1(a)
Security of web browser like Mozilla Firefox

Browser security is an important part in keeping your information safe: Your browser is the bridge between your system and the internet and also the first line of defence against malware threats.

Browser features and their security vulnerabilities: Browsers use many tools for various tasks, such as Java, Flash Player, ActiveX, etc, comes with security flaws which cybercriminals exploit to get access to your PC. Verify if these tools are needed or not.

Deactivate ActiveX: Preinstalled on Internet Explorer or Microsoft Edge. Interacts with other sites and his creates security problems by giving malicious websites into your PC. ActiveX is rarely used nowadays, so beware.

Try to disable JavaScript: JavaScript is a programming language used by websites to run various programs and features. Gives pop-ups in YouTube or Google Doc for advertising. Cybercriminals use JavaScript in malicious ways in order to infect your device with malware and other harmful software. If you disable JavaScript altogether you will get a much quicker and simplified browser experience, with little to no ads, pop-ups, page loads faster, etc.

Firefox hacks and tips for better security:
Hamburger icon top right → Options
General tab →Downloads section →Select “Always asks me where to save files” so that browser don't automatically download malicious files.
Privacy tab →Tracking section →"manage your Do Not Track settings” check “Always apply do not track”.
→History section →choose “Firefox will never remember history”, select “Use custom settings for history”. Check “Always use private browsing mode”.
Security tab →Security section →set up a Primary/Master Password.

2(a)
Security vulnerabilities of e-commerce services

Vulnerabilities due to Buffer Overflow: A buffer overflow condition occurs when a program attempts to copy more data in a buffer than it can hold. Buffer overflow is probably the best known form of software security vulnerability. At the code level, buffer overflow vulnerabilities usually involve the violation of a programmer's assumptions. Hackers use buffer overflows to corrupt the execution stack of a web application. Buffer overflow flaws can be present in both the web server or application server products that serve the static and dynamic aspects of the site. Buffer overflows generally resulted in to crashes.

Vulnerabilities due to Log Forging: Writing invalidated user input to log files can give access to attacker for forging log entries or injecting malicious content into the logs. Log forging vulnerabilities occur in following conditions: i) Data copied to an application from an unreliable source. ii) The data is copied to an application or system log file. Applications uses log file to store a history of events for later review and record, statistics gathering, or debugging.

Vulnerabilities in database servers: There are various techniques to attack a database. External attacks may exploit configuration weaknesses that expose the database server. Also weak and insecure Web application can be used to exploit the database. An application with excess privilege in the database can put database at risk. The main threats to a database
server are:

1. **SQL injection:** Technique used to attack database through website entry fields.
2. **Network eavesdropping:** It is a network level attack consisting of capturing packets from the networked computers.

3. **Unauthorized server access:** Attacked made unauthorized access through various loopholes in the system such as O/S, non-availability of firewall etc.
4. **Password cracking:** Technique of recovering password from data stored in computer.

3(a)
Techniques uses for web based password capturing

It is for attackers to take advantage of weak passwords, and therefore don't use a password manager or other means to make their passwords stronger. Proper use of a password manager can thwart some of these attacks and limit damages from most other types of attacks.

1. **Mass Theft of Password Files:** User names and passwords routinely get stolen while your computer is off and disconnected from the internet. Web sites with many users and weak security are prime targets for attackers who want to steal a password file which lists all user names and passwords. Recent examples include Monster.com and RockYou.com. While most sites do not store passwords as clear text, many sites store passwords in a form that can be read using widely available rainbow table software. For people who use the same password on many sites, the theft of this password on one site can be the starting point for an attack on all of your accounts.
   Protection:
   A simple and effective defence for users is to only use long, randomly generated passwords. How long? 15 characters. Rainbow tables easily crack passwords 8 or fewer characters long and in some cases up to 14 characters.
   Damage Control:
   In the unlikely case that a rainbow table attack manages to crack one of your 15 character passwords, at least your damages will be limited to one account if you have a unique password for each account. Change the password of any account that becomes compromised due to mass theft.
2. **Brute Force:** Brute Force refers to discovering passwords through trial and error, similar to trying every possible combination on a lock. The most well-known form of brute force attack is for password cracking software to methodically try millions of passwords on one specific user name on a specific account. A typically weak password can be cracked in less than a day using this method.
3. **Eavesdropping: Keystroke Logger on Your Browser:** Malicious JavaScript can be injected into any browser on any system, visiting any web site. Keystroke logging is something that is done by some of these JavaScript injections. In most browsers, malicious JavaScript can log keystrokes in all open tabs, until the browser is closed. Usernames and passwords entered during the session can be captured this way.
   Protection:
   Keystroke logging via browser is growing more common but is unfortunately one of the more difficult threats to defend against. Defences include: Use Firefox in conjunction with the No Script extension. A simpler option is to only access the internet using the Google Chrome browser, which is designed so that malicious JavaScript can be theoretically contained to a single tab. Some password managers such as RoboForm enter passwords and usernames in a way which most JavaScript keystroke loggers cannot intercept.
   Damage Control:
   Your damages are limited to logins captured while browsing, so long as you have a unique password for each account. Immediately change the password of the affected accounts. If using a browser-based or web-based password manager, you should also change your master password.
4. **Eavesdropping: Public Wi-Fi Monitoring:** Passwords are frequently stolen on public computers and over public Wi-Fi connections, using free Wi-Fi traffic monitoring software that is simple to operate.
   Protection:
   Never log in to online accounts using a public computer. When using open Wi-Fi hot spots, you should only log in with your own notebook with services that enforce secure logins and sessions (HTTPS), perhaps using the Firefox Add-on HTTPS Everywhere to help. It is far safer to access email and other accounts using your phone data service, if you have one.

