Department of CSE - Cyber Security

PRACTICAL HANDS-ON

BOOTCAMP ON CYBER SECURITY - 2023

REPORT

Title of the Program: Practical Hands-On Bootcamp on Cyber Security and Hackathon

Venue: FSD Lab (11102B)

Dates: 22nd - 27th June 2023

Industry Resource Persons: Mr. Rahul and team, Supraja Technologies, Vijayawada

Number of Participants: 89 Students

Faculty and Staff Participated: 12

Outcomes:

  i.   **Hands on working knowledge on the Security tools,**

  ii. **6 Hackathon winners**

  iii. **44 students grabbed the internship offer**

<div align="center">***</div>

1. About Program

The '**PRACTICAL HANDS-ON BOOTCAMP ON CYBER SECURITY' followed a hackathon** workshop was organized with the aim of raising awareness about cybersecurity best practices, providing practical knowledge about common threats and vulnerabilities, upskilling the students with latest tools and promoting a culture of cybersecurity among participants. The workshop was organized by **Department of CSE-Cyber Security, Sreenidhi Institute of Science and Technology, Hyderabad** in collaboration with **Supraja Technologies, Vijayawada**, during 22nd - 27th June 2023 and was attended by 89 students from various backgrounds.

Agenda:

The workshop covered a wide range of topics related to cybersecurity. The agenda included:

1. Introduction to Cyber Security
2. Basics of Networking
3. Sniffing
4. Virtualization
5. Steganography and Cryptography
6. Login Bypass
7. Basic Attacks and Security
8. Malwares
9. Google Hacks
10. Wireless Attacks

11. Web Application Attacks
12. Cyberlaws and Security

To ensure an interactive learning experience, the workshop incorporated various activities and practical demonstrations using different tools.

2. Session-wise Details

- **Session – 1 (22nd June 2023)**
  - ➢ On the first day of the workshop, resource persons gave a brief introduction about cyber security and its uses.
  - ➢ Various cybercrimes and cyberlaws have been discussed in order to create awareness about ethical and unethical issues.
  - ➢ Various types of cybercrimes like hacking, malware attacks, online scams, etc., were discussed.
  - ➢ Laws related to cybercrimes and their punishments were explained as they are essential to consult the specific laws and regulations of the jurisdiction to understand the legal framework surrounding cybercrimes in your area.
  - ➢ One good idea was mentioned about getting awarded for finding and reporting bugs in the websites to the concerned organizations.
  - ➢ Brief explanation of various hackers like Black Hat Hackers, White Hat Hackers, Red Hat Hackers, Grey Hat Hackers, Script Kiddies, Hacktivists, etc., has been given.
  - ➢ OSI and TCP/IP models were revised with some examples.
  - ➢ Coming to the basics of networking, most commonly used ports have been explained in detail and also provided with a link https://networkverge.com/common-ports/ to get a basic idea of those ports.
  - ➢ To know how the network is established between various countries, the details of an Interactive map (Submarine Cable Map) of the world's major submarine cable systems and landing stations https://www.submarinecablemap.com/ website were mentioned. Network connections are established undersea marine cables which are an assembly of conductors enclosed by an insulating sheath and laid on the ocean floor for the transmission of messages.
  - ➢ An information related to bulk messages from temporary numbers, fake profile pictures and fake social media profile creations has been provided with sample websites (https://receive-smss.com/) (https://this-person-does-not-exist.com/en) mentioned.
  - ➢ Certain websites were mentioned to be aware of that are built by Government of India to report various cybercrimes (https://cybercrime.gov.in/) and also to track lost mobile phones (https://ceir.gov.in/Home/index.jsp).
- **Session-2 (23rd June 2023)**
  - ➢ On Day-2, introduction to a popular tool named 'Wire Shark' has been given.
  - ➢ A brief explanation about Sniffing was given which refers to the process of capturing and analyzing network traffic to intercept and examine data packets as

they travel across a network. It is commonly done using specialized tools called network sniffers or packet sniffers.

