Module 5
(Ethics for Penetration Testers)

- At the end of this module, you should understand why some have a dim view of penetration testing and why it is essential for penetration testers to operate in a methodical and ethical manner.
Those Guys Are Just Hackers*

- There are common perceptions about penetration testers that cause problems for the industry:
  - Penetration testers are really pretty much criminal hackers.
  - What penetration testers do verges on illegality and inherently conflicts with law.
  - Penetration testers are undisciplined and their work is not methodical
- SySS suggests 10 concepts to avoid these perceptions.

1. Independence

- Don't participate in a penetration test of any company for which you have helped plan the or implement security measures.
- Don't test companies to whom you expect to sell software.
2. Prohibition on Commission Fees

- Don't accept payment in the form of a monetary commission (that is, a percentage of the price of some good or product sold to someone).
3. Care

- Notify the customer of any risks or negative outcomes that can arise as a result of the test.
4) Professionalism and Quality Assurance

• All work must be done in a professional way and in such a way that its quality may be assured.

• Penetration testers must work to the best of their technical knowledge.
5. Contractual Adherence

- Anything agreed to both by contract and orally in counseling interviews must be adhered to by the members of the penetration testing team and are binding.
6) Impartiality, Neutrality and Transparency

- Any results or conclusions must be presented in an impartial and comprehensible way.
7. Conflicts of Interest

- Conflicts of interest between penetration testers and customers must be avoided.
- If any conflicts of interest arise during the execution of a penetration test, they must be reported and resolved in a mutually amicable way.
8. Strict Obedience of Laws

- Law of the country in which the penetration test is performed must be strictly followed even if following the law can lead to an incomplete test.
- Penetration testers must acquaint themselves with legal constraints and requirements and carry out their work within legal boundaries.
9. Respect of Human Beings

- Social Engineering attacks are designed to exploit the behavior of human beings.
- They will only be performed with prior notice to and agreement of the customer.
10. Correct Attribution

- If external sources are used to achieve the results of the penetration test, sources and authors must be indicated in an appropriate way.