Certified Ethical Hacker
Module 1 - Ethical Hacking

Hacker Classes

- **Black Hats**
  - Excellent Computing Knowledge
  - Use hacking for offensive purposes
  - Security Analysts
  - Use hacking for defensive purposes

- **White Hats**
  - Individuals who both offensively and defensively at different times

- **Gray Hats**
  - Also known as Crackers
  - The Red Guys

Terms

- **Hacker**
  - A person who stretches the capabilities of computer systems

- **Hacking**
  - Rapid or reverse engineering of existing software to make it better

- **Cracker**
  - A person who uses his hacking skills for offensive purposes

- **Ethical Hacker**
  - A person who uses his hacking skills for defensive purposes

- **Threat**
  - A potential violation of security

- **Vulnerability**
  - Existence of a weakness within a system that can lead to an exploit

- **Target of Evaluation**
  - A system that is identified as requiring security evaluation

- **Attack**
  - An action that violates security

- **Exploit**
  - The exploitation of a vulnerability to cause an attack

- **Steganography**
  - Hiding information in another data file

- **Tunneling**
  - The act of sending data through a secure channel

- **Firewall**
  - A barrier that regulates network traffic

- **Sniffing**
  - The act of capturing data packets in transit

- **War Dialer**
  - A tool that dials phone numbers to find active hosts

- **ICMP**
  - Internet Control Message Protocol

- **Traceroute**
  - A tool that helps determine the path packets travel

- **DNS**
  - Domain Name System

- **RIPE/ARIN**
  - Regional Internet Registries

- **nmap**
  - A tool that can scan for open ports

- **ISS**
  - Internet Security Systems

- **eEye**
  - A company that provides vulnerability scanning tools

- **GFI**
  - A company that provides security solutions

- **Sam Spade**
  - A tool for gathering information

- **Pre Attack Phase**
  - Scans network with information gathered during Phase 1 - Recon

- **Subnets**
  - A logical grouping of devices within a network

- **Passive**
  - A phase that involves gathering information without acting

- **Active**
  - A phase that involves testing and exploiting vulnerabilities

- **Phases**
  - Phase 1 - Reconnaissance
  - Phase 2 - Scanning
  - Phase 3 - Gaining Access
  - Phase 4 - Maintaining Access
  - Phase 5 - Covering Tracks

- **Elements of Security**
  - Testing with no Prior Knowledge of the network infrastructure
  - Testing with knowledge of the network infrastructure

- **Black Box**
  - Security Testing

- **White Box**
  - Security Testing

Motivation and Study Techniques to help you learn, remember, and pass your technical exams!