Department of CSE

Details of Lesson Plan

S.No.	Particulars	Details
1.	Course Name	Foundations of Cyber Security
2.	Course Code	COM-303
3.	Academic Year	2024-25
4.	Semester	3rd
5.	Number of Lesson plans	42
6.	Faculty Assigned	Ms. Annu Sonania

Ms. Annu Sonania

Faculty Signature

Lesson Plan No. 1.1	Course Name: Foundations of Cyber Security Topic: Cyber Security Introduction: Computer Security	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the concept of computer security. b. Identify the importance of securing computer systems. c. Recognize the basic principles of confidentiality, integrity, and availability. d. Discuss the impact of computer security breaches on individuals and organizations.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you think are the key components of computer security? - Can you recall any recent news about a computer security breach? 2. Introduction - Discuss recent high-profile security breaches. **Development** (30 minutes) 3. Define computer security and its goals (confidentiality, integrity, and availability). 4. Discuss types of security measures: physical, technical, and administrative. 5. Show video to illustrate the importance of computer security. **Exercise** (5 minutes): 6. Discuss a recent security breach and identify what security measures could have prevented it. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 1 Spend 5 minutes to wrap up and consolidate the learnings

Evaluation	1. Reflective Questions - What are the key principles of computer security? - Why is it important to secure computer systems? - Who is affected by computer security breaches? 2. Nearpod Quiz on Cyber Security Introduction 3. Homework: - Research a recent security breach and prepare a short report on it. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 1.2	Course Name: Foundations of Cyber Security Topic: Threats, Harm, and Vulnerabilities	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Identify various types of security threats. b. Understand the concept of vulnerabilities and their impact. c. Recognize common harms caused by security threats. d. Discuss strategies to mitigate vulnerabilities.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What kinds of threats do you think your personal computer faces? - How do you think vulnerabilities in software can affect its users? 2. Introduction - Discuss common threats students have heard of. **Development** (30 minutes) 3. Explain different types of threats: viruses, worms, Trojans, ransomware. 4. Define vulnerabilities and how they can be exploited. 5. Show video to explain these concepts in detail. **Exercise** (5 minutes): 6. Case study: Identify threats and vulnerabilities in a given scenario. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 1 - https://www.youtube.com/watch?v=KQYV4uCzPqQ Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the different types of security threats? - Why are vulnerabilities a significant concern in cybersecurity? - How can we mitigate vulnerabilities? 2. Nearpod Quiz on Threats, Harm, and Vulnerabilities 3. Homework: - Identify and describe three recent cyber threats. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 1.3	Course Name: Foundations of Cyber Security Topic: Controls and Authentication	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Identify various types of security threats. b. Understand the concept of vulnerabilities and their impact. c. Recognize common harms caused by security threats. d. Discuss strategies to mitigate vulnerabilities.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What methods do you use to secure your online accounts? - Have you ever used two-factor authentication? 2. Introduction - Discuss the importance of security controls. **Development** (30 minutes) 3. Define and differentiate preventive, detective, and corrective controls. 4. Explain authentication methods: passwords, biometrics, two-factor authentication. 5. Show video to illustrate different authentication methods. **Exercise** (5 minutes): 6. Discuss the best authentication methods for different scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 2 - https://www.youtube.com/watch?v=Q1baWFnIxYY Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the different types of security controls? - Why is authentication important in cybersecurity? - Which authentication method do you think is the most secure and why? 2. Nearpod Quiz on Controls and Authentication 3. Homework: - Describe a scenario where two-factor authentication is crucial. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 1.4	Course Name: Foundations of Cyber Security Topic: Access Control	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the concept of access control. b. Learn different access control models. c. Discuss the importance of implementing effective access control. d. Evaluate scenarios to determine the best access control model.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - How do you control access to your personal information? - Why do you think access control is important in a business environment? 2. Introduction - Ask students what they know about access control. **Development** (30 minutes) 3. Define access control and its importance. 4. Explain different models: discretionary, mandatory, role-based, and attribute-based access control. 5. Show video to illustrate access control models. **Exercise** (5 minutes): 6. Discuss the best access control model for a given scenario. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 2 - https://www.youtube.com/watch?v=QtlyuGRrMGs Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the different access control models? - Why is access control important in cybersecurity? - Which access control model do you think is the most effective and why? 2. Nearpod Quiz on Access Control 3. Homework: - Research and write about the access control model used by a well-known company. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 1.5	Course Name: Foundations of Cyber Security Topic: Cryptography Introduction and Problems Addressed by Encryption	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the basics of cryptography. b. Identify the problems addressed by encryption. c. Discuss the role of encryption in ensuring data security. d. Evaluate the effectiveness of encryption in different scenarios.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - How do you think encryption protects your data online? - Can you name any encryption methods? 2. Introduction - Ask about students' understanding of cryptography. **Development** (30 minutes) 3. Define cryptography and its objectives. 4. Explain how encryption addresses confidentiality, integrity, and authenticity. 5. Show video to explain cryptography basics **Exercise** (5 minutes): 6. Discuss how encryption can solve real-world problems.. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 2 - https://www.youtube.com/watch?v=jhXCTbFnK8o Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the basic principles of cryptography? - How does encryption ensure data security? - In what scenarios is encryption most effective? 2. Nearpod Quiz on Cryptography Introduction 3. Homework: - Explain a real-world application of encryption. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 1.6	Course Name: Foundations of Cyber Security Topic: DES - The Data Encryption Standard	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand DES and its significance. b. Learn the basics of how DES works. c. Discuss the historical context of DES. d. Evaluate the strengths and weaknesses of DES.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - Have you heard of the Data Encryption Standard (DES)? - Why do you think older encryption methods might still be important to learn about? 2. Introduction - Brief history of DES. **Development** (30 minutes) 3. Explain how DES works. 4. Discuss the importance of DES in the history of cryptography. 5. Show video to illustrate DES encryption and decryption. **Exercise** (5 minutes): 6. Discuss how encryption can solve real-world problems.. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 2 - https://www.youtube.com/watch?v=WqJgN8F9PiE Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What is DES, and how does it work? - Why was DES significant in the history of cryptography? - How does DES compare to modern encryption methods? 2. Nearpod Quiz on DES 3. Homework: - Research the evolution of encryption standards from DES to present. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 1.7	Course Name: Foundations of Cyber Security Topic: AES - The Advanced Encryption Standard	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand AES and its importance. b. Learn the basics of how AES works. c. Discuss why AES replaced DES. d. Evaluate the effectiveness of AES.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - Have you heard of the Advanced Encryption Standard (AES)? - Why do you think AES replaced DES? 2. Introduction - Brief history of AES. **Development** (30 minutes) 3. Explain how AES works. 4. Discuss the reasons for developing AES. 5. Show video to illustrate AES encryption and decryption. **Exercise** (5 minutes): 6. Discuss scenarios where AES is used today. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 2 - https://www.youtube.com/watch?v=mlzxpkdXP58 Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What is AES, and how does it work? - Why was AES developed to replace DES? - In what scenarios is AES most effective? 2. Nearpod Quiz on AES 3. Homework: - Write about a modern application of AES in cybersecurity. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 1.8	Course Name: Foundations of Cyber Security Topic: Public Key Cryptography and RSA	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the principles of public key cryptography. b. Learn how RSA encryption works. c. Discuss the significance of RSA in cybersecurity. d. Evaluate the strengths and weaknesses of RSA.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you know about public key cryptography? - Have you heard of RSA encryption? 2. Introduction - Brief history and importance of public key cryptography. **Development** (30 minutes) 3. Explain the concept of public and private keys. 4. Discuss how RSA encryption and decryption work. 5. Show video to illustrate RSA. **Exercise** (5 minutes): 6. Compare public key cryptography with symmetric key cryptography. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 2 - https://www.youtube.com/watch?v=wXB-V_Keiu8 Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the basic principles of public key cryptography? - How does RSA encryption work? - What are the strengths and weaknesses of RSA? 2. Nearpod Quiz on Public Key Cryptography and RSA 3. Homework: - Research a real-world application of RSA. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.1	Course Name: Foundations of Cyber Security Topic: Unintentional (Non-malicious) Programming Oversights	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand common programming oversights. b. Identify how these oversights can lead to vulnerabilities. c. Discuss real-world examples of programming errors. d. Evaluate methods to mitigate these oversights.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What are some common mistakes you think programmers might make? - How do you think these mistakes could affect software security? 2. Introduction - Brief overview of non-malicious programming errors. **Development** (30 minutes) 3. Explain common programming oversights: buffer overflows, input validation errors, etc. 4. Discuss real-world examples and their impact. 5. Show video to illustrate programming oversights. **Exercise** (5 minutes): 6. Analyze a code snippet to identify potential oversights. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 3 - https://www.youtube.com/watch?v=hp3Qh7Vl1OM Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are common non-malicious programming errors? - How can these errors impact software security? - What strategies can be employed to mitigate these oversights? 2. Nearpod Quiz on Programming Oversights 3. Homework: - Research a recent incident caused by a programming oversight and prepare a report.

	Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.2	Course Name: Foundations of Cyber Security Topic: Malicious Code - Malware	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the different types of malware. b. Learn how malware infects systems. c. Discuss the impact of malware on cybersecurity. d. Evaluate strategies to prevent and combat malware.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - Can you name different types of malware? - How do you think malware spreads? 2. Introduction - Overview of malware types. **Development** (30 minutes) 3. Explain types of malware: viruses, worms, Trojans, ransomware. 4. Discuss how malware infects systems and its impact. 5. Show video to explain malware. **Exercise** (5 minutes): 6. Case study analysis of a malware attack. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 3 - https://www.youtube.com/watch?v=bWb3o5KjWkE Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the different types of malware? - How does malware spread and affect systems? - What are effective strategies to prevent and combat malware? 2. Nearpod Quiz on Malware 3. Homework: - Research and report on a recent malware outbreak.

	Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.3	Course Name: Foundations of Cyber Security Topic: Countermeasures Against Malware	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand various countermeasures against malware. b. Learn how antivirus software works. c. Discuss the importance of regular updates and patches. d. Evaluate the effectiveness of different countermeasures.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What measures do you take to protect your computer from malware? - Have you ever used antivirus software? 2. Introduction - Importance of countermeasures against malware. **Development** (30 minutes) 3. Explain different countermeasures: antivirus software, firewalls, regular updates. 4. Discuss how antivirus software detects and removes malware. 5. Show video to explain countermeasures. **Exercise** (5 minutes): 6. Compare the effectiveness of different antivirus software. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 3 - https://www.youtube.com/watch?v=6VvqeyyOaZQ Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are some effective countermeasures against malware? - How does antivirus software work? - Why are regular updates and patches important? 2. Nearpod Quiz on Countermeasures 3. Homework: - Write a report on the latest antivirus software and its features.

	Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.4	Course Name: Foundations of Cyber Security Topic: Web Security: User Side	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the basics of web security for users. b. Learn about common web threats targeting users. c. Discuss best practices for maintaining web security. d. Evaluate the effectiveness of various web security measures.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What web security measures do you currently use? - Have you ever encountered a web-based security threat? 2. Introduction - Overview of web security for users. **Development** (30 minutes) 3. Explain common web threats: phishing, spyware, adware. 4. Discuss best practices for users to maintain web security. 5. Show video to explain user-side web security. **Exercise** (5 minutes): 6. Analyze a phishing email and identify red flags. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 4 - https://www.youtube.com/watch?v=5VWdrNf3o7A Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are common web threats targeting users? - What best practices can users follow to maintain web security? - How effective are these web security measures? 2. Nearpod Quiz on User-Side Web Security 3. Homework: - Research and report on a recent web security incident affecting users.

	Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.5	Course Name: Foundations of Cyber Security Topic: Browser Attacks	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the various types of browser attacks. b. Learn how these attacks are executed. c. Discuss the impact of browser attacks on users. d. Evaluate strategies to prevent and mitigate browser attacks.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What browser do you use, and why do you prefer it? - Have you ever experienced a browser attack? 2. Introduction - Brief overview of browser attacks. **Development** (30 minutes) 1. Explain different types of browser attacks: man-in-the-middle, cross-site scripting, drive-by downloads. 2. Discuss how these attacks are executed and their impact. 3. Show video to explain browser attacks. **Exercise** (5 minutes): 4. Identify and discuss security features in popular browsers. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 4 - https://www.youtube.com/watch?v=nEITpzqrbtk Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are common types of browser attacks? - How are these attacks executed? - What strategies can prevent and mitigate browser attacks? 2. Nearpod Quiz on Browser Attacks 3. Homework: - Research a browser attack and its consequences. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.10	Course Name: Foundations of Cyber Security Topic: Rootkit	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand what a rootkit is and how it operates. b. Learn about the different types of rootkits. c. Discuss the impact of rootkits on system security. d. Evaluate strategies to detect and remove rootkits.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - Have you heard of rootkits before? - What do you think makes rootkits dangerous? 2. Introduction - Overview of rootkits. **Development** (30 minutes) 3. Explain what a rootkit is and how it operates. 4. Discuss different types of rootkits: kernel mode, user mode, firmware. 5. Show video to explain rootkits. **Exercise** (5 minutes): 6. Analyze a case study of a rootkit attack. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 4 - https://www.youtube.com/watch?v=Xu2H5KQ3qCg Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What is a rootkit, and how does it operate? - What are the different types of rootkits? - How can rootkits be detected and removed? 2. Nearpod Quiz on Rootkits 3. Homework: - Research and report on a recent rootkit attack. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.6	Course Name: Foundations of Cyber Security Topic: Web Attacks Targeting Users	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the different types of web attacks targeting users. b. Learn how these attacks compromise user data. c. Discuss the methods used to execute these attacks. d. Evaluate strategies to protect against web attacks targeting users.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you do to protect your personal information online? - Have you ever been a victim of a web attack? 2. Introduction - Overview of web attacks targeting users. **Development** (30 minutes) 3. Explain types of web attacks: phishing, social engineering, clickjacking. 4. Discuss how these attacks compromise user data. 5. Show video to explain web attacks. **Exercise** (5 minutes): 6. Case study analysis of a web attack targeting users. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 4 - https://www.youtube.com/watch?v=9uRKAizkU2I Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are common types of web attacks targeting users? - How do these attacks compromise user data? - What strategies can protect against these web attacks? 2. Nearpod Quiz on Web Attacks Targeting Users 3. Homework: - Write a report on a recent web attack targeting users. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.7	Course Name: Foundations of Cyber Security Topic: Obtaining User or Website Data	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand methods used to obtain user or website data. b. Learn about the implications of data breaches. c. Discuss real-world examples of data breaches. d. Evaluate measures to protect data from unauthorized access.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - How do you protect your data online? - What do you know about data breaches? 2. Introduction - Brief overview of obtaining user or website data. **Development** (30 minutes) 3. Explain methods used to obtain data: SQL injection, brute force attacks, man-in-the-middle attacks. 4. Discuss the implications of data breaches. 5. Show video to explain data breaches. **Exercise** (5 minutes): 6. Analyze a recent data breach incident. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 4 - https://www.youtube.com/watch?v=2KYeEQEGGo4 Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What methods are used to obtain user or website data? - What are the implications of data breaches? - How can data be protected from unauthorized access? 2. Nearpod Quiz on Obtaining Data 3. Homework: - Research a major data breach and prepare a report on its impact. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.8	Course Name: Foundations of Cyber Security Topic: Email Attacks	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the different types of email attacks. b. Learn how these attacks are executed. c. Discuss the impact of email attacks on users. d. Evaluate strategies to prevent and mitigate email attacks.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - Have you ever received a suspicious email? - What do you do to ensure the security of your email? 2. Introduction - Brief overview of obtaining user or website data. **Development** (30 minutes) 3. Explain different types of email attacks: phishing, spoofing, spam. 4. Discuss how these attacks are executed and their impact. 5. Show video to explain email attacks. **Exercise** (5 minutes): 6. Identify red flags in a suspicious email. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 4 - https://www.youtube.com/watch?v=2nQ_AkWHCrg Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are common types of email attacks? - How are these attacks executed? - What strategies can prevent and mitigate email attacks? 2. Nearpod Quiz on Email Attacks 3. Homework: - Research and report on a recent email attack incident. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.9	Course Name: Foundations of Cyber Security Topic: Security in Operating Systems	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the importance of security in operating systems. b. Learn about common security features in operating systems. c. Discuss vulnerabilities and threats to operating systems. d. Evaluate strategies to enhance operating system security.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What operating system do you use, and why? - Have you ever experienced a security issue with your operating system? 2. Introduction - Brief overview of security in operating systems. **Development** (30 minutes) 3. Explain common security features in operating systems: user authentication, access control, encryption. 4. Discuss vulnerabilities and threats to operating systems. 5. Show video to explain operating system security. **Exercise** (5 minutes): 6. Analyze the security features of a popular operating system. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 5 - https://www.youtube.com/watch?v=NkF5i_8ivVE Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are common types of email attacks? - How are these attacks executed? - What strategies can prevent and mitigate email attacks? 2. Nearpod Quiz on Operating System Security 3. Homework: - Write a report on the security features of your operating system. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 3.1	Course Name: Foundations of Cyber Security Topic: Network Concepts	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the fundamental concepts of networks. b. Identify different types of networks and their characteristics. c. Discuss the importance of network security. d. Evaluate the role of protocols in network communication..
