Hacking generally refers to technical effort for manipulating the behavior of the network connections and connected systems. At first, the hacking took place in 1960's with MIT students coming up with some findings in the computing process.

In this article, we are going to explore the below-mentioned topics related to Ethical Hacking:

Ethical Hacking - Table of Contents

What is Ethical Hacking?

Hacking is carried out to gain access to the computer system or related computer network with the loopholes existing & read all the private data or sensitive data existing in it! Hacking a system to find the loopholes or weakness of the system or network used for computer with legal permissions is called as “Ethical Hacking”.

Is Ethical Hacking a Cybercrime?

Ethical hacking cannot be considered as a cybercrime unless the hacker disobeys the rules & does not follow the code of ethics agreement. Typically, hacking refers to gaining computer/network access without the permission of the concerned person or organization and lead to unlawful review of data, theft & file destruction. The entire process violates both federal & state laws. At the federal level, FBI investigates the hacker, and, at state level, we have several law enforcements for investigating the hacker. The precise crime depends on the individual who commits the crime, based on

- What system is Hacked.
- What information is accessed.
- For what purpose the information is used after accessing.
- Based on the threat for the host.

What is Cybercrime?

Cybercrime is defined as a crime where in a computer system is used as tool for committing the offence. Cybercrime includes accessing your personal information, confidential data or disabling your device. Below mentioned are few category based cybercrimes.

Categories:

- Property
- Individual
- Government

Types of Cybercrimes:

- Botnets
- DDoS Attacks
- Identity Theft
- Social Engineering
- Cyberstalking
- Phishing Attacks
- Online Scams
- Illegal Content

Types of Hackers

We have different types of Ethical Hackers. Few of them are discussed below:

White Hat Hacker - These hackers are also called as ethical hackers as they perform penetration testing at organization level & identify the bugs in security. They work on various methods to ensure protection from black hat hackers & few malicious cybercrimes.

Black Hat Hacker - These hackers take negative persona of hacking. They are the culprits. The agenda of a black hat hacker is money all over the time. They look for loopholes in the network and systems. Using these loopholes, they can access the data and post virus or worms in your systems.

Grey Hat Hacker - These hackers are as a thin line between Black hat and White hat Hackers as they do not work for their personal profit. They hack into organizations and find vulnerabilities and a leak over the internet or intimate the same to the firm owners. Let me explain this. A grey hat hacker may not use his hacking expertise for personal profit and can not be defined as black hat hacker. Where as he can not hack organizations data as he is not authorised as ethical hacker.

Script Kiddies - They are the hackers who don't have much coding skills. They usually use tools or predefined codes by the developers and hackers. Their intention is to impress others or friends. They do not bother about the nature of attack and use off the shelves code for hacking. They often involve mostly in DDoS and DoS attacks.

Green Hat Hacker - These hackers are very curious to learn. We consider themselves as script kiddies, as the thin line which separates them is the desire of learning. These newbies has full desire to become one of the full-brown hackers. You can identify them within hacking communities as they engross the fellow member in the community. We can easily identify one of those by their zeal to learn the latest hacking trades.

Blue Hat Hacker - These hackers aim is to take revenge on people who make them angry. These are to be considered as script kiddies and their intention will be taking revenge with no desire to learn hacking by using simple attacks like IP overload with packets, which leads to (Dick Operating System) attacks. Blue hat hacker is considered as script kiddie, who has revenge nature.

Red Hat Hacker - These hackers are same as white hat hackers in performance and ethics. They halt black hat hackers in performing their duties. There is lot of difference in their operation. They will be ruthless when they trade with black hat hackers. They think in attacking black hat hackers and take them down completely instead of reporting. They implement a pack of attacks on black hat hackers which, in return, leads to whole system recovery.

Hacktivist - These are a group of hackers with an intention to make social changes, and they believe it strongly. They often hack govt organizations to prove that they exist and share their intentions and thoughts.

Phreaker - These hackers are mostly called as telecommunication hackers. They are very active in cloning the phone, network mimicry, blue hacking, and other forms of cellular hacks.

Stages Of Hacking

The below steps explain the different stages of hacking.

Stage 1 - Reconnaissance: It is the act of gathering information related to intelligence and preliminary data of your target to plan for attack in a better way. It can be carried out either actively or passively(Network, IP address, DNS records). Hacker will be spending his most of time in this stage.

Stage 2 - Scanning: It is a prior stage to launching the attack. At this stage we scan for open ports, services etc. The tools collectively used by the hacker during the

scanning would be port scanners, sweepers, dialers, and vulnerability scanners.

Stage 3 - Gaining Access: The blueprint of network of the targeted system will be ready from stages 1 & 2. At this stage we gain access for the targeted system by accessing one/more network devices to extract the data from target.

Stage 4 - Maintain Access: At this stage, the hacker will be in stealth mode to avoid getting caught while working in host environment. Once the hacker gains access, he lays path for future attacks and exploitations by making the target hardened. Hacker also secures the path by any other bypass accessing with rootkits, backdoors and trojans.

Stage 5 - Covering Tracks: At this stage the hacker covers his track in order to get caught & detected by cyber personnel. Removes evidence of hacking, to avoid legal actions. Hacker removes all log files, IDS(tunneling protocols, steganography, alter log files).

Platforms Used In Ethical Hacking

In the cyber world, security-focused OS is the hackers' best friend as it leads them to detect weakness in the

systems or networks. The basic tool for hacking a system for hacker is the OS. Usually, the specializations in hacking are dependent on Linux Kernel and are regarded as the advanced working systems. Below compiled are few top platforms for Ethical Hacking.

- **Kali Linux**
- **BackBox**
- **Parrot Security OS**
- **DEFT Linux**
- **Samurai Web Testing Framework**
- **Network Security Toolkit(NST)**
- **BlackArch Linux**
- **Cyborg Hawk Linux**
- **GnackTrack**
- **NodeZero**
- **Pentoo Linux**
- **Caine**
- **Bugtraq**
- **ArchStrike Linux**
- **Fedora Security Spin**

Skills required to become ethical hacker

As an Ethical Hacker, one needs to know about the various hacking techniques:

- Session Hijacking.
- SQL injection.
- Password Cracking.
- Session Spoofing.
- Denial of service attacks.

Basic Skills To Learn Ethical Hacking:

How to program?

