Report on
Incubation Centre for Cyber Security

Introduction

Cyber security touches nearly every part of our daily lives. Moreover, economic vitality, and national security depend on a stable, safe, and resilient cyberspace.

We rely on this vast array of networks to communicate and travel, powerour homes, run our economy, and provide government services. However, cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy. The nation has a significant shortage of cyber security professionals who canunderstand and effectively thwart the growing threats. As a result, education and training in cyber security has become a national priority. Students are also eager to acquire more knowledge and skills in this critical area.

The primary goal of setting up our cyber security lab was to give studentsthe possibility to understand different offensive cyber security activities, to detect ongoing attacks and also to perform defensive actions. In order to do all these activities, students need usually administrative privileges on the hosts. In the same time all these activities should not disturb the rest of the campus network. Therefore we must set up an isolated network environment where students have administrative (root) privileges on the systems.

Vision

To educate and develop high caliber technologists and scientists in Cyber Security Professionals for Research and Industry.

Objective

- Learn the principles and applications of basic science, software in order to prepare the students to understand various concepts, architectures, analytical and programming techniques for developing projects in Cyber Security.

- Know environmental issue, ethics, managerial skills and quality control that is required to maintain professionalism in the Cyber Security industries.

- Understand the usage and development of tools for developing graphic applications, network applications, hacking applications etc.

- To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

- To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

- To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.

- To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.

- To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.

Hardware Requirements:

- Processor:

  Quad core 2.8 Ghz 64 bit Intel i5 or AMD Ryzen 5 or A9, or more.

- RAM : 8gb ddr4 Or more.
- GPU: Nvidia GTX 1060 or more(4GB or more)
- Hard disk: 1 TB or more.
- Network Adapter
- A laptop or a desktop with as much RAM and processor power
- A large HDD or SSD to store your tools and other important files.
- Latest security patches must be installed on your guest OS before you start.
- A WiFi adapter that supports monitor mode.
- Keylogger
- Android Phone
- Router
- Pen drive for retrieving detected data.

Software Requirements:

- OS Updated window 10
- Updated Kali linux and Parrot
- Xampp
- Virtualization software(VMWare/VirtualBox)
- Guest Operating Systems

Essential Tools:

- Metasploit Framework (MSF):
- WireShark
- Nmap:
- John The Ripper:
- Burpsuite or OWASP ZAP:
- Kali Linux
- Invicti
- Acunetix
- Ettercap
- WebInspect
- Hashcat
- Rainbow Crack
- Cain and Abel
- Nessus
- Zenmap
- Netsparker

Education Facilities for Cyber security classes

Facilities include ample office and classroom space, as well as software to facilitateonline learning, and two telecommunications laboratories:

The School of Technology Telecommunications Laboratory incorporates a variety ofequipment aimed to teach students practical, basic and advanced applications of cyber-defense. The equipment specifically used for Cybersecurity practices includes:

- Six (6) CISCO 1941 Router w/802 11 a/b/g/n (2 ports)
- Five (5) Servers
    - Server IBM series 335
    - Server HP Proliant DL 360
    - Server IBM Series 335
    - 2 Windows Servers 12 R2
- Six (6) CISCO ASA 5512-X Firewalls WITH IPS SW 6GE
- Two (2) CISCO ASA 5512 firewalls full licensed with maximum cybersecuritysoftware
- Four (4) Palo alto PA 200 firewalls full licensed with maximum cybersecuritysoftware
- Four (4) CISCO CATALYST 2960-C 2 PORT switches
- About two dozen of different high capability Switches for diverse cybersecurityset-ups
- Iris recognition equipment/software
- Face recognition equipment/software
- Thirty (30) modern computers (LAPTOPS + DESKTOPS) for testing differentsecurity setups
- Nexpose/Rapid 7 software watchdog/scanner fully licensed for cybersecurity.

The above equipment used with some other legacy equipment (PIX Firewalls, CISCO2514 routers) allows development, application, and evaluation of more than a hundreddifferent practices in cybersecurity and data telecommunications.

