UNIT 5

Ethical Hacking Code of Ethics: Security, Risk & Issues

Hacking significantly affects the development of systems and networks. This is especially the case of systems and networks of organizations where sensitive or confidential information are used on a regular basis. Organizations must find solutions and measures to protect information technology assets. In this endeavor, organizations can use ethical hacking. Ethical hacking is a hacking role that business organizations can exploit for security purposes. Ethical hacking presents advantages to increase the capabilities of organizations to protect their IT and information assets. Ethical hacking sheds a positive light on hacking. Nonetheless, any organization that implements ethical hacking must consider the potential negative impacts and issues arising from the practice.

Legal Risks of Ethical Hacking

The legal risks of ethical hacking include lawsuits due to disclosure of personal or confidential information. Such disclosure can lead to a legal battle involving the organization and the ethical hacker. It is very easy for ethical hacking to result in a legal battle if it is not performed properly. It is also possible for the ethical hacker to commit errors to the point that the organization's profitability is negatively affected.

In such a case, the organization could sue the ethical hacker for failing to perform properly. The ethical hacker could be at legal risk if proper care and precaution are not seriously taken. To address these legal issues, it is imperative for the ethical hacker to always perform his job defensively to minimize compromising the client's system or network. Defensive performance emphasizes prevention and extra caution in ethical hacking.

Ethical Hacking Professional Issues

The professional issues of ethical hacking include possible ineffective performance on the job. Ethical hacking may be limited by the sensitivity of information involved in the client organization. Clients tend to impose requirements and limits on the activities of the ethical hacker.

For the ethical hacker to perform properly, access to the entire system or network might be needed. Because of the need for professionalism, the ethical hacker must not violate the limits imposed by the client so that professional issues are minimized.

Designing the Ethical Hacking Code of Ethics or Conduct

Codes of ethics or conduct for ethical hacking are focused on the duties, responsibilities and limits of the ethical hacker in doing his job. The ethical hacker makes sure that the

client's system or network is properly evaluated for security issues and vulnerabilities. Because of the nature of ethical hacking, it is not surprising that the ethical hacker could come across sensitive, personal, confidential or proprietary information. In this regard, the ethical hacking code of ethics should guide the actions of the ethical hacker in handling such information. The code of ethics must focus on the protection of the client's system or network, as well as the effectiveness of the ethical hacker in doing his job.

Code of Ethics for Ethical Hackers

- Before performing any ethical hacking, ensure that you know and understand the nature and characteristics of the client organization's business, system and network. This will guide you in handling sensitive, confidential or proprietary information you might encounter during the ethical hacking.
- Before and during ethical hacking, determine the sensitivity or confidentiality of the information involved. This should ensure that you do not violate laws, rules and regulations in handling sensitive personal, financial or proprietary information.
- During and after ethical hacking, maintain transparency with the client. Communicate all relevant information you found while ethically hacking the client's system or network. Transparency ensures that the client knows what is going on. Transparency enables the client to take necessary actions for security of the system or network.
- While performing ethical hacking, do not go beyond the limits set by the client. In ethical hacking, it is possible for you to have access beyond the target areas that the client signed up for. Stay within the target areas of the system or network specified in the work agreement. Do not go to other areas or components of the system or network that are not specified in the agreement. Minimize exposure of sensitive information. Increase your trustworthiness and reliability as an ethical hacker. Ensure the overall effectiveness of the ethical hacking activity.
- After performing ethical hacking, never disclose client information to other parties. Ensure the protection of the client. 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.

Does Ethical Hacking Need Legal Protection

Instead of providing legal protection to ethical hackers, focused laws defining the scope of work, roles and responsibilities of both parties need to be passed. The laws should address the following issues:

- The definition of ethical hacking

- Should ethical hacking be done only when solicited formally? Even so, there will be many opportunities for unsolicited hacking. How will unsolicited hacking be viewed?
- Only formal and detailed agreements between the hacker and the organization will be treated as solicited hacking. The agreement should derive content from the broader legal framework.
- Time is a critical factor in addressing a security flaw. When a security flaw is identified, it may need an immediate fix to prevent unauthorized breaches. Will every organization facilitate swift acceptance of the issue description and necessary action? Bureaucratic procedures can delay action and leave an opening for unauthorized hackers unaddressed. Will unsolicited hackers be punished if they bypass bureaucratic procedures and use other information channels like the MP did in the Netherlands?
- The legal agreement between the hacker and organization should clearly state the ethical hacker's job scope.
- Definition of compensation and rewards for both solicited and unsolicited hackers
- How do you address the issue if the unsolicited hacker misuses the security flaw?

