Phishing Workout Teacher Instructions

Background:

Phishing

Phishing is a type of Internet fraud that seeks to acquire a user's credentials by deception. It includes theft of passwords, credit card numbers, bank account details, and other confidential information. Learn how to identify and avoid phishing scams in 2019.

One common phishing attack is through fraudulent emails. As long phishing continues to be marketed as a service, sensitive data will never be truly secure. To learn more about how phishing attacks work, BeEF (Browser Exploitation Framework) can be used to launch example phishing attacks and demonstrate why suspicious links should never be clicked on. Learn how to hack web browsers with BeEF

Introduction:

For this workout, students will experience the dangers of social engineering attacks and learn the basics on how to protect themselves from similar attacks. To simulate the attacks, we will be using an open source tool called BeEF (Browser Exploitation Framework). It is important to note that due to how the workout is currently set up, not all the modules created for BeEF will work such as recording webcams, playing sounds, or stealing students personal information. And while the tool is used professionally, it was designed specifically to work as a demonstrative tool and not as a malicious actor.

The Workout:

BeEF UI Panel: *localhost:3002/ui/panel*

- Username: *workout*
- Credentials: *gonephishing*

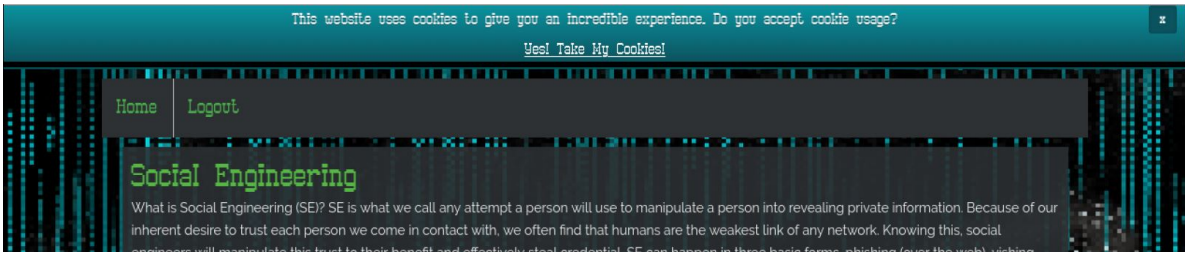
PhishPhactor: *http://10.1.1.20:3001/login*

- Username: *root*
- Credentials: *password*

> All browser activity will be from within the Cyber Gym machines provided

From within the Cybergym machine, go to localhost:3002/ui/panel/ and log in using *workout* and *gonephishing* for the username and password. We'll get back to this page later on in the workout.

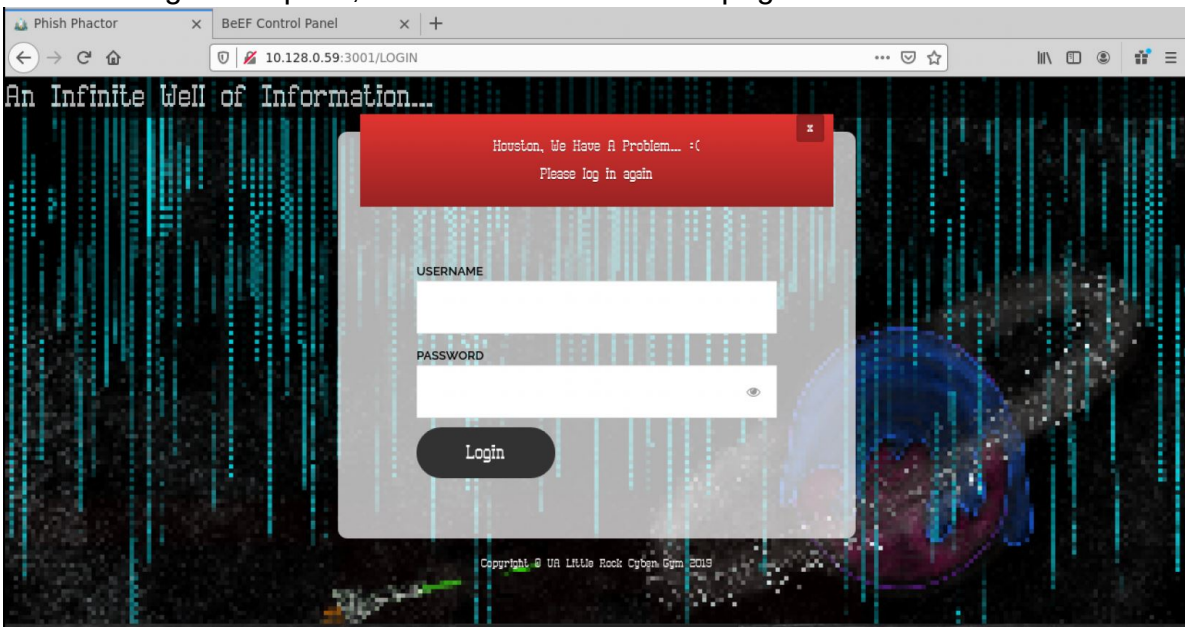
In a new tab, navigate to 10.1.1.20:3001/login and login using the *root* and *passwor* as the username and password.



