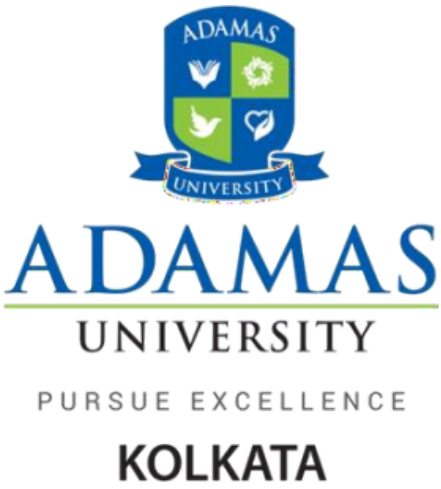


ADAMAS UNIVERSITY

SCHOOL OF ENGINEERING & TECHNOLOGY

Department of Computer Science and Engineering

MCA

Course File (THEORY)

Course Code & Name: CSE21917 &Cyber Security

Course Coordinator: Mr. Subhasish Mohapatra

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

THEORY COURSE FILE CONTENTS

Check list Course Outcomes Attainment

S. No.	Contents	Available (Y/N/NA)	Date of Submission	Signature of HOD
1.	Authenticated Syllabus Copy	Y	10-09-21	
2.	Individual Time Table	Y		
3.	Students' Name List (Approved Copy)	Y		
4.	Course Plan, PO, PSO, COs, CO-PO Mapping, COA Plan, Session Plan and Periodic Monitoring	Y		
5.	Previous Year End Semester Question Papers	Y		
6.	Question Bank (All Units - Part A, Part B & C)	Y		
7.	Dissemination of Syllabus and Course Plan to Students	Y		
8.	Lecture Notes - Unit I, II & III	Y		
9.	**Sample Documents and Evaluation Sheet for Internal Assessment** – Tutorials / Assignments / Class Test / Open Book Test / Quiz / Project / Seminar / Role Play if any (Before Mid Term)	Y	21-11-21	
10.	**Mid Term Examination** A. Question Paper / Any Other Assessment Tools Used B. Sample Answer Scripts (Best, Average, Poor) if required C. Evaluation Sheet D. Slow Learners List and Remedial Measures			
11.	Lecture Notes – Unit IV & V			
12.	**Sample Documents and Evaluation Sheet for Internal Assessment** – Tutorials / Assignments / Class Test /Open Book Test / Quiz / Project / Seminar / Role Play if any (After Mid Term)			
13.	Course End Survey (Indirect Assessment) & Consolidation			
14.	**End Term Examination** A. Question Paper & Answer Key B. Sample Answer Scripts (Best, Average, Poor) if required C. Evaluation Sheet			

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

	D. Slow Learners List and Remedial Measures.			
15.	Content Beyond the Syllabus (Proof)			
16.	Innovative Teaching Tools Used for TLP			
17.	Details of Visiting Faculty Session / Industry Expert / Guest Lecture / Seminar / Field Visit / Webinars / Flipped Class Room / Blended Learning / Online Resources etc.			
18.	Consolidated Mark Statement			
19.	CO Attainment (Mid Term + Internal Assessment + End Term)			
20.	Gap Analysis & Remedial Measures			
21.	CO - PO Attainment			
22.	Class Record (Faculty Logbook)			

Signature of HOD/ Dean **Signature of Faculty**

Date: **Date:**

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917

7. Course : Cybersecurity L: 0

8. Program : MCA T: 0

9. Target : 70% P: 3

C:3

Syllabus Copy

Course Code	CSE21917	L	T	P	C
Version 1.0		3	0	0	3
Pre-requisites/Exposure	Basic Knowledge of Cryptography				
Co-requisites					

Course Objectives

1. Describe the important computer system resources and the role of security system in their management policies and algorithms. To understand the role and responsibilities of OS in the computer system.
2. To enable student's compatibility with various security system and precision at industry.
3. To give the students a technology centric security exposure by exposing them to terminal in UNIX; and also, to enrich their knowledge.
4. To enable students, acquire knowledge in firewall security to build their expertise in this domain.

Course Content

Unit I **[9 lecture hours]**

Systems Vulnerability Scanning: Open Port / Service Identification, Banner / Version Check, Traffic Probe, Vulnerability Probe, Vulnerability Examples, OpenVAS, Metasploit.

Networks Vulnerability Scanning: Netcat, Socat, understanding Port and Services tools - Datapipe, Fpipe, WinRelay, Network Reconnaissance – N map, THC-A map and System tools. **Network Sniffers and Injection tools:** Tcp dump and Win dump, Wireshark, Ettercap

Unit II: **[9 lecture hours]**

Network Protection tools : Firewalls and Packet Filters, Firewall Basics, Comparison between Packet Filter and Firewall, Protection mechanism of Firewall, Packet Characteristic to Filter, Stateless and Stateful Firewalls, Network Address Translation (NAT) and Port Forwarding, the basic of Virtual Private Networks, Linux Firewall, Windows Firewall, Snort - Network Intrusion Detection and Prevention System (Links to an external site.)

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

Unit III **[9 lecture hours]**

Protection tools against web vulnerabilities: Nikto, W3af, HTTP utilities - Curl, OpenSSL and Stunnel, Application Inspection tools – Zed Attack Proxy, Sql map, Damn Vulnerable Web App (DVWA), Webgoat

Password Cracking and Brute-Force Tools: John the Ripper, L0htcrack, Pwdump, HTC-Hydra

Unit IV: **[9 lecture hours]**

Cyber Crime and law: Cyber Crimes, Types of Cybercrime, Hacking, Attack vectors, Cyberspace and Criminal Behavior, Clarification of Terms, Traditional Problems Associated with Computer Crime, Introduction to Incident Response, Digital Forensics, Computer Language, Network Language, Realms of the Cyber world, A Brief History of the Internet, Recognizing and Defining Computer Crime, Contemporary Crimes, Computers as Targets, Contaminants and Destruction of Data, Indian IT ACT 2000. 10

Unit V: **[9 lecture hours]**

Cyber Crime Investigation : Firewalls and Packet Filters, password Cracking, Keyloggers and Spyware, Virus and Warms, Trojan and backdoors, Steganography, DOS and DDOS attack, SQL injection, Buffer Overflow, Attack on wireless Networks

Text Books:

1.“Anti-Hacker Tool Kit (Indian Edition)”, Mike Shema, Publication McGraw Hill

2." Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives”, Nina Godbole and SunitBelpure, Publication Wiley

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917
7. Course : Cybersecurity L: 0
8. Program : MCA T: 0
9. Target : 70% P: 3

C:3

Faculty Individual Time Table

ADAMAS UNIVERSITY, KOLKATA
SCHOOL OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF CSE
Programme:MCA
Course Code & Course: CSE21917, Cyber Security Faculty Coordinator: Subhasish Mohapatra

Day & Time	10.30 - 11.20	11.20 - 12.10	12.10 - 01.00	01.00 - 01.50	01.50 - 02.40	02.40 - 03.30	03.30 - 04.20	04.20 - 05.10
Monday	-			LUNCH				
Tuesday	-		Cyber security					
Wednesday	Cyber security				-			
Thursday	-				-			-
Friday	Cyber security	-	-		-			

Signature of HOD

Date:

Signature of Class Coordinator

Date:

Students Name List

Roll Number	Registration Number	Name of the Student
PG/02/MCA/2020/001	AU/2020/0004456	NAMRATA SAMANTA

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

PG/02/MCA/2020/012	AU/2020/0004603	Tanmoy Adhikary
PG/02/MCA/2020/003	AU/2020/0004545	Deepika Barua
PG/02/MCA/2020/006	AU/2020/0004585	Oliva Roy
PG/02/MCA/2020/009	AU/2020/0004594	Ankit Kumar shah
PG/02/MCA/2020/002	AU/2020/0004534	SAYANI DAS
PG/02/MCA/2020/007	AU/2020/0004590	Ujjal Dey Sarkar
PG/02/MCA/2020/011	AU/2020/0004602	suraj agarwal
PG/02/MCA/2020/010	AU/2020/0004599	soham Das
PG/02/MCA/2020/004	AU/2020/0004551	J SAGAR SINGH
PG/02/MCA/2020/005	AU/2020/0004573	Santanu Soo
PG/02/MCA/2020/008	AU/2020/0004592	Sumita Choubey

