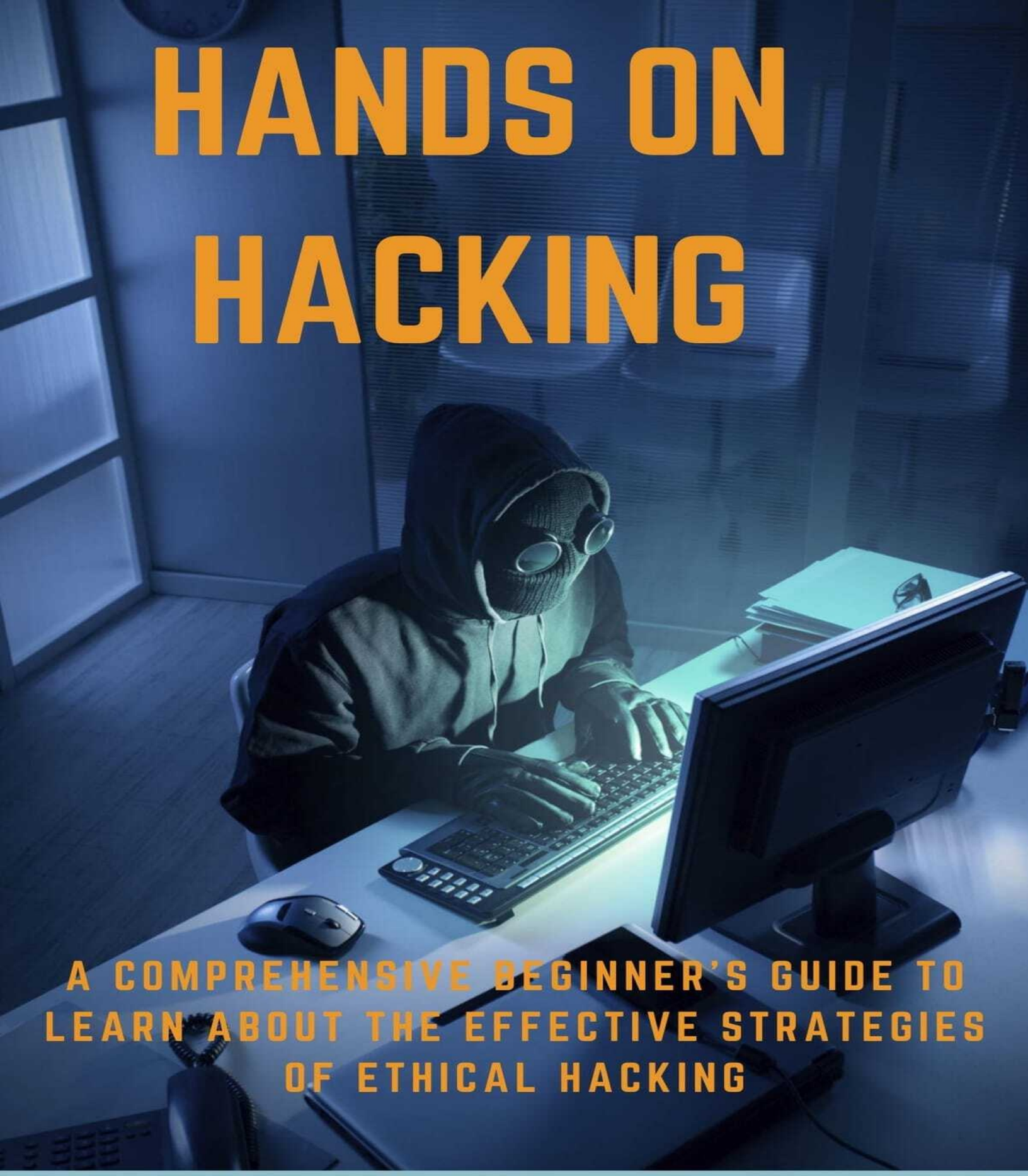
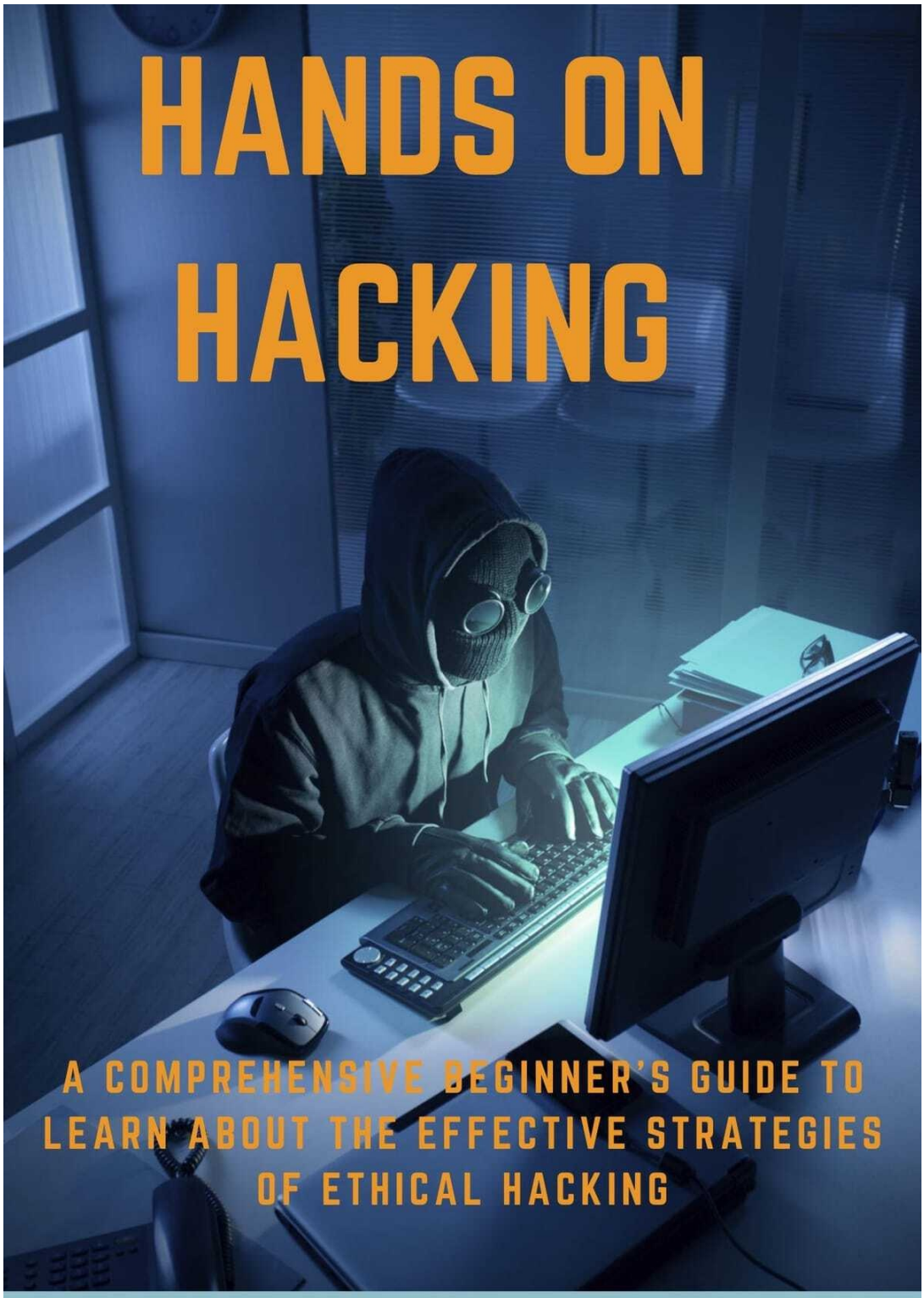
HANDS ON HACKING



