

**WEEKLY REPORT OF INTERNSHIP**

|  |  |  |  |
| --- | --- | --- | --- |
| **Subject Name** | **Internship** | **Subject Code** | **21CSI85** |
| **Phone Number** | **7204934603** | **Semester** | **8** |
| **USN** | **1GA21CS106** | **Section** | **C** |
| **Domain** | **Cyber Security** | | |
| **Internship Title** | **Cyber Security & Digital Forensics Intern** | | |
| **Internship Company Name** | **Cyber Secured India** | | |
| **External Guide name** | **Nikhil S Mahadeshwar** | | |
| **PO’s Mapping** |  | | |

|  |
| --- |
| **WEEK-1** |

|  |  |  |
| --- | --- | --- |
| **Date Range** | **01/09/2024 to 07/09/2024** | |
| **Work Assigned** | Begin foundational cybersecurity training by completing Linux and Windows fundamentals modules on TryHackMe and Hack The Box Academy platforms. | |
| **Weekly Progress** | * Completed *Linux Fundamentals Part 1* on TryHackMe * Completed *Windows Fundamentals 2* on TryHackMe * Completed *Windows Fundamentals 3* on TryHackMe * Started *Linux Fundamentals* course on Hack The Box Academy * Started *Windows Fundamentals* course on Hack The Box Academy | |
| **Mentor’s Comment** |  | |
| **Student Signature and Date** | **Internal Guide Signature and Date** | **External Guide Signature and Date** |
|  |  |  |

|  |
| --- |
| **WEEK-2** |

|  |  |  |
| --- | --- | --- |
| **Date Range** | **08/09/2024 to 14/09/2024** | |
| **Work Assigned** | Complete introductory networking modules on TryHackMe and Hack The Box Academy to build a strong foundation in networking concepts essential for cybersecurity. | |
| **Weekly Progress** | * Completed *Introductory Networking* room on TryHackMe * Completed *What is Networking?* room on TryHackMe * Chose appropriate typography and color schemes * Completed *Introduction to Networking* course on Hack The Box Academy | |
| **Mentor’s Comment** |  | |
| **Student Signature and Date** | **Internal Guide Signature and Date** | **External Guide Signature and Date** |
|  |  |  |

|  |
| --- |
| **WEEK-3** |

|  |  |  |
| --- | --- | --- |
| **Date Range** | **15/09/2024 to 21/09/2024** | |
| **Work Assigned** | Complete the *Passive Reconnaissance* module on TryHackMe to understand the basics of information gathering without direct interaction with target systems. | |
| **Weekly Progress** | * Completed *Passive Reconnaissance* room on TryHackMe * Practiced techniques like WHOIS lookup, DNS enumeration, and Google Dorking * Understood the importance of open-source intelligence (OSINT) in ethical hacking | |
| **Mentor’s Comment** |  | |
| **Student Signature and Date** | **Internal Guide Signature and Date** | **External Guide Signature and Date** |
|  |  |  |

|  |
| --- |
| **WEEK-4** |

|  |  |  |
| --- | --- | --- |
| **Date Range** | **22/09/2024 to 28/09/2024** | |
| **Work Assigned** | Completed *BurpSuite Basics* room on TryHackMe (Premium room skipped due to access limitations) | |
| **Weekly Progress** | * Completed *BurpSuite Basics* room on TryHackMe (Premium room skipped due to access limitations) * Completed *Burp Suite: Repeater* room on TryHackMe * Completed *HTTP request smuggling: basic TE.CL vulnerability* lab on PortSwigger * Practiced intercepting, modifying, and repeating HTTP requests for testing vulnerabilities | |
| **Mentor’s Comment** |  | |
| **Student Signature and Date** | **Internal Guide Signature and Date** | **External Guide Signature and Date** |
|  |  |  |

|  |
| --- |
| **WEEK-5** |

|  |  |  |
| --- | --- | --- |
| **Date Range** | **29/09/2024 to 05/10/2024** | |
| **Work Assigned** | Work on web authentication vulnerability labs on PortSwigger covering username enumeration, 2FA bypass, and password reset logic flaws. | |
| **Weekly Progress** | * Completed *Username enumeration via different responses* lab on PortSwigger * Completed *2FA simple bypass* lab on PortSwigger * Completed *Password reset broken logic* lab on PortSwigger * Completed *Username enumeration via subtly different responses* lab on PortSwigger * Completed *Username enumeration via response timing* lab on PortSwigger * Understood different authentication attack vectors and exploitation techniques | |
| **Mentor’s Comment** |  | |
| **Student Signature and Date** | **Internal Guide Signature and Date** | **External Guide Signature and Date** |
|  |  |  |

|  |
| --- |
| **WEEK-6** |

|  |  |  |
| --- | --- | --- |
| **Date Range** | **06/10/2024 to 12/10/2024** | |
| **Work Assigned** | Work on access control vulnerability labs on PortSwigger covering unprotected admin functionalities, role-based access control flaws, and user ID parameter manipulation. | |
| **Weekly Progress** | * Completed *Unprotected admin functionality* lab on PortSwigger * Completed *Unprotected admin functionality with unpredictable URL* lab on PortSwigger * Completed *User role controlled by request parameter* lab on PortSwigger * Completed User role can be modified in user profile lab on PortSwigger * Completed *User ID controlled by request parameter* lab on PortSwigger * Gained understanding of insecure direct object references (IDOR) and access control bypasses | |
| **Mentor’s Comment** |  | |
| **Student Signature and Date** | **Internal Guide Signature and Date** | **External Guide Signature and Date** |
|  |  |  |

