# Basic Web Attacks—Teacher Notes

This lesson assumes that the student is aware of web browsers, web servers, and HTML, but the student does not need much experience to do this lesson in Easy and Medium mode. In Hard mode, some experience is required, but inquisitive students should be able to follow along.

## Primary Learning Point

Anything that executes in a browser or any data returned by a browser to a web site can be edited or manipulated by a knowledgeable user. The web designer should keep this in mind at all times and keep all critical data on the server. Trust nothing that comes from the user or a browser.

## Requirements

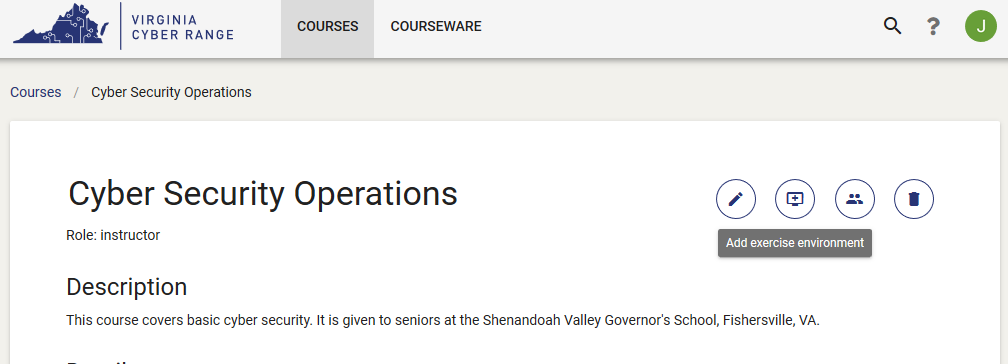
The basic lesson requires nothing but a browser and Internet access. This lesson uses the Chrome browser and the Developer tools that are part of the Chrome browser.

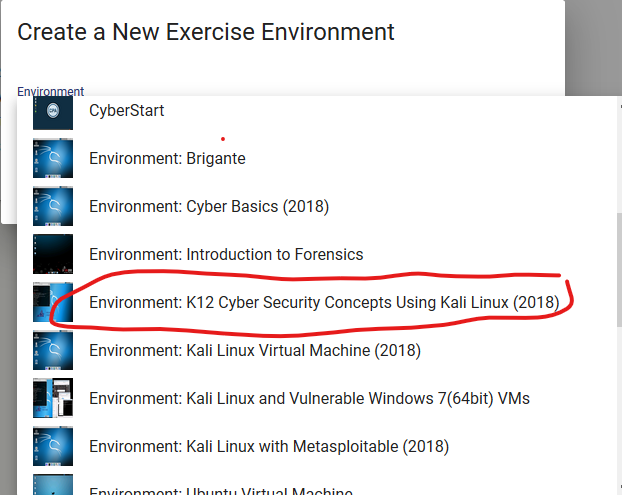
The optional lesson requires the use of Burp Suite, Web Application testing software. Burp Suite may be blocked by school networks because it can be used as a hacking tool. However, Burp Suite is installed on Kali Linux, which you can download and use if you have software like VMware Workstation Player <https://www.vmware.com/products/workstation-player.html> (They will let you pay for Workstation Player, but the license when you install it says the Workstation Player is free for academic use.)