Signature of HOD/Dean **Signature of Class Coordinator**

Date: **Date:**

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

Mapping between COs and POs		
	Course Outcomes (COs)	**Mapped Program Outcomes**
CO1	Understand the requirement of security in real life.	**PO10,PO2,PO3,PO5, PO8,PO10**
CO2	Communicate with proper security allocation policies.	**PO10, PO2,PO3,PO5, PO8,PO10,PO12**
CO3	Read the text, comprehend and make use of security tool in UNIX terminal .	**PO12, PO2,PO3,PO5,PO8,PO10**
CO4	Effectively analyse sniffing and cyber security management policies in security domain.	**PO12, PO8,PO10**

1=weakly mapped
2= moderately mapped
3=strongly mapped

COURSE PLAN

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

Target	60% (marks)
Level-1	50% (population)
Level-2	60% (population)
Level-3	70% (population)

1. Method of Evaluation

UG	**PG**
Internal Assessment (30%) (Quizzes/Tests, Assignments & Seminars etc.)	Internal Assessment (30%) (Quizzes/Tests, Assignments & Seminars etc.)
Mid Semester Examination (20%)	Mid Semester Examination (20%)
End Semester Examination (50%)	End Semester Examination (50%)

*Keep as per Program (UG/PG)

2. Passing Criteria

Scale	**PG**	**UG**
Out of 10 Point Scale	CGPA – "5.00" Min. Individual Course Grade – "C" Passing Minimum – 40	CGPA – "5.00" Min. Individual Course Grade – "C" Passing Minimum – 35

*Keep as per Program (UG/PG)

3. Pedagogy

- **Direct Instruction**
- Kinesthetic Learning
- **Flipped Classroom**
- Differentiated Instruction
- Expeditionary Learning
- Inquiry Based Learning
- Game Based Learning
- Personalized Learning

4. Topics introduced for the first time in the program through this course

- (New Topics Related to this Course – Syllabus Revision if any/Content Beyond Syllabus)

5. References:

Text Books	Web Resources	Journals	Reference Books
1	NA	NA	1

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917
7. Course : Cybersecurity L: 0
8. Program : MCA T: 0
9. Target : 70% P: 3

C:3

Signature of HOD/Dean

Date:

Signature of Faculty

Date:

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

GUIDELINES TO STUDY THE SUBJECT

Instructions to Students:

1. Go through the 'Syllabus' in the LMS in order to find out the Reading List.
2. Get your schedule and try to pace your studies as close to the timeline as possible.
3. Get your on-line lecture notes (Content, videos) at Lecture Notes section. These are our lecture notes. Make sure you use them during this course.
4. check your LMS regularly
5. go through study material
6. check mails and announcements on blackboard
7. keep updated with the posts, assignments and examinations which shall be conducted on the blackboard
8. Be regular, so that you do not suffer in any way
9. C**ell Phones and other Electronic Communication Devices:** Cell phones and other electronic communication devices (such as Blackberries/Laptops) are not permitted in classes during Tests or the Mid/Final Examination. Such devices MUST be turned off in the class room.
10. **E-Mail and online learning tool:** Each student in the class should have an e-mail id and a pass word to access the LMS system regularly. Regularly, important information – Date of conducting class tests, guest lectures, via online learning tool. The best way to arrange meetings with us or ask specific questions is by email and prior appointment. All the assignments preferably should be uploaded on online learning tool. Various research papers/reference material will be mailed/uploaded on online learning platform time to time.
11. **Attendance:** Students are required to have minimum attendance of 75% in each subject. Students with less than said percentage shall NOT be allowed to appear in the end semester examination.

This much should be enough to get you organized and on your way to having a great semester! If you need us for anything, send your feedback through e-mail XXX@adamasuniversity.ac.in Please use an appropriate subject line to indicate your message details.

There will no doubt be many more activities in the coming weeks. So, to keep up to date with all the latest developments, please keep visiting this website regularly.

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

RELATED OUTCOMES

1. **The expected outcomes of the Program are:**

PO1	Engineering Knowledge
PO2	Problem analysis
PO3	Design/development of solutions
PO4	Conduct investigation of complex problem
PO5	Modern tool usage
PO6	The engineer and society
PO7	Environment and sustainability
PO8	Ethics
PO9	Individual or Team work
PO10	Communication
PO11	Project management and finance
PO12	Life long learning

2. **The expected outcomes of the Specific Program are: (up to 3)**

PSO1	Adequate strong skills in learning new programming environments analyze and design algorithms for efficient computer-based systems of varying complexity.
PSO2	The ability to understand the evolutionary changes in computing, apply standard practices and strategies in software project development using open-ended programming environments to deliver a quality product for business success, real world problems and meet the challenges of the future.
PSO3	Ability to analyze the impact of Computer Science and Engineering solutions in the societal and human context, design, model, develop, test and manage complex software and information management systems.

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

3. **The expected outcomes of the Course are: (minimum 4 and maximum 6)**

CO1	Understand the requirement of security in real life.
CO2	Communicate with proper security allocation policies.
CO3	Read the text, comprehend and make use of security tool in UNIX terminal while shell programming.
CO4	Effectively analyse sniffing and cyber security management policies in security domain.
CO5	
etc.	

4. Co-Relationship Matrix

Indicate the relationships by 1- Slight (Low) 2- Moderate (Medium) 3-Substantial (High)

Program Outcomes / Course Outcomes	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO12	PSO 1	PSO 2	PSO 3
CO1	3	3	1					2	2	3					
CO2	3	3	1					2	2	3					
CO3	3	3						2	2	3					
CO4			1					2	2	3					
CO5	3	3													
etc.															
Average	**3**	**3**	**1**					**2**	**2**	**3**					

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

5. **Course Outcomes Assessment Plan (COA):**

Course Outcomes	Internal Assessment* (30 Marks)		Mid Term Exam (20 Marks)	End Term Exam (50 Marks)	Total (100 Marks)
	Before Mid Term	After Mid Term			
CO1	5	NA	7	8	20
CO2	5	NA	7	8	20
CO3	3	3	6	8	20
CO4	NA	7	NA	13	20
CO5	NA	7	NA	13	20
etc.					
Total	13	17	20	50	100

* Internal Assessment – Tools Used: Tutorial, Assignment, Seminar, Class Test etc.

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

OVERVIEW OF COURSE PLAN OF COURSE COVERAGE

Course Activities:

S. No.	Description	Planned			Actual			Remarks
		From	To	No. of Session	From	TO	No. of Session	
1.	Basic Concepts of security	11.09.2021	25.9. 2021	4	11.09.2021	25.9. 2021	4	Completed As per Plan
2.	Basics of Security tool	28.9. 2021	02.10. 2021	10	28.9. 2021	02.10. 2021	10	Completed As per Plan
3.	Firewall Management	12.10. 2021	24.10.2020	10	12.10. 2021	24.10.2020	10	Completed As per Plan
4.	MTM IPX,PP2P,tunneling	25.10. 2021	25.11.2021	17	25.10. 2021	25.11.2021	17	Completed As per Plan
5.	Overview Of Cyber security policy	28.11.2021	15.01.2022	4	28.11.2021	15.01.2022	4	Completed As per Plan

