Sai Vidya Institute of Technology, Rajanukunte, Bengaluru

Model Question Paper-I/II with effect from 2022-23 (CBCS Scheme)

USN

First/Second Semester B.E. Degree Examination

Introduction to Cyber Security (BETCK105I/205I)

Solution to Question Paper

TIME: 03 Hours **Max. Marks: 100**

Note: Answer any **FIVE** full questions, choosing at least **ONE** question from each **MODULE**.

		Module -1	*Bloom's Taxonomy Level	Marks
Q.01	a	**Define computer crime. Discuss about Cyberpunk and Cyber warfare** **Ans: Computer crime definition:** • **Cybercrime or computer crime** is any illegal behaviour directed by means of electronic operations that target to security of computer system and the data processed by them. • Crimes completed either on or with a computer • Any illegal activity done through the internet or on the computer • All criminal activities done using the medium of computers, the Internet, cyberspace and WWW. • Any financial dishonesty that takes place in computer environment • Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom • **Cyberpunk:** The term cyberpunk could mean something like " anarchy via machines", or "machines/ computer Rebel moment" • The two basic aspects of cyberpunk are **technology and individualism.** • It is a genre of science fiction set in a lawless subculture of oppressive society dominated by computer technology. • **Cyber warfare:** It is the use of computer network to disrupt the activities of a state or organization, especially the deliberate attacking of information system for strategic or military purpose. • Cyber warfare for many people, means information Warriors unleashing vicious attacks against an unsuspecting opponent computer networks and paralyzing nations information infrastructure. • It refers to information resources, including communication systems that support an industry, institution or population. Cyber-attacks are often presented as military forces and the internet has major implications for espionage and warfare.	L2	8
	b	List the various cybercrimes against property and against organization **Ans:** cybercrimes against property and against organization	L1	6

		The following are the crimes against property and against organization **Cybercrime against property** 1. Credit card frauds 2. Intellectual property crimes basically I P crimes include software piracy copyright infringement trademarks violations theft of computer source code etc., 3. Internet time theft **Cybercrime against organisation** 1. Unauthorised accessing of computer - hacking is one method of doing this and hacking is a punishable offence 2. Password sniffing 3. Denial-of-service attacks 4. Virus attacks dissemination of viruses 5. Email bombing or mail bombs 6. Salami attack or Salami technique 7. Logic bomb 8. Trojan horse 9. Data diddling 10. Crimes emanating from Usenet newsgroups 11. Industrial spying/Industrial espionage 12. Computer network instructions 13. Software piracy		
	c	Discuss cybercrime and the Indian ITA 2000 • India has the **fourth highest number** of **Internet users** in the world There are 45 million Internet users in India, 37% of all Internet accesses from happen cybercafes and 57% of Indian Internet users are between 18 and 35 years. • The **population of educated** youth is high in India. • It is reported that compared to the year 2006, cybercrime under the **Information Technology (IT) Act** recorded a whopping 50% increase in the year 2007. • The **National Crime Record Bureau (NCRB)** gives the report that, 46%, were related to incidents of cyberpornography, followed by hacking. • In over 60% of these cases, offenders were between 18 and 30 years, according to the "Crime in 2007". • The **Indian Government** is doing its best to control cybercrimes. • For example, **Delhi Police** have now **trained 100 of its officers** in handling cybercrime and placed them in its **Economic Offences Wing**. • The training gave to officers about computer hardware and software, computer networks comprising data communication networks, network protocols, wireless networks and network security about 6 weeks. • The **ITA 2000** was framed after the **United Nation General Assembly Resolution in January 30, 1997.** • ITA adopting the Model Law on Electronic Commerce (E-Commerce) adopted by Commission on the United Nations International Trade Law. • A total cybercrime was registered under the IT Act in 2007 compared to 142 cases registered 2006. • Under the IPC in to, 339 cases were recorded in 2007 compared noteworthy to 311 cases in 2006. The laws, crime details and punishment details given in table below.	L2	6

Section Ref. & Title	Chapter of the Act & Title	Crime	Punishment
Sec. 43 (Penalty for damage to computer)	CHAPTER IX Penalties and Adjudication	Damage to computer system,	Compensation for 1 crore
Sec. 66 (Hacking with computer system)	CHAPTER XI Offences	Hacking (with intent or knowledge)	Fine of 2 lakhs and imprisonment for 3 years
Sec. 67 (Publishing of information which is obscene in electronic form	CHAPTER XI Offences	Publication of obscene material in electronic form	Fine of 1 lakh imprisonment of 5 years and double Conviction on second offence
Sec. 68 (Power of controller to give directions)	CHAPTER XI Offences	Not complying with directions of controller.	Fine up to 2 lakhs imprisonment of 3 years
Sec. 70 (Protected system	CHAPTER XI Offences	Attempting or securing access to computer without his/her knowledge,	Imprisonment up to 10 years.
Sec. 72 (Penalty for breach of confidentiality and privacy)	CHAPTER XI Offences	Attempting or securing access to computer for breaking confidentiality	Fine up to 1 lakh and imprisonment up to 2 years
Sec. 73 (Penalty for publishing Digital Signature Certificate false in certain particulars)	CHAPTER XI Offences	Publishing false digital signature	Fine up to 1 lakh or imprisonment up to 2 years or both
Sec. 74 (Publication for fraudulent purpose)	CHAPTER XI Offences	Publication of Digital Signatures for fraudulent purpose	imprisonment up to 2 years and Fine up to 1 lakh

OR

Q.02	a	Who are cybercriminals? Discuss the three groups of cybercriminals Cybercriminals are those who conduct act such as child pornography; credit card fraud, cyber stalking, defame another online; gaining unauthorised access to a computer system; ignoring copyright, software licensing and Trademark protection; overriding encryption to make illegal copies; software piracy and stealing another's identity to perform criminal acts. They can be categorised into three groups that reflect their motivation.	L3	8

		We have three types of **Cybercriminals** • Type I: Cybercriminals hungry for recognition • Type II: Cybercriminals not interested in recognition • Type III: Cybercriminals the insiders **Type I: Cybercriminals-Hungry for recognition** • **Hobby hackers:** A person who enjoys exploring the limits of what is possible in the spirit of play full cleverness • **IT professionals:** ethical hacker • **Politically motivated hackers:** promote the objective of individuals groups or Nation supporting a variety of causes such as anti-globalization transitional conflict and protest. • **Terrorist organizations:** cyber terrorism terrorist using the internet for attacks, large scale destruction of computer networks. **Type II: Cybercriminals-not interested in recognition** • **Psychological perverts:** Express sexual Desire deviate from normal behaviour • **Financially motivated hackers (corporate espionage):** make money from cyberattacks: bots for hire; fraud through phishing information theft, spam and extortion. • **State sponsored hacking (National espionage or sabotage):** Extremely professional groups working for governments. • **Organized criminals:** have the ability to worm into the network of media, major corporations and different departments. **Type III: Cybercriminals-the insiders** • Disgruntled or former employees seeking revenge • Competing companies using employees to gain economic advantage through the damage for theft		
	b	Discuss about Cyber defamation in detail. • **Cyberdefamation occurs** when defamation takes place with the help of a computer and/or internet. • For example, someone publishing defamatory matter about someone's website or send emails contain defamatory information to all friends of that person. • **CHAPTER XXI of the Indian Penal Code (IPC)** is about the defamation. • According IPC section 499; • 1. It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives. • 2. It may amount to defamation to make an invitation concerning a company or an association of election of persons as such. • 3. Imputation in the form of an alternative or expressed ironically the amount to defamation.	L3	6

