Malware and its type in cyber security

Malware and its types

Malware stands for “Malicious Software” and it is designed to gain access or installed into the computer without the consent of the user. They perform unwanted tasks in the host computer for the benefit of a third party. There is a full range of malwares which can seriously degrade the performance of the host machine. There is a full range of malwares which are simply written to distract/annoy the user, to the complex ones which captures the sensitive data from the host machine and send it to remote servers. There are various types of malwares present in the Internet. Some of the popular ones are:

Adware

It is a special type of malware which is used for forced advertising. They either redirect the page to some advertising page or pop-up an additional page which promotes some product or event. These adware are financially supported by the organizations whose products are advertised.

Spyware

It is a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine. Mostly it gathers the browsing habits of the user and the send it to the remote server without the knowledge of the owner of the computer.  Most of the time they are downloaded in to the host computer while downloading freeware i.e. free application programs from the internet. Spywares may be of various types; It can keeps track of the cookies of the host computer, it can act as a keyloggers to sniff the banking passwords and sensitive information, etc.

Browser hijacking software

There is some malicious software which are downloaded along with the free software offered over the internet and installed in the host computer without the knowledge of the user. This software modifies the browsers setting and redirect links to other unintentional sites.

Virus

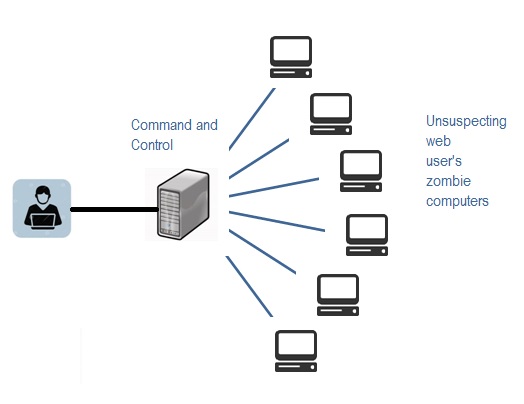
A virus is a malicious code written to damage/harm the host computer by deleting or appending a file, occupy memory space of the computer by replicating the copy of the code, slow down the performance of the computer, format the host machine, etc.  It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc. A virus may be present in a computer but it cannot activate itself without the human intervention. Until and unless the executable file(.exe) is execute, a virus cannot be activated in the host machine.

Worms

They are a class of virus which can replicate themselves. They are different from the virus by the fact that they does not require human intervention to travel over the network and spread from the infected machine to the whole network. Worms can spread either through network, using the loopholes of the Operating System or via email. The replication and spreading of the worm over the network consumes the network resources like space and bandwidth and force the network to choke.

Trojan Horse

Trojan horse is a malicious code that is installed in the host machine by pretending to be useful software. The user clicks on the link or download the file which pretends to be a useful file or software from legitimate source. It not only damages the host computer by manipulating the data but also it creates a backdoor in the host computer so that it could be controlled by a remote computer. It can become a part of botnet(robot-network), a network of computers which are infected by malicious code and controlled by central controller. The computers of this network which are infected by malicious code are known as zombies. Trojens neither infect the other computers in the network nor do they replicate.

[](https://storage.googleapis.com/swayam-node2-production.appspot.com/assets/img/nou19_cs08/botnet.jpg)

Scareware

Internet has changed how we talk, shop, play etc. It has even changed the way how the criminal target the people for ransom. While surfing the Internet, suddenly a pop-up alert appears in the screen which warns the presence of dangerous virus, spywares, etc. in the

user’s computer. As a remedial measure, the message suggests the used download the full paid version of the software. As the user proceeds to download, a malicious code, known as scareware is downloaded into the host computer. It holds the host computer hostage until the ransom is paid. The malicious code can neither be uninstalled nor can the computer be used till the ransom is paid. A sample message alert of a scareware is shown below in Fig 3[1]

[](https://storage.googleapis.com/swayam-node2-production.appspot.com/assets/img/nou19_cs08/scareware.jpg)  
Sample Warning Message of a Scareware1

**Encryption Methods and Vulnerabilities**

Encryption is a security method in which information is encoded in such a way that only authorized user can read it. It uses encryption algorithm to generate ciphertext that can only be read if decrypted.

