1 Introduction to Computer Crimes and Ethical Hacking

LEARNING OBJECTIVES

After reading this chapter, you will be able to:

- Understand the concept of 'cybercrime' and its effect on the digital world.
- Interpret and apply security mechanisms on various cybercrimes.
- Identify the different types of cybercrimes.
- Explore practical knowledge about ethical hacking methodology.
- Understand the concept of hacking and its effect on digital world.
- Understand the process of ethical hacking.
- Interpret and apply security mechanism to secure system.
- Distinguish different categories of hacking.

The first faults are theirs that commit them; the second faults are theirs that permit them.

— Thomas Fuller

1.1 Introduction to Cybercrime

Crimes in India, using computers as the tool, have been on the rise. With the increasing trend of crimes using computers, tools are being built to prevent such crimes from happening. In today's world, Internet has become an integral part of our everyday life. Everyday, hackers or criminals attack our computers to sniff into our personal data or other confidential data.

The term *cybercrime* refers to crimes committed using computer (Figure 1.1). Traditionally, cybercrime refers to the crime involving computer and computer network.

According to the law enforcement agency, internet-related crimes can be categorized as:

1. **Advanced cybercrime/high-tech crime:** Attacks against computer hardware and software;
2. **Cyber-enabled crime:** Numerous 'traditional' crimes have taken a new turn with the arrival of internet, such as crimes against youngsters, monetary crimes, and even acts of terrorism.

Cybercrimes have an adverse effect on governments, businesses, and even ordinary people. For example, Botnet is a network of internet-connected computers that are infected by viruses and controlled as a group.

Scanned by CamScanner

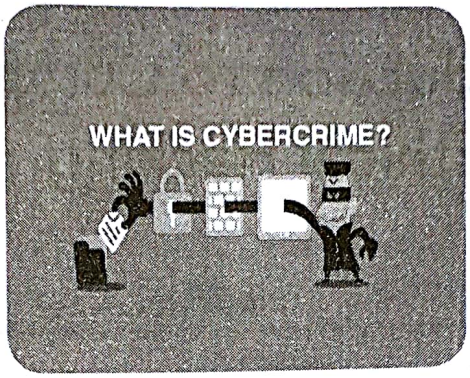


Figure 1.1 Cybercrime.

If an individual wants to prevent a cybercrime, he/she has to adopt digital forensic tools to reduce the vulnerability score. To protect our confidential data or any kind of personal data, the hard drive should be cleansed using a solution. As the crimes related to computer are increasing day by day, tools required to fight against the same are being developed faster.

1.2 Categories of Cybercrimes

Cybercrimes can be broadly divided into three major categories (Figure 1.2).

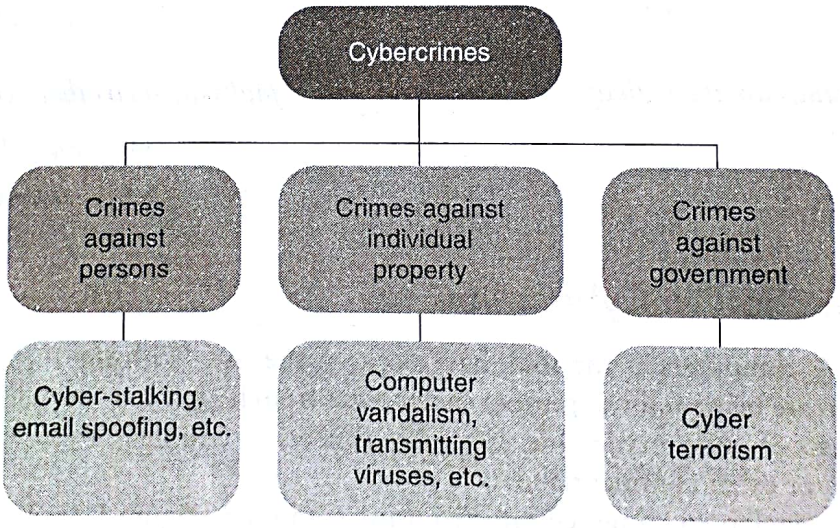


Figure 1.2 Categories of cybercrime.

1.2.1 Cybercrimes Against People

Cybercrimes committed against people include crimes such as cyber porn, transmission of child pornography, harassment of an individual through email, false legal agreement scams, etc. The trafficking, distribution, posting, and dissemination of obscene material, together with pornography and misdemeanour, constitute important cybercrimes committed against people. The potential impact of such a criminal offense to humanity can hardly be explained. Cyber harassment could be a distinct cybercrime. Various harassments can and do occur in internet, or through the use of internet. This includes sexual, racial, religious, or other harassments. People perpetuating such harassments are guilty of cybercrimes.

Scanned by CamScanner

1.2.2 Cybercrimes Against Property

Cybercrime against all forms of property is the second category of cybercrime. Crimes in this category include computer devilry, meaning destruction of others property and transmission of harmful viruses, worms, or programs. An Indian-based upstart engineering company lost its money and repute when the rival company, an associate degree business major, scarfed the technical catalogue from their computers with the assistance of a company cyber spy software.

1.2.3 Cybercrimes Against Government

Cybercrimes against Government is the third type of cybercrime. Cyber terrorism is a distinct crime in this category. The spread of internet has shown that this medium is used by people and teams to threaten the international governments conjointly to terrorize the voters of a rustic. This crime manifests itself into an act of terrorism once a private 'cracks' into a government or military maintained website.

1.3 Types of Cybercrimes

Cybercrimes can be broadly divided as:

1. **Violent or potentially violent cybercrimes:** Violent or potentially violent cybercrimes are those that pose a physical risk to some character or people. They can be further categorized as:
   (a) Cyber terrorism
   (b) Cyber talking
   (c) Assaults by threat
   (d) Child pornography
2. **Non-violent cybercrimes:** Non-violent cybercrimes are those that do not directly pose a physical risk to some character or persons, but indirectly they do pose a risk. They can be categorized further as:
   (a) Cyber theft
   (b) Cyber trespass
   (c) Cyber fraud
   (d) Destructive cybercrimes

In this section, we will discuss hacking, Dos attack, Trojan attack, credit card frauds, cyber pornography, online betting, software piracy, email spoofing, forgery, phishing, cyber terrorism, Salami attacks, defamation, and cyber stalking.

1.3.1 Hacking

Do not hack, but when you do, it should be ethical!

Eric Raymond, compiler of *The New Hacker's Dictionary*, defines a hacker as an artless coder. A 'good hack' may be a clever answer to a programming difficulty and 'hacking' (Figure 1.3) is the act of doing it.

According to Raymond, the following five likely characteristics qualify one as a hacker:

1. An individual who enjoys learning details of a programming language or system.
2. An individual who enjoys truly doing the programming instead of simply theorizing it.
3. An individual capable of appreciating somebody else's hacking.
4. An individual who picks up programming quickly.
5. An individual who is a professional in a specific programming language or system.

Scanned by CamScanner

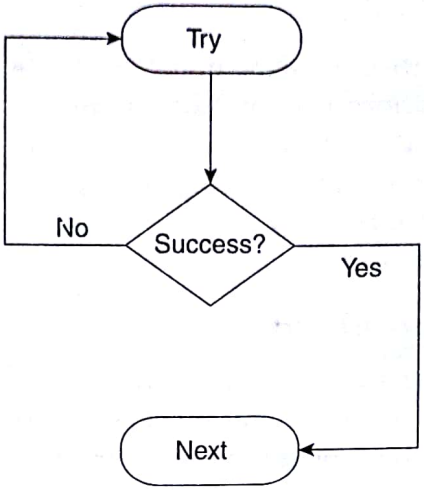


Figure 1.3 Hacking.

1.3.2 Denial-of-Service Attacks (DoS Attacks)

A Denial-of-Service (DoS) attack is a trial to make an online service unavailable by overloading the network traffic from multiple sources. DoS targets a large variety of resources (Figure 1.4).

