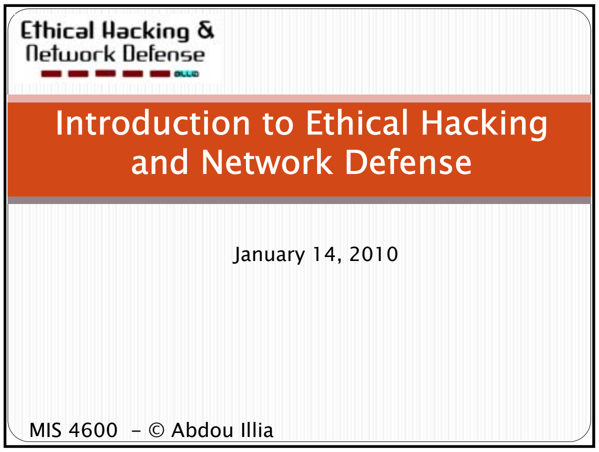
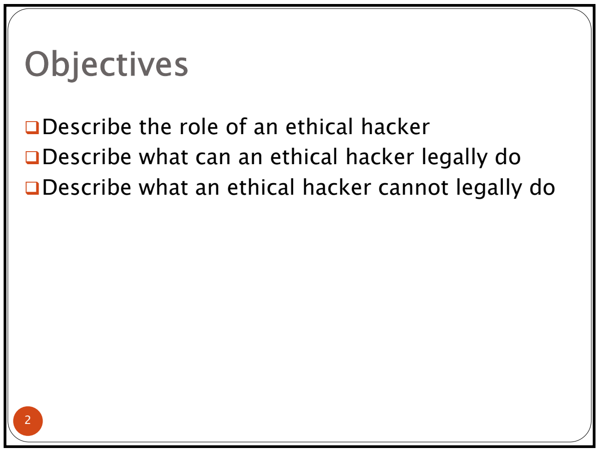


Ethical Hacking & Network Defense

Introduction to Ethical Hacking and Network Defense

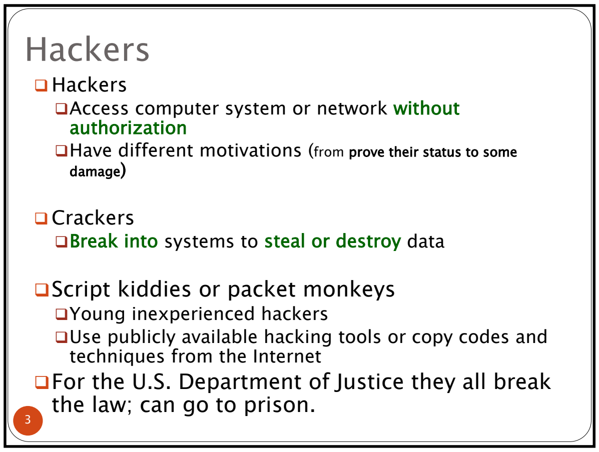
January 14, 2010

MIS 4600 – © Abdou Illia



Objectives

- Describe the role of an ethical hacker
- Describe what can an ethical hacker legally do
- Describe what an ethical hacker cannot legally do



Hackers

- Hackers
  - Access computer system or network **without authorization**
  - Have different motivations (from **prove their status to some damage**)
- Crackers
  - **Break into** systems to **steal or destroy** data
- Script kiddies or packet monkeys
  - Young inexperienced hackers
  - Use publicly available hacking tools or copy codes and techniques from the Internet
- For the U.S. Department of Justice they all break the law; can go to prison.

Hackers vs. Ethical Hackers

- Ethical hacker
  - Performs most of the same activities as hackers and crackers, but with owner’s permission
  - Employed by companies to perform penetration or security tests
- Red team
  - Team of ethical hackers with varied skills (social engineering, ethics/legal issues, break-ins, etc.)

