



Mangalmai Institute of Management Technology
Greater Noida (U.P.)



MANGALMAY
INSTITUTE OF MANAGEMENT TECHNOLOGY



CERTIFICATION PROGRAMME

On

Fundamental Concepts of Cyber Security

From

21-March-2023 to 09-May-2023

Convener: Mr. Abhay N Tripathi, Associate Professor

For BCA 6th Semester

Resource Person

Ms. Nisha Pandey

Assistant Professor, MIET



Fundamental Concepts of Cyber Security

Duration: 30 Hours

Module: 1

Networking Concepts Overview- Basics of Communication Systems, transmission Media, ISO/OSI and TCP/IP Protocol Stacks, Local Area Networks, Wide Area Networks, Internetworking, Packet Formats, Wireless Networks, The Internet

Module: 2

Application Security- Database Security, E-mail Security, Internet Security, Firewall, VPN's, Access Control, Backups, Archival Storage of Data,
Security Threats- Hacking and attacking, DOS attack, Card and ATM security, Password management, Risk Management.

Module: 3

Security Issues- Hardware and software, Physical Security of IT Assets, CCTV, Access Control, Security Policy and Its development, www security policy, Email standards and security policy.

Module: 4

Security standards & Cyber Laws- ISO, Early warning & response, CERT, I.T. Act. 2000, Copyright Act, Patent Law, IPR, Cyber Law in India

Reference Books:

1. Cyber Security by Dr. O.N. Pandey, Katson Publication
2. Fundamentals of Cyber Security by Mayank Bhushan, BPB Publication
3. Introduction To Cyber Security - Guide To The World Of Cyber Security by Anand Shinde, Notion Press



Schedule

Duration: 30 hours

Session	Content	Time	Date
1.	Basics of Communication Systems, transmission Media	3:00-5:00 PM	21-03-2023
2.	ISO/OSI and TCP/IP Protocol Stacks	3:00-5:00 PM	22-03-2023
3.	Local Area Networks, Wide Area Networks	3:00-5:00 PM	28-03-2023
4.	Internetworking, Packet Formats	3:00-5:00 PM	29-03-2023
5.	Wireless Networks, The Internet, VPN's	3:00-5:00 PM	04-04-2023
6.	Database Security, E-mail Security, Internet Security, Firewall	3:00-5:00 PM	05-04-2023
7.	Access Control, Backups, Archival Storage of Data	3:00-5:00 PM	11-04-2023
8.	Hacking and attacking, DOS attack	3:00-5:00 PM	12-04-2023
9.	Card and ATM security, Password management, Risk Management	3:00-5:00 PM	18-04-2023
10.	Hardware and software, Physical Security of IT Assets	3:00-5:00 PM	19-04-2023
11.	CCTV, Access Control, Security Policy and Its development	3:00-5:00 PM	25-04-2023
12.	www security policy, Email standards and security policy	3:00-5:00 PM	26-04-2023
13.	ISO, Early warning & response.	3:00-5:00 PM	02-05-2023
14.	CERT, I.T. Act. 2000, Copyright Act	3:00-5:00 PM	03-05-2023
15.	Patent Law, IPR, Cyber Law in India	3:00-5:00 PM	09-05-2023