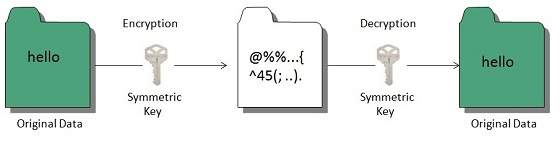
### **Types of Encryption**

There are two types of encryptions schemes as listed below:

* Symmetric Key encryption
* Public Key encryption

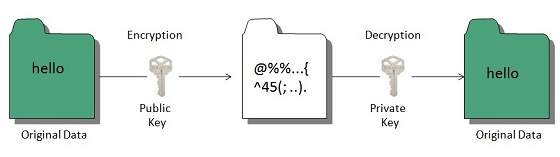
#### **Symmetric Key encryption**

**Symmetric key encryption** algorithm uses same cryptographic keys for both encryption and decryption of cipher text.



#### **Public Key encryption**

**Public key encryption** algorithm uses pair of keys, one of which is a secret key and one of which is public. These two keys are mathematically linked with each other.



## Hashing

In terms of security, hashing is a technique used to encrypt data and generate unpredictable hash values. It is the hash function that generates the hash code, which helps to protect the security of transmission from unauthorized users.

### **Hash function algorithms**

**Hashing algorithm** provides a way to verify that the message received is the same as the message sent. It can take a plain text message as input and then computes a value based on that message.

**Key Points**

* The length of computed value is much shorter than the original message.
* It is possible that different plain text messages could generate the same value

**Common Computer Security Vulnerabilities**

A computer vulnerability is a cybersecurity term that refers to a defect in a system that can leave it open to attack. This vulnerability could also refer to any type of weakness present in a computer itself, in a set of procedures, or in anything that allows information security to be exposed to a threat.

It is possible for network personnel and computer users to protect computers from vulnerabilities by regularly updating software security patches. These patches are capable of solving flaws or security holes found in the initial release. Network personnel and computer users should also stay informed about current vulnerabilities in the software they use and look out for ways to protect against them.

The most common computer vulnerabilities include:

* Bugs
* Weak passwords
* Software that is already infected with virus
* Missing data encryption
* OS command injection
* SQL injection
* Buffer overflow
* Missing authorization
* Use of broken algorithms
* URL redirection to untrusted sites
* Missing authentication for critical function
* Unrestricted upload of dangerous file types
* Download of codes without integrity checks

**Causes and Harms of Computer Security Vulnerabilities**

Computer system vulnerabilities exist because programmers fail to fully understand the inner programs. While designing and programming, programmers don’t really take into account all aspects of computer systems and this, in turn, causes computer system vulnerability. Some programmers program in an unsafe and incorrect way, which worsen computer system vulnerability.

The harm of computer [system vulnerability](https://enterprise.comodo.com/blog/what-is-vulnerability-assessment/?af=7639) can be presented in several aspects, for example, the disclosure of confidential data, and widespread of Internet virus and hacker intrusion, which can cause great harm to enterprises and individual users by bringing about major economic loss. With the steady improvement of the degree of information, very severe computer system vulnerabilities can become a threat to national security in the aspects of economy, politics, and military.

Computer security vulnerability can harm these kinds of system securities that include:  Reliability, confidentiality, usability, and undeniableness.

* **Reliability:** This refers to reducing the degreeof the operation of a computer system and enhancing the efficiency of a computer system.
* **Confidentiality:** This refers to protecting users’ information from disclosure and getting by unauthorized third party.
* **Usability:** This ensures that users can enjoy the services offered by computers and information networks.
* **Undeniableness:** This security refers to guaranteeing information actors to be responsible for their behavior.

