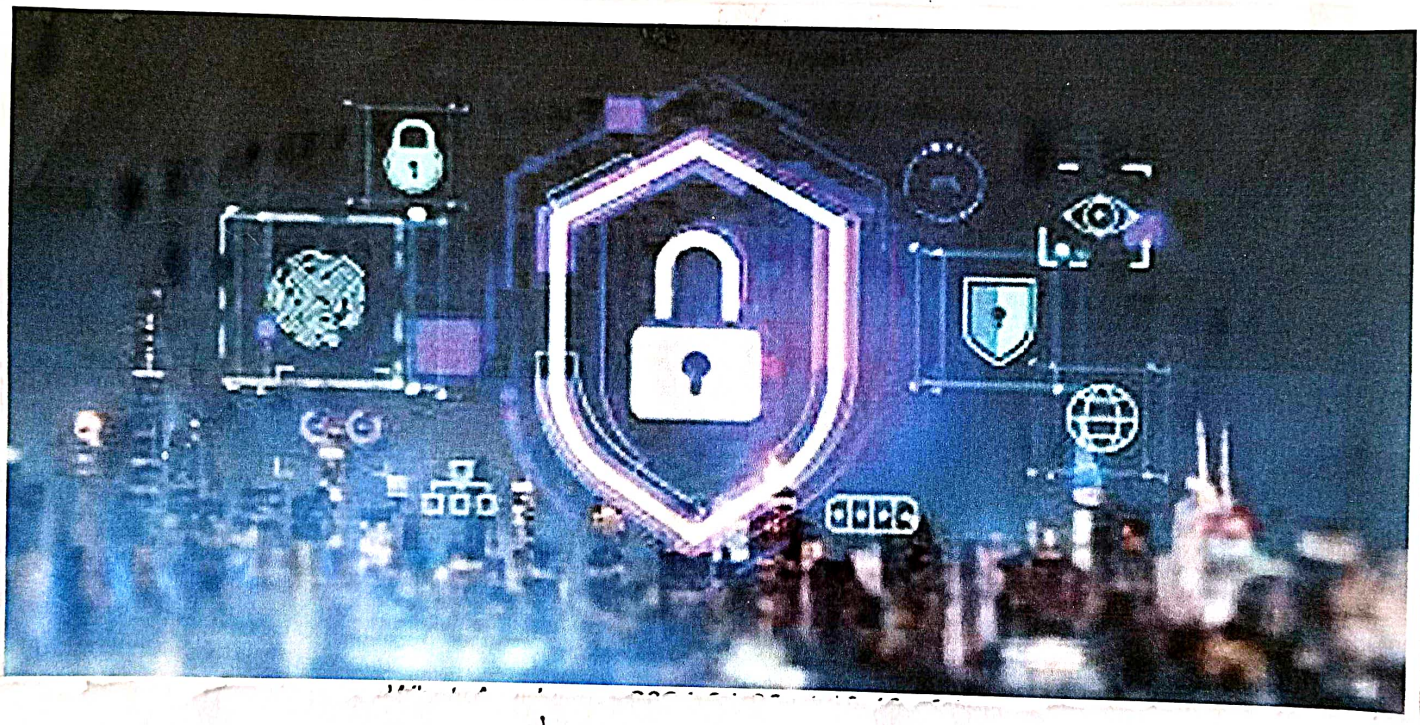
MASTERING WEBSITE SECURITY: TECHNIQUES FOR EFFECTIVE DEFENSE.

: Effective cyber defense relies on a combination of techniques and strategies.



Cybercrime is an increasingly serious problem, and to address it, strong cybersecurity is critical. Individuals, governments, for-profit companies, not for profit organization, and educational institutions are all at risk of cyber attacks and data breaches. of Cyber Security.

MASTERING WEBSITE SECURITY : TECHNIQUES FOR EFFECTIVE DEFENSE

Understanding Website Security Fundamentals.