A COMPREHENSIVE BEGINNER'S GUIDE TO LEARN ABOUT THE EFFECTIVE STRATEGIES OF ETHICAL HACKING

TOMMY JULIUS PH.D

HANDS ON HACKING



A COMPREHENSIVE BEGINNER'S GUIDE TO LEARN ABOUT THE EFFECTIVE STRATEGIES OF ETHICAL HACKING

TOMMY JULIUS PH.D

Contents

PRESENTATION

Most people think hackers have extraordinary skill and knowledge that allow them to hack into computer systems and find valuable information. The term hacker conjures up images of a young computer whiz who types a few commands at a computer screen—and poof! The computer spits out passwords, account numbers, or other confidential data. In reality, a good hacker, or security professional acting as an ethical hacker, just has to understand how a computer system works and know what tools to employ in order to find a security weakness. This book will teach you the same techniques and software tools that many

hackers use to gather valuable data and attack computer systems.

The realm of hackers and how they operate is unknown to most computer and security professionals. Hackers use specialized computer software tools to gain access to information. By learning the same skills and employing the software tools used by hackers, you will

be able to defend your computer networks and systems against malicious attacks. The goal of this first chapter is to introduce you to the world of the hacker and to define the terminology used in discussing computer security. To be able to defend against malicious hackers, security professionals

must first understand how to employ ethical hacking techniques. This book will detail the tools and techniques used by hackers so that you can

use those tools to identify potential risks in your systems. This book will guide you through

the hacking process as a good guy. Most ethical hackers are in the business of hacking for profit, an activity known as penetration testing, or pen testing for short. Pen testing is usually conducted by a security professional to identify security risks and vulnerabilities in systems and networks. The purpose of identifying risks and vulnerabilities is so that a countermeasure can be put in place and the risk mitigated to some degree. Ethical hackers are in the business of hacking and as such need to conduct themselves in a professional manner.

Additionally, state, country, or international laws must be understood and carefully considered prior to using hacking software and techniques. Staying within the law is a must for the ethical hacker. An ethical hacker is acting as a security professional when performing pen tests and must always act in a professional manner.