## Virginia Cyber Range

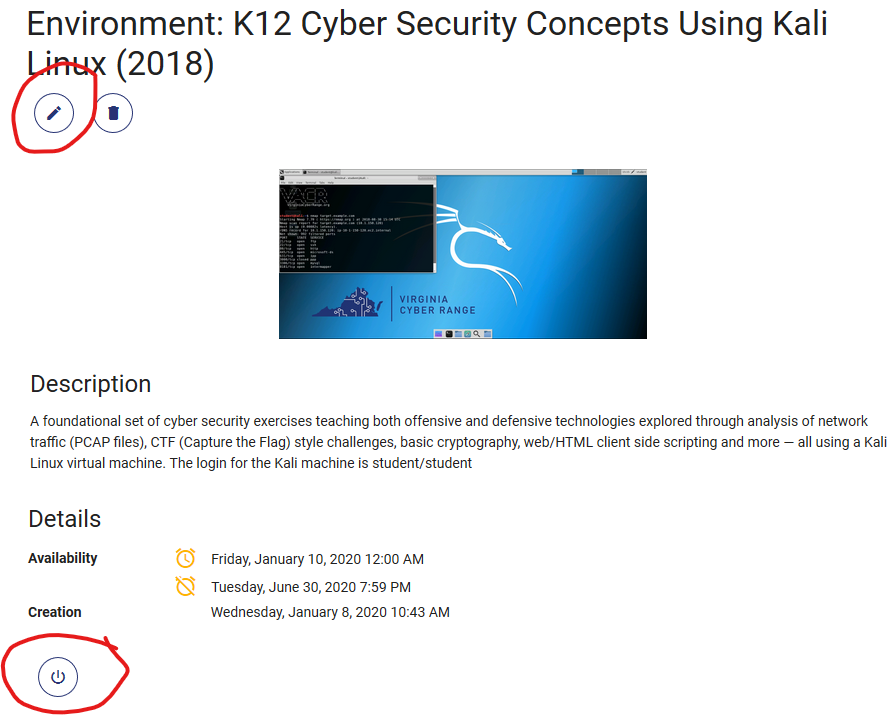
Kali Linux is availble to Virginia students and teachers through the Virginia Cyber Range, so the optional Burp Suite lesson can be done there. The instructor can also customize the environment ahead of time so the students do not have to spend class time configuring Burp and their browsers.

### Create an Environment

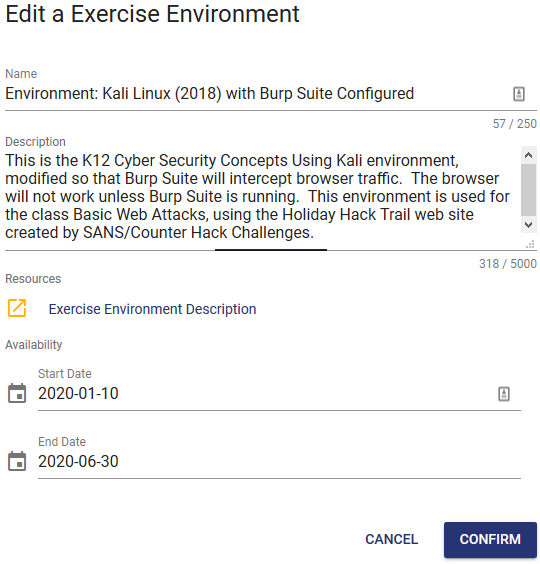
Add an Exercise Environment to your course.  


There are several Kali environments available, but not all of them can browse the Internet. I chose *K12 Cyber Security Concepts Using Kali Linux (2018)* for that reason.  


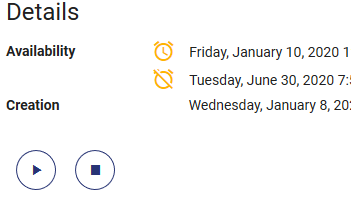
### Start the Environment

Click the Environment you just created, and you should see a page that allows you to edit the environment. The Power icon in the bottom left allows you to power the VM on.  
  


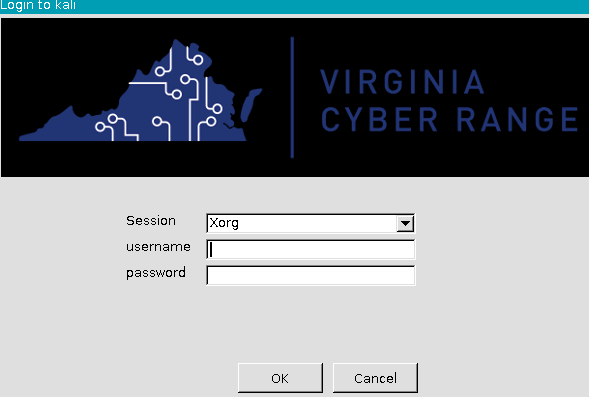
The pencil icon in the top left allows you to change the Name, Description, and Dates for the course. I changed the Name and Description as shown below.



