**PROJECT SELECTION FORM**

**Capacity Building Program (CBP) - CHUK - September 2024**

1. **Names of the Member**

|  |  |  |  |
| --- | --- | --- | --- |
| Sl No. | Name | Roll No. | Signature |
| 1. | Sudhan S | 202409332200652 | Sudhan S |
| 2. | Gowsicka R | 202409332200494 | Gowsicka R |
| 3. | Thiruvarulnathan K | 202409332200847 | Thiruvarulnathan K |
|  |  |  |  |
|  |  |  |  |

2. **Title of the Project**

|  |
| --- |
| Ransomware Attack Stimulation & Analysis |

3. **Brief Description of the Project**

|  |
| --- |
| This project aims to simulate ransomware attacks in a controlled environment to study their behavior, impact, and propagation methods. By analyzing different attack vectors and encryption techniques, we will assess the effectiveness of current defense mechanisms and incident response strategies. The findings will help identify vulnerabilities, improve detection and prevention systems, and guide organizations in mitigating ransomware risks. Ultimately, the project will provide actionable recommendations for enhancing cybersecurity measures. |

**4. Hardware Requirements of the Project**

|  |
| --- |
| **Development Environment Requirements:**  **Recommended Hardware:**   * + CPU: Quad-core processor or higher   + RAM: 16 GB or higher   + Storage: 100 GB SSD   + Network: Stable internet connection for testing tools |

**5. Software Requirements of the Project**

|  |  |
| --- | --- |
| **Category** | **Software/Tools** |
| **Operating System** | Ubuntu 22.04, Kali Linux (for pentesting tools), Windows 10/11 (for ransomware simulations) |
| **Virtualization** | VirtualBox, VMware Workstation, Docker (for containerized environments), KVM |
| **Ransomware Simulation** | Metasploit Framework, Social-Engineer Toolkit (SET), Veil Framework, Empire |
| **Static Analysis** | Radare2, Ghidra, YARA, PEiD, Binwalk |
| **Dynamic Analysis** | Cuckoo Sandbox, Process Monitor, Sandboxie |
| **Network Analysis** | Wireshark, Zeek (formerly Bro), Netcat, tcpdump |
| **Memory Analysis** | Volatility Framework, Rekall |
| **Defense Mechanisms** | ClamAV, OSSEC, iptables, CrowdStrike Falcon, Microsoft Defender ATP |
| **Data Recovery** | FTK Imager, TestDisk, Autopsy |
| **CTF Tools** | CTFd, CyberChef, Python/Bash scripting, OBS Studio |
| **Mitigation Tools** | Restic, Duplicity, Timeshift, Hashcat |
| **Threat Intelligence** | MISP (Malware Information Sharing Platform), OpenCTI, ThreatCrowd |
| **Log Analysis** | Splunk, Graylog, ELK Stack (Elasticsearch, Logstash, Kibana) |
| **Encryption Tools** | OpenSSL, Crypto++ Library |

|  |  |
| --- | --- |
| **Approved By (Guides Name & Signature)** | **Date of Submission** |
|  |  |