Internet Tracing Methods

## ****What Is IP Tracing?****

An Internet Protocol (IP) address is a unique numerical identifier assigned to all computer devices connected to a computer network. It is primarily used for interface identification, location addressing and to communicate over a network.

Tracing an IP address involves finding the device that an IP address was assigned to at a specific time, the location of the device and the user of the device at that specific time. IP tracing is an important aspect used in tracking the name and location of Cybercriminals.

There are a number of free public tools that can be used to trace IP addresses. However, they all have limited capability. If an IP address has been concealed either by using  a proxy, VPN or any anonymizer, you need the assistance of a professional cyber forensics investigator to trace the original I.

It is a common practice for Cyber Criminals to hide their IP address when they carry out illegal cyber activities such as [cyber stalking](https://cyberforensicsinvestigators.com/cyber-stalking/)(the repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails.), fraud, and other forms of cyber crimes.

## ****Cyberexpert Help With IP Tracing****

We have a team of cyber forensic investigator experts that are equipped with the  forensic tools needed to trace IP addresses. We harness our proprietary methods, paid tools, legal processes and connection with several Internet Service Providers to follow the trail of a network and find out where it is originating from.

Electronic passage through [the Internet](https://www.encyclopedia.com/science-and-technology/computers-and-electrical-engineering/computers-and-computing/internet) leaves a trail that can be traced. Tracing is a process that follows [the Internet](https://www.encyclopedia.com/science-and-technology/computers-and-electrical-engineering/computers-and-computing/internet) activity backwards, from the recipient to the user. As well, a user's Internet activity on web sites can also be tracked on the recipient site (i.e., what sites are visited and how often). Sometimes this tracking and tracing ability is used to generate email to the user promoting a product that is related to the sites visited. User information, however, can also be gathered covertly.

Techniques of Internet tracking and tracing can also enable authorities to pursue and identify those responsible for malicious Internet activity. For example, on February 8, 2000, a number of key commercial Internet sites such as Yahoo, Ebay, and Amazon were jammed with incoming information and rendered inoperable. Through tracing and tracking techniques, law enforcement authorities established that the attacks had arisen from the computer of a 15-year-old boy in [Montreal](https://www.encyclopedia.com/places/united-states-and-canada/canadian-political-geography/montreal), [Canada](https://www.encyclopedia.com/places/united-states-and-canada/canadian-political-geography/canada). The youth, whose Internet identity was "Mafiaboy," was arrested within months of the incidents.

Law enforcement use of Internet tracking is extensive. For example, the U.S. [Federal Bureau of Investigation](https://www.encyclopedia.com/social-sciences-and-law/political-science-and-government/us-government/federal-bureau-investigation) has a tracking program designated Carnivore. The program is capable of scanning thousands of emails to identify those that meet the search criteria.

## Tracking Tools

**Cookies.** Cookies are computer files that are stored on a user's computer during a visit to a web site. When the user electronically enters the web site, the host computer automatically loads the file(s) to the user's computer.

The cookie is a tracking device, which records the electronic movements made by the user at the site, as well as identifiers such as a username and password. Commercial web sites make use of cookies to allow a user to establish an account on the first visit to the site and so to avoid having to enter account information (i.e., address, [credit card](https://www.encyclopedia.com/social-sciences-and-law/economics-business-and-labor/money-banking-and-investment/credit-card) number, financial activity) on subsequent visits. User information can also be collected without knowing to the user and subsequently used for whatever purpose the host intends.

Cookies are files, and so can be transferred from the host computer to another computer. This can occur legally (i.e., selling of a subscriber mailing list,A **mailing list** is a collection of names and addresses used by an individual or an organization to send material to multiple recipients.) or illegally (i.e., "hacking in" to a host computer and copying the file). Also, cookies can be acquired as part of a law enforcement investigation.