Damage Control:
If you discover that this type of attack has occurred, then you will need to change the password for all of your accounts as well as your master password. If you know exactly when the attack occurred, you can change passwords only for the accounts you used during that session.

4(a)
Sniffing attack: problems and its preventive measure

Sniffing refers to the use of software or hardware to watch data as it travels over the Internet. There are some legitimate uses for the process. It is then called network analysis and helps network administrators diagnose problems. In the hands of the wrong person, however, a sniffing program can collect passwords and read email. Sniffing is considered a passive security attack, according to TechiWarehouse.

Problems:
- Sniffing means a loss of privacy along with trust for those on a network.
- Sniffing can compromise the privacy of passwords. An Ethernet sniffer can easily detect passwords.
- Sniffing can allow unauthorized persons access to financial information, including account numbers for banking and credit cards.
- Sniffing private and confidential information contained in email is very common.
- Sniffing can yield low-level protocol information.

Prevention:
- New data suggests that there is no way to detect when your computer has been sniffed. Measures may be taken, but it's almost impossible to totally prevent being sniffed.
- Encryption helps. Replacing the hub with a switch may also add protection. Taking care when using public Wi-Fi may also help reduce exposure.
- Don't click on an email link that requests personal information, even if it looks like a legitimate site.
- Be suspicious of anyone asking for personal information.
- Don't send personal information or financial information through a Web site. If caught and provide information notify the companies you do business with right away to put a fraud alert on your account. Also contact Consumer Fraud Reporting, a free service that helps protect consumers against fraud.

6(a)
Download a website using Website Copier tool (HTTrack)

HTTrack is a free (GPL, libre/free software) and easy-to-use offline browser utility. It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer.
1. Install **WinHTTrack**.
2. Create a folder on the Desktop and rename the folder.
3. Select the new project from the file menu.
4. Enter the project name in new project field.
5. Give the path where you need to download the files. In order to do this, Click on Desktop and then click the folder created. Press OK.
6. WinHTTrack option window is opened select the scan rules. Select all type of file to start the scan.
7. Now all the extension is added for the scan.
8. Now type the URL address to scan.
9. Enable the connection adjustment if needed and click the finish button. Mirroring process is get started.
10. All information and files are saved in the folder created. Manipulate as per your wish.

5(a)
Study of cyber forensic tools

Name	Platform	License	Version	Description
Autopsy	Windows, macOS, Linux	GPL	4.16	A digital forensics platform and GUI to The Sleuth Kit
AXIOM	Windows	proprietary	4.9	Full digital forensics suite by Magnet Forensics - Windows, MacOS, mobile and cloud supported in one platform
COFEE	Windows	proprietary	n/a	A suite of tools for Windows developed by Microsoft
Digital Forensics Framework	Unix-like/Windows	GPL	1.3	Framework and user interfaces dedicated to digital forensics
EnCase	Windows	proprietary	8.11	Digital forensics suite created by Guidance Software
Forensic Explorer	Windows	proprietary	5.4.2.1122	Digital forensics suite created by GetData
FTK	Windows	proprietary	7.3	Multi-purpose tool, FTK is a court-cited digital investigations platform built for speed, stability and ease of use.
IPED	Unix-like/Windows	GPL	3.17.2	Digital forensics tool created by the Brazilian Federal Police
ISEEK	Windows	proprietary	1	Hybrid-forensics tool running only in memory - designed for large networked environments
IsoBuster	Windows	proprietary	4.7	Essential light weight tool to inspect any type data carrier, supporting a wide range of file systems, with advanced export functionality.