Once logged in, at the very top of the page will be a request to accept cookies, *ignore that request for now.* Students can read the short article with a simple overview of what social engineering is and how it relates to phishing attacks. If students already know the relation, they can skip down to where the article provides basic web safety techniques.

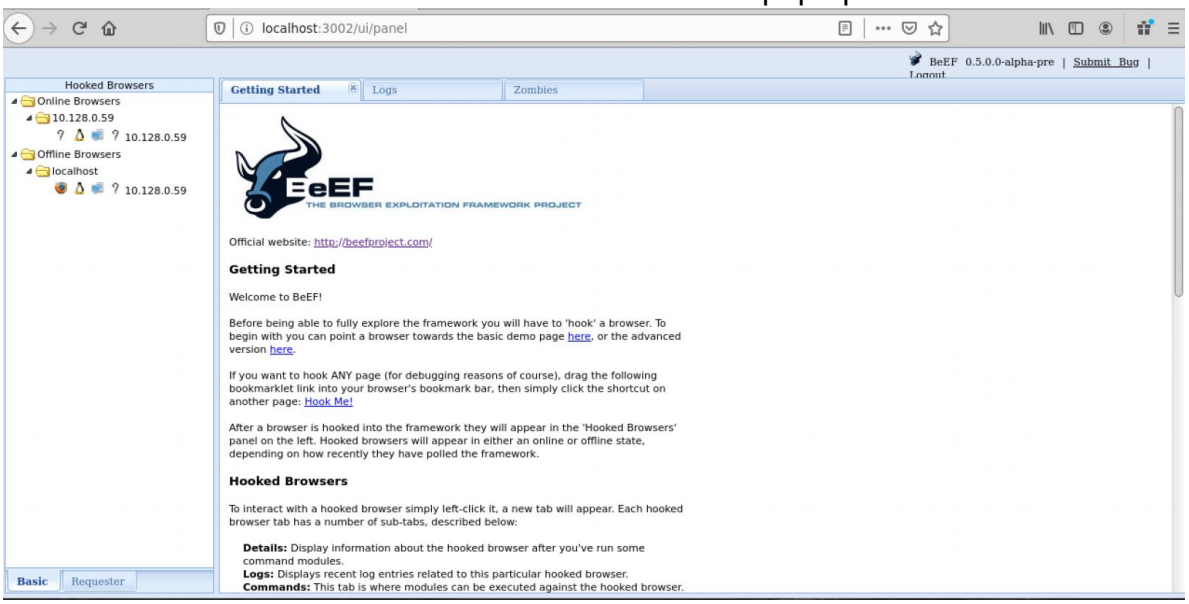
With that knowledge in mind, the students can proceed to the interactive part of the workout. Start by accepting the cookie request. If students don't see the request, just refresh the page and it should reappear.

