Ethic Hacking

CSC 4222

Partial slides from samsclass.info, deserve credits.

Hackers

- Hackers
  - Access computer system or network **without authorization**
  - Have different motivations (from **prove their status to doing some damage**)

- Crackers
  - **Break into** systems to **steal or destroy** data

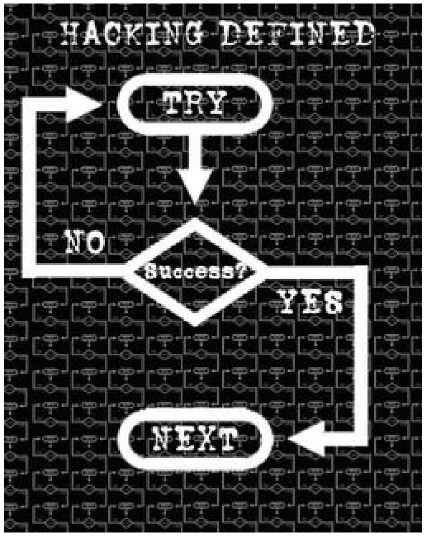
- For the U.S. Department of Justice they all break the law; can go to prison.

Types of Hackers

- Black Hat Hacker/cracker
  - with extraordinary computing skills, resorting to malicious or destructive activities, use their knowledge and skill for their own personal gains probably by hurting others.
- White Hat Hacker
  - professing hacker skills and using them for defensive purposes, use their knowledge and skill for the good of others and for the common good.
- Grey Hat Hacker
  - work both offensively and defensively at various times, cannot predict their behavior.

Hacking Process

- General step of hacking



- Foot Printing
- Scanning
- Gaining Access
- Maintaining Access

What do hackers do after hacking?...

- Patch Security hole
    - The other hackers can’t intrude
- Clear logs and hide themselves
- Install rootkit (backdoor)
    - The hacker who hacked the system can use the system later
    - It contains Trojan virus, and so on
- Install scanner program
    - mscan, sscan, nmap
- Install exploit program
- Install denial of service program
- Use all of installed programs silently

Duty is what counts!

- what we want is of no importance; duty is what counts.
  - Hacking into systems to gain knowledge of the software or to point out flaws is wrong, even if no damage is done to the system.
- Breaking and Entering- if you break into someone’s house, but don’t take anything or break anything you are still committing a crime.
  - Taking away a person’s sense of security.

information IS property

- According to United Kingdom, with the Criminal Damage Act of 1971.
  - Offender in the UK was convicted of property damage even though the property was not tangible and the damage could only be determined by the machine.
- The Computer Misuse Act of 1990
  - “unauthorized access”
  - “data modification”
  - makes crimes easier to prosecute.

Public Information

- Some information on the internet is made accessible to the public.
  - but should not be destroyed or edited without authorization.
- Other information that is not purposefully made accessible
  - Account numbers and personal information should not be sought after regardless of one’s intentions.

International Legislation

- International groups like the United Nations and the Council of Europe are writing legislation that applies internationally.
- Three types of Cybercrime as using a computer as a:
  - target- spreading viruses
  - tool- using a computer to commit traditional crimes such as credit card fraud
  - accessory- to store illegal or stolen information.

Freedom of Speech

- Hacktivism violates people’s first amendment rights of Freedom of Speech.
  - instead create you own website or blog rather than editing the site of a political group.
- According to Kant: no ones rights should be taken at the expense of another’s because all of mankind is equal.

Hidden Subculture

- Hackers design this subculture and trust system so they don’t get caught.
  - keep a low profile
  - don’t brag about what you are doing to people outside of the network
  - don’t narc on a fellow hacker if you are caught
- Why?
  - hackers know what they are doing is wrong and they develop a system of “cultural norms” to avoid prosecution.

Ethical Hacking

- Ethical hacking also known as penetration testing or white-hat hacking, involves the same tools, tricks, and techniques that hackers use, but with one major difference that Ethical hacking is legal.

- Independent computer security Professionals breaking into the computer systems.
- Neither damage the target systems nor steal information.
- Evaluate target systems security and report back to owners about the vulnerabilities found.

Required Skills of an Ethical Hacker

- Microsoft: skills in operation, configuration and management.
- Linux: knowledge of Linux/Unix; security setting, configuration, and services.
- Firewalls: configurations, and operation of intrusion detection systems.
- Routers: knowledge of routers, routing protocols, and access control lists
- Mainframes
- Network Protocols: TCP/IP; how they function and can be manipulated.
- Project Management: leading, planning, organizing, and controlling a penetration testing team.

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
  - Use hacking toolsets in authorized way

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.

