

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.

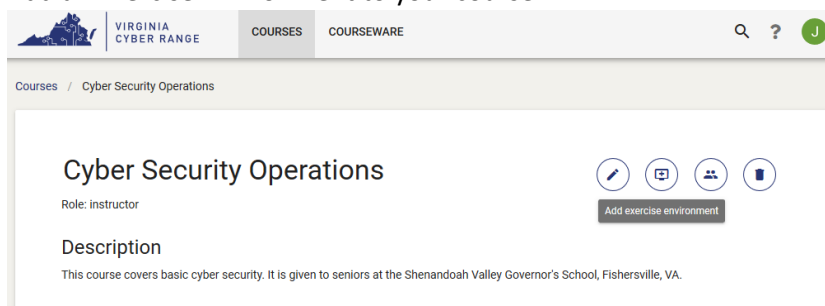
The [optional lesson](#) requires the use of Burp Suite, Web Application testing software. Burp Suite may be blocked by school networks because it can be used as a hacking tool. However, Burp Suite is installed on Kali Linux, which you can download and use if you have software like VMware Workstation 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

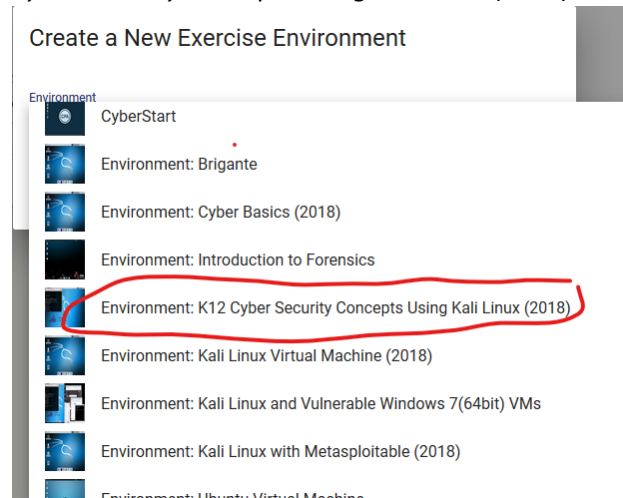
Kali Linux is available to Virginia students and teachers through the Virginia Cyber Range, so the optional Burp Suite lesson can be done there. The instructor can also customize the environment ahead of time so the students do not have to spend class time configuring Burp and their browsers.

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.

Environment: K12 Cyber Security Concepts Using Kali Linux (2018)



Description

A foundational set of cyber security exercises teaching both offensive and defensive technologies explored through analysis of network traffic (PCAP files), CTF (Capture the Flag) style challenges, basic cryptography, web/HTML client side scripting and more -- all using a Kali Linux virtual machine. The login for the Kali machine is student/student

Details

Availability

Friday, January 10, 2020 12:00 AM

Tuesday, June 30, 2020 7:59 PM


Creation


Wednesday, January 8, 2020 10:43 AM




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.



Edit a Exercise Environment


Name
Environment: Kali Linux (2018) with Burp Suite Configured 

Description
57 / 250
This is the K12 Cyber Security Concepts Using Kali environment, modified so that Burp Suite will intercept browser traffic. The browser will not work unless Burp Suite is running. This environment is used for the class Basic Web Attacks, using the Holiday Hack Trail web site created by SANS/Counter Hack Challenges. 