- Hackers are tool builders and problem solvers. Learning the programming will help the hacker to solve the problems.
- It will help hacker to automate so many tasks which takes a lot of time.
- Writing programs helps in identifying program errors that he/she is targeting.
- Hacker can use predefined codes, either implementing new code or by customizing the old ones.

What Language Should an Ethical Hacker Learn?

It depends on the target system and platforms. Few programs are used to develop only specific platforms.

Useful Languages For Hackers?

Below mentioned are few languages that are useful for hackers:

Languages	Explanation	Purpose
HTML	Used to build Web Pages	Used to fetch data in HTML forms.
JavaScript	Used for Client Side Scripting	It is used to execute on client side.
PHP	Used for Server Side Scripting	To process HTML forms and customised tasks this language is used.
SQL	Used to connect with DataBase.	Used for SQL Injection, delete data, override the application login credentials.
PYTHON Perl Ruby Bash	Used as High Level Programming languages	They are used to develop automation scripts and tools.
C & C++	Used as High Level Programming languages	They are used in writing your own code to extend the existing.

Java VB VB Script C Sharp	Programming languages	Depending on the purpose, we use these languages for coding.

What is Encryption Hacking?

Encryption helps in accessing unauthorised data with emails, bank details etc, as keeping secure communication between the two parties involved. This can be done via “Scrambling” the data sent from one to other person as lengthy code by making it unreadable who ever tries to access it.

In the data encryption the receiver and the sender parties only can Decrypt the data scrambled into a readable content. This can be achieved by “Keys”, which provides access to make the data Readable and Unreadable.

How To Break Encryptions?

Today, criminals and hackers find new ways in “Cracking” encrypted documents by finding loops in encrypted algorithms. That is how they can find out the necessary key used for reading the information in the plain text.

There are other ways in earlier days where they simply test with all the possible keys provided. But, now a days, it is performed by the computers which are capable of calculating billions of keys/second, and this method is called as “Brute Force.”

How To Bypass Encryption?

In encryption, we use complicated mathematical equations for hiding the information. In general, encrypted files require a key to decrypt the data or information. But, in few cases, hacker can bypass the encryption for stealing the data. By few ways, we can encounter these techniques. The ways are stated below.

- Key Theft
- Password Security
- Hashing
- Weak Encryption

Key Theft

The perfect way to bypass encryption is to steal the key simply. If a hacker can insert a keylogger in our system, he will read all necessary activities by recording. The best way to protect ourselves by updating the anti-malware programs regularly.

Password Security

A hacker can hash common passwords and look for matches in DB. The algorithms that convert these passwords are easier to identify. For preventing these type of attacks, we need to use complex passwords that are not available in the dictionary.

Hashing

Hashing is commonly used by DB-servers, and is a cryptographic method. It is a straight cryptographic algorithm which provides unique string for each input. For example, when creating an account and password, server stores hash version of the data, and when logging in, it hashes the stored data and checks whether both of them are same or not for validation.

Weak Encryption:

In few cases, cryptographic security is also capable of securing brute force violation. Brute force violation needs to try every possible way to break into encrypted scheme and this takes a lot of time for succeeding. Probably, in many customer forms, encryptions use 128/256 bit keys.

Ethical Hacking Tools List

Few of the below-mentioned tools are effective and some of them are free of cost. These tools help in finding the loopholes of the software or computer systems or networks. Few of these are opensource as well.

Netsparker	It is a web app security scanner which automatically identifies SQL, XSS and other loops in web apps and services.
Probe.ly	It continuously scans the web apps for loops.
Acunetix	It is fully automated hacking solution which mimics ethical hacker to keep ahead of malicious attacks.
Burp Suite	It is a Security Testing tool for web apps.
Aircrack	It is used to crack wireless connections and powered by WPA 2 and WEP WPA.
Ettercap	It helps in dissection of network and host analysis of active and passives modes devices.
GFI LanGuard	It can be as a “Virtual Consultant” which scans network for vulnerabilities.
Angry IP Scanner	It is used to scan ports and IP addresses as it is a cross platform and open source tool.
QualysGuard	It helps to build security to digital transformations. It also helps in identifying cloud system vulnerabilities.
WebInspect	It is a dynamic app security testing tool.

Savvius	It identifies issues and decrease security risk along deep analysis provided through Omnipeek.
Hashcat	It is a password cracking tool for ethical hackers.
IKECrack	It is an authentication cracking tool.
SQLMap	It detects and exploits the SQL injection loopholes in the system.
Medusa	It is used to crack password. It is speedy and the best online ethical hacking tool.
NetStumbler	It is the tool to detect wireless router networks for Windows OS.
Cain and Abel	It is a password recovery tool for Microsoft OS.
RainbowCrack	It is the password hacking tool used by most of the ethical hackers.
L0phtCrack	It is the tool used to recover and audit the password for the systems.
IronWASP	It is fortware available online for free for ethical hacking and it is open source.

Top Ethical Hacking Techniques, What Are They?

Hackers use different types of techniques. The familiar ones are mentioned below.

- **Password Cracking -** Recovering passwords transmitted via computers.
- **Vulnerability Scanner -** Network checking for known weakness.
- **Spoofing Attack -** Involves false sites, to be trusted by users for data breaching.
- **Packet Sniffer -** Apps that identify data packs for data/passwords view in transit via networks.
- **Trojan Horse -** It acts as backdoor for an intruder to gain access to the system.
- **Rootkit -** It provides a set of programs to have control over OS with legitimate operators.
- **Keyloggers -** Used to record each keystroke in the machine for collecting later.
- **Viruses -** These are self-replicating executable programs by themselves into different files.

Pros and Cons Of Ethical Hacking

	Features	Explanation
Pros	Experience	Requires experience to find the loopholes and log to security sys.
	Focus on Security	Need to find loopholes in the

	Features	Explanation
		security sys and report.
	Consult To Make Improvements	Need to improvise and fight back on current threats.
	Updated Security Sys	Need to make latest updates on security systems.
Cons	Illegal Background	Chances of making damages to the security system.
	Unhappy Clients	Leads to termination if the clients are not satisfied with the hacker background.
	Absence Of Faith	Absence of faith is another factor on former hacker to deal with our security systems.
	Direct Approach To Security System	Need to have a look over the hacker who access your system as you are providing direct access to him/her.