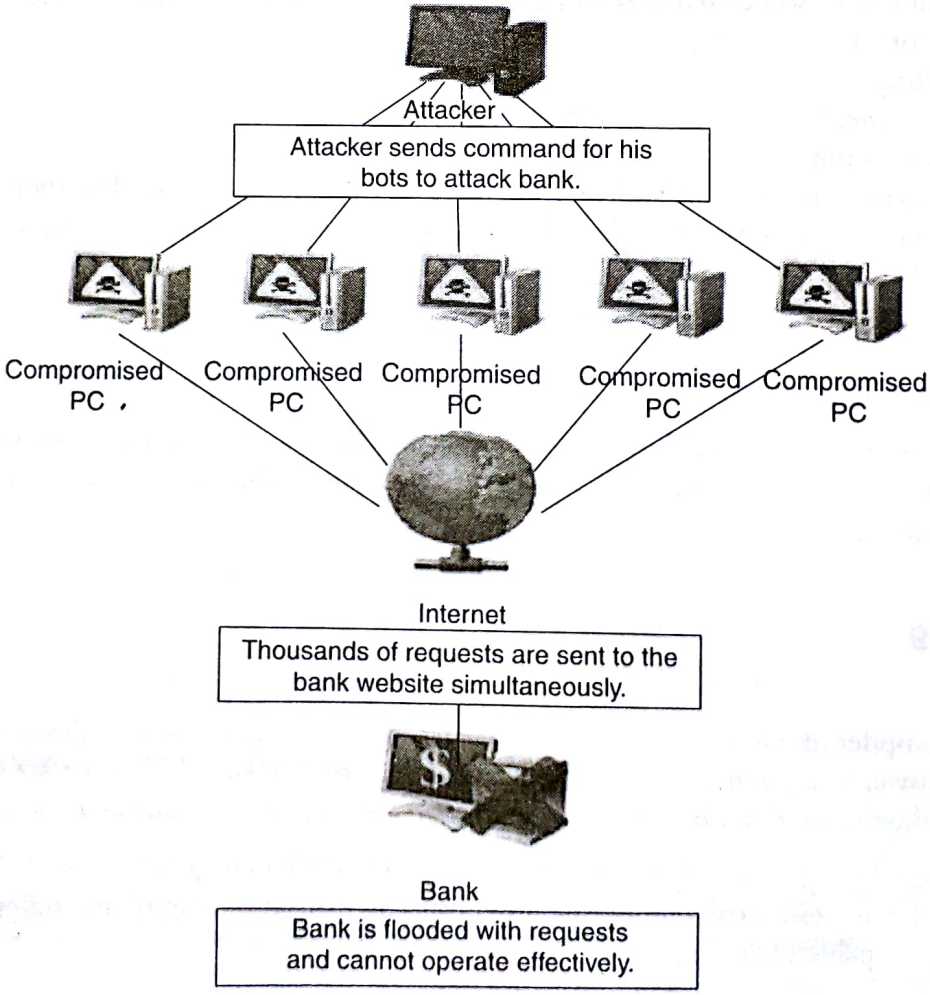


Figure 1.4 Denial-of-service attack.

Scanned by CamScanner

1.3.3 Trojan Attacks

Trojans are small particles of malware that allow the hacker to either gain or obtain remote access to any computer. Trojans can neither self-replicate nor automate as they interact with the hacker to meet and fulfill his/her purpose (Figure 1.5).

Trojans need to be installed from an executable file (.exe) or a compiler. Sometimes, Trojans exploit the bugs in the browser, media player, etc. Once the Trojan is installed, the hacker can use them to access all the sensitive or confidential and personal information or data.

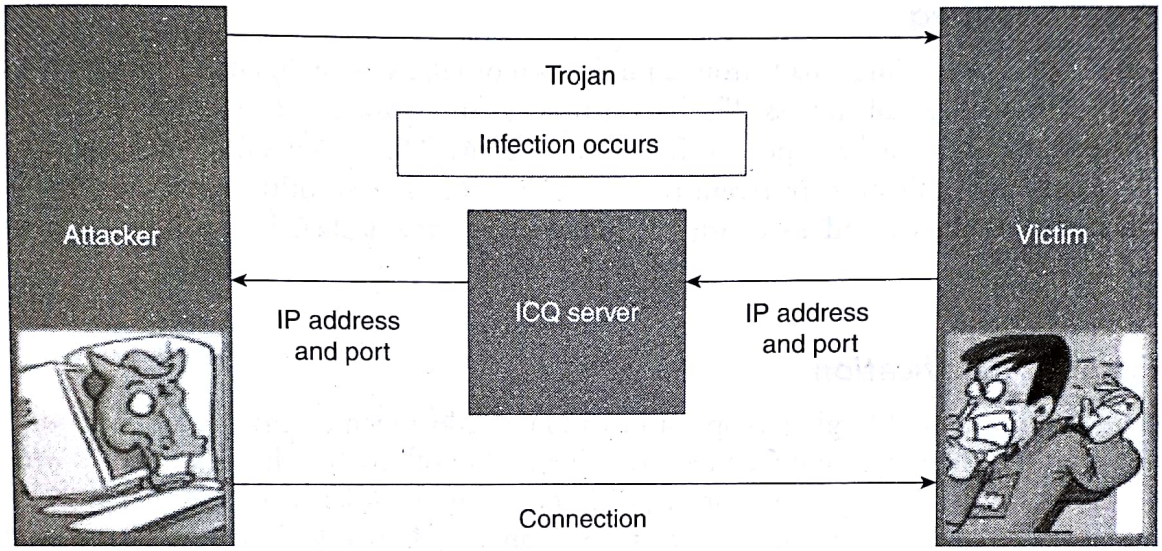


Figure 1.5 Trojan.

1.3.4 Credit Card Frauds

Credit card frauds usually occur when an individual discloses his/her confidential data such as credit card number, CVV number, secret code for transaction, expiry date, etc., to an unknown person, who could be a potential hacker. This is often the case when a card is stolen or lost or when mails are diverted from the actual recipient to the hacker. This kind of fraud is an identity fraud in which a hacker takes the necessary information about the credit card for his/her personal purpose.

1.3.5 Cyber Pornography

Cyber pornography refers to distributing pornography over the internet. People create and distribute porn or obscene materials over the internet. It includes children involved in sexual acts with adults. It is a criminal offense and is classified as causing harm to humans. It refers to Section 67 of IT Act, which is the most serious Indian Law. The other laws that deal with pornography are Indecent Representation of Women Act and the Indian Penal Code. It is a serious crime in India, but not considered so in many other countries such as United States of America (USA).

1.3.6 Online Betting

Online betting is also called online gambling or internet gambling and takes place over the internet. Online gambling is the basic term used for gambling over the internet. Many websites available over the internet are used for gambling.

Scanned by CamScanner

1.3.3 Trojan Attacks

Trojans are small particles of malware that allow the hacker to either gain or obtain remote access to any computer. Trojans can neither self-replicate nor automate as they interact with the hacker to meet and fulfill his/her purpose (Figure 1.5).

Trojans need to be installed from an executable file (.exe) or a compiler. Sometimes, Trojans exploit the bugs in the browser, media player, etc. Once the Trojan is installed, the hacker can use them to access all the sensitive or confidential and personal information or data.

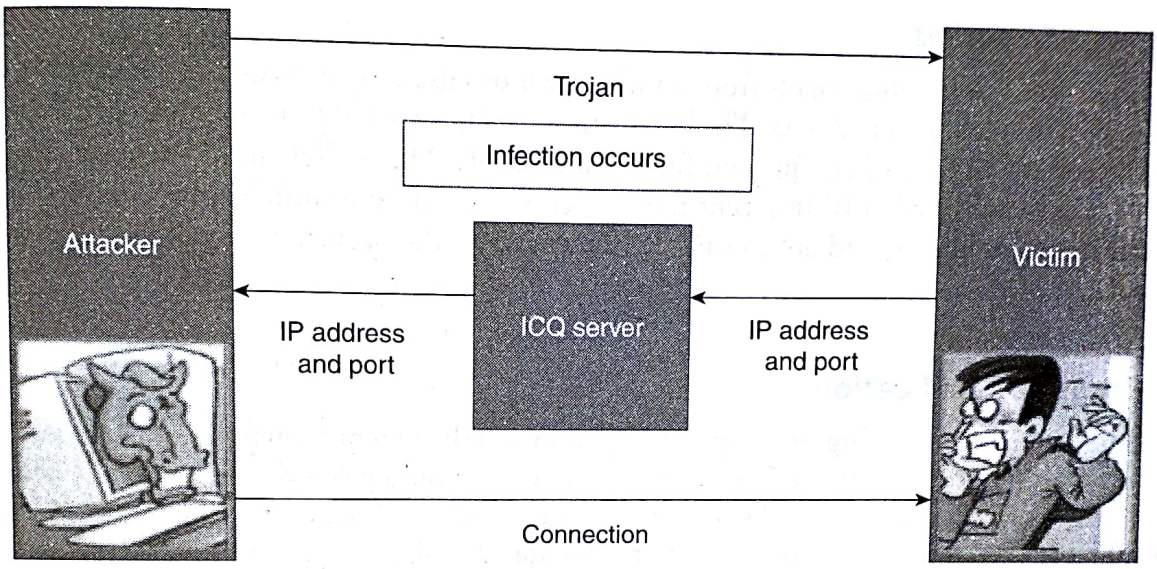


Figure 1.5 Trojan.

