IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

UNVEILING THE HACKERS' METHODOLOGY: EXPLORING CYBER CRIMES, CYBER LAWS AND PUNISHMENT

***The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable. — The Art of War,* Sun Tzu**

[1] Bandu B. Meshram
[1]Chairman,
[1] Jeman Educational Society, Sector 14, Airoli, Navi Mumbai
Maharashtra State (India)

[2] Manish Kumar Singh,
[2] Assistant Professor
[2], NIMS, School of Law. NIMS University
Rajasthan, Jaipur(India)

Abstract :This research introduces the vital areas of cyber information world having computer systems, language processors, web based applications and TCP/IP, networking which are commonly exploited by cyber criminals to carry out cyber-attacks. By drawing an analogy between a criminal's plan for a bungalow robbery and the activities of attackers targeting computing machines, the hacker's methodology is elucidated to enhance the understanding of stakeholders involved in cyber space. Cyber crimes can be perpetrated against individuals, organizations, government computing infrastructure and society at large. The impact of various attacks includes communication interruption, interception, information modification and fabrication. Moreover, the study extensively investigates TCP/IP attacks, meticulously categorizing them into probing, Denial Of Service Attacks (DOS), Remote-to-User Attacks (R2L), User-to-Root Attacks (U2R), and covers various attack types within each category. Additionally, it meticulously addresses the top 10 OWASP attacks projected for 2023, further enhancing the understanding of emerging vulnerabilities & threats. The profound impact of cybercrimes extends to the disruption of communication, stealing intellectual property and tampering of critical information, defamation and the infiltration of counterfeit elements into computing systems. In response to these challenges, cyber jurisprudence endeavours to establish robust legal frameworks aimed at regulating and safeguarding diverse aspects of cyberspace, combatting cybercrimes, and upholding digital rights by means of imprisonment and fine. This comprehensive work not only sheds light on prevalent cybercrimes but also explores the criminal investigation procedures employed to tackle cyber offenses, along with an examination of the pertinent cyber laws in India. It delves into the governing provisions outlined by the Indian Evidence Act of 1872 and outlines the corresponding punishments delineated within the Information Technology Act of 2000 and the Indian Penal Code. While the research offers an extensive list of cybercrimes and their associated punishments, it is essential to recognize that these are general guidelines derived from Indian law, subject to potential variations based on specific circumstances and the provisions of relevant statutes and court rulings. A holistic comprehension of these aspects is paramount to ensuring the protection of individuals, businesses, societal well-being, and national security as a whole.

Keywords: Cyberspace, Systems Programs, TCP/IP Stack, Cybercrimes, Cyber Laws & Punishment

1. INTRODUCTION

In an increasingly digital world, the rise of cybercrimes has become a significant concern globally. India, being one of the largest digital economies, is no exception. Cyber-crimes are offences relating to computers and their components, information technology, multimedia data temper, database, application on internet, IOT, mobiles, social media, networks, cloud computing and virtual reality and information technology assets. Cyber attacks are made against integrity, Availability & confidentiality of Network assets and services from associated threats and vulnerabilities. An asset is something to which an organization assigns value and hence for which it requires protection. Information technology cyberspace assets are

- **Hardware:** servers, client stations, communication devices(router, bridge etc),
- **Software**: Network and client operating systems, applications, tools
- **data/information**: organization data(database, email,), network data(network configurations, settings, user access privileges, password, user data, user owned files etc.

Threat (cyber attack) is anything that could cause damage/harm/loss to assets. Threats are damage to communication lines ,deterioration of storage media, hardware failure ,malicious software ,misuse of resources ,unauthorized access, theft, staff shortage, fire, misrouting or rerouting of messages, , use of network, facilities in an unauthorized way and physical threats are flood, lightning, earthquake, power fluctuation extreme temperature and humidity.

Vulnerability is weakness associated with assets. The weakness may be exploited by threats causing loss/damage/harm to the assets .A vulnerability in itself does not cause harm until exploited but it is caused due to various reasons like insufficient security training, lack of security awareness, inadequate recruitment procedures, insufficient preventive maintenance, ,unprotected public network connections , poor password management, well known flaws in the software, unsupervised work by outside staff, lack of security policies ,unprotected communication lines ,poor cable joint ,firewall is bypassed, gateway is bypassed, inadequate network management and lack of audit-trail and security measures.

Ethical hacking is a defensive tool that can be applied before an attack occurs to uncover vulnerabilities in information systems and network security and provide the basis for remediation of these weaknesses. Ethical hacking is also known as penetration testing or white-hat hacking, involves the same tools, tricks, and techniques that hackers use, but with one major difference that Ethical hacking is legal. Active attacks are security attacks that involve direct interaction with the target system or network infrastructure. Unlike passive attacks, active attacks aim to modify, disrupt, or destroy data or system components. These attacks are more noticeable as they actively interfere with the normal functioning of the system.

Passive attacks are security attacks that aim to gather information or data from a target system or network without altering or disrupting its normal functioning. Unlike active attacks, passive attacks do not involve direct interaction with the target system. Instead, they focus on covertly intercepting and observing data transmissions. As the digital landscape continues to evolve, cybercrimes pose a significant threat to individuals, businesses, and national security. The Indian government has taken proactive steps by enacting cyber laws and establishing punishment frameworks to combat these crimes effectively. However, raising awareness, promoting digital literacy, and strengthening cybersecurity infrastructure are crucial in safeguarding against cyber threats... The German State of Hesse enacted 1st computer specific law in the form of 'Data Protection Act, 1970' To regulate the cybercrimes Indian parliament passed its "Information Technology Act, 2000" to have its exhaustive law to deal with the technology in the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes.

The paper is organized as follows. Section 2 provides an overview of the cyber information world, including computer systems, language processors, cyber terminologies, the TCP/IP stack, and vulnerabilities that contribute to cyber-attacks. It also discusses the impact of cyber crime on computer assets. In Section 3, the focus is on Indian acts applicable to cyber crimes, such as the Criminal Procedure Code of 1973 for investigating cybercrime, the Evidence Act of 1872, the Information Technology Act of 2000, and the Indian Penal Code of 1860.Section 4 delves into the Proposed cyber hackers methodology, drawing an analogy between a criminal's plan for a bungalow robbery and the activities of attackers targeting computer systems. Section 5 involves a legal and diagnostic research on cybercrimes and punishment, specifically addressing cybercrimes against individuals, organizations, and society. It also explores advanced attacks related to TCP/IP Stack Attacks and the top 10 OWASP attacks 2023 . discussing the corresponding punishments as outlined in the IT Act and IPC. Additionally, it covers some special cyber-attacks and their associated punishments. In Section 6, the research focuses on information security and the modification of cyber laws, particularly the IPC and Cr.PC, in response to evolving cybercrimes.

2. The Cyber Information World

This section explores the components of the computing systems on which attacks can be made by the attacker.

2.1 What are Computer Systems?

A Computer is an electronic device capable of performing commands. The basic commands that a computer performs are input (get data), output(display result), storage, and performance of arithmetic and logical operations. The physical components of a computer, including the central processing unit (CPU), and control unit, memory (RAM), storage devices (hard drive, solid-state drive), input devices (keyboard, mouse), output devices (monitor, printer), and other peripherals

Central Processing Unit : The Central Processing Unit (CPU) is the brain of the computer and the single most expensive piece of hardware in a personal computer. The more powerful the CPU, the faster is the computer. There are mainly three components of a CPU: (i) The control unit (CU) has three main functions: fetch and decode the instructions, control the flow of information (instructions and data) in and out of main memory, and control the operation of the CPU's internal components. (ii)The Arithmetic Logic Unit (ALU) carries out all arithmetic and logical operations (iii)Registers: The CPU contains various registers. Some of the registers are for special purposes. For example, the instruction register (IR) holds the instruction currently being executed. The Program Counter (PC) points to the next instruction to be executed. All registers provide temporary storage. The computer hardware as shown in figure 1

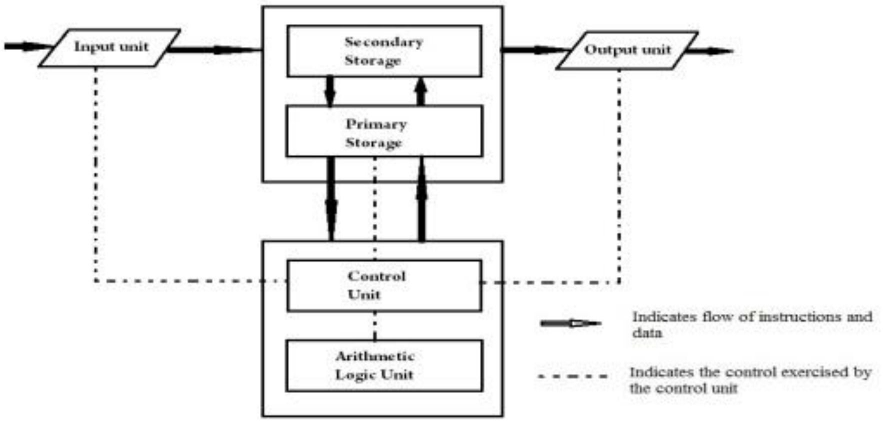
Input unit
Secondary Storage
Output unit
Primary Storage
Control Unit
Arithmetic Logic Unit
Indicates flow of instructions and data
Indicates the control exercised by the control unit

Figure 1 Block Diagram of a Computer

Main Memory (Random Access Memory): The main memory (Primary Memory) is directly connected to the CPU. All programs must be loaded into main memory before they can be executed. Similarly, all data must be brought into main memory before a program can manipulate it. When the computer is turned off, everything in main memory is lost for good. The main memory is an ordered sequence of cells, called memory cells. Each cell has a unique location in main memory, called the address of the cell. These addresses help you access the information stored in the cell. Today's computers come with main memory consisting of millions to billions of cells. The memory addresses can be expressed as sequences of 0s and 1s.

Secondary Storage: Because programs and data must be stored in main memory before processing and because everything in main memory is lost when the computer is turned off, information stored in main memory must be transferred to some other device for permanent storage. The device that stores the information permanently is called secondary storage. Examples of secondary storage are hard disks, flash drives, floppy disks, ZIP Disks, CD-ROMs, and tapes.

Input/output Devices: For a computer to perform a useful task, it must be able to take in data and programs and display the results of calculations. The devices that feed data and programs into computers are called input devices. Keyboard, Mouse are examples of input devices. The devices that the computer uses to display results are called output devices. A monitor, printer and secondary storage are examples of output devices.

2.2 SOFTWARE

Software is program written to perform specific tasks. All software's are written in programming languages. There are two types of programs: system programs and application programs. System programs control the computer. The system program that loads first when you turn on your PC is called the operating system. The operating system is a program which when executed control the overall operation of the computer systems. Some of the services include processor management, memory management, device management input/output activities, and storage management. The operating system has a special program that organizes secondary storage so that you can conveniently access information. Database Management System (DBMS) is collection of programs that enables users to create and maintain a database and facilitates the processes of defining, constructing, manipulating, and sharing databases among various users and applications. OS, DBMS, Compiler, assembler, loaders are the examples of systems programs. Application programs perform a specific task. Word processors, spreadsheets, and games are examples of application programs. **Computer Languages**: Programming languages that allow humans to write instructions for computers. Examples include high-level languages like Python, Java, C++, and low-level languages like assembly language and machine code.

2.3 LANGUAGE PROCESSORS

Pre-processor- First of all, the source program is fed into the pre-processor and the output of the pre-processor is modified source program. The task of collecting the source program is given to a separate program called a pre-processor. The pre-processor also expands shorthand's, called macros, into source language statements. The Modified source program is fed into compiler as shown in figure 2

Compiler- It is a program which translates a high level language program into a machine language program known as assembly language. Then the target assembly program is fed into assembler.

Assembler- A program which translates an assembly language program into a machine language program is called an assembler. The output generated by Assembler is fed into linker/loader. Usually a longer program is divided into smaller subprograms called modules. And these modules must be combined to execute the program. The process of combining the modules is done by the linker.

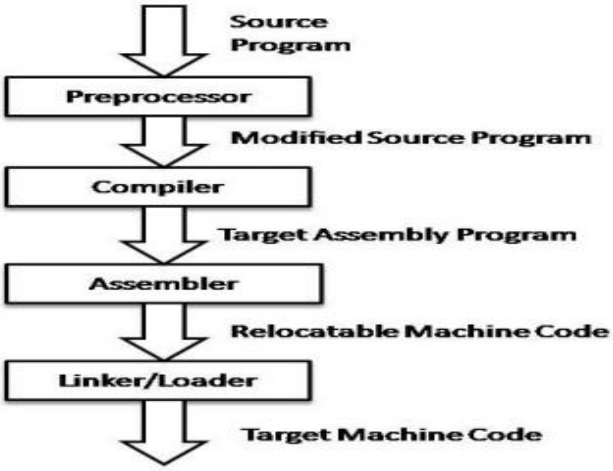

Figure 2 A language Processing Systems

Loader- Loader is a program that loads machine codes of a program into the main memory. In Computing, a loader is the part of an Operating System that is responsible for loading programs. It is one of the essential stage in the process of starting the execution of a program. Because it places programs into memory and prepares them for execution. Loading a program involves reading the contents of executable file into memory. Once loading is complete, the operating system starts the program by passing control to the loaded program code. All operating systems that support program loading have loaders. In many operating systems the loader is permanently resident in memory. Finally the machine code loaded into the memory is ready for execution. The complete process of the source program getting converted to the stage of execution is shown in figure 1.2. The memory is managed by operating systems.