Penetration test vs. Security test

- Penetration test
  - Legally breaking into a company’s network to find its weaknesses
  - Tester only reports findings
- Security test
  - More than a penetration test
  - Also **includes**:
    - Analyzing company’s security policy and procedures
    - Offering solutions to secure or protect the network

Security Policy

- Sets rules for expected behaviors by users (e.g. regular patches download, strong passwords, etc.), and IT personnel (e.g. no unauthorized access to users’ files, …), etc.

- Defines access control rules.

- Defines consequences of violations.

-Helps track compliance with regulations.

- Etc.

Passwords must not be written down

Access to files must be granted to the level required by users’ job

Hacking Tools

- Referred to as Tiger box in course textbook
- Collection of OSs and tools that assist with hacking
  - Network scanners
  - Traffic monitors
  - Keyloggers
  - Password crackers
  - Etc.
- Practical Extraction and Report Language (Perl)
- C programming language
- Scripts, i.e. set of instructions that runs in sequence

Questions

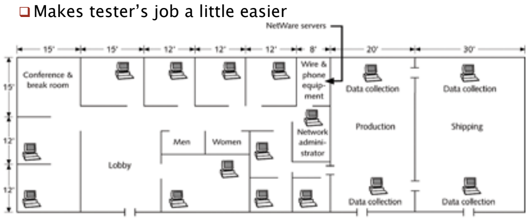
- Which of the following may be part of a penetration test (P) or a security test (S)? Use “X” to indicate your answer.

		P	S
1.	Breaking into a computer system without authorization.		
2.	Laying out specific actions to be taken in order to prevent dangerous packets to pass through firewalls.		
3.	Scanning a network in order to gather IP addresses of potential targets		
4.	Finding that patches are not timely applied as recommended by corporate rules.		
5.	Writing a report about a company’s security defense system.		
6.	Scanning a network in order to find out what defense tools are being used.		
7.	Finding that users cannot change their passwords themselves		
8.	Finding that a company does not have an effective password reset rule.		
9.	Finding out that a firewall does not block potentially dangerous packets		
10	Proposing a new procedure which implementation may help improve systems security		
11	Finding out that the administrator's account is called Admin and has a weak password		
12	Finding out that 1/3 of the security procedures are not actually implemented.		
13	Performing a denial-of service-attacks		
14	Disabling network defense systems		

Penetration Testing Models

➡ White box
Black box
Gray box

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



Note: some diagrams may show routers, firewalls, etc.

Figure 1-1 A sample network diagram

Penetration Testing Models (cont.)

➡ White box
Black box
Gray box

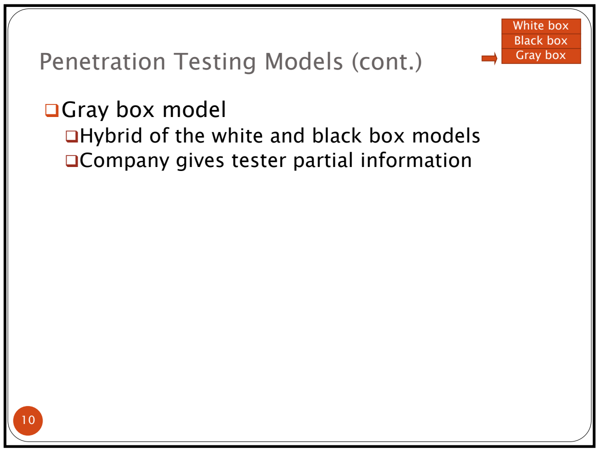
- Black box model
  - Company staff does not know about the test
  - Tester is not given details about the network.
    - Burden is on the tester to find these details
  - Tests if security personnel are able to detect an attack

  - Question: What is the disadvantage of letting the company’s employees know about the penetration test?

  ____

  - Question: What is the disadvantage of letting the IT staff know about the penetration test?