Respnsibilities of ethical hackers

An ethical hacker might employ all or some of these strategies to penetrate a system:

- Scanning ports and seeking vulnerabilities: An ethical hacker uses port scanning tools like Nmap or Nessus to scan one’s own systems and find open ports. The vulnerabilities with each of the ports can be studied, and remedial measures can be taken.
- An ethical hacker will examine patch installations and make sure that they cannot be exploited.
- The ethical hacker may engage in social engineering concepts like dumpster diving—rummaging through trash bins for passwords, charts, sticky notes, or anything with crucial information that can be used to generate an attack.
- An ethical hacker may also employ other social engineering techniques like shoulder surfing to gain access to crucial information or play the kindness card to trick employees to part with their passwords.
- An ethical hacker will attempt to evade IDS (Intrusion Detection systems), IPS (Intrusion Prevention systems), honeypots, and firewalls.
- Sniffing networks, bypassing and cracking wireless encryption, and hijacking web servers and web applications.
- Ethical hackers may also handle issues related to laptop theft and employee fraud.

Detecting how well the organization reacts to these and other tactics help test the

strength of the security policy and security infrastructure. An ethical hacker attempts the same types of attacks as a malicious hacker would try—and then help organizations strengthen their defenses.

How to face the domain of ethical hacking

Nowadays, ethical hacking has become increasingly mainstream and multinational tech giants like Google, Facebook, Microsoft, Mozilla, IBM, etc employ hackers or teams of hackers in order to keep their systems secure.

And as a result of the success hackers have shown at discovering critical vulnerabilities, in the last year itself there has been a 26% increase in organizations running bug bounty programs, where they bolster their security defenses with hackers. Other than this there are a number of benefits that ethical hacking has provided to organizations majorly in the software industry.

- ### Carry out adequate preventive measures to avoid systems security breach

An ethical hacker takes preventive measures to avoid security breaches, for example, they use port scanning tools like Nmap or Nessus to scan one's own systems and find open ports. The vulnerabilities with each of the ports is studied, and remedial measures are taken by them.

An ethical hacker will examine patch installations and make sure that they cannot be exploited.

They also engage in social engineering concepts like dumpster diving—rummaging through trash bins for passwords, charts, sticky notes, or anything with crucial information that can be used to generate an attack.

They also attempt to evade IDS (Intrusion Detection Systems), IPS (Intrusion Prevention systems), honeypots, and firewalls. They carry out actions like bypassing and cracking wireless encryption, and hijacking web servers and web applications.

- ### Perform penetration tests on networks at regular intervals

One of the best ways to prevent illegal hacking is to test the network for weak links on a regular basis. Ethical hackers help clean and update systems by discovering new vulnerabilities on an on-going basis. Going a step ahead, ethical hackers also explore the scope of damage that can occur due to the identified vulnerability. This particular process is known as pen testing, which is used to identify network vulnerabilities that an attacker can target. There are many methods of pen testing. The organization may use different methods depending on its requirements. Any of the below pen testing methods can be carried out by an ethical hacker:

Targeted testing which involves the organization's people and the hacker. The organization staff will be aware of the hacking being performed.

External testing penetrates all externally exposed systems such as web servers and DNS.

Internal testing uncovers vulnerabilities open to internal users with access privileges.

Blind testing simulates real attacks from hackers.

Testers are given limited information about the target, which requires them to perform reconnaissance prior to the attack. Pen testing is the strongest case for hiring ethical hackers.