Report	
Name of Activity	Fundamental Concepts of Cyber Security
Date	21-March-2023 to 09-May-2023
Venue	BCA Classroom
Organized by	Computer Application Department
Resource Person	Ms. Nisha Pandey, Assistant Professor, MIET
Beneficiary	BCA 6th Semester (40 students)
Coordinator	Mr. Abhay N Tripathi, Associate Professor, MIMT
Objective	This course on Cyber Security: <ul style="list-style-type: none">• To secure the information stored and conveyed, this is an invaluable resource of any organization• To update the knowledge of students in network security issues.
Content	<p>With the initiative of IQAC, Mangalmai Institute of Management and Technology organized add on certification course on “Cyber Security”.</p> <p>Day1: The session started with Basics of Communication Systems, transmission Media.</p> <p>Day 2: In this session, the resource person discussed about ISO/OSI and TCP/IP Protocol Stacks with their header formats.</p> <p>Day 3: In this session, the student learned about the various types of Networks and their standards.</p> <p>Day 4: This session was focused on Internetworking, Framing of the message and Packet Formats.</p> <p>Day 5: In this session, the student learned about Wireless Networks, The Internet, Virtual Private Networks.</p> <p>Day 6: In this session, the resource person discussed about various types of security: Database Security, E-mail Security, Internet Security, Firewall</p> <p>Day 7: This session was focused on Access Control, Backups, Archival Storage of Data</p> <p>Day 8: The session focused on Hacking and attacking, Hacking methods, DOS attack.</p> <p>Day9: In this session, the student learned about the various types of Card and ATM security, Password management, Risk Management.</p> <p>Day 10: In this session, the resource person discusses about Hardware and software, Physical Security of IT Assets</p> <p>Day 11: In this session, CCTV, Access Control, Security Policy and Its development was discussed.</p> <p>Day 12: In this session, the resource person discusses about www security policy, Email standards and security policy</p> <p>Day 13: In this session, ISO, Early warning & response was learnt.</p> <p>Day 14: In this session, the resource person discussed about CERT, I.T. Act. 2000, Copyright Act.</p> <p>Day 15: This session was on Brief about Patent Law, IPR, Cyber Law in India.</p>
Outcome of Activity	On completion of the programme : <ul style="list-style-type: none">• The students gain the most comprehensive knowledge and skills in the Network Security providing an opportunity to equip the Network System Administrators & Information.• To understand the security concerns, vulnerabilities, attacks and to plan and implement the desired e-Security solutions.



Resource Person Profile

Name: Ms. Nisha Pandey, Asst. Professor, MIET

Core Skills: C Programming, Automata Theory, Computer Networks, Operating Systems.

Qualification: B.Tech, M.Tech

Experience: 09 years

Research Area: Computer Networks, IoT.



Figure 1 Ms. Nisha Pandey during her session



Figure 2 Ms. Nisha Pandey during her session



Mangalmay Institute of Management Technology
Greater Noida (U.P.)



Certificate Template:

	<p>MANGALMAY INSTITUTE OF MANAGEMENT TECHNOLOGY Gr. NOIDA</p>	
<p>CERTIFICATE OF COURSE COMPLETION</p>		
<p>This is to certified the AMAN KUMAR student of BCA (Batch: 2020-23) has successfully completed 30 Hours course on “Fundamental Concepts of Cyber Security” from 21-March-2023 to 9-May-2023</p>		
<p>PRINCIPAL Mangalmay Institute of Management & Technology</p>	<p>CONVENER Mangalmay Institute of Management Technology</p>	



Mangalmai Institute of Management Technology
Greater Noida (U.P.)





Course: BCA

ADD-ON COURSE QUIZ
Course Name: Cyber Security

Time: 30 Min

Date:

Roll No:

Name: MD Danish

Year/Sem: III/VI

Invigilator's Sign:

Note: All questions are compulsory. Each question will carry '1' mark and there is no 'Negative Marking'

Q1. What does the term "phishing" refer to in cybersecurity?

- A) A method of securing network traffic
- B) An attempt to steal sensitive information by impersonating a trustworthy entity
- C) A type of malware that spreads through email attachments
- D) A technique used to encrypt data during transmission

1

Q2. Which of the following is NOT considered a strong password?

- A) Password123
- B) \$\$w0rd!
- C) CorrectHorseBatteryStaple
- D) Tr0ub4dor&3

1

Q3. What is the primary purpose of a firewall in network security?

- A) To prevent unauthorized access to a network
- B) To encrypt data transmissions
- C) To detect and remove malware from a network
- D) To provide secure remote access to a network

1

Q4. Which of the following is an example of two-factor authentication?

- A) Using a password and security questions to log in
- B) Using a fingerprint scan and a password to log in
- C) Logging in with a username and password
- D) Answering a CAPTCHA before logging in

1

Q5. What is the main goal of ransomware attacks?

- A) To steal sensitive information
- B) To disrupt the operation of a system or network
- C) To gain unauthorized access to a network
- D) To extort money from victims by encrypting their data

1

Q6. Which of the following is a common type of social engineering attack?

- A) SQL injection
- B) DDoS attack
- C) Phishing
- D) Cross-site scripting (XSS)

1

Q7. What is the purpose of encryption in cybersecurity?

- A) To hide the identity of the sender
- B) To prevent unauthorized access to data by encoding it
- C) To speed up data transmission over a network
- D) To detect and remove malware from a system

1

Q8. What does the acronym "DDoS" stand for in the context of cybersecurity?

