CYBERSECURITY COURSE

INTRODUCTION TO CYBER CRIME

The internet was born around 1960‟s where its access was limited to few scientist, researchers and the defense only. Internet user base have evolved exponentially. Initially the computer crime was only confined to making a physical damage to the computer and related infrastructure.

Around 1980‟s the trend changed from causing the physical damaging to computers to making a computer malfunction using a malicious code called virus. Till then the effect was not so widespread because internet was only confined to defense setups, large international companies and research communities. In 1996, when internet was launched for the public, it immediately became popular among the masses and they slowly became dependent on it to an extent that it have changed their lifestyle.

Every second around 25 computer became victim to cyber-attack and around 800 million individuals are affected by it till 2013. CERT-India have reported around 308371 Indian websites to be hacked between 2011-2013. It is also estimated that around $160 million are lost per year due to cyber-crime. This figure is very conservative as most of the cases are never reported.

Before discussing the matter further, let us know what the cyber-crime is?
The term **cyber-crime** is used to describe a unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal activity.

Course objectives:

- To understand various types of cyber-attacks and cyber-crimes
- To learn threats and risks within context of the cyber security
- To have an overview of the cyber laws & concepts of cyber forensics
- To study the defensive techniques against these attacks

Introduction to Cyber Security

Cyber Security Introduction - Cyber Security Basics:
Cyber security is the most concerned matter as cyber threats and attacks are overgrowing. Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT or non-IT firms have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

What is cyber security?
"Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

Why is cyber security important?
Listed below are the reasons why cyber security is so important in what’s become a predominant digital world:

- Cyber-attacks can be extremely expensive for businesses to endure.

 In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
 Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber-attacks.

Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

Cyber security Fundamentals –

Confidentiality:

Confidentiality is about preventing the disclosure of data to unauthorized parties.
It also means trying to keep the identity of authorized parties involved in sharing and holding data private and anonymous.
Often confidentiality is compromised by cracking poorly encrypted data, Man-in-the-middle (MITM) attacks, disclosing sensitive data.
Standard measures to establish confidentiality include:
 Data encryption
 Two-factor authentication
 Biometric verification
 Security tokens

Integrity

Integrity refers to protecting information from being modified by unauthorized parties.
Standard measures to guarantee integrity include:
 Cryptographic checksums
 Using file permissions
 Uninterrupted power supplies
 Data backups

Availability

Availability is making sure that authorized parties are able to access the information when needed.
Standard measures to guarantee availability include:
 Backing up data to external drives
 Implementing firewalls
 Having backup power supplies
 Data redundancy

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.
Cyber-attacks can be classified into the following categories:

