

2017-2018



CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.

CMRCET/PRIN/1/2017.

Date: 2nd September, 2017

OFFICE ORDER

This is to inform all faculty, staff and students that with the recommendations of IQAC, it is proposed to have the various committees and Clubs in the institution from this A.Y 2017-18 to improve the quality of educational standards and also for the benefit of faculty, staff, students and community.

The Following committees are proposed

1. Coding Club
2. Cyber Security Club

The above committees will be constituted with the following positions.

Chairman - Principal

Convener/coordinator - Senior Faculty

Member – 01 Faculty from each Department

Student Member – 01 Student from each Department (If Required)

Copy Submitted to: (1) The Secretary garu (for kind information please).

- Copy to:
- (1) Deans.
 - (2) Vice Principal
 - (3) IQAC
 - (4) All HODS / Incharges.
 - (5) Administrative Officer.
 - (6) Accounts Officer,
 - (7) Office Copy.

Principal

PRINCIPAL

CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

Principal

CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

CMRCET/PRIN/02/2017
Date: 06/09/2017
OFFICE ORDER

With reference to the office order "CMRCET/PRIN/1/2017, Dated 2nd September, 2017", this is to inform all the faculty, staff and students that the following are members of the composition of Cyber Security Club for the academic year 2017-18.

The composition of Cyber Security Club Committee is as follows:

S.No.	Member & Designation		
1.	Chairman - Dr.V.A Narayan, Principal CMRCET		
2.	Convener – Mr. Siva Skandha Sanagala, Assoc.prof,CMRCET		
3.	Coordinator-Mr.B.Tulasi Dasu, Assistant Professor,CMRCET		
3.	Faculty Members :		
	Sno	Name of the Faculty	Designation
	1.	K.Loheswaran	Assistant Professor
	2	P.Ramesh	Assistant Professor
	3	Y.CHITTIBABU	Assistant Professor
	4	M.SUNEEL KUMAR	Assistant Professor
	5	Vinayak B. Naduvinamani	Assistant Professor
			Department
			CSE
			CSE
			ECE
			EEE
			MECH
4.	Student Members :		
	Sno	Name of the Student	Branch
	01	Mr M Surya	CSE
	02	POLOJU VEENA	CSE
	03	VASA KARTHIK	CSE
	04	RAPOLU RAVI TEJA	CSE
	05	K MADHUSUDAN CHOWDARI	CSE
	06	POLINENI DIVYA	CSE
	07	SONALI	CSE



Coordinator




Principal

Copy Submitted to: (1) The Secretary Garu – For your kind information Pl.

Copy to:

1. IQAC Coordinator
2. Controller of Examinations
3. All HODS
4. Administrative Officer
5. Accounts Officer
6. Concerned Faculty



PRINCIPAL
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.



CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.

CMRCET/PRIN/IT/AY2017-18/CIR-03


Date: 07/09/2017

CIRCULAR

All the members of Cyber Security Club of the college are hereby informed that, the Cyber Security Club committee meeting is scheduled on 09.09.2017 & the Venue is CSE Seminar hall at 1:00 pm. All are requested to be present on time.

The Agenda of the meeting is:


- To Discuss about the SOP, Objectives, Roles & Responsibilities.
- Understanding the Behavior of Threat Actors
- Security for the future .
- Discuss Security Attacks and Preventions
- How to avoid Cyber Security in network


Principal

Copy Submitted to: (1)The Secretary Garu – For your kind information Pl.
PRINCIPAL,
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

Copy to:

1. IQAC Coordinator
2. Controller of Examinations
3. All HODS
4. Administrative Officer
5. Accounts Officer
6. Concerned Faculty


PRINCIPAL
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

Academic Year: 2017-18
CYBER SECURITY CLUB COMMITTEE
MINUTES OF MEETING

1. The Meeting was held on 9th September 2017 from 1:00 to 3:30 pm in the Department of CSE Seminar hall.
2. The Convener welcomed all the Club committee members
3. SOP was finalized during the meeting with Objectives, Roles & responsibilities

STANDARD OPERATING PROCEDURE OF CYBER SECURITY CLUB COMMITTEE

Purpose: The purpose of this committee is to form guidelines and procedures to be adopted for protect the usability, reliability, integrity and safety of the network.

Scope: With the advent of the modern technological age, people and surrounded things get connected with each other. For protecting those connections, there is a great need for the students of **all Engineering** to protect the security of these connections. The experts of this industry are trying to remove the threats but various scandals of big companies have become attractive attention. In the coming years, this market showed expected growth and is more likely to develop and rise.

Roles & Responsibility:


1. Monitor network and application performance to identify and irregular activity
2. Set up patch management systems to update applications automatically
3. Work with IT operations to set up a shared disaster recovery/business continuity plan
4. Work with HR and/or team leads to educate employees on how to identify suspicious activity

Frequency of committee meeting

- Four times in the every Academic Year. Every meeting at before starting the semester and end of semester.
- Committee may conduct meeting as and when required

I. Salient Aspects of Cyber Security Policy and Responsibility

- (a) Internet connections should be on standalone mode PCs only with no classified data on them. Strict air-gap to be main between Internet and Army networks.
- (b) No dial up access should be there on networked PCs. Official PCs will not be used to access Internet using mob phones/ USB dongles.
- (c) PCs should have strong booting and log on passwords.
- (d) No classified info to be stored on PCs permanently. Under no circumstances data classified as CONF and above will be typed/ viewed on PA/Steno's PC.
- (e) PCs used for processing cl info will NOT be connected on Army One/ Internet/ any other network and these will not have internal CD/DVD writers.



PRINCIPAL
CMR COLLEGE OF ENGG & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

II. Software & Hardware Security

System Software.

- Users must use proper licensed version of the system software like Operating System and this must be periodically updated.
- Default setting in the system software must be reviewed during the installation and the same to be checked from time to time. Vendor supplied default user IDs (like Administrator, Guest) must be deleted or password changed before allowing users to access the computer system.
- Critical components of the network like switches, servers, routers and security appliance must be powered using redundant online Uninterrupted Power Supply (UPS) with automatic shutdown facility in case of power failure to prevent crashing of associate system software.

Application software.


- All application software development will ensure secure coding practices such as Input data validations, checking for internal processing errors, output data validation, buffer overflow and use of minimum privileges for execution.
- The application software, both being developed in house or procured throughout outsourcing, also needs to be clear of any embedded malicious codes. The developing agency be asked to certify the same. Care needs to be taken to choose to a trusted developing agency with credible capability of producing error-free software.
- All computer issued to the environment are the property of the org for carrying out official tasks only. Only those applications will be installed in the network resources as are needed for official purposes

Hardware Security

- Hot-Standby Systems. Critical servers, at all nodes must always run with hot standby systems. Other servers must provision back up of their data through auxiliary storage devices, wherever possible.
- UPS Devices. All computer systems must always run with UPS devices. Online UPS devices must be used for all access/control equipment at all communication nodes and other types of UPS may be used for other computers.
- While procuring IT related hardware, the structured evaluation process, in vogue, be resorted to with the info security features duly identified within the Request for Proposal Compliance of these features be confirmed during installation and Acceptance Testing process. Necessary provisions be included in the contract document to allow up-gradation/modification to hardware by the seller to ensure desired info security.