1.3.4 Credit Card Frauds

Credit card frauds usually occur when an individual discloses his/her confidential data such as credit card number, CVV number, secret code for transaction, expiry date, etc., to an unknown person, who could be a potential hacker. This is often the case when a card is stolen or lost or when mails are diverted from the actual recipient to the hacker. This kind of fraud is an identity fraud in which a hacker takes the necessary information about the credit card for his/her personal purpose.

1.3.5 Cyber Pornography

Cyber pornography refers to distributing pornography over the internet. People create and distribute porn or obscene materials over the internet. It includes children involved in sexual acts with adults. It is a criminal offense and is classified as causing harm to humans. It refers to Section 67 of IT Act, which is the most serious Indian Law. The other laws that deal with pornography are Indecent Representation of Women Act and the Indian Penal Code. It is a serious crime in India, but not considered so in many other countries such as United States of America (USA).

1.3.6 Online Betting

Online betting is also called online gambling or internet gambling and takes place over the internet. Online gambling is the basic term used for gambling over the internet. Many websites available over the internet are used for gambling.

Scanned by CamScanner

1.3.7 Software Piracy

Software piracy refers to the act of distributing licensed or paid or copyrighted software for free or at a minimal cost over the internet. It is considered to be the most profitable business. According to the Business Software Alliance (BSA), approximately 39% of the total softwares that are currently being used across the globe are stolen or pirated. What it means is the unauthorized copying of software and retailing it over the internet for free or at lower cost. The percentage of software piracy grew to 39% in the recent survey carried out in May, 2015.

1.3.8 Email Spoofing

Email spoofing refers to sending emails from an unknown or false source. Spoofing means that the hacker sends an email from your email address. The hacker tries to send spam emails or emails that include attractive offers, which the individual accepts and fills certain details. The hacker simultaneously receives all the necessary email ids and passwords. In recent times, even viruses are transmitted over emails. These viruses reside in our device or emails, and are constantly monitored by the hacker. This will be discussed in detail in Chapter 12.

1.3.9 Forgery/Falsification

Forgery refers to the action of forging a copy or imitation of a document, signature, or banknote. It is done to earn a huge profit by selling the forged resource. Forgery is nothing but the creation of a wrong written document or alteration of an original document with the intention of defraud or deception. Forgery comes under criminal law, with the penal code as Forgery (Section 463, 465, 466, 468, 469, 471, 474, 476, 477A IPC). Forgery is a serious crime that harms any human for his/her personal benefit.

1.3.10 Phishing

Phishing is a fraud type wherein the hacker tries to get personal information, including login credentials or any bank account information, by pretending to be a genuine entity in email, messages, or other communication channels. In this type of crime, the victim receives a fake email from a company or organization or a genuine source. These emails generally include an attachment or an outbound link that installs harmful malware or virus on the victim's device or may redirect the victim to a harmful or malicious website, developed to cheat the victim and get the personal and other financial details or information such as username, email-ids, passwords, credit card or debit card details, etc. Phishing is an attempt to obtain sensitive information from the user or victim.

1.3.11 Cyber Terrorism

Cyber terrorism is a planned activity in the cyber space via computer networks. It includes the use of email as a communication medium. The term 'cyber terrorism' is a controversial term that includes actions of deliberateness, disruption of networks over a large-scale, especially personal desktops or devices which are attached to the internet by using tools such as viruses or malware. Examples of cyber terrorism include hacking of medical database, which involves changing or deleting the facts, leading to a wrong treatment.

1.3.12 Salami Attacks

Salami attack is a combination of many small attacks that can go undetected due to the nature of cybercrime. It is also known as **salami slicing** or **penny shaving**, where the attacker uses an online database to seize the customer information such as bank/credit card details, deducts minuscule amounts from every account over a period of time.

Scanned by CamScanner

These amounts, unnoticeably taken from collective accounts, add up to a large amount of money. Most people fail to report such deductions, often letting it go because of the amount involved, which could be a fraction of a cent, so as to avoid suspicion from the unsuspecting customer. A salami attack is a small attack that can be repeated many times efficiently. Thus, the overall impact of the attack is huge. For example, stealing the round-off amounts from the interest in bank accounts. Even though it is less than 1 cent per account, when multiplied by millions of accounts over many months, the adversary can retrieve quite a large amount. It is also less likely to be noticeable since your average customer would assume that the amount was rounded down to the nearest cent.

1.3.13 *Defamation*

Internet is an integral part of our life. It acts as a medium for interacting with people across the globe. Defamation implies causing harm to a reputed individual in front of others. Harm can be inflicted by oral words, visuals, or any other means. Cyber defamation is a new concept, and it involves defamation of a person or individual by a new or virtual medium. Cyber defamation is considered to be a cybercrime. Cyber defamation not only affects the welfare of the community, but also the victim.

1.3.14 *Cyber Stalking*

Cyber stalking refers to the use of an electronic medium to threaten someone or an individual or a group of people or certain organization. This may include wrong allegations, threatening calls or messages or emails, wrong accusations, any kind of defamation, wrong identity theft, and many more. Cyber stalking is a criminal offense under various harassment laws. It is a kind of online stalking. Cyber stalkers could be strangers, people who you may know, people who know you, ex-business partners, enemies, and many more.

1.4 The Internet Spawns Crime

The internet is a network of communication and content services that is globally accessible. As internet provides a lot of options for buying and selling, crimes are on the rise in this environment. A computer represents a tool of crime as in murder or fraud, the object of crime as in stealing of processor chips, or the theme of crime as in hacking and spreading viruses. The involvement of computers on criminal rule has been much ampler than the narrow field of activities such as hacking and spreading viruses, both not easy for traditional criminal concepts, and facilitating particular types of crimes such as child pornography.

Criminal commandment is not just about whether a particular work should be considered criminal or not. It is a law enforcement that investigates those that carry out criminal acts and prosecutes them; it is a procedure more significantly difficult in a computer environment. The implementation of internet technologies is not uniform, particularly between developed and developing nations. Wireless communication technologies have quickly eclipsed wire systems in many developing countries, where the inheritance communication was greatly underdeveloped. Differential technological use may mean dissimilar patterns of threats and vulnerabilities in terms of cybercrimes.

1.5 Worms Versus Viruses

Worms and viruses are malicious programs that can cause harm to our system. However, both these terms are very different.

Scanned by CamScanner

1.5.1 Viruses

A virus (vital information resources under siege) is a software that is designed to duplicate itself. This is done by replicating itself into various programs that are stored in the computer. Computer viruses attach themselves to a program or a file, spreading from one workstation to another, leaving infections as it travels. A computer virus can range in harshness, some may cause slightly irritating effects while others can damage hardware, software, or files. Almost all viruses are fond of an executable file, which means a virus cannot affect our computer unless and until we run or release the malicious program. It is significant to make a note that a virus cannot spread without human action, such as running the infected program (Figure 1.6).

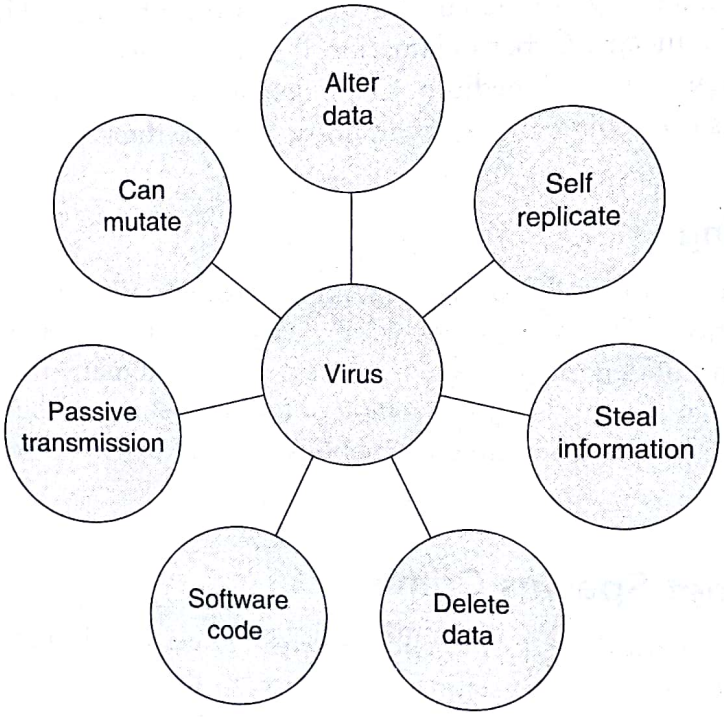


Figure 1.6 Virus.