Web Application Penetration Testing

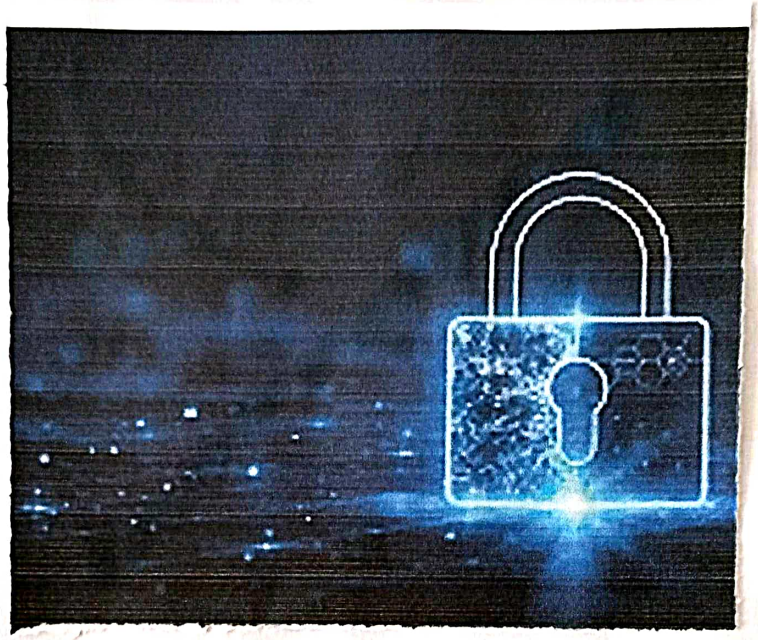
Vulnerability Analysis And Assessment

Defense Mechanism Design and Implementation

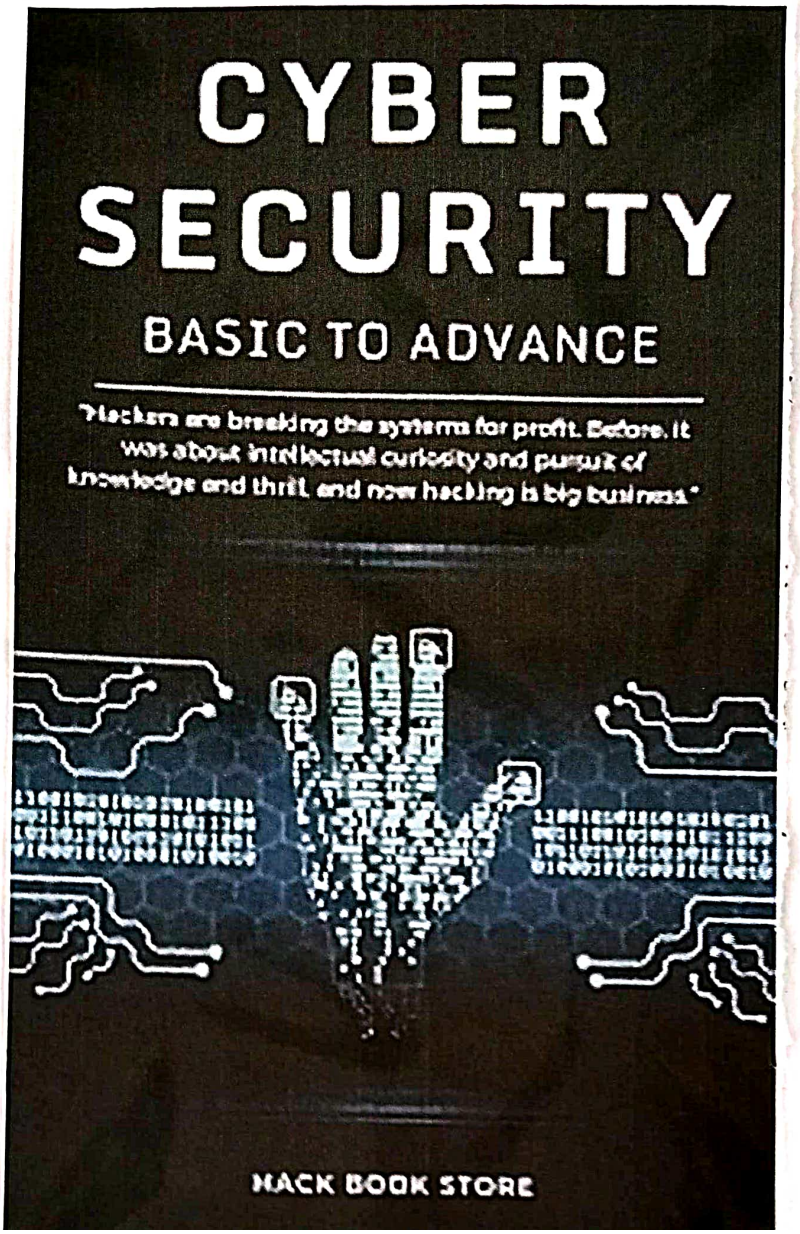
Incident Response Planning And preparation