How Ethnical Hacking is performed.

Ethical Hacking – Fingerprinting

The term OS fingerprinting in Ethical Hacking refers to any method used to determine what operating system is running on a remote computer. This could be –

- **Active Fingerprinting** – Active fingerprinting is accomplished by sending specially crafted packets to a target machine and then noting down its response and analyzing the gathered information to determine the target OS. In the following section, we have given an example to explain how you can use NMAP tool to detect the OS of a target domain.
- **Passive Fingerprinting** – Passive fingerprinting is based on sniffer traces from the remote system. Based on the sniffer traces (such as Wireshark) of the packets, you can determine the operating system of the remote host.

We have the following four important elements that we will look at to determine the operating system –

- **TTL** – What the operating system sets the **Time-To-Live** on the outbound packet.
- **Window Size** – What the operating system sets the Window Size at.
- **DF** – Does the operating system set the **Don't Fragment** bit.
- **TOS** – Does the operating system set the **Type of Service**, and if so, at what.

By analyzing these factors of a packet, you may be able to determine the remote operating system. This system is not 100% accurate, and works better for some operating systems than others.

Basic Steps

Before attacking a system, it is required that you know what operating system is hosting a website. Once a target OS is known, then it becomes easy to determine which vulnerabilities might be present to exploit the target system.

1. Whois.domaintool.com
2. Yougetsignal.com

Ethical Hacking - Sniffing

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of "tapping phone wires" and get to know about the conversation. It is also called **wiretapping** applied to the computer networks.

There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.

In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that

can be used for further attacks or to cause other issues for the network or system owner.

What can be sniffed?

One can sniff the following sensitive information from a network –

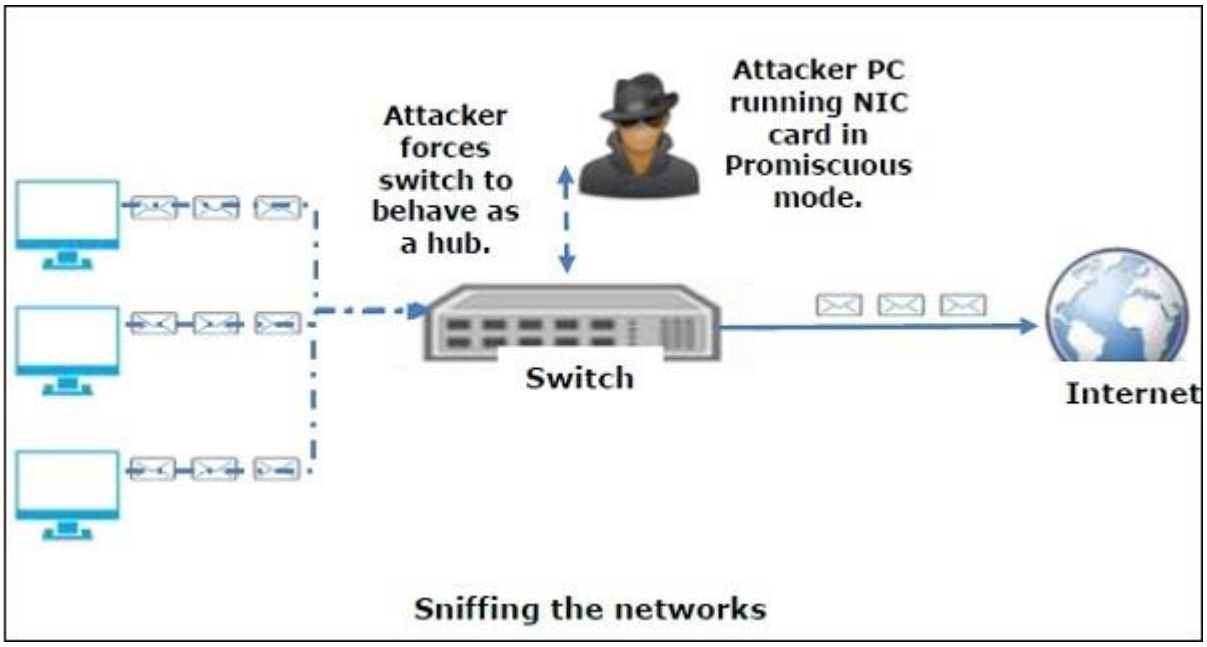
- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

How it works

A sniffer normally turns the NIC of the system to the **promiscuous mode** so that it listens to all the data transmitted on its segment.

Promiscuous mode refers to the unique way of Ethernet hardware, in particular, network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it,

which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.



A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

Types of Sniffing

Sniffing can be either Active or Passive in nature.

Passive Sniffing

In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

The good news is that hubs are almost obsolete nowadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

Active Sniffing

In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting **address resolution packets** (ARP) into a target network to flood on the switch **content addressable memory** (CAM) table. CAM keeps track of which host is connected to which port.

Following are the Active Sniffing Techniques

- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Spoofing Attacks
- ARP Poisoning

Protocols which are affected

Protocols such as the tried and true TCP/IP were never designed with security in mind and therefore do not offer much resistance to potential intruders. Several rules lend themselves to easy sniffing −

- **HTTP** − It is used to send information in the clear text without any encryption and thus a real target.
- **SMTP** (Simple Mail Transfer Protocol) − SMTP is basically utilized in the transfer of emails. This protocol is efficient, but it does not include any protection against sniffing.
- **NNTP** (Network News Transfer Protocol)− It is used for all types of communications,

but its main drawback is that data and even passwords are sent over the network as clear text.

- **POP** (Post Office Protocol) – POP is strictly used to receive emails from the servers. This protocol does not include protection against sniffing because it can be trapped.
- **FTP** (File Transfer Protocol) – FTP is used to send and receive files, but it does not offer any security features. All the data is sent as clear text that can be easily sniffed.
- **IMAP** (Internet Message Access Protocol) – IMAP is same as SMTP in its functions, but it is highly vulnerable to sniffing.
- **Telnet** – Telnet sends everything (usernames, passwords, keystrokes) over the network as clear text and hence, it can be easily sniffed.

Sniffers are not the dumb utilities that allow you to view only live traffic. If you really want to analyze each packet, save the capture and review it whenever time allows.