After clicking the request, students should see this page:

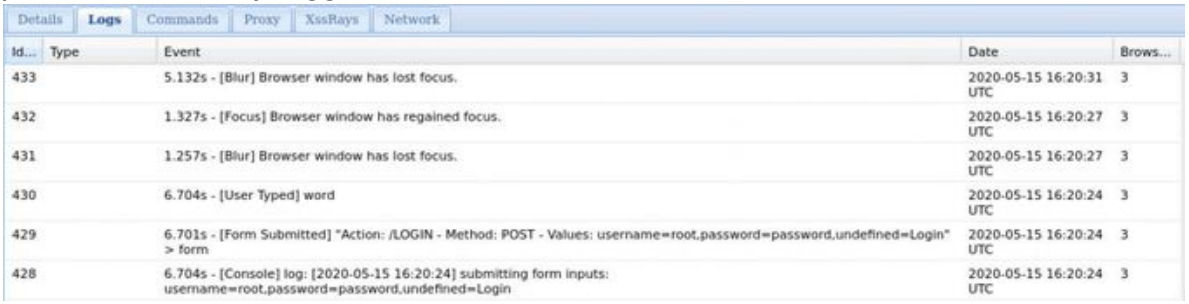


Have students log in again using the same username and password as before.

Now go back to BeEF that we logged into at the beginning of the workout. If they look at the folders on the left, they should see an IP address under the “Online Browsers” folder. This is the IP of the virtual computer that they are using! Click on that IP address and students should see several tabs pop up



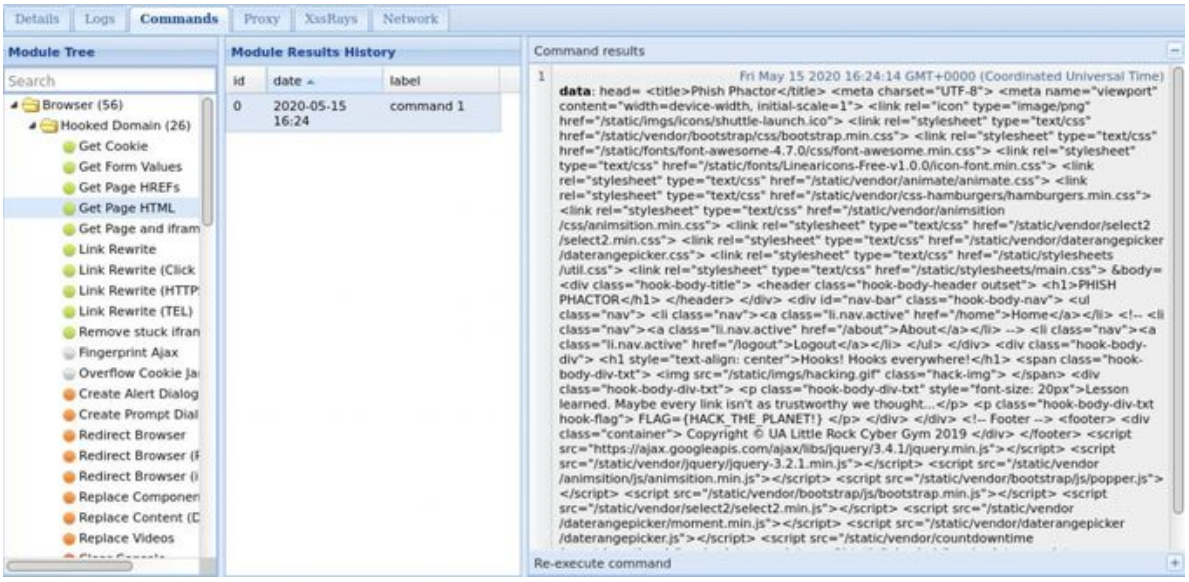
Look at the “Logs” tab. Several rows down, students should see the username and password that they logged in as!