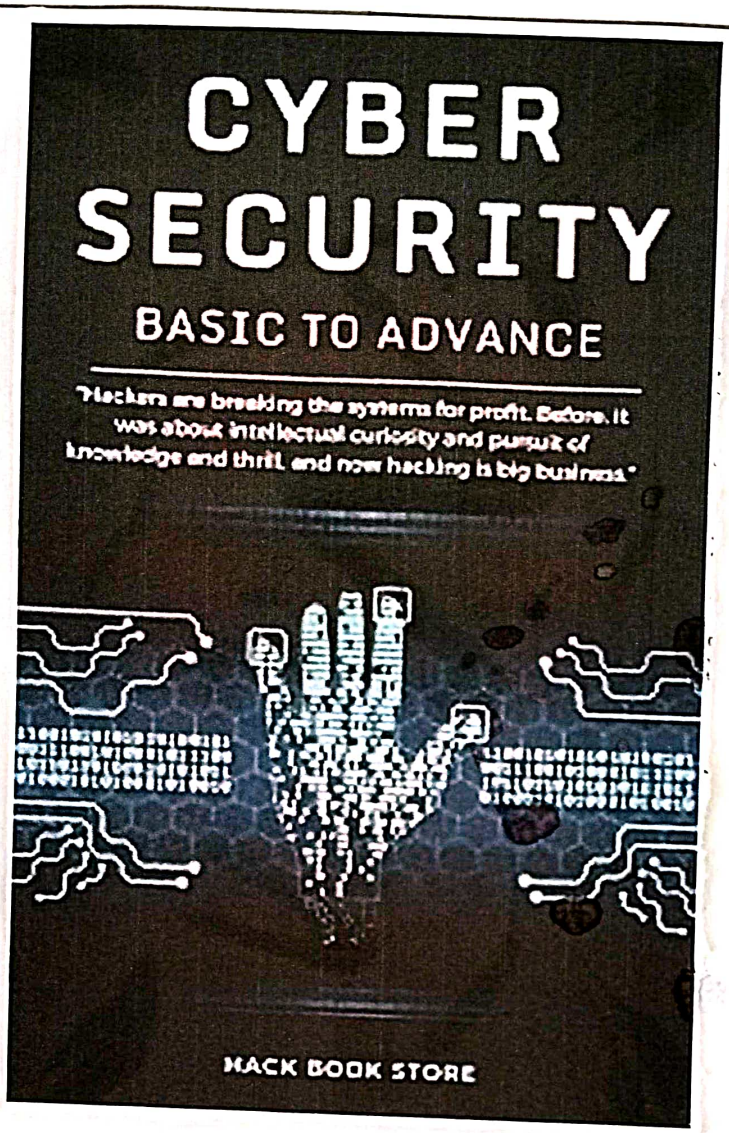
Continuous Monitoring And Improvement.