Total No. of Instructional periods available for the course: _____ Sessions

Signature of HOD/Dean **Signature of Faculty**

Date: **Date:**

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

SESSION PLAN

Session Plan				Actual Delivery			
Lect.	Date	Topics to be Covered	CO Mapped	Lect.	Date	Topics Covered	CO Achieved
1	11-09-21	Introduction to security	CO1	1	11-09-21	Introduction to security	CO1
2	13-09-21	Generation of Security aspect	CO1	2	13-09-21	Generation of Security aspect	CO1
3	16-09-21	Introduction to security vulnerability	CO1	3	16-09-21	Introduction to security vulnerability	CO1
4	5-10-21	Introduction to System Calls	CO1	4	5-10-21	Introduction to System Calls	CO1
5	7-10-21	Network vulnerability overview	CO1	5	7-10-21	Network vulnerability overview	CO1
6	11-10-21	Structure of Vulnerabilty	CO1	6	11-10-21	Structure of Vulnerabilty	CO1
7	14-10-21	N-MAP,THC in fundamental	CO1	7	14-10-21	N-MAP,THC in fundamental	CO1
8	15-10-21	Data pipe and F-pipe	CO1	8	15-10-21	Data pipe and F-pipe	CO1
9	16-10-21	Brief overview of Injection tool	CO1	9	16-10-21	Brief overview of Injection tool	CO1

UNIT-I

Remarks: **Signature of Faculty**

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

Date:

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

SESSION PLAN
UNIT-II

Session Plan				Actual Delivery			
Lect.	Date	Topics to be Covered	CO Mapped	Lect.	Date	Topics Covered	CO Achieved
1	17-10-21	Firewall and Process	CO2	10	17-10-21	Firewall and Process	CO2
2	18-10-21	Relationship, Different states of firewall	CO2	11	18-10-21	Relationship, Different states of firewall	CO2
3	21-10-21	State transition of firewall.	CO2	12	21-10-21	State transition of firewall.	CO2
4	22-10-21	Process security Context switching	CO2	13	22-10-21	Process security Context switching	CO2
5	23-10-21	Definition, Network Address Translation (NAT) ,Packet forwarding	CO2	14	23-10-21	Definition, Network Address Translation (NAT) ,Packet forwarding	CO2
6	29-10-21	Types of sniffers	CO2	15	29-10-21	Types of sniffers	CO2
7	2-11-21	Foundation and Scheduling objectives, Types of Schedulers, Scheduling	CO2	16	2-11-21	Foundation and Scheduling objectives, Types of Schedulers, Scheduling	CO2
8	4-11-21	Intrusion detection process	CO2	17	4-11-21	Intrusion detection process	CO2
9	6-11-21	Pre-emptive and Non pre-emptive, FCFS, SJF, RR; Multiprocessor Types and performance evaluation	CO3	18	6-11-21	Pre-emptive and Non pre-emptive, FCFS, SJF, RR; Multiprocessor	CO3

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

						scheduling: Types and performance evaluation	

Remarks:

Signature of Faculty

Date:

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

SESSION PLAN
UNIT-III

Session Plan				Actual Delivery			
Lect.	Date	Topics to be Covered	CO Mapped	Lect.	Date	Topics Covered	CO Achieved
1	6-11-21	Classical Nikto	CO3	19	6-11-21	Classical Nikto	CO3
2	7-11-21	DefinitionW3af	CO3	20	7-11-21	DefinitionW3af	CO3
3	10-11-21	HTTP and SSH/SSL	CO3	21	10-11-21	HTTP and SSH/SSL	CO3
4	11-11-21	Overview of Proxy,SQL map	CO3	22	11-11-21	Overview of Proxy,SQL map	CO3
5	14-11-21	Basics – Hardware And Control Structures in Proxy	CO3	23	14-11-21	Basics – Hardware And Control Structures in Proxy	CO3
6	18-11-21	Definition of RIPPER	CO3	24	18-11-21	Definition of RIPPER	CO3
7	22-11-21	Definition of Pwdump	CO3	25	22-11-21	Definition of Pwdump	CO3
8	24-11-21	Definition of HTC Hydra	CO3	26	24-11-21	Definition of HTC Hydra	CO3
9	25-05-21	ZED a ZED attack and webgoat ttack and webgoat	CO3	27	25-05-21	ZED a ZED attack and webgoat ttack and webgoat	CO3

Remarks:

Signature of Faculty

Date:

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

SESSION PLAN
UNIT-IV

Session Plan				Actual Delivery			
Lect.	Date	Topics to be Covered	CO Mapped	Lect.	Date	Topics Covered	CO Achieved
1	2-12-21	**Principles Of I/O Cyber crime**	CO4	28	2-12-21	**Principles Of I/O Cyber crime**	CO4
2	4-12-21	Computer crime	CO4	29	4-12-21	Computer crime	CO4
3	7-12-21	History of cyber crime	CO4	30	7-12-21	History of cyber crime	CO4
4	12-12-21	Digital Forensics, Computer Language, Network Langua	CO4	31	12-12-21	Digital Forensics, Computer Language, Network Langua	CO4
5	15-12-21	. Computer Language, Network Langua	CO4	32	15-12-21	. Computer Language, Network Langua	CO4
6	24-12-21	Doubt clearing	CO4	33	24-12-21	Doubt clearing	CO4
7	25-12-21	Contemporary Crimes,	CO4	34	25-12-21	Contemporary Crimes,	CO4

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

8	28-6-21	Computers as Targets, Contaminants	CO4	35	28-6-21	Computers as Targets, Contaminants	CO4
9	3-1-22	**Principles Of I/O IT Act of India**	CO4	36	3-1-22	**Principles Of I/O IT Act of India**	CO4

Remarks: **Signature of Faculty**

Date:

SESSION PLAN
UNIT-V

Session Plan				Actual Delivery			
Lect.	Date	Topics to be Covered	CO Mapped	Lect.	Date	Topics Covered	CO Achieved
1	5-01-22	Firewalls and Packet Filter	CO4	37	5-01-22	Firewalls and Packet Filter	CO4
2	6-01-22	Virus and Warms, Trojan and backdoors, Steganography	CO4	38	6-01-22	Virus and Warms, Trojan and backdoors, Steganography	CO4
3	13-01-22	DOS and DDOS	CO4	39	13-01-22	DOS and DDOS	CO4
4	17-01-22	Fundamental application of DDOS	CO4	40	17-01-22	Fundamental application of DDOS	CO4
5	21-01-22	Efficiency & Performance of firewall .	CO4	41	21-01-22	Efficiency & Performance of firewall .	CO4

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

6	23-01-22	Attack IN WSN	CO4	42	23-01-22	Attack IN WSN	CO4
7	24-01-22	Class test	CO4	43	24-01-22	Class test	CO4
8	25-01-22	Revision	CO4	44	25-01-22	Revision	
9	26-01-22	Revision	CO4	45	26-01-22	Revision	

Remarks:

Signature of Faculty

Date:

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917
7. Course : Cybersecurity L: 0
8. Program : MCA T: 0
9. Target : 70% P: 3

C:3

PERIODIC MONITORING

Actual date of completion and remarks, if any

Components		From	To	From	To
Duration (Mention from and to Dates)		From	To	From	To
Percentage of Syllabus covered		01.09.2021	08.11.2021	18.11.2021	17.01.2022
Lectures	100%	Revision			
	45	13(New students)			
Tutorials	1	45	46	58	
	NA				
Test/Quizzes/ Mid Semester/ End Semester	Planned				
	1(MID)	1	1 (END)		
	1	1	1		
	CO1 & CO2	CO3 & CO4	CO5		
Assignments	CO1	CO2	CO3 & CO4	CO5	
	1	1 (MID)	1	1(END)	
	1	1	1	1	
	CO1	CO2	CO3 & CO4	CO5	
Signature of Faculty		CO1		CO2	
Head of the Department		From		To	
OBE Coordinator		01.09.2021		08.01.2022	

Signature of HOD/ Dean

Date

Signature of Faculty

Date

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra Course Code: CSE21917

2Course : Cybersecurity L: 0

3.Program : MCA T: 0

4.Target : 70% P: 3

C:3

PERIODIC MONITORING

Attainment of the Course (Learning) Outcomes:

Components	Attainment level	Action Plan	Remarks
Assignment	CO1:	Submission Target 11.09.2021	Assignment Questions based on CO1
	CO2:	Submission Target 06.10.2021	Assignment Questions based on CO2
	CO3:	Submission Target 08.11.2021	Assignment Questions based on CO3,CO4
	CO4:		
	CO5:	Submission Target 19.11.2021	Assignment Questions based on CO5
Quiz/Test etc.	CO1:	Conducted on 11.12.2020	Based on CO1and CO2
	CO2:		
	CO3:	Conducted on 08-12-2021	Based on CO3, CO4 and CO5
	CO4:		
	CO5:		
Mid Semester	CO1:	Scheduled on 11.12.2021 – 16.12.2021	Study Materials are provided to the students based on CO1& CO2.
	CO2:		
	CO3:	NA	NA
	CO4:	NA	NA
	CO5:	NA	NA
End Semester	CO1:	Scheduled on 08.01.2022-22.01.22	Study Materials are provided to the students based on CO1, CO2, CO3, CO4 &CO5.