WHAT IS HACKING?

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect

themselves against such attacks.

Who is a Hacker?

A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

TYPES OF HACKER

Ethical Hacker(White hat)

A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.

Cracker (Black hat)

A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

Grey hat

A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.

Script kiddies

A non-skilled person who gains access to computer systems using already made tools.

Hacktivist

A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and

leaving the message on the hijacked website.

Phreaker

A hacker who identifies and exploits weaknesses in telephones instead of computers.

WHAT IS CYBERCRIME?

Cyber crime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using Mobile phones via SMS and online chatting applications.

Example of Cybercrime

Here, are some most commonly occurring Cybercrimes:

1. The fraud did by manipulating computer network.
2. Unauthorized access to or modification of data or application .
3. Intellectual property theft that includes software piracy .
4. Industrial spying and access to or theft of computer materials
5. Writing or spreading computer viruses or malware
6. Digitally distributing child pornography

Type of Cybercrime

The following list presents the common types of cybercrimes

1. Computer Fraud
2. Intentional deception for personal gain via the use of computer systems.
3. Privacy violation
4. Exposing personal information such as email addresses, phone number, account details, etc. on social media, websites, etc.
5. Identity Theft
6. Stealing personal information from somebody and impersonating that person.
7. Sharing copyrighted
8. files/information

9. This involves distributing copyright protected files such as eBooks and computer programs etc.
10. Electronic funds transfer
11. This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.
12. Electronic money laundering
13. This involves the use of the computer to launder money.
14. ATM Fraud
15. This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw
16. funds from the intercepted accounts.
17. Denial of Service Attacks
18. This involves the use of computers in multiple locations to attack servers with a view of shutting them down.
19. Spam
20. Sending unauthorized emails. These emails usually contain advertisements.

Cybercrime Attack Types

Cybercrime can attack in various ways. Here, is some most common cybercrime attack mode:

- **Hacking:** It is an act of gaining unauthorized access to a computer system or network.
- **Denial Of Service Attack:** In this cyberattack, the cyber-criminal uses the bandwidth of the victim's network or fills their e-mail box with spammy mail. Here, the intention is to disrupt their regular services.
- **Software Piracy:** Theft of software by illegally copying genuine programs or counterfeiting. It also includes the distribution of products intended to pass for the original.
- **Phishing:** Pishing is a technique of extracting confidential information from the bank/financial institutional account holders by illegal ways.
- **Spoofing:** It is an act of getting one computer system or a network to pretend to have the identity of another computer. It is mostly used to get access to exclusive privileges enjoyed by that network or computer.

Cyber Crime Tools

There are many types of Digital forensic tools

1. **Kali Linux:** Kali Linux is an open-source software that is maintained and funded by Offensive Security. It is a specially designed program for digital forensics and penetration testing.

2. **Ophcrack:** This tool is mainly used for cracking the hashes, which are generated by the same files of windows. It offers a secure GUI system and allows you to runs on multiple platforms.
3. **EnCase:**This software allows an investigator to image and examine data from hard disks and removable disks.
4. **SafeBack:** SafeBack is mainly using for imaging the hard disks of Intel-based computer systems and restoring these images to some other hard disks.
5. **Data dumper:** This is a command-line computer forensic tool. It is freely available for the UNIX Operating system, which can make exact copies of disks suitable for digital forensic analysis.
6. **Md5sum:** A tool to check helps you to check data is copied to another storage successfully or not.

WHAT IS ETHICAL HACKING?

Ethical Hacking sometimes called as Penetration Testing is an act of intruding/penetrating into system or networks to find out threats, vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages. The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found during testing. Ethical hackers may use the same methods and tools used by the malicious hackers but with the permission of the authorized person for the purpose of improving the security and defending the systems from attacks by malicious users. Ethical hackers are expected to report all the vulnerabilities and weakness found during the process to the management.

Why Ethical Hacking? Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization's

image and save an organization a lot of money.

Hacking can lead to loss of business for organizations that deal in finance such as PayPal. Ethical hacking puts them a step ahead of the cyber criminals who would otherwise lead to loss of business.

Method used for Ethical hacking

- **Penetration testing** In penetration testing, the hacker is given consent to adhere to a certain scope in order to discover vulnerabilities, exploit them in a controlled fashion and then document and present them to the client along with recommendations to fix the discovered issues. A non-disclosure agreement is also involved, restricting the hacker from communicating the findings or private data external parties.

- **Bug bounty hunting** In bounty hunting, the ethical hacker

adheres to the given scope and identifies previously unknown vulnerabilities, reporting them to the vulnerable party participating in the bounty hunting program. Programs like these are good for aspiring ethical hackers, as they allow you to hone your work in a practical environment. Some bug bounty programs even offer cash rewards for finding vulnerabilities.

- **Zero-day research** This involves discovering vulnerabilities that nobody has ever previously found, which are referred to as zero days. Ethical hackers are required to responsibly report these zero days; however, some malicious hackers could also obtain info on zero days and abuse them for self-gain.

