Cyber Attack Workout Teacher Instructions

Introduction

The *Cyber Attack* workout allows students to experience malware from both the adversary and the victim. This workout introduces students to a type of malware known as a botnet. A botnet is a type of malware run on a client computer that establishes a connection back to a botnet controller. The botnet controller can then do almost anything on the victim computer. To learn more about botnets, read this article: https://usa.kaspersky.com/resource-center/threats/botnet-attacks.

For this workout, the student logs into a victim computer built just for the student and run the botnet. Then an online service known as Shinobot provides the student the experience of controlling their botnet remotely.

Logging into the Victim Computer

- Log into the Guacamole web server using *cybergym* and *Let's workout!* as the username and password.
- The student may have to refresh the page if a screen does not come up.
- Then, the student will log in automatically.

Mission

- Once the student logs in, they should double click shinobot on the desktop.
- A command prompt opens and immediately starts executing. Look for the **host ID** and **password**. The student will want to write these down or take a picture of them with their phone. If the botnet scrolls through, they will need to scroll back up and take a picture.
- Go back to the browser on the school computer and browse to http://shinobotps1.com/. Then click on the C&C tab.
- Find the **host ID** that they wrote down from above and login with the credentials they were provided. The following tasks and answer key is provided for this workout.

Task 1: Verify you have successfully started your botnet victim by recording information requested

Assessment Answer: 10

Task 2: Log into the botnet Command and Control (C&C) Server at http://shinobotps1.com/. To verify you have successfully logged in, you will be asked

to provide the local IP address. Hint: it will be in the form of 10.x.x.x (where x is some number).

Assessment Answer: 10.1.1.11

Task 3: Run a command on the victim using the C&C server. In the assessment, you will run the following command and indicate which movie you see come up on the victim computer.

```
cmd /K start telnet towel.blinkenlights.nl
```

Assessment Answer: Star Wars

Task 4: Now, run a Command and Control script on the Desktop to find the password used for GitHub. Report the password you find in the assessment.

Assessment Answer: H00h00h00!

Task 5 (Challenge): Come up with your own script or action to perform on the botnet victim.

This has no automated grading, and the student is encouraged to explore and find a unique script to execute on the server.