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917
7. Course : Cybersecurity L: 0
8. Program : MCA T: 0
9. Target : 70% P: 3

C:3

	CO2:		
	CO3:		
	CO4:		
	CO5:		
Any Other	CO1:	Submission Target 11.05.2021	Assignment Questions based on CO1
	CO2:	Submission Target 06.06.2021	Assignment Questions based on CO2
	CO3:	Submission Target 08.01.2022	Assignment Questions based on CO3,CO4
	CO4:		
	CO5:	Submission Target 19.01.2022	Assignment Questions based on CO5

Signature of HOD/ Dean

Date

Signature of Faculty

Date

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

Previous Year Question Papers – Set 1

ADAMAS UNIVERSITY
SCHOOL OF ENGINEERING AND TECHNOLOGY

END-SEMESTER EXAMINATION: JULY 2020

Name of the Program: MCA Semester: III Stream: CSE
PAPER TITLE: Cyber Security PAPER CODE: CSE21917
Maximum Marks: 50 Time duration: 3 hours
Total No of questions: 12 Total No of Pages: 01

Instruction for the Candidate:

1. At top sheet, clearly mention Name, Univ. Roll No., Enrolment No., Paper Name & Code, and Date of Exam.
2. All parts of a Question should be answered consecutively. Each Answer should start from a fresh page.
3. Assumptions made if any, should be stated clearly at the beginning of your answer.

Section A (Answer All the Questions) (5 x 2 = 10)			
1.	**Describe** the OpenSSL and Stunnel.	**U**	**CO1**
2.	**Explain** the HTC-Hydra. .	**Evaluate**	**CO1**
3.	**Describe** Cyber Crimes.	**U**	**CO1**
4.	**Explain** Digital Forensics.	**Evaluate**	**CO2**
5.	**Describe** Contaminants and Destruction of Data.	**U**	**CO2**

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

	SECTION B (Attempt any **Three Questions) (3 x 5 = 15)**		
6.	**Write** Firewalls and Packet Filters.	**Ap**	**CO1**
7.	**Examine** Steganography.	**Ap**	**CO2**
8.	**Describe** DOS and DDOS attack.	**U**	**CO6**
9.	**Describe** with Example: i) XSS attack ii) SQL injection.	**U**	**CO3, CO5**
	SECTION C (Answer Any Two Questions) (2 x 12.5 = 25)		
10.	**Write** the steps of IT assessments or audits	**Ap**	**CO2**
11.	**Write** the steps of Cross-site scripting (XSS).	**Ap**	**CO4**
12.	**Describe** SQL injection and Cross-Site Request Forgery (CSRF) in details.	**U**	**CO3**

Question Bank Sample

School: SOET **Department: CSE**

Course Code: CSE21917 **Course Name: CYBER SECURITY**

Program: MCA **Semester: III**

UNIT-I

Sl. No.	**Question**	**Level of Difficulty (Easy/ Medium/ Difficult)**	**Knowledge Level (Bloom's Taxonomy)**	**Course Outcome (CO)**
	Part A (Multiple Choice Questions) (1 mark each)			
1.	What is cyber security?	**Easy**	U	**CO1**

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

2.	What is wireless scanner?	**Medium**	**A**	**CO2**
3.	Analyze the action of cloud security	**Difficult**	**Ap**	**CO4**
	Part B (Definition/Naming Questions) (2 marks each)			
1.	Discuss end point security	**Easy**	U	**CO1**
2.	What is open port and closed port	**Medium**	R	**CO2**
3.	Give a practical analysis on open port and closed port.	**Difficult**	**An**	**CO3**
Part C (Short Questions) (3-4 marks each)				
1.	Analyse the challenges in cyber security?	**Easy**	U	**CO1**
2.	Why NETCAT is used.	**Medium**	**R**	**CO2**
3.	What is the use of win relay tool?	**Difficult**	**An**	**CO3**
Part D (Explanation Based Questions) (5 marks each)				
1.	Why etter cap is used give your under standing	**Easy**	U	**CO1**
2.	NA	**Medium**	**R**	**CO2**
3.	NA	**Difficult**	**An**	**CO3**
Part E (Questions Based on Reasoning) (5 marks each)				
1.	Apply your thought why vulnerability scanner is required now a days	**Easy**	U	**CO1**
2.	Discuss the benefit of vulnerability scanner.	**Medium**	**R**	**CO2**
3.	Give a analytical report on Open VAS.	**Difficult**	**An**	**CO3**

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

Part F (Application Based Questions) (5-10 marks each)				
1.	Discuss the role of application and database scanner.	**Easy**	U	**CO1**
2.	Discuss the need of SOCAT.	**Medium**	R	**CO2**
3.	Analyze the action of metaspoilt with suitable example.	**Difficult**	**An**	**CO3**
Part G (Short Notes) (5 marks each)				
1.	Write a short notes in TCP,UDP and SSL	**Easy**	U	**CO1**
2.	Differentiate between host and network based scanner.	**Medium**	R	**CO2**
3.	Develop a a analytical report on vulnerability scanner.	**Difficult**	**Ap**	**CO4**

School: SOET **Department: CSE**

Course Code: CSE21917 **Course Name: CYBER SECURITY**

Program: MCA **Semester: III**

UNIT-II

Sl. No.	**Question**	**Level of Difficulty (Easy/ Medium/ Difficult)**	**Knowledge Level (Bloom's Taxonomy)**	**Course Outcome (CO)**
Part A (Multiple Choice Questions) (1 mark each)				
1.	What is phishing?	**Easy**	U	**CO1**

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

2.	Why session hijacking is so disastrous?	**Medium**	R	**CO2**
3.	Discuss the role of Trojan Horse.	**Difficult**	**Ap**	**CO4**
	Part B (Definition/Naming Questions) (2 marks each)			
1.	Discuss Brute force attack	**Easy**	U	**CO1**
2.	Apply your thought in dictionary attack and how to resolve it.	**Medium**	R	**CO2**
3.	Why code injection is so disastrous discuss on it.	**Difficult**	**Ap**	**CO4**
	Part C (Short Questions) (3-4 marks each)			
1.	Write a short notes on Trojan horse,BOT and Denial service attack.	**Easy**	U	**CO1**
2.	How insider threat is taken into action by cyber criminal.	**Medium**	R	**CO2**
3.	Discuss SQL injection.	**Difficult**	**Ap**	**CO4**
	Part D (Explanation Based Questions) (5 marks each)			
1.	What is the role of hacktivist.	**Easy**	U	**CO1**
2.	Discuss mail command injection.	**Medium**	R	**CO2**
3.	Analyse cross site scripting.	**Difficult**	**Ap**	**CO4**
	Part E (Questions Based on Reasoning) (5 marks each)			
1.	How cyber crime happen by cyber criminal give a analytical report on it.	**Easy**	U	**CO1**
2.	How the application gateway direct the FTP service .	**Medium**	R	**CO2**