		• 4. No imputation is said to be harm a person's reputation and less that imputation directly or indirectly in the estimation of the others Louis the moral or intellectual character of that person, his cast. • Liable is written defamation on slander is oral defamation		
	c	Explain password Sniffing and mail bombs techniques. **password Sniffing** • Password sniffers are program that monitor and record the name and password of a network uses as the login at a site. • Example keyloggers these are computer programs which one installed into a particular computer system records all the keystrokes and send it to the attacker so the attacker can get access to user credentials. • With the user credentials, the attacker will login and access restricted documents **Mail bombs techniques** • It refers to **sending a large number of emails** to the victim to **crash victim E-mail** account or to make victim's servers crash • computer program can be written to instruct a computer to do such tasks on a repeated basis. • The terrorism has hit the Internet in the form of **Email bombing.** • Here the Cybercrime repeatedly send the email to the particular persons email ID and shut down the entire system.	L2	6
		Module-2		
Q. 03	a	What is Social Engineering? Discuss Human Based Social Engineering with a suitable example • social engineering Is a Technique to influence and persuasion to device people to obtain the information or perform some action. • A social engineer uses telecommunications or internet to get them to do something that is against the security practices and/or policies of the organization. • Social Engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationship with insiders. • It is an art of exploiting the trust of people. • The goal of SE is to **fool someone** into **providing valuable** information or access to that information. • Social Engineering studies **human behavior** so that people will help because of the **desire to be helpful**, the **attitude to trust people**, and fear of getting into trouble. • **An example is calling a user** and **pretending** to be someone from the **service desk** working on a **network issue**; the attacker then proceeds to ask question about what the user is working on, what **files shares he/she uses**, what **his/her password** is and so on. • **Example:** Talking to an employee of a company, in the name of technical support from the same office. While taking with the employee the attacker will collect the confidential information such as name of the company, username and password etc. • **Human based Social Engineering** • It refers to person to person interaction to get the required/desired information. • **Impersonating an employee or valid user:** Impersonation" (e.g.. posing oneself as an employee of the same organization) is perhaps the greatest techniques used by SE to deceive people.	L3	8

SE take the advantages of the fact that most people are basically helpful, so they are harmless to tell someone who appears to be lost where the computer room is located. Or pretending some one as employee or valid user on the system.

- **Posing as an important user:**

The attacker pretends to be an important user for example a chief Executive Officer (CEO) or high-level manager who needs immediate assistance to gain access to a system.
They think that low level employee don't ask about the proof or questions to the higher level employees.

- **Using a third person:**

An attacker pretends to have permission from an authorized source to use a system. This trick is useful when the supposed authorized personnel is on vacation or cannot be contacted for verification.

- **Calling technical support**

Calling the technical support for assistance is a classic social engineering example. Help-desk and technical support personnel are trained to help users, which makes them good prey for Social Engineering attacks.

- **Shoulder surfing**

It is a technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping an attacker to
gain access to the system.

Fig Shoulder Surfing

- **Dumpster diving**

It involves looking in the trash for information written on pieces of paper or computer printouts. This is a typical North American term; it is used to describe the practice of rummaging through commercial or residential trash to find useful free items that have been discarded.
It is also called dumpstering, binning, trashing garbing or garbage gleaning "Scavenging is another term to describe these habits. In the UK, the practice is referred to as "binning or "skipping and the person doing it is a "binner" or a "skipper.

Example: gong through someone's trash for to recover documentation of his/her critical data [e.g., social security number (SSN) in the US, PAN/AADHAR number in India, credit card identity (ID) numbers, etc.

	b	Explain how criminals plan the attacks? List the phases involved in planning cyber crimes Ans: Criminal use many methods and tools to locate the vulnerabilities of their	L2	6

target. The target can be individual and/or organization.
Criminal plan active and passive attacks. Active attacks are used to alter the system or computer network.

Whereas passive attack attempts to gain information about the target. Active attacks may affect the availability, integrity, and authenticity of data whereas passive attacks lead to breaches of confidentiality.

Attacks can also be classified as inside or outside.
An attack attempted within the security perimeter is called as inside attack; this is done by insider who gains access to more resources than expected.
An outside attack is attempted by a source outside the security perimeter, who is indirectly associated with the organization.

Phases involved in planning Cybercrime:

1. Reconnaissance
2. Information gathering, first phase passive attack
3. Scanning and scrutinizing the gathered information
4. For validity of the information as well as to identify the existing vulnerabilities
5. Launching an attack and Gaining and maintaining the system access.

Phase 1: Reconnaissance

- It is an act of reconnoitering- explore, often with the goal of finding something or somebody (gain information about enemy (potential enemy)
- In the world of "hacking," reconnaissance phase begins with foot printing - this is the preparation toward **preattack phase,** and involves accumulating data about the target environment and computer architecture to find ways to **intrude into that environment**.
- The objective of this preparatory **phase** is to **understand the system, its networking ports and services, and any other aspects of its security that are needful for launching the attack**.
- Two phases: passive and active attacks.

Phase 2: Information gathering, first phase **passive attack**
This Phase Involves gathering information about the target without his/her knowledge.

1. Google or Yahoo search locate information about employees
2. Surfing online community groups Facebook to gain information about an individual
3. Organizations website for personal directly or information about the key employees used in social engineering attack to reach the target.
4. Blogs news groups press releases etc.,
5. Going through job posting
6. Network sniffing information on internet protocol address ranges hidden server or network or service on the system.

Active Attacks:

- It involves probing the network to discover individual host to confirm the information (IP address, operating system type and version, and services on the network) gathered in the passive attack phase
- Also called as Rattling the Doorknobs or Active Reconnaissance
- Can provide confirmation to an attacker about security measures in place (Whether front door is locked?)

Phase 3: Scanning and scrutinizing the gathered information

- Is a key to examine intelligently while gathering information about the

target

The objectives are:

1. Port scanning
2. Network scanning
3. Vulnerability scanning

Port scanning:

- The act of systematically scanning a computer port.
- Support is a place where information goes into and out of a computer port scanning identify is open doors to a computer.
- It is a similar to a test going through your neighborhood and checking every door and window on each house to see which ones are open and which ones are locked.
- There is no way to stop someone from port scanning your computer while you are on the Internet because accessing internet server open support which open the door to your computer.

Scrutinizing Phase

- It is also called as enumeration in the hacking world. The object to behind the step is to identify the following

1. The valid user accounts or groups;
2. Network resources and/or shared resources;
3. Operating System (OS) and different applications that are running on the OS.

Phase 4: For validity of the information as well as to identify the existing vulnerabilities. After collecting the data on the victim, validate the acquired information and also identify the vulnerabilities.

Phase 5: Launching an attack and gaining and maintaining the system access.

- After scanning and scrutinizing (enumeration) the attack is launched using the following steps.

1. Crack the password
2. Exploit the privileges
3. Execute the malicious command or application
4. Hide the files
5. Cover the tracks- delete access logs, so that there is no trial illicit activity

	c	List and briefly explain any six tips for safety and security while using the computers in a cybercafé Ans: (Any six you need to write) **1. Always logout do not save login information through automatic login information** While checking E-Mails or logging into chatting services such as instant messaging or using any other service that requires a username and a password, always click "logout or sign out" before leaving the system. Simply closing the browser window is not enough, because if somebody uses the same service after you then one can get an easy access to your account. However, do not save your login information through options that allow automatic login. Disable such options before logon **2. Stay with the computer** While surfing/browsing, one should not leave the system unattended for any period of time. If one has to go out, logout and close all browser windows.	L2	6

3. Clear history and temporary files

Internet Explorer saves pages that you have visited in the history folder and in temporary Internet files. Your passwords may also be stored in the browser if that option has been enabled on the computer that you have used. therefore, before you begin browsing, do the following in case of the browser Internet Explorer: Go to Tools> Internet options click the Content tab > click AutoComplete. If the checkboxes for passwords are selected, deselect them. Click OK twice.

After you have finished browsing, you should clear the history and temporary Internet files folders.

For this, go to Tools > Internet options again> click the General tab go to Temporary

Internet Files > click Delete Files and then click Delete Cookies

Then, under history, click clear history. Wait for the process to finish before leaving the computer

4. Be alert don't be a victim of Shoulder Surfing

One should have to stay alert and aware of the surroundings while using a public computer. Snooping over the shoulder is an easy way of getting your username and password.

5. Avoid online financial transaction

Ideally one should avoid online banking, shopping or other transactions that require one to provide personal, confidential and sensitive information such as credit card or bank account details. In case of urgency, one has to do it; however, one should take the precaution of changing all the passwords as soon as possible. One should change the passwords using a more trusted computer, such as at home and/or in office.