- ➢ Wireshark is a popular open-source network protocol analyzer and packet capture tool. It allows users to capture and analyze network traffic in real-time, helping to diagnose and troubleshoot network issues, investigate security incidents, and understand network behavior.
- ➢ Key features like packet capture, protocol analysis, live packet filtering, packet display and inspection, protocol filtering and decoding, statistical analysis, third-party extensions, etc., were explained by providing practical sessions.
- ➢ Students were given various challenges to solve with, like getting authentication details in a particular network, changing the usernames and passwords, decoding the hidden text, finding the hidden documents, images, etc., which provided a great exposure to Wire Shark tool.

- **Session-3 (24th June 2023)**
  - ➢ On Day-3, students were exposed to another powerful tool 'Quick Stego' which is a software tool that allows users to hide information (such as text, images, or files) within digital images using a technique called steganography.
  - ➢ Steganography is the practice of hiding information or data within other types of data, such as images, audio files, text, or video, in a way that conceals the presence of the hidden information. Unlike encryption, which focuses on making the content unintelligible, steganography aims to make the existence of the hidden data undetectable.
  - ➢ Various techniques like Image Steganography, Text Steganography, Audio Steganography were discussed in detail.
  - ➢ Interesting challenges related to steganography and cryptography were given to students to make them involve to the fullest.

- **Session-4 (25th June 2023)**
  - ➢ On Day-4, students were given with some special challenges related to Wire Shark and Quick Stego.
  - ➢ They are also given with some assignments related cyberlaws and cybercrimes.

- **Session-5 (26th June 2023)**
  - ➢ On Day-5, another popular cybersecurity testing tool 'Burp Suite' which is used for web application security and penetration testing was explained.
  - ➢ Key features of Burp Suite like Web Application Scanning, Intercepting Proxy, Web Application Spider, Vulnerability Scanner, Intruder, Repeater, Sequencer, Extensibility were discussed.
  - ➢ Practical session has been conducted on Burp Suite where it has ended up testing the vulnerabilities on ecommerce websites. Various vulnerabilities like changing of price, changing the quantity of items, etc., were discussed.
  - ➢ OTP (One-Time Password) bypass is a serious security concern and is generally considered unethical and illegal. OTP is designed to provide an additional layer of security by generating a unique password that is valid for a single login session or transaction. Bypassing OTP without proper authorization is a violation of privacy

and security, and it can lead to unauthorized access to sensitive information or systems.

➢ Challenges were solved related to Login and OTP bypassing using Brute Force attack listed in the Burp Suite.

- **Session-6 (27th June 2023)- Hackathon**
  - ➢ On the last day of the workshop, a Hackathon was conducted which was very interesting and students had a tough competition among themselves.
  - ➢ 44 teams with 2 members in each team participated in this Hackathon.
  - ➢ Finally, 3 teams were selected as first, second and third prize winners and certificates were presented to them.
  - ➢ The team Supraja Technologies also selected 46 students for internship and provided the offer letters to them on the same day.
  - ➢ Certificate of Participation were issued to all the students who attended the workshop.
  - ➢ All the details of students who won Hackathon and who were offered with internships are listed in this report.

3. List of Resource Persons from Supraja Technologies

S. No	Name of the resource persons	Designation and Affiliation
1.	Mr. Rahul	Senior Security Analyst, Chief Trainer at Supraja Technologies
2.	Mr. Krishna	Security Analyst, Red Teamer at Supraja Technologies
3.	Mr. Vishnu	Junior Security Analyst, Mentor at Supraja Technologies
4.	Mr. Surya	Junior Security Analyst, Mentor at Supraja Technologies

4. List of Tools with Hands-on sessions:

1. WireShark
2. Quick Stego
3. Burp Suite
4. Other popular tools used in Cyber Security Domain:
   i. Malware Bytes,
   ii. Emkei,
   iii. haveibeenpwned,
   iv. Google Dashboard,
   v. How secure is my Password?,
   vi. temp-mail,

