**HTTP Tutorial**

Overview

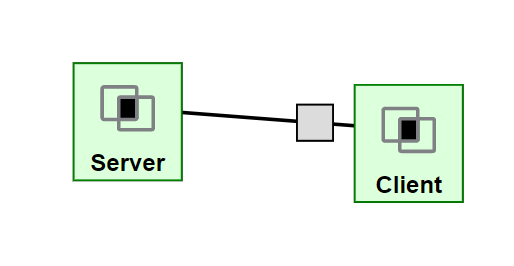
This tutorial will help you to get familiar with HTTP protocol. You will also become familiar with an HTTP Proxy, called ZAP, and looking at how HTTP works behind the scenes. First, we need to complete basic lab setup, as we would do with our GENI labs.

Lab Environment

RSPEC file:

<https://raw.githubusercontent.com/informationcomputerscience/EdGENI/master/Rspec-Files/WebGoat-Rspec.txt>

Lab Topology



For this lab, our topology will consist of two hosts. We will have a Server machine, where the WebGoat Web server is hosted. We also have a Client machine, where user can launch Firefox to visit the WebGoat Web server and run Zap, the HTTP Proxy tool to manipulate the HTTP transaction.

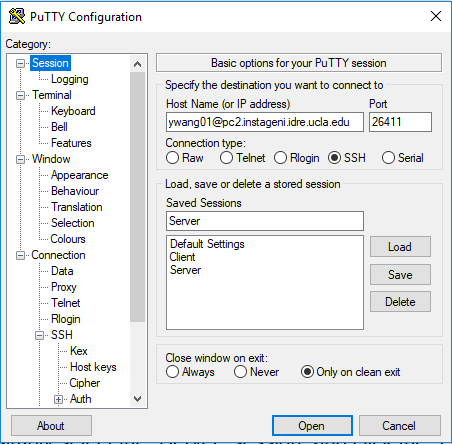
Preparation

This lab will use the GENI environment that you set up in Environment Setup. If you haven’t set up the environment, please refer to the instruction in Environment Setup.

**How to resume your VNC desktop?**

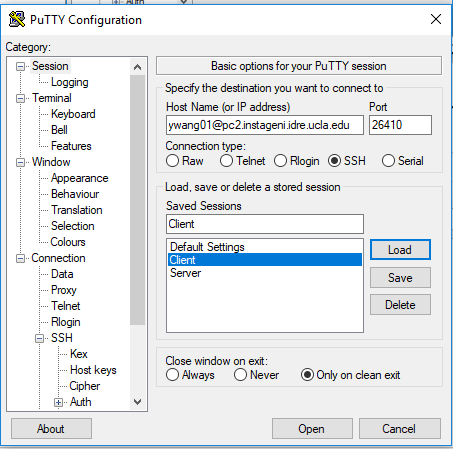
**If you are using your own Windows computer,**

you will have the Server and Client session saved on your Putty, as follows.



With the saved sessions on PuTTY, exiting and resuming your VNC desktop are easy.

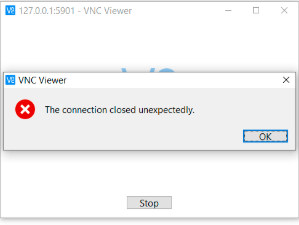
To resume your Client machine desktop, open PuTTY and load the *Client* session you have saved and click Open button to connect.



Type in your passphrase. Open vncviewer, connect with the address 127.0.0.1:5901.You will get to the resumed desktop

**NOTE:**Sometimes, the VNC server on the VM is down for some reasons.

If you failed to connect to the VNC server and get the below message, your VNC server might be down.



To verify if the VNC server is really down, type in the command **ps -ef | grep vnc** and if you see a result like below (only the *grep* process is listed), that means the VNC server is down.



In this case, you have to start the vncserver first. To start the vncserver, type in the following two commands in the PuTTY terminal (do not type in the texts in the parenthesis.):

**vncserver -kill  :1** (which makes sure the old vncserver is killed)

**vncserver** (which starts the vnc server on the Client)

Now you should be able to connect through VNC viewer.

To resume your Server machine desktop, open PuTTY and load the *Server* session you have saved and click Open button to connect. Type in your passphrase. Open vncviewer, connect with the address 127.0.0.1:5902. You will get to the resumed desktop

**NOTE:**Sometimes, the VNC server on the VM is down for some reasons. (Refer to the Client section to verify if the NVC server on the Server VM is down.) In this case, you have to start the vncserver first.To start the vncserver, type in the following two commands in PuTTY terminal:

**vncserver -kill  :2** (to make sure the old vncserver is killed)

**vncserver ：2** (to start the vnc server on the Client)

Now you should be able to connect through VNC viewer.