- **Security research** Some ethical hackers devote their time and effort to developing tools and resources that can be used to protect systems online from malicious attackers. Such tools can be used by other ethical hackers and, unfortunately, malicious hackers as well.

TYPES OF HACKING

We can segregate hacking into different categories, based on what is being hacked. Here is a set of examples:

1. **Website Hacking:** Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
2. **Network Hacking:** Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
3. **Email Hacking:** It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.
4. **Ethical Hacking:** Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.
5. **Password Hacking:** This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.
6. **Computer Hacking:** This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Advantages of Hacking

Hacking is quite useful in the following scenarios:

- To recover lost information, especially in case you lost your password.
- To perform penetration testing to strengthen computer and network security.
- To put adequate preventative measures in place to prevent security breaches.

Ethical Hacking − Overview

To have a computer system that prevents malicious hackers from gaining access.

Disadvantages of Hacking

Hacking is quite dangerous if it is done with harmful intent. It can cause:

1. Massive security breach.
2. Unauthorized system access on private information.
3. Privacy violation.
4. Hampering system operation.
5. Denial of service attacks
6. Malicious attack on the system.

Purpose of Hacking

There could be various positive and negative intentions behind performing hacking activities. Here is a list of some probable reasons why people indulge in hacking activities:

1. Just for fun
2. Show-off
3. Steal important information
4. Damaging the system
5. Hampering privacy
6. Money extortion
7. System security testing
8. To break policy compliance

ETHICAL HACKING

Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system. These different terms come from old Spaghetti Westerns, where the bad guy wears a black cowboy hat and the good guy wears a white hat.

White Hat Hackers

White Hat hackers are also known as Ethical Hackers. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments. Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

Black Hat Hackers

Black Hat hackers, also known as crackers, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information. Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

Grey Hat Hackers

Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner’s permission or knowledge. Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

Miscellaneous Hackers

Apart from the above well-known classes of hackers, we have the following categories of hackers based on what they hack and how they do it:

Red Hat Hackers

Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

Blue Hat Hackers

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term BlueHat to represent a series of security briefing events.

Elite Hackers

This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

Script Kiddie

A script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, hence the term Kiddie.

Neophyte

A neophyte, "n00b", or "newbie" or "Green Hat Hacker" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.

Hacktivist

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denialof-service attacks.

MORE ABOUT ETHICAL HACKING

With the amount of data that is being meted out by billions of connected user devices and organizational systems, Cybersecurity has taken center stage as one of the most important focal points of any firm's IT teams. From social media giants to large enterprises, every industry has been a victim of unprecedented data breaches and ransomware attacks in the recent past. But despite most of us knowing about the importance of Cybersecurity and the deployment of safety nets to protect against threats, we know very little on the people that initiate these attacks. Behind most of these attacks are cyber-criminals or more commonly known as hackers. These are people who find ways to either infiltrate systems or modify them to make them perform actions that the creator intended them to originally perform.

These hackers are conventionally after financial rewards but sometimes or forms of malicious intent like undue political activism is just as common. The modus operandi of hackers is that they try to find loopholes in a system's security infrastructure like zero day vulnerabilities and then work towards breaking in in order to wrest control of the system from the actual administrators. In Cybersecurity domain, they are known as Black hat hackers and organizations spend millions in recruiting the best talent from the Cybersecurity field along with installing the most updated systems in order to ensure that they black hat hackers are not successful in their attempts.

But as most of them have found out, these practices do make the job harder for cybercriminals but not impossible and with a little more effort, they can go past nearly all kinds of Cybersecurity blocks. So what's the best approach to stop cybercriminals

from attacking a certain, sensitive system? There is a very old saying that the best way to stop a criminal is to think like one and the same holds true in the case of these black hat hackers. In the past couple of years, firms have become increasingly reliant on ethical hackers to protect their systems from

cybercriminals. Ethical hackers work on the same lines as cybercriminals, deploying the same tactics and tools to etch out system vulnerabilities but instead of wreaking havoc on a system like black hat hackers do, these ethical hackers make the system vulnerabilities known to system admins so that they can patch them up and close an end from where a potential attack could have been initiated. While this strategy has been unconventional, it has been incredibly effective in performing the actual job assigned to it as ethical hackers are fast becoming the biggest roadblock towards black hat hacker's pursuits in the cyber domain.

If you are working in an organization's Cybersecurity team, then you too can benefit off of this highly lucrative field, but for this you have to know more about the types of ethical hacking being offered out there:

White Hat Hackers

These are the most typical type of ethical hackers but they often don't work for firms in any official capacity. They usually go solo, working their art on different Cybersecurity systems to find out vulnerabilities before making them public so that everyone knows they exist and instantaneous remedial action can be taken system or software admins to close off these gaps once and for all. However, most firms shy away from hiring them to work for them in an official capacity because even though they might be good at their jobs, they don't have any sort of skills validation on their end to justify their credibility or trustworthiness.

