Goal

- Be able to improve a system to avoid the threats we have discussed this semester
- Understand the requirements of penetration testing

Penetration Testing

- Penetration testers attack a system to evaluate its vulnerability
- Testing is carried out from the view of a potential attacker
- Some security standards require both annual and ongoing penetration testing

Black box vs. White box

- Black box penetration testing occurs when the tester does not have any knowledge of the internals of the system
  - Most closely resembles actual attacks
- White box testing is when the tester has full knowledge of the system possibly including source code and network configuration
  - Resembles an attack by an insider
  - May find more vulnerabilities

Penetration Testing Risks

- It is possible that the penetration testing will damage the system making it unavailable for others
- Some testing may consume resources creating a denial of service problem for others

Penetration Testing Manual

- Open Source Security Testing Methodology Manual (OSSTMM) is provided by the non-profit Institute for Security and Open Methodologies.

From the OSSTMM

"In art, the end result is a thing of beauty, whereas in science, the means of reaching the end result is a thing of beauty. When a security test is an art then the result is unverifiable and that undermines the value of a test. One way to assure a security test has value is to know the test has been properly conducted. For that you use a formal methodology. This is it."

Penetration Tester Certification

- Council of Registered Ethical Security Testers (CREST)
- Information Assurance Certification Review Board
- NSA Infrastructure Evaluation Methodology (IEM)
- Open Web Application Security Project (OWASP)

Password Protection

- Educate users
- Require passwords that are:
  - long
  - use at least three of the four character groups
  - not in the dictionary
- Use biometrics or other non-password methods of identification

Buffer Overflow Defenses

- Better software engineering
- Avoid dangerous functions
- Language choice
- Compiler tools (Stack Guard)
- Analysis tools
- Execution Prevention

Program Errors

- Buffer overflows are primarily caused by programs which fail to properly check for invalid input, particularly longer input than expected.

```
while (!inFile.eof()) {
  inFile.get(str[i]);
  i++;
}
```

```
while (!inFile.eof()
      && i<MAX) {
  inFile.get(str[i]);
  i++;
}
```

Use Safe I/O Functions

- Use **`cin.get`** and **`cin.getline`** functions instead of cin >>
  - They allow you to specify a maximum input length
- Avoid **gets()**. It has no way to limit input length
- Use precision specifiers with the **scanf()** family of functions. Otherwise they will not do any bounds checking for you.

Use Safe String Functions

- Use **strncpy()** instead of **strcpy()** and **strncat()** instead of **strcat()**.
- Functions like **fgets()**, **strncpy()**, and **memcpy()** are safe if you make sure your buffer is the size you say it is. Be careful of off-by-one errors.
- When using **streadd()** or **strecpy()**, make sure the destination buffer is four times the size of the source buffer.

SQL Injection Defenses

- Check input fields for proper format
  - Use positive instead of negative checking
- Use parameterized queries
- Minimize error messages in a production system
- Avoid obvious field names in databases
- Save the hash of a password in the database instead of the actual password

Cross Site Scripting Defenses

- Disallow JavaScript in any input
  - » Use positive instead of negative checking
- If you must allow HTML in the user input, allow only safe HTML tags
- Filter output to remove any JavaScript
  - Replace HTML special characters in output
  - » ex: replace < with < and > with > and also replace (,), #, &

Cookie Defenses

- Tag cookies to include IP address in cookie and only allow access to original IP address that cookie was created for.
- Prevent cookies from being accessed locally
- Encrypt the cookie contents

Firewalls

- Prevent network traffic unless you specifically allow it
- Prohibit exiting traffic that has an impossible source address