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What types of networks do you know about? - Why do you think network security is important? 2. Introduction - Brief overview of network concepts. **Development** (30 minutes) 3. Explain network types: LAN, WAN, MAN, PAN. 4. Discuss network topologies: bus, star, ring, mesh. 5. Show video. **Exercise** (5 minutes): 6. Identify network types and topologies in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 12, pp. 626-650 - https://www.youtube.com/watch?v=3QhU9jd03a0 Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the different types of networks? - How do network topologies affect communication? - Why is network security important? 2. Nearpod Quiz on Network Concepts 3. Homework: - Research and report on different network topologies used in modern networks. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 3.2	Course Name: Foundations of Cyber Security Topic: Network Concepts	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the different threats to network communications. b. Identify common network attack techniques. c. Discuss the impact of network threats on organizations. d. Evaluate mitigation strategies for network threats.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What are some common threats to network communications? - How do you think these threats can be mitigated? 2. Introduction - Brief overview of network communication threats. **Development** (30 minutes) 3. Explain common threats: eavesdropping, man-in-the-middle, IP spoofing, DNS poisoning. 4. Discuss the impact of network threats on organizations. 5. Show video. **Exercise** (5 minutes): 6. Identify types of network attacks in case studies. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 13, pp. 651-680 - https://www.youtube.com/watch?v=E7zwWJiOpRA Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the common threats to network communications? - How do network threats impact organizations? - What strategies can mitigate network threats? 2. Nearpod Quiz on Network Threats. 3. Homework: - Write a report on a recent network attack incident. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 3.3	Course Name: Foundations of Cyber Security Topic: Wireless Network Security	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the principles of wireless network security. b. Identify vulnerabilities in wireless networks. c. Discuss the importance of securing wireless communications. d. Evaluate strategies to enhance wireless network security.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - How do you connect to wireless networks? - What measures do you take to secure your wireless connection? 2. Introduction - Brief overview of wireless network security. **Development** (30 minutes) 3. Explain vulnerabilities: weak encryption, rogue access points, jamming. 4. Discuss security protocols: WEP, WPA, WPA2. 5. Show video **Exercise** (5 minutes): 6. Identify types of network attacks in case studies. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 14, pp. 681-700 - https://www.youtube.com/watch?v=5-lXS-m3vRQ Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the common vulnerabilities in wireless networks? - How do security protocols protect wireless communications? - What strategies can enhance wireless network security? 2. Nearpod Quiz on Wireless Network Security. 3. Homework: - Research and report on a recent wireless network security breach. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 3.4	Course Name: Foundations of Cyber Security Topic: Denial of Service (DoS)	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the concept of Denial of Service (DoS) attacks. b. Identify different types of DoS attacks. c. Discuss the impact of DoS attacks on organizations. d. Evaluate methods to prevent and mitigate DoS attacks.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - Have you ever experienced a service outage? - How do you think a DoS attack can affect an organization? 2. Introduction - Brief overview of DoS attacks. **Development** (30 minutes) 1. Explain types of DoS attacks: volume-based, protocol-based, application layer. 2. Discuss the impact of DoS attacks on organizations. 3. Show video **Exercise** (5 minutes): 4. Analyze a case study of a DoS attack. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 15, pp. 701-720. - https://www.youtube.com/watch?v=b0C9JkRC_Ug Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the different types of DoS attacks? - How do DoS attacks impact organizations? - What strategies can prevent and mitigate DoS attacks? 2. Nearpod Quiz on DoS Attacks. 3. Homework: - Write a report on a recent DoS attack incident. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 3.5	Course Name: Foundations of Cyber Security Topic: Distributed Denial-of-Service (DDoS)	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the concept of Distributed Denial-of-Service (DDoS) attacks. b. Identify the differences between DoS and DDoS attacks. c. Discuss the impact of DDoS attacks on organizations. d. Evaluate methods to prevent and mitigate DDoS attacks.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you know about DDoS attacks? - How do you think DDoS attacks differ from DoS attacks? 2. Introduction - Brief overview of DDoS attacks. **Development** (30 minutes) 3. Explain the nature of DDoS attacks. 4. Discuss the differences between DoS and DdoS attacks. 5. Show video. **Exercise** (5 minutes): 6. Analyze a case study of a DDoS attack. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 15, pp. 721-740. - https://www.youtube.com/watch?v=wph1bCTPYwA Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the differences between DoS and DDoS attacks? - How do DDoS attacks impact organizations? - What strategies can prevent and mitigate DDoS attacks? 2. Nearpod Quiz on DDoS Attacks. 3. Homework: - Write a report on a recent DDoS attack incident. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 3.6	Course Name: Foundations of Cyber Security Topic: Security Countermeasures	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand different security countermeasures. b. Identify the role of countermeasures in network security. c. Discuss the effectiveness of various countermeasures. d. Evaluate strategies to implement security countermeasures.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What security countermeasures do you use? - How effective do you think these countermeasures are? 2. Introduction - Brief overview of security countermeasures. **Development** (30 minutes) 3. Explain different countermeasures: firewalls, intrusion detection systems, encryption. 4. Discuss the role of countermeasures in network security. 5. Show video. **Exercise** (5 minutes): 6. Evaluate the effectiveness of countermeasures in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 16, pp. 741-765. - https://www.youtube.com/watch?v=V3TXdGoG7Bo Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the different security countermeasures? - How do countermeasures protect networks? - What strategies can enhance the effectiveness of countermeasures? 2. Nearpod Quiz on Security Countermeasures. 3. Homework: - Research and report on a security countermeasure used in an organization.

	Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 3.7	Course Name: Foundations of Cyber Security Topic: Firewalls	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the concept of firewalls in network security. b. Identify different types of firewalls. c. Discuss the role of firewalls in protecting networks. d. Evaluate strategies to implement and manage firewalls.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you know about firewalls? - How do firewalls protect your network? 2. Introduction - Brief overview of firewalls. **Development** (30 minutes) 3. Explain different types of firewalls: packet-filtering, stateful inspection, proxy. 4. Discuss the role of firewalls in protecting networks. 5. Show video. **Exercise** (5 minutes): 6. Analyze the use of firewalls in provided network scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 17, pp. 766-790. - https://www.youtube.com/watch?v=OqH56Y0mxaY Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the different types of firewalls? - How do firewalls protect networks? - What strategies can enhance the effectiveness of firewalls? 2. Nearpod Quiz on Firewalls. 3. Homework:

	- Write a report on the implementation of firewalls in an organization. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 3.8	Course Name: Foundations of Cyber Security Topic: Intrusion Detection and Prevention Systems (IDPS)	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the concept of Intrusion Detection and Prevention Systems (IDPS). b. Identify different types of IDPS. c. Discuss the role of IDPS in network security. d. Evaluate strategies to implement and manage IDPS..
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you know about IDPS? - How do IDPS help in network security? 2. Introduction - Brief overview of IDPS. **Development** (30 minutes) 3. Explain different types of IDPS: network-based, host-based, hybrid. 4. Discuss the role of IDPS in network security. 5. Show video. **Exercise** (5 minutes): 6. Evaluate the use of IDPS in provided network scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 18, pp. 791-815. - https://www.youtube.com/watch?v=OqH56Y0mxaY Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the different types of IDPS? - How do IDPS protect networks? - What strategies can enhance the effectiveness of IDPS? 2. Nearpod Quiz on IDPS. 3. Homework: - Research and report on the implementation of IDPS in an organization.

	Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 3.9	Course Name: Foundations of Cyber Security Topic: Cryptography in Network Security	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the role of cryptography in network security. b. Identify different cryptographic techniques used in networks. c. Discuss the importance of encryption and decryption. d. Evaluate strategies to implement cryptographic solutions.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What is your understanding of cryptography? - How do you think cryptography helps in network security? 2. Introduction - Brief overview of cryptography in network security. **Development** (30 minutes) 3. Explain different cryptographic techniques: symmetric, asymmetric. 4. Discuss the importance of encryption and decryption. 5. Show video. **Exercise** (5 minutes): 6. Analyze cryptographic techniques in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 19, pp. 816-840. - https://www.youtube.com/watch?v=3QnD2c4Xovk Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the different cryptographic techniques used in networks? - How does encryption and decryption work? - What strategies can enhance the effectiveness of cryptography? 2. Nearpod Quiz on Cryptography in Network Security. 3. Homework:

	- Write a report on the use of cryptography in network security. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 3.10	Course Name: Foundations of Cyber Security Topic: Network Management	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the concept of network management. b. Identify the role of network management in security. c. Discuss network management tools and techniques. d. Evaluate strategies to implement effective network management.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you know about network management? - How important do you think network management is for security? 2. Introduction - Brief overview of network management. **Development** (30 minutes) 3. Explain network management tools: SNMP, NetFlow, Wireshark. 4. Discuss the role of network management in security. 5. Show video. **Exercise** (5 minutes): 6. Evaluate network management tools in provided scenarios.. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 20, pp. 841-865. - https://www.youtube.com/watch?v=ciWML45JYXI Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the different network management tools? - How does network management help in security? - What strategies can enhance the effectiveness of network management?