Red Team Professionals

They are same as white hat hackers but they only have one major point of difference and that is, they work in an official capacity for firms to find out flaws in cyber systems and software. These professionals are often employees of the firm's own Cybersecurity teams who have extensive knowledge about hacking and they put it to use for the firm's benefit. Organizations often pit them against blue teams who are assigned the task of fixing the system's security shortcomings as soon as red teams find them out.

How Can You Become a Red Team Professional And What Are Its Benefits?

While often skills are the most basic criteria for becoming a red team professional, organizations are now changing the way they find and recruit personnel to be part of their red teams. Since this task is so sensitive, firms require validation of skills that can easily be acquire by aspiring individuals by

completing certifications related to ethical hacking. These certifications allow individuals to negotiate better salaries from organizations since they are bringing a very rare skill set that can benefit the

organization immensely. On top of this, information security certifications are also considered highly relevant for the field of ethical hacking within red teams and firms value them equally when searching for individuals to initiate acts like penetration testing in their systems. If you become a certified ethical hacker, then you can also offer your skills as a consultant, thereby diversifying your career choices and allowing you to open up an entirely different and valuable revenue stream for yourself. In the recent past, the demand for certified ethical hackers has grown significantly so it makes a lot of sense for you to enroll yourself in one. Ethical hacking certifications come with varying expertise levels ranging from beginners to advanced courses

that can allow individuals to grow their skills repertoire in the most streamlined way possible without following any unconventional strategies

PHASES OF ETHICAL HACKING PLANNING AND RECONNAISSANCE:

The first step in ethical hacking is to define the scope and goals of a test as well as the testing methods to be followed. It also addresses intelligence to understand the potential vulnerabilities and how a target works. The prospective footprinting is made through search engines, web services, social network sites, DNS, email, network, etc. by using footprinting tools.

1. **Scanning:** In the second step, scanning is performed to understand how a target reacts to various intrusion attempts, in two ways – when the application's code is static and when the application's code is functioning. The later is the most practical way to understand the application's performance in real-time.

2. **Gaining Access:** This is a crucial step where the web application is attacked using SQL injections, cross site scripting, backdoors, etc. to find the vulnerabilities and then exploit them by stealing, intercepting traffic, and interfering privileges to understand the amount of damage that it can cause.

3. **Maintaining Access:** In this step of penetration testing, the vulnerability is used as a persistent presence for a long duration in the infected system in order to steal sensitive information or to spread inside the network, quickly gaining access to the server.

4. **Analysis:** The final stage of a penetration test is to compile the result by analyzing and commenting about the vulnerabilities exploited, access to the data, and the amount of time that the tester can remain unnoticed in the system.

What are Hacking Tools?

Hacking Tools are computer programs and scripts that help you find and exploit weaknesses in computer systems, web applications, servers and networks. There are a variety of such hack tools available in the market. Some of them are open source while others are commercial solution.

Types of hacking tools

Netsparker Netsparker is an easy to use web application security scanner that can automatically find SQL Injection, XSS and other vulnerabilities in your web applications and web services. It is available as on-premises and SAAS solution. **Features** Dead accurate vulnerability detection with the unique Proof-Based Scanning Technology. Minimal configuration required. Scanner automatically detects URL rewrite rules, custom 404 error pages. REST API for seamless integration with the SDLC, bug tracking systems etc. Fully scalable solution. Scan 1,000 web applications in just 24 hours.

Acunetix Acunetix is a fully automated ethical hacking solution that mimics a hacker to keep one step ahead of malicious intruders. The web application security scanner accurately scans HTML5, JavaScript and Single-page applications. It can audit complex, authenticated webapps and issues compliance and management reports on a wide range of web and network vulnerabilities. **Features:** Scans for all variants of SQL Injection, XSS, and 4500+ additional vulnerabilities Detects over 1200 WordPress core, theme, and plugin vulnerabilities Fast & Scalable – crawls hundreds of thousands of pages without interruptions Integrates with popular WAFs and Issue Trackers to aid in the SDLC Available On Premises and as a Cloud solution.

SaferVPN SaferVPN is an indispensable tool in an Ethical hackers arsenal. You may need it to check target in different geographies, simulate nonpersonalized browsing behavior, anonymized file transfers, etc.

Features: No Log VPN with high security and anonymity Very fast speeds with 2000+ servers across continents Based in Hongkong, it does not store any data.

Split tunneling and 5 simultaneous logins 24/7 support Supports Windows, Mac, Android, Linux, iPhone, etc. 300,000+ IPs

Port Forwarding, Dedicated IO and P2P Protection

31 Day Money-Back Guarantee

Burp Suite: Burp Suite is a useful platform for performing Security Testing of web applications. Its various hacker tools work seamlessly together to support the entire pen testing process. It spans from initial mapping to analysis of an application's attack surface.

Features:

It can detect over 3000 web application vulnerabilities.