Year: 2
Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

3.	How FTP service is acting in application gateway suggest your answer.	**Difficult**	**Ap**	**CO4**
Part F (Application Based Questions) (5-10 marks each)				
1.	Give a analytical report on web based and system based attack	**Easy**	U	**CO1**
2.	Why firewall is used.	**Medium**	R	**CO2**
3.	Analyse the role of packet filter.	**Difficult**	**Ap**	**CO4**
Part G (Short Notes) (5 marks each)				
1.	Describe LDAP injection.	**Easy**	U	**CO1**
2.	How to prevent Injection attack.	**Medium**	R	**CO2**
3.	Describe mail command injection.	**Difficult**	**Ap**	**CO4**

School: SOET **Department: CSE**
Course Code: CSE21917 **Course Name: CYBER SECURITY**
Program: MCA **Semester: III**

UNIT-III

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

Sl. No.	Question	Level of Difficulty (Easy/ Medium/ Difficult)	Knowledge Level (Bloom's Taxonomy)	Course Outcome (CO)
Part A (Multiple Choice Questions) (1 mark each)				
1.	What is open access in firewall	**Easy**	U	**CO1**
2.	Difference between HTTP and HTTPS	**Medium**	R	**CO2**
3.	What is the usage of port number ?	**Difficult**	**Ap**	**CO4**
	Part B (Definition/Naming Questions) (2 marks each)			
1.	What is stateful firewall.	**Easy**	U	**CO1**
2.	What is state less firewall.	**Medium**	R	**CO2**
3.	Discuss John the Ripper, L0htcrack,	**Difficult**	**Ap**	**CO4**
Part C (Short Questions) (3-4 marks each)				
1.	What is the role of NAT	**Easy**	U	**CO1**
2.	Describe Pwdump,	**Medium**	R	**CO2**
3.	What is the role of HTC-Hydra	**Difficult**	**Ap**	**CO4**
Part D (Explanation Based Questions) (5 marks each)				
1.	Firewall is a hardware or software suggest your answer.	**Easy**	U	**CO1**
2.	How to write a firewall rule give a pictorial representation on It.	**Medium**	R	**CO2**

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

3.	Difference between stateful and state less firewall	**Difficult**	**Ap**	**CO4**
Part E (Questions Based on Reasoning) (5 marks each)				
1.	Differentiate between Curl, and stunnel	**Easy**	U	**CO1**
2.	Analyze the role of OpenSSL	**Medium**	R	**CO2**
3.	Write a short note on win dump and TCP dump.	**Difficult**	**Ap**	**CO4**
Part F (Application Based Questions) (5-10 marks each)				
1.	How firewall works give a step by step procedure on it.	**Easy**	U	**CO1**
2.	Discuss the Pros and Cons of Stateful vs. Stateless Firewalls	**Medium**	R	**CO2**
3.	How NAT is working.	**Difficult**	**Ap**	**CO4**
Part G (Short Notes) (5 marks each)				
1.	Analyze the action of Damn Vulnerable Web App (DVWA), Webgoat.	**Easy**	U	**CO1**
2.	Write a short note on Zed Attack Proxy, Sql map.	**Medium**	R	**CO2**
3.	Discuss network intrusion detection and prevention system.	**Difficult**	**Ap**	**CO4**

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

School: SOET **Department: CSE**
Course Code: CSE21917 **Course Name: CYBER SECURITY**
Program: MCA **Semester: III**

UNIT-IV

Sl. No.	Question	Level of Difficulty (Easy/ Medium/ Difficult)	Knowledge Level (Bloom's Taxonomy)	Course Outcome (CO)
	Part A (Multiple Choice Questions) (1 mark each)			
1.	What is DOS attack	**Easy**	U	**CO1**
2.	Difference between TCP and HTTPS	**Medium**	R	**CO2**
3.	What is the usage of cyber stalking?	**Difficult**	**Ap**	**CO4**
	Part B (Definition/Naming Questions) (2 marks each)			
1.	What is social networking.	**Easy**	U	**CO1**
2.	What is s.	**Medium**	R	**CO2**
3.	Discuss John the Ripper, L0htcrack,	**Difficult**	**AN**	**CO3**
	Part C (Short Questions) (3-4 marks each)			
1.	What is the role of NAT	**Easy**	U	**CO1**

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

2.	Describe Pwdump,	**Medium**	R	**CO2**
3.	What is the role of HTC-Hydra	**Difficult**	**AN**	**CO3**
Part D (Explanation Based Questions) (5 marks each)				
1.	Explain section 66 and 67 in ITA 2000.	**Easy**	U	**CO1**
2.	How to write a firewall rule give a pictorial representation on It.	**Medium**	R	**CO2**
3.	Difference between data destruction technique in HDD and SDD.	**Difficult**	**AN**	**CO3**
Part E (Questions Based on Reasoning) (5 marks each)				
1.	Discuss ITA 2000 act.	**Easy**	U	**CO1**
2.	Analyze the action of digital forensic	**Medium**	R	**CO2**
3.	Write a short note on win dump and TCP dump.	**Difficult**	**AN**	**CO3**
Part F (Application Based Questions) (5-10 marks each)				
1.	How cyber security aware ness mitigate cyber crime suggest your answer..	**Easy**	U	**CO1**
2.	Discuss the Pros and Cons of customer data theft vs. DOS attack	**Medium**	R	**CO2**
3.	Explain most common attack vector.	**Difficult**	**AN**	**CO3**
Part G (Short Notes) (5 marks each)				
1.	Analyze the action of incident response.	**Easy**	U	**CO1**
2.	Write a short note on CIRT team.	**Medium**	R	**CO2**
3.	Discuss the mitigation and detection of incident response.	**Difficult**	**AN**	**CO3**

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

Lecture Notes – Sample

UNIT I

What is Cyber security?

A DEFINITION OF CYBER SECURITY

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.

THE IMPORTANCE OF CYBER SECURITY

Cyber security (Links to an external site.) is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the **volume and sophistication of cyber attacks grow** (Links to an external site.), companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to

protect their sensitive business and personnel information. As early as March 2013, the nation's top intelligence officials cautioned that cyber attacks and digital spying are the top threat to national security, eclipsing even terrorism.

CHALLENGES OF CYBER SECURITY

For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system. **Elements of cyber** (Links to an external site.) encompass all of the following:

- **Network security:** The process of protecting the network from unwanted users, attacks and intrusions.
- **Application security:** Apps require constant updates and testing to ensure these programs are secure from attacks.
- **Endpoint security:** Remote access is a necessary part of business, but can also be a weak point for data. Endpoint security (Links to an external site.) is the process of protecting remote access to a company's network.
- **Data security** (Links to an external site.)**:** Inside of networks and applications is data. Protecting company and customer information is a separate layer of security.
- **Identity management:** Essentially, this is a process of understanding the access every individual has in an organization.
- **Database and infrastructure security:** Everything in a network involves databases and physical equipment. Protecting these devices is equally important.
- **Cloud security:** Many files are in digital environments or "the cloud". Protecting data in a 100% online environment presents a large amount of challenges.
- **Mobile security:** Cell phones and tablets involve virtually every type of security challenge in and of themselves.
- **Disaster recovery/business continuity planning:** In the event of a breach (Links to an external site.), natural disaster or other event data must be protected and business must go on. For this, you'll need a plan.End-user education: Users may be employees accessing the network or customers logging on to a company app. Educating good habits (password changes, 2-factor authentication, etc.) is an important part of cybersecurity.

The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known treats.

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

Analytical report on vulnerability scanners

What are vulnerability scanners

A vulnerability scanner is an automated tool that identifies and creates an inventory of all IT assets (including servers, desktops, laptops, virtual machines, containers, firewalls, switches, and printers) connected to a network. For each asset, it also attempts to identify operational details such as the operating system it runs and the software installed on it, along with other attributes such as open ports and user accounts. A vulnerability scanner enables organizations to monitor their networks, systems, and applications for security vulnerabilities.