1.5.2 Worms

A worm (write once read many) is similar to a computer virus by design. It is considered to be a secondary category of virus. A worm spreads from computer to computer, but unlike virus it has the capability to travel without any human action. The main threat with a worm is the capability to replicate itself on our system. So rather than our computer sending a single worm, it could send hundreds or thousands of copies of itself and cause a huge devastating effect. For example, a worm sending out a copy of itself to everyone listed in the address book, then the worm replicates itself to each of the receiver's address book and it manifests itself. Since the worm copies itself and also travels across networks, it consumes more system memory and network bandwidth, causing web servers and individual computers to stop responding (Figure 1.7).

Scanned by CamScanner

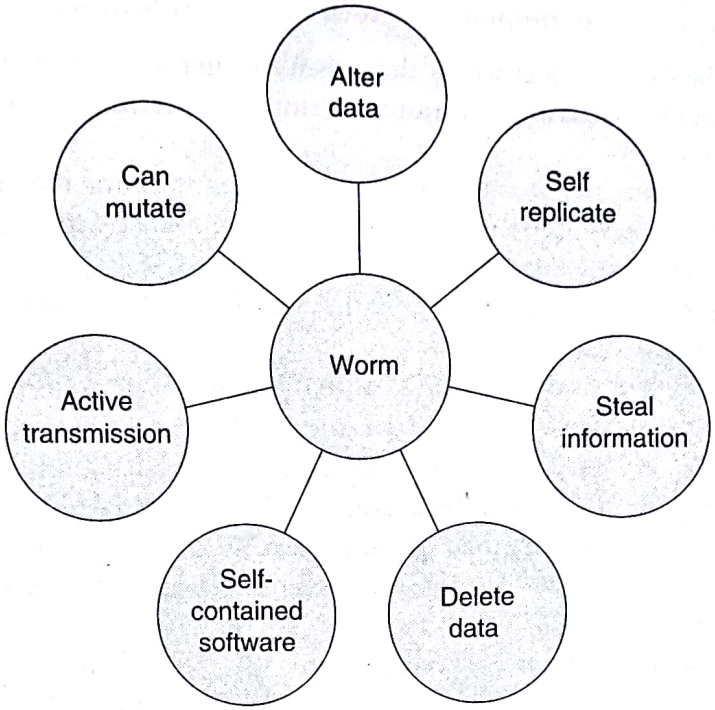


Figure 1.7 Worm.

1.6 Computer's Role in Crimes

Computers can play a vital role in crimes as shown in Figure 1.8. They can extract evidences, instrumentality, illegal imports, or the fruit of a crime.

1. They can act as a communication tool.
2. They can be the target of the attacker for criminal activity.
3. They can also be tangential to crime.

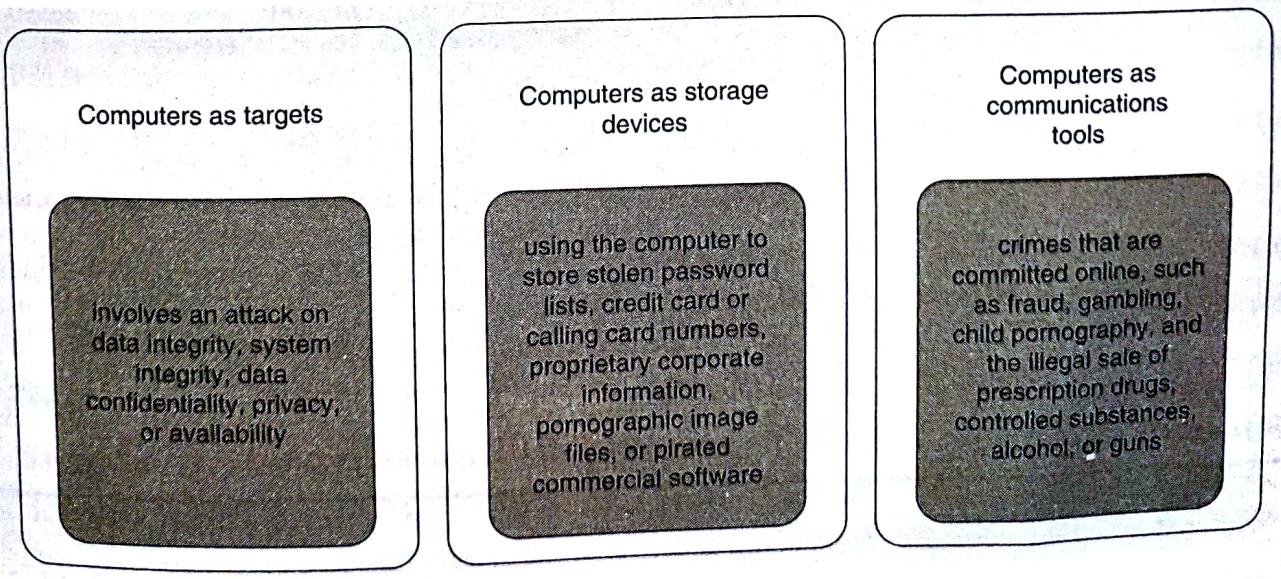


Figure 1.8 Roles of computer in crimes.

Scanned by CamScanner

Given below are instances where computers are used in crime scenarios.

1. Witnesses can view the suspect's picture on the screen through the use of computers.
2. DNA testing can be performed using computers. Using DNA testing, criminals can be identified from past crimes and booked.
3. Mini computers and laptops are used in police vehicles to determine the criminal records. The police cars are installed with wireless internet connections that are linked with satellites to perform the work with greater efficiency and in an easier manner.
4. Fingerprints can be taken using a computer and it can be used to determine whether the person is linked to any case in the past.
5. A computer can also determine how a fire was caused and what accelerant was used in the fire. This can be done using the computer investigation device.
6. Computers are also used at traffic junctions to find the vehicle identification number (VIN), whether the car is stolen, etc. In case of a crime, the person can be arrested immediately.
7. The databases of criminals are maintained in computers. With just a push of button, we can obtain all the information about the criminal. Also a list can be maintained of all citizens with prior tickets, bad behaviour, and felonies.
8. Simulations can be created by the use of computers.