Resources
318 / 5000
 [Exercise Environment Description](#)

Availability



Start Date
 2020-01-10 

End Date
 2020-06-30

[CANCEL](#) [CONFIRM](#)

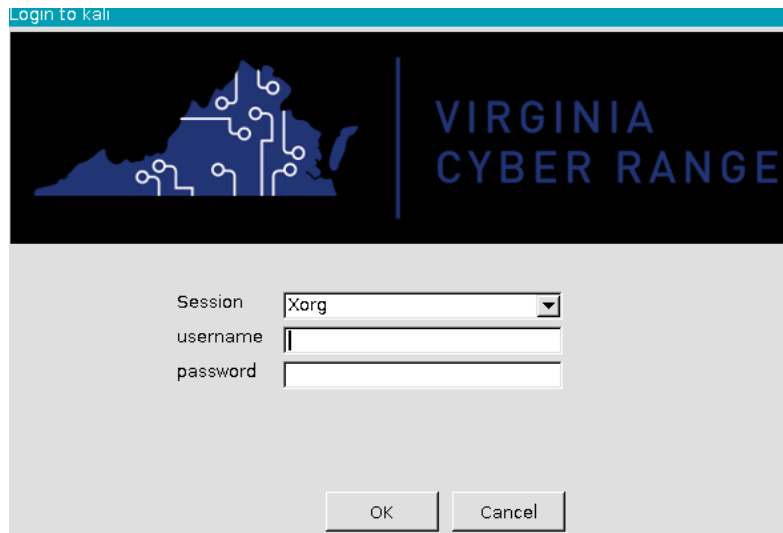
Start the VM using the Power button (bottom left.) The Power button should change to Play (Join) and Stop buttons.

Details

Availability  Friday, January 10, 2020 1
 Tuesday, June 30, 2020 7:
Creation Wednesday, January 8, 20:

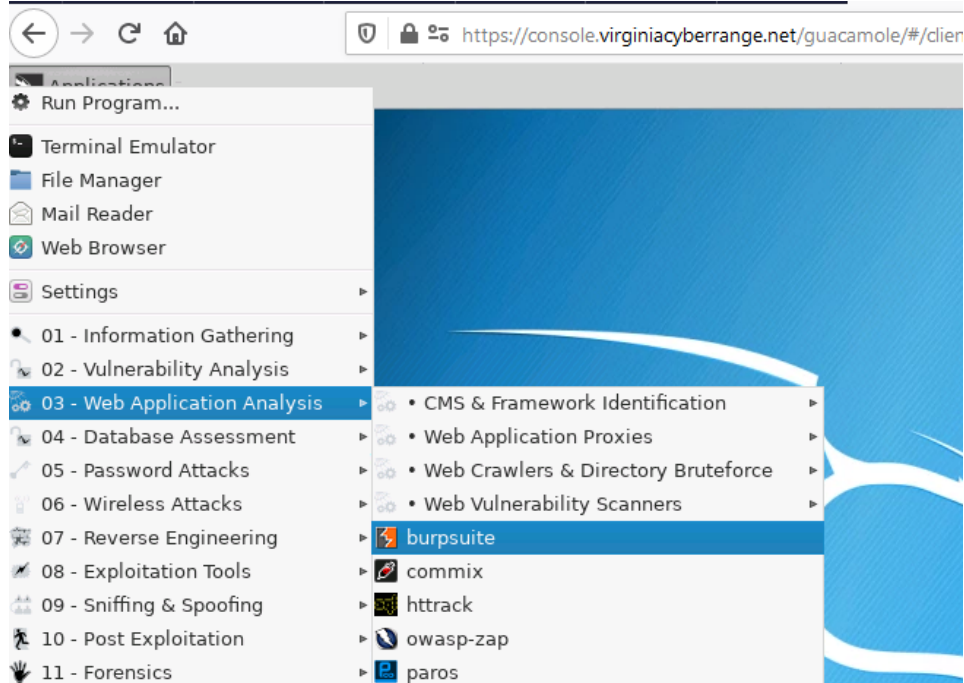


You should get a new window to log in to the VM. User is student, password is student. Hmm, I need to add the username and password to the description.