6. Change password

ICICI Bank/SBI about changing the bank account/transaction passwords is the best practice to be followed by everyone who does the online net banking.

7. Virtual Keyboard

Nowadays almost every bank has provided the virtual keyboard on their website. The advantages of utilizing virtual keyboard is we can avoid the keylogger attack.

8. Security warnings

One should take utmost care while accessing the websites of any banks/financial institution. The screenshot in Fig. 2.7 displays security warnings very clearly (marked in bold rectangle), and should be followed while accessing these financial accounts from cybercafe

OR

Q.04	a	Define Cyber Stalking along with its working. Explain two types of Stalkers	L3	8

Ans:

cyberstalking is the use of Internet or other electronics means to stalk or harass an individual, a group or an organization. It may include false accusation, defamation, slander and liable.

It also includes monitoring, identity (ID) theft, threats, vandalism, solicitation of minors for sex, or gathering information that may be used to threaten or harass a person.

Cyberstalking is sometimes referred to as Internet stalking, e-stalking or online stalking.

It refers to the use of Internet or electronic communication such as e-mail or instant messages to harass the individual.

As per Law **Cyber Stalking is a punishable offence** and attracts section 354 (D), 509 IPC, and section 67 under I.T. Amendment Act 2008. Information Technology Act, 2000 (amended in 2008) - When a person publishes or sends salacious material via electronic media is to be charged under Section 67 of the Act.

We have two types of stalkers namely, Online Stalkers and Offline Stalkers.

Both are criminal offenses, both are motivated by a desire to control, intimidate of influence a victim.

A Stalker may be an online stranger or a person whom the target knows. He may be anonymous and solicit involvement of other people online who do not even know the target.

Online Stalkers	Offline Stalkers
They aim to start the interaction with the victim directly with the help of s Internet. E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone cell phone. The stalker makes sure that the victim recognizes the attack attempted on him/her. The stalker can make use of a third party to harass the victim.	The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc. Searching on message boards/newsgroups. Personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet. The victim is not aware that the Internet has been used to perpetuate an attack against them.

b Differentiate between passive attacks and active attacks — L2 — 6

Key	Passive Attacks	Active Attacks
Definition	Attempts to Gain information about the target without his/her permission.	It involves probing the network to discover individual host to confirm the information **(IP address, operating system type and version, and services on the network)** gathered in the **passive attack phase**
Requirement	Leads to Breaches of confidentiality.	Affects the Availability, Integrity and Authenticity of data
Modification	In Passive Attack, information remains unchanged.	In Active Attack, information is modified.
Dangerous For	Passive Attack is dangerous for Confidentiality.	Active Attack is dangerous for Integrity as well as Availability.
Attention	Attention is to be paid on detection.	Attention is to be paid on prevention.
Impact on System	A Passive Attack does not have any impact on the regular functioning of a system.	An Active Attack can damage the system.

		Victim	The victim does not get informed in a passive attack.	The victim gets informed in an active attack.		
		Tracking	Comparatively easy to trace.	It is difficult to track, it does not leave the any traces of the attacker's interference.		
		Example of attacks	Spying, War driving, Eavesdropping, Dumpster diving, Foot printing, Traffic analysis	Session hijacking, Man-in the middle (MITM), impersonation, DoS, DDoS etc.,		
	c	Define Bot and Botnet. With a diagram, explain how Botnets create business?			L3	6

Ans:

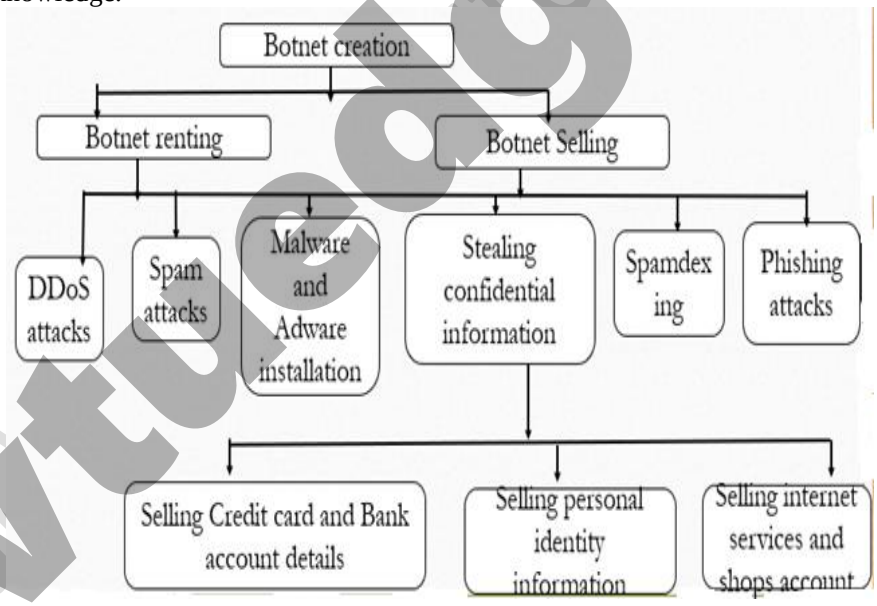
Bot: "An automated program for doing some particular task, often over a network".

A botnet (also known as a zombie army) is a number of internet computer that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses)

Any such computer is called as a zombie-in effect, a computer "robot" or "bot" that servers the wishes of some master spam or virus originator.

Most computers compromised in this way are home based. According to a report from Russian based Kaspersky labs botnets– not spam, viruses, or worms– currently pose the biggest threat to the Internet.

Botnet is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the user's knowledge.



Zombie networks have become a source of income for entire groups of cybercriminals.

If someone wants to start a business and has no programming skills, there are plenty of Bot for sale offers on forums.

Obfuscation and encryption of these programs code can also be ordered in the same way to protect them from detection by antivirus tools.

Another option is to steal an existing Botnet. Figure shows how Botnet creates business.

Module-3

Q. 05	a	What are hardware key loggers and Anti key loggers? List the advantages of using anti loggers • keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored. • Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the Victims IT savvy behavior. **Hardware Keyloggers** • To install these keyloggers, physical access to the computer system is required. Hardware keyloggers are small hardware devices. • These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device. • Cybercriminals install such devices on ATM machines to capture ATM Cards PINs. • Each keypress on the keyboard of the ATM gets registered by these keyloggers • These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence. • **Listed are few websites where more information about hardware keyloggers can be found:** • http://www.keyghost.com • http://www.keelog.com • http://www.keydevil.com • http://www.keykatcher.com **Antikeylogger** • Antikeylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool. • <u>Advantages of using antikeylogger are as follows:</u> 1. Firewalls cannot detect the installations of keyloggers on the systems; hence, antikeylogger can detect installations of keylogger. 2. This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs; if not updated, it does not serve the purpose, which makes the users at risk. 3. Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers 4. It prevents ID theft 5. It secures E-Mail and instant messaging/chatting **Note:** Visit http://www.anti-keyloggers.com for more information).	L2	8
	b	What is a Proxy server? What is its purpose? • **Proxy server** is computer on a network which acts a s an intermediary for connections with other computers in that network. • 1st attacker connects to proxy server • Proxy server can allow an attacker to hide ID • Purpose of proxy server 1. Keep the system behind the curtain	L2	6

2. Speed up access to resource. It is used to cache the webpages from a web server.
3. Specialized proxy servers are used to filter unwanted content such as advertisement
4. Proxy server can be used as IP address multiplexer to enable to connect number of computers on the internet, whichever has only one IP address.

Advantages of Proxy server is that its cache memory can serve all users.

