Computer Networks Theory + Lab

CS252 Labs ▾ > Lab09: DNS and Web ▾   ▼

Summary	Contents
	1. Lab09: Instructions (Document)

📄

Lab09: Instructions

Lab05: HTTP

Objective:

1. Learn how DNS works via dig
2. Learn how HTTP works via interpreting Wireshark based traces

Reference:

1. DNS, WWW videos on BodhiTree; especially the DNS demo video
2. https://linuxize.com/post/how-to-use-dig-command-to-query-dns-in-linux/ (dig)

Lab Instructions:

Part 1: DNS

Look at the reference sheet for the dig command and also the demo video. Play around with various arguments. dig works in WSL (windows) as well.

Answer the quiz "Lab09-DNS".

Part 2: WWW

We have studied about HTTP . Let us see it in action. The Safe quiz related to all the below parts is at "Lab09-http".

Part A: Simple HTTP Image download

We will start with a simple experiment involving downloading an image from a HTTP website. Through this we will explore HTTP format and client/server communication. Note you cannot use any HTTPS websites since you cannot explore application layer data since it is all encrypted.

Guidance:

1. Start your browser and ensure that there are no other tabs to avoid unnecessary background traffic.
2. Identify a http website and identify an image within. Select the image and then right click and do copy location and then paste it in a browser. This will give you the URL of the image. DO NOT press enter yet.
3. Start a wireshark trace. Then go to the browser and load the image. Save the trace.
4. Open the trace and ideally you should filter it based on the IP address of the http website (you can use ping to determine the ip address corresponding to the domain of the URL).
5. Explore the packets in the trace.

It is strongly recommended that you do this experiment yourself and collect your own trace. We have however provided a trace (http-image.pcapng) based on which answer Part A of the quiz "Lab09-HTTP". You can answer the same questions based on your trace too, but this if for practice and is not graded.

Part B: HTTP Conditional GET

You must have read of conditional GET aspect of HTTP to conserve network bandwidth. Let us explore this.

Guidance:

1. You can continue to work with the same image URL as before. But we will start this exercise afresh.
2. Before you load the page, first clear the browser cache. For Firefox: Options ☐ Privacy & Security ☐ Cookies & Site Data ☐ Clear Data. Check "Clear cached web content" and press clear. For Chrome: Setting ☐ Privacy & Security ☐ Clear browsing data. Check "cached images and files" and press clear data.
3. Start the Wireshark trace.
4. Load the image URL (http ONLY)
5. Right away, enter the same URL into your browser again by clicking the reload button.
6. Stop the trace, save and then explore.

It is strongly recommended that you do this experiment yourself and collect your own trace. We have however provided a trace (http-not-modified.pcapng) based on which answer Part B of the quiz "Lab09-HTTP". You can answer the same questions based on your trace too, but this if for practice and is not graded.

Part C: HTTP with many embedded objects

Let us explore a more complex case of downloading a page with many embedded objects.

Guidance:

1. Work with any http website, just ensure it has many embedded objects (e.g. http://www.barc.gov.in/).

2. Before you load the page, good to clear the browser cache.
3. Start the Wireshark trace.
4. Load the URL (http ONLY)
5. Once it fully loads, stop the trace, save and then explore.

It is strongly recommended that you do this experiment yourself and collect your own trace. We have however provided a trace (http-iitb.pcapng, when iitb website was http, not https) based on which answer Part C of the quiz "Lab09-HTTP". You can answer the same questions based on your trace too, but this if for practice and is not graded.
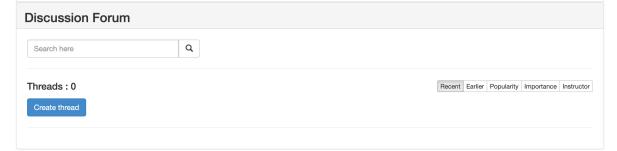
Part D: HTTP with authentication

How safe is HTTP? Let us look at a website which has a login screen.

Guidance:

1. You need to identify a http webpage which has a login screen. You can use http://testphp.vulnweb.com/login.php
2. Before you load the page, good to clear the browser cache.
3. Start the Wireshark trace.
4. Load the required URL. Enter username and password and click "login".
5. Once the page changes, stop the trace, save and then explore.

It is strongly recommended that you do this experiment yourself and collect your own trace. We have however provided a trace (http-auth.pcapng) based on which answer Part D of the quiz "Lab09-HTTP". You can answer the same questions based on your trace too, but this if for practice and is not graded.

[View Document]

Discussion Forum

Search here 🔍

Threads : 0

Recent | Earlier | Popularity | Importance | Instructor

[Create thread]