Cyber Attack Workout Teacher Instructions

Background:

A **cyber attack** is a deliberate attempt to disable computers/networks, steal data, or use a breached computer/network as a launch point for other attacks. There are several common types of cyber attacks: malware, phishing, ransomware, denial-of-service, man-in-the-middle attack, SQL injection, and zero-day exploit. On this site, you will learn about these different types of these cyber attacks.

Malware is any kind of malicious software intentionally designed to cause damage to a computer, server, or computer network. The attacks may render the computer or network inoperable, or gain unauthorized control to the system. Learn how to prevent malware.

Phishing is a technique that uses disguised email or any communication software to trick the recipient into believing that the messages are like an official notice from reputable public and public institutions. The goal is to steal sensitive data like credit card numbers or login information from recipients. Learn how to prevent network fishing.

Ransomware is a special kind of malware that makes the recipient lose control of the system or data and then the attackers demand a ransom from the victim to restore access to the data upon payment. Learn how to protect against ransomware: basic tips.

A **denial of service (DoS)** attack is an attempt to overwhelm an online service on a web site and render it unusable. DoS is different from hacker intrusion because it does not break into the system of the website but, instead, paralyzes the website function. Learn how to prevent DoS attacks.

A **man in the middle (MITM)** attack is an attack in which attackers secretly intercept the communications between two parties who are unaware of the man in the middle. When MITM attacks are successfully executed, attackers will have the ability to send fraudulent messages, eavesdrop on conversations, access private data, and do a number of damages to the victims. Learn how to prevent man in the middle attacks.

SQL injection (SQLi) is a security vulnerability that occurs between the application and database layer. An input string is included in a SQL command where character checks are ignored in the command. The malicious commands are then mistakenly executed by the database server as normal SQL commands. A successful SQL injection may result in unauthorized access of private data in the database. Learn How to prevent SQL injection attacks.

Zero-day exploits are attacks on security vulnerabilities in software that are not yet known or patched. Learn how to prevent zero-day exploits.

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. **(The Host ID and Password are located at the top of the window when you open shinobot.)**
- Go back to the browser on the school computer, not the computer you are running shinobot on, 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 (Located at the very top of the window after shinobot starts and lists information about the system.)

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 (If it reports as completed and nothing appeared, try to run the command again.)

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. (Teachers: the correct command will be in command template Credentials *Get the Credentials from Browser*, a result page will be shown on the shinobot computer and on the webpage with the information pulled by shinobot)

Assessment Answer: $hhhh…It's a secret!

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.

Additional Assessment Questions

Question 1: This workout demonstrates the operation of a botnet. You willfully executed the botnet client script, what are two ways an adversary could execute the script on a target victim's computer?

Answer 1: The adversary needs to either (i) have a trusted person perform the function through phishing or some other trick, (ii) have the script located in a place where the victim's computer would automatically execute it, or (iii) exploit a vulnerability which allows arbitrary execution on the computer without human interaction.

Question 2: If the adversary's motive included financial theft, how might they use this botnet to accomplish their objective?

Answer 2: They could monitor account credentials and banking data, and send back the data throught the Botnet on command.

Question 3: How could an adversary obtain remote screen access to the computer using this botnet script?

Answer 3: Sometimes referred to as a "reverse shell", they can establish a connection from the computer using web traffic that appears to go in the reverse direction. Students may not have awareness of the network traffic, which is OK. An acceptable answer simply need to touch on the ability to use the Botnet communication channel to establish a separate screen access communication.

Question 4: How might a defender identify the presence of this botnet through network traffic? Then, how could the adversary modify its tactics to evade the defender's detection?

Answer 4: Identify the command and control server IP address. An adversary could avert detection by continuously changing the C&C server with which it's communicating.