# Ethical Hacking

Mohona Ghosh

# How to be Ethical ?

1. Ethical hacking is usually conducted in a structured and organized manner, usually as part of a penetration test or security audit
2. The depth and breadth of the systems and applications to be tested are usually determined by the needs and concerns of the client
3. The ethical hacker must follow certain rules to ensure that all ethical and moral obligations are met. 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.

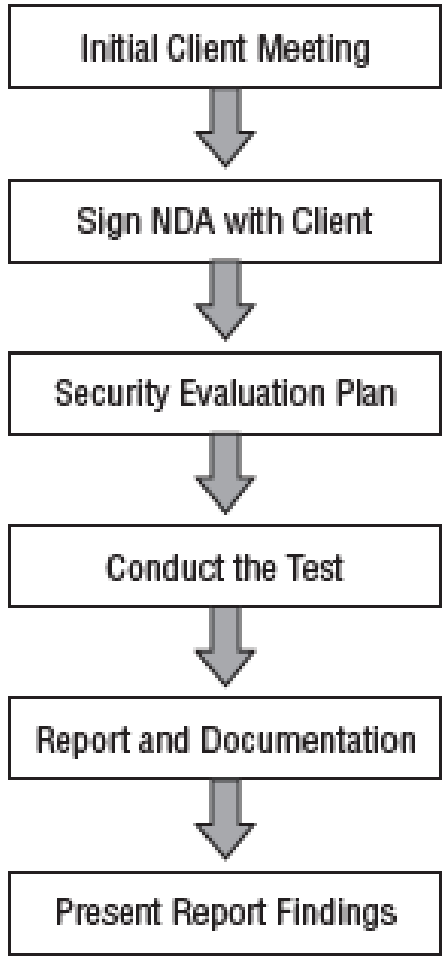
# How to be Ethical ?

- 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. For example, DoS attacks should only be run as part of the test if they have previously been agreed upon with the client. Loss of revenue, goodwill, and worse could befall an organization whose servers or applications are unavailable to customers as a result of the testing.

# How to be Ethical ?

The following steps are a framework for performing a security audit of an organization and will help to ensure that the test is conducted in an organized, efficient, and ethical manner:

- Talk to the client, and discuss the needs to be addressed during the testing.
- Prepare and sign NDA documents with the client.
- Organize an ethical hacking team, and prepare a schedule for testing
- Conduct the test
- Analyze the results of the testing, and prepare a report.
- Present the report findings to the client.



# Ethical Hacking Laws

- In USA
- In India

An ethical hacker should know the penalties of unauthorized hacking into a system. No ethical hacking activities associated with a network-penetration test or 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. Ethical hackers need to be judicious with their hacking skills and recognize the consequences of misusing those skills.

# Ethical Hacking Laws (USA)

## Cyber Security Enhancement Act and SPY ACT

The Cyber Security Enhancement Act of 2002 mandates life sentences for hackers who "recklessly" endanger the lives of others. Malicious hackers who create a life-threatening situation by attacking computer networks for transportation systems, power companies, or other public services or utilities can be prosecuted under this law.

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
- 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

The SPY ACT is important in that it starts to recognize annoying pop-ups and spam as more than mere annoyances and as real hacking attempts. The SPY ACT lays a foundation for prosecuting hackers that use spam, pop-ups, and links in emails.

# Ethical Hacking Laws (USA)

## 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," states that if you produce, sell, or use counterfeit access devices or telecommunications instruments with intent to commit fraud and obtain services or products with a value over $1,000, you have broken the law. Section 1029 criminalizes the misuse of computer passwords and other access devices such as token cards.

Section 1030, "Fraud and related activity in connection with computers," prohibits accessing protected computers without permission and causing damage. This statute criminalizes the spreading of viruses and worms and breaking into computer systems by unauthorized individuals.

# Ethical Hacking Laws (USA)

## Freedom of Information Act (FOIA)

The Freedom of Information Act (5 USC 552), or FoIA, makes many pieces of information and documents about organizations public. Most records and government documents can be obtained via the FoIA. Any information gathered using this act is fair game when you are performing reconnaissance and information gathering about a potential target.

# Ethical Hacking Laws (USA)

## Federal Information Security Management Act (FISMA)

The 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.