Scan open-source software and custom-built applications

An easy to use Login Sequence Recorder allows the automatic scanning

Review vulnerability data with built-in vulnerability management.

Easily provide wide variety of technical and compliance reports

Detects Critical Vulnerabilities with 100% Accuracy

Automated crawl and scan

Advanced scanning feature for manual testers

Cutting-edge scanning logic

Ettercap: Ettercap is an ethical hacking tool. It supports active and passive dissection includes features for network and host analysis.

Features:

It supports active and passive dissection of many protocols

Feature of ARP poisoning to sniff on a switched LAN between two hosts

Characters can be injected into a server or to a client while maintaining a live connection

Ettercap is capable of sniffing an SSH connection in full duplex

Allows sniffing of HTTP SSL secured data even when the connection is made using proxy

Allows creation of custom plugins using Ettercap's API

Aircrack Aircrack is one of the best, trustable, ethical hacking tool in the

market. It cracks vulnerable wireless connections. It is powered

by WEP WPA and WPA 2 encryption Keys.

Features:

More cards/drivers supported

Support all types of OS and platforms

New WEP attack: PTW

Support for WEP dictionary attack

Support for Fragmentation attack

Improved tracking speed

Angry IP Scanner: Angry IP Scanner is open-source and cross-platform ethical hacking tool. It scans IP addresses and ports.

Features:

Scans local networks as well as the Internet

Free and open-source hack tool

Random or file in any format

Exports results into many formats

Extensible with many data fetchers

Provides command-line interface

Works on Windows, Mac, and Linux

No need for Installation

GFI LanGuard: GFI LanGuard is an ethical tool that scan networks for vulnerabilities. It can acts as your 'virtual security consultant' on demand. It allows creating an asset inventory of every device.

Features:

It helps to maintain a secure network over time is to know which changes are affecting your network and

Patch management: Fix vulnerabilities before an attack

Analyze network centrally

Discover security threats early

Reduce cost of ownership by centralizing vulnerability scanning

Help to maintain a secure and compliant network

Savvius: It is an ethical hacking tool. It performance issues and reduces security risk with the deep visibility provided by Omnipeek. It can diagnose network issues faster and better with Savvius packet intelligence.

Features:

Powerful, easy-to-use network forensics software

Savvius automates the capture of the network data required to quickly investigate security alerts

Software and integrated appliance solutions

Packet intelligence combines deep analysis

Rapid resolution of network and security issues

Easy to use Intuitive workflow

Expert and responsive technical support

Onsite deployment for appliances

QualysGuard: Qualys guard helps businesses streamline their security and compliance solutions. It also builds security into their digital transformation initiatives. This tool can also check the performance vulnerability of the online cloud systems.

Features: It is trusted globally

No hardware to buy or manage

It is a scalable, end-to-end solution for all aspects of IT security

Vulnerability data securely stored and processed on an n-tiered architecture of load-balanced servers

It sensor provides continuous visibility

Data analyzed in real time

It can respond to threats in a real-time

WebInspect: WebInspect is automated dynamic application security testing that allows performing ethical hacking techniques. It provides comprehensive dynamic analysis of complex web applications and services.

Features: Allows to test dynamic behavior of running web applications to identify security vulnerabilities

Keep in control of your scan by getting relevant information and statistics at a glance

Centralized Program Management

Advanced technologies, such as simultaneous crawl professional-level testing to novice security testers

Easily inform management on vulnerability trending, compliance management, and risk oversight

Hashcat: Hashcat is a robust password cracking and ethical hackers tool. It can help users to recover lost passwords, audit password security, or just find out what data is stored in a hash.

F**eatures:** Open-Source platform

Multi-Platform Support

Allows utilizing multiple devices in the same system

Utilizing mixed device types in the same system

It supports distributed cracking networks

Supports interactive pause/resume

Supports sessions and restore

Built-in benchmarking system

Integrated thermal watchdog

Supports automatic performance tuning

L0phtCrack: L0phtCrack 6 is useful password audit and recovery tool. It identifies and assesses password vulnerability over local machines and networks.

Features: Multicore & multi-GPU support helps to optimize hardware

Easy to customize

Simple Password Loading

Schedule sophisticated tasks for automated enterprise-wide password

Fix weak passwords issues by forcing password resets or locking accounts

It allows multiple auditing OSes

Rainbow Crack: RainbowCrack RainbowCrack is a password cracking and ethical hacking tool widely used for hacking devices. It cracks hashes with rainbow tables. It uses time-memory tradeoff algorithm for this purpose.

Features: Full time-memory trade-off tool suites, including rainbow table generation

It Support rainbow table of any hash algorithm

Support rainbow table of any charset

Support rainbow table in raw file format (.rt) and compact file format

Computation on multi-core processor support

GPU acceleration with multiple GPUs

Runs on Windows OS and Linux

Unified rainbow table file format on every supported OS

Command line user interface

Graphics user interface

IKECrack: IKECrack is an open source authentication crack tool. This ethical hacking tool is designed to brute-force or dictionary attack. This tool also allows performing cryptography tasks.