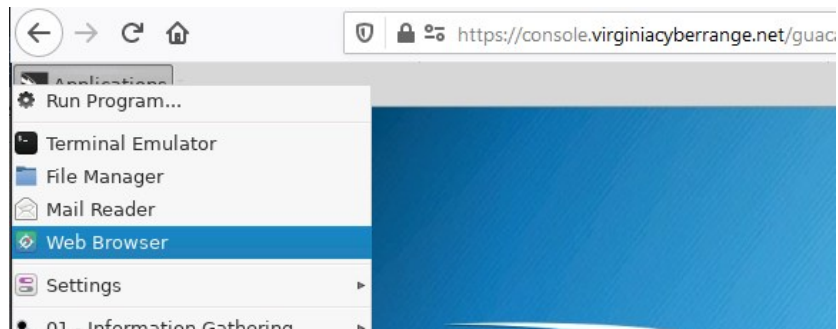


Configure Burp and the Browser

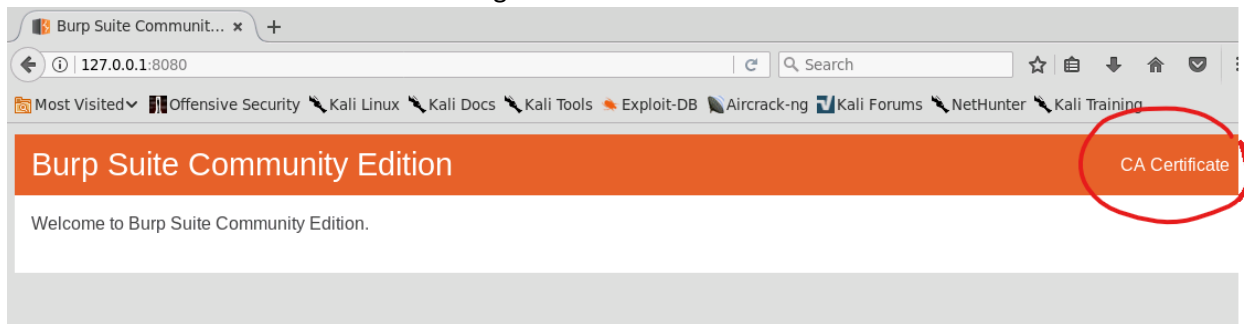
Start Burp Suite. (We need it running so we can grab its certificate.)



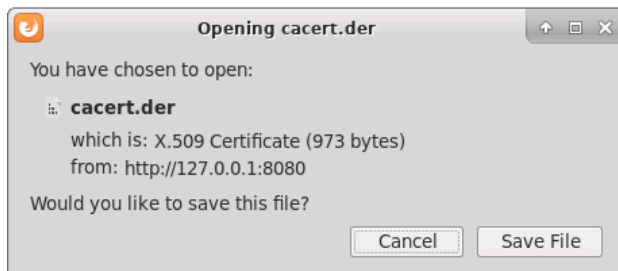
Start the web browser



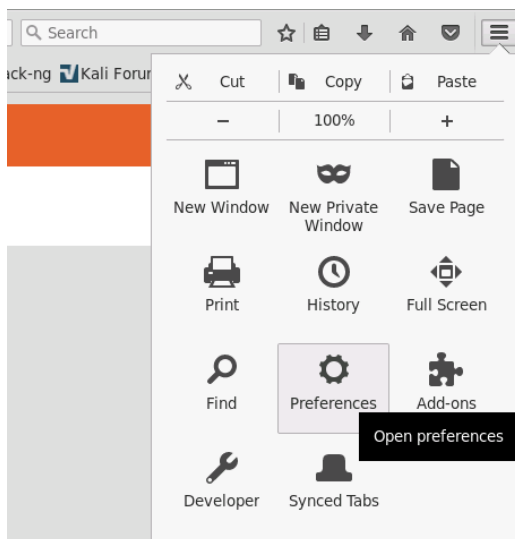
Enter 127.0.0.1:8080 in the browser navigation bar and enter.



