Capture the Flag - Computer Science Style

Kathy Robertson
Advisors: Dr. Dan Massey and Dr. Indrajit Ray

Future Work:
- An Annual Front Range Capture the Flag – Computer Science Style
- Tutorials on Security Concerns

Set Up:
- Set up exploitable machines
- Allow students to crack, hack, and intercept traffic
- Students work in teams to earn flags

Equipment:
- Username
- Password
- IP Addresses of Each Box
- Hacking Laptop
- Auditor (Live OS)
- Teammates

Motivation:
- Teach students about security
- Learn what students know about security
- Interaction between Front Range Schools

Box 1
- Play as Account
  - No User Account
  - No Root Account
  - No Webserver
  - No Observe Traffic
  - No Contains Flag
- Box 2
  - User Account
    - 5 SQL Injection
    - Webserver: SQL Vulnerability
  - Admin Account
    - 7 Get Root
  - Root Account
    - 2 Get Root Access
    - Contains Flag: yes

Capture the Flag Set Up

Box 1
- Get Root Access
  - 3 Capture
  - User: Hacker
  - Normal User
    - Username: Password
    - Hacker: User

Buffer Overflow
- High Addresses: Name = "bob"
- Low Addresses: Name = "flag"
- Code: NOP NOP NOP NOP NOP NOP NOP NOP NOP
- Buff Overflow Exploit

How a Buffer Overflow Works:
- Program Allocates Buffer Space
- Program inserts too large of data
- Overwrites Other Register
- Hacker can execute Code Remotely

Lessons Learned:
- Use Strong Passwords (flag 1)
- Encrypt Traffic with SSL (Secure Socket Layer) (flag 2)
- Patch Software (flag 3)
- Good Software Design (flag 4)

Attack Plan
Login to Box 1:
- ssh or ftp into Box 1 with provided username and password
- 5 out of 5 teams completed this mission in less than 5 minutes
- Crack root Password: (1 flag)
  - use a password cracker to decrypt an encrypted password file
- 5 out of 5 teams cracked the password in < 15 minutes
- Capture Username and Password Traffic:
  - capture packets with username and password
- 5 out of 5 teams completed this mission in less than 10 minutes

Login to Box 2: (1 flag)
- ssh or ftp into Box 2 with captured username and password
- 5 out of 5 teams completed this mission in less than 5 minutes
- Get Admin Password:
  - implement an sql injection to obtain username and password
- 4 out of 5 teams completed this mission in less than 30 minutes

Login to Admin Account: (1 flag)
- login to Admin Account with obtained username and password
- 4 out of 5 teams completed this mission in less than 5 minutes
- Get Root Access:
  - Successfully exploit vulnerable code with a Buffer Overflow
  - 4 out of 5 teams completed this mission