8 Simple Ways to improve your Website Security:



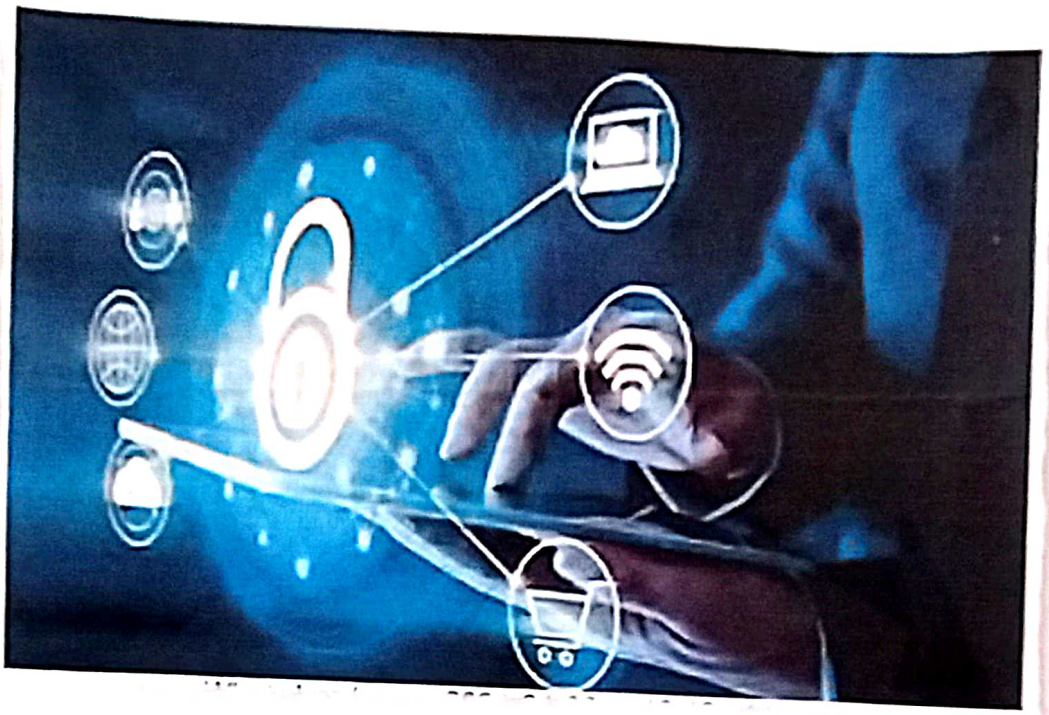
1. Keep your Software up-to-Date.
2. Enforce a Strong password policy.
3. Encrypt your Login pages....
4. Use a Secure Host.
5. Backup your Data
6. Scan your Website for vulnerabilities.
7. Hire a security Expert.


CYBER
SECURITY
BASIC TO ADVANCE
"Hackers are breaking the systems for profit. Before, it was about intellectual curiosity and pursuit of knowledge and thrill, and now hacking is big business"
HACK BOOK STORE



Cyber Security basic involve protecting system, networks, and data from digital attacks. It includes measures like strong passwords, regular software updates, firewalls, and antivirus software to safeguard against threats like malware, Phishing and unauthorized access. Training user's to recognize and avoid potential threats is also essential.

CYBER SECURITY



Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroyed sensitive information; extorting money from user via ransomware; or interrupting normal business processes.

Mastering Website Security: Techniques For Effective Defense:

Mastering website security is essential for protecting your site and its data from various online threats. Here's a comprehensive guide help you:

1. Stay updated:
   Keep all software, including your CMS.
   CMS ⇒ [content management system) plugins, and themes, up to date. Developers often release security patches to address vulnerabities.

2. USE HTTPS:
   Encrypt data transmitted between your website and user's browsers using HTTPS.
   This prevents eavesdropping and data tampering.

3. Strong passwords:
   Enforce strong password's policies for user account including a mix of uppercase and lowercase letters, numbers and special characters, consider implementing multi-factor authentication for added security.

4 Firewalls:

Use web applications firewalls [WAFs] to monitor and filter HTTP traffic to and from your web application. This helps block malicious traffic and attacks.

5. Regular Backups:

perform regular backup's of your website and database. In case of security breach or data loss, you can restore your site to a previous state.

6. Security Plugins / Extensions:

Depending on your CMS, install security plugins or extension's to enhance your website's security. These tools can help with tasks like malware scanning, firewall protection, and login security.

