1. Study of Step to protect your personal computer System by Creating user Account with password and types of user Accounts for Safety and Security.

→ Theory.

Steps to protect your personal computer System by creating user Accounts with password.

Step :-1

→ Create a Separate user account for each person who will be using your computer. This will help to keep your personal files and Setting Separate from those of other users.

Step :-2.

→ Set Strong password for all user accounts. Your password Should be at least 8 character long and include a mix of upper and lowercase letter, number & Symbol.

Step:3

3 Enable two-factor authentication (2FA) for all user accounts. 2FA adds an extra layer of security to your accounts by requiring you to enter a code from your phone in additional to your password when logging in.

* There are three main types of user accounts on window computer.

1) Administrator Account :- This account has the highest level of permission and can access and modify all system setting and files.

2) Standard user account :- This account has limited permission and can only access and modify files and setting that are specifically assigned to it.

Teacher's Signature

Date

Expt. No.

Page No. 3

3) Guest account :- This account has the lowest level of permission and can only access and modify file and setting that are specifically assigned to it.

Teacher's Signature

Date

Expt. No.

Page No. 4

2) Study the step to protect a MicroSoft Word Documment of different version with different operating System.

→ Theory:-

MicroSoft word is a Software tool that allow us to create documment files like articles, office letter, project files, and many more in a very simplest and easy manner.

This MS word Software saves our articles / letter in a form of a documment and save it on the computer forver.

→ Steps to protect the Documment.

* Step:-1

→ On the Navigation menu bar click on the file option.

Teacher's Signature

Date

Expt. No. Page No. 5

* Step 1-2

→ Next click on the info option from the left panel.

* Step-3

→ Then click on the down arrow icon in protect Document option.

* Step-4

→ Then select Encrypt with password option.

* Step-5

→ A Encrypt Document dialog box will open where you can set your password.

* Step-6

→ Create a strong password for your document.

Teacher's Signature

Step: 7.

→ Then click on ok.

Step: 8

→ Again a confirm password dialog box will open to confirm your password.

Step: 9

→ Reenter your password.

Step: 10

→ Next click on the ok option.

→ Finally, Your document is protected with a password. Whenever anyone tries to open it, it will first ask for a valid password as shown.

Date

Expt. No. Page No. 7

3) Study the step to remove password from MicroSoft Word.

→ Removing the password of a word document.

Step:-1

→ Open your word document and enter its password.

Step:-2

→ click on file → info → protect Document → Encrypt with password.

Step:-3

→ Delete the password in the password box. and then click ok.

Teacher's Signature

Date

Expt. No. Page No. 8

4) Study various method of protecting and securing databases.

→ There are many different methods of protecting and securing databases.

1) Encryption :- It is the process of converting data into a format that cannot be read by unauthorized users. Data can be encrypted at rest or in transit.

2) Authentication :- It is the process of verifying the identity of a user or device. This can be done using a variety of method such as password, multi-factor authentication.

3) Authorization :- It is the process of granting or denying access to database resource based on a user's identity and role.

4) Firewalls :- It can be used to restrict access to database server and to block malicious traffic.

Teacher's Signature

Date

Expt. No.

Page No. 9

5) Auditing :- It is the process of logging and reviewing database activity. This can be used to detect unauthorized access to the database and to investigate security incidents.

6) Backup :- It is important to regularly backup your database so that you can restore in the event of a data loss event.

Teacher's Signature

Date

Expt. No. Page No. 10

S) Study "How to make Strong password" & "Password cracking technique".

→ A Strong password is one that is difficult for attacking to guess or crack.

→ use a mix of upper and lowercase, letter, numbers and Symbols. The longer and more complex your password is the harder it will be to crack.

→ Avoid using personal information in your passwords, such as your name, birthdate or address.

→ Do not reuse password across different accounts. If one of your account is compromised, attackers could use the same password to access your other accounts.

→ Consider using a password manager to help you create and store password.

Teacher's Signature

Date

Expt. No. Page No. 11

→ Password cracking techniques.