Operating Systems: An operating system is the most important software that runs on a computer. It manages the computer's memory, processes, and all of its software and hardware. It also allows you to communicate with the computer. An Operating System is a collection of programs that act as an interface between machines hardware and users providing users with a set of facilities and maintenance of programs and at the same time controlling the allocation of resources to cause efficient operation. Its primary objective is to improve the performance and efficiency of a computer system and increase facility by providing functions of resource management, processor management, memory management, information management, device management Job management, I/O management, Data management, Security, communication of error, and control messages to the users etc. hence it is called as resource manager.

A Data Structure and algorithms : Data structure is a set of domains D, (field of thought and action), a set of functions F and the set of axioms A (Self-evident truth – reserved word or syntax). An algorithm is a procedure (a finite set of well-defined instructions) for accomplishing some task which, given an initial state, will terminate in a defined end-state. The computational complexity and efficient implementation of the algorithm are important in computing, and this depends on suitable data structures.

Networking: The ability of computers to connect and communicate with each other, enabling data sharing, collaboration, and access to resources over local area networks (LANs) or the internet using TCP/IP embedded into operating systems.

2.3 Cyber World

Internet: The internet is a global network of interconnected computer networks with a vast infrastructure comprising millions of interconnected devices, servers, routers, and other networking components. The internet facilitates numerous services and applications, such as email, web browsing, instant messaging, file sharing, online gaming, and video streaming

World Wide Web: The World Wide Web (WWW) is an information system invented by Sir Tim Berners-Lee in 1989 that allows users to access and navigate interconnected documents ,and collection of web pages, websites, multimedia content, and other online resources that are linked together through hyperlinks

URL /Web Addresses: Web addresses, is known as Uniform Resource Locators (URLs), are unique identifiers used to locate and access specific resources on the internet. A URL consists of multiple components.

Protocol: It indicates the communication protocol used to access the resource, such as "http://" or "https://" for web pages, "ftp://" for file transfers, or "mailto://" for email addresses.

Domain Name: It identifies the specific website or server hosting the resource. For example, in "www.jes.com," "jes.com" is the domain name.

R**Path**: It represents the specific location or directory within the website where the resource is located. For example in , www.jes.com/education /indexpage.html in "/education /indexpage.html" is the path. URLs are used by web browsers to retrieve and display the requested web page or resource. They provide a standardized way to access various types of content on the internet.

Intranet: an intranet is a private, internal network that functions similarly to the internet but is accessible only to a specific organization, such as a company, educational institution, or government agency to facilitate internal communication such as file sharing, document management, employee directories, internal messaging systems, and access to internal tools and applications , and information sharing within the organization.

Cyberspace/ Cyber World: Cyberspace refers to the virtual environment created by computer systems, networks, and the internet. Cyberspace is not limited to a specific physical location but exists in the interconnected world of digital information. It encompasses online platforms, websites, social media, cloud services, and other digital platforms where users can exchange information, engage in transactions, and access digital resources. It represents the interconnectedness of individuals, organizations, and devices through the internet. The cyber world includes various aspects such as online communities, virtual marketplaces, digital economies, online education, social networks, and other virtual environments where people interact, collaborate, and engage in diverse activities.

Web Browser: A web browser is a software application that allows users to access, retrieve, and view information on the World Wide Web. It acts as an interface between users and the internet, enabling them to navigate websites, view web pages, interact with online content, and perform various tasks. Popular web browsers include Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, and Opera. Web browsers interpret and display HTML (Hypertext Mark-up Language) documents, execute scripts, handle multimedia content, and provide features such as bookmarks, tabbed browsing, and extensions.

Cyber Jurisprudence: Cyber jurisprudence refers to the legal principles, theories, and frameworks that govern the use of technology, particularly in relation to cyberspace and the internet. It encompasses the study of laws, regulations, and policies that address the rights, responsibilities, and liabilities of individuals, organizations, and governments in the digital realm

2.4 TCP/IP Stack

Networks have layered architecture and interconnecting devices which communicate via myriad of protocols as shown in figure 3 and figure 4.The complexity of the network gives rise to various weaknesses which when not secured efficiently becomes target for intrusion and attacks.

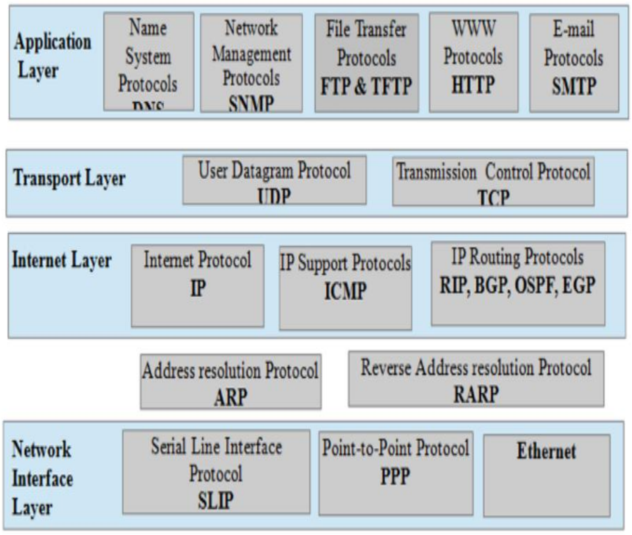
Application Layer
Name System Protocols DNS
Network Management Protocols SNMP
File Transfer Protocols FTP & TFTP
WWW Protocols HTTP
E-mail Protocols SMTP
Transport Layer
User Datagram Protocol UDP
Transmission Control Protocol TCP
Internet Layer
Internet Protocol IP
IP Support Protocols ICMP
IP Routing Protocols RIP, BGP, OSPF, EGP
Address resolution Protocol ARP
Reverse Address resolution Protocol RARP
Network Interface Layer
Serial Line Interface Protocol SLIP
Point-to-Point Protocol PPP
Ethernet

Figure 3. TCP/IP Protocol Suite

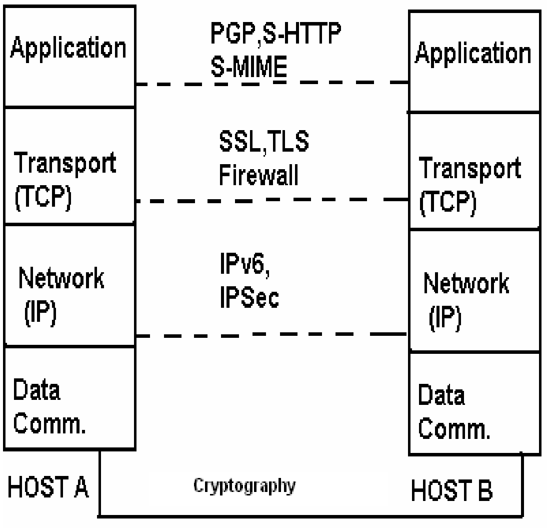

Figure 4. TCP/IP Stack Security.

The TCP/IP model is based on a five-layer model for networking. From bottom (the physical) to top (the user application), these are the physical, data link, network, transport, and application layers. The application layer in TCP/IP is equivalent to session, presentation and application layer in OSI model. Many protocols are defined at this layer such as SMTP, FTP, HTTP. DNS etc. At the transport layer, TCP/IP defines three protocols: Transmission Control protocol (TCP), User Datagram protocol (UDP) and Stream Control Transmission Protocol (SCTP). Most Internet services use a protocol called Transmission Control Protocol (TCP), which is layered on top of IP, and provides virtual circuits by splitting up the data stream into IP packets and reassembling it at the far end, asking for repeats of any lost packets. At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP), although there are some other protocols that support data movement in this layer. Data link layer uses protocols defined by the underlying networks. Local networks mostly use Ethernet, in which devices have unique Ethernet addresses, which are mapped to IP addresses using the Address Resolution Protocol (ARP). There are many other components in the protocol suite for managing communications and providing higher-level services.

Security mechanism on TCP/IP Stack is shown in figure 2 using security protocols on every layer of TCP/IP suit , still the cyber criminal can make the attacks on communication channel and resources.

3. INDIAN ACTS APPLICABLE IN CYBER CRIMES

The Criminal Procedure Code (CrPC) primarily deals with the procedural aspects of criminal cases and cybercrimes in India. Additionally, specific provisions and procedures under the Information Technology Act, 2000, and its subsequent amendments also apply to cybercrime investigations in India. Secondly there are several sections within the Indian Penal Code (IPC), which is the substantive law governing criminal offenses, that cover various cyber crimes. The digital evidence admissibility is governed by The Evidence Act 1872.

3.1 The Criminal Procedure Code (Cr.PC), 1973

The Criminal Procedure Code (CrPC) primarily deals with the procedural aspects of criminal cases in India, including those related to cybercrimes. When it comes to investigating cyber crimes, the police administration follows a specific procedure outlined in the CrPC and other relevant laws. Here is a general overview of the procedure adopted by the police administration to investigate cyber crimes:

Receipt of Complaint: The police administration receives a complaint or FIR (First Information Report) related to a cybercrime. The complaint can be filed by the victim, a witness, or any person with knowledge of the offense.

Registration of FIR: If the preliminary investigation reveals a cognizable offense, the police register an FIR. The FIR contains details of the offense, the parties involved, and other relevant information. It initiates the formal investigation process. The registration of an FIR (First Information Report) for a cybercrime in India typically falls under the provisions of the Information Technology Act, 2000, specifically Section 154 of the Code of Criminal Procedure (Cr.PC). Section 154 of the Cr.PC governs the registration of an FIR for various offenses, including cybercrimes. When an individual wants to report a cybercrime, they can approach the concerned police station and provide the details of the offense. The police are legally obligated to register an FIR upon receiving a complaint or information about a cognizable offense under Section 66 of the Information Technology Act. when reporting a cyber crime, it is advisable to mention both the provisions sect 154 CrPC & Section 66 of IT Act.

Preliminary Investigation: The police conduct a preliminary investigation to gather initial information regarding the cybercrime. They may interview the complainant, collect relevant evidence, and assess the nature and severity of the offense. Police can use Section 2 of the Code of Criminal Procedure for a cognizable offence and Section 154 of the Criminal Procedure Code As per IT Act -. Sec 78 Power to investigate offences. -Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of [Inspector] shall investigate any offence under this Act.

Procedure for Search and Seizure of Electronic Evidence: In cybercrime cases, the police may seize electronic devices such as computers, laptops, mobile phones, or storage media to preserve digital evidence. They follow the legal procedures for seizure, maintain the chain of custody, and ensure the integrity of the seized devices. The Section 93 of the CrPC, "mandates for a magistrate to issue a search warrant for any 'document or thing' also warrant for general search in the area only for the purpose of investigation". However, "Section 100 of the CrPC prerequisites search for a closed place, also it mandates a prior approved warrant for search and a witness at the searched premises. As per The Indian Evidence Act 1872, s 3.- "If any officer-in-charge feels that it would be time-consuming in acquiring a warrant and the evidence shall be lost then the officer can search the premises without a warrant.

Forensic Analysis in forensic laboratory: The seized electronic devices are sent to forensic laboratories for analysis. Forensic experts examine (section sec 45 and 45A The evidence Act) the devices to extract and analyse digital evidence, including files, communications, logs, metadata, and other relevant information. This analysis helps in establishing the facts of the case and identifying the perpetrators.

Collection of Witness Statements: The police administration collects statements from witnesses, victims, and individuals with relevant knowledge of the offense. The police administration can invoke Section 161 of the CrPC to collect statements from witnesses, victims, or any person with relevant knowledge of the offense. Section 161 of the CrPC is a general provision applicable to the investigation of all criminal offenses, including cyber crimes.These statements provide additional evidence and support the investigation. It was decided in the case of *State of Maharashtra v Dr. Praful B. Desai* [2003] 4 SCC 601. that, "evidence recorded through video-conferencing is legal as interpreted under Section 273 of the CrPC.

Tracking Digital Footprints: The police trace the digital footprints left by the offender, such as IP addresses, email accounts, social media profiles, or other online activities. Section 3 of the Evidence Act talks about evidence and includes electronic evidence. "Electronic record is a piece of documentary evidence. The police officer (IT Act -. Sec 78) may collaborate with Internet Service Providers (ISPs), cyber forensic experts or other agencies to gather this information(The evidence Act -Sec 45, 45A & 46). The collaboration between police officers and Internet Service Providers (ISPs) for cyber crime investigations in India is primarily governed by Section 91 of the Code of Criminal Procedure (CrPC) and Section 69B of the Information Technology (IT) Act, 2000. In the context of cyber crime investigations under Section 91 of the Cr.PC, the police may approach ISPs to obtain subscriber information, IP logs, access logs, or communication records, or any other relevant data that can assist in identifying and apprehending cyber criminals. Under Section 69B,IT Act, authorized agencies & forensic laboratories by Indian government, including the police, can seek cooperation from ISPs to to intercept, monitor, or decrypt information generated, transmitted, received, or stored in any computer resource related to cybercrimes.

Suspect Identification and Arrest: Based on the evidence gathered, the police identify and locate the suspects involved in the cybercrime. They follow legal procedures to effect arrests, if required, and present the suspects before the appropriate judicial authority. The identification and arrest of a cyber criminal in India is primarily governed by the provisions of the Code of Criminal Procedure (CrPC)- Section 41 of the CrPC and the Information Technology (IT) Act, 2000.-Section 75 of the IT Act, 2000. When the police have identified a suspect involved in cyber crimes covered under the IT Act, including unauthorized access or hacking, they can proceed with the arrest under Section 41 of the CrPC, while taking into account the provisions of Section 75 of the IT Act for determining the specific offense and punishment.

Case Documentation and Charge sheet: The police prepare a comprehensive investigation report, including all the collected evidence, witness statements, and forensic analysis reports. This report forms the basis for the charge sheet, which is filed in court, outlining the charges against the accused. The preparation of a comprehensive investigation report, including evidence, witness statements, and forensic analysis reports, is governed by the provisions of the Code of Criminal Procedure (CrPC) in India. The specific sections are as follows:

Section 173 of the CrPC : It requires the investigating officer to forward a report to the Magistrate, commonly known as the charge sheet or final report to the Magistrate ;

Section 207 of the CrPC: it requires to supply of copies of documents and statements to the accused.