1) Web-based attacks

2) System-based attacks

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

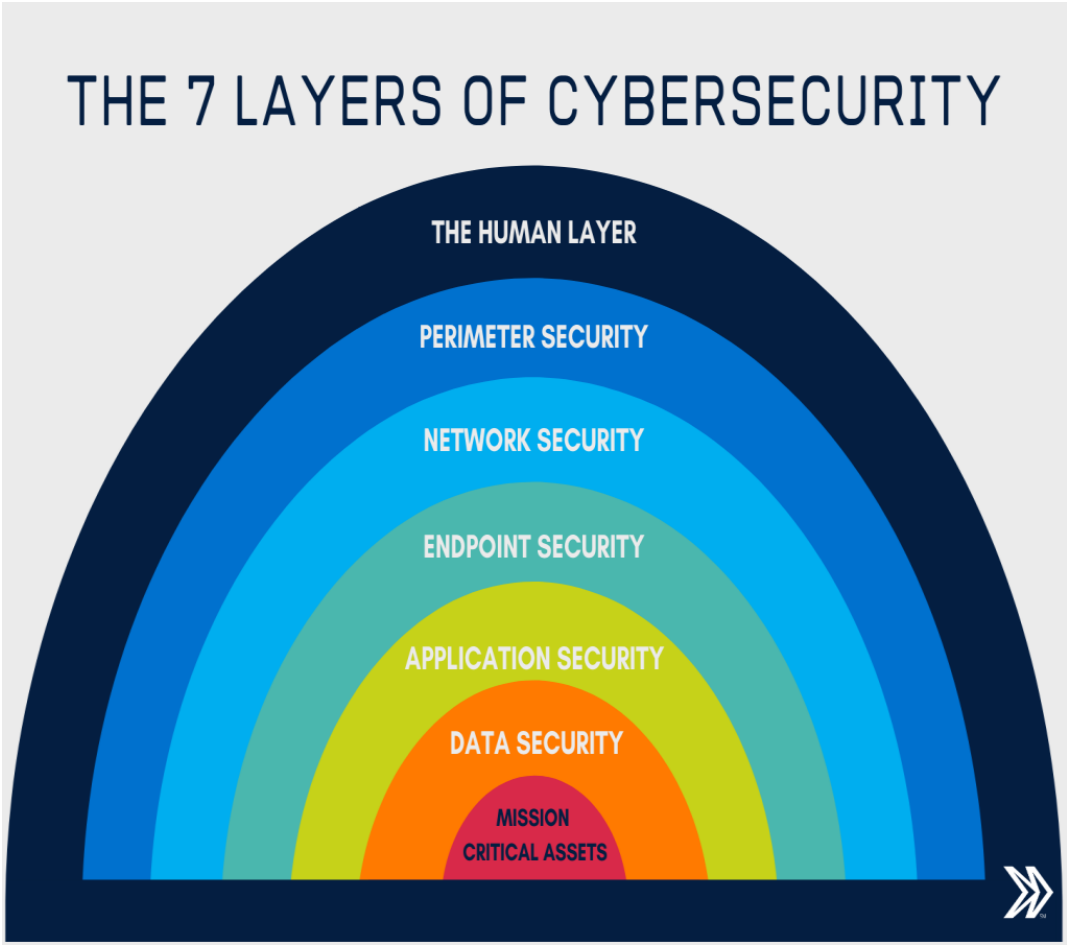
2. DNS Spoofing

DNS spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker’s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking
It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.
4. Phishing
Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.
5. Brute force
It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.
6. Denial of Service
It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-
Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.
Protocol attacks- It consumes actual server resources, and is measured in a packet.
Application layer attacks- Its goal is to crash the web server and is measured in request per second.
7. Dictionary attacks
This type of attack stored the list of a commonly used password and validated them to get original password.
8. URL Interpretation
It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.
9. File Inclusion attacks
It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.
10. Man in the middle attacks
It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.
System-based attacks
These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

1. Virus
It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.
2. Worm
It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.
3. Trojan horse
It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors
It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.
5. Bots
A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chartroom bots, and malicious bots.



Security Policies:
Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information.
A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.
We use security policies to manage our network security. Most types of security policies are automatically created during the installation. We can also customize policies to suit our specific environment.
Need of Security policies-
1) It increases efficiency.
2) It upholds discipline and accountability
3) It can make or break a business deal
4) It helps to educate employees on security literacy

There are some important cyber security policies recommendations describe below-
Virus and Spyware Protection policy:

It helps to detect threads in files, to detect applications that exhibits suspicious behavior. Removes, and repairs the side effects of viruses and security risks by using signatures.

Firewall Policy:

- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals and removes the unwanted sources of network traffic.

Intrusion Prevention policy:

- This policy automatically detects and blocks the network attacks and browser attacks.
- It also protects applications from vulnerabilities and checks the contents of one or more data packages and detects malware which is coming through legal ways.

Application and Device Control:

- This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system.
- The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

Who are the enemies and How Cyber Attacks Happen?