·

- ## Ethical hackers have built computers and programs for software industry

Going back to the early days of the personal computer, many of the members in the Silicon Valley would have been considered hackers in modern terms, that they pulled things apart and put them back together in new and interesting ways. This desire to explore systems and networks to find how it worked made many of the proto-hackers more knowledgeable about the different technologies and it can be safeguarded from malicious attacks.

Just as many of the early computer enthusiasts turned out to be great at designing new computers and programs, many people who identify themselves as hackers are also amazing programmers. This trend of the hacker as the innovator has continued with the open-source software movement. Much of the open-source code is produced, tested and improved by hackers – usually during collaborative computer programming events, which are affectionately referred to as "hackathons." Even if you never touch a piece of open-source software, you still benefit from the elegant solutions that hackers come up with that inspire or are outright copied by proprietary software companies.

- ## Ethical hackers help safeguard customer information by preventing data breaches

The personal information of consumers is the new oil of the digital world. Everything runs on data. But while businesses that collect and process consumer data have become increasingly valuable and powerful, recent events prove that even the world's biggest brands are vulnerable when they violate their customers' trust. Hence, it is of utmost importance for software businesses to gain the trust of customers by ensuring the security of their data.

With high-profile data breaches seemingly in the news every day, “protecting businesses from hackers” has traditionally dominated the data privacy conversation.

In such a scenario, ethical hackers will prepare you for the worst, they will work in conjunction with the IT-response plan to ensure data security and in patching breaches when they do happen. Otherwise, you risk a disjointed, inconsistent and delayed response to issues or crises. It is also imperative to align how your organization will communicate with stakeholders. This will reduce the need for real-time decision-making in an actual crisis, as well as help limit inappropriate responses. They may also help in running a cybersecurity crisis simulation to identify flaws and gaps in your process, and better prepare your teams for such a pressure-cooker situation when it hits.

.

.

.

- Information security plan to create security awareness at all levels

No matter how large or small your company is, you need to have a plan to ensure the security of your information assets. Such a plan is called a security program which is framed by information security professionals.

Primarily the IT security team devises the security program but if done in coordination with the ethical hackers, they can provide the framework for keeping the company at a desired security level. Additionally by assessing the risks the company faces, they can decide how to mitigate them, and plan for how to keep the program and security practices up to date.

Ethical Hacking and Social Engineering

Social engineering is the art of manipulating users of a computing system into revealing confidential information that can be used to gain unauthorized access to a computer system. The term can also include activities such as exploiting human kindness, greed, and curiosity to gain access to restricted access buildings or getting the users to installing backdoor software.

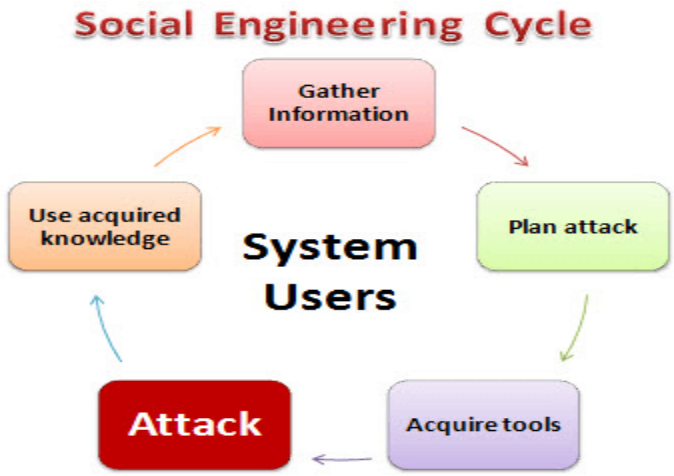
Knowing the tricks used by hackers to trick users into releasing vital login information among others is fundamental in protecting computer systems

In this tutorial, we will introduce you to the common social engineering

techniques and how you can come up with security measures to counter them.

How social engineering Works?

How to hack using Social Engineering



HERE,

Gather Information: This is the first stage, the learns as much as he can about the intended victim. The information is gathered from company websites, other publications and sometimes by talking to the users of the target system.