The School of Business Telecommunications Lab also incorporates a variety of equipment aimed to teach students practical, basic and advanced applications of computer networking and cyber security. The equipment specifically used for Cybersecurity practices includes:

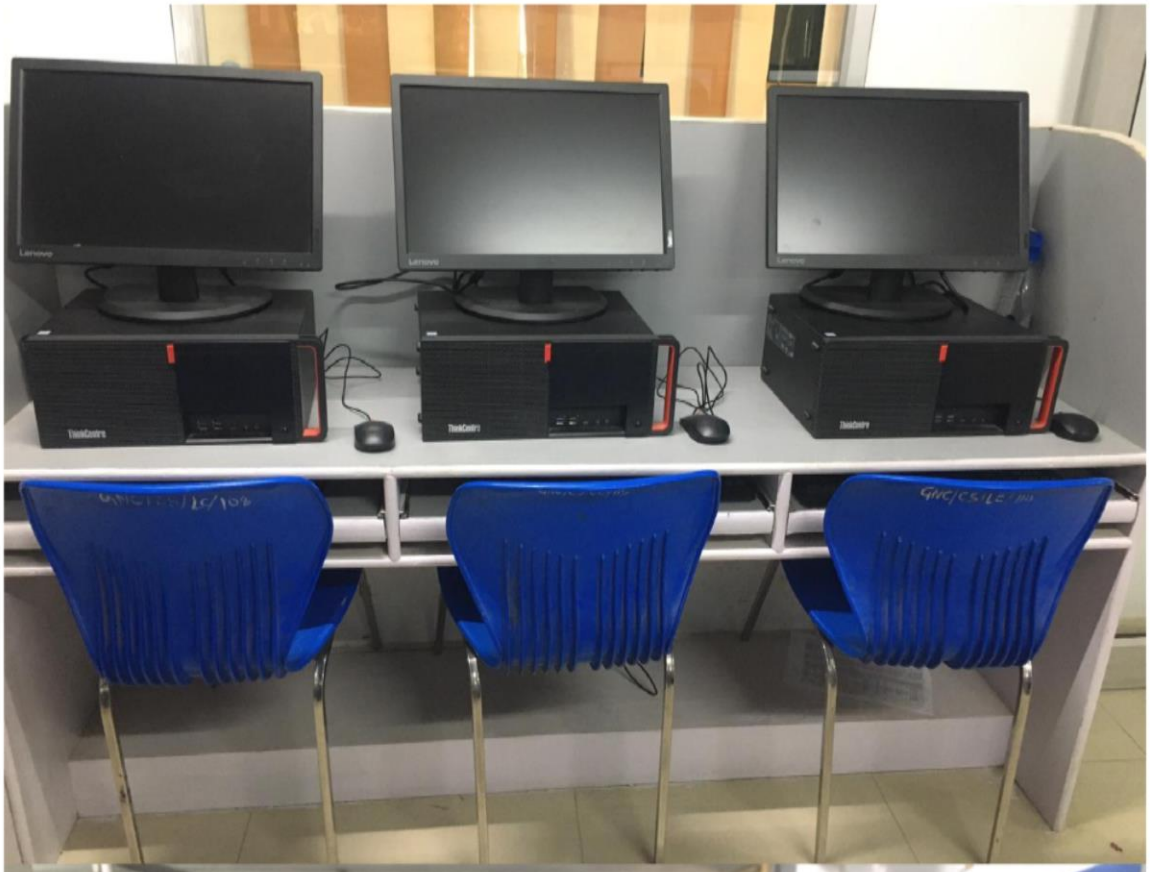
- One (1) rack server composed of ten (10) Dell PowerEdge 860 servers
- One (1) Dell PowerEdge T100 Tower server
- One (1) Sonicwall T2170 firewall
- One (1) Cisco 1700 router
- Three (3) APC SmartUPS 3000 UPS devices
- One (1) MGE Pulsar EX 10 UPS device
- Thirty (30) Dell VOSTRO 220s desktop computers
- Two (2) Netgear DS 116 Ethernet switches
- One (1) Netgear FS 108 Ethernet switch