Most security teams utilize vulnerability scanners to bring to light security vulnerabilities in their computer systems, networks, applications and procedures. There are a plethora of vulnerability scanning tools available, each offering a unique combination of capabilities.

Leading vulnerability scanners provide users with information about:

1. Weaknesses in their environment
2. Insights into degrees of risk from each vulnerability
3. Recommendations on how to mitigate the vulnerability

Five types of vulnerability scanners

Vulnerability scanners can be categorized into 5 types based on the type of assets they scan.

Details of five types of vulnerability assessment scanners – 1. network based scanners 2. Host bases scanners 3. Wireless scanners 4. Applications scanners, and 5. Database scanners

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917

7. Course : Cybersecurity L: 0

8. Program : MCA T: 0

9. Target : 70% P: 3

C:3

1. Network-based scanners

Network based vulnerability scanners identify possible network security attacks and vulnerable systems on wired or wireless networks. Network-based scanners discover unknown or unauthorized devices and systems on a network, help determine if there are unknown perimeter points on the network, such as unauthorized remote access servers, or connections to insecure networks of business partners.

2. Host-based scanners

Host based vulnerability scanners are used to locate and identify vulnerabilities in servers, workstations, or other network hosts, and provide greater visibility into the configuration settings and patch history of scanned systems. Host-based vulnerability assessment tools can also provide an insight into the potential damage that can be done by insiders and outsiders once some level of access is granted or taken on a system.

3. Wireless scanners

Wireless vulnerability scanners are used to identify rogue access points and also validate that a company's network is securely configured.

4. Application scanners

Applications vulnerability scanners test websites in order to detect known software vulnerabilities and erroneous configurations in network or web applications.

5. Database scanners

Database vulnerability scanners identify the weak points in a database so as to prevent malicious attacks

What is an open port?

Open port means either a TCP or a UDP port number is actively accepting packets. If a service runs on a specific port, that port is utilised and can't be used for other purposes (by another service). For example, you can run a website using an Apache web server on port 80/TCP. In contrast, a port that rejects or ignores the connection attempts is called a closed port.

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

A port can have three different port states. Open port scanners work on the same underlying concept to assess which ports are open, filtered or closed. The following are the different port states based on responses:

- **Open Port:** An application is actively accepting connections on this port that serve port scans' primary goal.
- **Closed Port:** A port is accessible, but no application is listening to it. Administrators should block such ports at the firewall level, which could be exploited in an already exploited situation where an attacker has compromised another system. This closed port can then be used as an outbound port traversing across the firewall.

Importance of port scanning

Port scanning techniques are used to check for open ports. These are performed using utilities known as port scanners that attempt connections to TCP/UDP ports. However, certain online open port scanner (Links to an external site.) websites are available to check if a port is open/closed. It is important to port scan to find the exposed attack surface of an asset.

Open ports in windows differ from open ports in Linux due to the way operating systems function. This is also one indicator during port scans to identify what operating system is in use and likely guesses the underlying architecture. For standard services such as web servers, it is already known that the port is open by browsing a website address using HTTP or HTTPS prefixes. HTTP and HTTPS (HTTP over SSL/TLS) services utilise standard ports 80 and 443; they can be configured on another port. Other standard port numbers include FTP service running on 21/TCP, SMTP server uses 25/TCP, SSH runs on 22/TCP, IMAP/POP3, and other services utilise their standards ports. For example, the OpenVPN port used for VPN connection and traffic transfers is 443. When it comes to protocols, OpenVPN uses UDP by default and TCP as the second choice.

Usage of Network Probe

Network Probe

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917

7. Course : Cybersecurity L: 0

8. Program : MCA T: 0

9. Target : 70% P: 3

C:3

REFINE YOUR IDEA IN NETWORK PROBE (Links to an external site.)
Do you know what's really traveling through your network (Links to an external site.)? Are you having problems finding the sources of network slowdowns?

Network Probe is the ultimate network monitor and protocol analyzer to monitor network traffic in real-time, and will help you find the sources of any network slow-downs in a matter of seconds.

Collect and analyze data from multiple probes using the Network Probe Enterprise (Links to an external site.) version for a total traffic overview of all your networks. Network Probe will show you which protocols are being used on your network, which hosts are sending and receiving data, where the traffic is coming from, and when all this happens. Configure Network Probe to notify you if anything out of the ordinary happens and proactively fix the problem before it grows into a serious one. Instantly get an overview of the throughput of the network being monitored and the number of hosts, conversations, and protocols seen on the network.

A vulnerability scanner is a software application that can be used to find security weaknesses in computers, networks, operating systems and other software applications. It's important to note that the same tool can be used proactively by system administrators and maliciously by cyber attackers. Therefore, it is essential for an organization to identify and remedy any areas of exposure before a hacker can exploit them and gain unauthorized access to critical data.

Types of vulnerability scanners

Vulnerability scanners can range in complexity from free, open-source tools to highly sophisticated enterprise-level systems. Some types include:

- Port scanners – Software applications that probe a server or host for open network ports
- Network enumerators – Programs that retrieve information about users and groups on networked computers
- Network vulnerability scanners – Systems that proactively scan for network vulnerabilities
- Web application security scanners – Programs that communicate with web applications to detect areas of exposure
- Computer worms – Self-replicating computer malware that can be used to find weak points

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

Benefits of vulnerability scanners

Vulnerability scanning can provide an organization with several key benefits, including:

- Early detection of security threats – Ongoing security assessments make it easier to identify and address vulnerabilities, both from an internal and an external perspective.
- Prompt discovery of unauthorized devices – A new device or system can potentially connect to a network without proper authorization. A vulnerability scanner can identify rogue machines that may threaten system security.
- Current verification of network device inventory – Vulnerability scanning can identify all devices on a network by device type, hardware configuration, operating system, patch level and other information.

A possible downside of vulnerability scanning is that it may inadvertently cause a system to crash if a potential threat is detected during a scan. For this reason, vulnerability scanning is typically scheduled outside of regular business hours. Additionally, because a scan result provides only a "snapshot in time" and new threats can emerge at any time, scanning must be performed on an ongoing basis to be fully effective.

OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated and authenticated testing, various high-level and low-level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.
The scanner obtains the tests for detecting vulnerabilities from a feed (Links to an external site.) that has a long history and daily updates.
OpenVAS has been developed and driven forward by the company Greenbone Networks (Links to an external site.) since 2006. As part of the commercial vulnerability management product family "Greenbone Security Manager" (GSM), the scanner forms the Greenbone Vulnerability Management (Links to an external site.) together with other Open Source modules.

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917

7. Course : Cybersecurity L: 0

8. Program : MCA T: 0

9. Target : 70% P: 3

C:3

Metasploit Framework (MSF)

WHAT IS METASPLOIT?

What is the role of security auditing tool Visit this LinK

https://youtu.be/P5tPx6AnyV8 (Links to an external site.)

The Metasploit Framework (Links to an external site.) (MSF) is far more than just a collection of exploits–it is also a solid foundation that you can build upon and easily customize to meet your needs. This allows you to concentrate on your unique target environment and not have to reinvent the wheel. We consider the MSF to be one of the single most useful security auditing tools freely available to security professionals today. From a wide array of commercial grade exploits and an extensive exploit development environment, all the way to network information gathering tools and web vulnerability plugins, the Metasploit Framework provides a truly impressive work environment.

This course has been written in a manner to encompass not only the front end "user" aspects of the framework, but rather give you an introduction to the capabilities that Metasploit provides. We aim to give you an in-depth look into the many features of Metasploit and provide you with the skills and confidence to take advantage of this amazing tool.

Ncat is a feature-packed networking utility which reads and writes data across networks from the command line. Ncat was written for the Nmap Project as a much-improved reimplementation of the venerable Netcat (Links to an external site.). It uses both TCP and UDP for communication and is designed to be a reliable back-end tool to instantly provide network connectivity to other applications and users. Ncat will not only work with IPv4 and IPv6 but provides the user with a virtually limitless number of potential uses.