Hardware Protocol Analyzers

Before we go into further details of sniffers, it is important that we discuss about **hardware protocol analyzers**. These devices plug into the network at the hardware level and can monitor traffic without manipulating it.

- Hardware protocol analyzers are used to monitor and identify malicious network traffic generated by hacking software installed in the system.
- They capture a data packet, decode it, and analyze its content according to certain rules.
- Hardware protocol analyzers allow attackers to see individual data bytes of each packet passing through the cable.

These hardware devices are not readily available to most ethical hackers due to their enormous cost in many cases.

Lawful Interception

Lawful Interception (LI) is defined as legally sanctioned access to communications network data such as telephone calls or email

messages. LI must always be in pursuance of a lawful authority for the purpose of analysis or evidence. Therefore, LI is a security process in which a network operator or service provider gives law enforcement officials permission to access private communications of individuals or organizations.

Almost all countries have drafted and enacted legislation to regulate lawful interception procedures; standardization groups are creating LI technology specifications. Usually, LI activities are taken for the purpose of infrastructure protection and cyber security. However, operators of private network infrastructures can maintain LI capabilities within their own networks as an inherent right, unless otherwise prohibited.

LI was formerly known as **wiretapping** and has existed since the inception of electronic communications.

Ethical Hacking - ARP Poisoning

Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine MAC addresses. All network devices that need to communicate on the network broadcast ARP queries in the system to find out other machines' MAC addresses. ARP Poisoning is also known as **ARP Spoofing**.

Here is how ARP works –

- When one machine needs to communicate with another, it looks up its ARP table.
- If the MAC address is not found in the table, the **ARP_request** is broadcasted over the network.
- All machines on the network will compare this IP address to MAC address.
- If one of the machines in the network identifies this address, then it will respond to the **ARP_request** with its IP and MAC address.
- The requesting computer will store the address pair in its ARP table and communication will take place.

What is ARP Spoofing?

ARP packets can be forged to send data to the attacker's machine.

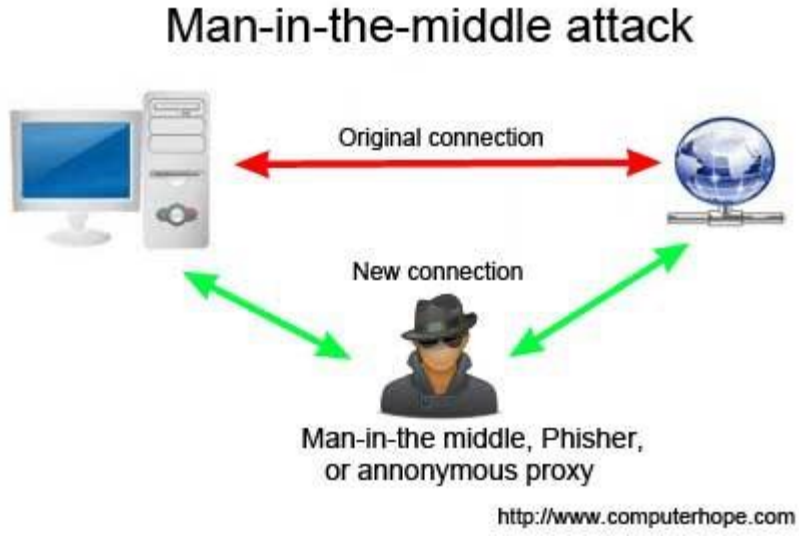
- ARP spoofing constructs a large number of forged ARP request and reply packets to overload the switch.
- The switch is set in **forwarding mode** and after the **ARP table** is flooded with spoofed ARP responses, the attackers can sniff all network packets.

Attackers flood a target computer ARP cache with forged entries, which is also known as **poisoning**. ARP poisoning uses Man-in-the-Middle access to poison the network.

What is MITM?

The Man-in-the-Middle attack (abbreviated MITM, MitM, MIM, MiM, MITMA) implies an active attack where the adversary impersonates the user by creating a connection between the victims and sends messages between them. In this case, the victims think that they are communicating

with each other, but in reality, the malicious actor controls the communication.



A third person exists to control and monitor the traffic of communication between two parties. Some protocols such as **SSL** serve to prevent this type of attack.

Ethical Hacking - DNS Poisoning

DNS Poisoning is a technique that tricks a DNS server into believing that it has received authentic information when, in reality, it has not. It results in the substitution of false IP address at the DNS level where web addresses are converted into numeric IP

addresses. It allows an attacker to replace IP address entries for a target site on a given DNS server with IP address of the server controls. An attacker can create fake DNS entries for the server which may contain malicious content with the same name.

Ethical Hacking - SQL Injection

SQL injection is a set of SQL commands that are placed in a URL string or in data structures in order to retrieve a response that we want from the databases that are connected with the web applications. This type of attacks generally takes place on webpages developed using PHP or ASP.NET.

An SQL injection attack can be done with the following intentions –

- To dump the whole database of a system,
- To modify the content of the databases, or
- To perform different queries that are not allowed by the application.

This type of attack works when the applications don’t validate the inputs properly, before passing them to an SQL

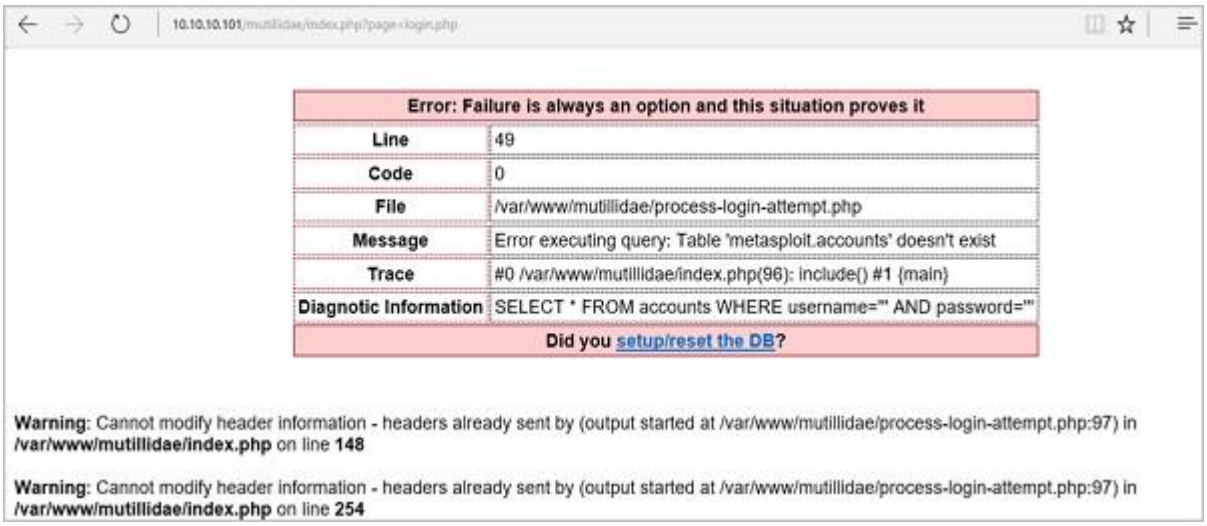
statement. Injections are normally placed put in address bars, search fields, or data fields.

