

## **KKR&KSR Institute of Technology and Sciences Vinjanampadu, Guntur, Andhra Pradesh-522017**

Approved by AICTE, New Delhi and Permanent Affiliation from JNTUK, Kakinada  
Accredited with "A" Grade by NAAC & NBA Accreditation Status for 4 UG (CSE, ECE, EEE, ME) Programs

**Organized A 10 Days workshop on Ethical Hacking and Cyber Security by Mr  
Bharat, CEO, LYFAUX, Bengaluru for III B Tech CSD from 17/08/2022 To  
27/08/2022.**

### **About the Webinar:**

Vulnerability assessment is the process of identifying, analyzing, and evaluating the vulnerabilities that exist in a system or network. The purpose of vulnerability assessment is to identify weaknesses in the system or network that could be exploited by attackers.

Vulnerability assessments typically involve using tools and techniques to identify vulnerabilities in a system or network. These tools may include vulnerability scanners, penetration testing tools, and network mapping tools.

Once vulnerabilities have been identified, they are typically prioritized based on their severity and the potential impact they could have on the system or network. This helps organizations to focus their resources on addressing the most critical vulnerabilities first.

### **About the Chief Guest:**

#### **Mr Kotha Surya – Xlenz Inc Usa, CEO**

Shri Surya Kotha has over 25 years of IT industry experience in the area of Product Building, Process automation, Enterprise Solutions, Law Enforcement & Cyber Security. Surya has been a digital transformation advisor to many C-level executives of Fortune 500 companies. His multi-billion dollar customer list includes Intel, Apple, ADP, Bosch, Cirrus Logic, Coke, Office Depot, US Government, GSA, Swiss Bank, and PGE to name a few. Surya also served as a mentor and advisory board member to various IT start-up companies in US and India. Furthermore, In addition to mentoring start-ups and evaluating technology businesses. He is also involved in various businesses like Broadcasting, Education, Retail etc. He is actively involved in a few charitable organizations to improve education and self-empowerment.

He currently works as CEO of Xlenz, a futuristic Augmented Reality Platform and 2 other AI Based start-ups. As recently as 2 weeks ago Surya has been invited as key note speaker at 1st National Emerging Technologies conference by Indian Ministry of Home affairs along with global tech giants like Meta, Google.

## 1. Objectives of the Event:

- Identifying vulnerabilities in systems, networks, and applications.
- Prioritizing vulnerabilities based on their severity and potential impact on the organization.
- Providing recommendations for remediation or mitigation of vulnerabilities.
- Identifying gaps in security controls and policies.
- Improving overall security posture by identifying weaknesses and taking corrective actions.
- Meeting compliance requirements by demonstrating due diligence in assessing and managing vulnerabilities.
- Providing a baseline for future assessments and monitoring progress in reducing vulnerabilities over time.

## 2. Venue of the Event:

The event is organized in a new seminar hall and conducted by KKR & KSR Institute of Technology and Sciences, Vinjanampadu, Guntur, Andhra Pradesh in association with SPARK.

3. **Date & Time of the Event:** The Event is organized on **27<sup>th</sup> Aug 2022**

4. **No. of students participated:** 210

5. **No. of faculties participated:** 7

6. **Event photographs.**



The poster features a central orange background with white and red text. At the top left is the KITS Autonomous logo, and at the top center is the LYFAUX logo. The main title reads 'A Ten Day Workshop on Ethical Hacking & Cyber Security (17th - 27th August 2022)'. Below this, it states 'In Association with Lyfaux, Bangalore'. The organizing department is 'Department Of CSE - DATA SCIENCE'. The KITS logo is prominently displayed in the center, with the full name 'KKR & KSR INSTITUTE OF TECHNOLOGY AND SCIENCES' and 'An Autonomous Institution' below it. At the bottom, there is a line of small text: '(Approved by AICTE, Affiliated to JNTUK, Kakinda) Accredited by NAAC with "A" grade; Accredited by NBA; VINJANAMPADU, GUNTUR, ANDHRA PRADESH - 522017.' The poster is decorated with several images: a 'WHITE HAT HACKER' in a dark suit, a person at a computer workstation, a hand holding a glowing padlock, a 'CYBER SECURITY' shield, and a close-up of a human eye.

**KITS**  
AUTONOMOUS

**LYFAUX**

**A Ten Day Workshop  
on  
Ethical Hacking & Cyber Security**  
(17th - 27th August 2022)

In Association with  
Lyfaux, Bangalore

Organized by :  
Department Of CSE - DATA SCIENCE

**KITS**  
KKR & KSR INSTITUTE OF TECHNOLOGY AND SCIENCES  
An Autonomous Institution

(Approved by AICTE, Affiliated to JNTUK, Kakinda)  
Accredited by NAAC with "A" grade; Accredited by NBA;  
VINJANAMPADU, GUNTUR, ANDHRA PRADESH - 522017.







