1. Introduction to Cyber World :

- **Introduction:**

Science is one of the greatest blessings in modern life. Scientific advancement has led to many important inventions. One of them is the computer. About a decade back, a computer was seen as a wonder machine. A few years later, this wonderful machine came closer to us as the Personal Computer (PC) entered the household scene.

The computer today plays a significant role in everybody's life. Computers are used practically everywhere. The use of computer in our country in the past two decades has taken a big jump. Today computers do much more than simply compute, super market scanners calculate our grocery bill while keeping store inventory; computerized telephone switching centers play traffic cop to millions of calls and keep lines of communications untangled, and Automatic Teller Machines (ATM) let us conduct banking transactions from virtually anywhere in the world.

Computers will never be able to replace man as they need detailed instructions from man and can never lead independent lives. In the Armed Forces computers are being widely used for collecting complex data for the aircrafts, missile and guns. The radar system is controlled with complex computers to give early warnings of coming enemy unit. Computers are also being widely used in mass communication and medical science.

Today the police have started storing data on crimes and criminals on computers. Computers now have become a need of the day, in modern life. They are being used in every field of work. Due to importance of computer, its knowledge has been thought an essential qualification for a job. No doubt computers are capable of doing everything, but it is falling short of thinking. This is still only reserved form of man. So here computers are only machines; it cannot compete with man though they have overcome him in many ways.

- **Information Security:**

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

- **Introduction to Hacking:**

Computer hacking is the most popular form of hacking nowadays, especially in the field of computer security. The Hacking word is basically known as “Unauthorized” access to a protected system. Hacking is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose. The person who is consistently engaging in hacking activities, and has accepted hacking as a lifestyle and philosophy of their choice, is called a hacker. Due to the mass attention given to black hat hackers from the media, the whole hacking term is often mistaken for any security related cyber crime. This damages the reputation of all hackers, and is very cruel and unfair to the law abiding ones of them, from who the term itself originated. Hacking means finding out weaknesses in a computer or computer network, though the term can also refer to someone with an advanced understanding of computers and computer networks. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge.

Computer crime refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Hacking refers to criminal exploitation of the Internet. Cybercrimes are defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation's security and financial health. Issues surrounding this type of crime have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise.

Hacking means finding out weaknesses in a computer or computer network, though the term can also refer to someone with an advanced understanding of computers and computer networks.

- **<u>Communities of Hackers:</u>**

There are many communities out of them the most popular are:

1) Hacker
2) Cracker
3) Script Kiddie
4) Phreakers

- **<u>Hackers:</u>**

The term "hacker" originally meant a very gifted programmer. In recent years though, with easier access to multiple systems, it now has negative implications. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge. The subculture that has evolved around hackers is often referred to as the computer underground but it is now an pen community. While other uses of the word hacker exist that are not related to computer security, they are rarely used in mainstream context. They are subject to the long standing hacker definition controversy about the true meaning of the term hacker.

- **<u>Cracker:</u>**

Cracking is the act of breaking into a computer system, often on a network. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there. Some breaking-and-entering has been done ostensibly to point out weaknesses in a site's security system. The term hacker is reclaimed by computer programmers who argue that someone breaking into computers is better called a cracker, not making a difference between computer criminals (black hats) and computer security experts (white hats). Some white hat hackers claim that they also deserve the title hacker, and that only black hats should be called crackers.

- **Script Kiddie:**

A script kiddie or skiddie, is a derogatory term used to describe those who use scripts or programs developed by others to attack computer systems and networks and deface websites. It is also used to describe those who do the previous, but do not have an understanding of programming or computer networks. The more immature but unfortunately often just as dangerous exploiter of security lapses on the Internet. The typical script kiddy uses existing and frequently well known and easy-to-find techniques and programs or scripts to search for and exploit weaknesses in other computers on the Internet—often randomly and with little regard or perhaps even understanding of the potentially harmful consequences.

- **Phreakers:**

Phreaking is a slang term coined to describe the activity of a culture of people who study, experiment with, or explore telecommunication systems, such as equipment and systems connected to public telephone networks. As telephone networks have become computerized, phreaking has become closely linked with computer hacking.

- **Types of hackers:**
  There are some more classified versions of hackers. They are:

- **White Hat:** A white hat hacker is someone who has non-malicious intent whenever he breaks into security systems and whatnot. In fact, a large number of white hat hackers are security experts themselves who want to push the boundaries of their own IT security ciphers and shields or even penetration testers specifically hired to test out how vulnerable or impenetrable a present protective setup currently is. A white hat that does vulnerability assessments and penetration tests is also known as an ethical hacker.
- **Black Hat:** A black hat hacker, also known as a cracker, is the type of hacker that has malicious intent whenever he goes about breaking into computer security systems with the use of technology such as a network, phone system, or computer and without authorization. His malevolent purposes can range from all sorts cybercrimes such as piracy, identity theft, credit card fraud, vandalism, and so forth. He may or may not utilize questionable tactics such as deploying worms and malicious sites to meet his ends.
- **Grey Hat:** A grey hat hacker is someone who exhibits traits from both white hats and black hats. More to the point, this is the kind of hacker that isn't a penetration tester but will go ahead and surf the Internet for vulnerable systems he could exploit. Like a white hat, he'll inform the administrator of the website of the vulnerabilities he found after

hacking through the site. Like a black hat and unlike a pen tester, he’ll hack any site freely and without any prompting or authorization from owners whatsoever. He'll even offer to repair the vulnerable site he exposed in the first place for a small fee.