User Awareness, Security Checks and Reporting of Security Breach

- Security of info especially in the context of cyber security is dynamic. All users of the computers and networks need to be aware about cyber security and must exercise better security consciousness.
- A six-monthly cyber security audit will be carried out in the HQ Dte Gen NCC by a bd of offrs. Proper records of such audit will be maint and a report will be fwd promptly if any security breach is detected/ reported. Imp DOs and DON'Ts on cyber security for all users are given at att appx.



PRINCIPAL
CMR COLLEGE OF ENGG & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

- Upon discovery of cyber security breach/ loss, report to be initiated on such occurrence and subsequent investigations will be carried as per instrs contained in classification and handling of classified documents 2001.

IMP CYBER SECURITY DOs AND DON'Ts FOR ALL USERS

Dos. Users are advised to observe the following Dos:-

- Do use computer lock when not in use to avoid unauth access. Do use passwords for:-
 - (i) Booting and screensaver.
 - (ii) Login/access to computer
 - (iii) Access to indl files/ folders.
- Do keep the backup data on CDs/DVDs which are kept in safe custody and are properly accounted for.
- Do keep only system files and programs on hard disk as far as possible.
- Do copy data/files created after each session on removable media like floppies/CDs and keep it at physically secure place.
- Do erase data/files by shredding from the hard disk.
- Do log off PCs in a network to obviate unauthorized client stations accessing e-mails and stored files.
- Do avoid networked configuration file sharing to rule out access by unauthorized persons.
- Do open email-box regularly and scrutinize its contents. Info/ data not required must be deleted periodically.
- Do scan external storage media for viruses before these are used on computers.
- Do report questionable/unidentified files on your PC.
- Do report any loss of media immediately to offr auth to ensure cyber security in the br/sec/est.

Don'ts. Users are advised to observe the following Don'ts:-

- Don't give access to the computer to any outside/ unauth pers and Don't disclose your password to any unauthorized pers.
- Don't permit copying of files/ info from your computer to any outsider.
- Don't let the vendor/ mech take away hard disk in the event of a hard disk crash /failure. If it is certified that the disk is unserviceable, it will be removed and destroyed by a bd of offrs.
- Don't use external storage media on your computer unless scanned for virus . Virus can destroy all the files on your hard disk.
- Don't copy programs from unauth sources.
- Don't leave any confd docu/letters on the computer hard disk. In case of large vol of confd data on hard disk being used repeatedly, ensure computer is kept in the auth offr's office and clk/opr work under supervision/obsn.
- Don't keep data of classified nature on hard disk of PCs on a network.

PRINCIPAL
CMR COLLEGE OF ENGG & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.

The List of Cyber Security Club Committee members attended the meeting:


S.No	Name of the member	Designation	Position	Signature
1.	Dr.V.A Narayan	Principal	Chairman	
2.	Mr S Siva Skanda	Associate Professor	Convener	
	Mr.B.Tulasidasu	Assistant Professor	Coordinator	
3	K.LOHESWARAN	Assistant Professor	Member	
4	Mr. P.Ramesh	Assistant Professor	Member	
5	Mr. Y.CHITTIBABU	Assistant Professor	Member	
6	Mr. M.SUNEEL KUMAR	Assistant Professor	Member	
7	Mr .Vinayak B. Naduvinamani	Assistant Professor	Member	


Convener

Copy Submitted to: (1) The Secretary Garu - For your kind information Pl.

Copy to:

1. IQAC coordinator
2. Concerned Faculty


PRINCIPAL
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.



CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.

Date: 14.09.2017

To
IQAC
CMRCET
Medchal
Kandlakoya

Subject : Requesting approval to conduct the Club of the **CYBER SECURITY CLUB** for the A.Y 2017-18.


I, Mr.B.Tulasidasu, coordinator of the **CYBER SECURITY CLUB** and Assistant professor of CSE department earnestly requesting your permission to conduct the following events.

Following is the schedule of events to be conducted under **CYBER SECURITY CLUB** for the Academic Year 2017-18

S.No	Program	Date
1	Creak of IP Address	23/09/2017
2	Hacking in browser	02/12/2017
3	Trace of IP Address	11/03/2018

I request you to grant me permission and do the needfu!

Thanking you,


PRINCIPAL
MR COLLEGE OF ENGG & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.


Coordinator



CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.

Date: 18/09/2017

To.
The Principal
CMRCET
Kandlakoya (V)
Hyderabad.

Dear Sir,

Sub: Requesting permission to conduct an Creak of IP Address in System with Hacking Techniques

I, Mr. B. Tulasidasu, coordinator of the **CYBER SECURITY CLUB** and Assistant professor of CSE department earnestly requesting your permission through IQAC Co-Ordinator to conduct an Cyber Security Club.

1. Date of Event : 23/09/2017
2. Name of event : **Creak of IP Address in System with Hacking Techniques**
3. Venue of event: Android Lab Block II , Room no 113
4. Target audience: students
5. Faculty, staff and students involved in the event: List Enclosed.


I request you to grant me permission and do the need full.


Thanking you

Yours sincerely


(B. Tulasidasu)

permitted


18/9/17


PRINCIPAL
CMR COLLEGE OF ENGG & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.



CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.

CMRCET/PRIN/IT/AY2017-18/CIR-04

Date: 20/09/2017

CIRCULAR

All the students of **CYBER SECURITY CLUB** are invited to participate in Creak of IP Address in System with Hacking Techniques

Event Details:

Date: 23/09/2017

Time: 01:00 PM to 4:00 PM

Venue: Android Lab 113, Block-II.

Contact: Mrs B Tulasi Dasu, coordinator (9676073625).

PRINCIPAL

CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

Copy Submitted to: (1) The Secretary Garu – For your kind information Pl.