- A) Digital Data Storage
- B) Distributed Denial of Service
- C) Data Destruction and Security
- D) Direct Data Spoofing

1

Q9. What is a common method used to protect data transmitted over public networks?

- A) Network segmentation
- B) End-to-end encryption

1

- C) Intrusion detection systems
- D) Firewalls

Q10. What is the purpose of penetration testing in cybersecurity?

- A) To test the speed of data transmission
- B) To identify and exploit vulnerabilities in a system
- C) To encrypt sensitive data
- D) To monitor network traffic for suspicious activity

1

Q11. What is the role of a Security Information and Event Management (SIEM) system?

- A) To prevent malware infections
- B) To monitor network traffic for suspicious activity
- C) To encrypt sensitive data
- D) To manage user authentication and access control

1

Q12. What does the term "zero-day exploit" refer to in cybersecurity?

- A) An attack that targets zero-day-old systems
- B) An exploit that occurs zero days after a vulnerability is discovered
- C) An attack that targets vulnerabilities that are unknown to the software vendor
- D) A software vulnerability that has been exploited for zero days

1

Q13. Which of the following is a best practice for securing a wireless network?

- A) Disabling encryption
- B) Broadcasting the SSID
- C) Using a strong password
- D) Keeping the network open

1

Q14. What is the purpose of antivirus software?

- A) To encrypt data
- B) To prevent unauthorized access to a network
- C) To detect and remove malware from a system
- D) To monitor network traffic for suspicious activity

1

Q15. What is the main purpose of a Virtual Private Network (VPN)?

- A) To provide secure remote access to a network
- B) To encrypt data transmissions
- C) To prevent unauthorized access to a network
- D) To detect and remove malware from a system

1

----- For Departmental use only -----

Max. Marks: 15

Marks Obtained: 15

Name of Evaluator:

Sign.

Nishi Pandey

Nishi Pandey



Course: BCA

ADD-ON COURSE QUIZ
Course Name: Cyber Security

Time: 30 Min

Date:

Roll No:

Name: Bardani

Year/Sem: III/VI

Invigilator's Sign:

Note: All questions are compulsory. Each question will carry '1' mark and there is no 'Negative Marking'

Q1. What does the term "phishing" refer to in cybersecurity?

- A) A method of securing network traffic
- B) An attempt to steal sensitive information by impersonating a trustworthy entity
- C) A type of malware that spreads through email attachments
- D) A technique used to encrypt data during transmission

Q2. Which of the following is NOT considered a strong password?

- A) Password123
- B) SSw0rd!
- C) CorrectHorseBatteryStaple
- D) Tr0ub4dor&3

Q3. What is the primary purpose of a firewall in network security?

- A) To prevent unauthorized access to a network
- B) To encrypt data transmissions
- C) To detect and remove malware from a network
- D) To provide secure remote access to a network

Q4. Which of the following is an example of two-factor authentication?

- A) Using a password and security questions to log in
- B) Using a fingerprint scan and a password to log in
- C) Logging in with a username and password
- D) Answering a CAPTCHA before logging in

Q5. What is the main goal of ransomware attacks?

- A) To steal sensitive information
- B) To disrupt the operation of a system or network
- C) To gain unauthorized access to a network
- D) To extort money from victims by encrypting their data

Q6. Which of the following is a common type of social engineering attack?

- A) SQL injection
- B) DDoS attack
- C) Phishing
- D) Cross-site scripting (XSS)

Q7. What is the purpose of encryption in cybersecurity?

- A) To hide the identity of the sender
- B) To prevent unauthorized access to data by encoding it
- C) To speed up data transmission over a network
- D) To detect and remove malware from a system

Q8. What does the acronym "DDoS" stand for in the context of cybersecurity?

- A) Digital Data Storage
- B) Distributed Denial of Service
- C) Data Destruction and Security
- D) Direct Data Spoofing

Q9. What is a common method used to protect data transmitted over public networks?

- A) Network segmentation
- B) End-to-end encryption

- C) Intrusion detection systems
- D) Firewalls

Q10. What is the purpose of penetration testing in cybersecurity?

- A) To test the speed of data transmission
- B) To identify and exploit vulnerabilities in a system
- C) To encrypt sensitive data
- D) To monitor network traffic for suspicious activity

1

Q11. What is the role of a Security Information and Event Management (SIEM) system?

