**Vaibhava Lakshmi**

| (475) 444 3375  | Chittapragadav@mail.sacredheart.edu |  [Vaibhava Lakshmi Chittapragada | LinkedIn](https://www.linkedin.com/in/vaibhava-lakshmi-chittapragada-694589178/) |
| --- | --- | --- |
|  |  |
| **Master of Science – Cyber Forensics and Counterterrorism** |  **Graduation: Dec 2022** |
| Sacred Heart University – Fairfield, Connecticut. |  **GPA 3.66/4** |
| **Bachelor of Technology – Electronics and Communication Engineering** |  **August 2017 – July 2021** |
| Jawaharlal Nehru Technical University – Hyderabad, India. |  |

SKILLS



| * CISCO Networking
 | * Burp Suite
 | * Network Security
 |
| --- | --- | --- |
| * Metasploit
 | * AWS, EC2, S3
 | * FTK Imager
 |
| * Kali Linux
 | * Wireshark
 | * Python, C++,
 |
| * Cellebrite, Forensic Analysis
 | * SQL
 | * OS: iOS, Linux, Windows
 |

PROFESSIONAL EXPERIENCE



**CTL Tutor February 2022 – December 2022 Sacred Heart University, Connecticut.**

* Used Python SDK and Java utilizing Maven and Spring Boot to implement AWS technologies including lambda, S3, and AWS machine learning.
* To gain insights, I applied CNN and ML algorithms to the large datasets.
* Handled all phases of responding to cyber forensic incidents, including data gathering, identification, containment, and analysis.
* To address the needs of cyber security, I performed penetration testing, security configuration checks, and system configuration scans.
* To efficiently find and safeguard firm assets, I performed network traffic analysis, host behavior analysis, PC forensics, windows event analysis, etc.
* To manipulate data, a Python module called Pandas was used.
* Manipulated files and updated database content using Python scripts.

TECHNICAL EXPERIENCE



**Reconnaissance from WAN:**

* Scanned for the open ports and using telnet scanned all the obtained open ports which resulted in unique banner messages.
* Nmap helped to perform banner grabbing and to get information about the OS and the applications running behind the firewall. Using the id command obtained the UID of the root.
* The hash values of the administrators are gathered using tail command.
* By performing John, the Ripper, login credentials of the target system are captured.
* Connected to the target machine using port 3389 with the help of remote desktop protocol.

**I Agree..! The risk behind one click:**

* Developed a machine learning cyber awareness project for the end user to read and understand the long, legal, and technical in nature in its verbiage in short.
* The machine learning model “pegasusforconditiongeneration ” from transformers, was trained with varies datasets of terms and conditions using Textgenrnn library.
* When the terms and conditions were given as input to the code, the output listed all the privacy related 40 – 50 statements.
* By using sentence-splitters and sentencePiece libraries the final output was a translated 7-8 statements.

| **Enumerate the target:** |
| --- |

* Using Wireshark, it detected all the hosts in the packets.
* Scanned for the host in Metasploit.
* Connected to the host using Armitage.

**Dictionary Attack:**

* Using NMAP, I have scanned for the open ports of the target machine’s IP.
* Opened Bruter.exe application of the target machine.
* Made minor changes like setting the IP of the target and its open port.
* Changed the username to admin and in the dictionary column “**wordlist.txt**” file is attached for password modes.
* Launched attack and the password is revealed.

ACTIVITIES



* Winner of CPP (Col Poly Pomona) – Cyber Security and Awareness Fair 2022 in awareness category for the project “**I AGREE–the risk behind one click.**”

CERTIFICATIONS



* CCO - Cellebrite Certified Operator
* Udemy – Ethical Hacking, Debugging and Malware Analysis.
* Cisco – Introduction of Networks- Routers and Switches.