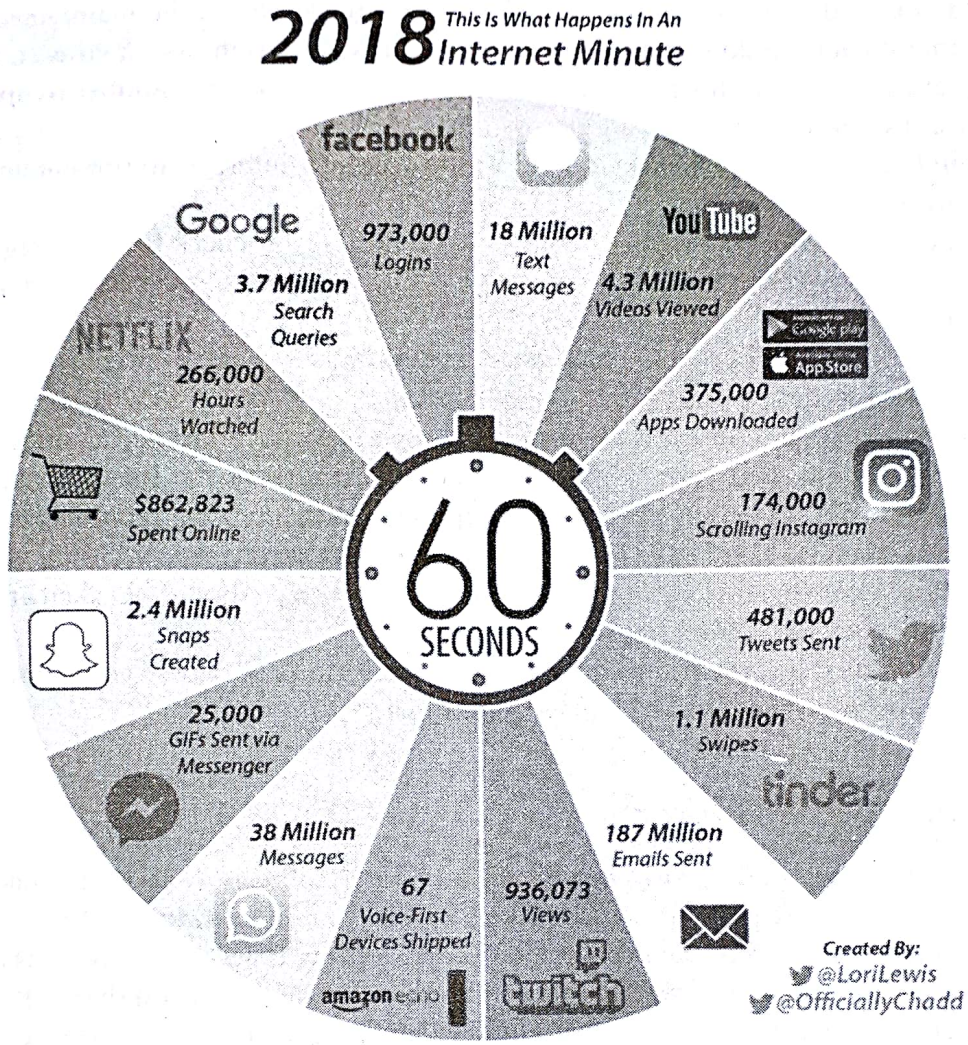
1.7 Cybercrime Statistics in India

Total cybercrimes, including fishing malicious code, website intrusion, denial of service, scanning, etc., that occurred in the last eight years are given in Table 1.1.

Table 1.1 Year-wise cybercrimes in India (Statistics presented in the Lok Sabha 2018)

Cyber attacks	*Cyber security incidents*	*Website hacking*	*Spam*
2011	28,127	21,700	2,480
2012	36,924	27,605	8,150
2013	41,319	28,481	54,677
2014	44,679	32,323	85,659
2015	49,455	27,025	61,628
2016	52,363	30,056	52,851
2017	53,000	22,230	50,665
2018 (Till September 2018)	28,547	20,589	35,687

Scanned by CamScanner



1.8 Prevention of Cybercrime

Prevention is always better than cure.

It is always better to take certain precautions while working on the internet.

The 5P's mantra for online security are as follows:

1. Precaution
2. Prevention
3. Protection
4. Preservation
5. Perseverance

Given below are a few steps that can be followed to prevent cybercrime.

1. Identification of exposures through education will help companies and firms meet these challenges.
2. One should avoid disclosing any personal information to strangers, a person whom they do not know, via email or while chatting or through any social networking site.
3. One must avoid sending any photograph to strangers online, as incidents of misuse or modification of photographs are on the rise.

Scanned by CamScanner

4. An updated anti-virus software to guard against virus attacks should be maintained by all netizens. Also, a backup of data should be taken regularly to avoid data loss in case of virus contamination.
5. A person should never send his/her credit card number or debit card number to any site that is not secured, to guard against frauds.
6. Parents should keep a watch when their children are accessing internet, to prevent any kind of harassment or deprivation.
7. Website owners should keep a watch on the network traffic, and check for any irregularities. It is the responsibility of the website owners to adopt policies for preventing cybercrimes as the number of internet users are growing every day.
8. Web servers running on public domain must be segregated physically and protected from internal network.
9. It is better to use a security program by the corporate body to control information on sites.
10. Strict statutory laws need to be passed by the Legislatures, keeping in mind the interest of netizens.
11. IT department should pass certain guidelines and notifications for the protection of computer system and should also come up with stringent laws to breakdown the criminal activities relating to cyberspace.
12. Cybercrime is a major threat to all the countries worldwide; steps should be taken at the international level to prevent cybercrimes from happening.
13. Complete justice must be provided to the victims of cybercrimes by way of compensatory remedy, and offenders must be punished with the highest punishment.

1.9 Definition of Hacker

The one who is curious about the workings of any computer software is termed a hacker. Very often, the hackers are a unit of smart programmers. Hackers have advanced knowledge of operative systems and programming languages. They need data concerning varied security holes among systems and are therefore the reasons for such holes. Hackers perpetually attempt to increase their data and share what they need to be discovered. Hackers never have dangerous intention like damaging or stealing knowledge.

1.10 Definition of Crackers

People who break into different systems with malicious intentions are referred to as crackers. Crackers cause issues to victims by an unauthorized access, destroying necessary information, stopping services provided by the server, and more. By their malicious actions, crackers are often simply known.

Hackers try to do constructive work, while crackers just destroy systems. Hackers are professionals, while crackers are criminals (Figure 1.9).

Hacker	Cracker
Lots of knowledge and Experience	Lots of knowledge and Experience
Good guy	Bad guy
Strong ethics	Poor ethics
No crime	Commits crime
Fights criminals	Is the criminal

Figure 1.9 Hacker versus cracker.

Scanned by CamScanner

1.11 Definition of Phreakers

Phreaker is the one who gains illegal access to the telephone system as shown in Figure 1.10. Phreakers are considered the original computer hackers and they are those who break into the telephone network illegally, typically to make free long distance phone calls or to tap phone lines.

Figure 1.10 Phreakers.

Phreakers are people who specialize in attacks on the telephone system. The word, which became popular in the mid-1980s, is probably a combination of the words *phone* and *freak* (Phreakers are also known as "phreaks" or "phone phreaks"). In the early days, phreakers whistled or used an instrument to mimic the tones of the phone system and then used to route calls and identify payment, especially as a way to avoid paying for an expensive call. Modern phreaking involves breaking into and manipulating the phone company's computer system, making it a specialized kind of hacking.

Recent examples of phreaker from the Web:

> In fact, the friends' first business venture together was marketing blue boxes to aspiring phreakers.
> —Laura Yan, *Popular Mechanics*, "An Early Hacker Used a Cereal Box Whistle to Take Over Phone Lines," 20 May 2018

1.12 Ethical Hacking

Hacking has been a locality of computing for nearly 5 decades and it is a really broad discipline, which covers a large variety of topics. The primary famed event of hacking had taken place in 1960 at Massachusetts Institute of Technology and at identical time, the term "Hacker" was originated. Hacking is the act of finding the possible entry points that exist in a very system or an electronic network and at last getting into them. Hacking is typically done to achieve unauthorized access to a system or an electronic network, either to hurt the systems or to steal sensitive data out there on the pc. Hacking is typically legal as long as it is being done to seek out weaknesses in a pc or network system for testing purpose. This type of hacking is what we have a tendency to decision moral hacking. An expert who does the act of hacking is called a "Hacker". Hackers are people who get information to know how systems operate, how they are designed, and then commit to play with these systems.

Scanned by CamScanner

1.13 Difference between Hacking and Ethical Hacking

Hacking	*Ethical Hacking*
Computer hacking refers to breaking into someone's system for personal or commercial gains. Hackers also called *pirates*, who use various tools to cause damage to information and assets.	Ethical hacking refers to the methodology adopted to find loopholes in information systems.
Same tools are used by both hackers and ethical hackers. The only difference is that hackers use tools to steal or destroy information, whereas ethical hackers use same tools to safeguard systems from "hackers with malicious intent". Ethical hacking is legal and hacking is done with permission from the client.	

1.14 Steps of Ethical Hacking

Like all good projects, ethical hacking too has a set of distinct phases. It helps hackers to make a structured ethical hacking attack. Even same process use for attacking the systems in illegal way.

Different security training manuals explain the process of ethical hacking in different ways, but the entire process can be categorized into the following five phases as shown in Figure 1.11:

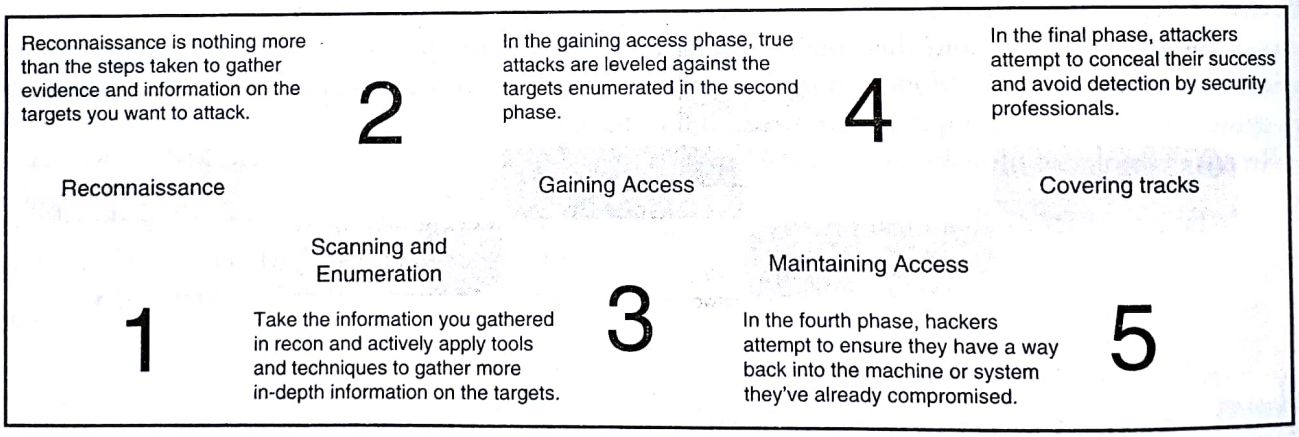


Figure 1.11 Steps of ethical hacking.