Hackers

This generic term applies to computer fans who take pleasure in gaining access to other people's computers or networks. Many hackers are content with simply breaking in and leaving their "footprints," which are joke applications or messages on computer desktops. Other hackers, often referred to as "crackers," are more malicious, crashing entire computer systems, stealing or damaging confidential data, defacing Web pages, and ultimately disrupting business. Some amateur hackers merely locate hacking tools online and deploy them without much understanding of how they work or their effects.

Unaware Staff

As employees focus on their specific job duties, they often overlook standard network security rules. For example, they might choose passwords that are very simple to remember so that they can log on to their networks easily.

However, such passwords might be easy to guess or crack by hackers using simple common sense or a widely available password cracking software utility. Employees can unconsciously cause other security breaches including the accidental contraction and spreading of computer viruses. One of the most common ways to pick up a virus is from emails or by downloading files from the Internet. Corporations also face the risk of infection when employees download files, such as PowerPoint presentations, software, emails from the Internet. Surprisingly, companies must also be wary of human error. Employees, whether they are computer novices or computer savvy, can make such mistakes as erroneously installing virus protection software or accidentally overlooking warnings regarding security threats.

Snoops

Whether content or disgruntled, some employees might also be curious or mischievous. Employees known as "snoops" partake in corporate espionage, gaining unauthorized access to confidential data in order to provide competitors with otherwise inaccessible information. Others are simply satisfying their personal curiosities by accessing private information, such as financial data, a romantic e-mail correspondence between associates, or the salary of a colleague. Some of these activities might be relatively harmless, but others, such as previewing private financial, patient, or human resources data, are far more serious, can be damaging to reputations, and can cause financial liability for a company.

Point-of-Sale (POS) Intrusions

"Restaurants, hotels, grocery stores, and other brick and mortar retailers are all potential targets" of POS intrusions. As far as the means of attack, the first step is to compromise the POS device to allow the installation of malware designed to collect magnetic strip data from credit cards as they are processed. The next step is to retrieve the data and use it for financial gain. According to recent research, almost all POS attacks can be attributed to "organized criminal groups operating out of Eastern Europe", their shared motive being monetary gain.

Web App Attacks

The web applications as "the proverbial punching bag of the Internet", making web app attacks the most common type of data breach. As to the methods used by those with malicious intent, weaknesses in the application, such as inadequate input validation, are exploited through the use of malware, phishing techniques and just plain guessing at the user's personal information. Stolen credentials are also used to gain access by impersonating a valid user.

Insider and Privilege Misuse

The unapproved or malicious misuse of organizational resources—primarily valuable intellectual property—by individuals working on the inside is a very real and ongoing threat for organizations. Such breaches can be very difficult to prevent, since the majority of insider misuse. Examples closer to home for most businesses

Physical Theft and Loss

With all of the sophisticated safeguards companies put into place to mitigate cyber threats, the theft of physical devices that store, process, or transmit information remains a very real risk for businesses. Surprisingly, employee carelessness and human nature as the root causes of device loss. "Accidents happen. People lose stuff. People steal stuff. While employees should be encouraged to keep better track of their gadgets, and recommends that companies back up their data and make sure that all devices are encrypted.

Miscellaneous Errors

Miscellaneous Errors and Omissions (E&O) covers the errors made while providing professional services. These errors can arise from negligence, faulty materials, and simply disagreements over the end result. A Miscellaneous E&O policy is tailored to professionals that have different than normal risks. A typical E&O policy is designed for lawyers, architects, accountants, etc. But a Miscellaneous policy is used to cover professions such as advertising agencies, appraisers, photographers, teachers, and many more.

Crime ware

The "crime ware" covers a broad range of malware related activities, such as stealing an online user's banking credentials, spamming, mounting DoS attacks, and other illicit actions. Web downloads and drive-by infections—wherein viruses can be inadvertently downloaded when unsuspecting users click on deceptive pop-up windows—are stated in the report as the most common ways of infecting a system. Keeping software such as browsers up to date is a recommended practice to combat "crimeware" attacks.