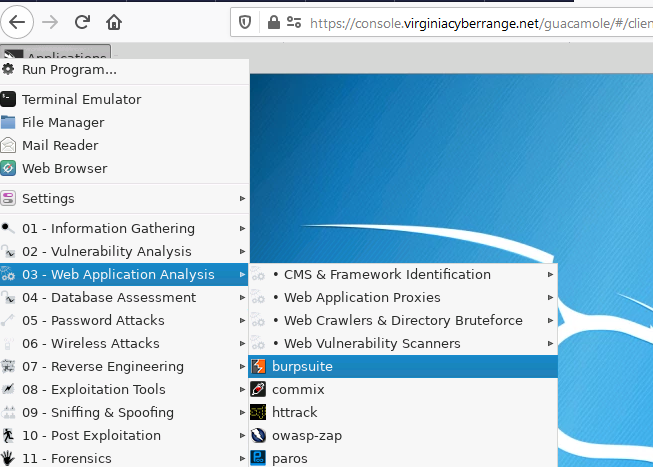
Start the VM using the Power button (bottom left.) The Power button should change to Play (Join) and Stop buttons.



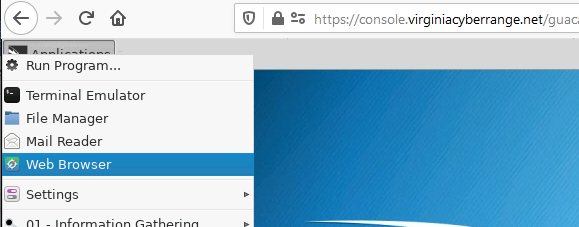
You should get a new window to log in to the VM. User is student, password is student. Hmm, I need to add the username and password to the description.

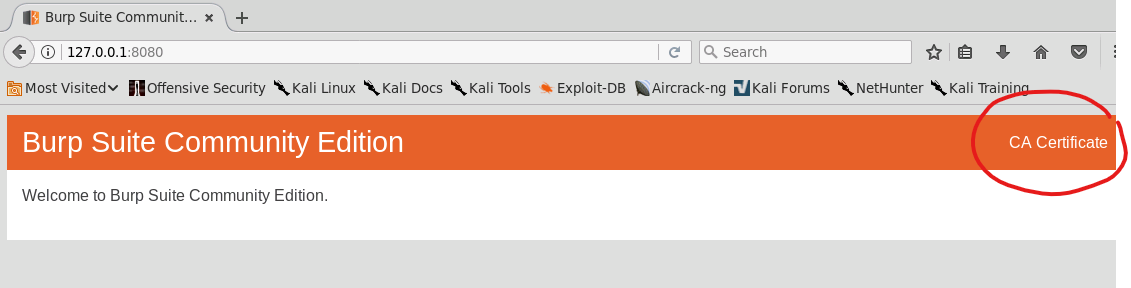


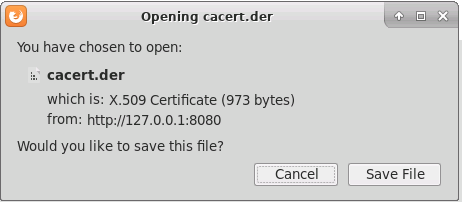
### Configure Burp and the Browser

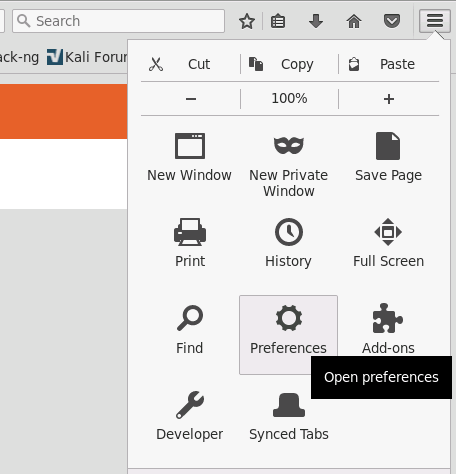
Start Burp Suite. (We need it running so we can grab its certificate.)  