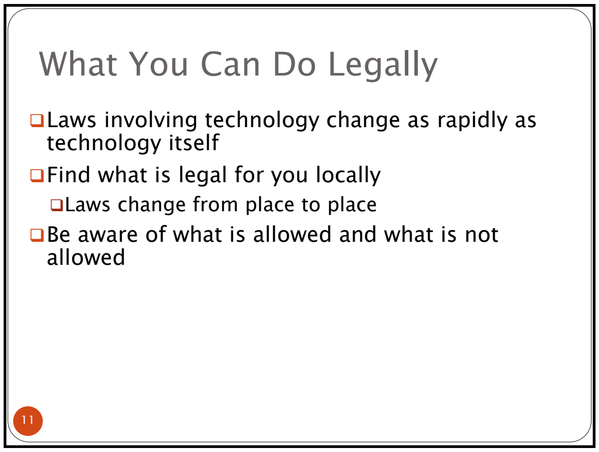
  ____



Penetration Testing Models (cont.)

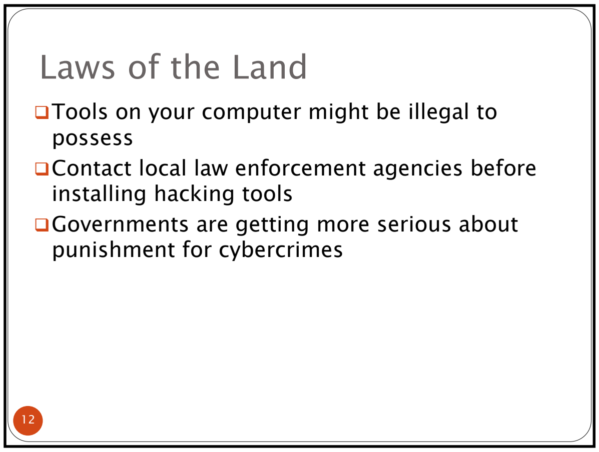
White box
Black box
Gray box

- Gray box model
  - Hybrid of the white and black box models
  - Company gives tester partial information



What You Can Do Legally

- Laws involving technology change as rapidly as technology itself
- Find what is legal for you locally
  - Laws change from place to place
- Be aware of what is allowed and what is not allowed

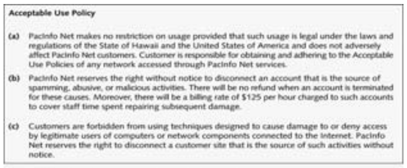


Laws of the Land

- Tools on your computer might be illegal to possess
- Contact local law enforcement agencies before installing hacking tools
- Governments are getting more serious about punishment for cybercrimes

Is Port Scanning Legal?

- ❑Some states deem it legal
- ❑Not always the case
- ❑Federal Government does not see it as a violation
  - ❑Allows each state to address it separately
- ❑Read your ISP's "Acceptable Use Policy"



Acceptable Use Policy

(a) PacInfo Net makes no restriction on usage provided that such usage is legal under the laws and regulations of the State of Hawaii and the United States of America and does not adversely affect PacInfo Net customers. Customer is responsible for obtaining and adhering to the Acceptable Use Policies of any network accessed through PacInfo Net services.

(b) PacInfo Net reserves the right without notice to disconnect an account that is the source of spamming, abusive, or malicious activities. There will be no refund when an account is terminated for these causes. Moreover, there will be a billing rate of $125 per hour charged to such accounts to cover staff time spent repairing subsequent damage.

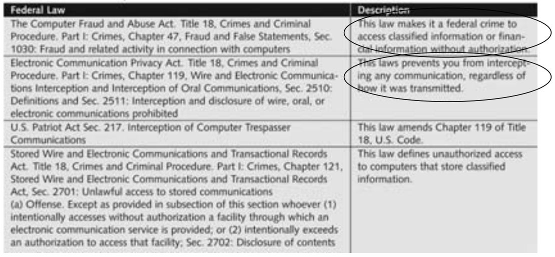
(c) Customers are forbidden from using techniques designed to cause damage to or deny access by legitimate users of computers or network components connected to the Internet. PacInfo Net reserves the right to disconnect a customer site that is the source of such activities without notice.