The easiest way to detect if a web application is vulnerable to an SQL injection attack is to use the " ` " character in a string and see if you get any error.

Example 1

Let's try to understand this concept using a few examples. As shown in the following screenshot, we have used a " ` " character in the Name field.

Now, click the **Login** button. It should produce the following response –



It means that the "Name" field is vulnerable to SQL injection.

Example 2

We have this URL – **http://10.10.10.101/mutillidae/index.php?page=site-footer-xssdiscussion.php**

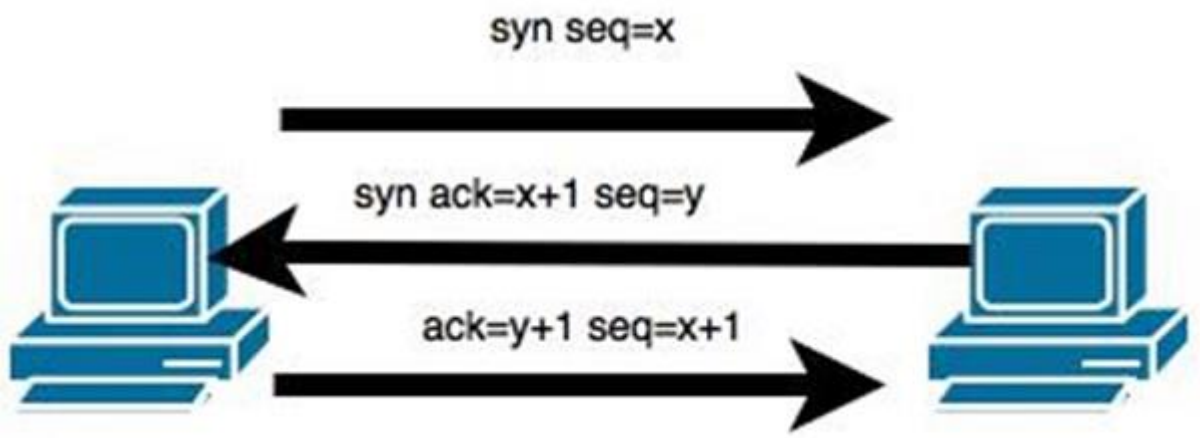
And we want to test the variable "page" but observe how we have injected a " ` " character in the string URL.

When we press Enter, it will produce the following result which is with errors.

Ethical Hacking - TCP/IP Hijacking

TCP/IP Hijacking is when an authorized user gains access to a genuine network connection of another user. It is done in order to bypass the password authentication which is normally the start of a session.

In theory, a TCP/IP connection is established as shown below –



To hijack this connection, there are two possibilities –

- Find the **seq** which is a number that increases by 1, but there is no chance to predict it.
- The second possibility is to use the Man-in-the-Middle attack which, in simple

words, is a type of **network sniffing**. For sniffing, we use tools like **Wireshark** or **Ethercap**.

Example

An attacker monitors the data transmission over a network and discovers the IP's of two devices that participate in a connection.

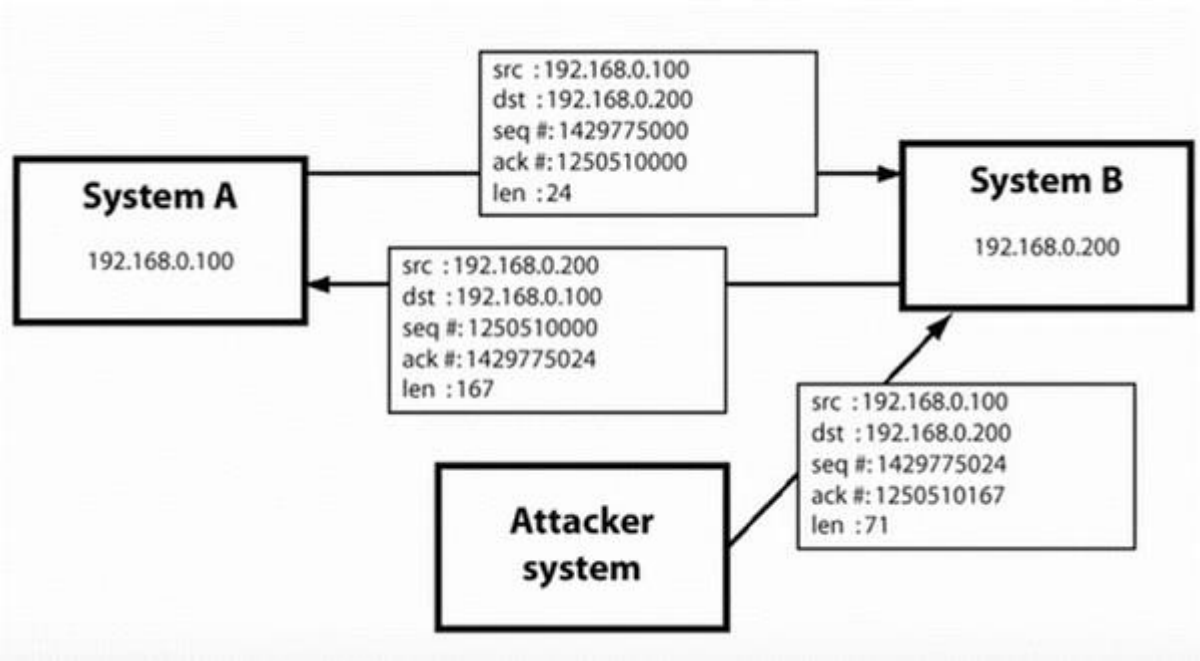
When the hacker discovers the IP of one of the users, he can put down the connection of the other user by DoS attack and then resume communication by spoofing the IP of the disconnected user.