Mobile Device Investigator	Windows,	proprietary	2.1	iOS and Android digital forensics and Smartphone triage tool by ADF_Solutions
Netherlands Forensic Institute / Xiraf/ HANSKEN	n/a	proprietary	n/a	Computer-forensic online service.
Open Computer Forensics Architecture	Linux	LGPL/GPL	2.3.0	Computer forensics framework for CF-Lab environment
OSForensics	Windows	proprietary	8	Multi-purpose forensic tool
PTK Forensics	LAMP	proprietary	2.0	GUI for The Sleuth Kit
SANS Investigative Forensics Toolkit - SIFT	Ubuntu		2.1	Multi-purpose forensic operating system
SPEKTOR Forensic Intelligence	Unix-like	proprietary	6.x	Easy to use, comprehensive forensic tool used worldwide by LE/Military/Agencies/Corporate - includes rapid imaging and fully automated analysis.

The Coroner's Toolkit	Unix-like	IBM Public License	1.19	A suite of programs for Unix analysis
The Sleuth Kit	Unix-like/Windows	IPL, CPL, GPL	4.1.2	A library of tools for both Unix and Windows
Windows To Go	n/a	proprietary	n/a	Bootable operating system
X-Ways Forensics	Windows	proprietary	n/a	Supports images and a bunch of volumes. And also memory and ram analysis

7(a)
Defamation and repairment solution caused by caused virus and Trojans

Virus:
The most potent and vulnerable threat of computer users is virus attacks. Virus attacks hampers important work involved with data and documents. It is imperative for every computer user to be aware about the software and programs that can help to protect the personal computers from attacks. One must take every possible measure in order to keep the computer systems free from virus attacks.
The top sources of virus attacks are highlighted below:

- Downloadable Programs
- Cracked Software
- Email Attachments
- Internet
- Booting From CD

Trojans:
Trojan horse attacks pose one of the most serious threats to computer security. If you were referred here, you may have not only been attacked but may also be attacking others unknowingly. According to legend, the Greeks won the Trojan war by hiding in a huge, hollow wooden horse to sneak into the fortified city of Troy. In today's computer world, a Trojan horse is defined as a "malicious, security breaking program that is disguised as something benign". For example, you download what appears to be a movie or music file, but when you click on it, you unleash a dangerous program that erases your disk, sends your credit card numbers and passwords to a stranger, or lets that stranger hijack your computer to commit illegal denial of service attacks.

Repairing the Damage

1. **Anti-Virus Software:** Compared to traditional viruses, today's trojans evolve much quicker and come in many seemingly innocuous forms, so anti-virus software is always going to be playing catch up. Also, if they fail to find every trojan, anti-virus software can give you a false sense of security, such that you go about your business not realizing that you are still dangerously compromised.
2. **Anti-Trojan Programs:** These programs are the most effective against trojan horse attacks, because they specialize in trojans instead of general viruses. A popular choice is The Cleaner, To use it effectively when you are done, make sure you've updated Windows with all security patches, then change all your passwords because they may have been seen by every "hacker" in the world.

8(a)
Security Issues and Threats in E-Mail Application

Security Issues and vulnerability in Email System:
E-mail is one of the main modes of communication today but in the following section it can be seen how insecure it is. Because e-mail is widely deployed, well understood, and used to communicate with untrusted, external organizations, it is frequently the target of attacks. Attackers can exploit e-mail to gain control over an organization, access confidential information, or disrupt IT access to resources.

Threats in Email Communication:

- **Eavesdropping:** E-mail messages pass through networks which are part of big picture i.e. Internet with a lot of people on it. So it is very easy for someone to track or capture your message and read it.

- **Identity Theft:**
  Means someone pretend to be you on the network. It may be possible if not proper security protocols are followed that someone may steal or capture your username/password and used to read your email messages. Further also send email messages from your account without your knowledge.

- **Unprotected Backups:**
  Messages generally stored in plain Text on SMTP server and also backups can be created. Even if you delete the message they can be residing on the severs/backup-servers for years. So anyone who accesses these servers can also access or read your message.

- **Repudiation:**
  As it is known that email messages can easily be forged so anyone sending you some message can later on deny regarding sending of message and it is very difficult to prove it. This has implications corresponding to emails use as contracts in business communications.

- **Email spoofing:**
  Sometime email that pretends to be received from an authentic source but in actual it is send from somewhere else.

- **Email Spamming:**
  Spam or junk mail refers to sending of email to no. of persons for any advertisement purpose or for some malicious intent. To send spam often lists are created by searching data from Internet, or by stealing mailing list from the internet.

- **Email bombing:**
  E-mail "bombing" is refers to sending identical mail repeatedly by abusers to a particular address/user.

- **Sending threats:**
  Threatening mails are sending to users which disturb their state of mind or to provoke them to take some wrong step. Sometimes false statements are also forwarded to third parties or users to injure the reputation of some particular person. It is called as Defamation, a communication is not considered defamatory unless it is forwarded to someone other than the target.

- **Email frauds:**
  Email Fraud is the intentional deception made for some personal or monetary gain. Emails used as tools to spread malicious software: Emails are also used as tools to spread viruses, worms and other malicious software. They are attached to your emails as attachment, when you click on them they attack your computer or browser.