The charge sheet includes all the relevant details and evidence gathered during the investigation, such as witness statements, forensic analysis reports, expert opinions, and any other supporting documents . The purpose of the charge sheet is to present a complete and accurate account of the investigation to the Magistrate or the court. It serves as the basis for further proceedings, including the trial, where the evidence is examined, arguments are presented, and a verdict is reached.

Judicial Proceedings: The case proceeds to the judicial stage, where the court examines the evidence, hears arguments from both sides, and delivers a verdict. The court takes into account the provisions of the relevant cybercrime laws , IT Act , The evidence Act, the Indian Penal Code, The specific relief Act and other applicable statutes.

3.2 Indian Evidence Act 1872

The Indian Evidence Act, 1872 does not specifically have sections dedicated to cybercrime. However, certain sections of the Evidence Act are applicable in the context of cybercrime investigations and trials. In the context of cybercrimes, The Evidence Act 1872 can be used to establish the admissibility of electronic records, computer-generated evidence, and expert opinions related to digital evidence. It helps establish the authenticity, ensure fairness, accuracy, integrity, and reliability in the presentation and evaluation of electronic evidence in court. Some of the sections related to cybercrimes and electronics evidence are as below:

Section 3: Interpretation Clause: This section defines several terms used throughout the Act, including "evidence," "document," "electronic record," and "computer."

Section 17. Admission defined.—. This section states that Admission as to the genuineness of electronic records . It states that if a person accepts the electronic record as being genuine, then it may be admitted as evidence.

Section 22A specifies that oral admissions made by a person about the contents of electronic records may be relevant in certain situations.

Section 45A.—When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000 (21 of 2000), is a relevant fact. For the purposes of this section, an Examiner of Electronic Evidence shall be an expert (sec 45). This section allows for the opinion of an examiner of electronic evidence (sec 45A) , such as a digital forensic expert, to be admissible in court.

Section 46 Facts, not otherwise relevant, are relevant if they support or are inconsistent with the opinions of experts, when such opinions are relevant.

Section 47: This section deals with the opinion of the court on the existence of certain facts. In cases involving cybercrime, where the court has to form an opinion on the authenticity or integrity of electronic evidence, this section may be relevant.

Section 65A..The contents of electronic records may be proved in accordance with the provisions of section 65B.

Section 65B lays down the requirements for the admissibility of electronic records as evidence. It specifies the conditions that must be met, such as certification and ensuring the integrity of the electronic record.

Section 73A deals with the proof as to verification of digital signatures on chain of custody and use of digital signatures for authentication and verification of electronic records preserved under chain of custody.

Section 79A establishes a presumption regarding the authenticity and integrity of electronic records and digital signatures, subject to certain conditions.

Section 85A. The Court shall presume that every electronic record purporting to be an agreement containing the [electronic signature] of the parties was so concluded by affixing the [electronic signature] of the parties. Chain of custody refers to the chronological documentation of who handled digital image, what they did with it, how did they obtain digital evidence and where they preserved it. In all chain of custody, the judge can rule the evidence inadmissible. Chain of custody forms the forensic link of evidence sequence of control, transfer, and analysis to preserve evidence's integrity and to prevent its contamination."

Section 85B. Presumption as to electronic records and [electronic signatures]. In The requirements that a Chain of Custody in digital forensic model process should have (1) Integrity (2) Traceability. (3)Authentication (5)Verifiability (5) Security. It should be achieved by digital signature and . These parameters are protected by section 85. The researcher proposes that The correctivity of the information in the chain of custody shall be checked by court by digital signature and electronics signature certificate.

Section 85C. Presumption as to [Electronic Signature Certificates]. The digital evidence in the enforcement of a digital agreement or contract, the digital signature is required. Digital forensic done by the external party with government digital forensic lab is digital agreement or contract , Chain of custody must be digitally signed. Digital signature is explored in Section , 3 and 3 A, 4, 5, and 6. Of Information Technology Act 2000.

Section 114: deals with the presumption of fact. It allows the court to draw certain inferences based on the available evidence. In the context of cybercrime, this section may be used to draw inferences regarding the authenticity, integrity, or reliability of electronic evidence

It's important to note that the interpretation and application of these sections in digital forensic investigations can vary depending on the specific circumstances, case law, and any relevant guidelines or regulations that may be in place.

3.3 Information Technology Act, 2000 (ITA , 2000) with ITA 2008.

"The digital forensic process model, its chain of custody, and electronic evidence are governed with respect to Sections 3, 3A, 4, 5, and 6.

Section 3**.** Authentication of electronic records states that any subscriber may authenticate an electronic record by affixing his digital signature and the authentication of the electronic record is made using asymmetric crypto system and hash function.

Section 3A. Electronic signature explore that a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique Section 4. Legal recognition of electronic records, Section 5. Legal recognition of electronic signatures. Section 6. Use of electronic records and [electronic signatures] in Government and its agencies.

To properly understand, please read Section 3, Section 3A, Section 4, Section 5, and Section 6 of the IT Act in conjunction with Section 85A, Section 85B, and Section 85C of the Evidence Act.

Read section 3 and 3 A, 4, 5, and 6. of IT Act in consonance with Section 73A ,sec 85A, 85B,& 85C of Evidence Act.

Section 43, Section 43A, Section 66, Section 66A, Section 66 B, C, D, Section 66 E, Section F, Section 67 of Information Technology Act, 2000 deals with punishment related to digital forensics.

Section 43 Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008) If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network **-** (a) accesses or secures access to such computer, computer system or computer network or computer resource (ITAA2008) (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; (e) disrupts or causes disruption of any computer, computer system or computer network; (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder, (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, (i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means (ITAA-2008) (i) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, (ITAA 2008) **he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.** (change vide ITAA 2008**)**

Section 43 A Compensation for failure to protect data (ITAA 2006) Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected.

Section 65 Tampering with Computer Source code Documents: Whoever knowingly or intentionally conceals, destroys or alters or intentionally causes another to conceal, destroy or alter any computer source code shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Section 66 Computer Related Offences (Substituted vide ITAA 2008) If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both.

Section 66 A Any person who sends **offensive messages through communication service, etc** by means of a computer resource or a communication device or by email any information that is grossly offensive or has menacing character; or false for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to two three years and with fine.

Section 66 B Punishment for dishonestly receiving stolen computer resource or communication device shall be imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66C Punishment for identity theft Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66 D Punishment for cheating by personation by using computer resource (Inserted Vide ITA 2008) Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E. Punishment for violation of privacy. (Inserted Vide ITA 2008) Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Section 66F. Punishment for cyber terrorism Whoever, knowingly or intentionally penetrates or accesses a restricted computer resource without authorisation or exceeding authorized access, and by means of such conduct with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by

(1)(A) (i) cause the denial of access; or (ii) access a computer resource without authorisation or exceeding authorized access; or (iii) introducing any Computer Contaminant. and likely to cause death or injuries to persons or destruction to cause damage or adversely affect the critical information infrastructure specified under section 70, or (B) obtains access to restricted information, data or computer database likely to cause, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism. (2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

Section 67 Punishment for publishing or transmitting obscene material in electronic form (Amended vide ITAA 2008) Whoever publishes or transmits or causes to be published in the electronic form, any lascivious, prurient interest material or if its effect is such as to tend to deprave and corrupt persons shall be punished on first conviction with imprisonment of either description for a term which may extend to two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Section 67 A Punishment for publishing or transmitting of material containing sexually explicit act,etc. in electronic form (Inserted vide ITAA 2008) Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form. Whoever,- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or (d) facilitates abusing children online or (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception: The section 67 and 67A does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form is in the interest of science, literature, art, or learning or other objects of general concern or (ii) which is kept or used for confide heritage or religious purposes.

3.4 The Indian Penal Code 1850

Amendments to the IPC to cover cyber-crimes*:* The Indian legislature has from time to time, made a number of amendments to the IPC by linking it with the various section in the IT Act to specifically cover cyber-crimes. Some of the important sections amendments are as follows:

- section 29A define "electronic record" , section 4(3) of the IPC - *extra territorial offences* "without and beyond India*",;*
- in sections 118 and 119 of the IPC -the words *"*voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design*" were inserted.* in section 464 of the IPC- phrase "digital signature" was replaced with the phrase "electronic signature" in all places and the phrase "affixing electronic signature" was given the same meaning as it has under the IT Act;
- "electronic record" was included within the ambit of sections 164, 172, 173, 175, 192, 204, 463, 466, 468, 469, 470, 471, 474 and 476 of the IPC. and in section 466 of the IPC the term "register" was defined to include any list, data or record of any entries maintained in an "electronic form", as defined in section 2(1) (r) of the IT Act;

Based on the interpretation of various sections of IT Act 2000 and IPC and court decisions, various sections for cybercrime under IPC are listed as below though may not be specified explicitly in the act.

- ***Obscenity*** sections 292 and 294 of the IPC would also be applicable for offences described under sections 67, 67A and 67B of the IT Act .Section 292 of IPC governs various cybercrimes such as the publication and transmission of obscene material or sexually explicit act in electronic form. Section 292 is imbibes the imprisonment and fine up to 2 years and Rs. 2000. If such cyber crimes are committed for the second time, the imprisonment could be up to 5 years and the fine could be maximum extend to Rs. 5,000.
- **Voyeurism** :Section 354C of IPC governs the cybercrime which deals with capturing or publication of a picture of private parts or acts of a woman without such person's consent and watching it--'voyeurism.' Section 292 of IPC(essential is gender) and Section 66E of IT Act, 2000 is broad enough to take the offenses The punishment voyeurism' includes 1 to 3 years of imprisonment for first-time offenders and 3 to 7 years for second-time offenders.
- **Cyber Stalking'** :Section 354D of IPC: The punishment for ' cyber stalking' offense is imprisonment extending up to 3 years for the first time and for the second time 5 years along with a fine imposed in both the instances.
- **Hacking And Data Theft** :Section 378 of the IPC will apply to the theft of any data, online ie hacking and data theft**.** The maximum punishment for theft under section 378 of the IPC is imprisonment of up to 3 (three) years or a fine or both. Sections 43 and 66 of the IT Act also penalise for ***hacking and data theft*** The maximum punishment for the above offences is imprisonment of up to 3 (three) years or a fine or Rs. 5,00,000 (Rupees five lac) or both. Section 379 of IPC: deals with data theft and the punishment for data theft is imprisonment for 3 years or fine or both. .
- ***Stolen On Line Cyber Assets****: The cyber crime receipt of stolen property fall under* Section 66B of the IT Act and Section 411 of the IPC. According to Section 411 of IPC presents that If anyone receives a stolen mobile phone, computer, or data as a crime under Section 379, then accordance with Section 411 of IPC, the punishment can be imposed in the form of imprisonment which can be extended up to 3 years or fine or both. As per Section 66B of the IT Act and Section 411 of the IPC, the imprisonment is the either description for a term of up to 3 (three) years, or with fine, or with both. Please note that the only difference in the prescribed punishments is that under the IPC, there is no maximum cap on the fine.
- **Cyber fraud** :Section 419 and Section 420 of IPC deals with frauds like email phishing (Section 419 of IPC). password theft & the creation of bogus websites for fraud (Section 420 of IPC).Depending on the gravity of the committed cybercrime, Section 419 carries a punishment up to 3 years of imprisonment or fine and Section 420 carries up to 7 years of imprisonment or fine.
- **Identity theft and cheating by personation*:*** Section 419 of the IPC prescribes punishment for 'cheating by personation' and criminal shall be punished with imprisonment of either description for a term which may extend to 3 (three) years or with a fine or with both without any cap on fine.
- **Data Theft** :Section 424 will also apply to data theft. The maximum punishment under section 424 is imprisonment of up to 2 (two) years or a fine or both.Section 425 of the IPC represent the cyber crime for damaging computer systems and denial of service or damaging computer systems and even denying access to a computer system access to a computer system. The maximum punishment for suc mischief as per section 426 of the IPC is imprisonment of up to 3 (three) months or a fine or both.
- **Cyber Forgery and cyber crime for the Purpose Of Cheating** :The provisions of sections 463, 465 and 468 of the IPC dealing with forgery and "forgery for the purpose of cheating", may also be applicable in a case of identity theft. Forgery/fraud has been defined in section 463 of the IPC .Section 465 of IPC states that In cyberspace, the forgery offenses like email spoofing and preparation of false documents are dealt with and punished under Section 465 is the imprisonment reaching up to 2 years or fine or both. Section 468 & section 420 IPC shall also prescribes punishment for cyber forgery of imprisonment of either description for a term which may extend to 7 (seven) years and also a fine. Section 468 of IPC: Cybercrimes such as email spoofing or the online forgery for committing cheating or other serious offenses The punishment is of seven years of imprisonment or fine or both. Section 469 of IPC presents the forgery for the purpose of defamation of a person through online, electronic forms, the criminal can be imposed with the imprisonment up to three years with fine.
- **Cyber crimes by Email or social media** :Section 500 of IPC deals with cybercrime of sending email for defamatory content or abusive messages and the imprisonment extends up to 2 years along with fine. Section 504 of IPC deals with any electronic form message or email or use of social media to threat, insult, or try to provoke another person with the intention of effecting peace, the punishment for such offense extends up to 2 years of imprisonment or fine or both. Section 506 of IPC amounts an offence of a person who tries to criminally intimidate another person through electronic means with respect ~~to~~ the life of a person, property destruction through fire or chastity of a woman, and punishment of imprisonment extended up to seven years or fine or both.
- **Modesty & privacy of a woman** :Section 509 of IPC can dealt with the electronic mode act having potential to harm the modesty of a woman & privacy of a woman and the punishment would be imprisonment of a maximum period of one year or fine or both.