7 Secure Hosting:

Choose a reputable web hosting provider that prioritize security and offers features like SSL certificates, server-side security measures, and regular software update

8. Security Headers:

Implement security headers like content security policy (CSP), HTTP strict transport security (HSTS), and X-content-Type-option to mitigate various types of attacks, such as cross site scripting (xss) and click-jacking

9. File upload security:

If your website allows file update, ensure proper validation and sanitization of update file's to prevent malicious files from being executed on your server.

10. Regular Security Audits :
Conduct regular security audits and vulnerability scans of your website to identify and address any security weaknesses or potential threats.

11. User permission :
Limit user permission to only what is necessary for their roles Avoid giving unnecessary administrative privileges to prevent unauthorized access to sensitive areas of your websites.

12. Incident Response plan :
Develop an incident response plan outlining the steps to take in the event of a security breach. This sound include the procedures for containing the breach. of investigating the incident. and restoring the website's security.

Techniques for effective defence.

Effective defense against cyber threats requires a multi-layred approach that combines of technology, processess, and user awarness. Here are some techniques for effective defense.

1. Network segmentation:
Divide your network into smaller segment to limit the impact of a security breach. This prevents attrackers from easily moving laterally across your networks.

Intrusion detection and prevention systems (IDPS):

Deploy IDPS to monitor network traffic for suspiciously activity and automatically block or alert on potential threats.

Patch management:

Keep all software and system up to date with the latest security patches to address know vulnerabilities. implement a patch management process to regularly asses, prioritize, and apply patches.

Secure Development practices:

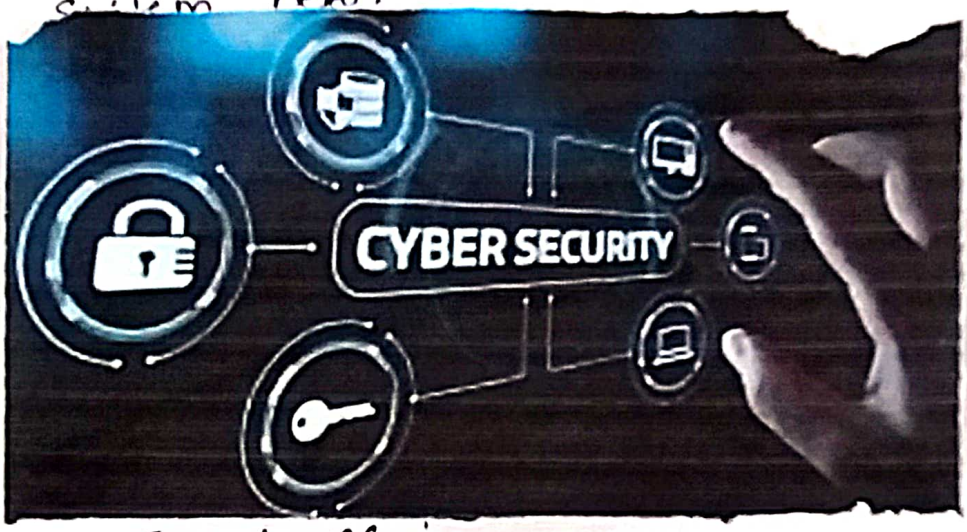
Incorporate security up to date of the software development lifecycle by following secure coding practices, conducting code review's, and performing security testing throughout the development process.

Access control:

Enforce strong access control to limit user privileges and restrict access to sensitive information based on the principle of least

privilege. Implement multi-factor authentication where possible.

Regular security Audits and penetration Testing: conduct periodic security audit and penetration tests to identify vulnerabilities and weakness in your system before attacks can exploit them.



Reactive Techniques:

1. Incident Response plane:

Develop and regularly update an incident Responce plan outling the step to take in the event of a security incident. Assign roles and responsibilities, establish communication protocols, and define procedure's for containing and mitigating the impact of an incident.

Incident Detection and Response :

Deploy tools and technologies for detection and responding to security incident, such as intrusion detection systems (IDS), security information and event managment.

