Computer Security and Ethical Hacking

WPI offers courses and independent studies that educate students about computer security and protection. As part of this education, students may learn about how to defend computer systems and networks and techniques that may allow the circumvention of computer security defenses.

As part of our "theory and practice" motto, computer security education may involve the use of security penetration tools and techniques in an artificial "sandboxed" environment using virtual machines. In these sandboxed environments, students are allowed to attack targets authorized by their instructors; this access, and only this access, is considered authorized under this agreement. If the student has any doubt about what computer systems and networks are in the sandboxed environment, they should contact their instructor prior to any experimentation.

Attacks on any other infrastructure are beyond the scope of the educational exercise and are not authorized by any WPI officials. Students are NOT authorized to attack any computers, networks, or infrastructure in the Computer Science Department, WPI, or outside organizations.

Unauthorized access to computer systems is a crime in many jurisdictions and often accompanies severe consequences, regardless of the perpetrator's motivations. It is the student's responsibility to be cognizant of and compliant with computer use laws.

Prior to any practical applications of computer attack software, the student must acknowledge the terms of this agreement.

Student Name

Date

Signature

Instructor's Name

Date

Signature