Attacks

Innumerable types of network attacks have been documented, and they are commonly classified in three general categories: reconnaissance attacks, access attacks, and denial of service (DoS) attacks.

Reconnaissance attacks

Active reconnaissance is a type of computer attack in which an intruder engages with the targeted system to gather information about vulnerabilities. Both active and passive reconnaissance are also used for ethical hacking, in which white hat hackers use attack methods to determine system vulnerabilities so that problems can be taken care of before the system falls prey to a real attack.

Access attacks
There are four types of access attacks: password attacks, trust exploitation, port redirection and man-in-the middle attacks.
A Network attacker uses packet sniffer tools to obtain user accounts and passwords information. Normally we log in and out of a system using authentication passwords to shared resources in a router or server, an attacker also repeatedly attempts to log in to a shared resource or to gain unauthorized access to an organization's network; this can also be referred to as dictionary or brute force attacks

Trust exploitation attacker is to compromise a trusted host, using it to stage attacks on other hosts in a network. If a host in a network of a company is protected by a firewall (inside host), but is accessible to a trusted host outside the firewall (outside host), the inside host can be attacked through the trusted outside host

A port redirection attack is another type of attack based on trust exploitation. The attacker uses a compromised host to gain access through a firewall that would otherwise be blocked

A man-in-the-middle (MITM) attack is implemented by intruders that manage to position themselves between two legitimate hosts. The attacker may allow the normal communication between hosts to occur, but manipulates the conversation between the two

Spam is the commonly used term for unsolicited electronic mail or the action of broadcasting unsolicited advertising messages via e-mail. Spam is usually harmless, but it can be a nuisance, taking up the recipient's time and storage space.

Cyber security Tools

After the potential sources of threats and the types of damage that can occur have been identified, putting the proper security policies and safeguards in place becomes much easier. Organizations have an extensive choice of technologies, ranging from vulnerability scanners, anti-virus software packages to dedicated network security hardware, such as firewalls and intrusion detection systems, to provide protection for all areas of the network.

Vulnerability scanners

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.
Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

Nessus - For security practitioners who assess complex enterprise networks for security flaws and compliance issues, Nessus is the world's most widely-deployed vulnerability and configuration assessment product.
OpenVAS - OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution.

Forensic

FTK Imager - FTK is a court-accepted digital investigations platform that is built for speed, analytics and enterprise-class scalability. FTK Imager supports storage of disk images in EnCase's or SMART's file format, as well as in raw (dd) format. The toolkit also includes a standalone disk imaging program called FTK Imager. The FTK Imager is a simple but concise tool. It saves an image of a hard disk in one file or in segments that may be later on reconstructed.

Sans Investigate Forensic Toolkit (SIFT) - The SIFT Workstation is a VMware appliance, pre-configured with the necessary tools to perform detailed digital forensic examination in a variety of settings. It is compatible with Expert Witness Format (E01), Advanced Forensic Format (AFF), and raw (dd) evidence formats.

Penetration Testing

A penetration test is a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky end-user behavior.
Software:

Steps to reduce cyber risk

Information Risk Management Regime

 Determine your risk appetite. Decide on the level of risk the organisation is prepared to tolerate and communicate it.

 Establish an effective governance structure and determine your risk appetite - just like you would for any other risk. Maintain the Board's engagement with the cyber risk. Produce supporting information risk management policies.

 Produce supporting risk management policies.

Network Security

 Monitor. Use intrusion monitoring tools and regularly audit activity logs.

 Test the security controls. Conduct regular penetration tests and undertake simulated cyber-attack exercises.

 Filter out unauthorised access and malicious content.

Managing User Privileges

 Monitor all users Monitor user activity, particularly access to sensitive information and the use of privileged accounts.

 Control access to activity and audit logs.

 Establish account management processes and limit the number of privileged accounts.

Malware Prevention

 Establish anti-malware defences across the organisation.