- A) To prevent malware infections
- B) To monitor network traffic for suspicious activity
- C) To encrypt sensitive data
- D) To manage user authentication and access control

1

Q12. What does the term "zero-day exploit" refer to in cybersecurity?

- A) An attack that targets zero-day-old systems
- B) An exploit that occurs zero days after a vulnerability is discovered
- C) An attack that targets vulnerabilities that are unknown to the software vendor
- D) A software vulnerability that has been exploited for zero days

1

Q13. Which of the following is a best practice for securing a wireless network?

- A) Disabling encryption
- B) Broadcasting the SSID
- C) Using a strong password
- D) Keeping the network open

1

Q14. What is the purpose of antivirus software?

- A) To encrypt data
- B) To prevent unauthorized access to a network
- C) To detect and remove malware from a system
- D) To monitor network traffic for suspicious activity

1

Q15. What is the main purpose of a Virtual Private Network (VPN)?

- A) To provide secure remote access to a network
- B) To encrypt data transmissions
- C) To prevent unauthorized access to a network
- D) To detect and remove malware from a system

1

----- For Departmental use only -----

Max. Marks: 15

Marks Obtained: 13

Name of Evaluator:

Miss Pandey

Sign.

Pandey



Course: BCA


ADD-ON COURSE QUIZ
Course Name: Cyber Security

Time: 30 Min
Date:

Roll No:

Name: Varun Kumar Yadav

Year/Sem: III/VI

Invigilator's Sign: 

Note: All questions are compulsory. Each question will carry '1' mark and there is no 'Negative Marking'

Q1. What does the term "phishing" refer to in cybersecurity?

- A) A method of securing network traffic
- B) An attempt to steal sensitive information by impersonating a trustworthy entity
- C) A type of malware that spreads through email attachments
- D) A technique used to encrypt data during transmission

Q2. Which of the following is NOT considered a strong password?

- A) Password123
- B) \$\$w0rd!
- C) CorrectHorseBatteryStaple
- D) Tr0ub4dor&3

Q3. What is the primary purpose of a firewall in network security?

- A) To prevent unauthorized access to a network
- B) To encrypt data transmissions
- C) To detect and remove malware from a network
- D) To provide secure remote access to a network

Q4. Which of the following is an example of two-factor authentication?

- A) Using a password and security questions to log in
- B) Using a fingerprint scan and a password to log in
- C) Logging in with a username and password
- D) Answering a CAPTCHA before logging in

Q5. What is the main goal of ransomware attacks?

- A) To steal sensitive information
- B) To disrupt the operation of a system or network
- C) To gain unauthorized access to a network
- D) To extort money from victims by encrypting their data

Q6. Which of the following is a common type of social engineering attack?

- A) SQL injection
- B) DDoS attack
- C) Phishing
- D) Cross-site scripting (XSS)

Q7. What is the purpose of encryption in cybersecurity?

- A) To hide the identity of the sender
- B) To prevent unauthorized access to data by encoding it
- C) To speed up data transmission over a network
- D) To detect and remove malware from a system

Q8. What does the acronym "DDoS" stand for in the context of cybersecurity?

- A) Digital Data Storage
- B) Distributed Denial of Service
- C) Data Destruction and Security
- D) Direct Data Spoofing

Q9. What is a common method used to protect data transmitted over public networks?

- A) Network segmentation
- B) End-to-end encryption

- C) Intrusion detection systems
- D) Firewalls

Q10. What is the purpose of penetration testing in cybersecurity?

- A) To test the speed of data transmission
- B) To identify and exploit vulnerabilities in a system
- C) To encrypt sensitive data
- D) To monitor network traffic for suspicious activity

1

Q11. What is the role of a Security Information and Event Management (SIEM) system?

- A) To prevent malware infections
- B) To monitor network traffic for suspicious activity
- C) To encrypt sensitive data
- D) To manage user authentication and access control

1

Q12. What does the term "zero-day exploit" refer to in cybersecurity?

- A) An attack that targets zero-day-old systems
- B) An exploit that occurs zero days after a vulnerability is discovered
- C) An attack that targets vulnerabilities that are unknown to the software vendor
- D) A software vulnerability that has been exploited for zero days

1

Q13. Which of the following is a best practice for securing a wireless network?

- A) Disabling encryption
- B) Broadcasting the SSID
- C) Using a strong password
- D) Keeping the network open

1

Q14. What is the purpose of antivirus software?