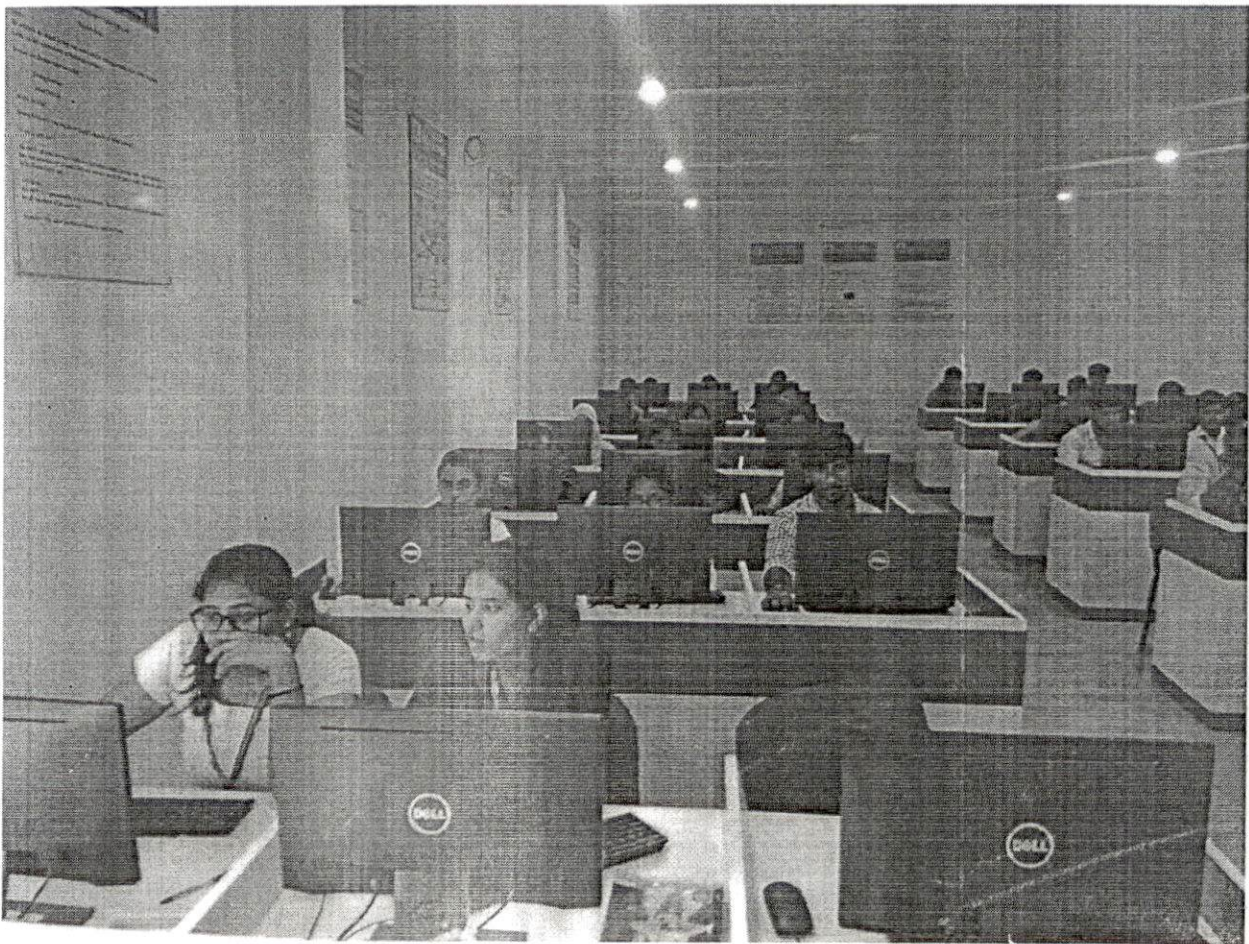
- (1) Deans
- (2) IQAC Coordinator
- (2) All HODS
- (3) Administrative Officer
- (4) Accounts Officer
- (5) Concerned Students members
- (6) Concerned Faculty Members

PRINCIPAL

CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

REPORT ON Creak of IP Address in System with Hacking Techniques on **23rd October 2017**

In our College we are conducting Cyber Security Club of Creak of IP Address in Systems Now a Days When a computer is attacked, it's often possible to obtain an IP address that's close to the attacker's location. Intrusion alerts from programs like Norton, McAfee and Malware bytes often provide the best address they can. And you can find similar information in the "full tracking headers" or "message sources" of email messages. These headers have different names in different email systems and are viewed in different ways. But once you determine how to open a full header in your email system, search it for a "from" or "source" IP and trace that address.




PRINCIPAL
CMR COLLEGE OF ENGG & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.



To do so, slip the address into a few of the many Web services that map IP locations. My current favorites (in this order) are:

- <http://www.liveipmap.com>
- <http://www.ip-address.com>




PRINCIPAL
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.



CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.

Date: 25/11/2017

To.
The Principal
CMRCET
Kandlakoya (V)
Hyderabad.

Sub: Requesting permission to conduct an Hacking in browser

I, Mr. B. Tulasidasu, coordinator of the **CYBER SECURITY CLUB** and Assistant professor of CSE department earnestly requesting your permission through IQAC Co-Ordinator to conduct an Cyber Security Club.

1. Date of Event : 02/12/2017
2. Name of event : **Hacking in browser with Hacking Techniques**
3. Venue of event: Android Lab Block II , Room no 113
4. Target audience: students
5. Faculty, staff and students involved in the event: List Enclosed.

I request you to grant me permission and do the need full.

Thanking you


Yours sincerely


(B. Tulas Dasu)

Permission granted


25/11/17

CMR COLLEGE OF ENGINEERING & TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad - 501401.


PRINCIPAL
CMR COLLEGE OF ENGG & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.



CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.

CMRCET/PRIN/IT/AY2017-18/CIR-05

Date: 28/11/2017

CIRCULAR

All the students of **CYBER SECURITY CLUB** are Invited to participate in **Hacking in browser with Hacking Techniques**

Event Details:

Date: 02/12/2017

Time: 01:00 PM to 4:00 PM

Venue: Android Lab 113, Block-II.

Contact: Mrs B Tulasi Dasu, coordinator (9676073625).

Principal

CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

Copy Submitted to: (1) The Secretary Garu – For your kind information Pl.

