



# Buddha Institute of Technology

Gorakhpur

Department of Mechanical Engineering  
ALLOTTMENT BASED ON COMPETENCY SKILLS  
Academic Session July.-Dec 2022

Name of the Staff	Pallavi Dixit
Area of Specialization	Data mining, DBMS, Computer system Security ,Python, DAA
Subject Allotted	COMPUTER SYSTEM SECURITY

Sl. #	Course Code	Course Title	Semester	Theory
1	KNC301	COMPUTER SYSTEM SECURITY	III-A	Theory
2	KNC301	COMPUTER SYSTEM SECURITY	III-B	Theory


**HOD**

Program : **B. Tech.**  
Branch : **ME**  
Semester : **III**  
Session : **2022-23**  
Name of the Course : **COMPUTER SYSTEM SECURITY**  
Code : **KNC-301**  
Name of the Course Instructor : **MS.Pallavi Dixit**  
Designation : **Assistant Professor**  
Department : **Information Technology**

**Course Outcome and Programme Outcome**

**Description of the Course Outcome:**

<b>CO</b>	<b>After completion of the course students will be able to:</b>
KNC401.1	Demonstration of all security terms related to network and computer.
KNC401.2	Remember all the concept of confidentiality policies and internet infrastructure.
KNC401.3	Explain mobile software bugs posing cyber security threats, .
KNC401.4	Describe the security terms and hacking technique
KNC401.5	Explain the all network security and architecture

Buddha Institute of Technology, Gorakhpur			
Department: Mechanical Engineering.			
Academic Semester July.-Dec 2022			
Semester: IV	Section: A/B	Course Code: KNC-301	Course: COMPUTER SYSTEM SECURITY
Course Instructor: PALLAVI DIXIT		Contact Hours /week: 02	# of credits: 02
CIE Marks: 25		SEE Marks:50	Exam Hours: 02

Prerequisites if any:			
Code No	Course Name	Description	Semester
NA	NA	NA	NA

Content delivery:	Chalk & Board
-------------------	---------------

COURSE SYLLABUS:			
ModuleNo	Contents of Module	Hrs	COs
1	<b>Computer System Security Introduction:</b> Introduction, What is computer security and what to learn? , Sample Attacks, The Marketplace for vulnerabilities, Error 404 Hacking digital India part 1 chase. Hijacking & Defence: Control Hijacking ,More Control Hijacking attacks integer overflow More Control Hijacking attacks format string vulnerabilities, Defence against Control Hijacking - Platform Defences, Defence against Control Hijacking - Run-time Defences', Advanced Control Hijacking attacks.	8	CO1
2	<b>Confidentiality Policies:</b> Confinement Principle ,Detour Unix user IDs process IDs and privileges , More on confinement techniques ,System call interposition ,Error 404 digital Hacking in India part 2 chase , VM based isolation ,Confinement principle ,Software fault isolation , Rootkits ,Intrusion Detection Systems	8	CO2
3	<b>Secure architecture principles isolation and leas:</b> Access Control Concepts , Unix and windows access control summary ,Other issues in access control ,Introduction to browser isolation . Web security landscape : Web security definitions goals and threat models , HTTP content rendering .Browser isolation .Security interface , Cookies frames and frame busting, Major web server threats ,Cross site request forgery ,Cross site scripting ,Defenses and protections against XSS , Finding vulnerabilities ,Secure development.	8	CO3
4	<b>Basic cryptography:</b> Public key cryptography ,RSA public key crypto ,Digital signature Hash functions ,Public key distribution ,Real world protocols ,Basic terminologies ,Email security certificates ,Transport Layer security TLS ,IP security , DNS security.	8	CO4
5	<b>. Internet Infrastructure:</b> Basic security problems , Routing security ,DNS revisited ,Summary of weaknesses of internet security ,.Link layer connectivity and TCP IP connectivity , Packet filtering firewall ,Intrusion detection	8	CO5

**COURSE OUTCOMES:** At the end of the Course, the Student will be able to:

<b>CO1</b>	Demonstration of all security terms related to network and computer.	
<b>CO2</b>	Remember all the concept of confidentiality policies and internet infrastructure.	
<b>CO3</b>	Explain mobile software bugs posing cyber security threats, .	
<b>CO4</b>	Describe the security terms and hacking technique	
<b>CO5</b>	Explain the all network security and architecture	

**Mapping of CO v/s PO v/s PSO**

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
KNC-401.1	1	-	-	-	-	-	-	-	-	-	-	-	1	-	-
KNC-401.2	1	-	-	-	-	-	-	-	-	-	-	-	1	-	-
KNC-401.3	1	-	-	-	-	-	-	-	-	-	-	-	1	-	-
KNC-401.4		-	-	-	-	-	-	-	-	-	-	-	1	-	-
KNC-401.5		-	-	-	-	-	-	-	-	-	-	-		-	-
<b>Average</b>	<b>1</b>												<b>1</b>		