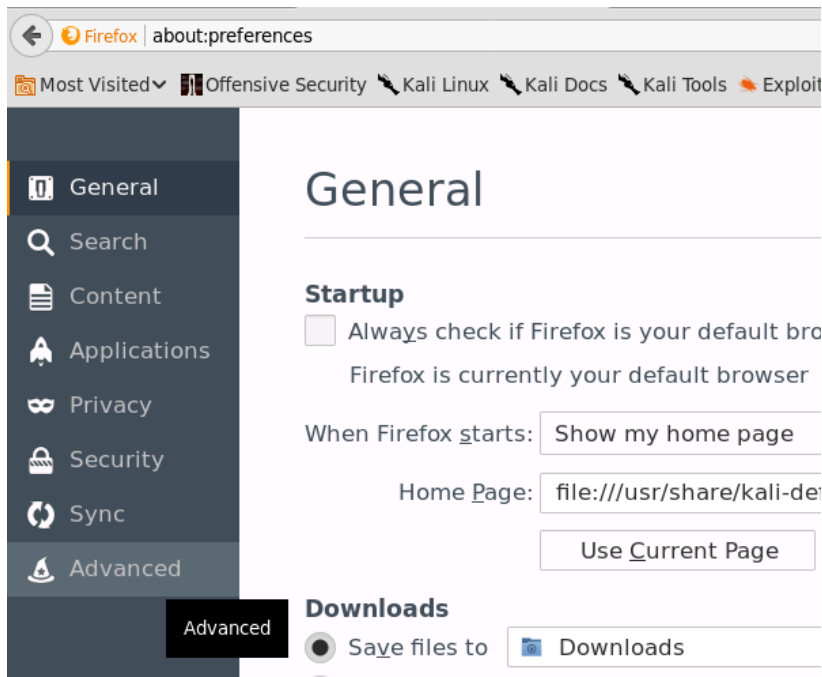
Click on CA Certificate and save the certificate.