Stealing a cookie requires knowledge of the file name. Unfortunately, this information is not difficult to obtain. A survey, conducted by a U.S. Internet security company in 2002, on 109, 212 web sites that used cookies found that

almost 55 percent of them used the same cookie name. Cookies may be disabled by the user, however, this calls for programming knowledge that many users do not have or do not wish to acquire.

**Bugs or Beacons.** A bug or a beacon is an image that can be installed on a web page or in an email. Unlike cookies, bugs cannot be disabled. They can be prominent. As examples of the latter, graphics that are transparent to the user can be present, as can graphics that are only 1x1 pixels in size (corresponding to a dot on a computer monitor). When a user clicks onto the graphic in an attempt to view, or even to close the image, information is relayed to the host computer.

Information that can be gathered by bugs or beacons includes:

* the user's IP address (the Internet address of the computer)
* the email address of the user
* the user computer's operating system (which can be used to target viruses to specific operating systems
* the URL (Uniform Record Locator), or address, of the web page that the user was visiting when the bug or beacon was activated
* the browser that was used (i.e., Netscape, Explorer)

When used as a marketing tool or means for an entrepreneur to acquire information about the consumer, bugs or beacons can be merely an annoyance. However, the acquisition of IP addresses and other user information can be used maliciously. For example, information on active email addresses can be used to send "spam" email or virus-laden email to the user. And, like cookies, the information provided by the bug or beacon can be useful to law enforcement officers who are tracking down the source of an Internet intrusion.

**Active X, Java Script.** These computer-scripting languages are automatically activated when a site is visited. The mini-programs can operate within the larger program, so as to create the "pop-up" advertiser windows that appear with increasing frequency on web sites. When the pop-up graphic is visited, user information such as described in the above sections can be gathered.

**Tracing email.** Email transmissions have several features that make it possible to trace their passage from the sender to the recipient computers. For example, every email contains a section of information that is dubbed the header. Information concerning the origin time, date, and location of the message is present, as is the Internet address (IP) of the sender's computer.

If an alias has been used to send the message, the IP number can be used to trace the true origin of the transmission. When the message source is a personally owned computer, this tracing can often lead directly to the sender. However, if the sending computer serves a large community—such as a university, and through which malicious transmissions are often routed—then identifying the sender can remain difficult.

Depending on the email program in use, even a communal facility can have information concerning the account of the sender.

The information in the header also details the route that the message took from the sending computer to the recipient computer. This can be useful inthe identitfies of the sender. For example, in the case of Mafiaboy, examination of the transmissions led to a computer at the University of [California](https://www.encyclopedia.com/places/united-states-and-canada/us-political-geography/california) at Santa Barbara that had been commandeered for the prank. Examination of the log files allowed authorities to trace the transmission path back to the sender's [personal computer](https://www.encyclopedia.com/science-and-technology/computers-and-electrical-engineering/computers-and-computing/personal-0).

**Chat rooms.** Chat rooms are electronic forums where users can visit and exchange views and opinions about a variety of issues. By piecing together the electronic transcripts of the chat room conversations, enforcement officers can track down the source of malicious activity.

Returning to the example of Mafiaboy, enforcement officers were able to find transmissions at certain chat rooms where the upcoming malicious activity was described. The source of the transmissions was determined to be the youth's [personal computer](https://www.encyclopedia.com/science-and-technology/computers-and-electrical-engineering/computers-and-computing/personal-0). Matching the times of the chat room transmissions to the malicious events provided strong evidence of the youth's involvement.

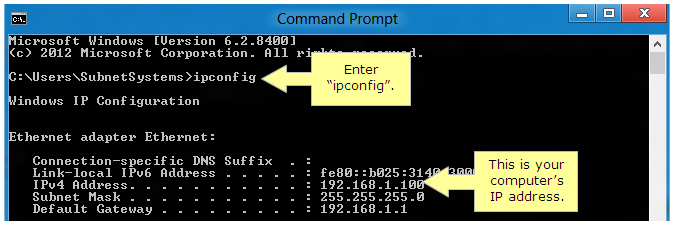
**Internet Protocol Address**

The **Internet Protocol Address** (IP Address) is one of the core components of the Internet. All computers or devices use IP address for communication that is allotted either on a Static or Dynamic basis. This is the main reason why Law Enforcement Agencies all over the World use IP Addresses to trace a Cyber Criminal or Accused. An IP Address may not be what it appears to be on the first look; it can be involved in many **IP address Spoofing** cases, that’s the reason why we cannot rely upon an IP address to convict a Cyber Criminal.