→ Attackers use a variety of techniques to crack password.

→ Brute force attack:- A brute force attack is a trial - and - error attack in which the attacker tries every possible combination of character until they find the correct passwords.

→ Dictionary attacks:- A dictionary attack is an attack in which the attackers tries to guess the password by trying word from a dictionary or other list of common words and phrases.

→ Rainbow table attack:- A rainbow table attack is an attack in which the attacker uses a pre-computed table of pre-hashed passwords to crack passwords.

→ Phishing attack:- A phishing attack is an in which the attacker tries to trick the user into revealing their password.

Teacher's Signature

Date

Expt. No. Page No. 12

7) Study of the feature of firewall in providing network security and to set firewall security.

→ A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

→ Packet filtering :- It can filter network traffic based on a variety of criteria, such as IP address, port number, and protocol.

→ Stateful inspection :- Firewall can inspect the state of networking traffic to identify and block malicious activity.

→ Instrusion Prevention :- firewall can prevent a variety of network attacks, such as Dos attack, port scanning and malware infection.

Teacher's Signature

Firewalls also play an important role in protecting networks from unauthorized access and malware infection.

To Set Firewall Security in Windows:-

1) Open control panel.
2) Click System and Security
3) Click Windows Defender Firewall.
4) Click Turn Window Defender Firewall on or off.
5) Select the type of network you want to protect and turn on Window Defender Firewall.
6) Click ok.

Date

Expt. No.

Page No. 17

8) Step to ensure Security of any one Web browser (Mozilla Firefox / Google Chrome)

→ Theory:-

1) Use the latest version of your browser.

2) Enable automatic updates

3) Use a strong password and enable two factor authentication.

4) Be careful about what extention you install.

5) Be careful about what links you click on and what attachments you open.

Teacher's Signature

In addition to these general steps, there are some specific security setting that you can adjust in your browser.

Google Chrome:

→ Enable Safe Browsing :- This feature help to protect you from malware and phishing attacks.

Disable third-party cookies :- This feature helps to protect your privacy by blocking third-party cookies from tracking you online.

Enable HTTPS-always :- This feature forces your browser to use HTTPS whenever possible, which encrypts your traffic and helps to protect your privacy.

Date

Expt. No. _____ Page No. 19

9) Study of different type of vulnerabilities for hacking a websites / web Application.

→ Theory.

→ There are many different types of vulnerabilities that can be exploited to hack websites and web applications.

→ Some of the most common vulnerabilities includes:-

Injection vulnerabilities:-

→ It allow attackers to inject malicious code into a web application.

→ This code can then the executed by the web application, giving the attacker control of the application or access to sensitive data.

Teacher's Signature _____

Cross Site Scripting (XSS)

→ It allow attackers to inject malicious code into a web page.
→ This code can then be executed by the victim's browser.

Broken authentication and Session Management.

→ It allow attackers to hijack or steal user accounts or to impersonate legitimate users.

Insecure direct object references.

→ It allow attackers to access sensitive data or functionality that they should not have access to.

Security misconfiguration :

→ These caused by incorrect or insecure configuration of web applications or servers.

Cross-Site request forgery (CSRF)

* It allow attackers to trick user into performing actions that they do not intend to perform.

* These are just a few of the many different type of vulnerabilities that can be exploited to hack website and web-application.

10) Analysis the security vulnerabilities of E-commerce services.

→ E-commerce service are particularly vulnerable to attacks because they handle sensitive customer data, such as credit card numbers, address and passwords.

Some of the most common security vulnerabilities in e-commerce service include:-

1) Implement a comprehensive security program.

This program should include measure such as security awareness training for employee, regular security audits.

2) Use a web application firewall.

A WAF can help to protect your web application from a variety of attacks, including injection attacks, xss attack, & CSRF attacks.

Teacher's Signature

Date

Expt. No.

Page No.

→ Keep your Software up to date. Software developer regularly.

Teacher's Signature