Among Ncat's vast number of features there is the ability to chain Ncats together, redirect both TCP and UDP ports to other sites, SSL support, and proxy connections via SOCKS4 or HTTP (CONNECT method) proxies (with optional proxy authentication as well). Some general principles apply to most applications and thus give you the capability of instantly adding networking support to software that would normally never support it.

The socat (Links to an external site.) utility is a relay for bidirectional data transfers between two independent data channels.

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

There are many different types of channels socat can connect, including:

- Files
- Pipes
- Devices (serial line, pseudo-terminal, etc)
- Sockets (UNIX, IP4, IP6 - raw, UDP, TCP)
- SSL sockets
- Proxy CONNECT connections
- File descriptors (stdin, etc)
- The GNU line editor (readline)
- Programs
- Combinations of two of these

This tool is regarded as the advanced version of netcat (Links to an external site.). They do similar things, but socat has more additional functionality, such as permitting multiple clients to listen on a port, or reusing connections.

Why do we need socat?

There are many ways to use socate effectively. Here are a few examples:

- TCP port forwarder (one-shot or daemon)
- External socksifier
- Tool to attack weak firewalls (security and audit)
- Shell interface to Unix sockets
- IP6 relay
- Redirect TCP-oriented programs to a serial line
- Logically connect serial lines on different computers
- Establish a relatively secure environment (su and chroot) for running client or server shell scripts with network connections

Analogy

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

If you use a house or apartment block analogy the IP address corresponds to the street address.

All of the apartments share the same street address.

However each apartment also has an apartment number which corresponds to the Port number.

Port Number Ranges and Well Known Ports

A port number uses 16 bits and so can therefore have a value from **0** to **65535** decimal

Port numbers are divided into ranges as follows:

Port numbers 0-1023 – Well known ports. These are allocated to **server services** by the **Internet Assigned Numbers Authority** (IANA). e.g Web servers normally use **port 80** and SMTP servers use **port 25** (see diagram above).

Ports 1024-49151- Registered Port -These can be registered for services with the **IANA** and should be treated as **semi-reserved.** User written programs should not use these ports.

Ports 49152-65535– These are used by **client programs** and you are free to use these in client programs. When a Web browser connects to a web server the browser will allocate itself a port in this range. Also known as **ephemeral ports**.

TCP Sockets

A connection between two computers uses a **socket.**

*A socket is the combination of **IP address plus port***

Each end of the connection will have a socket.

Imagine sitting on your PC at home, and you have two browser windows open.

One looking at the Google website, and the other at the Yahoo website.

The connection to Google would be:

Your PC – **IP1**+port 60200 ——– Google IP2 +port **80** (standard port)

The combination IP1+60200 = the socket on the client computer and **IP2 + port 80** = destination socket on the Google server.

The connection to Yahoo would be:

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

your PC – **IP1**+port 60401 ——–Yahoo IP3 +port **80** (standard port)

The combination IP1+60401 = the socket on the client computer and **IP3 + port 80** = destination socket on the Yahoo server.

Notes: **IP1** is the IP address of your PC. Client port numbers are dynamically assigned, and can be reused once the session is closed.

TCP and UDP -The Transport Layer

Note: You may find reading the article on the TCP/IP protocol suite (Links to an external site.)useful to understand the following

IP addresses are implemented at the networking layer which is the **IP layer.**

Ports are implemented at the transport layer as part of the **TCP or UDP header** as shown in the schematic below:

The TCP/IP protocol supports two types of port- **TCP Port** and **UDP Port**.

TCP – is for connection orientated applications. It has built in error checking and will re transmit missing packets.

UDP – is for connection less applications. It has no has built in error checking and **will not** re transmit missing packets.

Applications are designed to use either the UDP or TCP transport layer protocol depending on the type of connection they require.

Checking For Open Ports

Windows and Linux systems have a utility called **netstat** which will give you a list of open ports on your computer.

These articles show you how to use **netstat** on windows (Links to an external site.) and on linux (Links to an external site.).
You can check the **port status** of remote machines using a port scanner line nmap (Links to an external site.).

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917

7. Course : Cybersecurity L: 0

8. Program : MCA T: 0

9. Target : 70% P: 3

C:3

You can install NMAP on windows,Linux and Apple. It can be used with a graphical user interface of as a command line tool.

Datapipe was a provider of managed hosting services and data centers (Links to an external site.) for information technology (Links to an external site.) services and cloud computing (Links to an external site.) with

UNIT-2

WinRelay tool Overview

WinRelay is another Windows-based port-redirection tool. It and FPipe share the same features, including the ability to define a static source port for redirected traffic. Consequently, it can be used interchangeably with FPipe on any Windows platform.

Using winrelay or fpipe for port redirection via a Windows host

When attacking networks in a pentest, it is sometimes useful to be able to redirect tcp or udp traffic, via an intermediary system.

This may be to obfuscate the source of the attack, or perhaps because the victim host (ip address and port combination) is not directly accessable for the attacking machine.

This is commonly used in pivoting, i.e. to attack an initial host, and then use that compromised system to attack other systems on the network, which were not initially accessable.

Here we look at two Windows commandline tools which can be used for port redirection; winrelay and fpipe, and test them.

These techniques should only be used on your own test systems, or where you have express permittion to do penetration testing.

winrelay from ntsecurity.nu

Network Reconnaissance for Beginners

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

After gaining access to a Wi-Fi, Ethernet, or remote network, the first step for most hackers is to conduct recon to explore the network and learn more about any available targets. You may be familiar with some devices that announce themselves on a network, like other computers advertising file sharing. While this is a useful way of discovering devices on the same network as you, most devices do not advertise their presence on the network in this obvious of a fashion.

The solution to the problem of exploring a network is network scanning, made possible by programs like Nmap (Links to an external site.) and arp-scan (Links to an external site.). We're only interested in the former here, which allows for highly detailed exploration and mapping of local and remote networks, though we can use Nmap to perform an ARP scan as you'll see later on. With Nmap, you can see who is on the network, what applications or operating system a target is running, and what the available attack surface is.
To use Nmap, you'll need a system that supports it. Fortunately, Nmap is cross-platform and works on Windows (Links to an external site.), Linux (Links to an external site.), and macOS (Links to an external site.), and comes preinstalled on many systems. If you don't have it, it's easy to install (Links to an external site.).

You'll also need a network to connect to and scan to try these techniques, but be aware that scanning is often seen as a prelude to an attack and may be met with increased scrutiny. What this means is that if you have a job that monitors suspicious behavior, scanning their entire network is a great way to gain attention.

What Does Wireshark Mean?

Wireshark is a free and open source network protocol analyzer that enables users to interactively browse the data traffic on a computer network. The development project was started under the name Ethereal, but was renamed Wireshark in 2006.

Many networking developers from all around the world have contributed to this project with network analysis, troubleshooting, software development and communication protocols. Wireshark is used in many educational institutions and other industrial sectors.

Ettercap is a free and open source (Links to an external site.) network security (Links to an external site.) tool for man-in-the-middle attacks (Links to an external site.) on LAN (Links

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

to an external site.). It can be used for computer network protocol (Links to an external site.) analysis and security (Links to an external site.) auditing (Links to an external site.). It runs on various Unix-like (Links to an external site.) operating systems (Links to an external site.) including Linux (Links to an external site.), Mac OS X (Links to an external site.), BSD (Links to an external site.) and Solaris (Links to an external site.), and on Microsoft Windows (Links to an external site.). It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping (Links to an external site.) against a number of common protocols. Its original developers later founded Hacking Team (Links to an external site.). Ettercap works by putting the network interface into promiscuous mode (Links to an external site.) and by ARP poisoning (Links to an external site.) the target machines. Thereby it can act as a 'man in the middle' and unleash various attacks on the victims. Ettercap has plugin support so that the features can be extended by adding new plugins. Ettercap supports active and passive dissection of many protocols (Links to an external site.) (including ciphered ones) and provides many features for network and host analysis. Ettercap offers four modes of operation:

- IP-based: packets are filtered based on IP source and destination.
- MAC-based: packets are filtered based on MAC address (Links to an external site.), useful for sniffing connections through a gateway.
- ARP (Links to an external site.)-based: uses ARP poisoning (Links to an external site.) to sniff on a switched LAN between two hosts (full-duplex).
- PublicARP-based: uses ARP poisoning to sniff on a switched LAN from a victim host to all other hosts (half-duplex).