1.14.1 Reconnaissance

Reconnaissance is the phase where the attacker gathers information about a target using active or passive means as shown in Figure 1.12. The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks (these Tools are discussed in later part of this chapter).

1.14.2 Scanning

In scanning, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited as shown in Figure 1.13. The tools used in this process are Nessus, Nexpose, Wireshark, and NMAP (tools are discussed in later part of this chapter).

Scanned by CamScanner

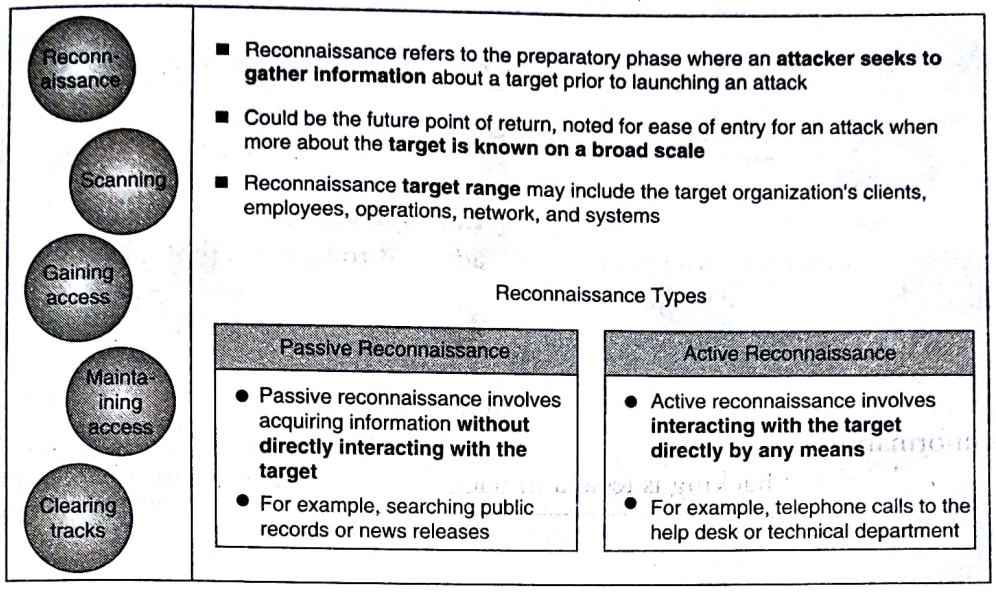


Figure 1.12 Reconnaissance.

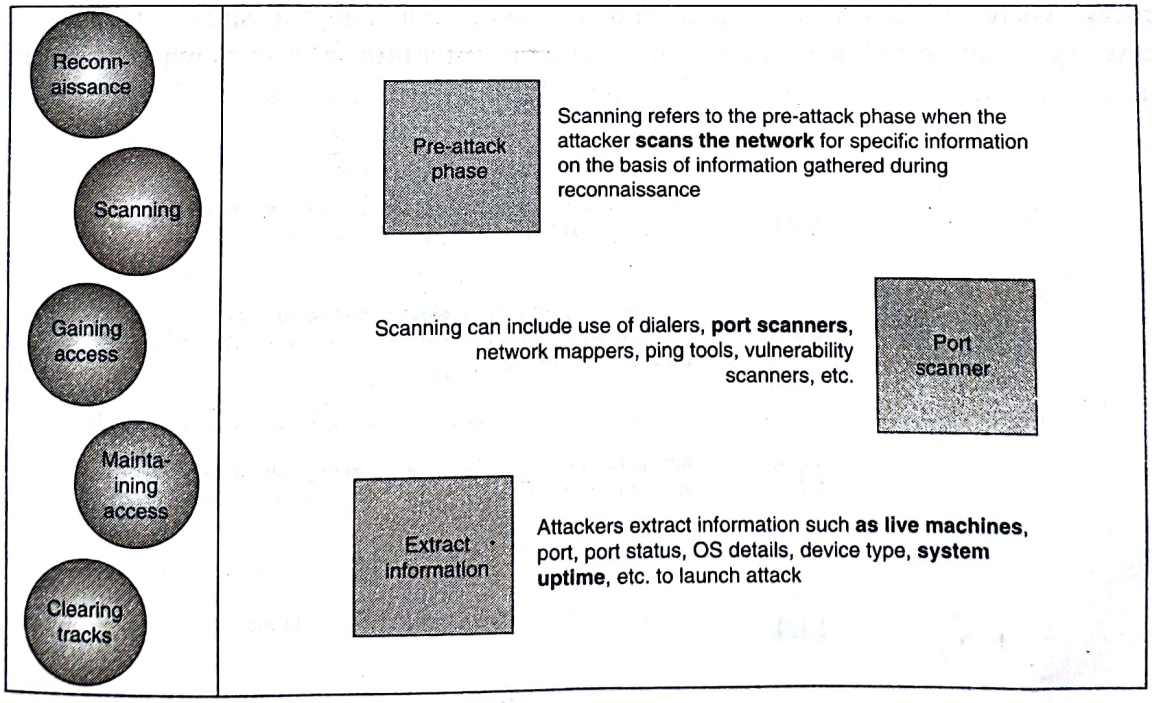


Figure 1.13 Scanning.

1.14.3 Gaining Access

In this process, the vulnerability is located and you attempt to exploit it in order to enter into the system as shown in Figure 1.14. The primary tool that is used in this process is Metasploit.

Scanned by CamScanner

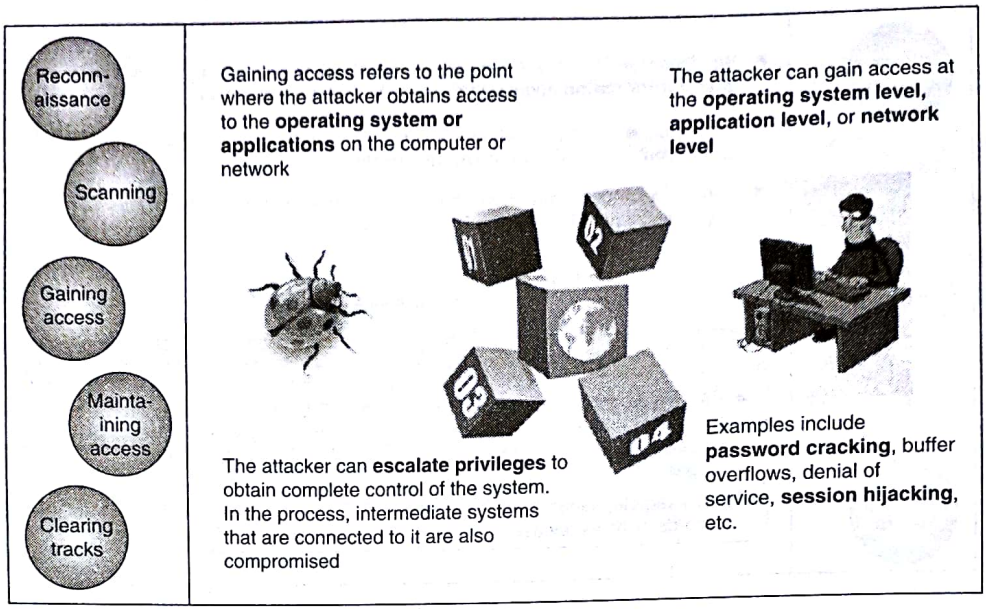


Figure 1.14 Gaining access.

