, and the telnet protocol. We will also be using the telnet application, the web browser application, and the command line ping application. We will be using the telnet application to log into a remote server and then use the telnet application to Telnet to a remote server. We will be using the web browser application to access a remote web server. We will be using the ping application to ping a remote server. We will be using the command line ping application to ping a remote server. We will be using Wireshark to capture packets sent and received by these applications and network services. We will be using Wireshark to capture packets that are sent and received between two other computers, for example, between two web servers.

"Tell me and I forget. Show me and I remember. Involve me and I learn."

Chinese proverb

Since understanding of network protocols can often be greatly deepened by seeing them in action, we'll be using Wireshark throughout the course to explore the operation of various protocols, and to gain a deeper understanding of network protocols and network services. This will be done in a hands-on, "learn by doing" manner. Wireshark is a powerful network measurement and analysis tool, and it can be used for many purposes. We may also be able to use Wireshark to help us understand the operation of various network services. Wireshark is also a very powerful "learn by doing" tool for understanding how network protocols are implemented and operate. Wireshark can be used to capture packets sent and received by applications and network services running on your computer. Wireshark can also be used to capture packets that are sent and received between two other computers, for example, between two web servers.

Wireshark is a free, open-source, network packet sniffer. Wireshark can be used to capture packets sent and received by applications and network services running on your computer. Wireshark can also be used to capture packets that are sent and received between two other computers, for example, between two web servers. Wireshark can be used to troubleshooting network problems, to detect malicious traffic, and to reverse engineer network protocols