Shijack

In practice, one of the best TCP/IP hijack tools is Shijack. It is developed using Python language and you can download it from the following link – https://packetstormsecurity.com/sniffers/shijack.tgz

Here is an example of a Shijack command –

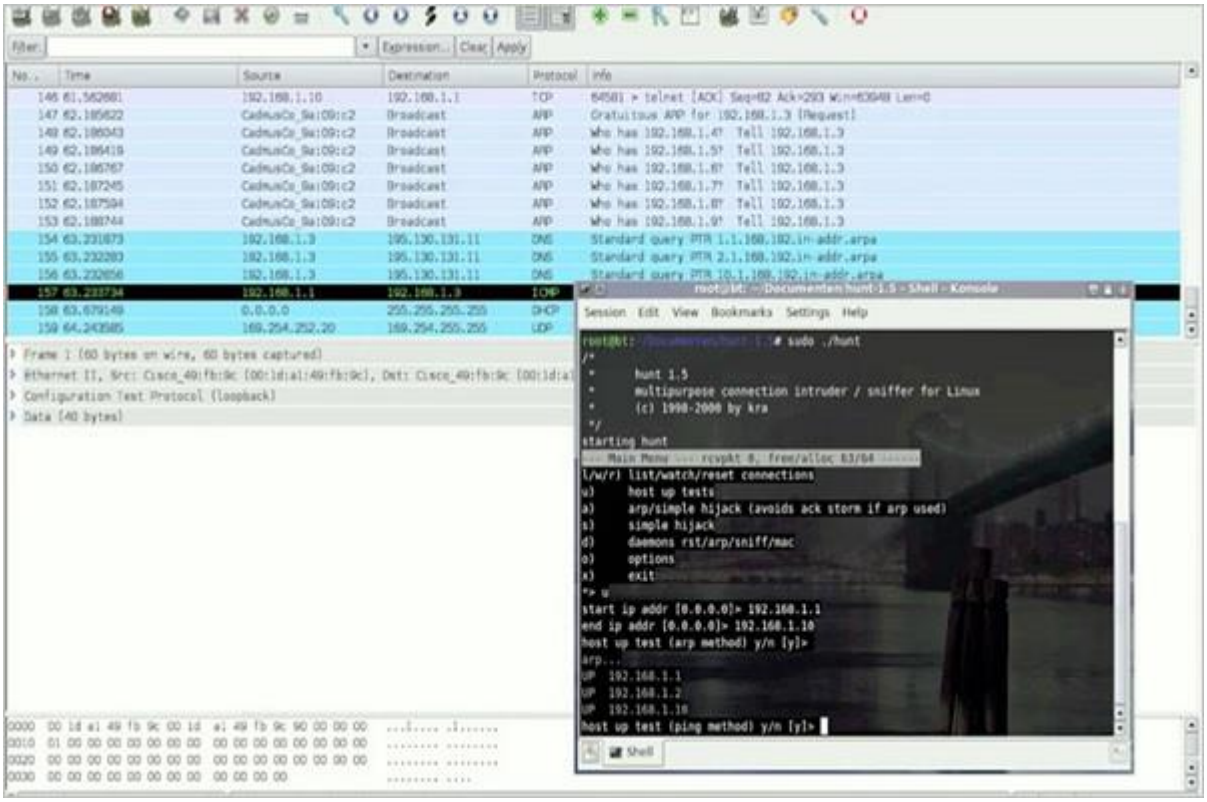
```
root:/home/root/hijack# ./shijack eth0
192.168.0.100 53517 192.168.0.200 23
```



Here, we are trying to hijack a Telnet connection between the two hosts.

Hunt

Hunt is another popular tool that you can use to hijack a TCP/IP connection. It can be downloaded from – https://packetstormsecurity.com/sniffers/hunt/



Ethical Hacking - Pen Testing

Penetration Testing is a method that many companies follow in order to minimize their security breaches. This is a controlled way of hiring a professional who will try to hack your system and show you the loopholes that you should fix.

Before doing a penetration test, it is mandatory to have an agreement that will explicitly mention the following parameters –

- what will be the time of penetration test,
- where will be the IP source of the attack, and
- what will be the penetration fields of the system.

Penetration testing is conducted by professional ethical hackers who mainly use commercial, open-source tools, automate tools and manual checks. There are no restrictions; the most important objective here is to uncover as many security flaws as possible.

Types of Penetration Testing

We have five types of penetration testing –

- **Black Box** – Here, the ethical hacker doesn't have any information regarding the infrastructure or the network of the organization that he is trying to penetrate. In black-box penetration testing, the hacker tries to find the information by his own means.
- **Grey Box** – It is a type of penetration testing where the ethical hacker has a

partial knowledge of the infrastructure, like its domain name server.

- **White Box** – In white-box penetration testing, the ethical hacker is provided with all the necessary information about the infrastructure and the network of the organization that he needs to penetrate.
- **External Penetration Testing** – This type of penetration testing mainly focuses on network infrastructure or servers and their software operating under the infrastructure. In this case, the ethical hacker tries the attack using public networks through the Internet. The hacker attempts to hack the company infrastructure by attacking their webpages, webservers, public DNS servers, etc.
- **Internal Penetration Testing** – In this type of penetration testing, the ethical hacker is inside the network of the company and conducts his tests from there.

Penetration testing can also cause problems such as system malfunctioning, system

crashing, or data loss. Therefore, a company should take calculated risks before going ahead with penetration testing. The risk is calculated as follows and it is a management risk.

RISK = Threat × Vulnerability

Example

You have an online e-commerce website that is in production. You want to do a penetration testing before making it live. Here, you have to weigh the pros and cons first. If you go ahead with penetration testing, it might cause interruption of service. On the contrary, if you do not wish to perform a penetration testing, then you can run the risk of having an unpatched vulnerability that will remain as a threat all the time.