Department of CSE - Cyber Security

vii.   temporary mobile number,
viii.   tafcop- Sancharsath

5. List of Hackathon Winners

Winners	Team Name	Team Members	Roll No.
1st	Leo-Aquarius	Rishitha Ranabothu (Cyber Security)	21311A6215
		Manoj Kumar Gurram (Cyber Security)	21311A6240
2nd	West Taiwan	N. N. A. G. Sadasiva Murthy (Cyber Security)	21311A6201
		M. V. S. Ashish (AI & ML)	21311A6602
3rd	Testcase69	Milkuri Abhiram Reddy (Cyber Security)	21311A6206
		N. Shashank (Cyber Security)	21311A6219

6. List of Students Selected for Internship @ Supraja Technologies-44
(29-CSE-CS, 8-CSE_AIML, 3-CSE, 3-IT, 1- Sathya Sai, B'lore)

S.No	Name	Branch
1	NNAG Sadasiva Murthy	Cyber Security
2	Manoj Kumar Gurram	Cyber Security
3	Rishitha Ranabothu	Cyber Security
4	Milkuri Abhiram Reddy	Cyber Security
5	N Shashank	Cyber Security
6	Ananya Rao	Cyber Security
7	Nyamathabad Koushik Sai	Cyber Security
8	Charan Karthik Ketha	Cyber Security
9	Jeshwa Erla	Cyber Security
10	Ankit Cheripally	Cyber Security
11	Tejaswini Shagonda	Cyber Security
12	Vishnu Priya Vuppu	Cyber Security
13	Palle Shashank	Cyber Security
14	Nishath	Cyber Security
15	Nalla Sai Preetham	Cyber Security
16	Vangala Malavika	Cyber Security
17	Buddha Anjali	Cyber Security
18	S Hansika	Cyber Security
19	Ravindranath Porandla	Cyber Security
20	Sahasritha Mallela	Cyber Security
21	Reethika Gajulapati	Cyber Security
22	Nandini Guduru	Cyber Security
23	Shaik Atif Rehan	Cyber Security
24	Gottiparthi Abhinav	Cyber Security
25	Madhavi Yedapally	Cyber Security
26	S Suprith Vardhan Rao	Cyber Security

Department of CSE - Cyber Security

27	Syed Sofiyan	Cyber Security
28	S Santhosh Kumar	Cyber Security
29	Srikanth Reddy Vemireddy	Cyber Security
30	Malla Venkata Sai Ashish	AI & ML
31	G Vishnu Vardhan	AI & ML
32	Mohammad Moiz Pasha	AI & ML
33	Prem Kiran Laknaboina	AI & ML
34	Naalla Venkateshwarlu	AI & ML
35	Neelothpal Samala	AI & ML
36	Srivani Konda	AI & ML
37	Ujwala Katragadda	AI & ML
38	Tunuguntla Kedari Sreeya	CSE
39	Ettadi Shriya Reddy	CSE
40	T Shivani	CSE
41	Medavarapu Swethan Rao	IT
42	Nagothu Vamshi	IT
43	Aamir Mohammad Maaz	IT
44	C Ramdev Prasad	Bangalore

Convenor: Prof. K. Shirisha, HoD, CSE-CS

Coordinators: Mrs. V. Geeta,
        Mr. K. Gnaneshwar

Student Coordinators: Manoj Kumar Gurram,
        Vishnu Priya Vuppu
        Gottiparthi Abhinav

Prof. K. Shirisha
HoD, CSE-CS, SNIST

Encl:
1. Participants' List- Internal and External
2. Bootcamp Poster
3. Permissions and Approvals
4. Attendance Lists- Daywise
5. Sample Photographs of the event- Inaugural, sessions and Valedictory
6. Certificates – Participation, Organization, Hackathon Winners, Internships (samples)
7. Soft-copy of all the certificates.