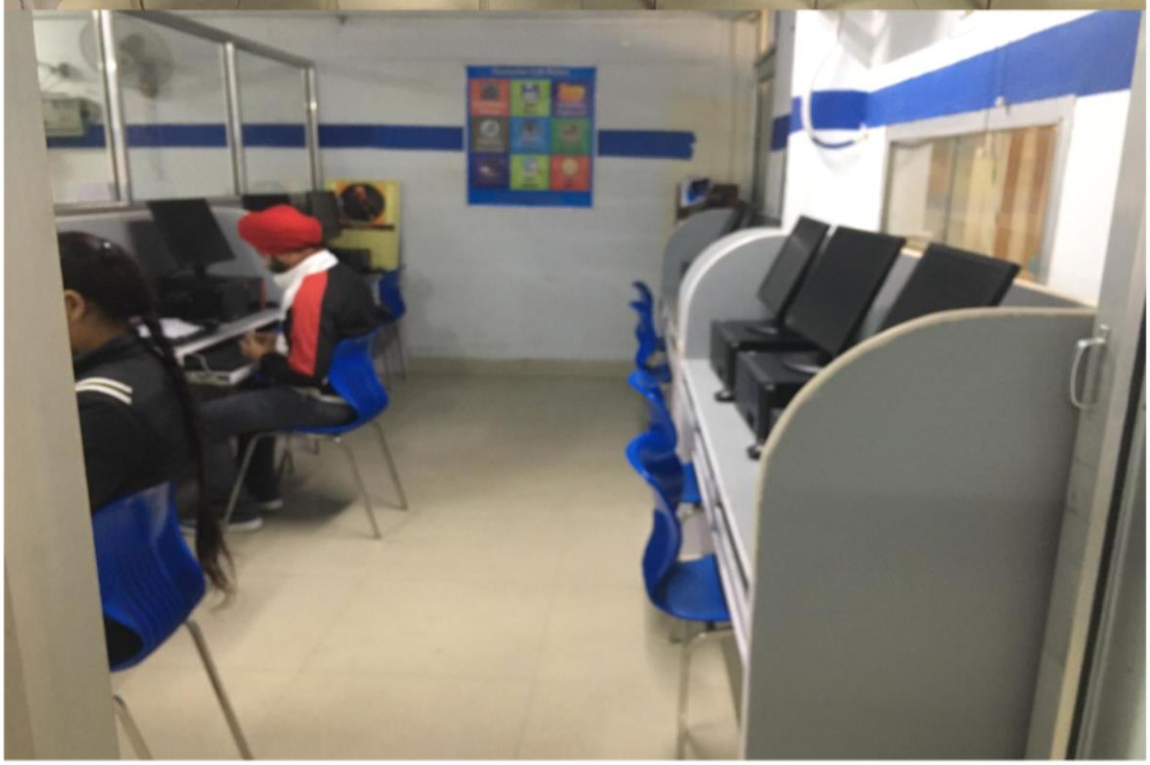
The School of Business Telecommunications Lab equipment is part of a local area network (LAN), where students enrolled in Cybersecurty-related courses install approved hacking tools and network defense software that they use for learning anddeveloping ethical hacking and network defense skills.

GURU NANAK COLLEGE BUDHLADA

Under the Management of Shiromani Gurdwara Parbandhak Committee, Sri Amritsar Sahib

