NETWORK SECURITY

Ch. 7: Legal & Ethics

PROGRAM TEKNOLOGI INFORMASI DAN ILMU KOMPUTER

Term Hacker

- Most people think hackers have extraordinary skill and knowledge that allow them to hack into computer systems and find valuable information
- How your thought?

In reality

- a good hacker, or security professional acting as an ethical hacker, just has to understand how a computer system works and know what tools to employ in order to find a security weakness
- Hackers use specialized computer software tools to gain access to information

Ethical hacker act?

- Most ethical hackers are in the business of hacking for profit, an activity known as *penetration testing*, or *pen testing* for short
- Conduct themselves in a professional manner.
- Staying within the law is a must for the ethical hacker

Defining

- Gaining the trust of the client and taking all precautions to do no harm to their systems during a pen test are critical to being a professional
- gain permission from the data owner prior to accessing the computer system

Purpose

- Can hacking be ethical?
- Ethical hackers are usually security professionals or network penetration testers who use their hacking skills and toolsets for defensive and protective purposes

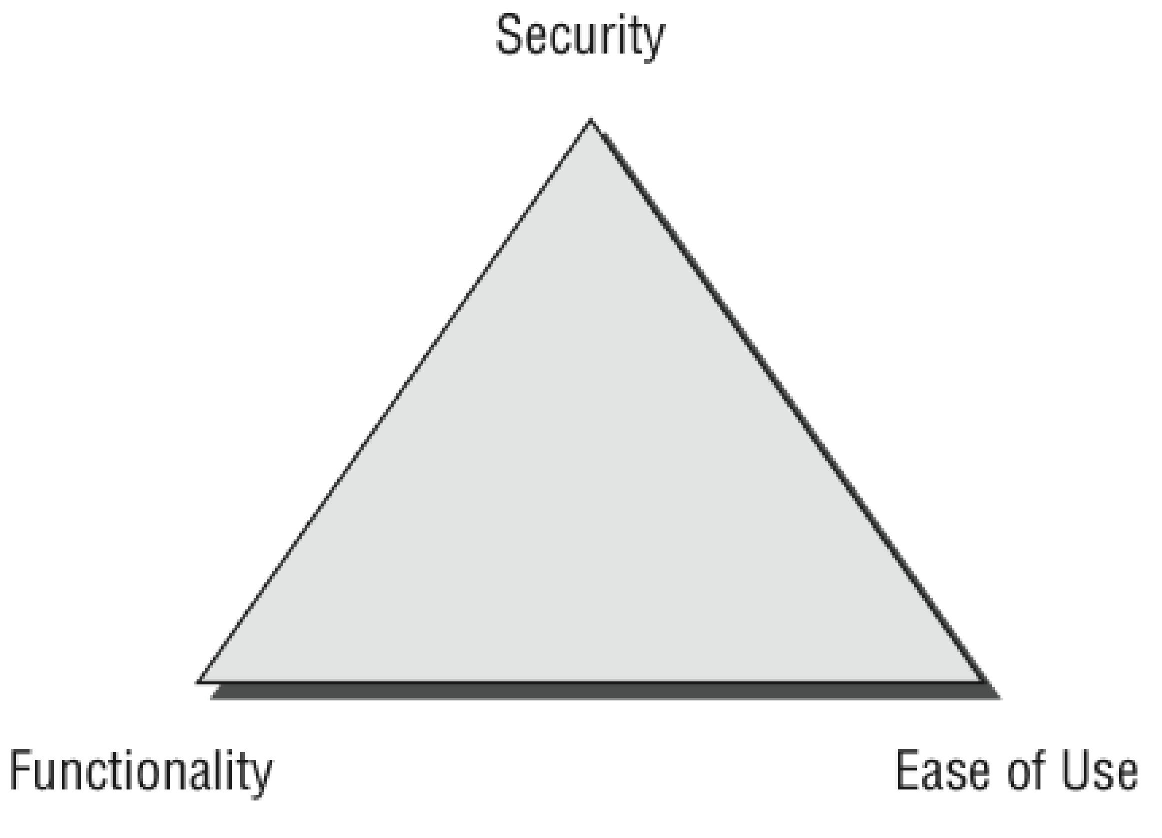
Malicious hacker

- The term *cracker* describes a hacker who uses their hacking skills and toolset for destructive or offensive purposes such as disseminating viruses or performing denial-of-service (DoS) attacks to compromise or bring down systems and networks
- Note :
  - White hacker
  - Black Hacker
  - Gray Hacker

Goals Attackers Try to Achieve

- All attacks are an attempt to breach computer system security.
  - Confidentiality
  - Authenticity
  - Integrity
  - Availability