## **7. Benefits in terms of learning/Skill/Knowledge obtained.**

Webinars are an essential part of academic life, Listeners will get the knowledge on the following topics.

**Improved security:** Vulnerability assessments help organizations to identify and prioritize potential vulnerabilities in their systems and networks, enabling them to take proactive measures to mitigate risks and improve their security posture.

**Reduced risk:** By identifying vulnerabilities and taking corrective actions, organizations can reduce the risk of cyber attacks and data breaches, protecting their critical assets and data.

**Compliance:** Vulnerability assessments are often required by regulatory standards such as PCI DSS, HIPAA, and GDPR, helping organizations to meet compliance requirements and avoid penalties.

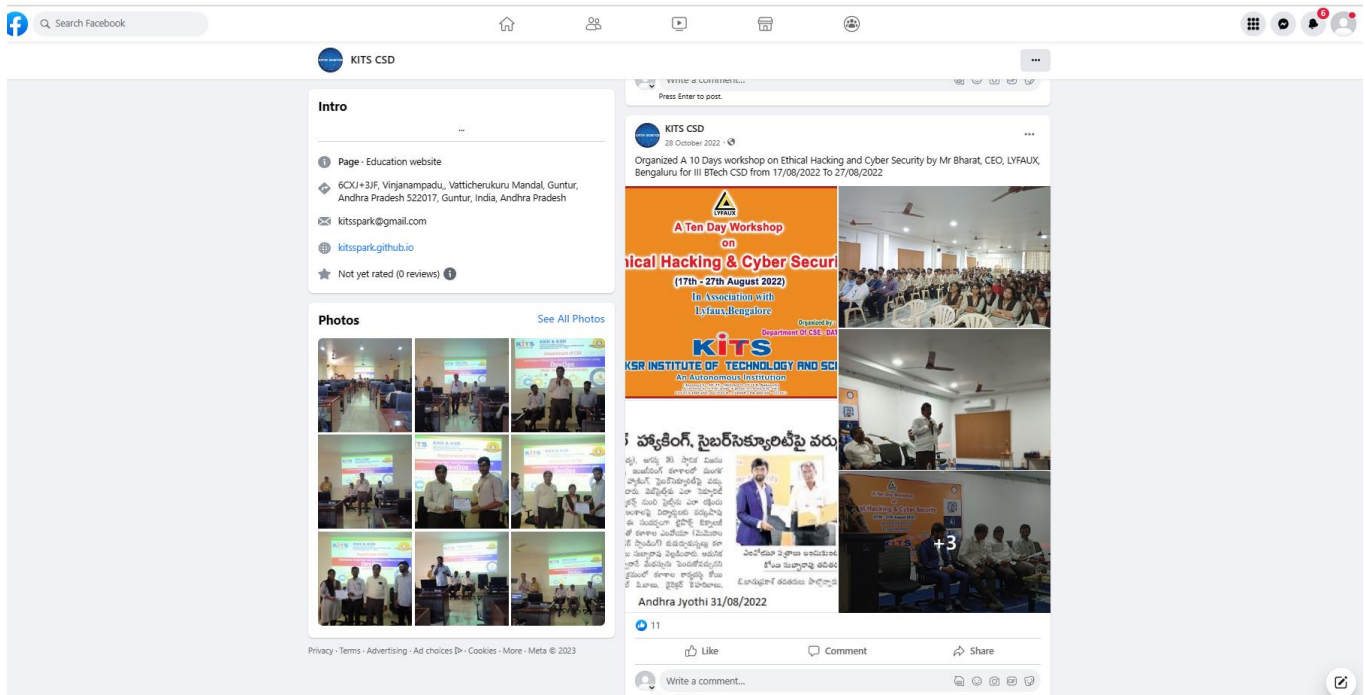
**Cost savings:** By identifying and addressing vulnerabilities before they are exploited, organizations can save the costs associated with data breaches, including legal fees, remediation costs, and loss of reputation.

**Reputation:** By taking proactive measures to secure their systems and networks, organizations can enhance their reputation and build trust with their customers and stakeholders.

**Continuous improvement:** Vulnerability assessments provide a baseline for future assessments and enable organizations to monitor their progress in reducing vulnerabilities over time, promoting continuous improvement and risk management.