Id...	Type	Event	Date	Brows...
433		5.132s - [Blur] Browser window has lost focus.	2020-05-15 16:20:31 UTC	3
432		1.327s - [Focus] Browser window has regained focus.	2020-05-15 16:20:27 UTC	3
431		1.257s - [Blur] Browser window has lost focus.	2020-05-15 16:20:27 UTC	3
430		6.704s - [User Typed] word	2020-05-15 16:20:24 UTC	3
429		6.701s - [Form Submitted] "Action: /LOGIN - Method: POST - Values: username=root,password=password,undefined=Login" > form	2020-05-15 16:20:24 UTC	3
428		6.704s - [Console] log: [2020-05-15 16:20:24] submitting form inputs: username=root,password=password,undefined=Login	2020-05-15 16:20:24 UTC	3

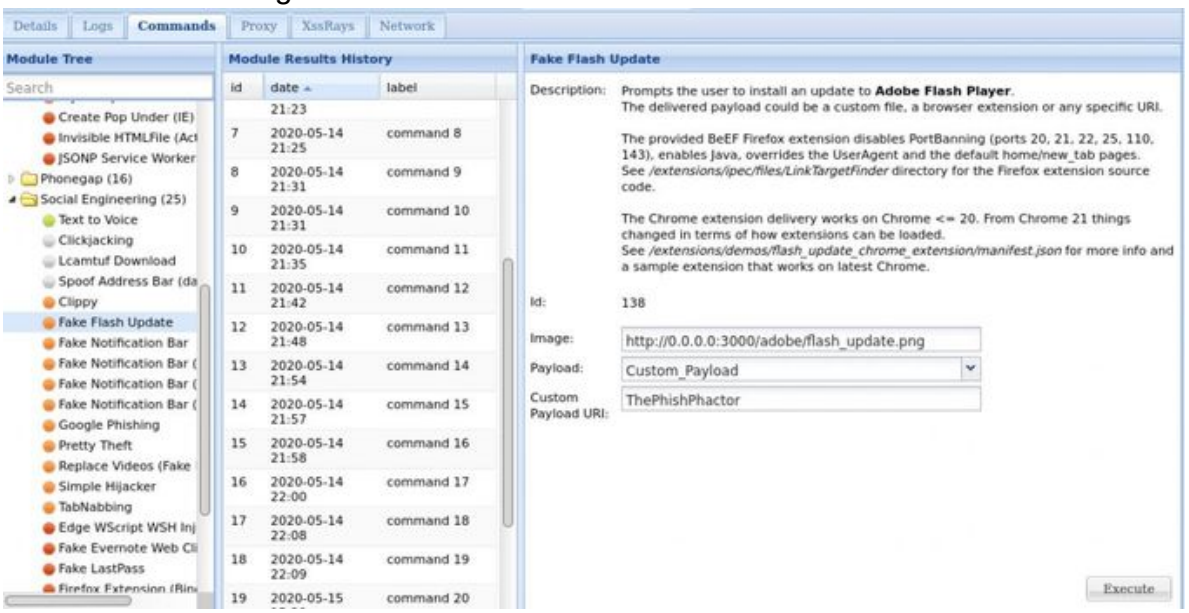
Go to the “Commands” tab. This tab contains all the available modules that come installed with BeEF.

Under the Browser folder, try the “Get Page HTML”. This modules will pull the source for whatever page was infected or in this case, PhishPhactor. Just click the module name and then execute. There should be a new entry in the middle column. Click on that entry to see the results of the command.