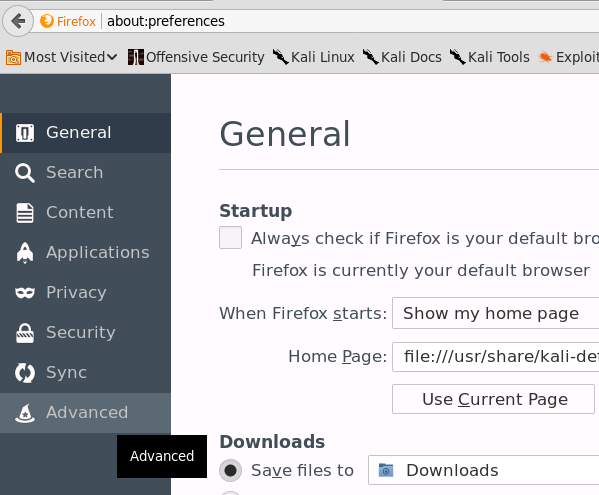
Start the web browser

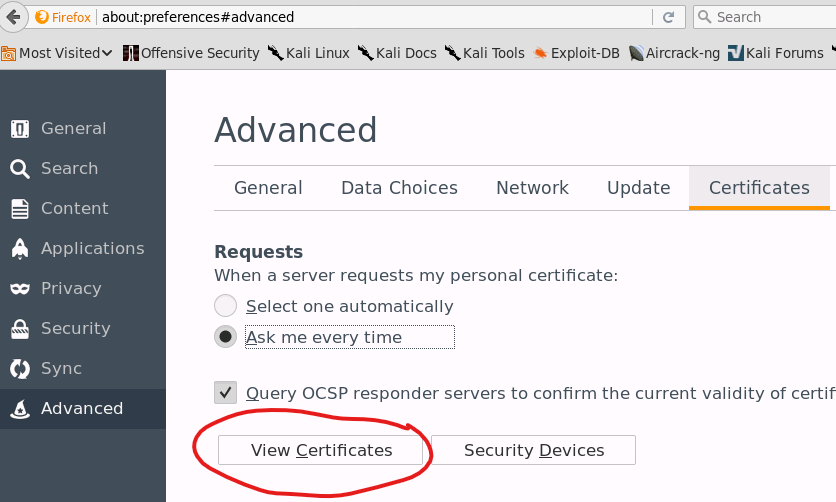


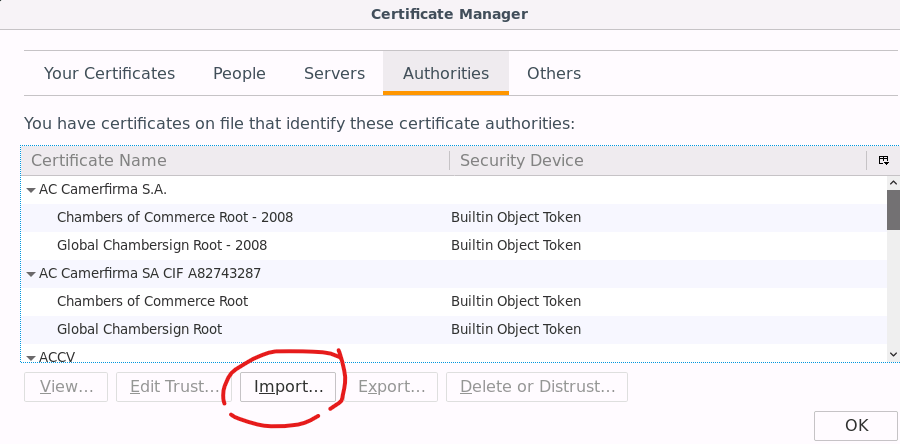
Enter 127.0.0.1:8080 in the browser navigation bar and enter.  