FISMA requires that each federal agency develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The information security program must include the following:

- Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each agency information system
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the agency) of the information security risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce these risks
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices (including the management, operational, and technical controls of every agency information system identified in their inventory) with a frequency depending on risk, but no less than annually
- A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency
- Procedures for detecting, reporting, and responding to security incidents (including mitigating risks associated with such incidents before substantial damage is done and notifying and consulting with the federal information security incident response center, and as appropriate, law enforcement agencies, relevant Offices of Inspector General, and any other agency or office, in accordance with law or as directed by the President
- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency

This act is guaranteed job security for ethical white hat hackers to perform continual security audits of government agencies and other organizations.

# Ethical Hacking Laws (USA)

## Privacy Act of 1974

The Privacy Act of 1974 (5 USC 552a) 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.

# Ethical Hacking Laws (India)

- The abuse of computers has given birth to a gamut of new age crimes that are addressed by the **Information Technology Act, 2000**. **Cyber crimes** can be categorised in two ways:
  - **The Computer as a Target :** Using a computer to attack other computers. e.g., Hacking, Virus/Worm attacks, DOS attack etc**.**
  - **The computer as a weapon :** Using a computer to commit real world crimes. e.g., Cyber Terrorism, IPR violations, Credit card frauds, Pornography etc.

# Ethical Hacking Laws (India)

**Notable features of the ITA 2000 are:**

- Focusing on data privacy
- Focusing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognizing the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- Authorizing an Inspector to investigate cyber offenses (as against the DSP earlier)

# Ethical Hacking Laws (India)

- **Under the Information Technology Act, 2000, various sections penalizes various offenses**
  - **Section 65:**
    - **For:** Tampering with computer source documents - Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

# Ethical Hacking Laws (India)

- **Under the Information Technology Act, 2000, various sections penalizes various offenses**
  - **Section 43:**
    - **For:** Penalty and Compensation for damage to computer, computer system etc. - The section deals with the compensation that should be made for failure of protection of the date. The corporate responsibility for data protection is greatly emphasized by inserting Section 43A whereby corporate are under an obligation to ensure adoption of reasonable security practices. Under this new law, "sensitive personal data or information of a person" means such personal information which consists of information relating to:
      (i) password;
      (ii) financial information such as Bank account or credit card or debit card or other payment instrument details;
      (iii) physical, physiological and mental health condition;
      (iv) sexual orientation;
      (v) medical records and history;
      (vi) Biometric information etc.
    - Negligence in implementing and maintaining reasonable security practices and procedures may make a person liable to pay damages. It is interesting to note that the Information Technology Act originally capped compensation claims at Rs 1 crore under section 43. This cap has now been removed. Compensation claims upto Rs 5 crore are now handled by Adjudicating Officers while claims above Rs 5 crore are handled by the relevant courts.

# Ethical Hacking Laws (India)

- **Under the Information Technology Act, 2000, various sections penalizes various offenses**
  - **Section 66:**
    - **For:** Hacking with computer system- If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.
    - **Punishment:** Imprisonment up to three years, or/and with fine up to ₹500,000
  - **Section 66B:**
    - **For:** Receiving stolen computer or communication device – If A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen
    - **Punishment:** Imprisonment up to three years, or/and with fine up to ₹100,000

# Ethical Hacking Laws (India)

- **Under the Information Technology Act, 2000, various sections penalizes various offenses**
  - **Section 66C:**
    - **For:** Using password of another person- If a person fradulently uses the password, digital signature or other unique identification of another person
    - **Punishment:** Imprisonment up to three years, or/and with fine up to ₹100,000
  - **Section 66E:**
    - **For:** Publishing private images of others
    - **Punishment:** Imprisonment up to three years, or/and with fine up to ₹200,000

# Ethical Hacking Laws (India)

- **Under the Information Technology Act, 2000, various sections penalizes various offenses**
  - **Section 67B:**
    - **For:** Publishing child porn or predating children online - If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct or If a person induces a child into a sexual act. A child is defined as anyone under 18.
    - **Punishment:** Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
  - **Section 67C:**
    - **For:** Failure to maintain records - Persons deemed as intermediary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.
    - **Punishment:** Imprisonment up to three years, or/and with fine.

# Ethical Hacking Laws (India)

- **Under the Information Technology Act, 2000, various sections penalizes various offenses**
  - **Section 69:**
    - **For:** Failure/refusal to decrypt data - If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.
    - **Punishment:** Imprisonment up to seven years and possible fine.

# Ethical Hacking Laws (India)

- **Under the Information Technology Act, 2000, various sections penalizes various offenses**
  - **Section 70:**
    - **For:** Securing access or attempting to secure access to a protected system – The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.
    - **Punishment:** Imprisonment up to ten years, or/and with fine.
- REF: https://en.wikipedia.org/wiki/Information_Technology_Act,_2000#Section_66