Features: IKECrack is a tool that allows performing Cryptography tasks

Initiating client sends encryption options proposal, DH public key, random number, and an ID in an unencrypted packet to the

gateway/responder.

It is freely available for both personal and commercial use. Therefore, it is

perfect choice for user who wants an option for

Cryptography programs

IronWASP

IronWASP is an open source hacking software. It is web application vulnerability testing. It is designed to be customizable so that users can create their custom security scanners using it.

Features: GUI based and very easy to use

It has powerful and effective scanning engine

Supports for recording Login sequence

Reporting in both HTML and RTF formats

Checks for over 25 types of web vulnerabilities

False Positives and Negatives detection support

It supports Python and Ruby

Extensible using plug-ins or modules in Python, Ruby, C# or VB.NET

Medusa Medusa is one of the best online brute-force, speedy, parallel password crackers ethical hacking tool. This hacking toolkit is also widely used for ethical hacking.

Features: It is designed in such a way that it is speedy, massively parallel, modular, login brute-forcer

The main aim of this tool is to support as many services which allow remote authentication

Allows to perform Thread-based parallel testing and Brute-force testing

Flexible user input. It can be specified in a variety of ways

All the service module exists as an independent .mod file.

No modifications are needed to the core application to extend the supported list of services for brute-forcing

NetStumbler NetStumbler is used to detect wireless networks on the Windows platform.

Features: Verifying network configurations

Finding locations with poor coverage in a WLAN

Detecting causes of wireless interference

Detecting unauthorized ("rogue") access points

Aiming directional antennas for long-haul

SQLMap SQLMap automates the process of detecting and exploiting SQL Injection weaknesses. It is open source and cross platform. It

supports the following database engines.

MySQL

Oracle

Postgre SQL

MS SQL Server

MS Access

IBM DB2

SQLite

Firebird

Sybase and SAP MaxDB

It supports the following SQL Injection Techniques;

Boolean-based blind

Time-based blind

Error-based

UNION query

Stacked queries and out-of-band.

Cain & Abel Cain & Abel is a Microsoft Operating System passwords recovery tool. It is used to - Recover MS Access passwords

Uncover password field

Sniffing networks

Cracking encrypted passwords using dictionary attacks, brute-force, and cryptanalysis attacks.

Nessus Nessus can be used to perform;

Remote vulnerability scanner

Password dictionary attacks

Denial of service attacks.

It is closed source, cross platform and free for personal use.

Zenmap Zenmap is the official Nmap Security Scanner software. It is a multi-platform free and open source application. It is easy to use for beginners but also offers advanced features for experienced users.

Features: Interactive and graphical results viewing

It summarizes details about a single host or a complete scan in a convenient display.

It can even draw a topology map of discovered networks.

It can show the differences between two scans.

It allows administrators to track new hosts or services appearing on their networks. Or track existing services that go down

KNOWLEDGE REQUIRED TO BECOME AN ETHICAL HACKER

Now that we have a rough idea of what ethical hacking is, let's discuss what knowledge we need to have in order to become proficient ethical hackers. Before you can consider yourself an ethical hacker or apply for ethical hacking jobs, there is quite a lot that you will need to familiarize yourself with. You will need to have a good grasp of the following:

1. **Programming** You will need to understand, at the very least, how to read code, if not write code yourself. Some experts suggest that being a master coder will make you a better hacker, but there are plenty of master hackers who are not coders. However, the more you know about coding concepts, the better you'll be able to conceptualize and think through the issues surrounding certain hacking techniques and vulnerability detection.

2. **Networking** You really ought to understand the basics of networking and how routing and switching is done. A firm grasp of the OSI layer is a must. You want to be able to understand how networks and network devices behave. Why? Imagine you are being hired to break into a well-defended bank or government building. It wouldn't do for you to avoid learning about the building's network of hallways, ventilation systems and door lock systems prior to trying to break in!

3. **Databases** Most systems have databases underlying them, which is where information is stored. You will want to be able to know how to make queries for when you will find yourself with database access as you hack ethically. Again, it's important to understand the nuts and bolts of every type of system that you will be paid to try to break into.

4. **Operating systems** As you hack ethically, you will stumble on Windows, Linux and Mac OSes. You might also be tasked with conducting tests on mobile operating systems as well. You will thus need to be comfortable with flexing your hacking muscles around many

different types of OSes.

You should also understand that persistence and passion contribute a great deal to becoming a great ethical hacker. Some situations require that you chain different vulnerabilities together to achieve a successful exploit or exercise patience to obtain results, e.g., during brute-forcing.

BENEFITS OF ETHICAL HACKING

The sudden rise in the demand for ethical hacking that is being noticed is a result of technological advances that lead to many threats in the technology sphere in the world. An ethical hacker serves as an organization by protecting their system and its information from illegal hackers as cyber-attacks and cyber terrorism is greatly growing. Understanding and getting accustomed to ethical hacking comprises of delving into the psyche and techniques of the hackers and thus learning how to penetrate into the systems through identifying and evaluating vulnerabilities in the software and computer networks. Pursuing ethical hacking can add immense value to an organization, if practiced and exercised efficiently and correctly.