Figure 1-2 An example of an acceptable use policy

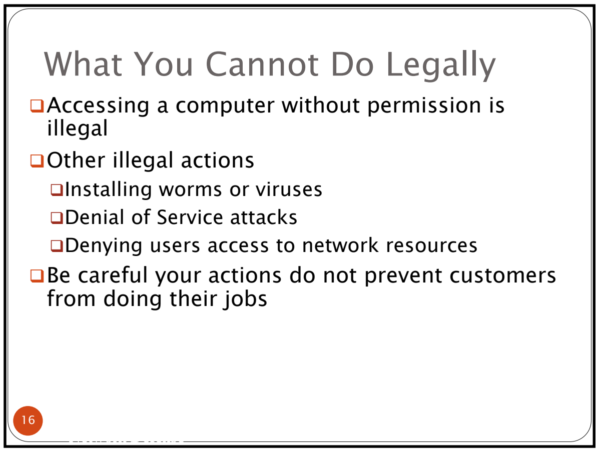
Federal Laws

- ❑Federal computer crime laws are getting more specific
  - ❑Cover cybercrimes and intellectual property issues
- ❑Computer Hacking and Intellectual Property (CHIP)
  - ❑New government branch to address cybercrimes and intellectual property issues

Table 1-2 Federal computer crime laws

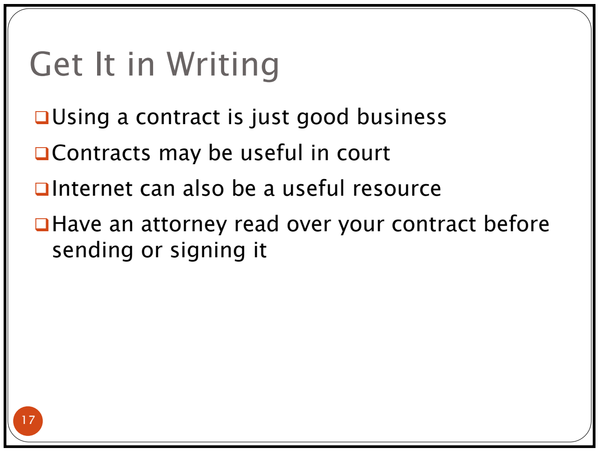


Federal Law	Description
The Computer Fraud and Abuse Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 47, Fraud and False Statements, Sec. 1030: Fraud and related activity in connection with computers	This law makes it a federal crime to access classified information or financial information without authorization.
Electronic Communication Privacy Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 119, Wire and Electronic Communications Interception and Interception of Oral Communications, Sec. 2510: Definitions and Sec. 2511: Interception and disclosure of wire, oral, or electronic communications prohibited	This laws prevents you from intercepting any communication, regardless of how it was transmitted.
U.S. Patriot Act Sec. 217. Interception of Computer Trespasser Communications	This law amends Chapter 119 of Title 18, U.S. Code.
Stored Wire and Electronic Communications and Transactional Records Act. Title 18, Crimes and Criminal Procedure. Part I: Crimes, Chapter 121, Stored Wire and Electronic Communications and Transactional Records Act, Sec. 2701: Unlawful access to stored communications (a) Offense. Except as provided in subsection of this section whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; Sec. 2702: Disclosure of contents	This law defines unauthorized access to computers that store classified information.