1.14.4 Maintaining Access

It is the process where the hacker has already gained access into a system as shown in Figure 1.15. After gaining access, the hacker installs some backdoors in order to enter into the system when he/she needs access in this owned system in future. Metasploit is the preferred tool in this process.

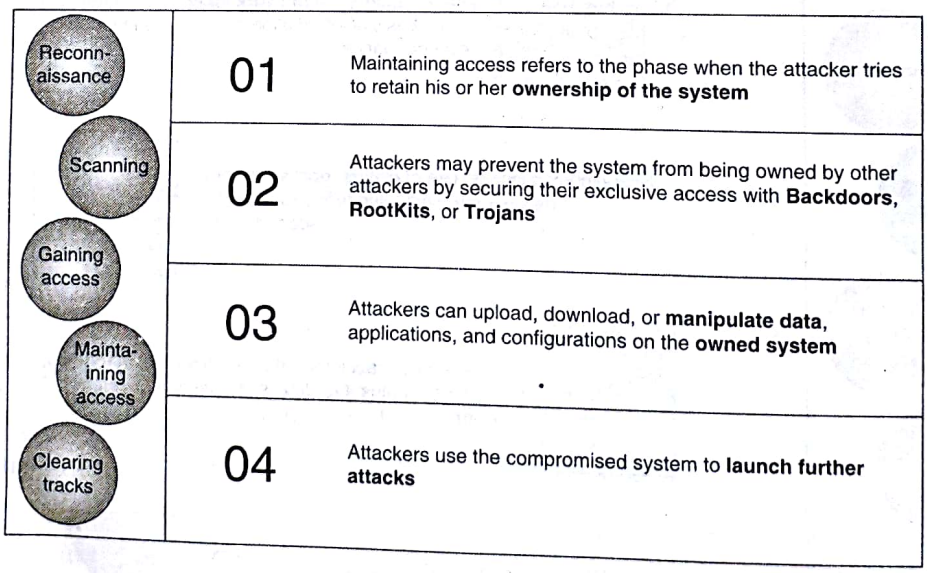


Figure 1.15 Maintaining access.

1.14.5 Clearing Tracks

This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process as shown in Figure 1.16.

Scanned by CamScanner

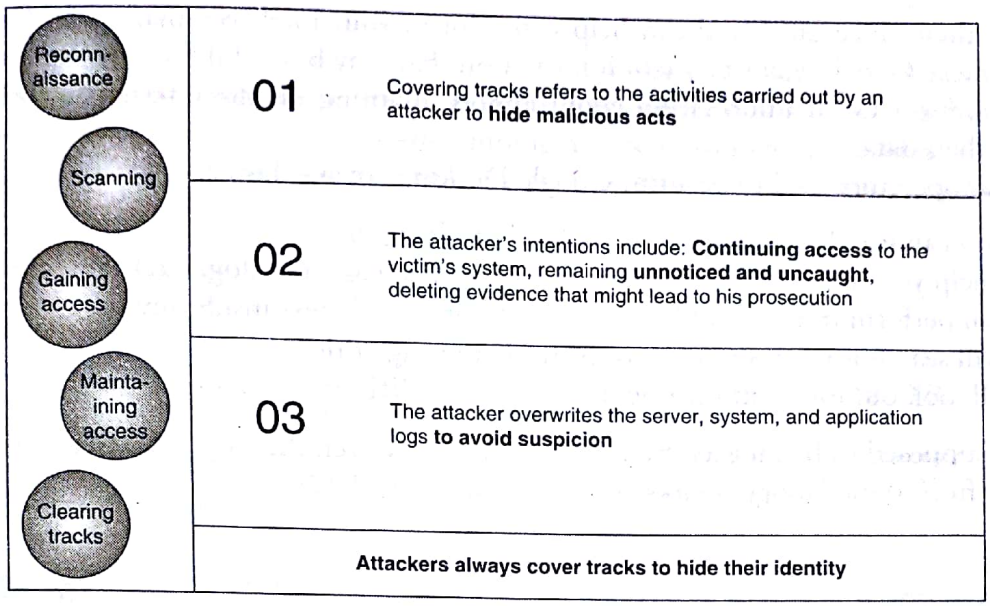


Figure 1.16 Clearing tracks.

1.15 Exploring Some Tools for Ethical Hacking

As with any project, it is troublesome in accomplishing the task if you do not have the correct tools for ethical hacking. Simply because the correct tools are used does not mean that you simply can discover all vulnerabilities. It is necessary to understand the private and technical limitations. Many security-assessment tools generate false positives and negatives (incorrectly identifying vulnerabilities). Others may miss vulnerabilities. If you are performing tests such as social engineering or physical-security assessments, you may miss weaknesses. One tool will take a look at everything, as some concentrate on specific tests. Therefore, you will want a group of specific tools that you simply will invoke for the task at hand. The more tools you have, the easier your ethical hacking efforts are.

1.15.1 *Reconnaissance Tools*

1.15.1.1 *Nmap*

Nmap or "Network Mapper" is one of the most popular and widely used security auditing tools. Is a free and open-source utility that is utilized for security auditing and network exploration across local and remote hosts.

Some of the main features include:

1. **Host detection:** Nmap has the ability to identify hosts inside any network that have certain ports open, or that can send a response to ICMP and TCP packets.
2. **IP and DNS information detection:** It includes device type, Mac addresses, and even reverse DNS names.
3. **Port detection:** Nmap can detect any port open on the target network, letting you know the possible running services on it.
4. **OS detection:** Provides full OS version detection and hardware specifications of any host connected.
5. **Version detection:** Nmap is also able to get application name and version number.

1.15.1.2 *Google Dorks*

While investigating people or companies, a lot of IT security newbies forget the importance of using traditional search engines for recon and intel gathering. In this case, Google Dorks can be your best friend.

Scanned by CamScanner

They have been there since 2002 and can help you a lot in your intel reconnaissance. Google Dorks are simply ways to query Google against certain information that may be useful for your security investigation. Search engines index a lot of information about almost anything on the internet, including individual, companies, and their data.

Some popular operators used to perform Google Dorking are as follows:

1. **Filetype:** You can use this dork to find any kind of file types.
2. **Ext:** It can help you to find files with specific extensions (e.g., .txt, .log, etc.).
3. **Intext:** It can perform queries and helps to search for specific text inside any page.
4. **Intitle:** It will search for any specific words inside the page title.
5. **Inurl:** It will look out for mentioned words inside the URL of any website.

Log files are not supposed to be indexed by search engines; however, they are indexed and you can get valuable information from these Google Dorks, as you see in Figure 1.17:

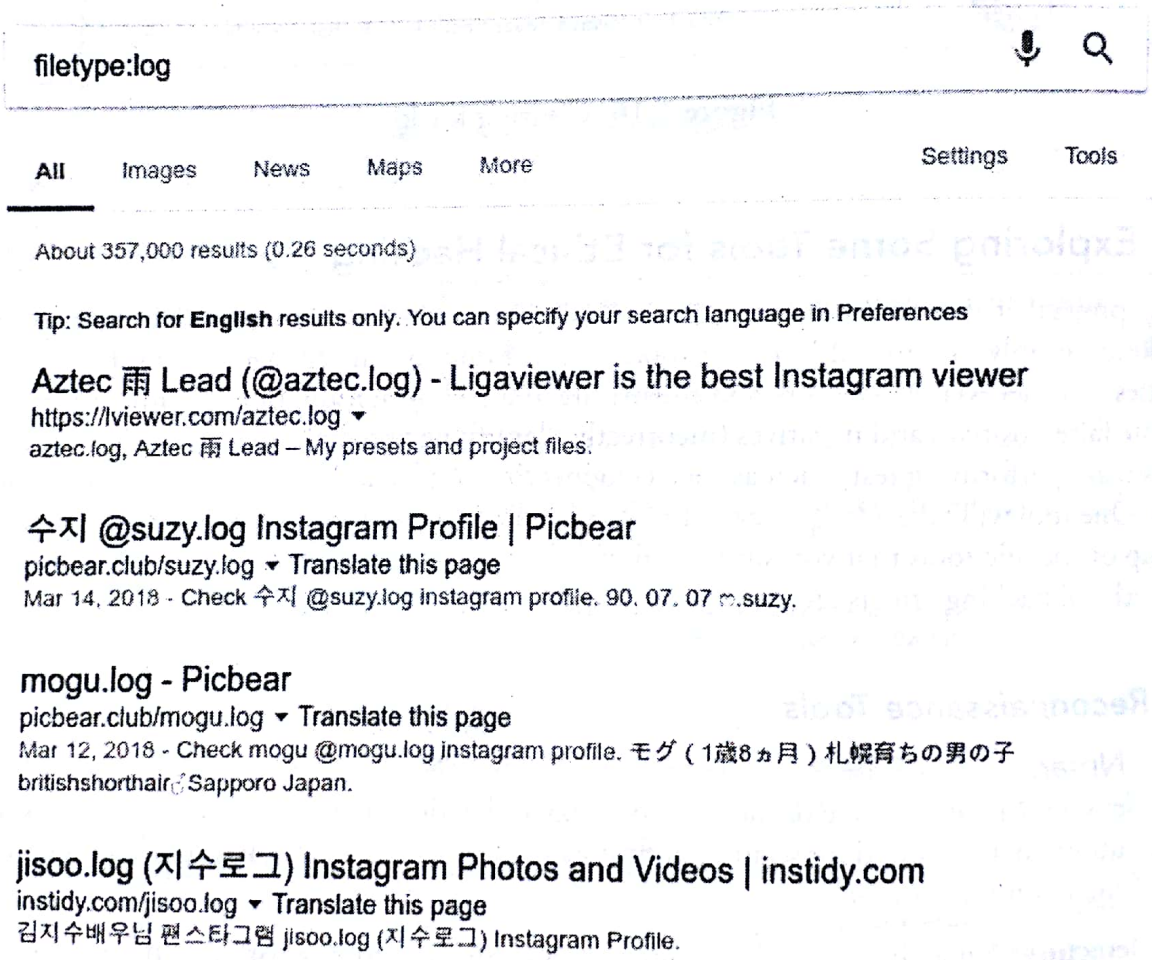


Figure 1.17 Valuable information from Google Dorks.

1.15.1.3 Maltego

It is a tremendous tool to trace down footprints of any target you wish to match. This piece of software package has been developed by Paterva, and it is a part of the Kali UNIX system distribution.

Using Maltego can enable you to launch intelligence activity testes against specific targets. One of the simplest things this software package includes is about their "decision 'transforms". Transforms are offered without charge in some cases, and on others, you will realize industrial versions solely. They are going to assist you to run a unique quite tests and knowledge integration with external applications.

Scanned by CamScanner

In order to use Maltego, you wish to open a free account on their website, after that, you will launch a replacement machine or run transforms on the target from Associate in Nursing existing one. Once you have chosen your transforms, Maltego app can begin running all the transforms from Maltego servers. Finally, Maltego can show you the results for the desired targets, such as IP, domains, AS numbers, and far additional.

1.15.2 Scanning tools

1.15.2.1 Nexpose

Nexpose vulnerability scanner, developed by Rapid7, which is an open-source tool is developed by Rapid7 isand is used to scan the vulnerabilities and performs various network checks as:

1. Nexpose is employed to watch the exposure of vulnerabilities in time period, acquaint itself to new hazards with recent information.
2. Generally, most of the vulnerability scanners categorize the risks employing a high or medium or low scale.
3. Nexpose considers the age of the vulnerability like that malware kit is employed in it, what blessings area unit utilized by it etc., and fix the difficulty supported its priority.
4. Nexpose mechanically detects and scans the new devices and assesses the vulnerabilities once they access the network.
5. Nexpose may be integrated with a Metaspoilt framework.

1.15.2.2 Wireshark

Wireshark is the world's leading and extensively used network protocol analyzer.

1. Wireshark is employed across varied streams, like instructional establishments, government agencies, enterprises, etc., to appear into the networks at a microscopic level.
2. Wireshark encompasses a special feature am fond of it captures the problems on-line and performs the analysis offline.
3. Wireshark runs on varied platforms like Windows, Linux, masOS, Solaris, etc.
4. Wireshark has the potential of deeply inspecting several protocols with additional supplementary all the time.
5. Among the protection practitioners toolkit, Wireshark is that the most powerful tool.

1.15.2.3 Nessus

Nessus is a patented and branded vulnerability scanner developed by Tenable Network Security.

1. This tool has been put in and employed by countless users throughout the planet for vulnerability assessment, configuration problems etc.
2. Nessus is employed to forestall the networks from the penetrations created by hackers by assessing the vulnerabilities at the earliest.
3. Nessus supports wide-range of OS, applications, DBs, and lots of more network devices among cloud infrastructure, physical and virtual networks.
4. Nessus is capable of scanning the vulnerabilities which permit remote hacking of sensitive information from a system.

1.16 What to Do if Been Hacked?

1. **Cut-off your internet connection:** If you think that you simply are being hacked, the primary factor to try to do is to cut-off internet from your system so as to prevent any more intrusion.

Scanned by CamScanner

2. **Turn on firewall:** Typically, we have a tendency to close up windows firewall so as to put in some package. From a security purpose of read , forever we must always activate firewalls. Hardware firewall is another smart choice to install. It acts as an associate isolator between external network and your internal systems.
3. **Contact your internet service supplier:** It's a decent apply to contact your ISP within the case of hacking as a result of they need their own policy and pointers for any malicious intrusion.

Summary

Criminalization is a social phenomenon, which has witnessed an increasing trend in the last few years. Crime investigation analysis is a field where digital forensic investigation plays a vital role in terms of predicting and analyzing criminals. There is the anti-spyware program. As if viruses were not enough, corporations from around the world determined to make programs that might develop knowledge from your PC so as to amass data for his/her databases. It should not be as dangerous as a deadly disease; however, it is an intrusion into your privacy. Wipe them out with this piece of package. Nowadays, hackers' hindrance has become a task for everyone. It is not the responsibility of the supervisor of our company. After all, he/she will install every protection within the company's network; however, if you let a deadly disease in due to your carelessness, he/she will not be ready to stop it. The same goes for your PC reception. Keep in mind that there are new hacker tricks every day. Therefore, you need to be ready.

Key Terms

- **Bot:** For 'robot' – a program used for a specific function such as keeping a port open or launching a flood of packets in a distributed denial-of-service attack.
- **Cracking:** Malicious or criminal hacking. Unauthorized penetration of computer systems and networks, abuse of privilege, unauthorized use of services.
- **Easter egg:** Undocumented, unauthorized program functions in a production program; a kind of Trojan horse.
- **Identity theft:** Creating a false identity using someone else's identity, identifying information (e.g., name, social security number, birthday) to create new credit cards or establish loans which then go into default and affect the original victim's credit record.
- **Malware:** Malicious software, including Trojan horses, viruses, worms, logic bombs, exploits, and time bombs.
- **Zombie:** A program inserted into a vulnerable system to await further instructions; usually part of a distributed denial-of-service (DDoS) attack.
- **Cookie:** Cookies are text files sent from your Web browser to a server, usually to customize information from a website.
- **Cracking:** To break into a secure computer system, frequently to do damage or gain financially, though sometimes in political protest.
- **Firewall:** A system using hardware, software, or both to prevent unauthorized access to a system or machine.
- **Hash:** A hash is a number generated by an algorithm from a string of characters in a message or other string.
- **IRC:** Internet relay chat is a protocol used by both groups and for one-on-one conversations. Often utilized by hackers to communicate or share files.
- **Malware:** A software program designed to hijack, damage, or steal information from a device or system.
- **Packet sniffer:** Sniffers are programs designed to detect and capture certain types of data. Packet sniffers are designed to detect packets travelling online.

Scanned by CamScanner

- **Rootkit:** A rootkit is a set of software programs used to gain administrator-level access to a system and set up malware, while simultaneously camouflaging the takeover.
- **Spear phishing:** A more focused type of phishing, targeting a smaller group of targets, from a department within a company or organization down to an individual.

Review Questions

1. What is a computer crime? Explain.
2. List and explain the various types of cyber theft.
3. Explain the term 'cyber terrorism' with examples.
4. What are the different categories of cybercrime?
5. Distinguish between viruses and worms.
6. What is cybercrime? Explain in detail.
7. What is a virus? What are the types of viruses?
8. What is the role of computer in cybercrimes?
9. Explain how cybercrimes can be prevented.
10. Explain in detail 'internet spawn crimes'.
11. What is a worm? What are the types of worms?
12. What is the difference between hacking and cracking?
13. Why do hackers do hack? What is the motive behind their hacking?
14. Who is known as an ethical hacker?
15. What is foot printing and how does one perform foot printing? What are the various techniques for foot printing?
16. Explain the various types of hackers and which type is most dangerous. Justify.
17. Explain different types of ethical hackers.
18. What are the various tools available for ethical hacking?
19. Explain steps of hacking with example.

Scanned by CamScanner