Organizations under cyber-attack

Banks are easily susceptible to cyber threats as they are heavily and constantly targeted by hackers. Banks spend a large amount, in billions worldwide to safeguard themselves against such attacks and heighten digital security. Security is a valued requirement in today's times due to the amount of data hacks and information breaches happening every day around the world. In order to catch a hacker, one needs to have the mentality of a hacker, which is the fundamental of ethical hacking. Ethical hackers almost always work with the organization's consent to protect their computer and network systems.

UNRAVELING THE HACKER MINDSET

The first and foremost benefit of ethical hacking is its capability to upgrade a corporate organization's network and thoroughly defend it from threats in cyberspace. The prime threat to network security is always a hacker. Therefore, it is important to gauge how hackers work and operate. It is never possible to completely eliminate all threats from a system, therefore one must put themselves in the hacker's shoes to be able to execute their work as a hacker.

Development and Quality Assurance

More focus needs to be placed on security testing as it is often ignored, which leaves the software very vulnerable to attacks and threats. An ethical hacker who is trained well can provide a major impetus to a team by helping them to conduct security testing efficiently and successfully as opposed to relying on house practices that require more time and energy. The concept of hacking has led to the development of certain tools to eradicate prominent and common vulnerabilities. This makes it easier for the developer to learn coding errors which can be steered clear of.

Professional Development

There is a major gap between the requirement for workers with cybersecurity skills and the amount of untapped talent which is humongous. An approximate of 350,000 jobs in the field of cybersecurity is vacant in the United States, which is further expected to increase tenfold by 2021. Although this may not be exciting to hear for companies who want to retain their hackers and cyber security talent within their companies, it serves as a promising opportunity for potential hackers and people interested in this specific field. Studying ethical hacking can provide ways to breakthrough into the field of cyber security and reap its benefits.

Transition to Cloud

Cloud technology is gaining momentum in the information technology world in which virtualization and IT outsourcing play a crucial role. This passage has given rise to threats and increased the intensity of these threats, which justifies the demand of ethical hackers. Cloud computing often witnesses a lot of security breaches and is responsible for many data leaks and hacks.

This is a major concern for individuals as well as organizations.

Cyber Security Training Ethical hackers should be employed to keep this growing concern in check as well as to enjoy the benefits of cloud without

letting it negatively impacting the systems and its security. Businesses are perpetually required to stay updated with the trends and hence amp up their security networks to keep up with the cyber universe.

Employment With the amount of competition vying for jobs, any advantage or edge that sets you apart from others is valued as it demonstrates competency and could help you get the job. This is mostly highlighted in entry-level positions where employers and organizations do not focus so much on practical experience, but instead lookout for special skills to set the candidate apart. A very promising way to enter the cybersecurity field is to gather certifications regarding the same. One of the most prestige cybersecurity certification is the Certified Ethical Hacker offered by the EC-Council. If this certification is pursued by an applicant, it showcases his eagerness regarding the subject and going through the exam successfully proves the applicant’s ability and skill for the desired role.

WHY HIRE AN ETHICAL HACKER?

1. To construct a computer system that prevents systems from hackers and malicious threats and at the same time protects them.
2. To take precautionary measures in order to ward off safety breaches.
3. To defend customer data and information present in business exchanges.
4. To build and facilitate security awareness at all hierarchies in an organization.
5. Network defenders and risk management experts can easily understand and gauge the hacker's mindset which is beneficial for determining and examining possible potential threats incorporate network systems.
6. Security testing procedures and processes can be enhanced and improved with the help of penetration testing tools and practices to implement them. For better protection of data, employees can undergo ethical hacking training to further build the network defense.

Advantages of Ethical Hacking

Most of the benefits of ethical hacking are obvious, but many are overlooked. The benefits range from simply preventing malicious hacking to preventing national security breaches. The benefits include:

- Fighting against terrorism and national security breaches
- Having a computer system that prevents malicious hackers from gaining access
- Having adequate preventative measures in place to prevent security breaches

Disadvantages of Ethical Hacking

As with all types of activities which have a darker side, there will be…..dishonest people presenting drawbacks. The possible drawbacks of ethical hacking include:

- The ethical hacker using the knowledge they gain to do malicious hacking activities
- Allowing the company's financial and banking details to be seen
- The possibility that the ethical hacker will send and/or place malicious code, viruses, malware and other destructive and harmful things on a computer system Massive security breach

CONCLUSION

Computers have become mandatory to run a successful businesses. It is not enough to have isolated computers systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks. Before we go any further, let’s look at some of the most commonly used terminologies in the world of hacking. A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security. Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent. Cyber crime is the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using Mobile phones via SMS and online chatting applications.