## ****IP Configuration Command (ipconfig): –****

**Step 1: –**Press the **Windows Key** to access the Start screen. Enter **cmd**in the field and click **OK**.

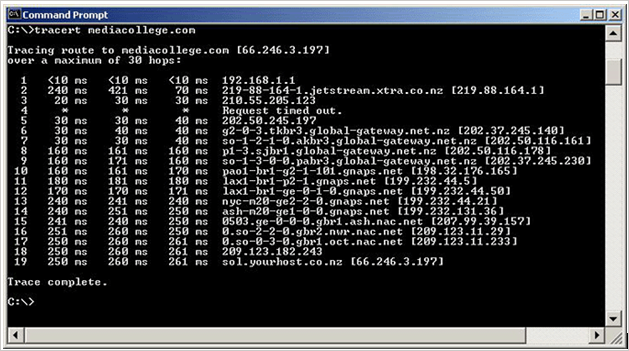
**Step 2**: – Enter **“ipconfig”**and press the (Enter key).



* The **IPv4** **Address** is your computer’s IP address.
* The **IPv4 Default Gateway** is your router’s IP address.
* **Subnet Mask** identifies the network address of an IP address by performing a bitwise AND operation on the netmask.

## ****IP Configuration Command (Traceroute): –****

**Traceroute command** shows the path, a packet of information takes from your computer to the one you specify. It creates a list of all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it also shows that how long each hop from router to router takes.



**1** is the internet gateway on the network this traceroute was done from (an ADSL modem in this case).

**2** is the ISP, the originating computer is connected

**3** is also in the extra network.

**4**show timed out.

**5 – 9**are all routers on the global-gateway.net.nz network.

**10 – 14**are all gnaps.net in the USA (a telecom supplier in the USA).

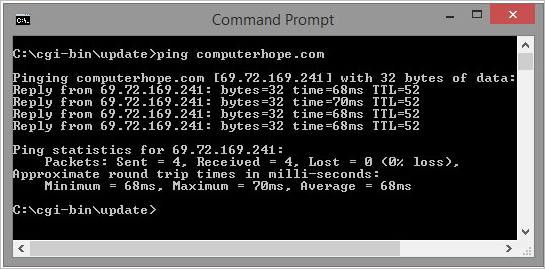
**15 – 17** are on the NAC (Net Access Corporation) network and an ISP in the New York area.

**18**is the router on which the network mediacollege.com is hosted on.

Finally**, 19**is the computer mediacollege.com is hosted on (sol.yourhost.co.nz)

### **IP Configuration Command (Ping): –**

The **ping command** is used to test the ability of the source computer to reach a specified destination computer. The ping command is usually used to verify that a computer can communicate over the network with other computer or network device.



**Number of Pings: –** By default, the ping cmd sends out 4 packets of 32 bytes each.

**Size of Packet: –** By default, the packets sent are a small 32 bytes. A user can set own size up to the maximum 65500 bytes.

**Time Out: –**The timeout by default is 4,000 milliseconds which amounts to 4 minutes.

**Tracking, tracing, and privacy.** While Internet tracking serves a useful purpose in law enforcement, its commercial use is increasingly being examined from the standpoint of personal privacy. The 1984 Cable Act in the [United States](https://www.encyclopedia.com/places/united-states-and-canada/us-political-geography/united-states) permits the collection of such information if the information is deemed to aid future commercial developments. User consent is required, however, if the information that is capable of being collected can exceed that needed for commerce