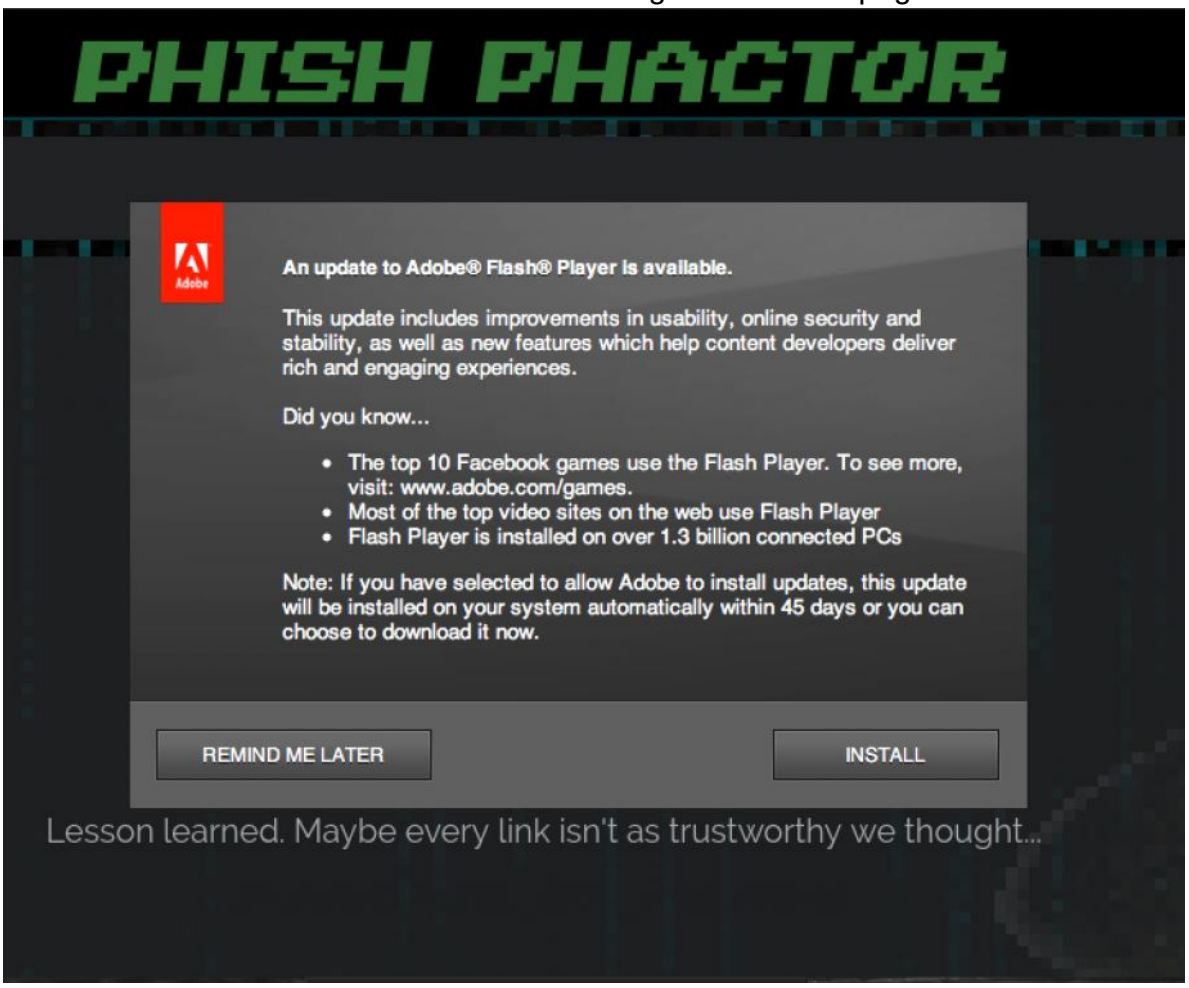


In the same folder, about 13 modules down, students can send JavaScript dialog and alert prompts to the PhishPhactor. After executing either command, students can return to the tab with the PhishPhactor loaded and see the JS box pop up in their browser. If they respond to a dialog message, the response will appear as a new event in the Module Results History column.

Finally, go down the the Social Engineering folder at the very bottom of the Module Tree column. Inside there should be a module called “Fake Flash Update”. Run that command and go back to the PhishPhactor tab.



Something should pop up that wasn't there before! This fake flash update prompt is loaded so that no matter if the students click "Remind Me Later" or "Install", it will execute code in the backend before redirecting them to final page of the workout.



If students see this page, they've completed the workout!

It is important to stress that one should never click links unless they trust the source and most definitely, if a page is asking you to update software installed on

your machine, ignore that prompt! More than likely, they will update a lot more software. Even more so with Flash updates since Adobe is dropping support of Flash by December of 2020.