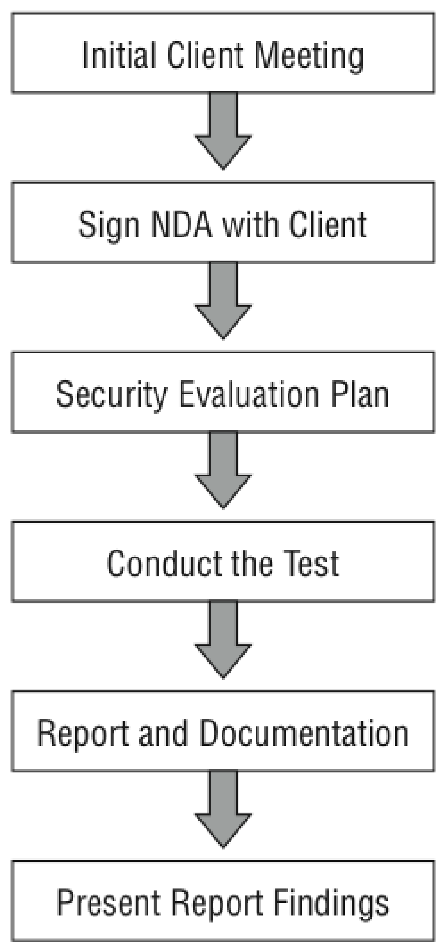
Security, Functionality, and Ease of Use Triangle



How to Be Ethical

- An ethical hacker must do the following:
  - Gain authorization from the client and have a signed contract giving the tester permission to perform the test.
  - Maintain and follow a nondisclosure agreement (NDA) with the client in the case of confidential information disclosed during the test.
  - Maintain confidentiality when performing the test. Information gathered may contain sensitive information. No information about the test or company confidential data should ever be disclosed to a third party.
  - Perform the test up to but not beyond the agreed-upon limits

Ex: Security audit steps



Initial Client Meeting

Sign NDA with Client

Security Evaluation Plan

Conduct the Test

Report and Documentation

Present Report Findings

Keeping It Legal

- An ethical hacker should know the penalties of unauthorized hacking into a system.
- security audit should begin until a signed legal document giving the ethical hacker express permission to perform the hacking activities is received from the target organization.
- to be judicious with their hacking skills and recognize the consequences of misusing those skills.

Cyber Security Enhancement Act and SPY ACT

- The Securely Protect Yourself Against Cyber Trespass Act of 2007 (SPY ACT) deals with the use of spyware on computer systems and essentially prohibits the following:
  - Taking remote control of a computer when you have not been authorized to do so
  - Using a computer to send unsolicited information to people (commonly known as spamming)
  - Redirecting a web browser to another site that is not authorized by the user

Cyber Security Enhancement Act and SPY ACT (Cont.)

- Displaying advertisements that cause the user to have to close out of the web browser (pop-up windows)
- Collecting personal information using keystroke logging
- Changing the default web page of the browser
- Misleading users so they click on a web page link or duplicating a similar web page to mislead a user

18 USC §1029 and 1030

- The U.S. Code categorizes and defines the laws of the United States by titles
  - Title 18 details “Crimes and Criminal Procedure.”
  - Section 1029, “Fraud and related activity in connection with access devices,”
  - Section 1030, “Fraud and related activity in connection with computers,”

U.S. State Laws

- Many states have their own laws associated with hacking and auditing computer networks and systems.
- The National Security Institute has a website listing all the state laws applicable to com- puter crimes
  - http://nsi.org/Library/Compsec/computerlaw/statelaws.html

Federal Managers Financial Integrity Act

- Responsibility act to ensure that those managing financial accounts are doing so with the utmost responsibility and are ensuring the protection of the assets
- The act essentially ensures that
  - Funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation.
  - Costs are in compliance with applicable laws.

Freedom of Information Act (FOIA)

- makes many pieces of information and documents about organizations public.
- Most records and government documents can be obtained via the FoIA

Federal Information Security Management Act (FISMA)

- Basically gives ethical hackers the power to do the types of testing they perform and makes it a mandatory requirement for government agencies.

Privacy Act of 1974

- Ensures nondisclosure of personal information and ensures that government agencies are not disclosing information without the prior written consent of the person whose information is in question.

USA PATRIOT Act

- Gives the government the authority to intercept voice communications in computer hacking and other types of investigations.

Government Paperwork Elimination Act (GPEA)

- Requires federal agencies to allow people the option of using electronic communications when interacting with a government agency.
- GPEA also encourages the use of electronic signatures.

Cyber Law in Indonesia

- Other countries each have their own applicable laws regarding protection of information and hacking attacks
  - UU-ITE-11-2008
  - UU14th2008 KIP
  - RUU Rahasia Negara
  - 19-02 UU Hak Cipta
  - PP-60 TAHUN 2008-SISTEM PENGENDALIAN INTERNAL PEMERINTAH
  - SNI 7512 2008 Pengelolaan Insiden Keamanan Informasi

UU ITE

- BAB VII PERBUATAN YANG DILARANG
  - Pasal 27, …. Pasal 39
- Pidana
  - Jail up to 10 years
  - Denda 12 Million