Before doing a penetration test, it is recommended that you put down the scope of the project in writing. You should be clear about what is going to be tested. For example −

- Your company has a VPN or any other remote access techniques and you want to test that particular point.

- Your application has webservers with databases, so you might want to get it tested for SQL injection attacks which is one of the most crucial tests on a webserver. In addition, you can check if your webserver is immune to DoS attacks.

Ethical Hacking - Cross-Site Scripting

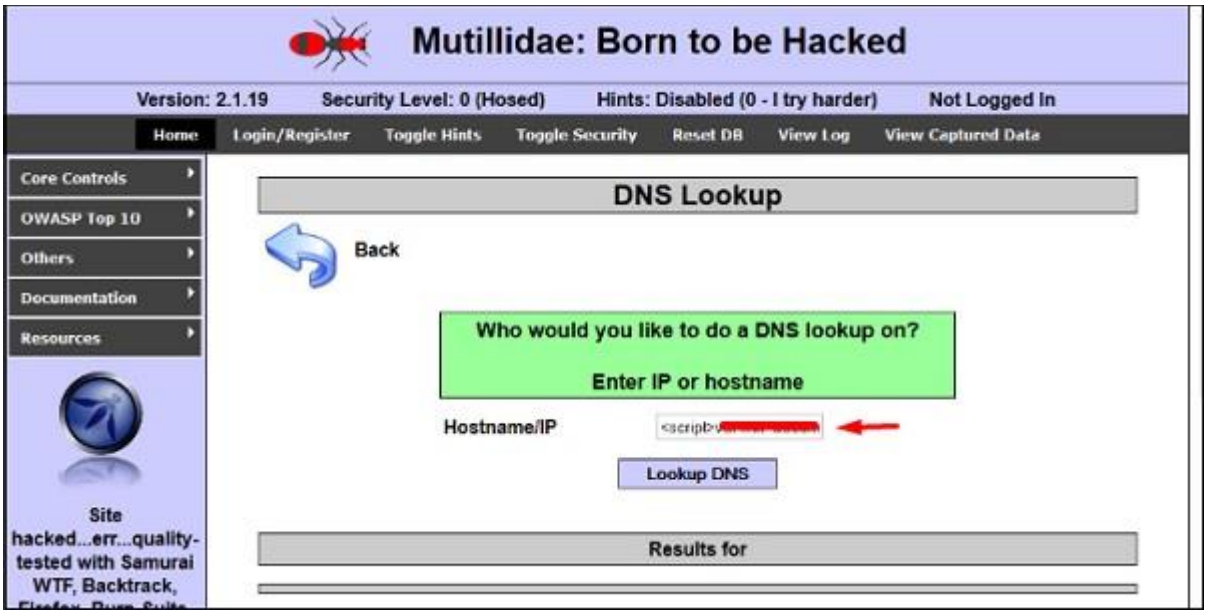
Cross-site scripting (XSS) is a code injection attack that allows an attacker to execute malicious JavaScript in another user's browser.

The attacker does not directly target his victim. Instead, he exploits a vulnerability in a website that the victim visits, in order to get the website to deliver the malicious JavaScript for him. To the victim's browser, the malicious JavaScript appears to be a legitimate part of the website, and the website has thus acted as an unintentional accomplice to the attacker. These attacks can be carried out using HTML, JavaScript, VBScript, ActiveX, Flash, but the most used XSS is malicious JavaScript.

These attacks also can gather data from account hijacking, changing of user settings, cookie theft/poisoning, or false advertising and create DoS attacks.

Example

Let’s take an example to understand how it works. We have a vulnerable webpage that we got by the **metasploitable** machine. Now we will test the field that is highlighted in red arrow for XSS.



First of all, we make a simple alert script

```
<script>
   alert(‘I am Vulnerable’)
</script>
```

It will produce the following output –

Types of XSS Attacks

XSS attacks are often divided into three types –

- **Persistent XSS,** where the malicious string originates from the website's database.
- **Reflected XSS,** where the malicious string originates from the victim's request.
- **DOM-based XSS,** where the vulnerability is in the client-side code rather than the server-side code.

Generally, cross-site scripting is found by **vulnerability scanners** so that you don't have to do all the manual job by putting a JavaScript on it like

```
<script>
   alert('XSS')
</script>
```

Burp Suite and **acunetix** are considered as the best vulnerability scanners.

Ethical Hacking - DDOS Attacks

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service or a website unavailable by overloading it with huge floods of traffic generated from multiple sources.

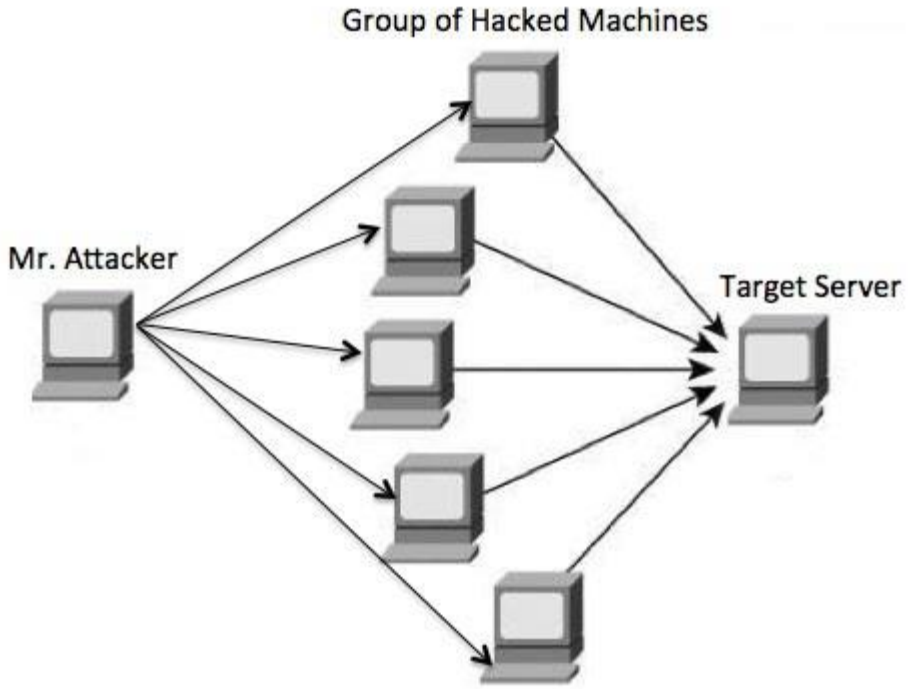
Unlike a Denial of Service (DoS) attack, in which one computer and one Internet connection is used to flood a targeted resource with packets, a DDoS attack uses many computers and many Internet

connections, often distributed globally in what is referred to as a **botnet**.