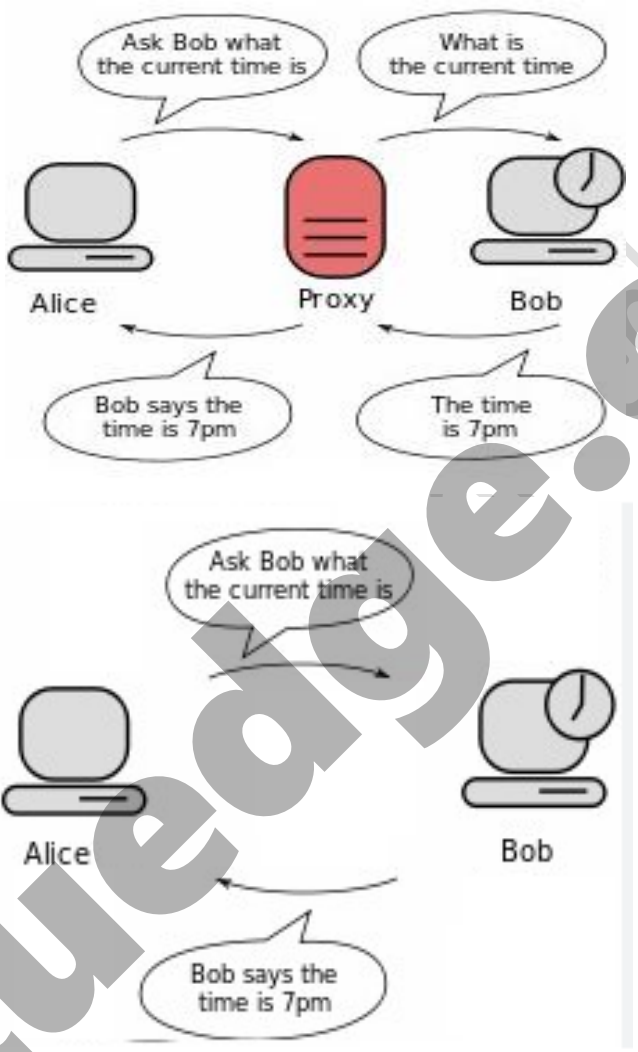


Fig. Proxy server and Normal server

List of website for free proxy servers
1. http://www.proxy4free.com 2. http://www.publicproxyservers.com 3. http://www.proxz.com 4. http://www.anonymitychecker.com 5. http://www.surf24h.com **6.** http://www.hidemyass.com

	c	What is a Backdoor? Discuss any four examples of Backdoor Trojans Ans: • It means of access to a computer program that bypass security mechanisms • Programmer use it for troubleshooting • Attackers often use backdoors that they detect or install themselves as part of an exploit • Works in background and hides from user • Most dangerous parasite, as it allows a malicious person to perform any possible action • Programmer sometimes leave such backdoor in their software for diagnostic and troubleshooting purpose. Attacker discover these undocumented features and use them. **What a backdoor does?** 1. It allows an attacker to create, delete, rename, copy or edit any file; change any system setting, alter window registry; run control and terminate application; instal arbitrary software 2. The control computer hardware devices, modify related setting, shutdown or restart a computer without asking for user permission 3. Steals sensitive personal information, logs user activity, tracks web browsing habits 4. Record Keystrokes that a user types on a computer's keyboard and captures screenshots 5. Sends all gathered data to predefined E-Mail address 6. It infects files, corrupts installed app and damage entire system 7. It distributes infected files to remote computers and perform attack against hacker-defined remote hosts. 8. It installed hidden FTP server that can be used by malicious person 9. It degrades Internet connection speed and overall system performance 10. It provides uninstall features and hides processes, files and other objects to complicate its removal as much as possible. **Examples of Backdoor Trojans** 1. **Back office:** Enable user to control a computer running the Microsoft windows OS from remote location 2. **Bifrost**: Infect Windows 95 through Vista 3. **SAP backdoors:** SAP is an Enterprise Resource Planning (ERP) system and nowadays ERP is the heart of the business technological platform. These systems handle the key business processes of the organization, such as procurement, invoicing, human resources management, billing, stock management and financial planning. 4. **Onapsis Bizploit:** It is the open-source ERP penetration testing framework developed by the Onapsis Research Labs. Bizploit assists security professionals in the discovery, exploration, vulnerability assessment and exploitation phases of specialized ERP penetration tests.	L2	6
		OR		

Q. 06	a	Discuss various types of Viruses categorized based on attacks on various elements of the system. Ans:	L3	8

Categorized based on attacks on various elements of the system

1. **Boot sector viruses:** It Infects the storage media on which OS is stored and which is used to start the computer system. Spread to other systems when shared infected disks and pirated software's are used.
2. **Program viruses:** These viruses becom Active when the programs files (usually with extension .bin, .com, .exe,. ovl, .drv) is executed. Makes copy of itself.
3. **Multipartite viruses:** It is hybrid of a boot sector and program viruses. It infects program files along with the record when the infected program is active.
4. **Stealth viruses:** It camouflages and/or Masks (hides) itself so detecting this virus is difficult. It can hide itself such a way that anti-virus software also cannot detect it. Memory to remind in the system and detected. Example of stealth virus is Brain virus.
5. **Polymorphic viruses:** It acts like a "Chameleon" that changes its virus signature (I,e., binary pattern) every time it spread through the system (i.e., multiplies and infects a new file). Polymorphic generators are routines (small programs) that can be linked with the existing viruses.

   Generators are not viruses but purpose to hide actual viruses under the cloak of polymorphism. It is difficult to detect polymorphic virus with the help of an antivirus program.First Polymorphic generator was the Mutation Engine (MtE). Other Polymorphic generators are Dark Angel's Multiple Encryptor (DAME), Darwinian Genetic Mutation Engine (DGME), Dark Slayer Mutation Engine (DSME), MutaGen, Guns'nRoses Polymorphic Engine (GPE), and Dark Slayer Confusion Engine (DSME)

6. **Macro viruses:** Many applications, such as Microsoft word and Microsoft Excel, support MACROs (i.e., macrolanguages). These macros are programmed as a macro embedded in a document. Once macro virus gets onto a victim's computer then every document he/she produces will become Infected.
7. **Active X Java control:** All the web browsers have settings about Active X and Java Commands. Little awareness is needed about managing and controlling these settings of a web browser to prohibit and allow certain functions to work.
8. Which invites the threats for the computer system being targeted by unwanted software. **Examples of The World's Virus attacks !!!**

Conficker	INF/AutoRun	Win32 PSW.OnLineGames	Win32/Agent (Trojan)
Win32/FlyStudio (Trojan with characteristic of backdoor)	Win32/Pacex.Gen	Win32/Qhost	WMATrojanDownloader.GerCodec

	b	What is Phishing? How Phishing works? Ans: Phishing is introduced in 1996. Phishing refers to an attack using mail programs to deceive internet users into disclosing confidential information that can be then exploited for illegal purpose. • While checking electronic mail (E-Mail) one day a user finds a message from the bank threatening him/her to close the bank account if he/she does not reply immediately. • Although the message seems to be suspicious from the contents of the message, it is difficult to conclude that it is a fake/false E-Mail. • **Examples**: stealing personal and financial data - and can infect systems with viruses and also a method of online ID theft in various cases. • Fake email using other reputed companies or individual identity • People associate phishing with E-mail message that spoof or mimic banks credit card companies or other business such as Amazon, and eBay **<u>Phishers works as follows</u>** 1. **Planning:** Criminals called as phisher, decide the target & determine how to get E-mail address 2. **Setup:** Once phishers know which business/business house to spoof and who their victims are, they create methods for delivering the message & to collect the data about the target. 3. **Attack:** Phisher sends a phony message that appears to be from a reputed source 4. **Collection:** Phisher record the information of victims entering into web pages or pop-up window 5. **Identity theft and fraud:** Phisher use Information that they have gathered to make illegal purchases and commit fraud. Recently more and more organisation/Institute provides greater online access for their customers and hence criminals are successfully using phishing techniques to steal personal information and conduct ID theft at global level.	L3	6
	c	Discuss four types of DoS attacks Ans: **1. Flood attack (Ping flood)** • This is the warliest form of DoS attack and is also known as ping flood. Attacker sending number of ping packets, using ping command, which result into more traffic than victim can handle. • This requires the attacker to have faster network connection than the victim • It is very simple to launch, but Prevention is difficult **2. Ping of death attack** • The ping death attack sends oversized ICMP (Internet Control Message Control) packets, and it is core protocol of IP Suite. • It is mainly used by networked computers OS's to send error messages indicating datagrams to the victim.	L2	6

- The maximum packet size allowed is of 65,536 octets. Some system upon receiving the oversized packet, will crash, freeze or reboot system resulting DoS.

