- **Information gathering:**

Security Assessment (IT Security Assessment) is an explicit study to locate IT security vulnerabilities and risks. The goal is to study security and identify improvements to secure the systems. An assessment for security is potentially the most useful of all security tests. The first phase in security assessment is focused on collecting as much information as possible about a target application. Information Gathering is a necessary step of a penetration test. This task can be carried out in many different ways.

Information gathering or foot-printing is generally a first step of Ethical hacking/penetration testing process. The more information you have the more chance of success, information gathering is the important phase because all of the process of hacking based on information that you have. By using public tools (search engines), scanners, sending simple HTTP requests, or specially crafted requests, it is possible to force the application to leak information, e.g., disclosing error messages or revealing the versions and technologies used.

An assessment can start by using some form of an information gathering tool. When assessing the entire network, map the layout first to find the hosts that are running. Once located, examine each host individually. Focusing on these hosts requires another set of tools. Knowing which tools to use may be the most crucial step in finding vulnerabilities.Just as in any aspect of everyday life, there are many different tools that perform the same job. This concept applies to performing vulnerability assessments as well. There are tools specific to operating systems, applications, and even networks (based on the protocols used). Some tools are free; others are not. Some tools are intuitive and easy to use, while others are cryptic and poorly documented but have features that other tools do not.

Finding the right tools may be a daunting task and in the end, experience counts. If possible, set up a test lab and try out as many tools as you can, noting the strengths and weaknesses of each. Review the README file or man page for the tool. Additionally, look to the Internet for more information, such as articles, step-by-step guides, or even mailing lists specific to a tool.

Effective information gathering can:

• utilise your time more efficiently and effectively

• develop critical thinking through the use of sifting/sorting techniques

• broaden your outlook and inform your subject understanding through the exploration of more diverse sources

Information gathering can be used for a variety of different reasons; however, the main benefit with regards to your academic studies is that you will become aware of more diverse sources, opinions and approaches which can only enhance your academic work.

The most critical phases or investigation processes revolve around the accessibility of various online resources such as:

- Internet Service Registration – The global registration and maintenance of IP address information
- Domain Name System – Local and global registration and maintenance of host naming
- Search Engines – The specialist retrieval of distributed material relating to an organisation or their employees
- Email Systems – The information contained within each email delivery process
- Naming Conventions – The way an organisation encodes or categorises the services their online hosts provide
- Website Analysis – The information intentionally made public, that may pose a risk to security

There are many ways to gather information. Some of them are:

- Info Gathering using blogs & forums.
- Info Gathering using search Engine and tools
- Info Gathering using Meta tags & Words.
- People Search (social engineering)
- Info gathering using job, matrimonial websites.

Blogs and forums are the best medium to gather information about something. Forums and blogs are the hacker friendly sites. They share any information about new technologies and hacking tips. An Internet forum, or message board, is an online discussion site where people can hold conversations in the form of posted messages. A blog is a personal journal published on the World Wide Web consisting of discrete entries typically displayed in reverse chronological order so the most recent post appears first. Blogs are usually the work of a single individual, occasionally of a small group, and often are themed on a single subject. Almost 80% internet users use blogs or forums for knowledge sharing purpose. Information gathering from specific blog will also helpful in investigations.

Search engines are efficient mediums to get specific results according to your requirements. There are many search engines to gather information out of which mostly used search engines are:

- Google
- Yahoo
- Kartoo
- Maltego
- MSN live
- Baidu
- Bing
- AOL
- Ask
- whitepages.com
- wink.com
- peekyou.com
- yoname.com

There are many online based tools. We can get the IP, DNS, OS details using these websites. Some of them are:

- Whois.net
- Samspade.org
- Domaintools.com
- Dnsreports.com
- Network-tools.com
- Netcraft.com
- dnsstuff.com

Today most of the people are using social networking websites. We can use these websites too to gather information. Of them the most famous are:

- Facebook
- Orkut
- LinkedIn
- Twitter
- Myspace
- Google Plus
- Deviantart
- Tagged
- Badoo