	2. Nearpod Quiz on Network Management. 3. Homework: - Research and report on a network management tool used in an organization. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 4.1	Course Name: Foundations of Cyber Security Topic: Cloud Computing Concepts	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the fundamental concepts of cloud computing. b. Identify different types of cloud services (IaaS, PaaS, SaaS). c. Discuss the advantages and disadvantages of cloud computing. d. Evaluate the impact of cloud computing on businesses.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you know about cloud computing? - How do you think cloud computing benefits businesses? 2. Introduction - Brief overview of cloud computing concepts. **Development** (30 minutes) 3. Explain types of cloud services: IaaS, PaaS, SaaS. 4. Discuss advantages and disadvantages of cloud computing. 5. Show video. **Exercise** (5 minutes): 6. Identify types of cloud services in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 8 - https://www.youtube.com/watch?v=E7zwWJiOpRA Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the different types of cloud services? - How does cloud computing benefit businesses? - What are the disadvantages of cloud computing? 2. Nearpod Quiz on Cloud Computing Concepts. 3. Homework: - Research and report on a cloud service used by a business. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 4.2	Course Name: Foundations of Cyber Security Topic: Moving to the Cloud	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the process of moving to the cloud. b. Identify key considerations for cloud migration. c. Discuss the challenges of cloud migration. d. Evaluate strategies for successful cloud migration.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - Have you experienced using cloud services? - What do you think are the challenges of moving to the cloud? 2. Introduction - Brief overview of moving to the cloud. **Development** (30 minutes) 3. Explain the process of cloud migration. 4. Discuss key considerations: data security, cost, compliance. 5. Show video. **Exercise** (5 minutes): 6. Evaluate cloud migration plans in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 8 - https://www.youtube.com/watch?v=REaBzQSS7PM Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the key considerations for cloud migration? - What challenges are associated with moving to the cloud? - What strategies can ensure successful cloud migration? 2. Nearpod Quiz on Cloud Migration. 3. Homework: - Write a report on a company's experience with cloud migration. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 4.3	Course Name: Foundations of Cyber Security Topic: Cloud Security	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the principles of cloud security. b. Identify common cloud security threats. c. Discuss cloud security best practices. d. Evaluate strategies to secure cloud environments..
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What are your concerns about cloud security? - How do you think cloud providers secure their services? 2. Introduction - Brief overview of cloud security. **Development** (30 minutes) 3. Explain common cloud security threats: data breaches, insider threats, account hijacking. 4. Discuss cloud security best practices. 5. Show video. **Exercise** (5 minutes): 6. Identify cloud security threats in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 8 - https://www.youtube.com/watch?v=EvqnOHM_F_o Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are common cloud security threats? - How can cloud environments be secured? - What are the best practices for cloud security? 2. Nearpod Quiz on Cloud Security. 3. Homework: - Research and report on a cloud security breach incident. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 4.4	Course Name: Foundations of Cyber Security Topic: Tools and Techniques for Cloud Security	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the tools and techniques used for cloud security. b. Identify popular cloud security tools. c. Discuss the application of security tools in cloud environments. d. Evaluate the effectiveness of different cloud security techniques.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What tools do you know that are used for cloud security? - How effective do you think these tools are? 2. Introduction - Brief overview of cloud security tools and techniques. **Development** (30 minutes) 3. Explain popular cloud security tools: firewalls, encryption, IAM. 4. Discuss the application of these tools in cloud environments. 5. Show video. **Exercise** (5 minutes): 6. Evaluate the use of security tools in provided cloud scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 8 - https://www.youtube.com/watch?v=3IdwH6NnGDs Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the popular cloud security tools? - How are these tools applied in cloud environments? - What techniques can enhance cloud security? 2. Nearpod Quiz on Cloud Security Tools. 3. Homework: - Write a report on a cloud security tool used by an organization. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 4.5	Course Name: Foundations of Cyber Security Topic: Cloud Identity Management	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the concept of cloud identity management. b. Identify the challenges of managing identities in the cloud. c. Discuss the importance of identity and access management (IAM) in cloud security. d. Evaluate strategies to implement effective cloud identity management.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you know about identity management? - How do you think IAM is different in the cloud? 2. Introduction - Brief overview of cloud identity management. **Development** (30 minutes) 3. Explain the challenges of managing identities in the cloud. 4. Discuss the role of IAM in cloud security. 5. Show video. **Exercise** (5 minutes): 6. Evaluate IAM strategies in provided cloud scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 8 - https://www.youtube.com/watch?v=_gZlCjG0K4I Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the challenges of managing identities in the cloud? - How does IAM enhance cloud security? - What strategies can ensure effective cloud identity management? 2. Nearpod Quiz on Cloud Identity Management. 3. Homework: - Research and report on an IAM tool used in the cloud.

	Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 4.6	Course Name: Foundations of Cyber Security Topic: Securing IaaS	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the principles of securing Infrastructure as a Service (IaaS). b. Identify the security challenges unique to IaaS. c. Discuss best practices for securing IaaS environments. d. Evaluate strategies to implement effective IaaS security.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you know about IaaS? - How do you think security is different for IaaS compared to other cloud services? 2. Introduction - Brief overview of IaaS security. **Development** (30 minutes) 3. Explain the security challenges unique to IaaS. 4. Discuss best practices for securing IaaS environments. 5. Show video. **Exercise** (5 minutes): 6. Evaluate IaaS security strategies in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 8 - https://www.youtube.com/watch?v=XYjZqxMjZ6I Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the security challenges unique to IaaS? - How can IaaS environments be secured? - What are the best practices for IaaS security? 2. Nearpod Quiz on IaaS Security.

	3. Homework: - Write a report on the security measures used in an IaaS environment. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 4.7	Course Name: Foundations of Cyber Security Topic: Privacy Concepts	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the concepts of privacy in computing. b. Identify the principles and policies of privacy. c. Discuss the impact of privacy on data and user behavior. d. Evaluate the challenges in maintaining privacy in modern computing environments.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What does privacy mean to you in the context of computing? - How do you think privacy policies affect user behavior? 2. Introduction - Brief overview of privacy concepts. **Development** (30 minutes) 3. Explain privacy principles and policies. 4. Discuss the impact of privacy on data and user behavior. 5. Show video. **Exercise** (5 minutes): 6. Evaluate privacy policies in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 8 - https://www.youtube.com/watch?v=XYjZqxMjZ6I Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the principles and policies of privacy? - How does privacy affect data and user behavior?

	- What are the challenges in maintaining privacy in modern computing environments? 2. Nearpod Quiz on Privacy Concepts. 3. Homework: - Research and report on a privacy breach incident. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 4.8	**Course Name: Foundations of Cyber Security** **Topic: Authentication and Privacy**	**Course No.: COM-301**

Objectives	At the end of the lesson the student shall be able to: a. Understand the relationship between authentication and privacy. b. Identify different authentication mechanisms. c. Discuss the impact of authentication on user privacy. d. Evaluate strategies to balance authentication and privacy needs.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What is the role of authentication in security? - How do you think authentication affects user privacy? 2. Introduction - Brief overview of privacy concepts. **Development** (30 minutes) 3. Explain different authentication mechanisms: passwords, biometrics, multi-factor authentication. 4. Discuss the impact of authentication on user privacy. 5. Show video. **Exercise** (5 minutes): 6. Evaluate authentication strategies in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 9 - https://www.youtube.com/watch?v=Ho0g_MZHzvA Spend 5 minutes to wrap up and consolidate the learnings

Evaluation	1. Reflective Questions - What are the different authentication mechanisms? - How does authentication affect user privacy? - What strategies can balance authentication and privacy needs? 2. Nearpod Quiz on Authentication and Privacy. 3. Homework: - Write a report on the privacy implications of a specific authentication mechanism. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 4.9	**Course Name: Foundations of Cyber Security** **Topic: Privacy on the Web**	**Course No.: COM-301**

Objectives	At the end of the lesson the student shall be able to: a. Understand the concepts of privacy on the web. b. Identify the threats to privacy on the web. c. Discuss best practices for maintaining privacy online. d. Evaluate strategies to protect user privacy on the web.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - How do you protect your privacy online? - What are the common threats to privacy on the web? 2. Introduction - Brief overview of privacy on the web. **Development** (30 minutes) 3. Explain threats to privacy on the web: tracking, data breaches, phishing. 4. Discuss best practices for maintaining privacy online. 5. Show video. **Exercise** (5 minutes): 6. Identify privacy threats in provided web scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 9 - https://www.youtube.com/watch?v=ahcOKdVe5X4

	Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the common threats to privacy on the web? - How can users maintain their privacy online? - What strategies can protect user privacy on the web? 2. Nearpod Quiz on Privacy on the Web. 3. Homework: - Research and report on a web privacy tool. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 4.10	Course Name: Foundations of Cyber Security Topic: Email Security and Privacy	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the importance of email security and privacy. b. Identify common email threats. c. Discuss best practices for securing email communications. d. Evaluate strategies to maintain email privacy.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you do to secure your email communications? - How do you think email privacy is maintained? 2. Introduction - Brief overview of email security and privacy. **Development** (30 minutes) 3. Explain common email threats: phishing, spam, malware. 4. Discuss best practices for securing email communications. 5. Show video. **Exercise** (5 minutes): 6. Identify email threats in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 10 - https://www.youtube.com/watch?v=0F7GBMDdeDw Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the common email threats? - How can email communications be secured? - What strategies can maintain email privacy? 2. Nearpod Quiz on Email Security and Privacy. 3. Homework: - Write a report on an email security breach incident. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 5.1	Course Name: Foundations of Cyber Security Topic: Security Planning	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the importance of security planning in an organization. b. Identify the key components of a security plan. c. Discuss the process of creating and implementing a security plan. d. Evaluate the effectiveness of different security planning strategies.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you think are the key components of a security plan? - How important is security planning for an organization? 2. Introduction - Brief overview of security planning. **Development** (30 minutes) 3. Explain the key components of a security plan: risk assessment, security policy, incident response plan. 4. Discuss the process of creating and implementing a security plan. **Exercise** (5 minutes): 5. Evaluate a sample security plan in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 10 Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the key components of a security plan? - How is a security plan created and implemented? - What strategies can ensure effective security planning? 2. Nearpod Quiz on Security Planning. 3. Homework: - Research and report on a security plan used by an organization. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 5.2	Course Name: Foundations of Cyber Security Topic: Business Continuity Planning	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the concept of business continuity planning (BCP). b. Identify the steps involved in developing a BCP. c. Discuss the importance of BCP in mitigating risks. d. Evaluate strategies for successful business continuity.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you know about business continuity planning? - How do you think BCP helps in risk management? 2. Introduction - Brief overview of security planning. **Development** (30 minutes) 3. Explain the steps involved in developing a BCP: risk assessment, impact analysis, recovery strategies. 4. Discuss the importance of BCP in mitigating risks. **Exercise** (5 minutes): 5. Evaluate a sample BCP in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 10 Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the steps involved in developing a BCP? - How does BCP mitigate risks? - What strategies can ensure successful business continuity? 2. Nearpod Quiz on Business Continuity Planning. 3. Homework: - Write a report on a business continuity plan used by an organization. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 5.3	Course Name: Foundations of Cyber Security Topic: Handling Incidents	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the process of handling security incidents. b. Identify different types of security incidents. c. Discuss best practices for incident response. d. Evaluate strategies for effective incident management.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What are some examples of security incidents? - How do you think organizations should handle security incidents? 2. Introduction - Brief overview of handling incidents. **Development** (30 minutes) 3. Explain different types of security incidents: data breaches, malware attacks, insider threats. 4. Discuss best practices for incident response. **Exercise** (5 minutes): 5. Evaluate an incident response plan in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 10 Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are different types of security incidents? - How should organizations handle security incidents? - What strategies can ensure effective incident management? 2. Nearpod Quiz on Handling Incidents 3. Homework: - Research and report on an organization's response to a security incident. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 5.4	Course Name: Foundations of Cyber Security Topic: Risk Analysis	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the concept of risk analysis in security. b. Identify the steps involved in conducting a risk analysis. c. Discuss the importance of risk analysis in decision-making. d. Evaluate strategies for effective risk management.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you know about risk analysis? - How important is risk analysis in managing security risks? 2. Introduction - Brief overview of handling incidents. **Development** (30 minutes) 3. Explain the steps involved in conducting a risk analysis: risk identification, risk assessment, risk control. 4. Discuss the importance of risk analysis in decision-making. **Exercise** (5 minutes): 5. Evaluate a risk analysis report in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 10 Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the steps involved in conducting a risk analysis? - How does risk analysis aid in decision-making? - What strategies can ensure effective risk management? 2. Nearpod Quiz on Risk Analysis 3. Homework: - Write a report on a risk analysis conducted by an organization. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 5.5	Course Name: Foundations of Cyber Security Topic: Dealing with Disaster	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the process of disaster recovery in security. b. Identify different types of disasters that can impact organizations. c. Discuss best practices for disaster recovery planning. d. Evaluate strategies for effective disaster recovery.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What types of disasters can impact organizations? - How important is disaster recovery planning for an organization? 2. Introduction - Brief overview of handling incidents. **Development** (30 minutes) 3. Explain different types of disasters: natural disasters, cyber-attacks, equipment failure. 4. Discuss best practices for disaster recovery planning. **Exercise** (5 minutes): 5. Evaluate a disaster recovery plan in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 10 Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What types of disasters can impact organizations? - How can organizations effectively plan for disaster recovery? - What strategies can ensure effective disaster recovery? 2. Nearpod Quiz on Disaster Recovery 3. Homework: - Research and report on a disaster recovery plan used by an organization. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 5.6	Course Name: Foundations of Cyber Security Topic: Legal Issues in Protecting Programs and Data	Course No.: COM-301

Objectives	At the end of the lesson the student shall be able to: a. Understand the legal issues related to protecting programs and data. b. Identify laws and regulations that impact data protection. c. Discuss the rights of individuals and organizations in protecting programs and data. d. Evaluate strategies for legal compliance in data protection.
Teaching Aids (if any)	d. Presentation e. Chalkboard/Whiteboard f. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What legal issues are involved in protecting programs and data? - How do you think laws affect data protection practices? 2. Introduction - Brief overview of legal issues in protecting programs and data. **Development** (30 minutes) 3. Explain key laws and regulations: GDPR, HIPAA, CCPA. 4. Discuss the rights of individuals and organizations in data protection. **Exercise** (5 minutes): 5. Evaluate legal compliance in provided scenarios. Use Nearpod to collect responses and discuss the answers.
Closure	3. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 4. Suggested Reading - Textbook 1, Chapter 11 Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	4. Reflective Questions - What types of disasters can impact organizations? - How can organizations effectively plan for disaster recovery? - What strategies can ensure effective disaster recovery? 5. Nearpod Quiz on Disaster Recovery 6. Homework: - Research and report on a disaster recovery plan used by an organization. Spend 5 minutes to evaluate student assimilation of the lesson contents