Assignment 5: Capture the Flags

Due: Thursday, April 7th in class

This assignment is worth 20 points. You must work on this assignment individually!

UPDATED 3/30/2011: If you complete this assignment using an "unscientific", "legal cheating" method (read: assuming physical access to the box, the VM), I will accept it at a 25% penalty!

UPDATED 3/31/2011: If you fail to follow directions for a flag, it will not count!

Overview

In this traditional game, you will exploit vulnerabilities on a *web server* and on a *website* to gain access to files you should not have access to. In particular, your goal is to find a few "flags" placed on the server. You will also need to explain how to patch the vulnerabilities.

About the web server: it is a Ubuntu 10.10 server, 32-bit, with all system updates installed as on March 27, 2011. MySQL, PHP, Tomcat, and a slew of other software are loaded on successful start of the server. There is no GUI or desktop manager installed on the server. *There are five (5) flags planted on the box.* A flag can be either a text file named **`FLAG.txt`** on the filesystem or embedded inside of a file on the filesystem (starting with **`FLAG:`** --yes, the colon matters).

Instructions

Download and run the new Ubuntu VM: **`CTF.zip (837 MB; MD5 checksum=e37b7c1f411e731e17cf9f27e38171cd)`**. To access the web server (VM) from your web browser (host), you have to determine the server's IP address first (for me it is **`192.168.156.133`**). Once you can communicate with the web server, happy hacking!

For each of the 5 flags, please answer or provide:

- Provide a screenshot of the flag (and follow additional directions, if instructed...)
- Where is the exact location of the flag (path or file name)?

- What exploit or methodology did you use to find the flag?
- If the exploit pertains to configuration or insecure programming, provide a patch for the vulnerability. That is, rewrite the snippet of code or describe how the configuration change.

(BONUS +3) Change the password for the **`ubuntu`** user and explain your methodology. Enough said.

Submitting the Assignment

Please provide a report of your findings at the beginning of class on Thursday, April 7th. Lateness is one (1) point per each day late. *Your submission will be considered late if it is not submitted by the beginning of class!*

Hints

- The password pair **`ubuntu:!templinpw!`** will not work. :-)
- I do not need to tell you the number of users on the server.
- It is important that you tinker / break / bang on the website / web application.
- Use your creativity. That is, if you were a bad guy, what would do?
- Be sure to view the source of all the web pages.
- You should research how PHP works: installation and vulnerabilties.
- The result of the exploit should result in a reverse shell.