**Correlation levels: 1-Slight (Low)      2-Moderate (Medium)      3-Substantial (High)**

<b>Gap in the syllabus</b>	NA
----------------------------	----

<b>Topics to be covered beyond syllabus</b>	NA
---	----

**Assessment Methodologies:**

Sl. No.	Description	Type
1	Student Assignment	Direct
2	Internal assessment	Direct
3	University exam	Direct
4	Student feedback	Indirect
5	Alumni feedback	Indirect
6	Employers feedback	Indirect

## LESSON PLAN

Lecture #	Module#	Topics	RBT Levels	Course Outcome Mapping	Planned Date	Actual Date	Faculty Sign	Remarks
1	1	Introduction , What is computer security and what to Learn	L1	CO1	30-8-22			
2		Sample Attacks			1-9-22			
3		The Marketplace for vulnerabilities			2-9-22			
4		Error 404 Hacking digital India part 1chase			6-9-22			
5		Error 404 Hacking digital India part 1chase			8-9-22			
6		Control Hijacking			9-9-22			
7		More Control Hijacking attacks integer overflow ,			13-9-22			
8		Defense against Control Hijacking			15-9-22			
9		Platform Defenses, Defense against Control Hijacking - Run-time Defenses			16-9-22			
10		More on confinement techniques ,System call interposition			20-9-22			
11		Error 404 digital Hacking in India part 2 chase			22-9-22			
12		VM based isolation Confinement principle Software fault isolation			23-9-22			
13		Rootkits ,Intrusion Detection Systems			27-9-22			
14	2	Platform Defenses, Defense against Control Hijacking - Run-time Defenses	L1	CO2	29-9-22			
15		More on confinement techniques ,System call interposition			30-9-22			
16		Error 404 digital Hacking in India part 2 chase			11-10-22,			
17		VM based isolation Confinement principle Software fault isolation			13-10-22,			
18		Rootkits ,Intrusion Detection Systems			14-10-22,			

19		Access Control Concepts , Unix and windows access			18,20-10-22,			
20		Other issues in access control ,Introduction to browser solution			21-10-22			
21		Web security definitions goals and threat models			1-11-22			
22		Web security definitions goals and threat models			03-11-22			
23		HTTP content rendering .Browser isolation .Security interface			04-11-22			
24		Cookies frames and frame busting, Major web server threats			8-11-22			
25		Cross site request forgery ,Cross site scripting			10-11-22			
26		Defenses and protections against XSS,, Finding vulnerabilities Secure development			15-11-22			
27		Public key cryptography ,RSA public key crypto			17,18-11-22			
28		Digital signature Hash functions			22,24,-11-22			
29		Public key distribution Real world protocols			25-11-22			
30	4	Basic terminologies Email security certificates	L1	CO4	1,2-12-22			
31		Transport Layer security TLS ,IP security DNS security			6,8-12-22			
32		Transport Layer security TLS ,IP security DNS security			9,12-12-22			
33		Basic security problems Routing security ,DNS revisited			19,21-12-22			
34		Summary of weaknesses of internet security			28,-12-22			
35	5	Link layer connectivity and TCP IP connectivity	L1	CO5	29-12-22			
36		Packet filtering firewall Intrusion detection			2,5-1-23			
37		Finding vulnerabilities Secure development			6-1-23			

**Syllabus for Sessionals:**

<b>Sessional</b>	<b>Syllabus</b>
CT1	Class 1- Class 20
CT2	Class 21- Class 47
Pre - AKTU	Full Syllabus

**\*L1 - Remembering; L2 - Understanding; L3 - Applying; L4 - Analysing; L5 - Evaluating; L6 - Creating**

**Literature:**

**Literature:**

**Reference:**

Dewar, R. 2014. 'the Triptych of Cyber Security: A Classification of Active Cyber

Defense'. 6th International Conference on Cyber Security

Dunn-Cavelty, M. 2010. 'Cyber Security' in A. Collins, Contemporary Security Studies. Oxford: OUP

Dunn-Cavelty, M. 2013. From Cyber-Bombs to Political fallout: threat Representations with an impact in Cyber-Security Discourse. *International Studies Review*, 15, pp. 105-122

Hansen, L. and Niessanbaum, H. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53, pp. 1155-1175

McLean, S. 2013. Beware the Botnets: Cyber Security is a Board Level Issue. *Intellectual Property & Technology Law Journal*, 25 (12), pp. 22-27