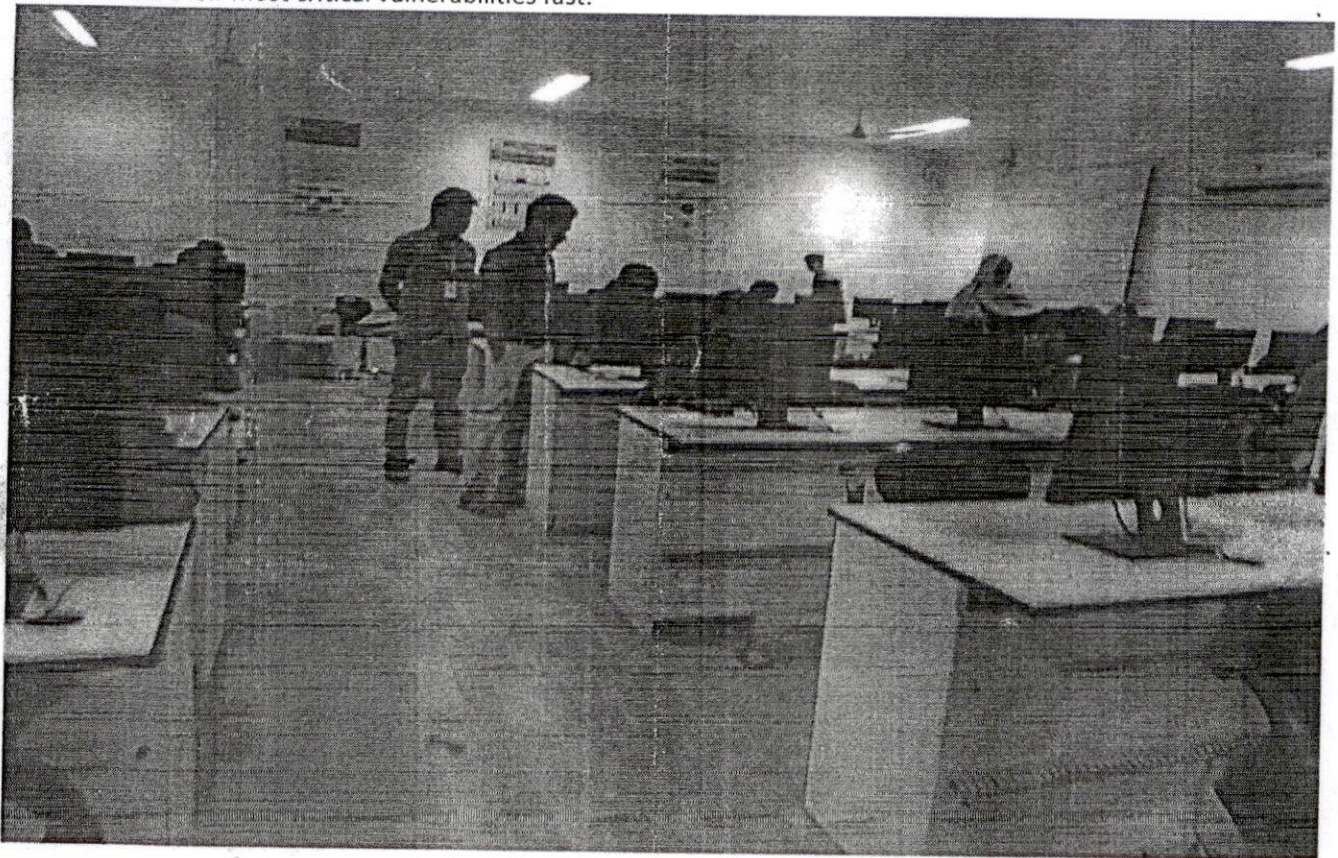
- (1) Deans
- (2) IQAC Coordinator
- (2) All HODS
- (3) Administrative Officer
- (4) Accounts Officer
- (5) Concerned Students members
- (6) Concerned Faculty Members

PRINCIPAL

CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

Report on Hacking in browser with Hacking Techniques on
30th November 2017

HackerOne's community of hackers includes representatives from practically every country and territory on the planet. India, the United States, Russia, Pakistan and the United Kingdom round out the top five countries represented, with 43% based in India and the United States combined. The fact that hackers hail from nearly every longitude and latitude, provides a true meaning to "hack the planet". With the online nature of hacker-powered security programs it is easy for hackers to find new and potentially lucrative opportunities from anywhere. A company in the United States or the United Kingdom can seamlessly work directly with leading hackers in India and Russia to find their most critical vulnerabilities fast.



The Department of Defense has fixed over 3,000 vulnerabilities in the past 18 months - that's over 167 vulnerabilities a month, or approximately 6 submitted each day. Read the Wired recap of "Hack the Pentagon" and the DoD's ongoing vulnerability disclosure policy published on HackerOne.

✓
PRINCIPAL
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

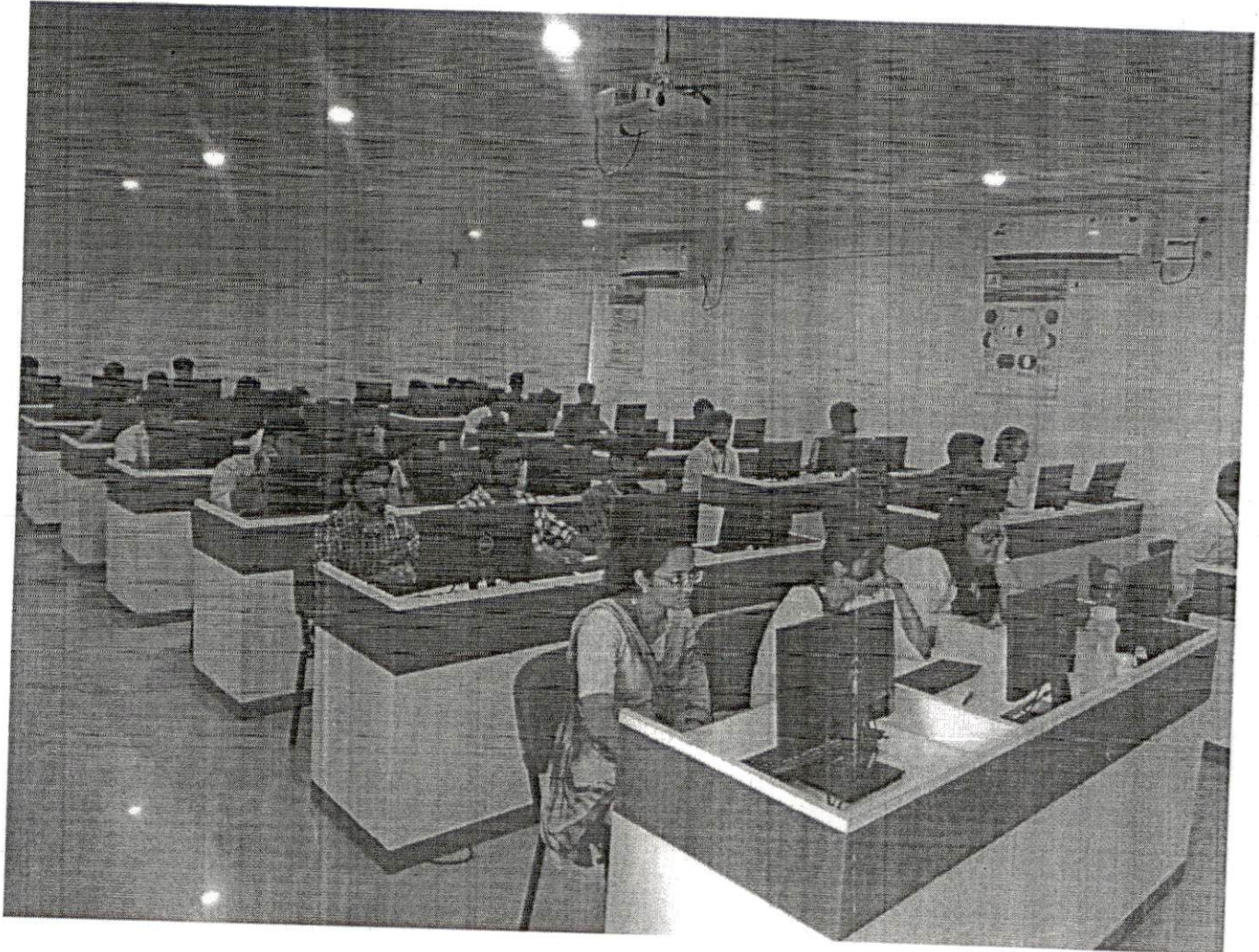



CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.

To do so, slip the address into a few of the many Web services that map IP locations. My current favorites (in this order) are:

- <http://www.liveipmap.com>
- <http://www.ip-address.com>




PRINCIPAL
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.



CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.

Date: 02/03/2018

To.
The Principal
CMRCET
Kandlakoya (V)
Hyderabad.

Dear Sir,

Sub: Requesting permission to conduct an Trace of IP Address Hacking Techniques

I, Mr. B. Tulasidasu, coordinator of the **CYBER SECURITY CLUB** and Assistant professor of CSE department earnestly requesting your permission through IQAC Co-Ordinator to conduct an Cyber Security Club.

1. Date of Event : 11/03/2018
2. Name of event : **Trace of IP Address Hacking Techniques**
3. Venue of event: Android Lab Block II , Room no 113
4. Target audience: students
5. Faculty, staff and students involved in the event: List Enclosed.


I request you to grant me permission and do the need full.


Thanking you

Yours sincerely


(B. Tulasidasu)

Permitted to conduct


02/03/18


PRINCIPAL
CMR COLLEGE OF ENGG & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

CMRCET
Kandlakoya



CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.

CMRCET/PRIN/IT/AY2017-18/CIR-05

Date: 09/03/2018

CIRCULAR

All the students of **CYBER SECURITY CLUB** are invited to participate in **Trace of IP Address Hacking Techniques**


Event Details:

Date: 11/03/2018

Time: 01:00 PM to 4:00 PM


Venue: Android Lab-113, Block-II.

Contact: Mrs B Tulasi Dasu, coordinator (9676073625).


PRINCIPAL
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.


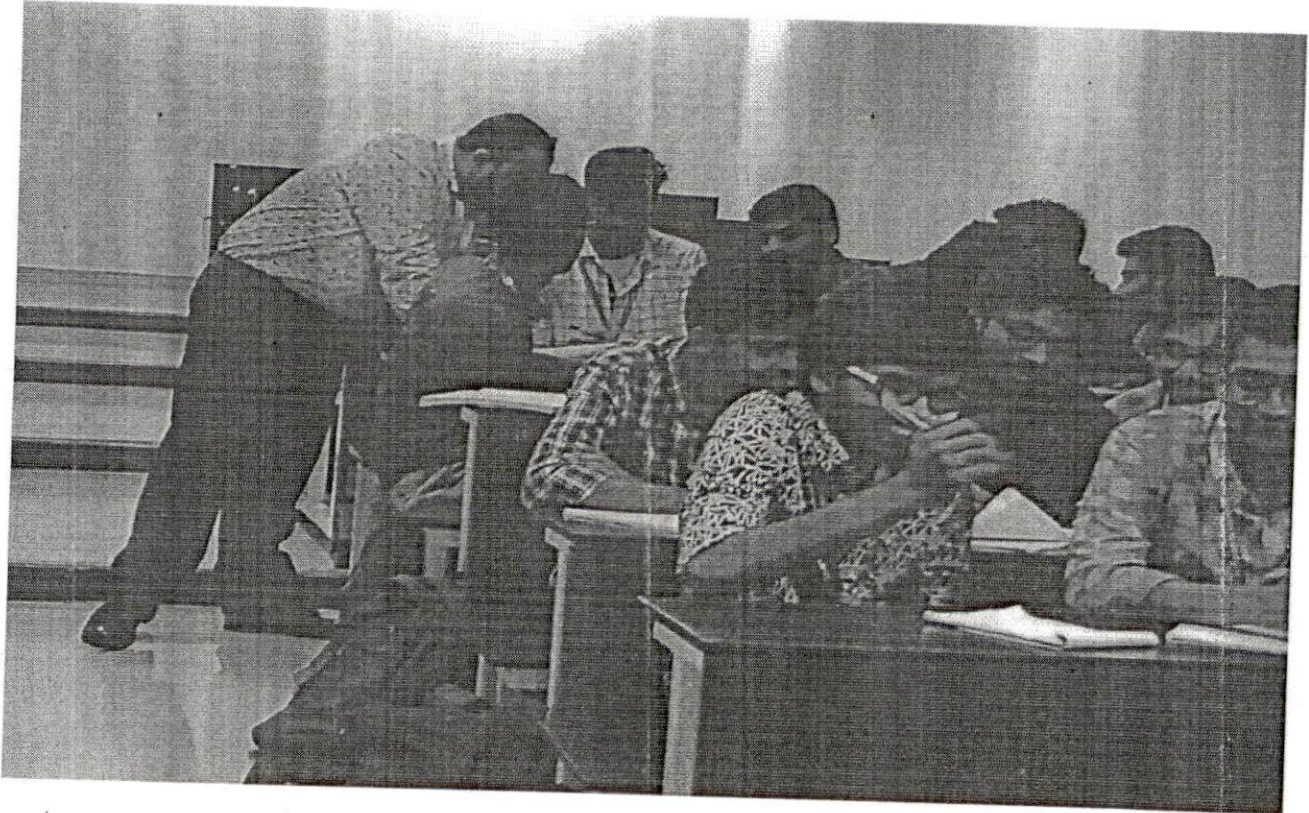
Copy Submitted to: (1) The Secretary Garu – For your kind information Pl.

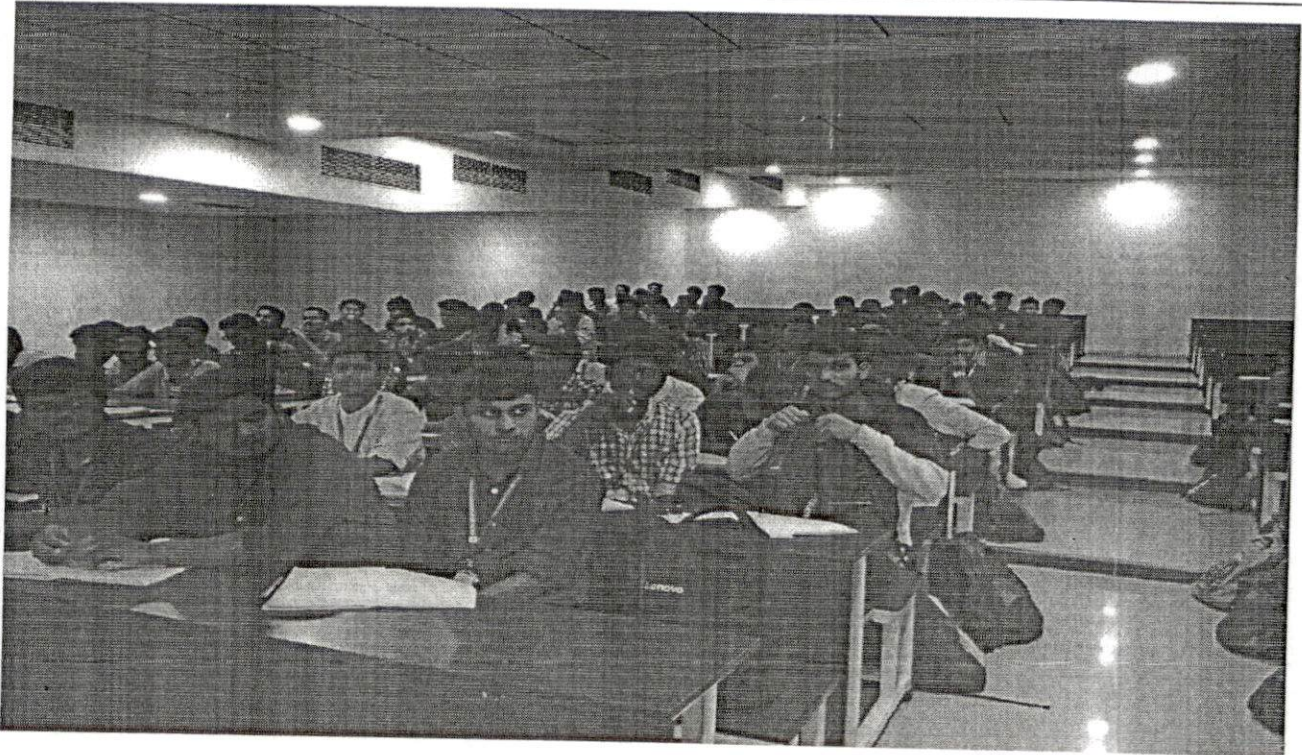
- (1) Deans
- (2) IQAC Coordinator
- (2) All HODS
- (3) Administrative Officer
- (4) Accounts Officer
- (5) Concerned Students members
- (6) Concerned Faculty Members