Plan Attack: The attackers outline how he/she intends to execute the attack

Acquire Tools: These include computer programs that an attacker will use when launching the attack.

Attack: Exploit the weaknesses in the target system.

Use acquired knowledge: Information gathered during the social engineering tactics such as pet names, birthdates of the organization founders, etc. is used in attacks such as password guessing.

Common Social Engineering Techniques:

Social engineering techniques can take many forms. The following is the list of the commonly used techniques.

Familiarity Exploit: Users are less suspicious of people they are familiar with. An attacker can familiarize him/herself with the users of the target system prior to

the social engineering attack. The attacker may interact with users during meals, on social events, etc. This makes the attacker familiar to the users. Let's suppose that the user works in a building that requires an access code or card to gain access; the attacker may follow the users as they enter such places. The users are most like to hold the door open for the attacker to go in as they are familiar with them. The attacker can also ask for answers to questions such as where you met your spouse, the name of your high school math teacher, etc. The users are most likely to reveal answers as they trust the familiar face. This information could be used to hack email accounts and other accounts that ask similar questions if one forgets their password.

Intimidating Circumstances: People tend to avoid people who intimidate others around them. Using this technique, the attacker may pretend to have a heated argument on the phone or with an accomplice in the scheme. The attacker may then ask users for information which would be used to compromise the security of the users' system. The users are most likely give the correct answers just to avoid having a confrontation with the attacker. This technique can also be used to avoid been checked at a security check point.

Phishing: This technique uses trickery and deceit to obtain private data from users. The social engineer may try to impersonate a genuine website such as Yahoo and then ask the unsuspecting user to confirm their account name and password. This technique could also be used to get credit card information or any other valuable personal data.

Tailgating: This technique involves following users behind as they enter restricted areas. As a human courtesy, the user is most likely to let the social engineer inside the restricted area.

Exploiting human curiosity: Using this technique, the social engineer may deliberately drop a virus infected flash disk in an area where the users can easily pick it up. The user will most likely plug the flash disk into the computer. The flash disk may auto run the virus, or the user may be tempted to open a file with a name such as Employees Revaluation Report 2013.docx which may actually be an infected file.

Exploiting human greed: Using this technique, the social engineer may lure the user with promises of making a lot of money online by filling in a form and confirm their details using credit card details, etc.

How to hack using Social Engineering

Most techniques employed by social engineers involve manipulating human biases. To counter such techniques, an organization can;

- To counter the familiarity exploit, the users must be trained to not substitute familiarity with security measures. Even the people that they are familiar with must prove that they have the authorization to access certain areas and information.
- To counter intimidating circumstances attacks, users must be trained to identify social engineering techniques that fish for sensitive information and politely say no.
- To counter phishing techniques, most sites such as Yahoo use secure connections to encrypt data and prove that they are who they claim to be. Checking the URL may help you spot fake sites. Avoid responding to emails that request you to provide personal information.
- To counter tailgating attacks, users must be trained not to let others use their security clearance to gain access to restricted areas. Each user must use their own access clearance.
- To counter human curiosity, it's better to submit picked up flash disks to system administrators who should scan them for viruses or other infection preferably on an isolated machine.
- To counter techniques that exploit human greed, employees must be trained on the dangers of falling for such scams.

Laws To Remember as an Ethical Hacker

Hacking has traveled from being an intellectual curiosity to a cybercrime around the world and has bothered the nations with the security, data breach, financial breach, only frauds etc. An unethical hacking is clearly an offence in the eyes of every nation. These offences have risen tremendously; Information technology and law were two different fields which never intersected but with the misuse of technology the law had to safeguard the rights of the netizens. Various legislations and laws have been framed across the world to safeguard the right of an individual in the virtual world of which ethical hacker has to keep in mind while working in good faith.

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.

There is a thin line between a black hat hacker and a white hat hacker which is laid in section 84 stating that the protection granted to the government, the controller or any person acting on behalf of them to act in good faith. If an ethical hacker is appointed by a government or a controller and the person has to act in pursuance of this act or any rule and regulation or order.

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.

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.

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 year years.

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 cybersecurity 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.

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.