3.5 The Specific Relief Act 1963

The Specific Relief Act is not directly tailored for cybercrimes; it can still be invoked in certain cases involving cybercrimes to seek appropriate relief like injunctions or specific performance orders. This action seeks to prevent further harm and protect the affected individual's rights. If the hacker violates the injunction, they can be held in contempt of court, leading to additional legal consequences. The Specific Relief Act, 1963 is a law in India that deals with providing specific remedies in civil matters, including the enforcement of rights and obligations arising from contracts hence it can be used in digital agreements or digital contracts.

4. Proposed Cyber Hackers Methodology

The process of legal and authorized attempts to discover and successfully exploit the computer system in an attempt to make the computer system more secure is called Ethical Hacking. The phases of ethical hacking, also known as penetration testing or white-hat hacking, typically follow a systematic approach to identify and address security vulnerabilities in a target system or network. An ethical hacker follows processes similar to those of a malicious hacker. Malicious Hacking referred in Section 3 and Section 66 of ITA is labelled as amongst the most serious of all cyber crimes

The hacker's methodology is described by in Table 1 showing the Analogy Between Bungalow Robbery And Hacking.

Table 1 **Ethical Hacking**

4.1 Criminals Plan For Bungalow Robbery	**4.2 Attackers Activities For Hacking Computing Machine**
Information 1. Information Gathering: building monitoring	**Phase 1: Recconanence**
Intruders watch a building to identify what time employees enter the building and when they leave. 1.Criminal make Friends to security and Supporting staffs, dogs on bungalow. 2.Criminal use to study the Surveillance System at the building 3.Criminal use to study timings of people coming to house, alarm systems ,Entry/exit points, doors, windows Systems, alert(burglar), Door locking and the like.	Recconanence is discovery of useful information to use in an attack.Hacker or ethical hacker collect following information about the computing machine; 1.Social Engineering to know about the network, computer assets, software and hardware 2.Security Provided, Monitoring Systems of the organization 3.Address space, namespace acquisition 4.Sniffing the network for IP address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. 5. Recconanence Tools are Nmap ,Google darks/google digging, maltego and the like.
2 Survey of the Bungalow	**Phase 2 Scanning**
Preparation is made for robbing house as below: Thieves choose targets according to visible signs. 1. Thieves do rehearsal to robe the house 2. Intruders see the probable opportunities-watchman sleeping, nobody in house, house is locked and its timings 3. Intruders decide Entry plan, Exit Plan from the house after robbery, 4. Team required tools or outsourcing for robbery. 5. Milkmen, Newspaper, Cloth Washing, Cloth Iron and their timing for entry and exit from home and many more	Scanning involves taking the information discovered during reconnaissance and using it to examine the network. Hackers are seeking any information that can help them perpetrate attack such as computer names, IP addresses, and user accounts. Attacker discover the following information during scanning: 1. Hidden plan , not to keep any traces of scanning 2.Port Scanning 3. Services provided by the machines 4. OS, DBMS, compilers , software's used by machine. 5. Vulnerability scanning of the machines. 6.Scanning Tools **are** Nexpose ,Wireshark ,Nessus ,Snort ,Super scan and Nbtscan 7 the like.

3. Gain Access in Bunga low	**Phase 3—Gaining Access**
Theft of 1.Moneys, 2.Goods 3. Jewelry etc.	Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access Into Machine. Gaining access means owning the system for the communication and transactions to exploit a local area network (LAN, either wired or wireless), local access to a PC, the Internet, or offline. 1.Attcks on Systems Program Like, DBMS, OS,TCP/IP, security protocols, routing Protocols, 2.Attacks on applications Programs and, data networks 3.Bypass Firewalls, IPS
4.**Maintain Access of House**	**Phase 4—Maintaining Access**
1.Make friendship with security and watchmen to do future theft. 2. Keep watch on bungalow for future theft	1.Access for future exploitation and attacks. 2.Hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits, and Trojans. 3.Once the hacker owns the system, they can use it as a base to launch additional attacks. The owned system is known to as a zombie system. **…**
5.Wipe out any evidence	**Phase 5—Covering Tracks**
1.Do not leave any evidence about finger prints, footprints or any other biometric symptoms. 2. Sometimes murder of the insider. 3.Thif do not leave any evidence at bungalow about them, depends how smart he is….	1.Attacker clears the traces of access. to avoid legal action 2.Hackers to remove evidence of hacking to avoid legal action. Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms And Firewall Logs.
Output result ..after all..	
Police /Court Case	**Digital Forensic Analysis**
1.Policing 2. Court case 3. laws used IPC, CrPC, Evidence Act , CPC Or any other act as per crime 3.Result and punishment	1.Identify who is responsible for the Attacks, 2. What type of Activities are performed by the attacker. etc. 3.Laws used IT Act as well as IPC, CrPC & Evidence Act 5. Proof in court and punishment. 6. Executive strategy for information security

For every cyber crime Section 67C ITA : Preservation and retention of information by intermediaries :Failure to preserve and retain information as required can result in imprisonment up to three years and/or a fine is applicable to produce it in the court of law by the digital forensic investigators and other Actors involve in chain of custody

5. Cyber Crimes and Punishment

This section explore three types of cyber crimes committed against individuals, organizations, and society, along with some important crimes in each category and punishment for each crime. It's important to note that the applicability and punishment for Cyber Crime would depend on the specific circumstances of the case, the impact of crime on assets, the evidence presented, and the interpretation of the law by the courts..

5.1 Cyber Crimes against an Individual

a) Identity Theft: Identity thieves usually obtain personal information such as passwords, ID numbers, credit card numbers or social security numbers, and misuse them to act fraudulently in the victim's name. These sensitive details can be used for various illegal purposes including applying for loans, making online purchases, or accessing victim's medical and financial data. This is Unauthorized use of personal information for fraudulent purposes. Various identity thefts are social security identity theft, medical identity theft, synthetic identity theft, child identity theft, tax identity theft and criminal identity theft etc. For example A criminal steals someone's identity to open bank accounts and make financial transactions by using phishing and social engineering attack.. Section 66C of the Information Technology Act, 2000, provides Punishment for imprisonment up to three years and/or a fine.

b) Cyber Harassment, This is also known as cyberbullying, trolling, flaming,: cyber aggression, cyberbullying, cyber-harassment, cyberhate, cybervictimisation.Online harassment can be defined as the use of information and communication technologies by an individual or group to repeatedly cause harm intentionally to another person using email or social media and instant messaging or through digital means . This may involve threats, embarrassment, or humiliation expressions of discriminatory attitudes and beliefs—such as sexism, racism, xenophobia, homophobia, transphobia or ableist prejudices, online sexual harassment, cyberstalking, and image based sexual abuse or other unwanted online conduct of a sexual nature, threatening or abusive messages, spreading rumours, or posting embarrassing photos or videos of someone. For women, The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, the PoSH Act, 2013 is enacted by India.

Punishment: Depending on the nature of the offense, charges can be filed under various sections of the Indian Penal Code (IPC), such as defamation, criminal intimidation, or stalking or any other law as below.

- criminal intimidation (Section 507 IPC):Punishment : term which may extend to two years of imprisonment.
- defamation (Section 499, IPC) and criminal intimidation :Section 503 of IPC :The offences under S. 499 and S. 503 are punishable with imprisonment which may extend to two years, and/or fine.
- personal harassment(Section 294 of IPC) :The offender would be liable for an imprisonment up to three years or with a fine or both.
- Section 354A of IPC punishes offence of sexual harassment with 3 years of imprisonment and/or fine.
- Vengeful posting of images or videos of rape victims is punishable with imprisonment which may extend to two years and fine under section 228a of IPC.
- IPC domestic mental harassment of women(Section 498A IPC) detainment upto to three years along with fine.
- The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, the PoSH Act, 2013, :Section 3(3) to (9) of the 1997 Act makes it an arrestable criminal offence for a person, without reasonable excuse, to breach an injunction prohibiting harassment issued as part of the civil remedy set out in section 3 Conviction may result in imprisonment for up to five years, or a fine, or both.
- The Protection from Harassment Act 1997, UK- Section 3(3) to (9)- imprisonment for up to five years, or a fine, or both.

c) Cyber Stalking: Cyberstalking is a offensive behaviour committed repeatedly and persistently following, monitoring, or harassing an individual online by the cyber criminal using email, social media, chat rooms, instant messaging or any other online media to harass the victim by targeted victim specifically k for reasons of anger, revenge or control. Cyberstalking can take many forms, including: harassment, embarrassment and humiliation of the victim causing distress, fear, or alarm, of obscene or threatening unwanted letters or phone calls, waiting or loitering around home or workplace, or following or watching, or interfering with, or damaging personal property carried out by any person. Cyberstalking often falls into four main types: vindictive, composed, intimate, and collective. Vindictive cyberstalking involves threats, composed cyberstalking involves annoyance and harassment, intimate involves exes or people infatuated with the victim, and collective involves a person being cyber stalked by a group of individuals.

For cyber stalking, Section 354D of the IPC provides for imprisonment up to three years and/or a fine.

The IT Act of 2008 does not directly deal with the offence of stalking. However the following sections of ITA 2008 shall be used for investigation and punishment for cyber stalking.

- Offence of stalking: Section 72. IT Act of 2008: punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
  - Publication or transmission of obscene content. Section 67 IT Act of 2008 punishment :imprisonment extending up to three years and fine for the first conviction and to five years and fine upon second conviction, the publication, transmission and causing of transmission of obscene content.
  - sexually explicit act':Section 67A punishable with imprisonment extending up to five years and fine for first conviction and to seven years and fine upon second conviction.
  - causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred :Section 66A of IT Act: shall be punishable with imprisonment for a term which may extend to three years and with fine

d)Financial Fraud: The Prince Waterhouse Coopers organization has defined cyber economic crimes as" an economic crime committed using computers and the internet and it includes distributing viruses, illegally downloading files, phishing and farming and stealing personal information like bank account details, credit card details and committing fraud against an individual through online platforms. The financial cybercrimes include cheating, credit card frauds, money laundering, forgery, online investment etc.

The word fraud is clearly defined in Section 7 , The Indian Contract Act 1872, Fraud defined. Section 25 IPC defines the world fraudulently. The IT Act 2000 deals with internet fraud and online investment frauds in Section 43(d),65 and 66.Depending on the specific offense, charges can be filed under sections of the IPC, such as cheating, criminal breach of trust, or forgery. Sections of the Indian Penal Code (IPC) that are commonly invoked in cases related to financial offenses: Cheating (Section 415-420 IPC), Criminal Breach of Trust (Section 405-409 IPC) and Forgery (Section 463-470 IPC). The specific charges filed would depend on the nature of the offense, evidence presented, and the interpretation of the law by the courts. Other related enactments are the Companies Act 2013 and the securities and the exchange board of India Act 1992.

e)SMS Spoofing: is a blocking through spam which means the unwanted uninvited messages. Or SMS spoofing refers to the act of sending text messages with a falsified sender identity to deceive or mislead the recipient. Section 66D, ITTA 2008 offense of cheating by personation using a computer resource or electronic communication device. The punishment for this offense is as follows :First Conviction: Imprisonment for a term which may extend to three years and/or a fine which may extend to INR 1 Lakh).,Subsequent Convictions: second time or thereafter, the punishment is imprisonment for a term which may extend to five years and/or a fine which may extend to INR 2, Lakhs.

Section 416 IPC: Cheating by personation,, Section 463 IPC: Forgery and Section 468 IPC: forging a document or electronic record with the intention to commit fraud.

f)E-Mail Spoofing: A spoofed e-mail may be said to be one that appears to originate from one source but actually has been send from another source .Email spoofing is a technique commonly used for spam email and phishing to hide the origin of an email message.

By IT A: Punishment by Section 66C (Identity Theft) : imprisonment upto 3 years and fine upto Rs 1 lakh. and Section 66D (cheating by personation): imprisonment may extend to three years and fine which may extend to one lakh rupees. Punishment under IPC: Section 417 IPC (Punishment for cheating) is imprisonment for a term which may extend to one year, or a fine, or both,

According to Section 419 IPC (Punishment for cheating by personation) punishment is imprisonment for a term which may extend to three years, or a fine, or both and Section 465 IPC(Punishment for forgery) punishment is imprisonment for a term which may extend to two years, or a fine, or both.

g)Email Bombing :refers to sending a large number of emails to the victim resulting in the victims email account(In case of individual) or mail servers(in case of company or an email service provider) crashing. Section 66 of the IT Act deals with computer-related offenses, including email bombing. First Conviction: Imprisonment for a term which may extend to two years and/or a fine which may extend to INR 5 Lakhs, Subsequent Convictions: the punishment is imprisonment for a term which may extend to three years and/or a fine which may extend to INR 10 Lakh.

