**Network**

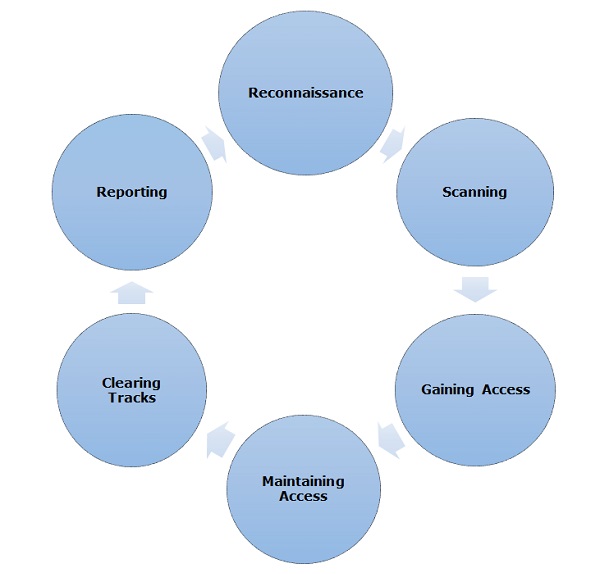
**Security**

**Class 9**

**Lab 29**

|  |
| --- |
| Lab Objectives:  * Reconnaissance * Footprinting tools |

# Ethical Hacking Process



## Information Gathering and getting to know the target systems is the first process in ethical hacking. Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system.

## ***Active Reconnaissance***

## In this process, you will directly interact with the computer system to gain information.

## ***Passive Reconnaissance***

## In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

## IMG_256

# Footprinting

## Footprinting is a part of reconnaissance process which is used for gathering possible information about a target computer system or network. Footprinting could be both **passive**and active.



## During this phase, a hacker can collect the following information −

## Domain name

## IP Addresses

## Namespaces

## Employee information

## Phone numbers

## E-mails

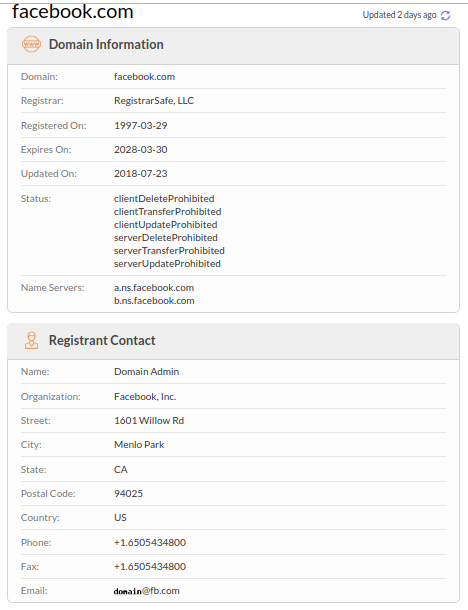
## Job Information

## In the following section, we will discuss how to extract the basic and easily accessible information about any computer system or network that is linked to the Internet.

# Domain Name Information

## You can use <https://www.whois.com/whois> website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.

 type facebook.com and search to see the results



# IP Address

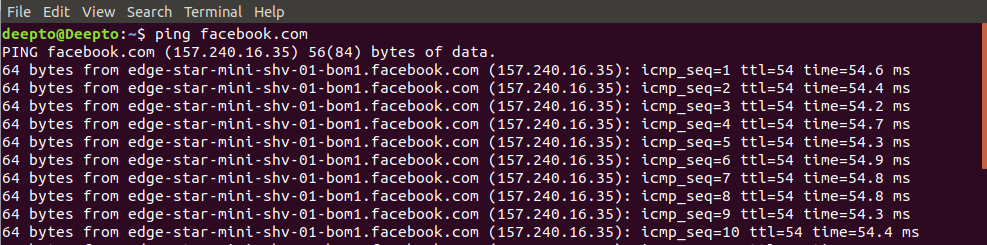
## a unique string of numbers separated by full stops that identifies each computer using the Internet Protocol to communicate over a network.