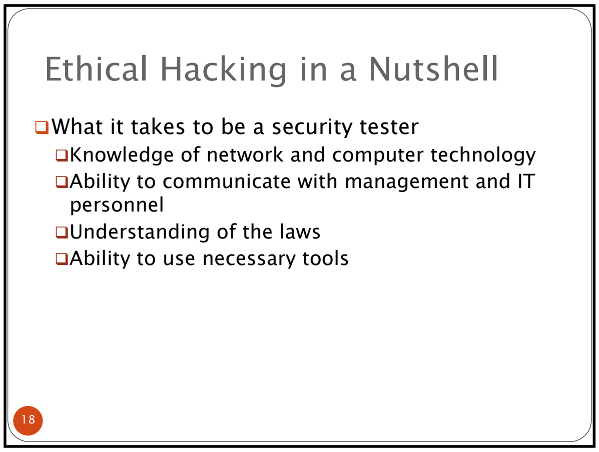
What You Cannot Do Legally

- Accessing a computer without permission is illegal
- Other illegal actions
  - Installing worms or viruses
  - Denial of Service attacks
  - Denying users access to network resources
- Be careful your actions do not prevent customers from doing their jobs



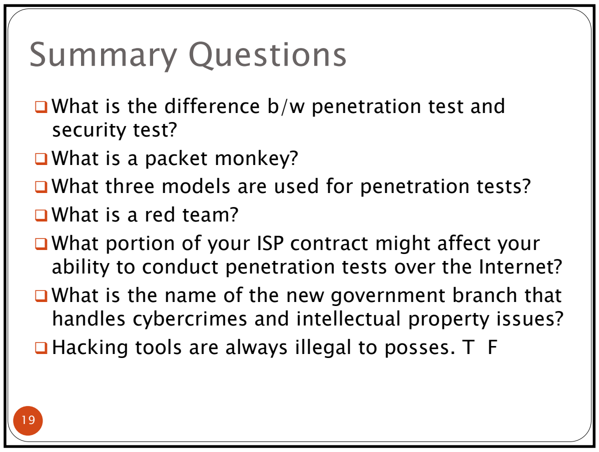
Get It in Writing

- Using a contract is just good business
- Contracts may be useful in court
- Internet can also be a useful resource
- Have an attorney read over your contract before sending or signing it



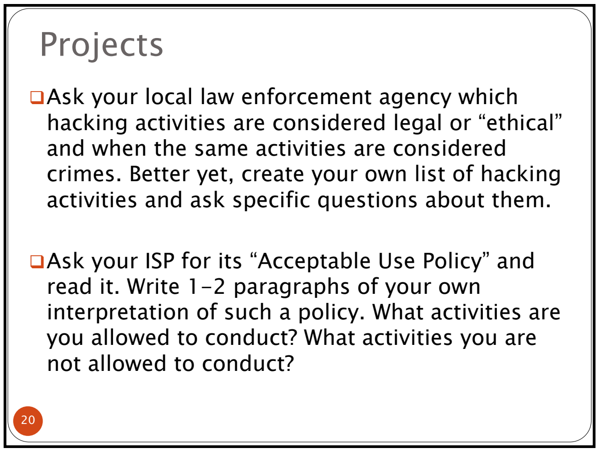
Ethical Hacking in a Nutshell

- What it takes to be a security tester
  - Knowledge of network and computer technology
  - Ability to communicate with management and IT personnel
  - Understanding of the laws
  - Ability to use necessary tools



Summary Questions

- What is the difference b/w penetration test and security test?
- What is a packet monkey?
- What three models are used for penetration tests?
- What is a red team?
- What portion of your ISP contract might affect your ability to conduct penetration tests over the Internet?
- What is the name of the new government branch that handles cybercrimes and intellectual property issues?
- Hacking tools are always illegal to posses. T F



Projects

- Ask your local law enforcement agency which hacking activities are considered legal or “ethical” and when the same activities are considered crimes. Better yet, create your own list of hacking activities and ask specific questions about them.
- Ask your ISP for its “Acceptable Use Policy” and read it. Write 1-2 paragraphs of your own interpretation of such a policy. What activities are you allowed to conduct? What activities you are not allowed to conduct?