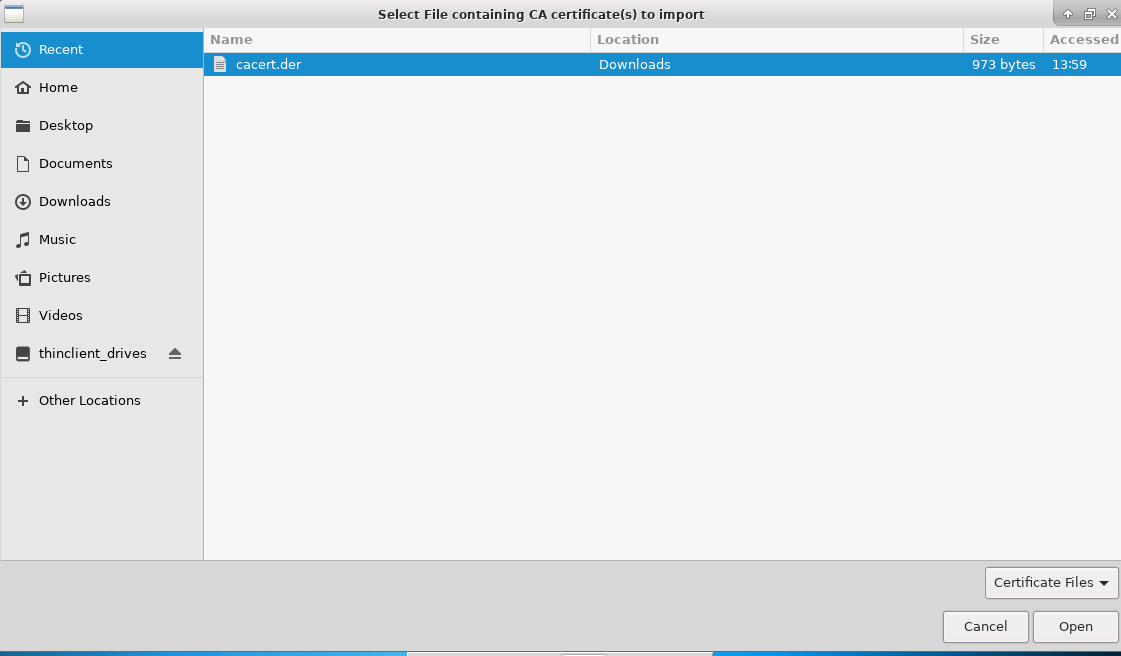
Click on CA Certificate and save the certificate.  


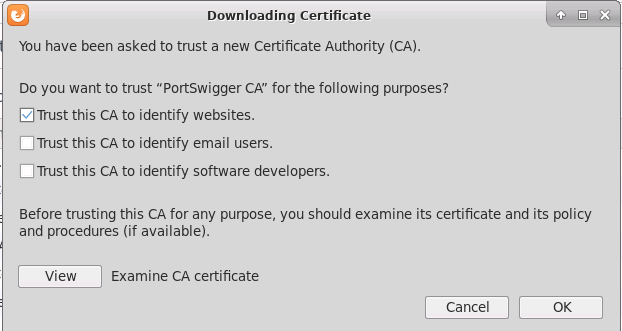
Select Preferences  


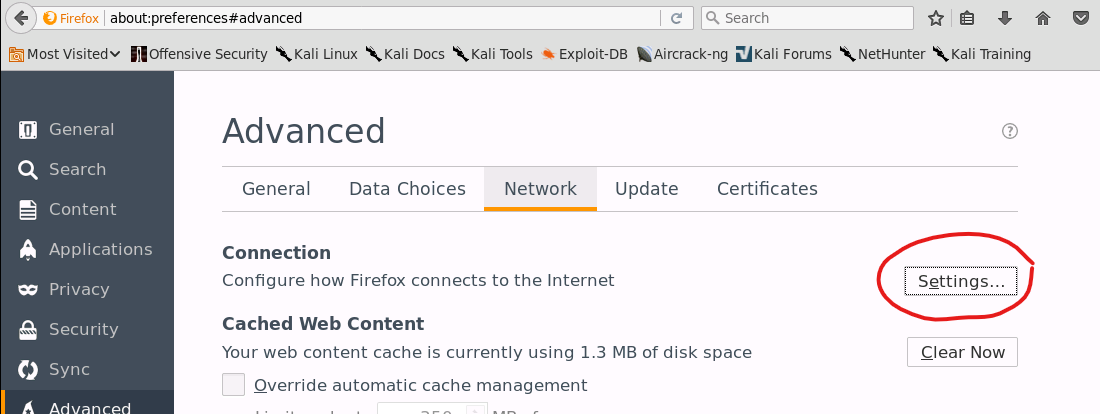
Select Advanced  


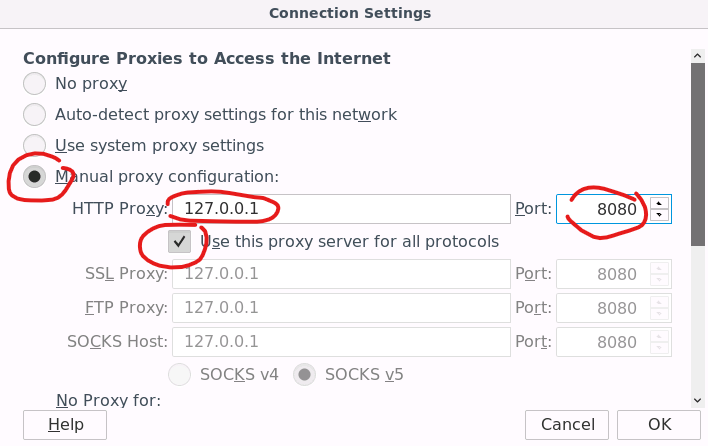
Select Certificates, and click View Certificates  


