ETHICAL DISCLOSURE

INTRODUCTION TO ETHICAL DISCLOSURE

Session Agenda:

1.what is ethical hacking disclosure?

2.Ethics of Ethical Hacking

3.Ethical Hacking and the legal system

4.How does Ethical hacking work?

5.Laws To Remember as an Ethical Hacker

INTRODUCTION TO ETHICAL DISCLOSURE

> What is ethical hacking disclosure?

Ethical hacking is done for the security of the client's system or network.

Disclosure of **the client's confidential information renders ethical hacking ineffective.**

Private information must be kept private, and confidential information must be kept confidential.

INTRODUCTION TO ETHICAL DISCLOSURE

Ethics of Ethical Hacking

Ethical hacking is **always performed with consent.**

While the object of engagements is to accurately reproduce the tactics, techniques and procedures used by cybercriminals, it is never designed to be malicious and aims to avoid damage and disruption to businesses.

Ethical hacking uses the principles and techniques of hackers to help businesses protect their infrastructure and information (You could also say it is used as an offensive part of a modern army's arsenal, but that is not what we do).

Many people wonder about our trademark tagline: "Professionally Evil," and we would like to discuss the benefits and ethics of our ethical hacking.

INTRODUCTION TO ETHICAL DISCLOSURE

Ethics of Ethical Hacking

Protecting the Defenseless

Finding and Fixing Vulnerabilities

Ensuring a More Secure World

Keep private and confidential information gained in your professional work, (in particular as it pertains to client lists and client personal information).

Not collect, give, sell, or transfer any personal information (such as name, e-mail address, Social Security number, or other unique identifier) to a third party without client prior consent.

INTRODUCTION TO ETHICAL DISCLOSURE

Ethics of Ethical Hacking

Protect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator.

Disclose to appropriate persons or authorities potential dangers to any ecommerce clients, the Internet community, or the public, that you reasonably believe to be associated with a particular set or type of electronic transactions or related software or hardware.

Ethics of Ethical Hacking

Provide service in your areas of competence, being honest and forthright about any limitations of your experience and education.

Ensure that you are qualified for any project on which you work or propose to work by an appropriate combination of education, training, and experience.

Never knowingly use software or process that is obtained or retained either illegally or unethically.

Not to engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

Ethics of Ethical Hacking

Use the property of a client or employer only in ways properly authorized, and with the owner's knowledge and consent.

Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

Ensure good management for any project you lead, including effective procedures for promotion of quality and full disclosure of risk.

Add to the knowledge of the e-commerce profession by constant study, share the lessons of your experience with fellow EC-Council members, and promote public awareness of benefits of electronic commerce.

Ethics of Ethical Hacking

Conduct oneself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in your knowledge and integrity.

Ensure ethical conduct and professional care at all times on all professional assignments without prejudice.

Not to neither associate with malicious hackers nor engage in any malicious activities.

Not to purposefully compromise or allow the client organization's systems to be compromised in the course of your professional dealings.

Ethics of Ethical Hacking

Ensure all penetration testing activities are authorized and within legal limits.

Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks.

Not to be part of any underground hacking community for purposes of preaching and expanding black hat activities.

Not to make inappropriate reference to the certification or misleading use of certificates, marks or logos in publications, catalogues, documents or speeches. Not convicted in any felony, or violated any law of the land.

Ethical Hacking and the legal system:

How does Ethical hacking work?

As ethical hacking is likely to be done with the permission of the victim or the targeted system, the only way to tackle black hat hacking is tackling it through ethical hacking, the techniques used in penetration are created in a way to emulate the real attacks without causing any damage and safeguard the organization or an individual against the cyber attacks.

After it is discovered how the attackers work the Network administrators, engineers and security professional emulate the environment of security level to conduct a penetration test.

The Steps that are involved in Penetration tests are as follows:

- **Ground rules should be established:** to set the expectation, to identify the parties involved, written permissions or an agreement of access mainly known as Statement of work in the United state

- **Passive Scanning**: Gathering information about the target without his knowledge also known as Open Source Intelligence, information such as Social Networking Site, Online databases etc.

- **Active Scanning and Enumeration**: Using investigating tools to scan the target's public exposure

The Steps that are involved in Penetration tests are as follows:

Fingerprinting: Performing investigation of the target systems to identify, operating system, applications, and patch level open ports, user accounts etc.
Selecting a target system.

Exploiting the uncovered vulnerabilities: executing the appropriate tools targeted at the suspected exposures.

Escalating privilege: escalate the security context so the ethical hacker has more control like gaining root or administrative rights, using cracked passwords for unauthorized access

Documenting and reporting: A file shall be maintained about every technique used or every tool that was used, vulnerabilities that were exploited and much more.

Laws To Remember as an Ethical Hacker

With the growth in usage of internet in India, cyber attacks have impacted the security of the computer networks as well; India adopted the model law on electronic commerce which was adopted by the United Nations Commission on International Trade Law consequently **Information Technology Act of 2000** came into force, the purpose of the act was an Act to provide legal recognition for transactions by means of electronic data interchange and, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information.

Laws To Remember as an Ethical Hacker

Section 43 of the Act states that if any person without permission of the owner or any other person who is an in charge of a computer, computer system or computer network, if modifies, damages, disrupts computer network, downloads, copies or extract any data or information from such computer network or accesses to such computer system he may be penalized for damages.

The term used in this provision is without permission of the owner that gives an impression if a person is working under the authority or in a good faith he may not be liable for the damages.

Laws To Remember as an Ethical Hacker

Section 43- A of the Act states that if any person fails to protect the data he is liable for compensation, so if an ethical hacker is a body corporate and he fails to protect the data he his handling he will be liable under section 43-A of IT Act.

Laws To Remember as an Ethical Hacker

Section 66 of the IT Act deals with the computer-related offences which state that any person who dishonestly and fraudulently does any act mentioned in section 43 of the Act he shall be penalized with 3 years.

Laws To Remember as an Ethical Hacker

The government agencies like CBI, Army and law enforcement bodies, Intelligence Bureau, Ministry of Communication and Information Technology under the Information Technology Act can form government agency under **section 70-A** and **Section 70-B** for the Critical Information Infrastructure Protection can recruit the cyber security experts to protect itself from cyber terrorism as laid down in **section 66-F** of the Information Technology Act where it has been mentioned without authorization or exceeds authorized access.

Laws To Remember as an Ethical Hacker

The IT law of India does penalize a hacker who does not have proper authorization to get access to the computer hacker but it does not protect ethical hackers unless he is employed by the government under **section 84**. Ethical hackers cannot be ignored, as their presence is much required to protect the computer networks against cyber terrorism and cyber attacks.

Thank You All