# Finding IP Address

## You can use ping command at your prompt. This command is available on Windows as well as on Linux OS. Following is the example to find out the IP address of [www.facebook.com](http://www.facebook.com)

## Type $ ping facebook.com

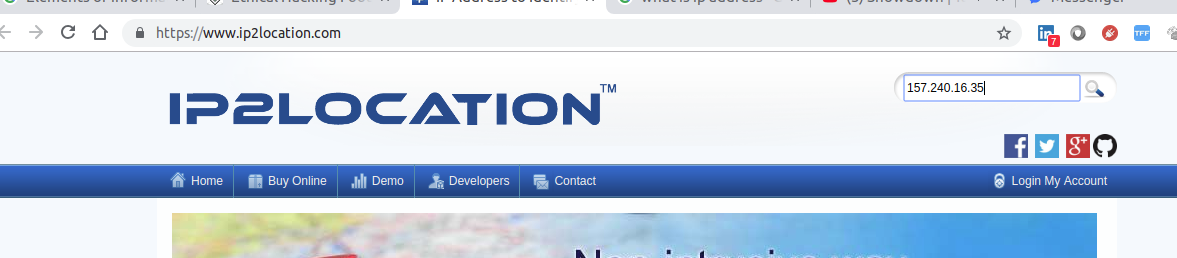
## It will produce the following result −

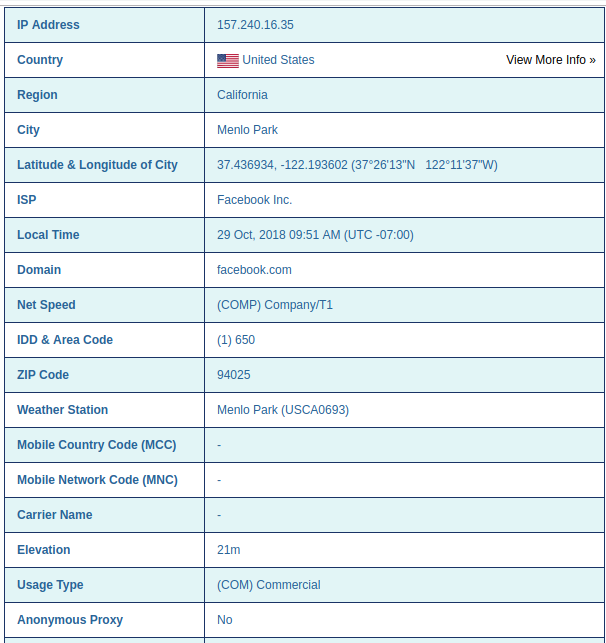
157.240.16.35 is the IP address of Facebook. If you type this to your browsers url and hit enter it will connect to [www.facebook.com](http://www.facebook.com)

# Finding Hosting Company

## Once you have the website address, you can get further detail by using ip2location.com website. Following is the example to find out the details of an IP address −

## Type the ip address of facebook and hit search





# Quick Fix

## If a computer system or network is linked with the Internet directly, then you cannot hide the IP address and the related information such as the hosting company, its location, ISP, etc. If you have a server containing very sensitive data, then it is recommended to keep it behind a secure proxy so that hackers cannot get the exact details of your actual server. This way, it will be difficult for any potential hacker to reach your server directly.

## Another effective way of hiding your system IP and ultimately all the associated information is to go through a Virtual Private Network (VPN). If you configure a VPN, then the whole traffic routes through the VPN network, so your true IP address assigned by your ISP is always hidden.

# IP Address Ranges

## Small sites may have a single IP address associated with them, but larger websites usually have multiple IP addresses serving different domains and sub-domains.

## You can obtain a range of IP addresses assigned to a particular company using [American Registry for Internet Numbers](https://www.arin.net/" \t "/home/deepto/Documents\\x/_blank) <https://www.arin.net/>



You can enter company name in the highlighted search box to find out a list of all the assigned IP addresses to that company.

# History of the Website

## It is very easy to get a complete history of any website using <https://web.archive.org/>



## You can enter a domain name in the search box to find out how the website was looking at a given point of time and what were the pages available on the website on different dates.

# Quick Fix

Though there are some advantages of keeping your website in an archive database, but if you do not like anybody to see how your website progressed through different stages, then you can request archive.org to delete the history of your website.

# Summery:

## Footprinting is the part of information gathering. You can use various tools to gather precious information about website. If you want to protect your network you have to work like a hacker also you have to see what a hacker can see so that you can ensure the security of your network.

## Domain name information: <https://www.whois.com/whois>

## Finding IP Address: open command prompt or terminal and type “ $ping websiteName.com” $

## Finding Hosting Company: <https://www.ip2location.com/>

## IP Address Ranges: <https://www.arin.net/>

## History of the Website: <https://archive.org/>