Select Import  


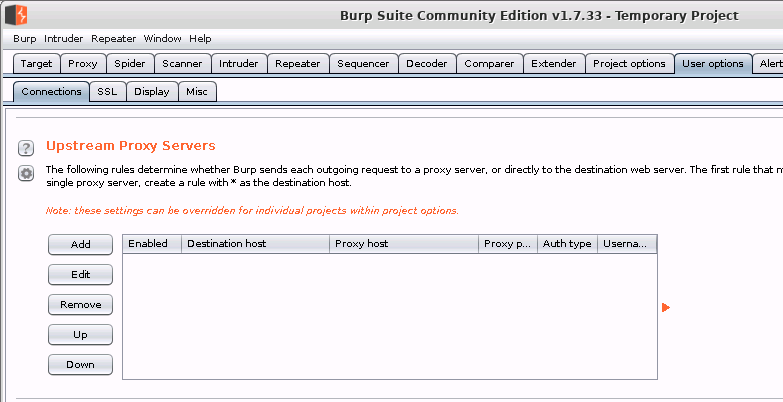
Select the certificate you downloaded, cacert.der, and click open.  


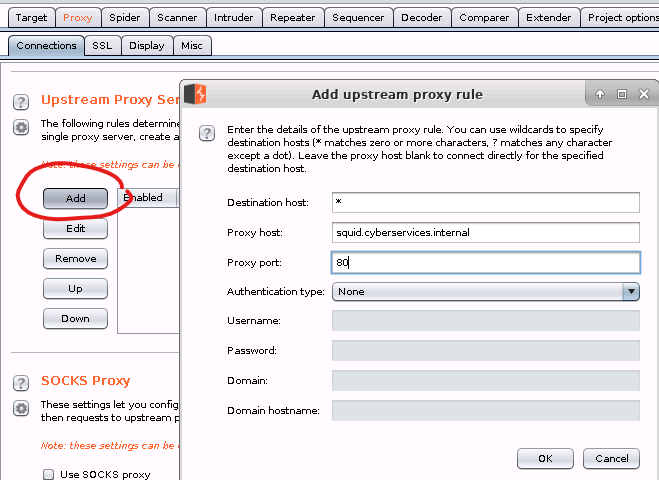
Select “Trust this CA to identify websites” and click OK.  


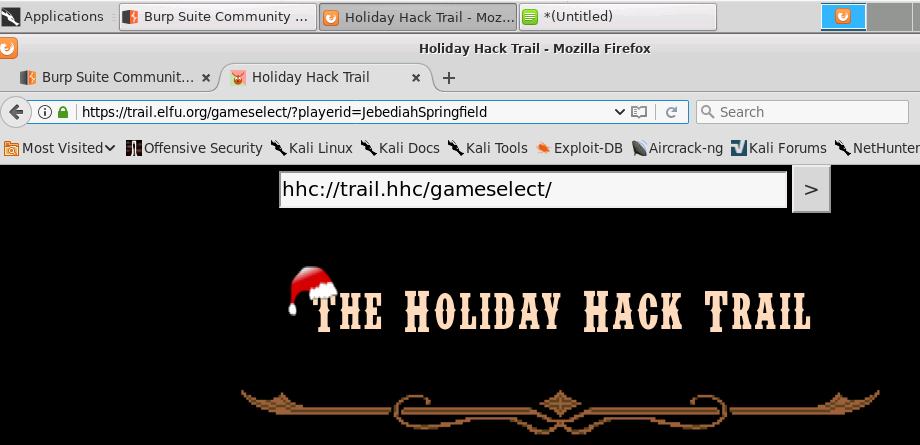
Go back to advanced preferences as we need to configure the web site to send its requests to the Burp proxy. With Network selected, click on Connection Settings.  