A large scale volumetric DDoS attack can generate a traffic measured in tens of Gigabits (and even hundreds of Gigabits) per second. We are sure your normal network will not be able to handle such traffic.

What are Botnets?

Attackers build a network of hacked machines which are known as **botnets**, by spreading malicious piece of code through emails, websites, and social media. Once these computers are infected, they can be controlled remotely, without their owners' knowledge, and used like an army to launch an attack against any target.



A DDoS flood can be generated in multiple ways. For example –

- Botnets can be used for sending more number of connection requests than a server can handle at a time.
- Attackers can have computers send a victim resource huge amounts of random data to use up the target's bandwidth.

Due to the distributed nature of these machines, they can be used to generate distributed high traffic which may be difficult to handle. It finally results in a complete blockage of a service.

Types of DDoS Attacks

DDoS attacks can be broadly categorized into three categories −

- **Volume-based Attacks**
- **Protocol Attacks**
- **Application Layer Attacks**

Volume-Based Attacks

Volume-based attacks include TCP floods, UDP floods, ICMP floods, and other spoofedpacket floods. These are also called **Layer 3 & 4 Attacks**. Here, an attacker tries to saturate the bandwidth of the target site. The attack magnitude is measured in **Bits per Second** (bps).

- **UDP Flood** − A UDP flood is used to flood random ports on a remote host with numerous UDP packets, more specifically port number 53. Specialized firewalls can be used to filter out or block malicious UDP packets.
- **ICMP Flood** − This is similar to UDP flood and used to flood a remote host with numerous ICMP Echo Requests. This type of attack can consume both outgoing and

incoming bandwidth and a high volume of ping requests will result in overall system slowdown.

- **HTTP Flood** – The attacker sends HTTP GET and POST requests to a targeted web server in a large volume which cannot be handled by the server and leads to denial of additional connections from legitimate clients.
- **Amplification Attack** – The attacker makes a request that generates a large response which includes DNS requests for large TXT records and HTTP GET requests for large files like images, PDFs, or any other data files.

Protocol Attacks

Protocol attacks include SYN floods, Ping of Death, fragmented packet attacks, Smurf DDoS, etc. This type of attack consumes actual server resources and other resources like firewalls and load balancers. The attack magnitude is measured in **Packets per Second**.

- **DNS Flood** – DNS floods are used for attacking both the infrastructure and a

DNS application to overwhelm a target system and consume all its available network bandwidth.

- **SYN Flood** – The attacker sends TCP connection requests faster than the targeted machine can process them, causing network saturation. Administrators can tweak TCP stacks to mitigate the effect of SYN floods. To reduce the effect of SYN floods, you can reduce the timeout until a stack frees memory allocated to a connection, or selectively dropping incoming connections using a firewall or **iptables**.
- **Ping of Death** – The attacker sends malformed or oversized packets using a simple ping command. IP allows sending 65,535 bytes packets but sending a ping packet larger than 65,535 bytes violates the Internet Protocol and could cause memory overflow on the target system and finally crash the system. To avoid Ping of Death attacks and its variants, many sites block ICMP ping messages altogether at their firewalls.

Application Layer Attacks

Application Layer Attacks include Slowloris, Zero-day DDoS attacks, DDoS attacks that target Apache, Windows or OpenBSD vulnerabilities and more. Here the goal is to crash the web server. The attack magnitude is measured in **Requests per Second**.

- **Application Attack** – This is also called **Layer 7 Attack**, where the attacker makes excessive log-in, database-lookup, or search requests to overload the application. It is really difficult to detect Layer 7 attacks because they resemble legitimate website traffic.
- **Slowloris** – The attacker sends huge number of HTTP headers to a targeted web server, but never completes a request. The targeted server keeps each of these false connections open and eventually overflows the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients.
- **NTP Amplification** – The attacker exploits publically-accessible Network

Time Protocol (NTP) servers to overwhelm the targeted server with User Datagram Protocol (UDP) traffic.

- **Zero-day DDoS Attacks** – A zero-day vulnerability is a system or application flaw previously unknown to the vendor, and has not been fixed or patched. These are new type of attacks coming into existence day by day, for example, exploiting vulnerabilities for which no patch has yet been released.

Legal Issues.

Information technology (IT) Act, 2000 is a watershed movement in Indian legal system and a landmark in the cyber law arena. If we look at the provisions of IT act cautiously, we can deduce that it covers almost all the wrongs that emerge from hacking because hacking is such offence which is very wide and covers a lot of other offenses e.g. a person who hacks the system of another person can leak the private information of the owner, it can also be used to extort money, a

black hat hacker can also use the information to enrich himself etc.

Chapter XI Section 66 of IT Act, 2000 particularly deals with the act of hacking. Section 66(1) defines a hack as, any person, dishonestly or fraudulently, does any act referred to in Section 43 is called hacking, and Section 66(2) prescribes the punishment for it. Hacking is a punishable offense in India with imprisonment up to 3 years, or with fine up to two lakh rupees, or with both.

Chapter IX Section 43 of IT act, 2000 prescribes a penalty for the damage to computer or computer system. It is a common thing which happens whenever a computer system is hacked. Black hats damage the system that they hack and steal the information. This enumerative provision includes a lot of activities.

Chapter XI Section 65 of the said act makes tampering with computer source documents an offense. Section 72 of the same chapter makes the breach of confidentiality and

privacy, a punishable offense. This is the most common aftermath of hacking.

All the above-mentioned provisions mandatorize the need of mala fide i.e intention to cause harm which is absent in ethical hacking therefore ethical hacking is not illegal in India.

Code of Ethics

1. 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.

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

3. 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.

4. 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.

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

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

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

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

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

10. 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.

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

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

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

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

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

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

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

18. Not to make inappropriate reference to the certification or misleading use of certificates, marks or logos in publications, catalogues, documents or speeches.

19. Not convicted in any felony, or violated any law of the land.