- A) To encrypt data
- B) To prevent unauthorized access to a network
- C) To detect and remove malware from a system
- D) To monitor network traffic for suspicious activity

1

Q15. What is the main purpose of a Virtual Private Network (VPN)?

- A) To provide secure remote access to a network
- B) To encrypt data transmissions
- C) To prevent unauthorized access to a network
- D) To detect and remove malware from a system

1

----- For Departmental use only -----

Max. Marks: 15

Marks Obtained:

13

Name of Evaluator:

Nisha Pandey

Sign.

Pandey



Course: BCA

ADD-ON COURSE QUIZ
Course Name: Cyber Security

Time: 30 Min

Date:

Roll No:

Name: Vikash Chaudhary

Year/Sem: III/VI

Invigilator's Sign:

Note: All questions are compulsory. Each question will carry '1' mark and there is no 'Negative Marking'

Q1. What does the term "phishing" refer to in cybersecurity?

- A) A method of securing network traffic
- B) An attempt to steal sensitive information by impersonating a trustworthy entity
- C) A type of malware that spreads through email attachments
- D) A technique used to encrypt data during transmission

Q2. Which of the following is NOT considered a strong password?

- A) Password123
- B) \$Sw0rd!
- C) CorrectHorseBatteryStaple
- D) Tr0ub4dor&3

Q3. What is the primary purpose of a firewall in network security?

- A) To prevent unauthorized access to a network
- B) To encrypt data transmissions
- C) To detect and remove malware from a network
- D) To provide secure remote access to a network

Q4. Which of the following is an example of two-factor authentication?

- A) Using a password and security questions to log in
- B) Using a fingerprint scan and a password to log in
- C) Logging in with a username and password
- D) Answering a CAPTCHA before logging in

Q5. What is the main goal of ransomware attacks?

- A) To steal sensitive information
- B) To disrupt the operation of a system or network
- C) To gain unauthorized access to a network
- D) To extort money from victims by encrypting their data

Q6. Which of the following is a common type of social engineering attack?

- A) SQL injection
- B) DDoS attack
- C) Phishing
- D) Cross-site scripting (XSS)

Q7. What is the purpose of encryption in cybersecurity?

- A) To hide the identity of the sender
- B) To prevent unauthorized access to data by encoding it
- C) To speed up data transmission over a network
- D) To detect and remove malware from a system

Q8. What does the acronym "DDoS" stand for in the context of cybersecurity?

- A) Digital Data Storage
- B) Distributed Denial of Service
- C) Data Destruction and Security
- D) Direct Data Spoofing

Q9. What is a common method used to protect data transmitted over public networks?

- A) Network segmentation
- B) End-to-end encryption

- C) Intrusion detection systems
- D) Firewalls

Q10. What is the purpose of penetration testing in cybersecurity?

- A) To test the speed of data transmission
- B) To identify and exploit vulnerabilities in a system
- C) To encrypt sensitive data
- D) To monitor network traffic for suspicious activity

0/

Q11. What is the role of a Security Information and Event Management (SIEM) system?

- A) To prevent malware infections
- B) To monitor network traffic for suspicious activity
- C) To encrypt sensitive data
- D) To manage user authentication and access control

0/

Q12. What does the term "zero-day exploit" refer to in cybersecurity?

- A) An attack that targets zero-day-old systems
- B) An exploit that occurs zero days after a vulnerability is discovered
- C) An attack that targets vulnerabilities that are unknown to the software vendor
- D) A software vulnerability that has been exploited for zero days

1

Q13. Which of the following is a best practice for securing a wireless network?

- A) Disabling encryption
- B) Broadcasting the SSID
- C) Using a strong password
- D) Keeping the network open

1

Q14. What is the purpose of antivirus software?

- A) To encrypt data
- B) To prevent unauthorized access to a network
- C) To detect and remove malware from a system
- D) To monitor network traffic for suspicious activity

0/

Q15. What is the main purpose of a Virtual Private Network (VPN)?

- A) To provide secure remote access to a network
- B) To encrypt data transmissions
- C) To prevent unauthorized access to a network
- D) To detect and remove malware from a system

1

----- For Departmental use only -----

Max. Marks: 15

Marks Obtained:

12

Name of Evaluator:

Nishu Pandey

Sign.

Nishu Pandey