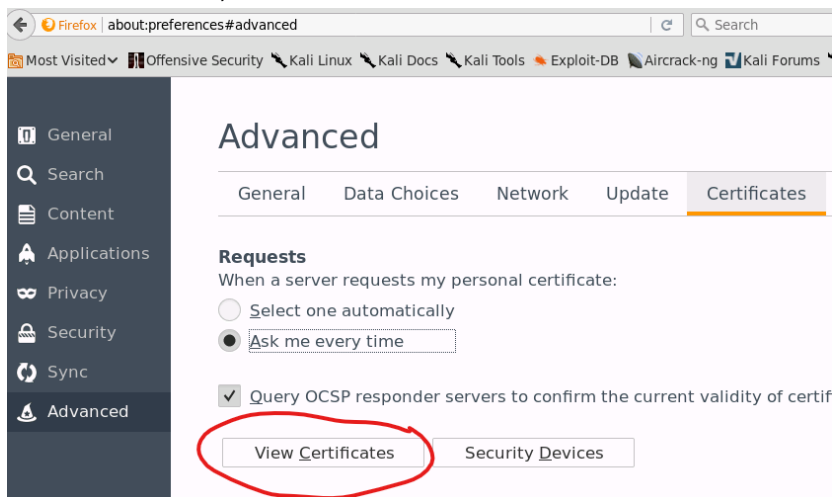
Select Preferences



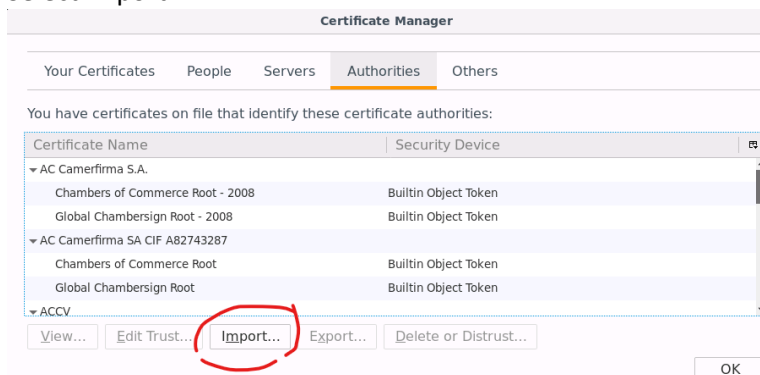
Select Advanced



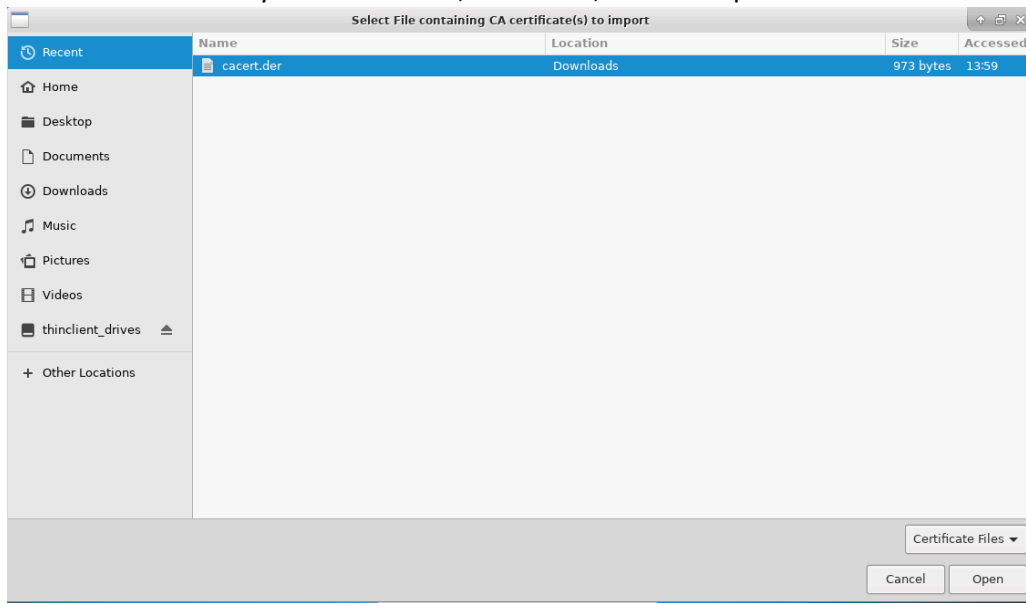
Select Certificates, and click View Certificates



Select Import



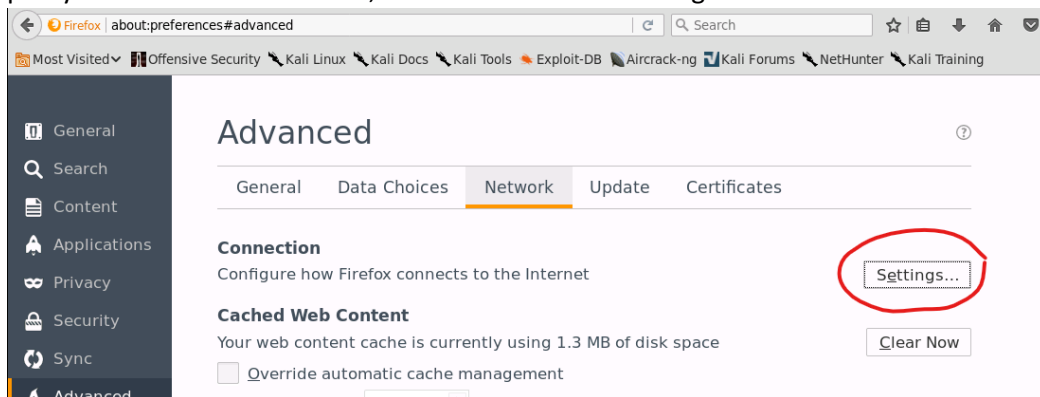
Select the certificate you downloaded, cacert.der, and click open.



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.