- **Phases of Hacking:**

There are five phases of hacking. They are:

1) Information Gathering or Reconnaissance
2) Network Scanning
3) Gaining Access
4) Maintaining Access
5) Clearing Tracks

- **Reconnaissance:**

Before hacking a ‘Online business or corporate infrastructure’, hackers first perform routine and detailed reconnaissance. Hackers must gather as much information about your business and networks as possible. Anything they discover about their target (you) can be valuable during their attack phases. Strategies for hacking rely on a foundation of knowledge and understanding, arising initially from whatever the hacker can learn about you and your business. Methods of reconnaissance include Dumpster Diving, Social Engineering, Google Searching & Google Hacking, and work their way up to more insidious methods such as infiltrating your employee’s environments from coffee shops to simply walking in and setting up in a cubicle and asking a lot of questions. Whatever methods are used to perform reconnaissance, hackers will usually collect a large amount of information varying from trivial to sensitive, all of which may be useful during their attacks.

- **Network Scanning:**

Probing a network can reveal vulnerabilities that create a hit list, or triage list, for hackers to work through. Hackers may be either general hackers or specialized hackers, such as phreakers, but their intent is majorly the same to access information and services that they should not gain access to. Much of the information gather during the hacker’s reconnaissance phase now come into play. In many ways, this phase of network scanning is an extension of the reconnaissance phase. Hackers want to learn more about your network mapping, phone system structure, and internal informational architecture. Learning what routers, firewalls, IDS systems, and other network components exist can lead hackers to beneficial hacking information by researching known vulnerabilities of known network devices. Typically, hackers perform port scans and port mapping, while attempting to discover what services and versions of services are actively available on any open or available ports. Regardless of how secure a network may feel to the business operator and network administrator, there is great value in remaining paranoid and to maintain continual logging and analysis, always looking for potential intrusion. Once complacency makes its way into your business operations, it's only a matter of time before vulnerability becomes an exploit.

- **Gaining Access:**

Open ports can lead to a hacker gaining direct access to services and possibly to internal network connections. This phase of attack is the most important and the most dangerous. Although some hack attacks don't need direct network access to damage your business, such as Denial of Services (DoS), simple methods of attack are available to network-connected hackers including session hijacking, stack-based buffer overflow, and similar security exploits. Smurf attacks try to get network users to respond and the hacker uses their real IP Addresses to flood them with problems. Whether the hacker is successful attacking an internal system has much to do with how vulnerable the specific system is, which is related to system configurations and architecture. Even if only one of one hundred network users has a vulnerability, it could lead to an exponential increase in network exploit through distributed Zombie software and internal denial of service attacks. The degree and scope of attack depends much on the level of access the hacker gains and their skill level.

- **Maintaining Access:**

Hackers may choose to continue attacking and exploiting the target system, or to explore deeper into the target network and look for more systems and services. Not all attackers remain connected to the exploited network, but from a defensive strategy it must be expected. Hackers may deploy programs to maintain access by launching VNC clients from within your network, providing access to external systems, opening Telnet sessions and similarly serious services like FTP and SSH, or upload rootkits and Trojans to infiltrate and exploit your network and systems to the point where they have complete root level control. Hackers can continue to sniff your network looking for more information to use against you. Trojans can export sensitive information to hackers, such as credit card records, usernames and passwords. Efficiently maintained access to your network and systems can last years without detection. Maintained access allows hackers the benefits of time to collect the information they need for the purpose of their attack. Although some hackers simply seek fame, other seek fortune. Those that seek the latter will likely leverage sensitive information into direct theft, resale of internal information, using internet information to improve their profitability, or even leveraging your company into paying them directly. Intrusion detection Systems (IDS), Honeypots/Honeynets, and professional ethical security consultation can be employed to detect and defend against hackers and their exploits.

- **Clearing Tracks:**

Most hackers will attempt to cover their footprints and tracks as carefully as possible. Although not always the case, remove proof of a hacker's attacks is their best defense against legal and punitive action. It is most likely that low-end hackers and newbie hackers will get caught at a much higher rate than expert level hackers who know how to remain hidden and anonymous. Gaining root level access and administrative access is a big part of covering one’s tracks as the hacker can remove log entries and do so as a privileged administrator as opposed to an unknown hacker. Placing programs inside your network to continually send sensitive information out to anonymous drop-off points allows hackers to cover their tracks while maintaining access. Steganography allows hackers to hide information inside objects that are not obvious, such as image headers and meta tags. Tunneling allows hackers to perform their insidious work through one service that is carried over another service, to increase the difficulty of finding them.

These five phases of a hacker’s attack loop back to the beginning. A successful attack with maintained access often results in continuing reconnaissance. The more the hacker learns about your internal operations means the more likely he will be back to intrude and exploit more networks, systems, internal services, and your business resources. As scary as all of these phases and attacks sound, there are tools and methods available to detect, track, expunge, and defend against future attacks for network security professionals. Knowing what tools are available and which to use in the appropriate situations are simply one small aspect of network security consultation. There is a difference between Operating System Hacks, Application-Level Hacks, Shrink Wrap Code Hacks and Attacks on Misconfigured Systems.