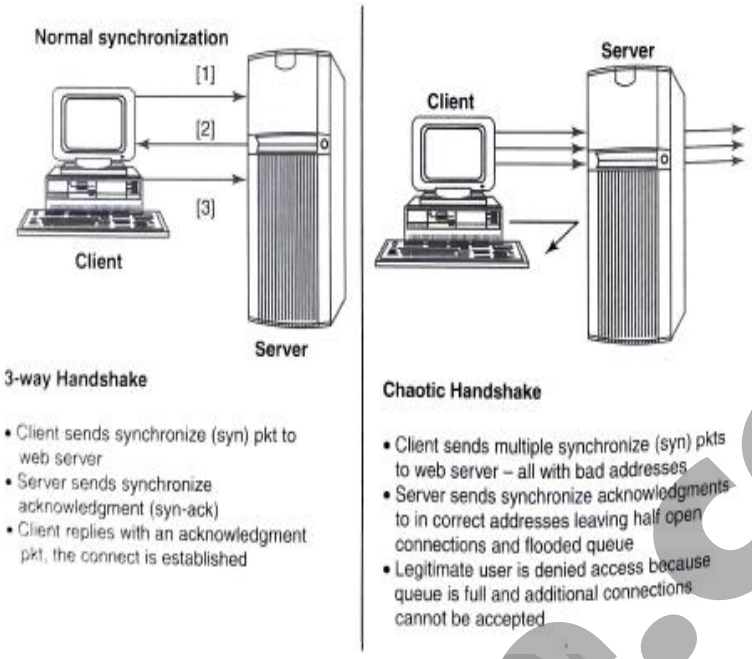


Fig. Denial-of-service (DoS) attack.

3. SYN attack (TCP SYN flooding)

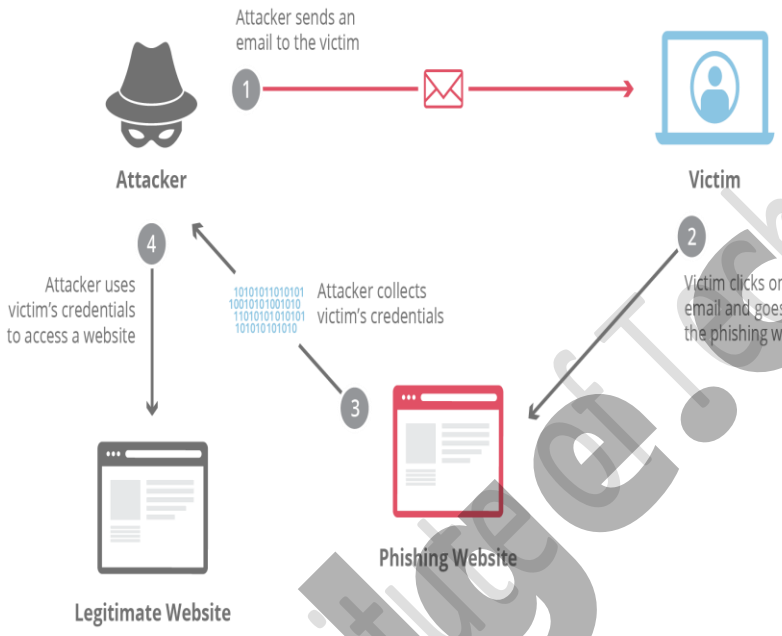
- In this Transmission control protocol handshaking of network connections is done with SYN and ACK messages. An attacker initiates a TCP connection to the server with an SYN (using a legitimate or spoofed source address).
- The server replies with an SYN-ACK. The client then does not send back an ACK, causing the server (i.e., target system) to allocate memory for the pending connection and wait.
- This fills up the buffer space for SYN messages on the target system, preventing other systems on the network from communicating with the target system. Figure 3.5 explains how the DoS attack takes place.

4. Teardrop attack

- Teardrop attack is an attack where fragmented packets are forged to overlap each other when the receiving host tires to reassemble them.
- IP's packet fragmentation also is used to send corrupted packets to confuse the victim and may hang the system. This attack can crash various Oss due to a bug in their TCP/IP fragmentation reassembly code.
- Windows 3.1x, 95 and NT, Linux versions 2.0.32 and 2.1.63 are vulnerable to this attack

		5.Smurf attack • Generating significant computer network traffic on victim network using foods via spoofed broadcast ping message • Attack consists of a host sending ICMP echo request to network broadcast ping address • Every host receive this packet and send back ICMP echo response • Internet relay chat (IRC) servers are primarily victim of smurf attack 6. **Nuke:** • An old DoS attack against computer network is consisting of fragmented or otherwise invalid ICMP packets sent to target. • Achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until comes to complete stop • Eg. WinNuke which is exploited the vulnerability in the NetBIOS handler in windows 95. A string of out of band data was sent to TCP port 139 of victim's machine, causing it to lock up and display Blue Screen of Death (BSOD).		
		Module -4		
Q. 07	a	Explain four types of methods used by the phishers to reveal personal information on Internet Ans: Dragnet 2. Road-and-reel 3. Lobsterpot 4. Gillnet **1. Dragnet** • A method involves the use of spammed E-Mails, bearing falsified corporate identification (ne.., corporate names, logos and Customers of trademarks), which are addressed to a large group of people (a particular financial institution or members of a particular auction site) to web- sites or pop-up windows with Similarly falsified identification. • Dragnet phishers do not identify specific prospective victims in advance. • Instead, they rely on false information included in an E-Mail to trigger an immediate response by victims-typically, clicking on links in the body of the E-Mail to take the victims to the websites or pop- up windows where they are requested to enter bank or credit card account data or other personal data. **2. Road-and-reel** • In this method, phishers identify specific prospective victims in advance, and convey false information to them to prompt their disclosure of personal and financial data. • For example, on the phony webpage, availability of similar item for a better price (i.e., cheaper price) is displayed which the victims may be searching for and upon visiting the webpage, victims were asked for personal information such as name, bank account numbers and passwords, before confirming that the "sale" and the information is available to the phisher easily. • **3. Lobsterpot** • This method focuses upon use of spoofed websites.	L2	10

- It consists of creating of bogus/ phony websites, similar to legitimate corporate ones, targeting a narrowly defined class of victims, which is likely to seek out.
- These attacks are also known as "content injection Phishing."
- Here the phisher places a weblink into an E-Mail message to make it look more legitimate and actually takes the victim to a phony scam site, which appears as legitimate website similar to official site. These fake sites are spoofed websites.
- Ones the netizens is into the one of these spoofed sites, he/she might willingly send personal information to the con artist. Then they use your information to purchase goods, apply new credit card or to steal your identity.



4. Gillnet

- This technique relies far less on social engineering techniques and phishers introduce Malicious Code into E-Mails and websites.
- They can, for example, misuse browser functionality by injecting hostile content into another site's pop-up window.
- Merely by opening a particular E-Mail or browsing a particular website, netizens may have a Trojan Horse introduced into their systems.
- In some cases, the Malicious Code will change settings in user's systems so that users who want to visit legitimate banking websites will be redirected to a look-alike Phishing site.

In other cases, the malicious code will record user's keystrokes and passwords when they visit legitimate banking sites, then they transmit those data to phisher for later illegal access to user's financial accounts.

	b	Discuss various types of Phishing Scams Ans: **1.Deceptive Phishing→** • Phishing scams started by broadcasting deceptive E-Mail messages with objective of ID theft. • E-Mails are broadcasted to a wide group of netizens asking about the need to verify banking account information/system failure requiring users to re-enter their personal information. • The netizens easily get enticed and reveal their information by responding to these E-Mails and/or clicking on weblinks or signing onto a fake website designed by the phisher.	L3	10

2.Malware-based Phishing→

- It refers to scams that involve running Malicious Code on the netizens system.
- Malware can be launched as an E-Mail attachment or as a downloadable file from a website or by exploiting known security vulnerabilities.
- For example, small and medium businesses are always found to be ignorant to keep their operating systems (OS) antivirus software up to date with latest patch updates released by vendors.

3.Keyloggers→

- A small integrity program to steal information sends to phisher, keylogger log, to the phisher through the Internet.
- The keyloggers can also be embedded into netizen's browser as a small utility program which can start automatically when the browser is opened or can be embedded into system holes as device drivers.