Session 2022-23

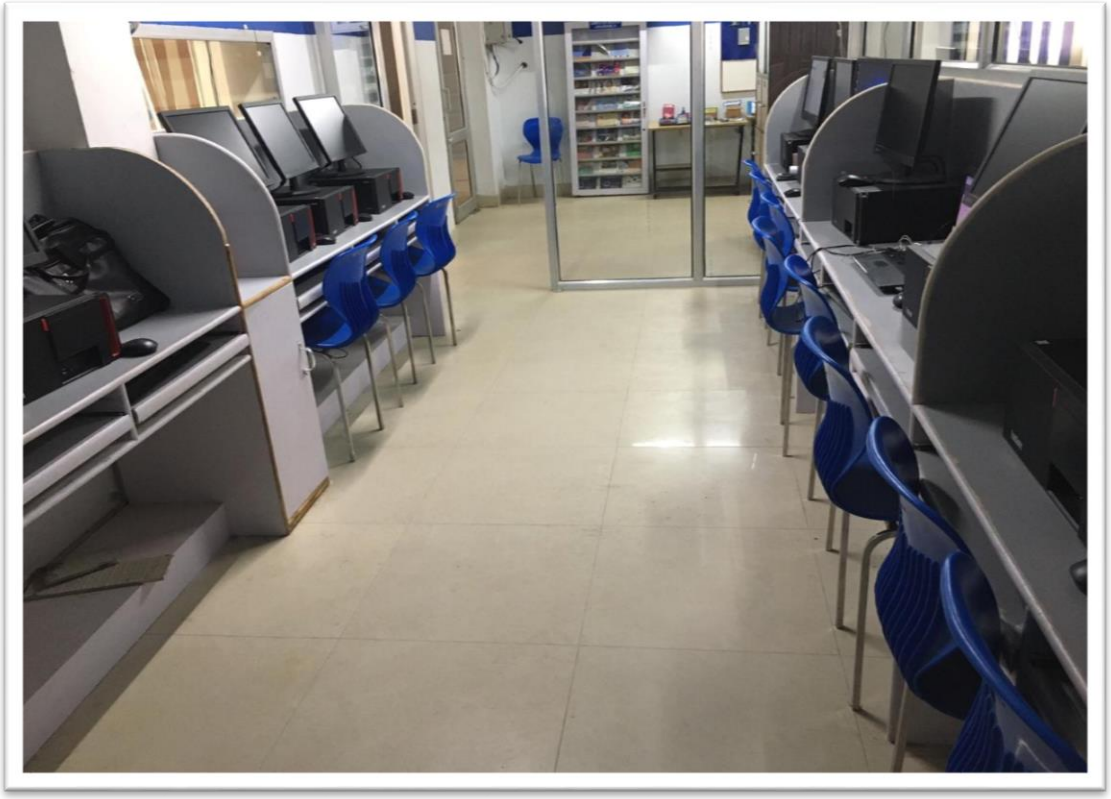


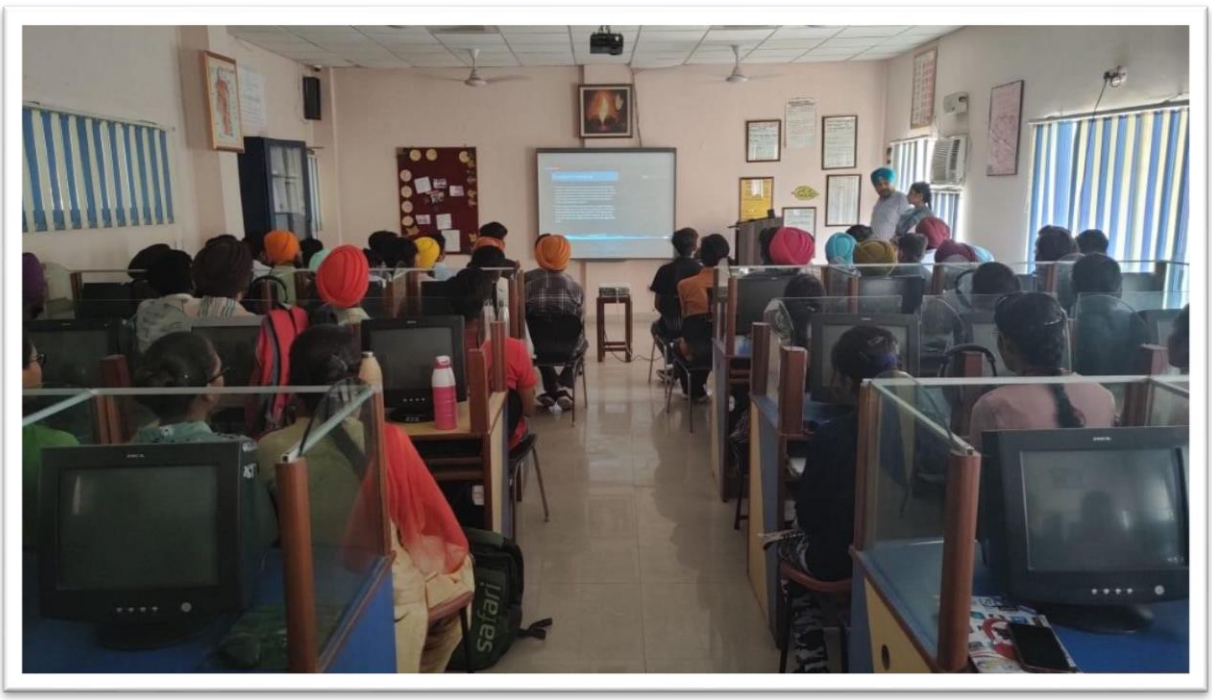


GURU NANAK COLLEGE BUDHLADA

Under the Management of Shiromani Gurdwara Parbandhak Committee, Sri Amritsar Sahib