Section 469 IPC: Forgery for the purpose of harming reputation, which includes forging electronic records or creating fake emails to damage someone's reputation. Section 500 IPC: Defamation, which can include defamatory emails or communication sent through electronic means. Section 509 IPC: Word, gesture or act intended to insult the modesty of a woman, which may include sending offensive or sexually explicit emails with an intention to insult or harass a woman. Section 503 IPC: Criminal intimidation, which can include sending threatening emails or communication.

h)Sending Threatening Emails(Stalking by email): the offender directly sends email to the victim to threaten her or to harass her by sending hate , obscene, pornographic material and threatening mail to victim. Section 66 A of ITTA 2008, imprisonment upto 3 years and fine.(No Limit Of Fine). By IPC: Punishment: Section 504 IPC imprisonment up to 2 years or fine or both.

i)Malicious Hacking is an act done dishonestly, or fraudulently, referred to in section 43..Section 66,ITA : Hacking with computer systems is unauthorised access to others computer systems or network and according to Section 66 of the IT Act , the maximum punishment is imprisonment of up to 3 (three) years or a fine of Rs. 5Lakh or both and Section 378 of the IPC gives imprisonment of up to 3 (three) years or a fine or both.

j)Data Theft : Sections 43ITA :Data theft. Section 379 of IPC also deals with data theft and the punishment for data theft is imprisonment for 3 years or fine or both.

k)Pornography : The term “pornography” is a generic, not a legal term. It relates a broad range of sexual material. Here for cyber crime, pornography deals with obscene as something which is repulsive and indecent(non-conformance with accepted standards of morality) which tend to deprave and corrupt. For more details see . The United States Supreme court Lanmark case “Miller V California. The Supreme court cases for more clarification on pornography are Ranjit D. Udeshi Vs State of Maharashtra, AIR 1965 SC 881 the Udeshi case established the Hicklin test as the standard for determining obscenity in India. It recognized the importance of balancing freedom of speech and expression with the need to protect public morality and laid down guidelines for evaluating whether a work can be deemed obscene based on its impact on susceptible individuals.

Under the Information Technology (IT) Act, 2000 in India, the punishment for various offenses related to pornography depends on the specific provisions violated. Some relevant sections of the IT Act and their corresponding punishments (non-bailable offence) are as below:

Section 67: Publishing or transmitting obscene material electronically and Imprisonment up to three years and/or a fine up to ₹5 lakhs for the first conviction, secondly Imprisonment up to five years and/or a fine up to ₹10 lakhs for subsequent convictions.

Section 67A: Publishing or transmitting sexually explicit material and Imprisonment up to five years and/or a fine up to ₹10 lakhs for the first conviction whereas for subsequent convictions, the Imprisonment is up to seven years and/or a fine up to ₹10 lakhs for subsequent convictions.

Section 67B: Publishing or transmitting child pornography and Imprisonment up to five years and a fine up to ₹10 lakhs for the first conviction. Whereas for subsequent convictions, the Imprisonment
Is up to seven years and a fine up to ₹10 lakhs..

Additionally, there are relevant sections in the Indian Penal Code (IPC) that can be applied to offenses (Bailable offence)related to pornography:

Section 292: Sale, circulation, or exhibition of obscene material and Imprisonment up to two years and/or a fine, or both.

Section 293: Sale, etc., of obscene objects to young persons and Imprisonment up to three years and/or a fine, or both.

Section 294: Obscene acts and songs in public and depending on the nature of the act, it can be punished with imprisonment up to three months, a fine, or both. Sec 500, 506 and 500 ipc deals with Imprisonment up to five years and a fine up to Rs10 lakhs.

l)Child Pornography : 67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form and Punishment is : first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees

m) Revenge Porn: Sharing explicit or private images or videos without consent to harm or embarrass the individual is known as revenge Porn. Example: Distributing intimate photos or videos of an ex-partner without their permission. Section 67A of the Information Technology Act, 2000, provides for imprisonment up to seven years and/or a fine

n) Online Defamation: Section 499 IPC: Publishing false information that damages an individual's reputation. For Example: Spreading false rumours about someone on social media, tarnishing their image. Defamation can be charged under sections 500 of the IPC, for imprisonment for a term which may extend to two years, or with fine, or with both.

o) Sextortion: Coercing an individual into providing explicit images or engaging in sexual acts under threat of exposure. Example: Blackmailing someone by threatening to release compromising photos or videos unless they comply.The imprisonment carried under Section 67B of the Information Technology Act, 2000 extends up to 7 years and/or a fine. Section 67B of the Information Technology Act, 2000, provides for imprisonment up to seven years. Section 509 IPC: Insult to Modesty: imprisonment of up to three years, a fine, or both.

q) Cyber Bullying and Trolling: Using digital platforms to intimidate, harass, or threaten an individual. Example: Sending abusive messages or engaging in targeted online campaigns to humiliate someone. ITA section about is scrapped by SC.

Section 500 IPC: Defamation, punishment: imprisonment of up to two years, a fine, or both. Section 506 IPC: Criminal Intimidation: The maximum punishment is imprisonment of up to seven years and/or a fine and Section 507 IPC: Criminal Intimidation by Anonymous Communication and imprisonment for a term which may extend up to two years, a fine, or both.

r) Phishing: Tricking individuals into revealing sensitive information through deceptive emails or websites. Section 66D of the Information Technology Act, 2000, provides for imprisonment up to three years and/or a fine.

5.2 Cyber Crimes against an Organization

a) Hacking: Unauthorized access to computer systems or networks. Section 66 of ITA , 2000, provides for imprisonment up to three years and/or a fine.

b) Data Breach: Illegally accessing and stealing sensitive information from dada base of an organization. Section 43A of the ITA, 2000, provides for compensation to victims of data breaches, and Section 72A covers punishment for breach of confidentiality.

c) Insider Threat: Insider leak confidential data / Misuse privileged access or internal knowledge to commit fraud or theft. Depending on the specific offense, charges can be filed under various sections of the IPC, such as theft, **(**Sections 43ITA and Section 379 of IPC) Fraud(online investment frauds in Section 43(d),65 and 66), or unauthorized access(sec 43 and 43 A). Cheating (Section 415-420 IPC), Criminal Breach of Trust (Section 405-409 IPC) and Forgery (Section 463-470 IPC)

d) Intellectual Property Theft: Unauthorized use, reproduction, or distribution of copyrighted materials or trade secrets. For Example: Illegally copying and distributing copyrighted software or proprietary formulas.Sections 63 and 65 of the Copyright Act, 1957, and the Trade Marks Act, 1999, provide for imprisonment and/or a fine.

e) **Distributed Denial of Service (DDoS) Attacks**: Overwhelming an organization's network or website with a flood of traffic, rendering it inaccessible. For example: Flooding a company's website with requests, causing it to crash and disrupt operations. Depending on the specific offense, charges can be filed under various sections of ITA and the IPC such as causing damage to computer systems or networks.

f) Ransomware Attacks: Deploying malicious software that encrypts an organization's data and demanding a ransom for its release. Example: Infecting a company's systems with ransomware and demanding payment to restore access.(Section 43 with section 66 of ITA-damage to computer systems o without the owners consent, punishable with imprisonment up to three years or a fine rs,5 Lakh or both. Punishment for ransomware attack under Federal computer Fraud and Abuse Act shall be up to 10 years or a fine or both for first offence. For second offence imprisonment
shall be up to 20 years , fine or both.

g) Financial Fraud: FF Attack conducts fraudulent activities to target an organization's financial resources. For Example: Manipulating financial records or embezzling funds from company accounts. Depending on the specific offense, charges can be filed under various sections of the IPC, such as cheating, forgery, or criminal breach of trust as specified in (c) Insider Threat.

h) Sabotage: Intentionally causing damage or disruption or criminal mischief to an organization's computer systems or networks, Example: Planting malware to destroy critical data or disrupt operations. Depending on the specific offense, charges can be filed under various sections of the IPC, such as causing damage to computer systems as per section 425 IPC or section 43 ITA then punishment as per section 65 ITA-imprisonment upto three years or with fine upto 2 lakh or with both or criminal mischief(Sec 426 IPC shall be up to -3 months or a fine or both –there is no maximum cap for fine)

i)Insider Trading: Illegally trading stocks or securities based on confidential information is known as insider trading. For example: An employee using non-public information about a company to make stock trades for personal gain. The Securities and Exchange Board of India (SEBI) regulates insider trading under the SEBI (Prohibition of Insider Trading) Regulations, 2015, with penalties including fines and imprisonment.

j) Business Email Compromise (BEC): Manipulating or impersonating an organization's email communication to deceive employees or clients. Example: Sending fraudulent emails purporting to be from the CEO, instructing employees to transfer funds to a fraudulent account. Depending on the specific offense, charges can be filed under various sections of the IPC/ITA, such as cheating or impersonation.

5.3 Cyber Crimes against Society/Government

a) Cyber Terrorism: Using technology to create fear, panic, or disruption for ideological, political, or religious reasons. Example: Launching cyber attacks on critical infrastructure or government networks to disrupt services or Parliamentary attack 13th Dec 2001 and use of mobiles,& laptops in crime. Under the Unlawful Activities (Prevention) Act, 1967, acts of cyber terrorism can be punishable with imprisonment, fines, or both.

b) Spread of Hate Speech: Disseminating or promoting content or multimedia data that incites hatred or violence using computer or mobile communication or social media is known as hate speech. Example: Sharing online messages inciting communal violence or spreading racial hatred.

Punishment: Depending on the specific offense, charges can be filed under various sections of the IPC, such as promoting enmity between different groups or causing disharmony. As per IPC sections : 153 (A)Hate speech ,promoting enmity between different group), Section 294(Punishment for obscene act or words in public), 295A(hurting religious sentiments), Sec 124 IPC(Sedition- acts involving intension or tendency to create disorder of law incitement to violence- punishable by imprisonment or fine or both which depends on the severity of the case and judgement of the court), Sec 499 define defamation and Sec 500 defamation is punishable by imprisonment up to 2 years or fine or both.,

Sec 505(1)C-Spreading rumour or alarming news against any class or community is punishable by imprisonment up to 3 years or fine or both . Sec 505(2) to create , promote hatred, ill will about religion, language, racial, caste &communities is punishable by imprisonment up to 3 years or fine or both. Section 298 to wound religious feelings is punishable by imprisonment up to 1 year or fine or both.

c) Cyber Espionage: attack against business or government by hackers is unauthorised access or Illegally obtaining classified Data or sensitive information or intellectual property Rights (IPR) from computing systems for political, economic, Competitive advantage, or personal gain is also known as electronic espionage. Example: Infiltrating government systems to steal confidential defence information. Depending on the specific offense, charges can be filed under various sections of the IPC, such as theft, spying, or unauthorized access.

d) Spread of Fake News: Disseminating false information to mislead or manipulate the public. Example: Creating and spreading fabricated news stories to manipulate public opinion.

Punishment: Depending on the specific offense, charges can be filed under various sections of the IPC, such as spreading rumours, causing public mischief, or defamation.

e) Cyber Extortion: Using digital means to threaten individuals or organizations and demand payment or other concessions. Example: Threatening to release sensitive information unless a ransom is paid. Sections 384 and 386 of the IPC cover extortion and provide for imprisonment and/or a fine.

f) Online Child Exploitation: Engaging in the sexual exploitation or abuse of children through online platforms. Example: Producing, distributing, or accessing child pornography through the internet.

The Protection of Children from Sexual Offences (POCSO) Act, 2012, and the Information Technology Act, 2000, provide for stringent punishments, including imprisonment and fines.

g) Online Drug Trafficking: Illegally selling or distributing drugs through online platforms. For Example: Operating an online marketplace for illicit drugs. The Narcotic Drugs and Psychotropic Substances Act, 1985, and relevant provisions of the IPC provide for imprisonment and/or fines.

h) Money Laundering: Concealing the origins of illegally obtained money through digital transactions. Example: Using online platforms to transfer illicit funds, disguising their true source.

The Prevention of Money Laundering Act, 2002, provides for imprisonment and fines for money laundering.

i) Cyber Activism: Using digital platforms to promote social or political causes through peaceful means. Example: Organizing online campaigns for human rights or environmental activism. However if cyber activism is against human rights, then IPC Sections 153A: Promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony, Section 295A: Deliberate and malicious acts intended to outrage religious feelings of any class by insulting its religion or religious beliefs, Section 505: Statements conducing to public mischief are applicable. In addition, the IT Act, specifically the Section 66A (which was declared unconstitutional by the Supreme Court of India in 2015) used to criminalize certain online speech and communication.

j) Cyber Vandalism: Defacing or destroying websites or online content for malicious purposes. For Example: Hacking into a website and replacing the content with offensive or inappropriate material.

Section 66 of the Information Technology Act, 2000, covers hacking and provides for imprisonment and/or fines.

k)Multimedia Temper Attack : Sophisticated digital multimedia editing software is making it easier to tamper with multimedia data. This attack can be made on individual, organization or society's data. This falls under forgery case under ITA Section 43(i) read with section 66.and IPC sections 463,464, 468 and 479.punishment is for 3 years imprisonment and/or 2 lakh fines or both.

5.4 Advanced Attacks

This section discusses network attack and application attacks.

5.4.1 Network Attack : TCP/IP Stack Attacks

According to W. Stallings, Network Security Essentials — Applications and Standards, Prentice-Hall, Englewood, the normal information flow from source to destination and several categories of attacks that target it are shown in Figure 1A.

Interruption: The attacker targets the source or the communication channel and prevents information from reaching its intended destination by modification of data, overloading the link so that the information gets dropped because of congestion or cut the wire. An asset of the systems (hardware or software) gets destroyed or becomes unavailable. Interruption attempt to perform denial-of-service (DOS) attack.

Interception: An unauthorized/authorized party gains access to the information by eavesdropping into the communication channel (e.g., wiretapping).

Modification: The information is not only intercepted, but modified by an unauthorized party while in transit from the source to the destination. By tampering with the information, it is actively altered (e.g., modifying message content).