**If you are using Citrix Virtual Desktop or Mac/ Linux Computer**

Server and Client session might not be saved on your Putty. You need to follow the instruction in “connect to virtual machine” to connect to Client or Server. **Remember do not execute the vncserver or vncserver :2 command again, since you have already started it in Lab 1.**

**How to exit your Lab desktop?**

Simply close the PuTTY/SSH program and VNC viewer.

Task 0 – Start and Visit WebGoat

1. Open a terminal on the Server machine, type in command ifconfig to find out its IP address. It should be in the format of 10.10.x.x. Normally it is 10.10.1.2.
2. On the terminal of the Server, type in the following two commands

cd /vPark

java -jar ./webgoat-server-8.0.0.M24.jar --server.address=<Server IP>

, where <Server IP> is the IP address you found in Task 0A. Wait for a while. The WebGoat is ready when you see the message “Started StartWebGoat in xx.xxx seconds(……)”. Take a screenshot to show you have set up the WebGoat on the Server machine.

1. On the Client machine, type in command firefox & in a terminal to start Firefox.
2. Type in the following address in firefox of Client machine: http://<Server IP>:8080/WebGoat, where <Server IP> is the IP address you found in Task 0A. Take a screenshot showing you can visit the WebGoat on the Client machine.
3. Register an account on WebGoat and log in with your registered account. Remember the account. You will also use it in next week’s lab.

The following labs are all performed on the Client Machine

Task 1 – HTTP Basics

1. Under the “General” tab of WebGoat (on the left bar), click on the “HTTP Basics”.
2. Complete page 1 on the WebGoat page



1. Take a screenshot to show you have completed page 2 on the WebGoat page and answer the question “How does the server handle the HTTP request”.

Task 2 – HTTP Proxy Zap

1. Under the “General” tab of WebGoat (on the left bar), click on the “HTTP Proxies”.
2. Study what a HTTP Proxy is in page 1 on the WebGoat page
3. Start ZAP in your Client Machine by following page 2 on the WebGoat page. Notice the following difference from the WebGoat tutorial:
   1. ZAP is preinstalled under folder /vPark/ZAP\_2.7.0 . You can start ZAP by issue the following commands

