Phishing Workout Student Instructions

Introduction:

You've learned a little about what Social Engineering is and almost everyone knows what spam is (the electronic kind), but what would happen if you were to click one of those links in the spam emails? Let's find out! In this workout, you will experience the dangers of a special form of social engineering attack known as phishing and some simple measures you can take to defend yourself from these attacks. You will be using a popular *demonstrative* tool called BeEF (Browser Exploitation Framework) to run remote commands to control the browser inside your virtual machine.

A Quick Rundown on BeEF:

BeEF is a very fun tool to play with and pretty easy to learn too. On the left side, you'll see all active 'hooked' browsers. If a browser is hooked, this means that that browser visited a page that was 'infected' by BeEF. To interact with a browser, click on the hooked browser. With a browser selected, you can see these new sections added to the page: *Details*, *Logs*, *Commands*, *Proxy*, XssRays, and *Netwo rk.* We're only interested in the first three.

In the *Commands* section, you will see all the modules that are built in to BeEF on the left column. The right column shows the details of a selected module and the option to execute it. The middle column, *Module Results History*, will show a running list of results for completed commands. If you click on an event, it will show the results of that command.

Logging on to Your Computer:

- Log into the Guacamole web server using the username and password generated on the landing page
- You may have to refresh the page if a screen does not come up.
- Them, you will log in automatically

Your Mission:

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 machine provided

1. Once logged in, open up the web browser and go to the *BeEF UI* panel (localhost:3002/ui/panel/) and log in using *workout* and *gonephishing* as the username and password. We'll need this later.
2. Open up a new tab and go to http://10.1.1.20:3001/login and login using *root* and *password* as the username and password. If you see something pop up on the top of your screen, just ignore it for now.
3. Read the short article to refresh yourself on what social engineering is and how it relates to spam or phishing attacks and the basic measures you can take to protect yourself.
4. **Task 1:** Accept the cookie request! (Who doesn't like a good cookie?)
5. **Task 2:** Go back to the first BeEf tab you logged into, and check the logs in the BeEF panel. Do you see anything important?
6. **Task 3:** Try running a few modules (see below) and see their effects on the PhishPhactor tab.
7. **Task 4:** Can you find a hidden flag on the PhishPhactor?

Modules to try:

Use the Commands tab in the BeEF panel (next to the logs)

Anything between the [ ] is a module found under the commands tab, what follows is a specific command to run

- [Browser]=>Get-HTML
- [Browser]=>Create Alert Dialog Box or Create Prompt Dialog (or both!)
- [Social Engineering]=>Fake_Flash

[hint] You may need to install Flash ...