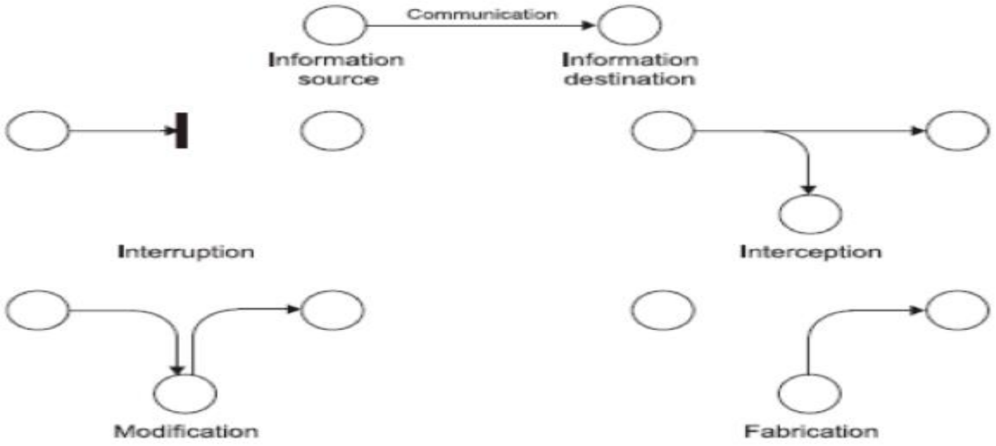

Figure 5 : Categories of attacks.

Fabrication: An attacker inserts counterfeit objects into the system without having the sender doing anything. When a previously intercepted object is inserted, this processes is called replaying.When the attacker pretends to be the legitimate source and inserts his desired information, the attack is called masquerading (e.g., replay an authentication message, add records to a file).

Table 2 Attack types with their corresponding categories

Category	Attack types
Probe	ipsweep, mscan, nmap, portsweep, saint, satan
DoS	apache, back, land, mailbomb, neptune, pod, processtable, smurf, teardrop, udpstorm, arpposion, crashiis, dosnuke, mailbomb, selfping
R2L	ftp_write, guess_password, imap, multihop,named, phf, sendmail, snmpgetattack, snmpguess, warezmaster,worm, xlock, xsnoop, httptunnel
U2R	buffer_overflow, loadmodule, perl, rootkit, ps, sqlattack, xterm

5.4.1.1 Probe

Probing is an attack in which the hacker scans a machine or a networking device in order to determine weaknesses or vulnerabilities that may later be exploited so as to compromise the system. This technique is commonly used in data mining e.g. saint, port sweep, mscan, nmap. In recent years, a growing number of programs have been distributed that can automatically scan a network of computers to gather information or find known vulnerabilities. These network probes are quite useful to an attacker who is staging a future attack. An attacker with a map of which machines and services are available on a network can use this information to look for weak points. Some of these scanning tools (satan, saint, mscan) enable even a very unskilled attacker to very quickly check hundreds or thousands of machines on a network for known vulnerabilities

Table 3 Attack types of Probe

Attack types	Definition
Insidesniffer	A probe attack in which the attacker gains access to the physical network and adds a host that is then used to sniff network traffic, perhaps allowing for the collection of passwords, or other data from any traffic flowing on that network/segment. The attack can be carried out in a stealthy manner, in which dns lookups are disabled, and a clear manner in which the sniffer used dns to resolve names of ips as it sniffs them.
Ipsweep	Surveillance sweep performing either a port sweep or ping on multiple host addresses.
Mscan	Multi-scan, looks for known vulnerabilities (named, imap, etc). Popular because it scans for Remote to User.Vulnerabilities in Linux
Ntinfoscan	A process by which the attacker scans an NT machine for information concerning its configuration, including ftp services, telnet services, web services, system account information, file systems and permissions.
Portsweep	Surveillance sweep through many ports to determine which services are supported on a single host.
Queso	A probe that consist of 7 packets, whose purpose is to identify the operating system and version of a particular host. It can be run successfully against many different host types.
Satan	Network probing tool which looks for well-known weaknesses. Operates at three different levels. Level 0 is light.
Is	A probe attack in which the attacker uses "nslookup", setting the server to the victim's dns server, to list all hosts/ips within that domainname. This attack may be followed by a probe of all of these ips/hosts.
Resetscan	ResetScan sends reset packets to a list of IP addresses in a subnet to determine which machines are active. If there is no response to the reset packet, the machine is alive. If a router or gateway responds with "host unreachable," the machine does not exist.

5.4.1.2 Denial of Service(DOS) Attacks

A DoS attack is a type of attack in which the hacker makes a computing or memory resources too busy or too full to serve legitimate networking requests and hence denying users access to a machine. There are many varieties of denial of service (or DoS) attacks. Some DoS attacks (like a mailbomb, neptune, or smurf attack) abuse a perfectly legitimate feature. Others (teardrop, Ping of Death) create malformed packets that confuse the TCP/IP stack of the machine that is trying to reconstruct the packet. Still others (apache2, back, syslogd) take advantage of bugs in a particular network daemon.

Table 4 Attack types of DoS

Attack types	Definition
Apache2	Denial of service against Apache web server, sends many Mime (Multipurpose Internet Mail Extensions) Headers in Many HTTP Get Requests.
Arppoison	An arp-level denial of service, where the attacker sends out bogus responses to "arp-who-has" requests for the victim's mac address. In order to carry out this attack, the attacker must gain access on a machine on the victim's subnet, so it often involves a remote attacker logging into a local machine, then running the attack against another machine (the victim).
Crashiis	A single, malformed http request causes the webserver to crash
Dosnuke	DoSNuke is a Denial of Service attack that sends Out Of Band data (MSG_OOB) to port 139 (NetBIOS), crashing the NT victim (bluescreens the machine).
Mailbomb	A Denial of Service attack where we send the mailserver many large messages for delivery in order to slow it down, perhaps effectively halting normal operation.
Neptune	Syn flood denial of service on one or more ports.
Pod	Denial of service ping of death.
Processtable	Fill up the Victim’s Process Table by slowly opening many Tcp(Telnet, Finger, etc) Connections to a Server and Letting them Hang.

	Once processtable is full victim cannot lanch new processes.
Smurf	Denial of service icmp echo reply flood.
Teardrop	Denial of service where mis-fragmented UDP packets cause some systems to reboot.
Udpstrom	Sends one Spoofed Packet Which starts Inifinite Loop of Packets from Chargen Port to echo of one machine or several machines.
Back	Denial of service attack against apache webserver where a client requests a URL containing many backslashes.
land	Denial of service where a remote host is sent a UDP packet with the same source and destination.
Selfping	A denial of service attack in which a local user on a Solaris 2.5.1 machine can ping the localhost in such a way as to case the machine to crash and subsequently reboot
Syslogd	Denial of service for the syslog service connects to port 514 with unresolvable source ip.
Tcpreset	A Denial of Service where the attacker, generally sitting on the same subnet as the victim, resets any tcp connections that it sees go through the handshake phase with the victim. To do this it spoofs the victims ip on the reset packets.

5.4.1.3 R2L- A Remote to User Attack and Punishments

Remote to Local (R2L**)** is an attack in which a user sends packets to a machine over the internet, which she/he does not have access to in order to expose the machines vulnerabilities and exploit privileges which a local user would have on the computer .It occurs when an attacker who has the ability to send packets to a machine over a network, but who does not have an account on that machine exploits some vulnerability to gain local access as a user of that machine. There are many possible ways an attacker can gain unauthorized access to a local account on a machine. Some of the attacks discussed within this section exploit buffer overflows in network server software (imap, named, sendmail). The Dictionary, Ftp-Write, Guest and Xsnoop attacks all attempt to exploit weak or misconfigured system security policies. The Xlock attack involves social engineering order for the attack to be successful the attacker must successfully spoof a human operator into supplying their password to a screensaver that is actually a trojan horse.

Table 5 Attack types of R2L

Attack types	**Definition**
Guessftp	Try to guess password via ftp for guest account
Guesstelnet	Try to guess password via telnet for guest account
Named	Remote Buffer Overflow of Named Daemon which sends Attacker a Root Xtrem Over the Named Port
Netbus	Remote-to-local (NT) attack with the potential to be a remote-to-root attack. The attacker must install the NetBus server on the victim's machine by either emailing a trojan horse to the victim or by sitting down at the victim's console. Once the serve is installed, the attacker can use the NetBus client remotely to do almost anything: upload/download files, run programs, etc. The attacker's access privileges are identical to the user currently logged on to the victim machine. So if an admin is using the victim, the attacker can run an adduser command to setup a new admin user => remote-to-root attack. Can also be used as a probe attack to scan IP addresses for NetBus servers.
Netcat_breakin	NetCat is a Remote to Local attack against NT. The attacker uses a trojan to install and run the netcat program on the victim machine on a specific port (53). Once netcat is running, it acts as a backdoor. The attacker can remotely access the machine through the netcat port without a username or password.
Ppmacro	This Remote to Local attack uses a trojan PowerPoint macro to read secret files. This attack is based on a particular scenario. The victim user usually receives PowerPoint templates from an outside source via email attachment. He runs a built-in macro which inserts a graph displaying web statistics, saves the presentation as a ppt file, and posts it on the web.
Sendmail	The Sendmail attack exploits a buffer overflow in version 8.8.3 of sendmail and allows a remote attacker to execute commands with superuser privileges. By sending a carefully crafted email message to a system running a vulnerable version of sendmail, intruders can force sendmail to execute arbitrary commands with root privilege.
Xlock	Display Trojan Screenlock and Spoof a user with an Open X Server Into Revealing their password
Dict	Guess passwords for a valid user using simple variants of the account name

	over a telnet connection.
Framespoofer	Data attack where the attacker sends a fake email to the victim directing the victim to a tru sted web site. When the user clicks on the link in the email it actually links to a javascript which brings up the trust ed web site but then inserts a malicious web page into one of its frames. The URL displayed in the browser remains unchanged.'
Httptunnel	There are two phases to this attack: Setup — a web "client" is setup on the machine being attacked, which is configured, perhaps via crontab, to periodically make requests of a "server" running on a non-privilaeged port on the attacking machine. Action — When the periodic requests are received, the server encapsulates commands to be run by the "client" in a cookie.. things like "cat /etc/passwd".. etc..
Imap	Remote buffer overflow using imap port leads to root shell
Ncftp	An R2L attack which exploits a bug in a particular version of ncftp, the popular ftp client. The a user on the victim host ftp's to the attackers machine, and attempts to download, recursively, a directory. Contained in the directory is directory with a very long name, embedded in the name is one or more commands that are then executed (un-intentionally) by the ftp client with the permissions of that user.
Netcat	NetCat is a Remote to Local attack against NT. The attacker uses a trojan to install and run the netcat program on the victim machine on a specific port (53). Once netcat is running, it acts as a backdoor. The attacker can remotely access the machine through the netcat port without a username or password.
Phf	Exploitable CGI script which allows a client to execute arbitrary commands on a machine with a misconfigured web server.
Snmpget	Monitor a router after guessing the SNMP "community" password.During training a monitoring host collected data from the router every 5 seconds. During testing a second machine (from outside the eyrie domain) also began monitoring the router,If SNMP Configuration is Allowed, an Attacker with the SNMP Community Password Can Modify Routing Tables
Xsnoop	Monitor Keystrokes on an Open X Terminal and look for passwords

5.4.1.4 U2R- User to Root

User to Root Attacks (U2R): are exploitations in which the hacker starts off on the system with a normal user account and attempts to abuse vulnerabilities in the system in order to gain super user privileges. It exploits are a class of exploit in which the attacker starts out with access to a normal user account on the system (perhaps gained by sniffing passwords, a dictionary attack, or social engineering) and is able to exploit some vulnerability to gain root access to the system. There are several different types of User to Root attacks. The most common is the buffer overflow attack. Buffer overflows occur when a program copies too much data into a static buffer without checking to make sure that the data will fit.

Table 6. Attack types of U2R

Attack types	**Definition**
Casesen	CaseSen is a User to Root attack that exploits the case sensitivity of the NT object directory. The attacker ftps three attack files to the victim: soundedt.exe, editwavs.exe, psxss.exe (the names of the files were chosen to make the attack more stealthy). The attacker then telnets to the victim and runs soundedt.exe. A new object is created in the NT object directory called \??\c: which links to the directory containing the attack files. A posix application is started activating the trojan attack file, psxss.exe, which results in the logged in user being added to the Administrators user group.
Sechole	The attacker logs on to the NT machine as a normal user. He then runs the secHole program which manipulates an API function and executes a DLL which adds the user to the administrator group. The attacker may have to reboot is the system locks up.
Anypw	AnyPW is a Console User to Root attack that allows the attacker to logon to the system without a password. A boot disk is used to modify the NT authentication package so that a valid username can login with any password string. Logins via telnet also work with any password.
Eject	Buffer overflow using eject program on Solaris. Leads to a user->root transition if successful.
Fdformat	Buffer overflow using the fdformat UNIX system command leads to root shell

Ffbconfig	The Ffbconfig attack exploits a buffer overflow is the 'ffbconfig' program distributed. Due to insufficient bounds checking on arguments, it is possible to overwrite the internal stack space of the ffbconfig program.
Loadmodule	Non-stealthy loadmodule attack which resets IFS for a normal user and creates a root shell.
Perl	Perl attack which sets the user id to root in a perl script and creates a root shell
Ps	Ps takes advantage of a racecondition in the ps command in Sol. 2.5, allowing a user to gain root access.
Sqlattack	A U2R attack where a user makes a TCP connection with the sql database server on the linux machine, issues a special escape sequence to exit the database shell, then enters and runs the perlmagic script to obtain a root shell.
Sshtrojan	An r2l attack where the attacker tricks a system administrator into installing a trojan version of the sshd server which has a back door embedded into the binary. Subsequent instances of the sshtrojan attack involve exercising this backdoor.
Xterm	Buffer overflow of xterm binary in Redhat Linux, Allows illegal Transition from Normal User to Root
Yaga	User-to-root attack creates a new user in the Administrators group by hacking the registry. The attacker edits the victim's registry so that the next time a system service crashes on the victim, a new admin user is setup. To setup the attack, the attacker must put 3 files on the victim machine: a file containing the new user info, a file with the registry edit info, and a batch file to setup the new user. The attacker must also edit the registry. All this can be done via a telnet session or by physically accessing the victim machine. Once the setup is complete, the attacker can remotely crash a service on the victim machine (using crashIIS for example) to setup the new admin user.