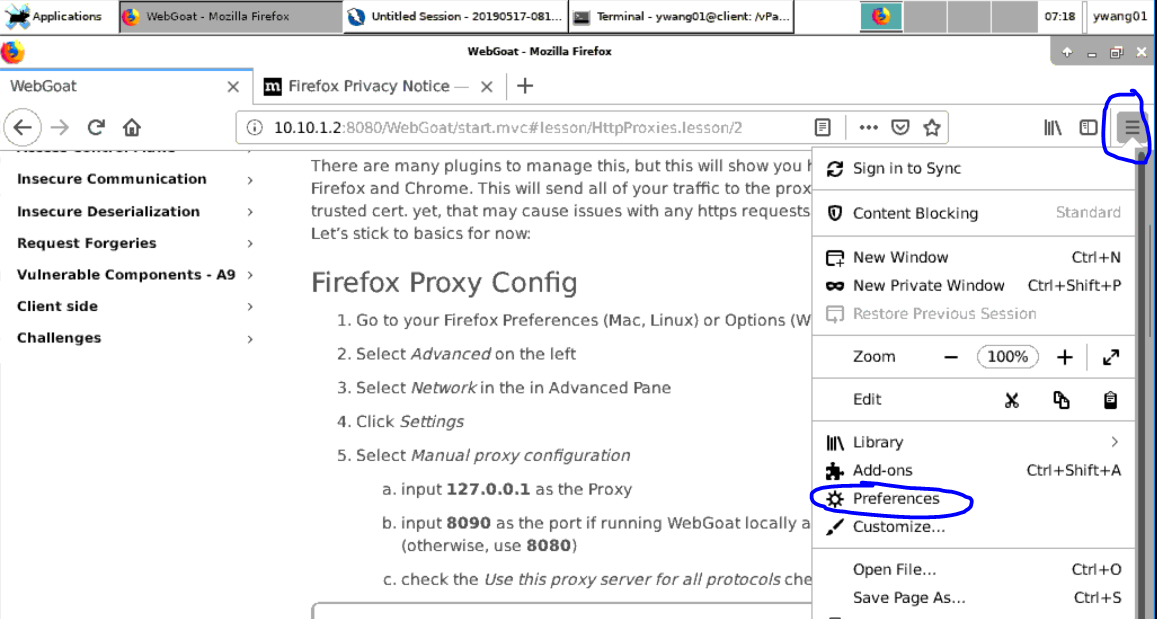
cd /vPark/ZAP\_2.7.0

sudo ./zap.sh

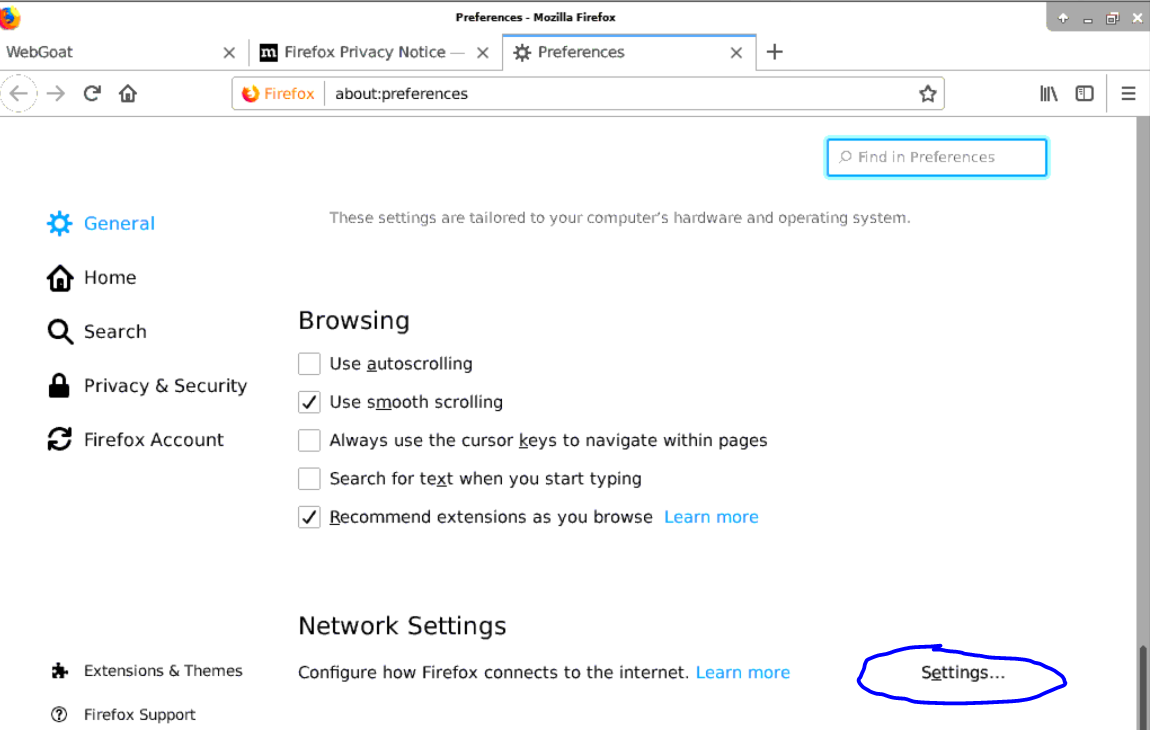
* 1. WebGoat is not running locally. Therefore you don’t need to set ZAP’s port.

Take a screenshot when the ZAP is started.

1. Follow page 3 on the WebGoat page to set up Firefox Proxy. Notice the following differences
   1. The preference menu of Firefox can be found when clicking the “three bar icon” to the right of the address bar, as shown below.



* 1. The Network setting is at the bottom of the “General” category of the preferences. Click the button *Settings…*, you will be able to configure the proxy.



* 1. Since we are not hosting WebGoat locally, use port number 8080, instead of 8090.

1. Make a screenshot like page 4 on the WebGoat page to show ZAP is working.
2. Follow page 5 on the WebGoat page to exclude internal requests. Notice the following difference from the instruction.
   1. Since we are hosting WebGoat server on the Server machine, you need to replace “localhost” with the IP address of Server machine. (To find IP address, refer to Task 0A, normally, the IP address is 10.10.1.2).
3. Follow page 6 on the WebGoat page to intercept and modify an HTTP request. Describe what will happen when you click the “Submit” button on WebGoat and how did you modify the HTTP request. Take a screenshot to prove your modification. Take a screenshot to show what did you see when submitting a modified request (Hint: If you saw a message under the text field saying “Well done, ……”, your work is correct).
4. Click the *General🡪HTTP Basics* item on the WebGoat menu, and select page 3 on the WebGoat page. Complete the Quiz by using ZAP. Make a screenshot proving completing the Quiz.(Hint: you should see a message saying “Congratulations. …”, if you have filled in the form with correct information.)