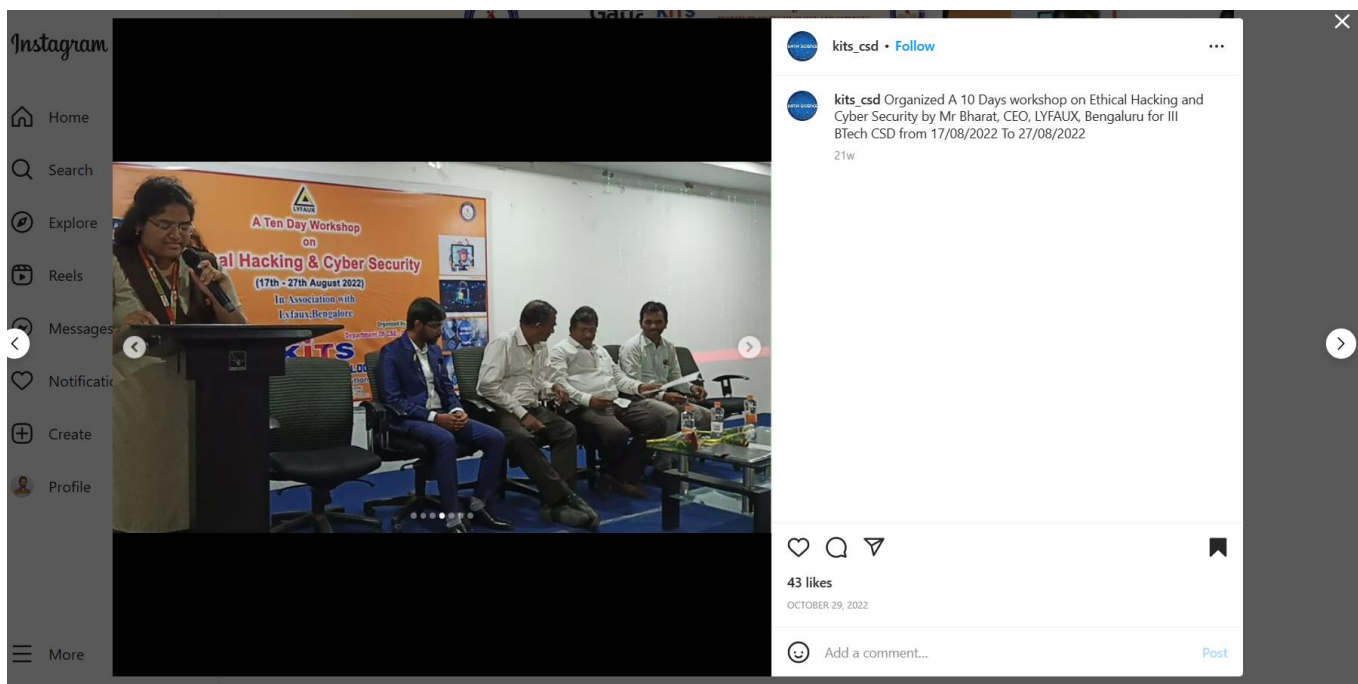
**8. Promotion of the Event on the Social Media Website: (Link and Screenshot):**

**(6) KITS CSD | Guntur | Facebook**



**9. Event on the University/college Website :( Link and Screenshot)**

[KITS\\_CSD \(@kits\\_csd\) • Instagram photos and videos](#)



**10. Expenditure Amount ( If any): Nil**

**11. Remarks:** The webinar is organized smoothly with practical orientation.

**12. Experiences and Output of the Session**

Many faculty, research scholars and students from various colleges attended this **Organized A 10 Days workshop on Ethical Hacking and Cyber Security by Mr Bharat, CEO, LYFAUX, Bengaluru for III BTech CSD from 17/08/2022 To 27/08/2022.**, conducted by KKR & KSR Institute of Technology and Sciences in association with SPARK.

**The following outcomes are achieved with the webinar**

Identification of vulnerabilities: The primary outcome of vulnerability assessment is the identification of security weaknesses, flaws, or loopholes that could be exploited by attackers. This includes vulnerabilities in hardware, software, network devices, and applications.

Assessment of risk: Once vulnerabilities have been identified, the next step is to assess the level of risk associated with each vulnerability. This includes evaluating the likelihood of an attack, the potential impact of a successful attack, and the overall risk to the organization.

**Prioritization of vulnerabilities:** Based on the level of risk associated with each vulnerability, vulnerabilities are prioritized based on their severity, likelihood of exploitation, and potential impact.

**Remediation recommendations:** Once vulnerabilities have been identified and prioritized, vulnerability assessment reports typically include recommendations for remediation. This may include patches, configuration changes, or other measures to mitigate the identified vulnerabilities.

**Compliance requirements:** Vulnerability assessments may also identify compliance requirements that the organization must adhere to, such as regulatory requirements or industry standards.