4.Session hijacking →

- It is an attack in which netizens' activities are monitored until they establish their bonafide credentials by signing into their account or begin the transaction and at that point the Malicious Code takes over and comport unauthorized actions such as *transferring funds without netizen's knowledge*.

5.In-session Phishing→ another parallel session in the same browser.:

- It is a Phishing attack based upon one web browsing session being able to detect the presence of another session (such as visit to an online banking website) on the same web browser and then a pop-up window is launched that pretends to be opened from the targeted session

6.Web Trojans→

- Pops up to collect netizen's credentials and transmit them to the phisher while netizens are attempting to log in. Such pop-ups are usually invisible

7.Pharming→ I

- It is a new threat evolved with a goal to steal online identity of the netizens and Pharming
- Is known as one of the "P" in cybercrime
- In Pharming, following two techniques are used:
- **Hosts file poisoning:**
- The most popular operating system (OS) in the world is Windows and It has "host names" in their "hosts" file.
- A simple text file was used in web address during early days of the Internet. (before DNS)
- Phisher used to "poison" the host file to redirect the netizen to a fake/bogus Website, designed and developed by the phisher, which will "look alike the original website, to Steal the netizen's personal information easily.
- **DNS-based Phishing:**
- Phisher tampers with a DNS so that requests for URLs or name service return a fake address and subsequently netizens are directed to a fake site.
- Netizens usually are unaware that they are entering their personal confidential information in a website controlled by phishers and probably not even in the same country as the legitimate website.
- DNS-based Phishing is also known as DNS hijacking.
- Along with this attack Click Fraud is an advanced form of technique evolved to conduct Phishing scams.

8. System configuration attacks:

- Phisher intrude into netizens system to modify settings for malicious purposes.
- For example, URLs saved under favourites in the browser De modified to redirect the netizen to a fake/bogus "look alike" websites (i.e., URL for a of a bank can be changed from "www.xyzbank.com to www.xyzbanc.com.).

9. Data theft →

- Critical and confidential data getting stolen is one of the biggest concerns in the modern times.

		• As more information resides on the corporate a servers and the web attackers have a boom time because taking away/copying information in electronic form is easy. • Unsecured systems are often found to be inappropriately maintained from cybersecurity perspective. • When such system is connected, the web servers can launch an attack with numerous methods and techniques. Data theft is used in business espionage. **10. Content injection Phishing**: • In these types of scams, phisher replaces the part of the content of a legitimate website with false content. **11. Man-in-the middle Phishing:** • Phisher is positioned himself in between the netizens and legitimate website or system. • Phisher records the input being provided by the netizen but continues to pass it on to the web server so that netizens transactions are nor affected. **12. Search engine Phishing:** • It occurs when phishers create websites with attractive sounding offers (often found too good to be true) and have them indexed legitimately with search engines. • Netizens find websites during their normal course of search for products or services and are trapped to reveal their personal information. • For example, phishers set up fake/ bogus banking websites displaying an offer of lower credit costs or better interest rates than other banks offer of lower credit costs or better interest rates than other banks. **13. SSL certificate Phishing:** • Phishing is an advanced type of scam. Phishers target web servers with SSL certificates to create a duplicitous website with fraudulent webpages displaying familiar "lock" icon. • It is important to note that, in such types of scams, SSL certificates are always found to be legitimate as they match the URL of the fake pages that are mimicking the target brands but in reality, had no connection to these brands displayed. • It is difficult to recognize such websites; however, smart netizens can detect such deception after reviewing the certificate and/or whether the website has been secured with an extended validation SSL certificate.		
		OR		
Q. 08	a	Discuss the various techniques used by Phishers to launch Phishing attacks **Ans:** various techniques used by Phishers to launch Phishing attacks are • URL (weblink) Manipulation • Filter Evasion • Website Forgery • Flash Phishing • Social Phishing • Phone Phishing **1. URL (weblink) manipulation** • URLs are the weblinks (i.e., Internet addresses) that direct the netizens/users to a specific website.	L3	10

- In Phishing attack, these URLs are usually supplied as misspelled, for example, instead of www.abcbank.com, URL is provided as www.abcbank1.com.
- Phishers use Lobsterpot method of Phishing and make the difference of one or two letters in the URLs, which is ignored by netizens.
- This makes a big difference and it directs users to a fake/bogus website or a webpage.

Homograph Attack

- It is used by Phisher to attack on Internationalized Domain Name (IDN) to deceive the netizens by redirecting them on the phony website which look like the original website.
- ASCII has several characters and/or pairs of characters which look alike,
- Eg. 0 and "O". "l" (L lower case) and I("i" alphabet in uppercase) [GOOGLE.COM can be registered as G00GLE.COM]
- Microsoft.com or/rnicrosoft.com
- Phisher could create and register a domain name which appears almost identical to an existing domain and takes netizens to the Phony websites.
- Phisher could easily record password or account details though spoofed websites, while passing traffic through the original websites.

2. Filter Evasion

- This technique use graphics (i.e., images) instead of text to obviate from netting such E-Mails by anti-Phishing filters. Normally, these filters are inbuilt into the web browsers. For example,
- Internet Explorer version 7 has inbuilt "Microsoft phishing filter." One can enable it during the installation or it can be enabled post-installation. It is important to note that it is not enabled by default.
- Firefox 2.0 and above has inbuilt "Google Phishing filter." duly licensed from Google. It is enabled by default.
- The Opera Phishing filter is dubbed Opera Fraud Protection and is included in version 9.5+.

3.Website forgery

- In this technique the phisher directs the netizens to the website designed and developed by him, to login into the website, by altering the browser address bar through JavaScript commands.
- As the netizen logs into the fake/bogus website, phisher gets the confidential information very easily.
- Another technique used is known as "cloaked" URL-domain forwarding and/or inserting control characters into the URL while concealing the weblink address of the real website.

4. Flash Phishing

- Anti-Phishing toolbars are installed/enabled to help checking the webpage content for signs of Phishing, but have limitations that they do not analyse flash objects at all.
- Phishers use it to emulate the legitimate website.
- Netizens believe that the website is "clean" and is a real website because anti-Phishing toolbar is unable to detect it.

5. Social Phishing

- Phishers entice the netizens to reveal sensitive data by other means and it works in a systematic manner.
- Phisher sends a mail as if it is sent by a bank asking to call them back because there was a security breach.

		• The victim calls the bank on the phone numbers displayed in the mail. • The phone number provided in the mail is a false number and the victim gets redirected to the phisher. • Phisher speaks with the victim in the similar fashion/style as a bank employee, asking to verify that the victim is the customer of the bank. For example, "Sir, we need to make sure that you are indeed our customer. Could you please supply your credit card information so that I can verify your identity". • Phisher gets the required details swimmingly. **6. Phone Phishing** • Phisher can use a fake caller ID data to make it appear that the call is received from a trusted organization to entice the users to reveal their personal information such as account numbers and passwords. • Mishing- Mobile Phishing attacks (Vishing and Smishing)		
	b	Discuss various types of Identity Theft techniques. Ans: • 1. Financial Identity Theft • 2. Criminal Identity Theft • 3. Identity Cloning • 4. Business Identity Theft • 5. Medical Identity Theft • 6. Synthetic Identity Theft • 7. Child Identity Theft **Financial Identity Theft** • In total, 25 types of financial ID thefts are investigated by the US Secret Service. • Financial identity occurs when a fraudster makes a use of someone else's identifying details, such as name, SSN and bank account details, to commit fraud that is detrimental to a victim's finances. **Criminal Identity Theft** • It involves taking over someone else's identity to commit a crime such as enter into a country, get special Permits, hide one's own identity or commit acts of terrorism. These criminal activities can include: • 1 Computer and cybercrimes; • 2. organized crime; • 3. drug traffickings • alien smugglings • 5. money laundering. **Identity Cloning** • Identity cloning may be the scariest variation of all ID theft. • Instead of stealing the personal information for financial gain or committing crimes in the victim's name, identity clones compromise the victims life by actually living and working as the victim. • ID clones may even pay bills regularly, get engaged and married, and start a family.	L3	10

- In summary, identity cloning is the act of a fraudster living a natural and usual life similar to a victim's life, may be at a different location.