Warner, M. 2012. Cybersecurity: A Pre-history. *Intelligence and National Security*, 27 (5), pp. 781-799

Vacca, JR. 2013. *Cyber Security and IT infrastructure protection*. Waltham: St



Reference:

Dewar, R. 2014. 'the Triptych of Cyber Security: A Classification of Active Cyber

Defense'. 6th International Conference on Cyber Security

Dunn-Cavelty, M. 2010. 'Cyber Security' in A. Collins, Contemporary Security Studies. Oxford: OUP

Dunn-Cavelty, M. 2013. From Cyber-Bombs to Political fallout: threat Representations with an impact in Cyber-Security Discourse. International Studies Review, 15, pp. 105-122

Hansen, L. and Niessanbaum, H. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53, pp. 1155-1175

McLean, S. 2013. Beware the Botnets: Cyber Security is a Board Level Issue. *Intellectual Property & Technology Law Journal*, 25 (12), pp. 22-27

Warner, M. 2012. Cybersecurity: A Pre-history. *Intelligence and National Security*, 27 (5), pp. 781-799

Vacca, JR. 2013. *Cyber Security and IT infrastructure protection*. Waltham: St Reference:

Dewar, R. 2014. 'the Triptych of Cyber Security: A Classification of Active Cyber

Defense'. 6th International Conference on Cyber Security

Dunn-Cavelty, M. 2010. 'Cyber Security' in A. Collins, *Contemporary Security Studies*. Oxford: OUP

Dunn-Cavelty, M. 2013. From Cyber-Bombs to Political fallout: threat Representations with an impact in Cyber-Security Discourse. *International Studies Review*, 15, pp. 105-122

Hansen, L. and Niessanbaum, H. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53, pp. 1155-1175

McLean, S. 2013. Beware the Botnets: Cyber Security is a Board Level Issue. *Intellectual Property & Technology Law Journal*, 25 (12), pp. 22-27

Warner, M. 2012. Cybersecurity: A Pre-history. *Intelligence and National Security*, 27 (5), pp. 781-799

Vacca, JR. 2013. *Cyber Security and IT infrastructure protection*. Waltham: St

Reference:

Dewar, R. 2014. 'the Triptych of Cyber Security: A Classification of Active Cyber

Defense'. 6th International Conference on Cyber Security

Dunn-Cavelty, M. 2010. 'Cyber Security' in A. Collins, Contemporary Security Studies. Oxford: OUP

Dunn-Cavelty, M. 2013. From Cyber-Bombs to Political fallout: threat Representations with an impact in Cyber-Security Discourse. International Studies Review, 15, pp. 105-122

Hansen, L. and Niessanbaum, H. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53, pp. 1155-1175

McLean, S. 2013. Beware the Botnets: Cyber Security is a Board Level Issue. Intellectual Property & Technology Law Journal, 25 (12), pp. 22-27

Warner, M. 2012. Cybersecurity: A Pre-history. Intelligence and National Security, 27 (5), pp. 781-799

Vacca, JR. 2013. Cyber Security and IT infrastructure protection. Waltham: Steven

<https://ict.iitk.ac.in/product/computer-system-security>

Sample Questions:

Question No.	Questions
1	Explain active attack also discuss their type with diagram
2	Describe confinement principal and problem
3	Discuss different security modell? Explain virus, worm and spoofs
4	What is cryptography? Explain their type
5	What is internet? define their weakness in
6	Write down short note on firewall and DNS
7	Explain IDS and their type with diagram

8	Discuss packet filtering and TLS
9	What do you mean by cookies frame and frame busting?
10	What is hash function? explain digital signature with diagram
11	Discuss RSA public key with example
12	Explain access control? Also discuss DAC and MAC
13	What is unix? write down difference between windows and unix
14	What is buffer overflow attack ?also discuss passive attack

**Assessment rubrics that is going to be adopted for direct attainment is depicted in below table**

<b>Level of Achievement</b>	<b>Elaboration on Course Grading Description</b>	<b>Bench Mark Set (Out of 100)</b>
<b>Excellent (A)</b>	The Student's performance is outstanding in almost all the intended course learning outcomes	<b>75</b>
<b>Good (B)</b>	The student's performance is good in most of the intended course learning outcomes.	<b>60</b>
<b>Marginal (C)</b>	The student's performance is barely satisfactory. It marginally meets the intended course learning outcomes	<b>45</b>
<b>Fail (F)</b>	The Students performance is inadequate. Student fails to meet many of the intended course learning outcomes	<b>35</b>

**NOTE:** Have different Assessment pattern for tests, assignments, quizzes etc.

**Staff In-charge**

**HOD**