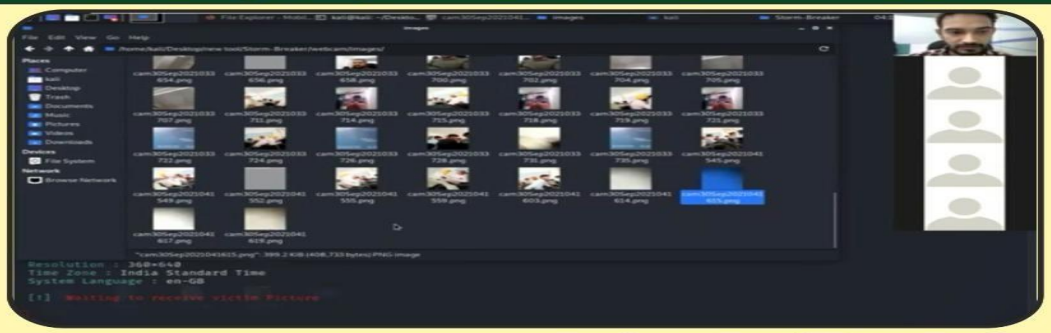
Session 2022-23





GURU NANAK COLLEGE BUDHLADA
Under the Management of Shiromani Gurdwara Parbandhak Committee, Sri Amritsar Sahib
Session 2022-23