Business Identity Theft

- Bust-out" is one of the schemes fraudsters use to steal business identity; it is paid less importance n
- parison with individual's ID theft
- A fraudster rents a space in the same building as victims office
- A fraudster rents a space in the same building as victims office
- Hence, it is extremely important to protect business sensitive information (BSI) to avoid any further scams.

Medical Identity Theft

- India is known for medical tourism.
- Thousands of tourists visit India every year, getting their medical problems attended (surgeries, total health check-up Kerala massage etc.,)
- Because of Good Quality and Reasonable in Price in medical services.
- protected health information (PHI).
- The stolen information can be used by the fraudster or sold in the black market to people who "need them.

Synthetic Identity Theft

- This is an advanced form of ID theft in the ID theft world.
- The fraudster will take parts of personal information from many victims and combine them.
- The new identity is not any specific person, but all the victims can be affected when it is used.

Child Identity Theft

- Parents might sometimes steal their children's identity to open credit card accounts, utility accounts, bank accounts and even to take out loans or secure leases because their own credit history is insufficient or too damaged to open such accounts.

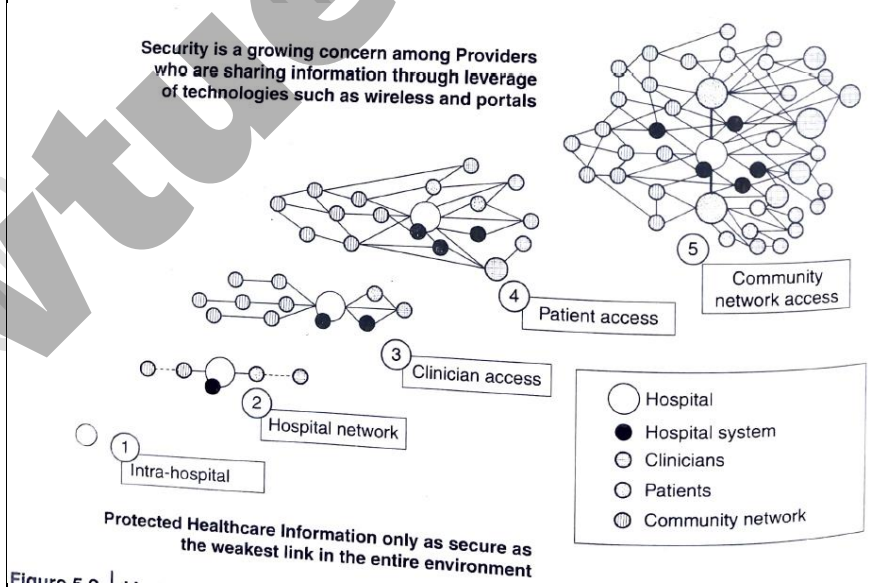


Fig. Medical domain interconnected entities

Module-5

Q. 09 a Discuss the following phases of Forensics life cycles

i) Preparation and Identification

ii) Collection and Recording

Ans:

Preparing for the evidence and identifying the evidence

In order to be processed and applied evidence must be first identified as evidence. it can happen that there is an enormous amount of potential evidence of available for a legal matter and it is possible that the vast majority of the potential evidence may never get identified.

consider that every sequence of events within a single computer might cause interaction with files the file system in which day recite other processes and the program they are executive and
the files they produce and manage and block files and file of various sorts.

Network environment these extents to all network devices potentially all over the world.

evidence of an activity that cause Digital forensic evidences to come into being might be continuous contained in a time stamp associated with the different program in a different computer on the other side of the word that was offset from its usual pattern of behaviour by a few many microseconds.

If the evidence cannot be identified as relevant evidence it may be never be collected or process that all and may not even continue to exit in digital form by the time it is discovered to have relevance

Collecting and Recording Digital Evidence.

- Digital evidence can be collected from many sources.
- The sources are computers, cell phones, digital cameras hard drives, CD-ROM, USB memory devices and so on.
- Non-obvious sources include settings of digital thermometers, black boxes inside automobiles, RFID tags and webpages (which must be preserved as they are subject to change).
- Special care must be taken when handling computer evidence: most digital
- information is easily changed, and once changed it is usually impossible to detect that a change has taken place unless other measures have been taken.
- For this reason, it is common practice to calculate a cryptographic hash of an evidence file and to record that hash elsewhere, usually in an investigator's notebook, so that one can establish at a later point in time that the evidence has not been modified as the hash was calculated.
- Figures and show the media that typically holds digital evidence.

Collecting volatile data requires special technical skills

If the machine is still active any intelligence that can be gained by examining the applications currently open is recorded.

if the machine is suspected of being used for illegal communication such as terrorist traffic not all of this information may be stored on the hard drive.

If information told solely in Random Access Memory and not recovered before powering down it may be lost.

This results in the need to collect volatile data from the computer at the onset of the response.

Memory falls under the family of solid-state non-time memory it is used in some drive USB sticks cell phone game console secure digital card and multimedia cards.

This technology differs from the normal hard disc by not containing any moving parts in every device that interact with our daily life.

The benefit of Embedded memory continues to increase life expectancy. figure 5.8 shows the various types of embedded memories inside a computer ROM, PROM, EPROM, EEPROM.

Fig.: Media that can hold digital evidences_.

Fig. Some more media that can hold digital evidences

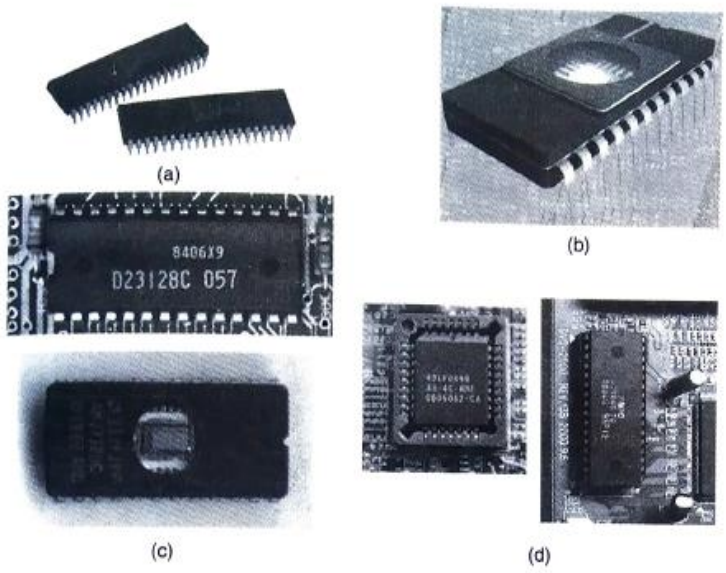


Fig. Embedded memories inside computer

	b	List various Computer Forensics services available, explain any two of them. **Ans:** Digital evidence plays an important role in threat management life cycle, from incident response to high-stakes corporate litigation. Evidences involve computer hard drives, portable storage, floppy diskettes, portable music players and PDA's, etc..... Key evidences often reside on more than a user hard drive or file server, requiring the capture and analysis of evidence from enterprise productivity servers, network logs or proprietary databases. Many threats arise from illegal internet activities that extend beyond the firewall and require new investigative and forensics approaches. Forensics professionals need supporting solution for the acquisition, management and analysis of digital evidence. **Such computer forensics services include the following:** 1. Data culling and targeting 2. Discovery/subpoena process 3. Production of evidence 4. Expert affidavit support 5. Criminal/Civil testimony 6. Cell phone forensics 7. PDA (Personal Digital Assistants) forensics	L2	6
	c	Briefly explain RFC2822 Ans: RFC2822 is the Internet Message Format. According to the Internet specification RFC2822, there are several formats of valid E-Mail addresses, like joshi@host.net, john@[10.0.3.19], "Joshi Ganesh'@host.net or "Joshi Ganesh"@[10.0.3.19]. Many E-Mail address validators on the Web fail to recognize some of those valid E-Mail addresses. Some examples of invalid E-Mail addresses are as follows: 1. joshi@box@host.net: Two at signs (@) are not allowed; 2. joshi@host.net: Leading dor () is not allowed; 3. joshi@-host.net: Leading dash (-) is not allowed in on domain name; 4. joshi@host.web: Web is not a valid top-level domain; 5. joshi@[10.0.3.1999]: Invalid IP address. The RFC2822 standard applies only to the Internet Message Format and some of the semantics of messages contents. It contains no specification of the information in the envelope. RFC2822 states that each E-Mail must have a globally unique identifier. It is included into the header of an E-Mail.	L2	4

