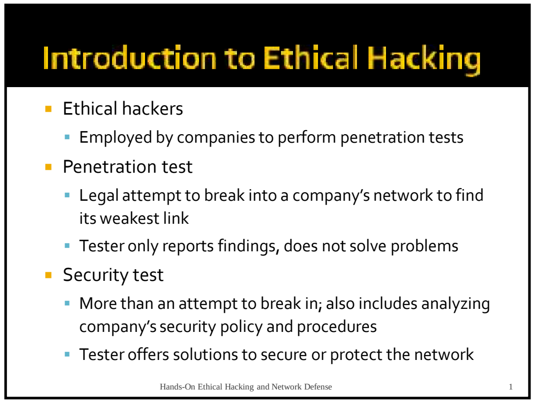
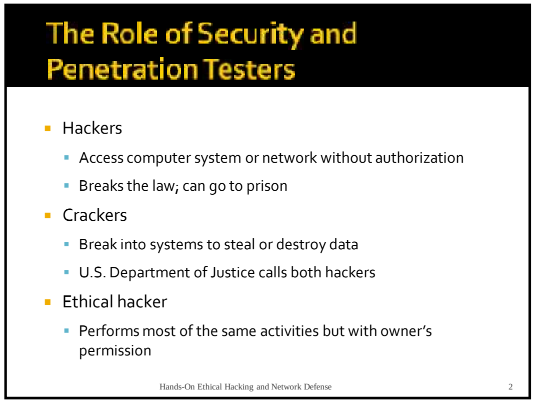


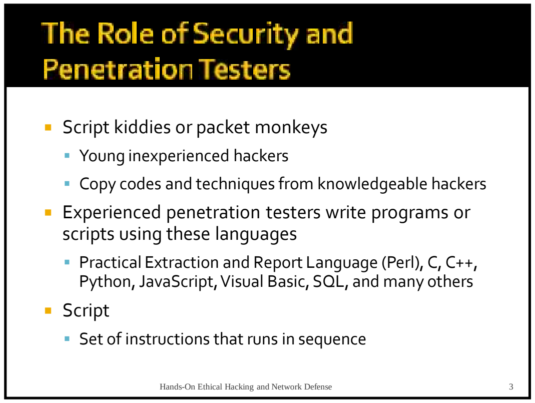
Introduction to Ethical Hacking

- Ethical hackers
  - Employed by companies to perform penetration tests
- Penetration test
  - Legal attempt to break into a company's network to find its weakest link
  - Tester only reports findings, does not solve problems
- Security test
  - More than an attempt to break in; also includes analyzing company's security policy and procedures
  - Tester offers solutions to secure or protect the network



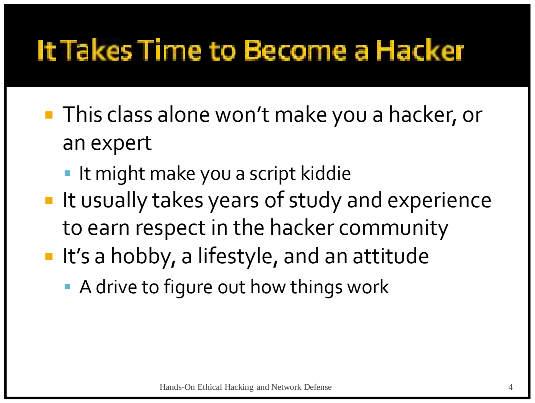
The Role of Security and Penetration Testers

- Hackers
  - Access computer system or network without authorization
  - Breaks the law; can go to prison
- Crackers
  - Break into systems to steal or destroy data
  - U.S. Department of Justice calls both hackers
- Ethical hacker
  - Performs most of the same activities but with owner's permission