Connection Settings

Configure Proxies to Access the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration:

HTTP Proxy: 127.0.0.1 Port: 8080

☒ Use this proxy server for all protocols

SSL Proxy: 127.0.0.1 Port: 8080

FTP Proxy: 127.0.0.1 Port: 8080

SOCKS Host: 127.0.0.1 Port: 8080

☐ SOCKS v4 ☒ SOCKS v5

No Proxy for:

Help Cancel 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.

Burp Suite Community Edition v1.7.33 - Temporary Project

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alert

Connections SSL Display Misc

Upstream Proxy Servers

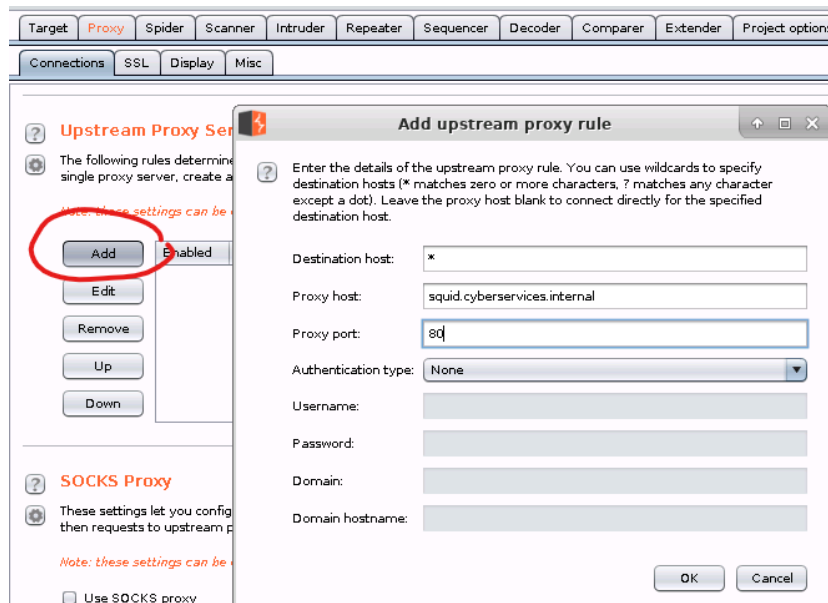
The following rules determine whether Burp sends each outgoing request to a proxy server, or directly to the destination web server. The first rule that matches a single proxy server, create a rule with * as the destination host.

Note: these settings can be overridden for individual projects within project options.

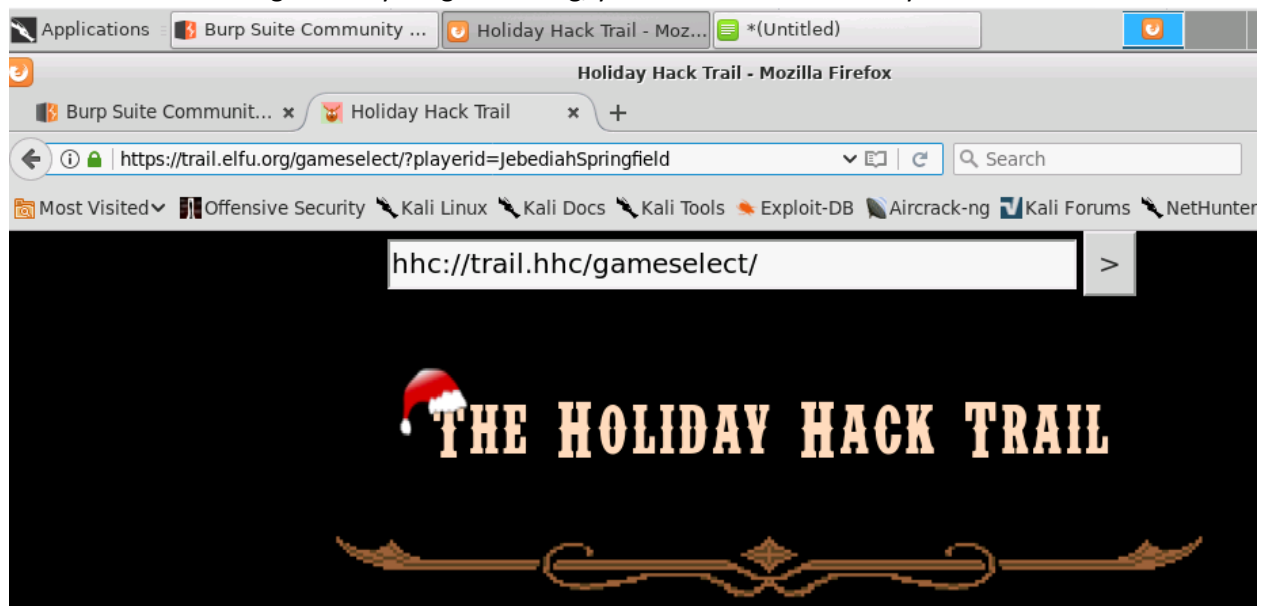
Enabled	Destination host	Proxy host	Proxy p...	Auth type	Userna...
---------	------------------	------------	------------	-----------	-----------