ਐਥੀਕਲ ਅਤੇ ਐਂਡਰਾਇਡ ਹੈਕਿੰਗ 'ਤੇ ਆਨ-ਲਾਈਨ ਲੈਕਚਰ ਦਾ ਆਯੋਜਨ



ਬੁਢਲਾਡਾ, 05 ਅਕਤੂਬਰ
-ਸਥਾਨਕ ਗੁਰੂ ਨਾਨਕ ਕਾਲਜ ਦੇ ਕੰਪਿਊਟਰ ਸਾਇੰਸ ਵਿਭਾਗ ਵੱਲੋਂ ਇਕ ਦਿਨਾ ਆਨ-ਲਾਈਨ ਐਥੀਕਲ ਅਤੇ ਐਂਡਰਾਇਡ ਹੈਕਿੰਗ 'ਤੇ ਆਨ-ਲਾਈਨ ਲੈਕਚਰ ਦਾ ਆਯੋਜਨ ਕੀਤਾ ਗਿਆ। ਇਸ ਲੈਕਚਰ ਦਾ ਮਕਸਦ ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਆਈ.ਟੀ ਸੈਕਟਰ ਵਿੱਚ ਐਥੀਕਲ ਹੈਕਿੰਗ ਤਕਨਾਲੌਜੀ ਦੀਆਂ ਨਵੀਆਂ ਤਕਨੀਕਾ ਅਤੇ ਐਡਰਾਇਡ ਹੈਕਿੰਗ ਸਬੰਧੀ ਜਾਣਕਾਰੀ ਦੇਣਾ ਸੀ। ਕੰਪਿਊਟਰ ਸਾਇੰਸ ਵਿਭਾਗ ਦੇ ਮੁਖੀ ਡਾ. ਰੇਖਾ ਕਾਲੜਾ ਨੇ ਦੱਸਿਆ ਕਿ ਕੰਪਿਊਟਰ ਸਾਇੰਸ ਦੇ ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਨਵੀਆਂ ਖੋਜਾਂ ਬਾਰੇ ਜਾਣਕਾਰੀ ਦੇਣਾਂ ਜਰੂਰੀ ਹੁੰਦਾ ਹੈ ਜਿਸ ਕਰਕੇ ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਸਮੇਂ ਸਮੇਂ ਤੇ ਆਈ.ਟੀ. ਖੇਤਰ ਨਾਲ ਸਬੰਧਤ ਗੈਸਟ ਲੈਕਚਰਾਂ ਦਾ ਪ੍ਰਬੰਧ ਕੀਤਾ ਜਾਂਦਾ ਹੈ। ਉਨ੍ਹਾਂ ਕਿਹਾ ਕਿ ਅੱਜ ਦੇ ਆਨ-ਲਾਈਨ ਲੈਕਚਰ ਵਿੱਚ ਨਵੀਂ ਦਿੱਲੀ ਤੋਂ ਇੰਨੋਬੁਜ਼ ਲਰਨਿੰਗ ਸੋਲੂਸ਼ਨ ਦੇ ਸਾਇਬਰ ਸਕਿਓਟੀ ਐਕਸਪਰਟ ਅਤੇ ਟ੍ਰੇਨਰ ਸ੍ਰੀ ਰੋਹਿਤ ਕਾਸਵਾਂਨ ਨੇ ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਐਥੀਕਲ ਅਤੇ ਐਂਡਰਾਇਡ ਹੈਕਿੰਗ ਬਾਰੇ ਪ੍ਰੈਕਟੀਕਲ ਵਿੱਚ ਜਾਣਕਾਰੀ ਦਿੱਤੀ। ਉਨ੍ਹਾਂ ਸੰਸਥਾਵਾਂ, ਉਦਯੋਗ ਦੀਆਂ ਸ਼ਾਖਾਵਾਂ, ਬੈਕਿੰਗ, ਆਨ-ਲਾਈਨ ਲੈਣ-ਦੇਣ ਨੂੰ ਸੀਮਤ ਸਾਧਨਾਂ ਰਾਹੀ ਹੈਕਰਾਂ ਤੋਂ ਬਚਾਉਣ ਲਈ ਵਿਸਥਾਰ ਸਹਿਤ ਜਾਣਕਾਰੀ ਦਿੱਤੀ। ਉਨ੍ਹਾਂ ਦੱਸਿਆ ਕਿ ਅੱਜ ਆਈ.ਟੀ ਸੈਕਟਰ ਵਿੱਚ ਜਿੱਥੇ ਵੀ ਕਿਤੇ ਆਨ-ਲਾਈਨ ਦੇਣ-ਲੈਣ, ਵਪਾਰ ਆਦਿ ਹੁੰਦਾ ਹੈ ਉਥੇ ਹੈਕਰਾਂ ਵੱਲੋਂ ਕੰਮਜ਼ੋਰ ਪਾਸਵਰਡ ਵਾਲੇ ਸਿਸਟਮਾਂ ਨੂੰ ਪਛਾਣਕੇ ਉਨ੍ਹਾਂ ਵਿੱਚੋਂ ਅਨ-ਅਧਕਾਰਿਤ ਤੌਰ ਤੇ ਡਾਟਾ ਚੋਰੀ ਕਰ ਲਿਆ ਜਾਂਦਾ ਹੈ ਜਿਸ ਕਰਕੇ ਸੰਵੇਦਨਸ਼ੀਲ ਡਾਟਾ ਦਾ ਨੁਕਸਾਨ ਹੋ ਜਾਂਦਾ ਹੈ। ਇਸ ਮੌਕੇ ਕਾਲਜ ਪ੍ਰਿੰਸੀਪਲ ਡਾ. ਕੁਲਦੀਪ ਸਿੰਘ ਬੱਲ ਨੇ ਵਿਭਾਗ ਦੇ ਕੀਤੇ ਉਪਰਾਲੇ ਦੀ ਸ਼ਲਾਘਾ ਕੀਤੀ। ਇਸ ਗੈਸਟ ਲੈਕਚਰ ਮੌਕੇ ਕੰਪਿਊਟਰ ਸਾਇੰਸ ਵਿਭਾਗ ਦੇ ਸਹਾਇਕ ਪ੍ਰੋ. ਡਾ. ਰਾਜਕਮਲ ਕੌਰ, ਮਨਪ੍ਰੀਤ ਕੌਰ, ਇੰਸਟ੍ਰਕਟਰ ਅਨੂਪ ਸਿੰਘ ਹਾਜ਼ਿਰ ਸਨ।
ਕੈਪਸ਼ਨ: ਗੈਸਟ ਲੈਕਚਰ ਮੌਕੇ ਦੀਆਂ ਤਸਵੀਰਾ।

(ਜੀ.ਐਨ.ਸੀ. ਪ੍ਰੈਸ ਕਲੱਬ)