EECS 444 Project Proposal

Nathan McKinley, Benjamin Kaplan, Evan Gallo, Jason Kuster

March 9, 2012

For our Security project, we propose to implement a single-player, multi-machine, networked, offensive Capture the Flag game. Capture the Flag is a game where the players attempt to gain unauthorized access to a specific machine, up to and including root access. This is done through exploitation of various services pre-installed on the machine such as SSH, Telnet, and Apache. Capture the Flag games are regularly run at computer security conferences. The United States government is currently sponsoring a computer security initiative that includes Capture the Flag[1] competitions.

The player works their way through a number of challenges on several machines networked together. These challenges consist of exploiting a particular vulnerability and obtaining access to the user account corresponding to the next challenge. Each user account is locked out of services not required for their challenge. It's possible for multiple, non-sequential challenges to take place on the same machine. The challenges are ordered by difficulty of exploit. The player is not informed of the exploit required for each challenge ahead of time.

Types of challenges that we may use include:

- Buffer overflow in C programs for which the source is provided
- SQL injection in a website
- Print format string injection
- Unix Path hijacking
- identifying unsecured remote access
- forge email requesting password
- bypassing IP verification
- required man-in-the-middle, with and without cryptography
- decrypting poorly encrypted file
- frequency analysis of ciphertext

[1] http://www.whitehouse.gov/files/documents/cyber/The United States Cyber Challenge 1.1 (updated 5-8-09).pdf