Forensics and investigation :

Conduct forensic analysis to determine the root cause of a security incident, collect evidence and gather intelligence to prevent similar inident in the future.

post incident Remediation:

After resolving a security incident, conduct a through post-incident review to identify lesson learned, update security control and the procedures as necessary. and improve overall resilience against future attacks.

WEEKLY REPORT

WEEK – 1 (From Dt 5/2/24 to Dt 10/2/24)

Objective of the Activity Done: The courses aim to provide a comprehensive understanding.

Detailed Report:

The objective across the course mentioned revolves around equipping participants with essential skills and knowledge relvent to cyber security and related filies.

Cyber security Internship program: The Aim is providing a comprehensive understang of cybersecurity principle, including ethical hacking, SOC/SIEM setup and CTI, Preparing interns to contribute effectively to the cyber security landscape.

Cyber security will gain insights into security fundamentals, the CIA Triad. legal and ethical considerations in ethical hacking and the role of ethical hackers in organization.

ACTIVITY LOG FOR THE SECOND WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day – 1	Installing and configuring virtual box	overview about the project	
Day - 2	Active and passive footprinting techniques	Illustration of techniques.	
Day – 3	Packet Analyzers.	Topic / Titles of the project.	
Day – 4	Port Scanning techniques tools.	Exploring a network for active hosts.	
Day – 5	* Network enmeration * Operation System and application	Enumeration plays a crucial role.	
Day –6	Risk assessment and prioritization of Vulnerabilities	Vulnerability assessment.	

WEEKLY REPORT

WEEK – 2 (From Dt..12/4/24.. to Dt...17/4/24..)

Objective of the Activity Done: They will explore various networking tools.

Detailed Report:

Setting up virtualized environment with Virtual Box : participants will acquire comprehensive skills in setting up and managing the virtualized enviroments using virtual Box.

we have learn about install and configure virtual BOX software on their systems. create and configure virtual environments.

This module focuses on reconnaissance techniques to gather information about target networks.

ACTIVE and passive footprinting methods to collect data about network infrastructure and services. Techniques for gathering information from public sources such as search engines.

ACTIVITY LOG FOR THE THIRD WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day - 1	Techniques and tools for accessing systems. • covering tracks and main -taining access	participants will master techniques and tools for access -ing system	
Day - 2	Types of malwares and their impacts • malware delivery meth -ods and vectors	participants will de velop a thorough understanding	
Day - 3	Network Sniffing concepts and tools • packet analysis tech -niques	participants will del -ve into network Sniffing concepts	
Day - 4	Types of social Engineering attacks • Human behaviour and psychology in social Eng attacks	participants will become familiar will all social Engineering tracks	
Day - 5	Types of DOS attacks. and their impacts. • DOS attack tools and techniques	participants will explore various types of DOS	
Day - 6	Types of session hijacking attacks • Tools and techniques for session hijacking	participants will study different types of session	

WEEKLY REPORT

WEEK – 3 (From Dt...18/3/24 to Dt..24/3/24..)

Objective of the Activity Done: cyber Security topics including techniques

Detailed Report:

* Network Sniffing Concepts and Tools :- participants will Explore the fundamentals of network Sniffing, including packet analysis techniques and the protocols com-monly targeted by attackers. They will gain hands on Experience with tools.

* Types of Social Engineering work attacks: In this section, participants will learn about different types of social Engineering attacks, including phishing, pretexting, baiting and tail gating. They will study the physhlogical principles behind these atte-cks and understand how human behavio-ur can be exploited by attackers. The module will also cover mitigation str-ategies and best practices for recogni-zing and defending against Social En-gineering tactics that also called the Social Engineering attacks various types.

ACTIVITY LOG FOR THE FORTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day – 1	Web server protection	Created Github repository	
Day - 2	Web application protection	Created Github folders.	
Day – 3	Security risks	Created an access to teamates	
Day – 4	Symmetric and asymmetric.	Collaborated all teammated	
Day – 5	Types of CTI and their impact organization	Doubts Clarification in CTI.	
Day –6	Understanding the basics of SIEM and IBM. QRadar.	Folders of Basic IBM. QRadar.	