PRINCIPAL
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

Report on Trace of IP Address Hacking Techniques on 11th March 2018

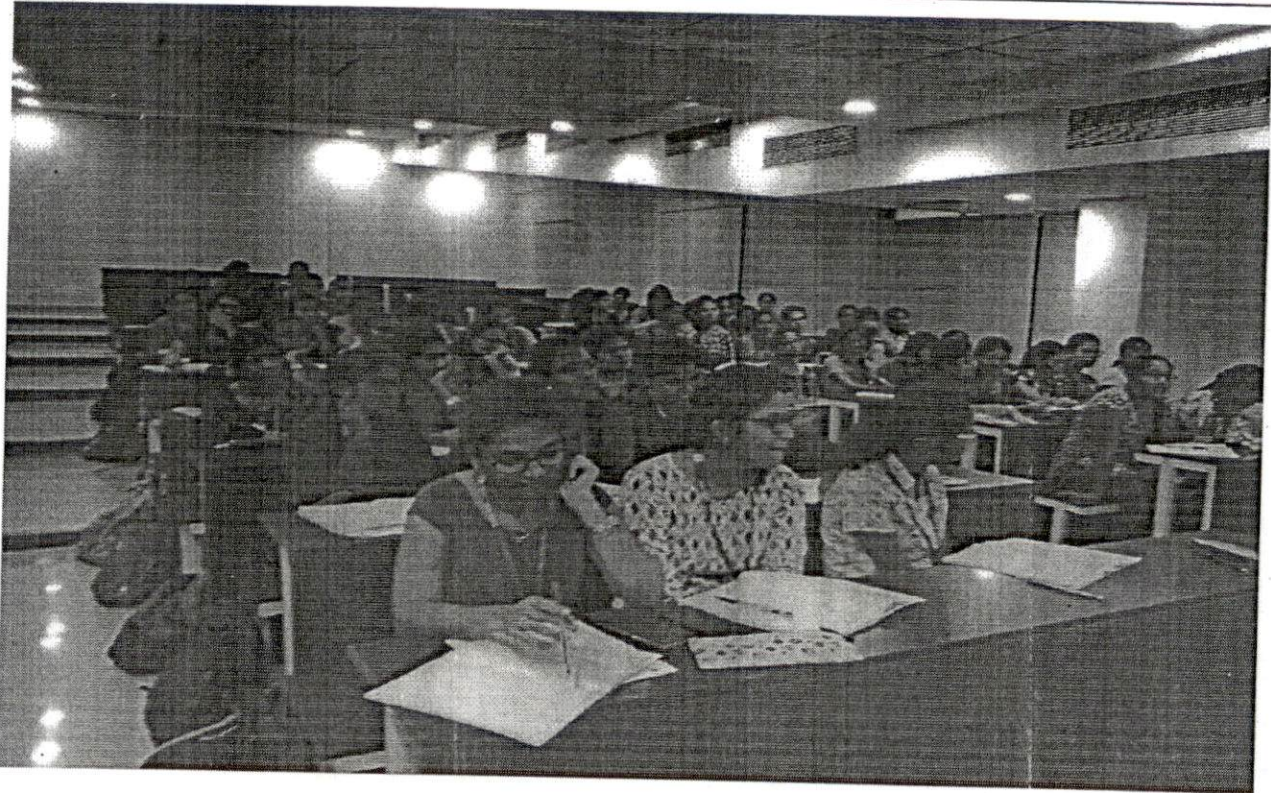
Here are a few basic guidelines to help you trace computer hackers. Keep in mind that many sophisticated computer hackers will be more cautious about tracing their steps. Many hackers use proxies or dark web sites such as Tor. They can still be traced, but doing so may be a bit more difficult. These guidelines may help you identify some hackers, but you may need the assistance of an expert to catch many in real life.


PRINCIPAL
CMR COLLEGE OF ENGG & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.



```
C:\Windows\system32>ping facebook.com -t

Pinging facebook.com [157.240.16.35] with 32 bytes of data:
Reply from 157.240.16.35: bytes=32 time=27ms TTL=128
Reply from 157.240.16.35: bytes=32 time=27ms TTL=128
Reply from 157.240.16.35: bytes=32 time=27ms TTL=128
Reply from 157.240.16.35: bytes=32 time=35ms TTL=128
Reply from 157.240.16.35: bytes=32 time=26ms TTL=128
Reply from 157.240.16.35: bytes=32 time=52ms TTL=128
Reply from 157.240.16.35: bytes=32 time=26ms TTL=128
Reply from 157.240.16.35: bytes=32 time=27ms TTL=128
Reply from 157.240.16.35: bytes=32 time=27ms TTL=128
```

You will need to identify the IP address of the intruder. There are a variety of Linux commands and tools that can tell you what the IP address is of any computer that is trying to make a connection. You can find the IP address of anyone trying to hack your own website on your hosting logs, Google Analytics or another analytics tool. You can try to use a tool such as NetStat to identify the IP addresses of anyone trying to connect to your computer.

What to do with the information: Once you have an IP address you can find out where the connection is coming from. Keep in mind that these simpler tools won't be able to tell you exactly where they are, but can give you a reasonable idea what city they are in and what hosting provider they are using.

You can use the traceart command to find the hostname of the IP address that the hacker is using to access your machine. You can also put the IP address on the trace-route tool on the Princeton website. Another alternative is to use the GEOIPTool to get a rough idea where the hacker is located.