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

Passwords must not be written down

Questions

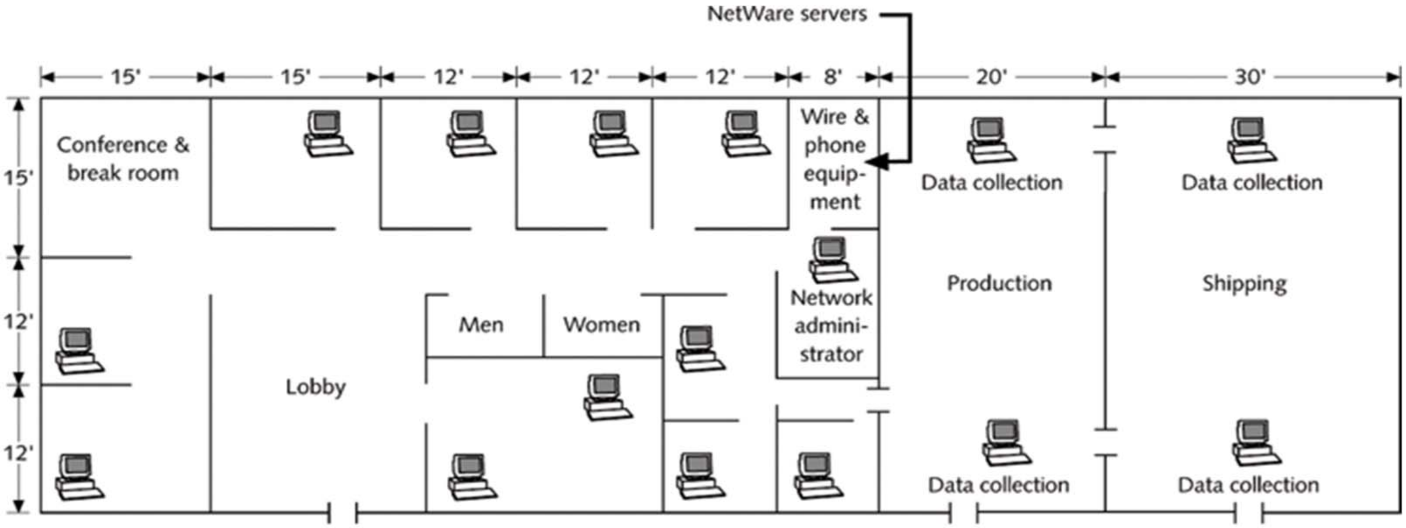
- Which of the following may be part of a penetration test (P) or a security test (S)? Use “X” to indicate your answer.

		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		

White box
Black box
Gray box

Penetration Testing Models

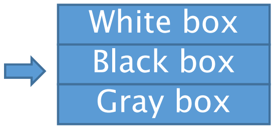
- White box model
  - Tester is told everything about the network topology and technology
  - Tester is authorized to interview IT personnel and company employees



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?

____

White box
Black box
Gray box

Penetration Testing Models (cont.)

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

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

Some Tools

- **Kali Linux / Backtrack 5R3** : Attacker's System.
- **NMAP** : Used for identifying ports and services running on victims machine. "King of Scanners"
- **Metasploit Framework** : Used for exploiting, generating payloads and establishing session with victim's machine.

Advantages - Ethical Hackers

- “To catch a thief you have to think like a thief”
- Helps in closing the open holes in the system network
- Provides security to banking and financial establishments
- Prevents website defacements
- An evolving technique

Disadvantages - Ethical Hackers

- All depends upon the trustworthiness of the ethical hacker

- Hiring professionals is expensive.

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
- 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

Laws of the Land

- Tools on your computer might be illegal to possess
- Contact local law enforcement agencies before installing hacking tools
- Written words are open to interpretation
- 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"
  - IRC "bots" may be forbidden
    - Program that sends automatic responses to users
    - Gives the appearance of a person being present

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

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

what do YOU think?

- Hacking into government systems to point out security flaws without harm to the system?
  - Ethical?
  - Not Ethical?

- Hacking into a home computer to point out security flaws?
  - Ethical?
  - Not Ethical?

what do YOU think?

- A graduate student specializing in computer security creates a website similar to Northwest Airlines to demonstrate that terrorists can make fake boarding passes.
  - Ethical?
  - Not ethical?

what do YOU think?

- A data collecting company claims to keep certain information private, such as SSN and account numbers. A hacker discovers that the company did not keep its promise. The private information is actually published on the report. The hacker makes his findings public in a news outlet.
  - Ethical?
  - Not ethical?

what do YOU think?

- Hacking into the website of a political candidate and editing information because you disagree with his position?
  - Ethical?
  - Not Ethical?

Conclusion and Personal suggestion

- In the preceding sections we saw the methodology of hacking, why should we aware of hacking and some tools which a hacker may use.
- Now we can see what can we do against hacking or to protect ourselves from hacking.
- The first thing we should do is to keep ourselves updated about those software's we and using for official and reliable sources.
- Educate the employees and the users against black hat hacking.