 Develop and publish corporate policies to manage the risks to the business processes from malware.

 Scan for malware across the organisation.

Removable Media Controls

 Limit the use of removable media types that can be used together with user and system access and the information types that can be stored on removable media.

Secure Configuration

 Apply security patches and ensure that the secure configuration of all ICT systems is maintained.

 Create a system inventory and define a baseline build for all ICT devices.

 Create and maintain hardware and software inventories.

User Education and Awareness

 Produce user security policies covering acceptable and secure use of the organisation's systems.

 Establish a staff training programme. Maintain user awareness of the cyber risks.

Monitoring

 Monitor all ICT systems. Ensure that the solution monitors all networks and host systems (eg clients and servers).

 Analyse logs for unusual activity that could indicate an attack.

Home and Mobile Working

 Educate users and maintain their awareness about the risks and train them to use their mobile device securely by following the security procedures.

 Protect data both in transit and at rest.

 Develop a mobile working policy and train staff to adhere to it.

Incident Management

 Establish an incident response and disaster recovery capability with clear roles and responsibilities.

 Regularly test your plans.

 Provide specialist training

3.1 INTRODUCTORY PRINCIPLES OF LAW AND LEGAL RESEARCH

Cyber security practitioners and researchers come from an incredibly wide array of educational backgrounds. Experience teaching legal and regulatory subjects to cyber security postgraduate students, and providing legal advice to cyber security practitioners, suggests that much of this knowledge area's content will be novel to those whose education is based in science, technology, engineering, mathematics, many social sciences, and many of the humanities. These introductory observations are offered as an aid for those who are approaching the subject without significant experience.

3.1.1 The nature of law and legal analysis

Although the reader is assumed to have some degree of familiarity with the process of law making and law enforcement, a review of some of the most common sources of law should help to orient those who are unfamiliar with legal research and analysis.

Law should be analyzed with rigorous logic. Unlike scientific disciplines such as physics or mathematics, however, the study of law is not conceptualized as an effort to discover immutable principles of our world. Law is bound together with social and political values, human desire, and human fragility.

Society influences the development and interpretation of law even as law influences the behavior of members of society. Societies evolve and values change. Changes to law and to methods of interpreting law tend to follow. This creates a number of challenges for legal scholarship, as the topic under study continues to change.[11] Perhaps as a result the study of law is often presented in the form of historical dialectic: examining the evolution of law and its interpretation over time, often through case studies. This method provides all-important context, aids in the interpretation of law as it exists, and often suggests the direction of future developments.

Distinguishing criminal and civil law

3.1.3.1 Criminal law

Criminal law is the body of law that prohibits behaviour generally abhorred by society. Criminal law is normally enforced by an agency of the state. Examples include prohibitions against bank fraud and computer hacking. Depending upon the society in question, the purposes of criminal law are usually described as some combination of:

• deterrence (seeking to deter bad behaviour, for both members of society generally and a criminal speci_cally);
• incapacitation (limiting the ability of the criminal to further harm society);
• retribution (causing a criminal to suffer some type of loss in response to crime);
• restitution (causing a criminal to compensate a victim or some related person);
• rehabilitation (seeking to change the long-term behaviour of a criminal).

Terms such as 'guilty' and 'innocent' are normally reserved as descriptions of verdicts (outcomes)
in a criminal case. These terms should not be used when referring to outcomes of civil actions.

Civil (non-criminal) law

Civil law[31] is the area of law that regulates private relationships among and between persons. Examples include the laws of contract and negligence. A person injured as a result of breach

of civil law can normally bring legal action against the responsible party.
Remedies available under civil law (depending on the circumstances)may include some combination of:
• an order for the liable party to pay compensation to the injured party;
• an order to terminate some legal relationship between the parties;
• an order for the liable party to discontinue harmful activity; or
• an order for the liable party to take some type of af_rmative act (e.g., transferring ownership of property).