		OR		
Q. 10	a	Discuss the following phases of Forensics life cycle i) Storing and Transporting ii) Examination/Investigation Ans: ***Storing and Transporting digital Evidence*** The following are specific practices char have been adopted in the handling of digital evidence. **1.** Image computer media using a write-blocking tool to ensure that no data is added to suspect device; **2.** Establish and maintain the chain of custody (refer co Section 5.7); **3.** Document everything that has been done; **4.** Only use cools and methods that have been tested and evaluated to validate their accuracy and reliability. Storage must be adequately secure to assure proper "chain of custody Many things can go wrong in storage, including decay over time; environment changes resulting in the presence of a necessary condition for preservation; ***Examining/Investigating digital Evidence*** Investigation in which the owner of the digital vision has not given consent to have his or her media examined as in some criminal cases some care must be taken to ensure that the forensic specialist has the legal authority to C copy and examine the data sometimes authority stems from search warrant. It is understanding the difference between live and dead analysis after that we explain about the imaging of the media. Traditionally computer for insect investigations for performed on a data at rest. For a exam well the content of hard drives the scan we brought thought of as a analysis investigators were told to shut down computer system when they are impounded for fear that digital time bomb might cause data to be at rest. Process of creating an exact duplicate of the original evidence media is often called imaging computer forensics software packages make this possible by converting an entire hard drive into a single searchable file is file is called an image.	L2	10
	b	Discuss the need for concept of Computer Forensics. ▶ Ans: The convergence of information and communication technology (ICT) advances and the pervasive use of computer worldwide together have brought many advantages to mankind. ▶ At the same time, this tremendously high technical capacity of modern computer/computing devices provides avenues for misuse as well as opportunities for committing crime. ▶ This leads to new risks for computer users and also increased opportunities for social harm. ▶ The users, businesses and organizations worldwide have to live with a constant threat from hackers who use a variety of techniques and tools to break into the computer to steal information, change data and cause havoc. ▶ The widespread use of computer forensics is the result of two factors: 1.The increasing dependence of law enforcement on digital evidence. 2. Ubiquity of computers that followed from the microcomputer revolution. ▶ The media on which clues related to cybercrime reside may vary from case to case. There are many challenges for the forensics investigator because storage devices are getting miniaturized due to advances in electronic technology; for example, external storage devices such as mini hard disks (pen drives) are available in amazing shapes.	L3	6

- Looking for digital forensics evidence (DFE) is like looking for a needle in the haystack.
- Here is a way to illustrate why there is always the need for forensics software on suspect media - the capacity of a typical regular hard disk is 500 GB (gigabytes).
- In an A4 size page, there are approximately 4,160 bytes (52 lines x 80 Characters = 4160 bytes assuming 1 byte per character). This is equivalent to 4 KB (kilobytes). An A4 size of paper sheet has thickness of 0.004 inches.
- Data of 4 MB (megabyte; 1,000 times of 4 KB) when printed on A4 size of paper would be 4 inches thick.
- Data of 4 GB if printed on A4 sheet would be 4,000 inches, that is, 1,000 times of be virtually impossible to "retrieve" relevant forensics data from this heap!! There comes the help from forensics MB.
- This would turn out to be 4 inches thick. The printout of 500 GB would be 500,000 inches!
- It would be virtually impossible to "retrieve" relevant forensics data from this heap!!

There comes the help from forensics software-it helps sieve relevant data from the irrelevant mass (vital few from trivial many as the proverb goes).

Fungibility:

- ***"Fungibility"*** means the extent to which the components of an operation or product can be inter- changed with similar components without decreasing the value of the operation or product.
- For a person to be considered as "identifiable person," he/she must always have the physical custody of a piece of evidence.
- Practically speaking, this means that a police officer or detective will take charge of a piece of evidence, document its collection and hand it over to an evidence clerk for storage in a secure place.
- All such transactions as well as every succeeding transaction between evidence collection and its appearance in court need to be completely documented chronologically to withstand legal challenges to the authenticity of the evidence.
- Documentation must include conditions under which the evidence is collected, the identity of all those who handled the evidence, duration of evidence custody, security conditions while handling or storing the evidence and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs (along with the signatures of persons involved at each step).
- Chain of custody is also used in most evidence situations to maintain the integrity of the evidence by providing documentation of the control, transfer and analysis of evidence.
- Chain of custody is particularly important in situations where sampling can identify the existence of contamination and can be used to identify the responsible party.

	c	Briefly explain Network Forensics • Open networks can be source of many network-based cyberattack • Wireless Forensics • Wireless Forensics is a discipline included within the computer forensics science, and specifically, within the network forensics field. • The goal of wireless forensics is to provide the methodology and) tools required to collect network traffic that can be presented as valid digital evidence a court of law. •	L2	4

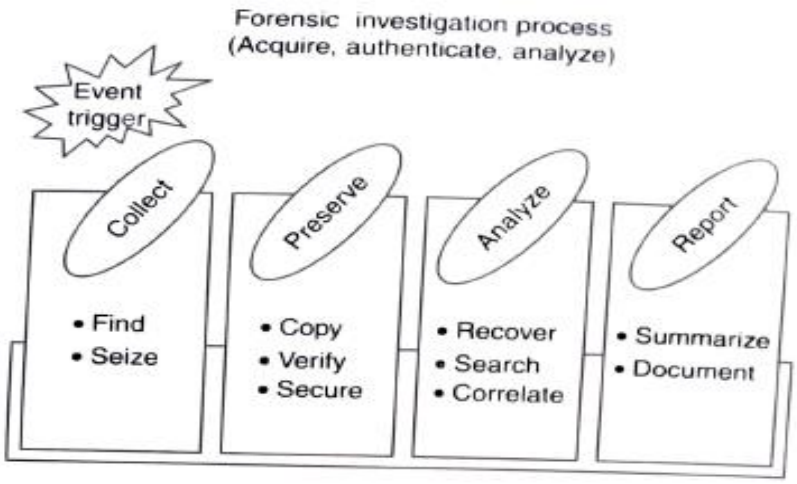


Fig. Maintaining chain of custody

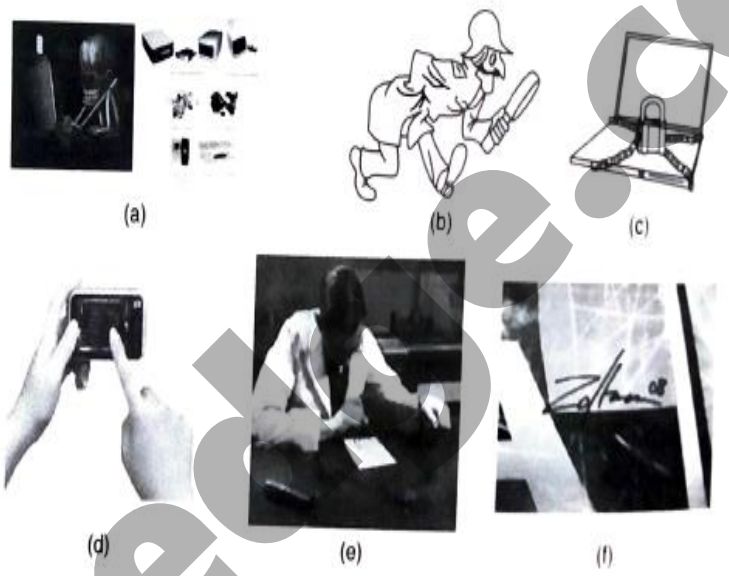


Fig. : Maintaining chain of custody 2. (a) Source of evidence - where did it come (b). Who found it? (c) Where was it stored/locked up? (d) Who touched it/tampered With it? (e) What did they do to it? What did they do with it? (f) Human signature always required