Select Manual proxy configuration, enter 127.0.0.1 and port 8080. Select “Use this proxy for all protocols” and click OK.  


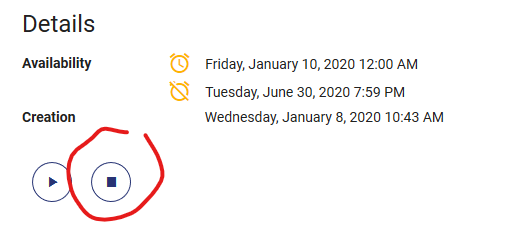
Configure Burp Suite. We need to tell Burp to send its data to the VACR proxy, and not straight to the Internet. VACR blocks Internet requests that don’t go through their proxy.

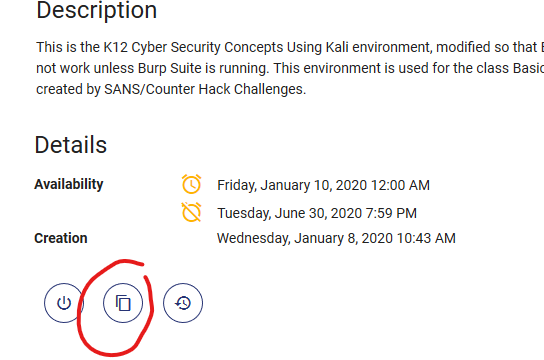
In Burp Suite select User Options and scroll down to Upstream Proxy Servers.  


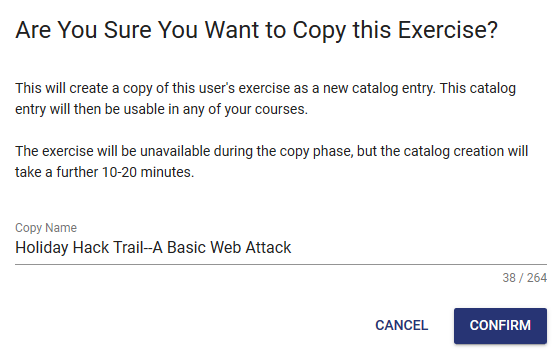
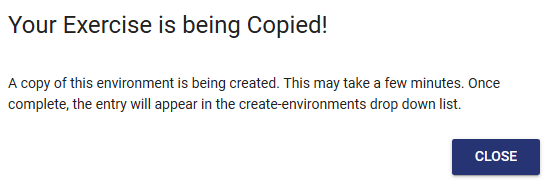
Click Add. Enter \* in Destination host, squid.cyberservices.internal in Proxy host, and 80 in Proxy port. Click OK.  


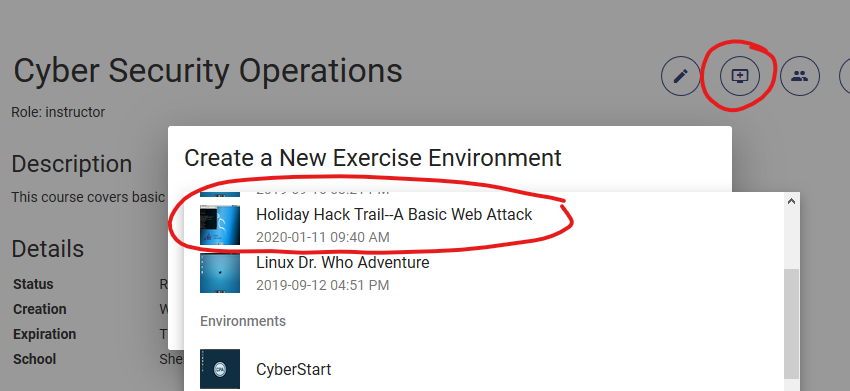
Browse to trail.elfu.org. If everything is working, you should see the Holiday Hack Trail.  


## Save the changes you made in VACR

Close the console window and click the Stop icon on the VACR page.  


Once you’ve done that, the icons should change and give you a Copy icon. Click it.  


Name the copy and click Confirm.  
  
  


Once the elves have done their work behind the scenes, you’ll be able to create a new Exercise Environment with your changes included.  


Be sure to test it well before class starts!