|  |
| --- |
| **WEEK-7** |

|  |  |  |
| --- | --- | --- |
| **Date Range** | **13/10/2024 to 19/10/2024** | |
| **Work Assigned** | Work on vulnerability exploitation labs covering OS Command Injection, SQL Injection, and XML External Entity (XXE) attacks via PortSwigger. | |
| **Weekly Progress** | * Completed *OS command injection (simple case)* lab on PortSwigger * Completed *SQL Injection* * Completed *XXE Exploitation* * Exploiting XXE using external entities to retrieve files * Vulnerability in WHERE clause allowing retrieval of hidden data * Vulnerability allowing login bypass | |
| **Mentor’s Comment** |  | |
| **Student Signature and Date** | **Internal Guide Signature and Date** | **External Guide Signature and Date** |
|  |  |  |

|  |
| --- |
| **WEEK-8** |

|  |  |  |
| --- | --- | --- |
| **Date Range** | **20/10/2024 to 26/10/2024** | |
| **Work Assigned** | Complete a CSRF (Cross-Site Request Forgery) vulnerability lab on PortSwigger to understand how unauthorized actions can be triggered on behalf of authenticated users. | |
| **Weekly Progress** | * Completed *CSRF vulnerability with no defenses* lab on PortSwigger * Learned how CSRF exploits trust in authenticated sessions to perform unintended actions * Practiced crafting malicious CSRF exploit pages | |
| **Mentor’s Comment** |  | |
| **Student Signature and Date** | **Internal Guide Signature and Date** | **External Guide Signature and Date** |
|  |  |  |

|  |
| --- |
| **WEEK-9** |

|  |  |  |
| --- | --- | --- |
| **Date Range** | **27/10/2024 to 02/11/2024** | |
| **Work Assigned** | Practice network scanning and host discovery techniques using Nmap through dedicated TryHackMe rooms. | |
| **Weekly Progress** | * Completed *Nmap* room on TryHackMe * Completed *Nmap Live Host Discovery* room on TryHackMe * Learned advanced Nmap scanning techniques and host discovery methods * Practiced identifying open ports, services, and detecting live hosts within a network | |
| **Mentor’s Comment** |  | |
| **Student Signature and Date** | **Internal Guide Signature and Date** | **External Guide Signature and Date** |
|  |  |  |

|  |
| --- |
| **WEEK-10** |

|  |  |  |
| --- | --- | --- |
| **Date Range** | **03/11/2024 to 09/11/2024** | |
| **Work Assigned** | Get introduced to the Metasploit Framework using the TryHackMe room, covering basics of exploitation and framework navigation. | |
| **Weekly Progress** | * Completed *Metasploit: Introduction* room on TryHackMe * Learned about Metasploit modules, exploit selection, payload configuration, and executing exploits * Practiced using auxiliary and exploit modules for vulnerability assessment | |
| **Mentor’s Comment** |  | |
| **Student Signature and Date** | **Internal Guide Signature and Date** | **External Guide Signature and Date** |
|  |  |  |

|  |
| --- |
| **WEEK-11** |

|  |  |  |
| --- | --- | --- |
| **Date Range** | **10/11/2024 to 16/11/2024** | |
| **Work Assigned** | Work on Linux privilege escalation techniques using dedicated TryHackMe rooms to understand common privilege escalation vectors and misconfigurations. | |
| **Weekly Progress** | * Completed *Linux PrivEsc* room on TryHackMe * Completed *Linux Privilege Escalation* room on TryHackMe * Learned enumeration techniques, kernel exploits, file permissions abuse, and PATH manipulation for privilege escalation * Practiced escalating privileges from a standard user to root in controlled environments | |
| **Mentor’s Comment** |  | |
| **Student Signature and Date** | **Internal Guide Signature and Date** | **External Guide Signature and Date** |
|  |  |  |

|  |
| --- |
| **WEEK-12** |

|  |  |  |
| --- | --- | --- |
| **Date Range** | **17/11/2024 to 23/11/2024** | |
| **Work Assigned** | Practice Windows privilege escalation techniques using dedicated TryHackMe rooms, focusing on enumeration and exploiting common Windows misconfigurations. | |
| **Weekly Progress** | * Completed *Windows PrivEsc Arena* room on TryHackMe * Completed *Windows PrivEsc* room on TryHackMe * Learned about enumeration tools like winPEAS, privilege escalation through services, registry abuses, unquoted service paths, and token impersonation * Practiced escalating privileges from standard user to Administrator in Windows environments | |
| **Mentor’s Comment** |  | |
| **Student Signature and Date** | **Internal Guide Signature and Date** | **External Guide Signature and Date** |
|  |  |  |

|  |
| --- |
| **WEEK-13** |

|  |  |  |
| --- | --- | --- |
| **Date Range** | **24/11/2024 to 30/11/2024** | |
| **Work Assigned** | Complete introductory training on Digital Forensics fundamentals via TryHackMe. | |
| **Weekly Progress** | * Completed *Intro to Digital Forensics* room on TryHackMe * Understood the basics of forensic imaging, volatile and non-volatile data acquisition, chain of custody, hashing, and investigation tools * Practiced analyzing disk images and memory dumps | |
| **Mentor’s Comment** |  | |
| **Student Signature and Date** | **Internal Guide Signature and Date** | **External Guide Signature and Date** |
|  |  |  |