5.4.1.5 TCP/IP Stack Attacks And Punishment

Table 7. TCP/IP Attack Categories and Punishment.

Network Attacks	Punishment
Probe	Under the Information Technology (IT) Act in India, network probing may fall under Section 43 (Unauthorized Access to Computer Systems or Networks) or Section 66 (Computer Related Offenses). As per Indian Penal Code (IPC), network probing may not have a specific provision. relevant sections related to hacking, data theft, or other offenses may apply. UNDER Section 66C (Identity Theft), Section 66D (Cheating by Personation by using Computer Resources), or Section 66E (Violation of Privacy). In USA, network probing or scanning, is known as known as network reconnaissance.. There is no specific provision in the USA that directly. Under the CFAA, unauthorized access to computer systems or networks is prohibited. computer systems or networks, In the United Kingdom (UK), network probing or scanning without proper authorization is generally considered a violation of the Computer Misuse Act 1990 (CMA). Section 1 of the CMA specifically addresses unauthorized access to computer material, and Section 3 addresses unauthorized acts with intent to impair the operation of a computer.
Denial of Service(DOS) Attacks	Under the Information Technology (IT) Act in India, DoS attacks fall under Section 43 (Unauthorized Access to Computer Systems or Networks) or Section 66 (Computer Related Offenses). The Act provides for both civil remedies and criminal penalties, including imprisonment and fines, depending on the severity of the offense. In terms of the Indian Penal Code (IPC), depending on the impact and intent of the attack, , Section 426 (Punishment for Mischief) or Section 420 (Cheating and dishonestly inducing delivery of property) could be applicable. In the United States, DoS attacks are generally considered illegal under the Computer Fraud and Abuse Act (CFAA), which is the primary federal law addressing computer-related offenses. The CFAA prohibits unauthorized access to computer systems and networks, including actions that cause damage or disrupt services. The punishment for DoS attacks under the CFAA can include criminal charges, fines, and imprisonment. Additionally, other federal laws and regulations such as the) Wiretap Act, the Stored Communications Act, or the Racketeer Influenced and Corrupt Organizations Act (RICO) may also be applicable in certain cases, depending on the specifics of the attack. In the United Kingdom, DoS attacks can be prosecuted under the Computer Misuse Act 1990 (CMA), The CMA provides for criminal penalties, including fines and imprisonment, for individuals found guilty of carrying out DoS attacks.

R2L- A Remote to User Attack	The punishment for the act, known as "Remote to Local (R2L)" attack, can be analysed under both the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC) **Information Technology (IT) Act, 2000**:,Section 43: Penalty and compensation for damage to computer, computer systems, etc.,Section 66: Computer-related offenses, including hacking.,Section 66C: Punishment for identity theft.,Section 66D: Punishment for cheating by personation by using a computer resource.,Section 66F: Punishment for cyberterrorism., **Indian Penal Code (IPC**):Section 378: Theft, Section 379: Punishment for theft,Section 383: Extortion,Section 384: Punishment for extortion, Section 465: Punishment for forgery ,Section 468: Forgery for the purpose of cheating ,Section 469: Forgery for the purpose of harming reputation ,Section 470: Forgery of a document or an electronic record.
User to Root Attacks (U2R):	Information Technology (IT) Act, 2000:Section 43: Penalty and compensation for damage to computer, computer systems, etc.,Section 66: Computer-related offenses, including hacking. Section 66C: Punishment for identity theft ,Section 66D: Punishment for cheating by personation by using a computer resource,Section 66F: Punishment for cyberterrorism, **Indian Penal Code (IPC):**Section 378: Theft,Section 379: Punishment for theft,Section 383: Extortion,Section 384: Punishment for extortion. Section 465: Punishment for forgery,Section 468: Forgery for the purpose of cheating ,Section 469: Forgery for the purpose of harming reputation ,Section 470: Forgery of a document or an electronic record. Section 471: Using as genuine a forged document or electronic record. Section 477A: Falsification of accounts.

5.4.2 OWASP Top 10 Attacks

The tremendous increase in online transactions has been accompanied by an equal rise in the number and type of attacks against the security of online payment systems. The different OWASP vulnerabilities that are applicable to E-commerce application are

SQL Injection :Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

Cross-Site Scripting (XSS) :XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Broken Authentication and Session Management:Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities

Insecure design refers to the design and implementation of a system, application, or software that contains vulnerabilities, weaknesses, or flaws that can be exploited by attackers. It involves the failure to incorporate appropriate security measures during the design phase, leaving the system susceptible to various types of attacks. In the context of information technology, insecure design can manifest in several ways, including:(i)Lack of Input Validation (SQL injection or cross-site scripting (XSS) attacks).(ii)Insufficient Authentication and Access Controls: can result in unauthorized access, privilege escalation, or unauthorized manipulation of sensitive data.(iii)Weak Encryption or Cryptographic Practices can undermine the confidentiality and integrity of data.(iv)Failure to Handle Errors and Exceptions Securely can reveal sensitive information or allow attackers to gain insights into the underlying system.(v)Inadequate Secure Configuration can lead to vulnerabilities, such as default or weak passwords, unnecessary services or features enabled, or insecure network configurations.(vi) Lack of Secure Communications: Failing to use secure protocols (e.g., HTTPS) or not implementing proper encryption during data transmission can expose sensitive information to interception or manipulation.

To mitigate the risks associated with insecure design, it is crucial to follow secure coding practices, perform security assessments and testing during the design and development stages, and regularly update and patch systems to address known vulnerabilities.

Cryptographic failure: Cryptographic failure refers to situations where the implementation or use of cryptographic techniques or systems fails to provide the intended level of security, leading to vulnerabilities or breaches. These failures can occur due to various reasons such as weak encryption algorithms, flawed key management practices, improper implementation of cryptographic protocols, or inadequate protection of cryptographic keys.Determining responsibility for cryptographic failures can vary depending on the specific circumstances and legal jurisdiction. Generally, responsibility can be attributed to multiple parties involved in the design, development, implementation, and maintenance of the cryptographic system or application. This may include Cryptographic System Developers ,Application Developers and System Administrators and .Users or Organizations.

Insecure Direct Object References :A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

Sensitive Data Exposure : Many web applications and APIs don't properly protect sensitive data, like credit cards, tax IDs, and authentication credentials financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct MasterCard fraud, fraud, or other crimes. Sensitive data could also be compromised without extra protection, like encryption at rest or in transit, and requires special precautions when exchanged with the browser.

Missing Function Level Access Control :Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

Cross-Site Request Forgery (CSRF) :A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

Unvalidated Redirects and Forwards :Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages

Security Misconfiguration: - Security misconfiguration is that the most ordinarily seen issue. this can be commonly a results of insecure default configurations, incomplete or impromptu configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they have to be patched and upgraded in a very timely fashion. **It** refers to the failure to properly configure the operating system (OS) and database management system (DBMS) settings, resulting in potential security vulnerabilities. These misconfigurations can occur due to oversight, lack of awareness, or insufficient knowledge of secure configuration practices. You can provide the security by Security Awareness and Training, Least Privilege Principle, Secure Authentication and Access Controls, and Regular Vulnerability Scanning and Penetration Testing

Insecure Deserialization: - Insecure deserialization often results in remote code execution. whether or not deserialization flaws don't lead to remote code execution, they'll be wont to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

Insufficient Logging & Monitoring: -Insufficient logging and monitoring, plus missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties instead of internal processes or monitoring.

5.4.3 Web based Application Attacks and Punishment.

The punishment for the **OWASP attacks** attacks may vary depending on the jurisdiction and the specific circumstances of the case. it's important to note that legal penalties can differ between countries and even within different regions or states. In India, the punishment for cyberattacks and related offenses is primarily governed by the Information Technology Act, 2000 (IT Act) and the Indian Penal Code (IPC). The IPC and IT Act does not specifically mention the name of OWASP attack crimes, AND , the specific punishment for OWASP attacks is not explicitly defined. However specific provisions related to attacks and their impact on applications are specified as given table 2. It's important to note that the application of these sections and the specific punishment can depend on the circumstances, the severity of the offense, the intent of the offender, and the discretion of the court. The actual punishment can vary based on the specifics of the case and the judgment of the legal authorities.

Table 8: Punishment For OWASP Top 10 attacks.

Punishment By ITAA : Penalties can include imprisonment up to three years and/or a fine up to INR 5 lakhs (500,000) for the first offense.

OWASP Attack Crime	Acts And Sections For Punishment
SQL Injection and Cross-Site Scripting (XSS)	Under the Information Technology (IT) Act, 2000 and the Indian Penal Code (IPC), the punishment for SQL injection and Cross-Site Scripting (XSS) attacks can be as follows: Information Technology (IT) Act, 2000: SQL Injection and XSS attacks can fall under certain provisions of the IT Act, such as: 43. Penalty and compensation for damage to computer, computer system, etc. Section 43 (Damage to computer resource) and the punishment for causing damage to a computer resource through SQL injection or XSS attacks can include imprisonment up to three years and/or a fine of up to INR 5 lakh.

	Section 66 (Computer-related offenses) and If the SQL injection or XSS attack results in more severe offenses, such as unauthorized access, data theft, or manipulation, the punishment can include imprisonment up to three years and/or a fine of up to INR 2 lakh. 66. Computer related offences.–If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both. Indian Penal Code (IPC): Under the IPC, specific provisions related to SQL injection and XSS attacks may not exist. However, certain sections can be applicable depending on the consequences of the offense such as Section 425 (Mischief): If the SQL injection or XSS attack is considered an act of mischief, the punishment can include imprisonment for up to two years, a fine, or both. Section 426 (Punishment for mischief):If the SQL injection or XSS attack is considered an act of mischief causing damage, the punishment can include imprisonment for up to three years, a fine, or both.
Broken Authentication and Session Management (Broken Access Control:	Broken authentication and session management offenses can fall under certain provisions of the IT Act, such as: Section 43 (Damage to computer resource) and the punishment for causing damage to a computer resource due to broken authentication or session management can include imprisonment up to three years and/or a fine of up to INR 5 lakh. Section 66 (Computer-related offenses):If broken authentication or session management results in more severe offenses, such as unauthorized access or misuse of computer systems, the punishment can include imprisonment up to three years and/or a fine of up to INR 2 lakh. **Under the IPC**, specific provisions related to broken authentication and session management may not exist. However, certain sections can be applicable depending on the consequences of the offense: Section 425 (Mischief): If broken authentication or session management is considered an act of mischief, the punishment can include imprisonment for up to two years, a fine, or both. Section 426 (Punishment for mischief):If broken authentication or session management is considered an act of mischief causing damage, the punishment can include imprisonment for up to three years, a fine, or both.
Cross-Site Request Forgery (CSRF)	CSRF attacks may fall under various sections of the Act, such as Section 43 (Unauthorized Access to Computer Systems or Networks) or Section 66 (Computer Related Offenses). The Act provides for both civil remedies and criminal penalties, including imprisonment and fines, depending on the severity of the offense. For instance, if CSRF attacks involves fraudulent or dishonest intentions, it may be covered under Section 415 (Cheating), Section 463 (Forgery), or Section 420 (Cheating and dishonestly inducing delivery of property).
Insecure Design	The consequences of Insecure design attacks can fall under different sections of these acts based on the nature and extent of the offense. Information Technology (IT) Act, 2000: Insecure design attacks can be addressed under certain provisions of the IT Act, such as(i)Section 43 (Damage to computer resource) and the punishment for causing damage to a computer resource due to insecure design can include imprisonment up to three years and/or a fine of up to INR 5 lakh. Section 66 (Computer-related offenses) and the insecure design results in more severe offenses, such as unauthorized access or misuse of computer systems, the punishment can include imprisonment up to three years and/or a fine of up to INR 2 lakh. Under the IPC :Section 425 (Mischief) and If the insecure design attack is considered an act of mischief, the punishment can include imprisonment for up to two years, a fine, or both. As per Section 426 (Punishment for mischief): If the insecure design attack is

	considered an act of mischief causing damage, the punishment can include imprisonment for up to three years, a fine, or both.
Cryptographic Failures. Injection.	Under the Information Technology (IT) Act of India :: Section 43. If a cryptographic failure leads to unauthorized access or damage to computer systems, penalties may be imposed under this section. Section 66: If a cryptographic failure results in any of these offenses, penalties could be applied. Section 72 If a cryptographic failure leads to the unauthorized disclosure of sensitive information, it may be considered a breach of confidentiality under this section. In addition to the IT Act, the Indian Penal Code (IPC) may also have relevant sections depending on the specific circumstances and consequences of the cryptographic failure. For example: Section 420:. If a cryptographic failure is found to be a part of a fraudulent activity, penalties could be imposed under this section. Section 406. If a cryptographic failure involves a breach of trust resulting in financial loss or harm to individuals or entities, penalties may be applicable.
Security Misconfiguration	Certain provisions of the IT Act are relevant that may apply: Section 43: If a service provider or administrator's security misconfiguration leads to unauthorized access, damage, or disruption, they may be liable for punishment under this section. The penalties can include imprisonment and/or fines. Or he shall be liable to pay damages by way of compensation to the person so affected. 43A. Compensation for failure to protect data: corporate shall be liable to pay damages by way of compensation to the person so affected.43 and 43A punishment are as per the decision of the court. Section 66: If a service provider or administrator's security misconfiguration enables hacking or the introduction of malicious code, they may be subject to punishment under this section. The penalties can include imprisonment and/or fines. 66. Computer related offences.–If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both. Section 72: If a service provider or administrator's security misconfiguration results in the unauthorized disclosure or use of personal information, they may be liable for punishment under this section. The penalties can include imprisonment and/or fines.
Vulnerable and Outdated Components	Under the IT Act Section 43 and Section 66 may be relevant if providing vulnerable and outdated components leads to unauthorized access, damage, or disruption of computer systems, networks, or data. These sections provide for both civil remedies and criminal penalties, including imprisonment and fines, depending on the severity of the offense. Under the IPC Section 415- cheating, Section 463- fraud, or other offenses may be applicable if there is evidence of intentional deception or harm caused by the provision of such components.
Unvalidated Redirects and Forwards	Unvalidated Redirects and Forwards deal with offenses related to unauthorized access, damage, or disruption of computer systems, networks, or data. Hence Under the Information Technology (IT) Act in India, unvalidated redirects and forwards may fall under Section 43 (Unauthorized Access to Computer Systems or Networks) or Section 66 (Computer Related Offenses The Act provides for both civil remedies and criminal penalties, including imprisonment and fines, depending on the severity of the offense. In terms of the Indian Penal Code (IPC), unvalidated redirects and forwards may not have a specific provision. However, if these vulnerabilities are exploited to commit fraud, identity theft, or any other criminal act, relevant sections related to cheating, forgery, or other offenses may apply. Hence Section 415 (Cheating), Section 463 (Forgery), or Section 420 (Cheating and dishonestly inducing delivery of property) could be applicable.
Insufficient Logging	Insufficient logging and monitoring may fall under various sections of the It

And Monitoring	Act, because this attack deals with offenses related to unauthorized access, damage, or disruption of computer systems, networks, or data . Section 43 (Unauthorized Access to Computer Systems or Networks) or Section 66 (Computer Related Offenses). The Act provides for both civil remedies and criminal penalties, including imprisonment and fines, depending on the severity of the offense.

