Trojan Arena Level 4 Teacher Instructions

Introduction

Welcome to the Trojan Arena where you go head to head with other students in a cybersecurity competition.

Logging into your Computer

On your landing page, you will be provided with a username and password. The username will be cybergym followed by some number, and your password will be a random string of characters. When you are ready, click to enter the arena and log in.

> If your instructor recently started the arena, then it may take up to five minutes for the login screen to show up.

Capture the Flag

Your team will compete for points in the arena. You win points by finding the flags indicated below. For this arena, you do not have to find flags sequentially. In other words, you can work on these as a team in parallel.

Points

Your team will receive points for each of the flags you find. The first team to find a given flag will also receive half of the bonus points. For example, if you find a flag worth 100 points first, then your team receives a total of 150 points. Your team may only submit a flag once.

Submitting Your Flags

The flags will typically look like this, Cybergym{ d89g0vka4c }. You do not need to copy over the braces and dollar signs. Only copy over the text between them. Once you find a flag, go back to your landing page and type the flag in the assessment section. You can submit any number of times. Once you submit a correct answer, your response will be recorded and timestamped.

To the Arena!

Let’s go! Here are your puzzles to solve. Work as a team, encourage each other, and have fun! Good luck!

Task	Points	Description
1 - Cross Site Scripting	100	Students won’t need their Cyber Gym machine to complete this challenge
2 - Firewall Management	100	
3 - Hidden Weakness	100	
4 - Buffer Overflow	100	
5 - Ghidra	100	
6 - Crypto: Split Keys	150	This challenge is based off the vulnerability found on ProFTPd 1.3.5. It has a few extra steps so students shouldn’t get frustrated if they don’t get it right away. A recently terminated employee was ‘feline’ catty and has locked everyone out of his old workstation. Not only that, but he changed his password as well so we can’t get back in! See if there is a way to get in using your knowledge on SSH keys. (This website could be helpful) **What we do know about the machine:**

- **Target username**: *incatnito*
- **Target IP**: 10.1.1.104
- There is a vulnerable FTP server that allows any user to connect and copy / move files on the machine
  - Use *nc <target_ip> 21* to connect to the server.
- SMB was poorly configured to allow any user to share files in certain locations
  - *What is SMB? (Google me!)*
  - Use File Explorer and enter the IP address in the address bar. Example:
    - \\10.9.8.7\

Method of Attack:

- First we need to generate an SSH keys through *cmd* for our account*:*
    - From the Start menu, search for *cmd.exe* and run it. Then run the following command:

      ```
      ssh-keygen -t rsa
      ```

      You can save it in the default location (`C:\Users\<your username>\.ssh\`)
- Now we connect to the SMB share folder and copy our newly created public key to the

  ```
  /share/incatnito/
  ```

  folder.
- Now we'll need to connect to the FTP server with

  ```
  nc 10.1.1.104
  ```

  Yes, there is a built in FTP command you can use from *cmd*, but the whole premise of the exploit is to run commands without an authenticated user--even if that authenticated user is '*anonymous*'.
- Once connected, we'll need to move the public SSH key from the

  ```
  /share/incatnito/
  ```

  folder to the authorized_keys file for the target user, *incatnito*. These are the FTP commands you'll need to do this.
- Once the file is successfully copied over, students should be able to SSH into the machine as the user, *incatnito.*

7 - Bonus Round	50	On the SMB server connected to for the Split-Key challenge, what was the default password that IT uses to setup new users? **Answer:** In *File Explorer*, navigate to the SMB server. Students should see two folders, *IT* and *incatnito.* Inside the *IT* folder, there is one file. The password can be found as part of a Perl command that is run by the shell script.

1 - XSS:

2 - Firewall:

3 - Hidden Weakness: Use *Nessus* to scan the network for any suspicious or illegitimate user accounts. The ability to look for illegitimate user accounts is critical for detecting network vulnerabilities. Nessus allows you to choose the type of scan you want to execute for a target network IP address. When the vulnerability scan is complete, it will list the scanned hosts by IPs scanned and the associated risks. When an individual vulnerability is selected, it displays more details on that particular vulnerability. Unfortunately, like other vulnerability scanners, some vulnerabilities may be false positives, so each vulnerability must be examined.

4 - Buffer Overflow:

5 - Ghidra:

6 - Crypto: Split Keys: This challenge throws around a lot of protocols. SSH, SMB, FTP. What are they?

- *SSH* is primarily used to connect to remote systems. It uses asymmetric keys to provide a secure connection between the client and host. Once a connection is made, users can run system commands on the remote machine. You can connect to a remote machine by running the following command from your Windows Command Prompt or terminal:

```
ssh <your_username>@<target_ip>
```

- *SMB* is a file sharing protocol used when sharing files between different operating systems (Windows, Linux, Mac OS). On Windows, you can connect to connect machines by opening *File Explorer* and entering \\ followed by your target IP address in the address bar. Example: \\192.168.10.110

- FTP is another file sharing protocol on port 21 that allows users to copy or move files from the local machine to the remote machine. For this challenge, you can connect to an ftp server running the following command in your Windows Command Prompt:

```
nc <target_ip> 21
```

This command utilizes a tool called *netcat* to make the connection. Normally, you'll be prompted for a username and password, but since this server wasn't "set up securely", *you don't need any credentials to send commands to the ftp server*.