WEEKLY REPORT

WEEK – 4 (From Dt.25/3/24. to Dt.27/3/24.)

Objective of the Activity Done: Developing of long term internship project.

Detailed Report:

On the first day we are given a barief idea about the development process of the project. We had to login into the official Smart Interz. Size and get access to our projects. On second day we are explained a demo projects and we got on brief idea on how to develop the project based on the ttles which we choose.

On third day till the last day of the week we are explained various ttles of the projects and we had to choose any one of the ttle and develop the project for this internship based on the topic choosen by us.

ACTIVITY LOG FOR THE FIFTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day - 1	project Development	overview about the project	
Day - 2	project development	Illustration of demo project	
Day - 3	project development	Topic / Titles of project	
Day - 4	project development	Titles of the project	
Day - 5	project development	Titles of the project	
Day - 6	project development	titles of the project	

WEEKLY REPORT

WEEK - 5 (From Dt.28/3/24 to Dt..30/3/24..)

Objective of the Activity Done: To complete the project work

Detailed Report:

The whole 5th week was dedicated in Explaining how to use github and this included the following steps.

Step-1:- Creating a repository on Github

step:-2:- Creating a repository on Github

step:-3 :- Collaborating with teammates on Github

step:-4 :- creating folders related to the project work on Github

Step:5: Uploading Essential files releated to the project on the Github.

ACTIVITY LOG FOR THE SIXTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day - 1	project work	Signed into APSCHE smart intern site.	
Day - 2	project work	Understand the project milestone's.	
Day - 3	project work	Assigning tasks to team member	
Day - 4	project work	Evaluated the whole output.	
Day - 5	project work	Combining all gathering	
Day -6	project work.	Creating a project video.	

WEEKLY REPORT

WEEK – 6 (From Dt..30/3/24 to Dt..3/4/24..)

Objective of the Activity Done: To complete project work.

Detailed Report:

After we learned how to use Github, we were still left with some doubt regarding the projects, so the Smart Interns team offered us a whole week to get our doubts clarified. till a vast extent. some doubts. which have arised during our project development were as follows,

Should all teammates do the projects individually?

Should each teammate assignment be included in the leader's Github repository?

What files should the team leader give in his/her repository?

ACTIVITY LOG FOR THE SEVENTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day-1	Project Development	Overview about the project.	
Day-2	project development	Illustration of demo project	
Day-3	project development	Topic/Titles of the project	
Day-4	project development	Titles of the project	
Day-5	project development	Titles of the project	
Day-6	project development	Title's of the project.	

WEEKLY REPORT

WEEK-7 (From Dt 25/3/24 to Dt 30/3/24)

Objective of the Activity Done: Developing of long Term internship project.

Detailed Report

on the first day we are given a barief idea about the development process of the project. We had to login into the official smartinternz. Size and get access to our projects.

On second day we are explained a demo project and we got on brief idea on how to develop the project based on the titles which we choose.

On third day till the last day of the week we are explained various titles of the project and we had to choose any one of the title and develop the project for this internship based on the topic choosen by us.

ACTIVITY LOG FOR THE EIGHTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day-1	project work	Explanation of Github	
Day-2	project work	Explanation of Github	
Day-3	project work	Explanation of Github	
Day-4	project work	Explanation of Github	
Day-5	project work	Explanation of Github	
Day-6	project work	Explanation of Github	

WEEKLY REPORT

week-8 (From Dt. 25/3/24 to Dt. 30/3/24.)

Objective of the Activity Done: To complete the project works

Detailed Report:

The whole 8th week was dedicated in explaining how to use Github and this included the following step's.

Step-1: Creating a repository on Github.

Step-2: Creating a repository on Github.

Step 3: Collaborating with teammates on GitHub.

Step 4: Creating folder's related to the project work on GitHub.

Step 5: Uploding essential files related to the projeut on GitHUb.