5.4.4 Other Important Cyber Crimes in Cyber Space and Punishment.

Other cyber advanced crimes are listed below under various acts in Table.

Table 9. Cybercrime Chart with Punishment under different Acts

Cyber crime	IT A 2008 SECTIONS	IPC SECTIONS	Other Acts for Punishments
Cyber Terrorism	66F Imprisonment may extend up to imprisonment for life.	153 A	. National investigation Agency(NIA) Act 2008, The Unlawful Activities(Prevention Act 2008(UAPA) Sec 17,18,18A,18B,43D), CRPC 167), TADA, POTA
Credit Card Fraud	43(a 0, (g) read with section 66 7 66C	420,467,468 471	Imprisonment for 3 years imprisonment or 5lakh fine or both
Copy Right Violation	Sec 63 of ITAA 2008 –upto 3 Years of imprisonment or fine upto Rs 5 Lakh or both	405 &420	copy right Act 1957 under section 51,63,63A, 63b
IPR Infringement	Sec 43(I) read with Sec 66 for IPR forgery	463,464,468, 479	Under ITAA and IPC -accused punishable for b3 years imprisonment or 2 lakh fine or both Patent Act 1970, copy right Act 1957, The Trade Marks Act, 1999 The International Trade Commission (ITC), USA, Under the IPC, intellectual property violations may be treated as criminal offenses. leading to criminal prosecution. The penalties may include imprisonment, fines, or both depending on. the severity. The infringer may be required to pay monetary damages to the rights holder based on actual losses suffered by the rights holder or based on a reasonable royalty that would have been payable
Bogus website, cyber frauds	**Section 66D-** upto 3 Years of imprisonment or fine upto Rs 1Lakh.	**Sec 419 IPC-** imprisonment upto 3 Years or fine . **Sec 420 IPC-** imprisonment upto 7 Years AND fine .	--
Malicious use of WI-FI against the state or Planning computer virus	**Section 66-** imprisonment upto 3 Years or fine upto rs.5 Lakh or both. Sec66F-Life	---	----

against the state or DDOS against government	imprisonment		
Web Defacement	Sec 65 (non bailable offence)	468 (non bailable offence) 464 &469(bailable offence)	imprisonment upto 3 Years or fine rs.2 Lakh or both.
Web Jacking	65(bailable offence)	384 (non bailable offence)	imprisonment upto 3 Years or fine rs.2 Lakh or both.
Electronic Digital Signature	65,73 & (sec 74 bailable offence)	417 & 420 74 (bailable offence)	imprisonment upto 2 Years or fine rs.1 Lakh or both.
On line Sale of drugs	--	--	Narcotic-Drugs and Psychotropic Substances Act 1985 chapter 4:Offences and punishment(Section 15 To section 33)
On Line Sale of Arms	--	--	Arms Act 1959- Chapter V Offences And Penalties (Section 25 To section 33)

ITA Section 43 deals with unauthorized access, computer contamination, and introducing viruses, while Section 66 covers computer-related offenses, including the dissemination of viruses or ransomware.

6. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This section concludes the results and future research directions

6.1 CONCLUSION

Cyberspace refers to the virtual environment created by computer networks and the internet, while the cyber world encompasses the collective digital reality comprising all the entities and activities in cyberspace. The research on unveiling the hackers' methodology and exploring cyber crimes, punishment, and Indian cyber laws has shed light on the computer systems environment- hardware and software with systems programs with complex landscape of cyber threats and the legal frameworks in place to combat them. Through the analogy of a bungalow robbery plan, the study has provided valuable insights into the activities of attackers targeting computer systems and enhanced the understanding of stakeholders involved in tackling cybercrime. The ethical hacking is a real world testing used to evaluate the security of the organizations computing assets like operating systems, databases, application programs, Intrusion Protection systems firewalls and other devices by exploiting and performing cyber-attacks through the vulnerabilities into the computing &network assets and then providing security planning to the executives to harden the information security to avoid security breaches.

Because of the increased interconnection among information systems and networks, the consequences of successful attacks by malicious individuals can have far-reaching implications. In addition, numerous scripts available to unskilled individuals can be used to initiate various types of harmful attacks. The results of malicious attacks can include financial loss, loss of reputation, a drop in the value of a company’s stock, and many legal issues.

By staying informed and adhering to cyber laws, individuals can contribute to creating a safer and more secure digital ecosystem in India. Cybercrime ranges variety of activities. Cybercrime can be basically divided into three major categories: (i) Cybercrimes against persons like harassment occur in cyberspace or through the use of cyberspace. Harassment can be sexual, racial, religious, or other. (ii) Cybercrimes against property like computer wreckage (destruction of others' property), transmission of harmful programs, unauthorized trespassing, unauthorized possession of computer information.(iii) Cybercrimes against government like Cyber terrorism. Cyber jurisprudence relates to the legal principles governing the use of technology and cyberspace

The examination of various cyber crimes against individuals, organizations, and society has highlighted the significant impact of attacks such as communication disruption, interception, information modification, and fabrication. The categorization and investigation of TCP/IP attacks, including probing, Denial of Service Attacks (DoS), Remote-to-User Attacks (R2L), and User-to-Root Attacks (U2R), have deepened our understanding of the diverse methodologies employed by cyber criminals. The OWASP top 10 attacks dictate how to write the secure code. There is a need to investigate secure software life cycle to combat top 10 OWASP attacks.

The research has emphasized the crucial role of cyber jurisprudence in establishing legal frameworks to regulate and protect cyberspace, encompassing areas such as data privacy, cyber crimes, and digital rights. By analyzing the relevant provisions in Indian cyber laws, including the Indian Evidence Act of 1872, the Information Technology Act of 2000, and the Indian Penal Code, Criminal Procedure code , the study has provided guidance on the punishments associated with different cybercrimes. It's important to note that while the Indian Evidence Act provides guidelines for the admissibility of electronic evidence, other statutes such as the Information Technology Act, 2000, and the Code of Criminal Procedure, 1973, contain provisions specific to cybercrime investigation and prosecution. These laws may address the collection, preservation, and admissibility of electronic evidence more comprehensively in the context of cybercrime cases. It is important to note that the actual investigation process may vary depending on the nature and complexity of the cybercrime, as well as the available resources and expertise of the police administration or digital forensic investigator's expert opinion about the loss or damage of computing resources.

6.2 Future Research Directions

While this research has provided valuable insights into the hackers' methodology, cyber crimes, and Indian cyber laws, there are several areas that warrant further investigation:

Emerging Threats and Countermeasures: Future research could focus on identifying and analyzing emerging cyber threats and the corresponding countermeasures needed to mitigate them. This would involve staying updated with evolving attack techniques and exploring innovative approaches to enhance cybersecurity.

International Cooperation: As cybercrimes transcend national boundaries, future studies could delve into the importance of international cooperation in addressing cyber threats. This would involve examining the effectiveness of international legal frameworks, information-sharing initiatives, and collaborative efforts in combating cyber crime.

Technological Advancements: Given the rapid pace of technological advancements, future research could explore the impact of emerging technologies such as artificial intelligence, blockchain, and quantum computing on the landscape of cyber crimes and the legal frameworks needed to regulate them.

Legal Reforms: There is a need to assess the adequacy and effectiveness of existing cyber laws in addressing contemporary cyber threats. Future research could focus on proposing legal reforms that align with the evolving nature of cyber crimes and ensure a robust legal framework to combat them effectively.

By pursuing these future research directions, we can enhance our understanding of hackers' methodologies, strengthen cyber laws, and develop comprehensive strategies to tackle cyber crimes, ultimately fostering a safer and more secure digital environment.

REFERENCES

[1]. B. B. Meshram , Object Oriented Paradigm with C++, Shroff Publishers & Distributers Pvt. Ltd, Mumbai, Oct 2016. ISBN Number -978-93-5213-4120.

[2]. B. B. Meshram, Ms. K.A. Shirsath , TCP/IP and Network Security, Shroff Publishers 7 Distributors Pvt, Ltd. Mumbai feb 2018, ISBN Number 978-93-5213-355-0

[3]. CHFI(Computer Hacking Forensic Investigator), Course Material EC-Council , USA, Nov 2004

[4]. PG, Advanced Cybersecurity Course Notes,. Stanford, Engineering School, USA, Oct 2022.

[5]. The Constitution of India.

[6]. Indian Evidence Act of 1872, Kamal Publishers, New Delhi

[7]. The Information Technology Act of 2000,

[8]. The Indian Penal Code, Bare Act 2018

[9]. Criminal Procedure code 1973, Bare Act, 2019

[10]. The Specific Relief Act 1963, Bare Act 2020

[11]. The Prevention of Terrorism Act 2002, Bare Act 2019

[12]. Dr. Gupta and Agrwal , Cyber Laws, Premier Publishing Company, 2023

[13]. Dr. Santosh Kumar, Cyber Laws and Crimes, Whites Mann, Publishing Company, Sept 2020

[14]. S. Khadsare, Cyber Security Hand Book, Council of Information Security, New Delhi, ISBN Number 978-93-5268-442-7.

[15]. Patil Jatin, Cyber laws in India: An Overview, Indian Journal Of Law And Legal Research , March 3, 2022.

[16]. Dr. Kalpesh B. Gelda, Cyber Crime, Cyber Law And Cyber Security, Paripex - Indian Journal Of Research , Volume-8 , Issue-9 , September - 2019

[17]. Apoorva Bhangla, And Jahanvi Tuli, "A Study on Cyber Crime and its Legal Framework in India", International Journal of Law Management & Humanities, vol 4, issue 2, 2021

[18]..Ali Alharbi Sulaiman Alhaidari, Michigan Mohamed Zohdy , Denial-of-Service, Probing, User to Root (U2R) & Remote to User (R2L) Attack Detection using Hidden Markov Models , International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 07– Issue 05, September 2018

[19]. Balarezo, J.F., Wang, S., Chavez, K.G., Al-Hourani, A. and Kandeepan, S. A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. *Engineering Science and Technology, an International Journal*, 2021. A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks - ScienceDirect

[20]. Jeya, P.G., Ravichandran, M. and Ravichandran, C.S., Efficient classifier for R2L and U2R attacks. International Journal of Computer Applications, 2012. (PDF) Efficient Classifier for R2L and U2R Attacks (researchgate.net)

[21]. Types of Cyber Attacks You Should Be Aware of in 2023, https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks

[22].Shreya Taneja ,Landmark Judgments On Cyber Law, (01 June 2021):https://www.lawyersclubindia.com/articles/landmark-judgments-on-cyber-law-14025.asp.

[23].Vinod Joseph and Deeya Ray, Cyber Crimes under the IPC and IT Act - An Uneasy Co-Existence <https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence> accessed on 22 July 2021

[24].The Times of India] https://timesofindia.indiatimes.com/blogs/toi-editorials/another-reminder-that-india-needs-to-invest-more-to-combat-cyber-threats/ (Jun. 24, 2022, 01:48 PM).

[25].The times of India] https://timesofindia.indiatimes.com/india/pegasus-spyware-used-to-hack-phones-of-journalists-politicians-in-india-report/articleshow/84531126.cms (Jun. 25, 2022, 03:26 AM).

[26].OWASP Top 10 2020, https://owasp.org/www-project-top-ten/

[27]. Dafydd Stuttard Marcus Pinto, “The Web Application Hacker’s Handbook”, Second Edition, Wiley Publication Inc. 2018

[28].Lior Ben Dayan ,OWASP Top 10 vulnerabilities 2022: what we learned, (January 04, 2023, https://vulcan.io/blog/owasp-top-10-vulnerabilities-2022-what-we-learned)

[29]..Pavan Duggal, Text book on Cyber Law , Universal Law Publishing , 1 January 2016

[30]..Ouissem Ben Fredj , Omar Cheikhrouhou ,et.al. “An OWASP Top Ten Driven Survey on Web Application Protection Methods,: (20 November 2020): https://www.researchgate.net/publication/346035890

[31].Ahmad Syaufi , Mursidah , et.al. Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes, International Journal of Cyber Criminology
https://www.cybercrimejournal.com/