You won't be able to track the hacker's exact identity when you try these techniques. However, there are a couple of ways that you can use it:

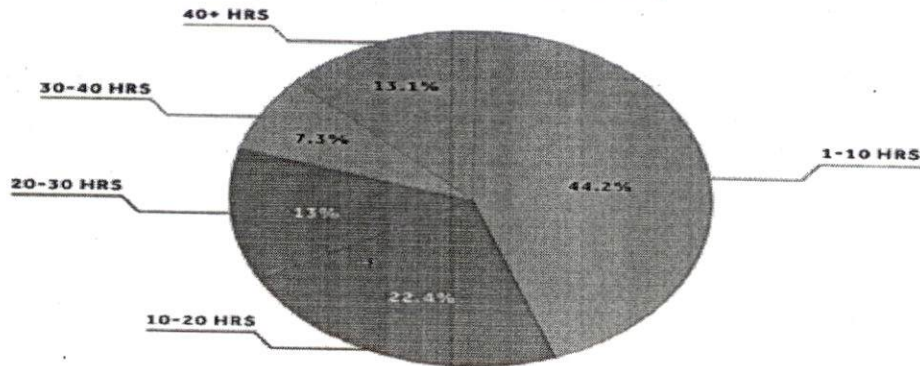
- You can turn them over to the authorities.
- You can report them to their hosting provider after learning their identity.

I would suggest the former in most situations. You will know which country's jurisdiction to contact to report the crime.

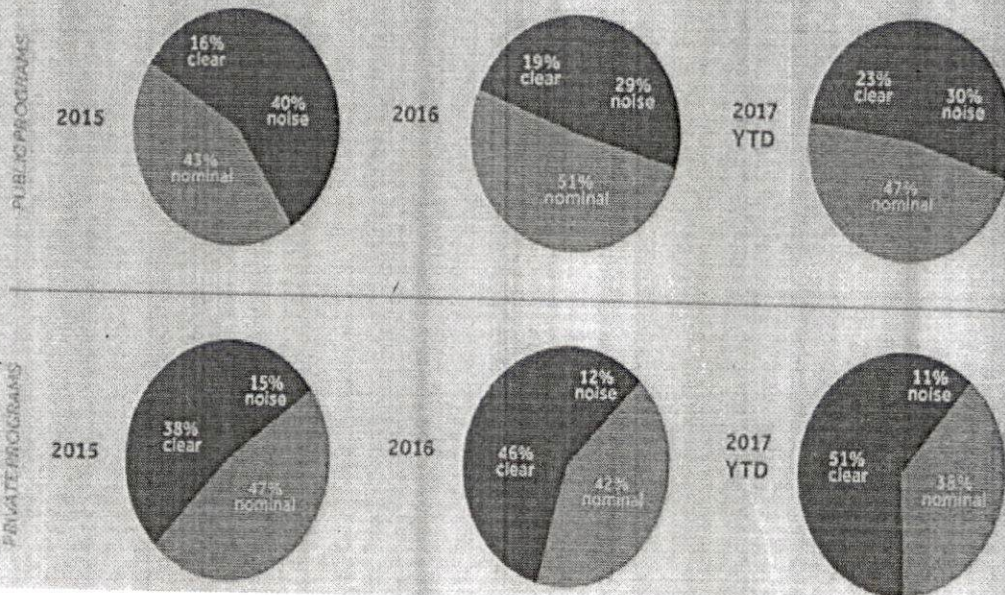
HOURS PER WEEK SPENT HACKING

Over 66% of hackers spend 20 hours or less per week hacking, with 44% spending 10 hours or less per week. More than 20% of hackers spend over 30 hours per week.

On Average, Approximately How Many Hours Per Week Do You Spend Hacking?



HackerOne has the highest published Signal-To-Noise Ratio (SNR) in the industry. To read more, see "Improving Signal Over 10KBugs"



PRINCIPAL
CMR COLLEGE OF ENGG & TECH
 Kandlakoya (V), Medchal Road,
 Hyderabad-501401.

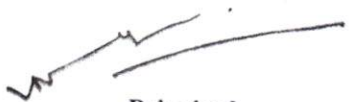
Date: 18/04/2018

CIRCULAR

All the members of Cyber Security Club of the college are hereby informed that, the Cyber Security Club committee meeting is scheduled on 21.04.2018 & the Venue is CSE Seminar hall at 1:00 pm. All are requested to be present on time.

The Agenda of the meeting is:

- Understanding the Behavior of Threat Actors
- Different programs for next academic year
- Security for the future
- Discuss Security Attacks and Preventions
- How to avoid Cyber Security in network




Principal

Copy Submitted to: (1) The Secretary Garu – For your kind information Pl.

Copy to:

1. IQAC Coordinator
2. Controller of Examinations
3. All HODS
4. Administrative Officer
5. Accounts Officer
6. Concerned Faculty



PRINCIPAL
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

Academic Year: 2017-18

CYBER SECURITY CLUB COMMITTEE

MINUTES OF MEETING

Date: 21st April 2018

Time: 2:00-3:30 PM

Venue: HOD Cabin, CSE Dept.

Chaired By: Dr.V.A Narayan, Principal, CMR College of Engineering & Technology

Members present:

1. Chairman: Dr.V.A Narayan, Principal of CMRCET
2. Convener : Mr. Siva Skandha Sanagala
3. Coordinator: Mr .B. Tulasi Dasu
4. One faculty from Each Department
5. One Students member from Each Department

The chairman Dr.V.A Narayan welcomed all the committee members.


Agenda: End of the Academic year summary

Minutes of Meeting:

A meeting was conducted by the Cyber Security Club Committee to review the events conducted in the Academic Year 2017 – 2018 and to discuss the various Programs to be conducted for the Academic Year 2018 – 2019.

- The chairman, Dr.V.A Narayan welcomed all the members.
- All the three (3) events conducted for the Academic Year 2017-2018 were discussed.
- The additional events that were conducted if any and missed out were asked for.
- The Programme that were part of the agenda but were not conducted were also discussed and the reasons for not being conducted were discussed at length.
- The events that were planned for the next academic year were also discussed.
- Inputs were sought about the other events that can be included as part of the club.

Resolution 01: The Cyber Security Club committee members appreciated one another for the successful completion of the events for the academic year on the agenda and were braced up with the list of events for the next academic year.


PRINCIPAL
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

Resolution 01: The Cyber Security Club committee members appreciated one another for the successful completion of the events for the academic year on the agenda and were braced up with the list of events for the next academic year.


The meeting concluded with the Chairman thanking the members for their valuable suggestions.

Summary of Programmes Conducted during A.Y 2017-18 under "CYBER SECURITY".