Add Edit Remove Up Down

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.

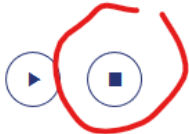


Save the changes you made in VACR

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

Details

Availability  Friday, January 10, 2020 12:00 AM
Creation  Tuesday, June 30, 2020 7:59 PM
Wednesday, January 8, 2020 10:43 AM





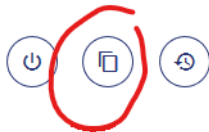
Once you've done that, the icons should change and give you a Copy icon. Click it.

Description

This is the K12 Cyber Security Concepts Using Kali environment, modified so that it not work unless Burp Suite is running. This environment is used for the class Basic created by SANS/Counter Hack Challenges.

Details

Availability  Friday, January 10, 2020 12:00 AM
Creation  Tuesday, June 30, 2020 7:59 PM
Wednesday, January 8, 2020 10:43 AM



Name the copy and click Confirm.

Are You Sure You Want to Copy this Exercise?

This will create a copy of this user's exercise as a new catalog entry. This catalog entry will then be usable in any of your courses.

The exercise will be unavailable during the copy phase, but the catalog creation will take a further 10-20 minutes.

Copy Name

Holiday Hack Trail--A Basic Web Attack

38 / 264

CANCEL

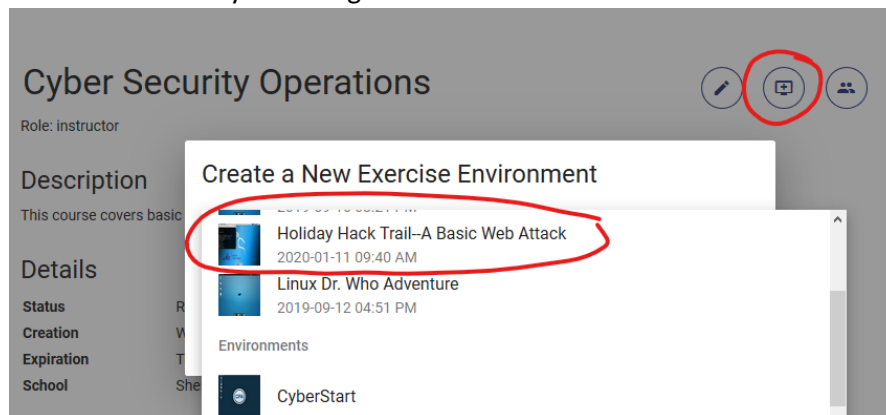
CONFIRM

Your Exercise is being Copied!

A copy of this environment is being created. This may take a few minutes. Once complete, the entry will appear in the create-environments drop down list.

CLOSE

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!