ACTIVITY LOG FOR THE NINTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day-1	project work	Clarified doubts	
Day-2	project work	Clarified doubts	
Day-3	project work	Clarified doubts	
Day-4	project work	Clarified doubts	
Day-5	project work	Clarified doubts	
Day-6	project work.	Clarified doubts	

WEEKLY REPORT

WEEK-9(From Dt. 1/4/24 to Dt. 6/4/24)

Objective of the Activity Done: To complete the project work.

Detailed Report:

After we learned how to use Github, we user still left with some doubt's regarding the project, so the smart-Intern. team offered us a whole week to get our double clarified till a best extent.

Some doubts which have arised during our project development were as follows,

* Should all treatments do the project individually?

* Should each teammate assignment be include in the leader's Github repository?

* Is there any reference for completing the project?

ACTIVITY LOG FOR THE TENTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day-1	Project work	Created GitHub repository	
Day-2	project work	Created GitHub folders	
Day-3	project work	Created an access to teamates	
Day-4	project work	Collaborated all teammated	
Day-5	project work	Doubts clarification	
Day-6	project work	Doubts clarification	

WEEKLY REPORT

WEEK-10(From Dt. 8/4/24 to Dt. 13/4/24)

Objective of the Activity Done: To complete the projet work.

Detailed Report:

During this week we decided to start our project work:
For that first we as a team created accounts personally on GitHub.
Then we created a folder in name of assignments and uploaded all the assigments given during our term in long term internship.
After that all the team members were made to be collaborated to the leader's Repository and were given push access to the team leaders. respository so that they could upload their assign-ments individually into the folder created by the tearm leader in name of "Assignments".
last two days we clarified few other douth which we were unable to configure.

ACTIVITY LOG FOR THE ELEVENTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day-1	Project work	Understanding the title.	
Day-2	Project work	Gathering required materials.	
Day-3	Project work	Updating the software.	
Day-4	Project work	Installation of required application.	
Day-5	Project work	Doubts classification	
Day-6	Project work	Doubts clarification	

WEEKLY REPORT

week-11 (From Dt. 13/4/24 to Dt. 20/4/24)

Objective of the Activity Done: To Complete the project work

Detailed Report

During this week we started our project. The title which we took is "Understanding Cyber Threats : Exploring Nessus and Beyond scanning Tools.

On the first day we understand our project title. our project was based on exploring Nessus tools for vulnerability scanning and also exploring various other tools. rather than Nessus.

one second day we gather all the materials required for the project, these include laptop's. wifi connection's reference books etc..

On third day we updated our system so that we don't log in the project development phase.

On fourth day we installed the applications and other software for our project these include Nessus application's.

ACTIVITY LOG FOR THE TWELTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day-1	project work	Signed into APSCHE smart-interns site	
Day-2	project work	Understand the project milestones	
Day-3	project work	Assigning tasks to team members	
Day-4	project work	Evaluated the whole output.	
Day-5	project work	combining all gathering.	
Day-6	project work	Creating a project video	

WEEKLY REPORT

week-12 (From Dt 22/4/24 to Dt 27/4/24..)

Objective of the Activity Done: To complete the project work.

Detailed Report

On the first day we logged into the APSCHE SmartInternz website using our credentials and then went into the project workspace to get acess for our project.

Then next day we understand the to complete our project and the other day each team members was assigned specific milestone to reach by to complete the whole project.

After that on fourth day, all the work done individually by the teamm -ates was revieused to complete the project and few errors were rectified on this day. One day five we combined all the final output and have complete our project successfully. We done demostration viedo regarding our project. and submit to GitHub repository of the team Project.

Conclusion :

The conclusion of cyber security is that it's ongoing battle against evolving threats, required a multi-layered approach involving technology, processes, and people to safeguard data and systems effectively.

Cyber security is indispensible in today's interconnected world. It's not merely a technical challenge but also a societal one, impacting individuals, businesses, and government alike. As technolgy advances, so do cyber threats, making it imperative to continuosly adapt strategies, invest in robust defenses and foster a culture of security awarness. Collaboration between stakeholders, including governments industrie's, and the public is crucial to effectively mitigate cyber risk and ensure a safer digital future for all.