Sno	Name of the Event	Date	Venue	Conducted / Not Conducted
1	Creak of IP Address	23/09/2017	Android Lab 113	Conducted
2	Hacking in browser	02/12/2017	Android Lab 113	Conducted
3	Trace of IP Address	11/03/2018	Android Lab 113	Conducted

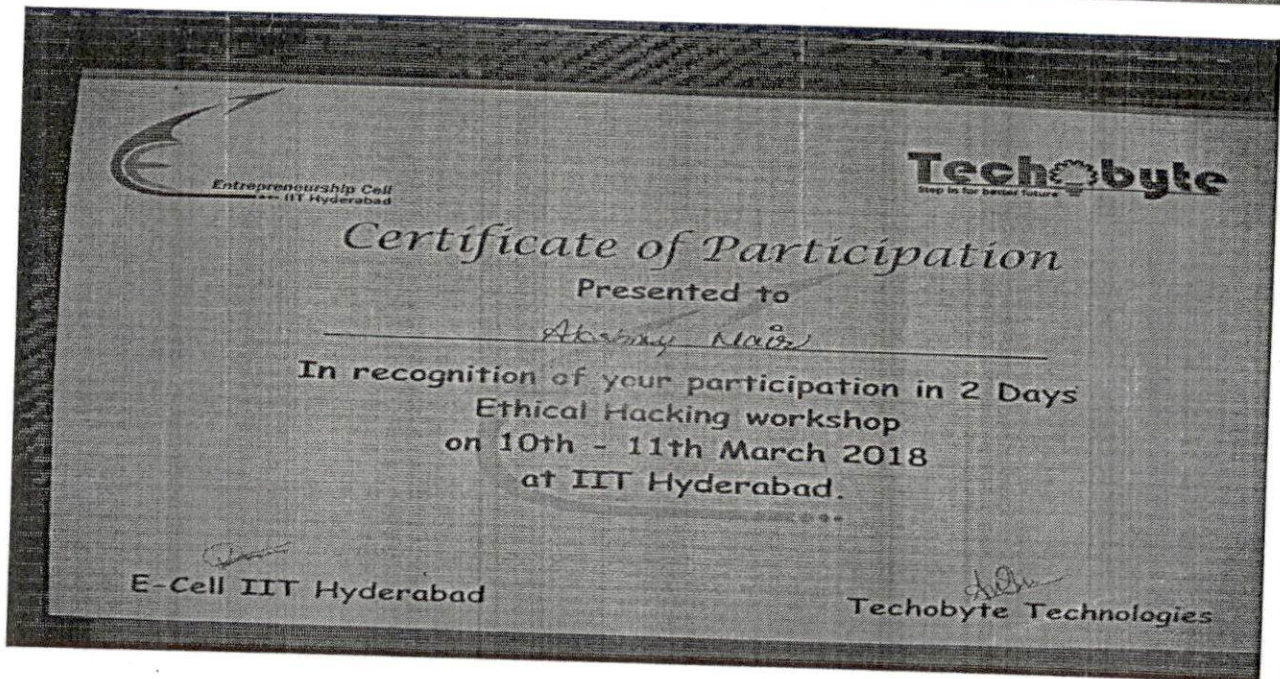



Convener



PRINCIPAL
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

Certificates in various workshop:

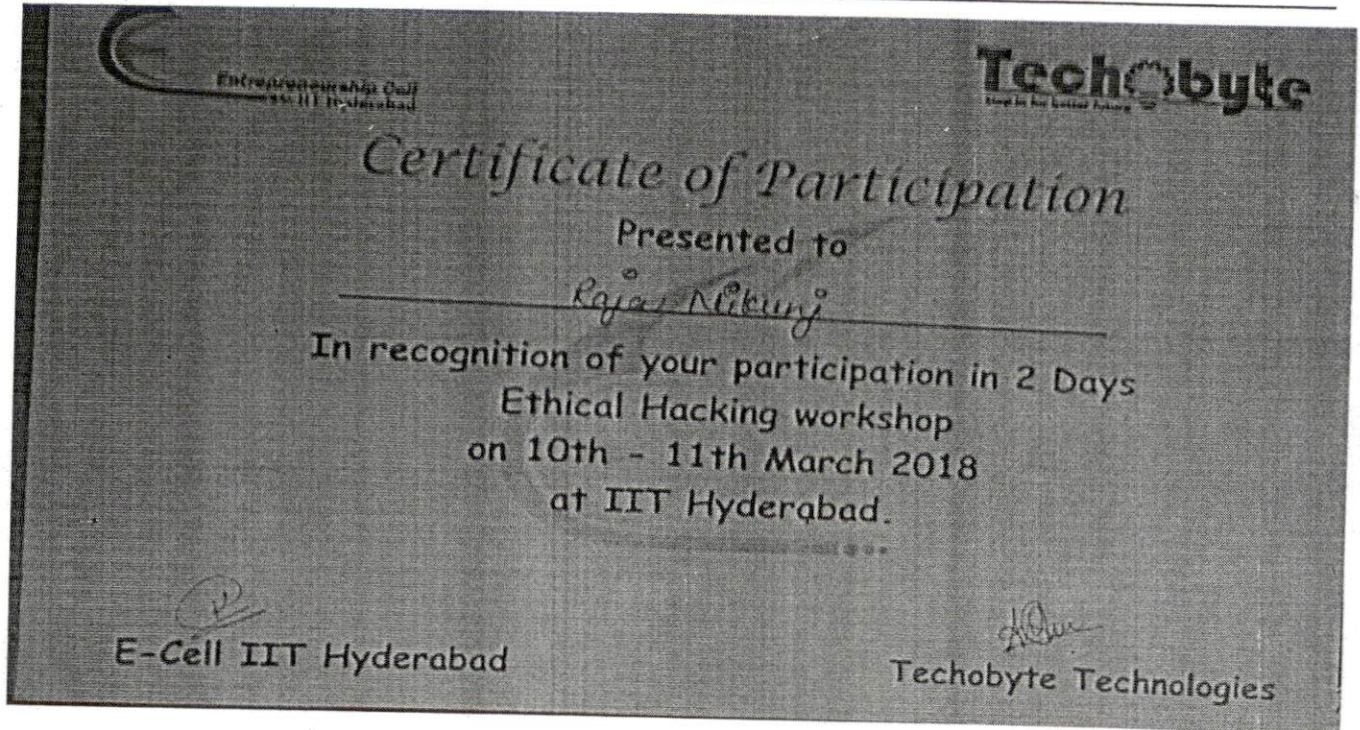



PRINCIPAL
CMR COLLEGE OF ENGG & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.



CMR COLLEGE OF ENGINEERING & TECHNOLOGY

Kandlakoya (V), Medchal Road, Hyderabad -501401.



[Signature]
PRINCIPAL
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.

21.04.2018

TO

The IQAC coordinator
CMR College of Engineering & Technology
Kandlakoya
Medchal.

Sir,

Sub: **ANNUAL REPORT** of the **CYBER SECURITY CLUB** for the year 2017-18. Reg.

The **CYBER SECURITY CLUB** in the year 2017-18 has conducted the following programs according to the original schedule decided in the first **CSC** meeting held on 21st of April 2018

S.No	Program	Date
1	Creak of IP Address	23/09/2017
2	Hacking in browser	02/12/2017
3	Trace of IP Address	11/03/2018

The **outcome** of all these programs is that all the students, faculty. The Cyber Security Club committee members appreciated one another for the successful completion of the events for the academic year on the agenda and were braced up with the list of events for the next academic year.

S Siva Skanda



Convener

Cyber Security Club

PRINCIPAL
CMR COLLEGE OF ENGG. & TECH.
Kandlakoya (V), Medchal Road,
Hyderabad-501401.