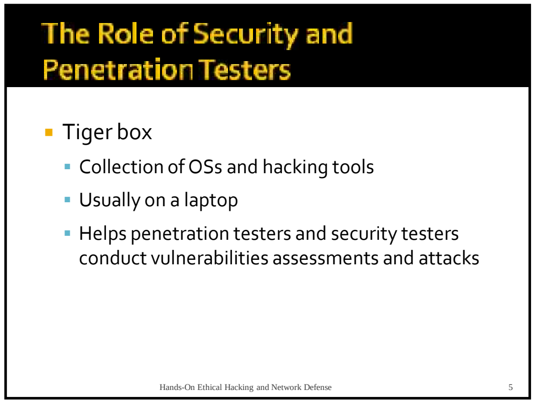
The Role of Security and Penetration Testers

- Script kiddies or packet monkeys
  - Young inexperienced hackers
  - Copy codes and techniques from knowledgeable hackers
- Experienced penetration testers write programs or scripts using these languages
  - Practical Extraction and Report Language (Perl), C, C++, Python, JavaScript, Visual Basic, SQL, and many others
- Script
  - Set of instructions that runs in sequence



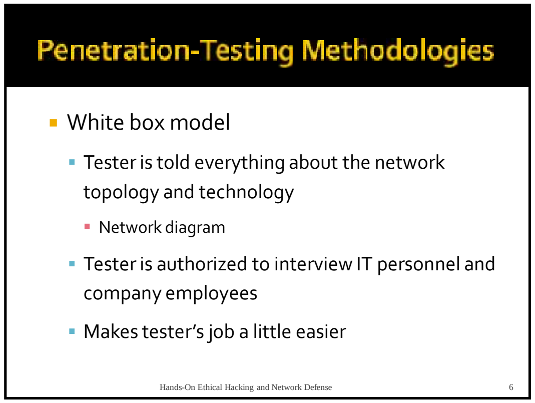
It Takes Time to Become a Hacker

- This class alone won't make you a hacker, or an expert
  - It might make you a script kiddie
- It usually takes years of study and experience to earn respect in the hacker community
- It's a hobby, a lifestyle, and an attitude
  - A drive to figure out how things work



The Role of Security and Penetration Testers

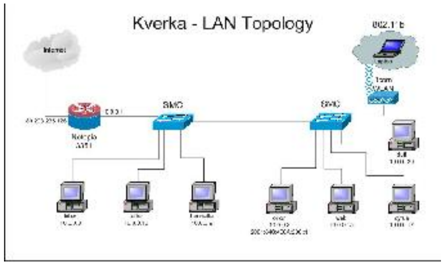
- Tiger box
  - Collection of OSs and hacking tools
  - Usually on a laptop
  - Helps penetration testers and security testers conduct vulnerabilities assessments and attacks



Penetration-Testing Methodologies

- White box model
  - Tester is told everything about the network topology and technology
    - Network diagram
  - Tester is authorized to interview IT personnel and company employees
  - Makes tester's job a little easier

Network Diagram



- From ratemynetworkdiagram.com (Link Ch 1g)

This is a Floor Plan

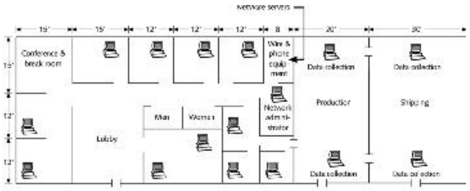


Figure 1-1 A sample network diagram

Penetration-Testing Methodologies

- Black box model
  - Company staff does not know about the test
  - Tester is not given details about the network
    - Burden is on the tester to find these details
  - Tests if security personnel are able to detect an attack

Certification Programs for Network Security Personnel

- Certification programs available in almost every area of network security
- Basics:
  - CompTIA Security+ (CNIT 120)
  - Network+ (CNIT 106 or 201)

CompTIA

CompTIA Security+™ Certification

Take Certification Tests Here

- CNIT is a Prometric Vue testing center
  - Certification tests are given in S214
  - CompTIA and Microsoft
  - The next tests will be in the second week of April, right after Spring Break
  - Email sbowne@ccsf.edu if you want to take a test

Certified Ethical Hacker (CEH)

Defend your Network Against Hackers.
Master the Hacking Technologies.
Become a Certified Ethical Hacker.
Ethical Hacking and Countermeasures
http://www.eccouncil.org
EC-Council

- But see **Run Away From The CEH Certification**
  - Link Ch 1e on my Web page