Cyber attack Type

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

We are living in a digital era. Now a day, most of the people use computer and internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

Cyber-attacks can be classified into the following categories:

Year: 2
Semester: III

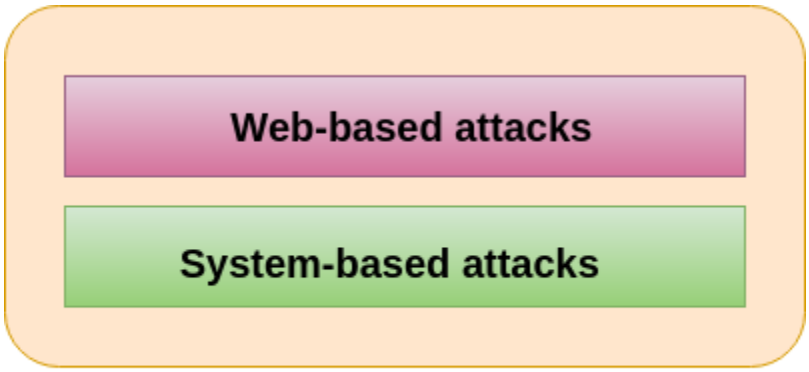
1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3



Classification of Cyber attacks

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker?s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second

7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

1. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

UNIT 3

Types of Cyber Attackers

Types of Cyber Attackers

In computer and computer networks, an attacker is the individual or organization who performs the malicious activities to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

As the Internet access becomes more pervasive across the world, and each of us spends more time on the web, there is also an attacker grows as well. Attackers use every tools and techniques they would try and attack us to get unauthorized access.

There are four types of attackers which are described below-

Year: 2
Semester: III

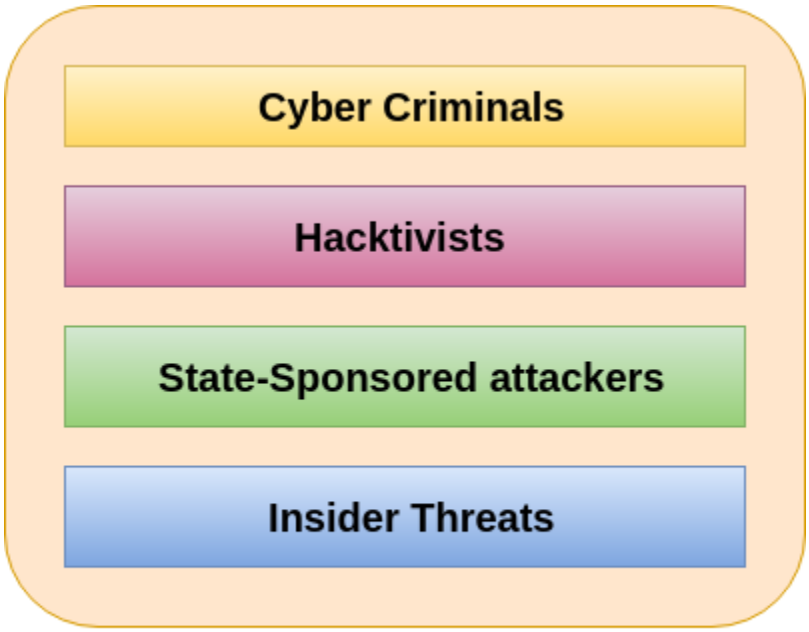
1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3



Types of CyberAttackers

Cyber Criminals

Cybercriminals are individual or group of people who use technology to commit cybercrime with the intention of stealing sensitive company information or personal data and generating profits. In today's, they are the most prominent and most active type of attacker.

Features of Java - Javatpoint

Cybercriminals use computers in three broad ways to do cybercrimes-

- **Select computer as their target**- In this, they attack other people's computers to do cybercrime, such as spreading viruses, data theft, identity theft, etc.

6. **Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917**
7. **Course : Cybersecurity L: 0**
8. **Program : MCA T: 0**
9. **Target : 70% P: 3**

C:3

- **Uses the computer as their weapon**- In this, they use the computer to do conventional crime such as spam, fraud, illegal gambling, etc.
- **Uses the computer as their accessory**- In this, they use the computer to steal data illegally.

Hacktivists

Hacktivists are individuals or groups of hackers who carry out malicious activity to promote a political agenda, religious belief, or social ideology. According to Dan Lohrmann, chief security officer for Security Mentor, a national security training firm that works with states said "Hacktivism is a digital disobedience. It's hacking for a cause." Hacktivists are not like cybercriminals who hack computer networks to steal data for the cash. They are individuals or groups of hackers who work together and see themselves as fighting injustice.

State-sponsored Attacker

State-sponsored attackers have particular objectives aligned with either the political, commercial or military interests of their country of origin. These type of attackers are not in a hurry. The government organizations have highly skilled hackers and specialize in detecting vulnerabilities and exploiting these before the holes are patched. It is very challenging to defeat these attackers due to the vast resources at their disposal.

Insider Threats

The insider threat is a threat to an organization's security or data that comes from within. These type of threats are usually occurred from employees or former employees, but may also arise from third parties, including contractors, temporary workers, employees or customers.

Insider threats can be categorized below-

Year: 2
Semester: III

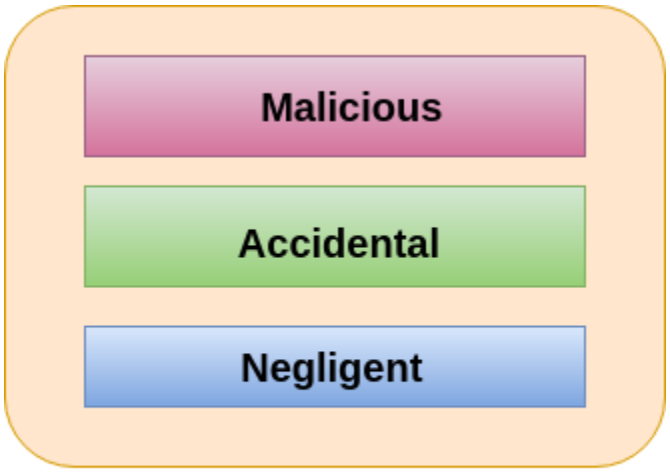
1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3



Insider Threats

Malicious-

Malicious threats are attempts by an insider to access and potentially harm an organization's data, systems or IT infrastructure. These insider threats are often attributed to dissatisfied employees or ex-employees who believe that the organization was doing something wrong with them in some way, and they feel justified in seeking revenge.

Insiders may also become threats when they are disguised by malicious outsiders, either through financial incentives or extortion.

Accidental-

Accidental threats are threats which are accidently done by insider employees. In this type of threats, an employee might accidentally delete an important file or inadvertently share confidential data with a business partner going beyond company?s policy or legal requirements.

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917
7. Course : Cybersecurity L: 0
8. Program : MCA T: 0
9. Target : 70% P: 3

C:3

Negligent-

These are the threats in which employees try to avoid the policies of an organization put in place to protect endpoints and valuable data. For example, if the organization have strict policies for external file sharing, employees might try to share work on public cloud applications so that they can work at home. There is nothing wrong with these acts, but they can open up to dangerous threats nonetheless.

Code injection

Code injection is one of the most common types of injection attacks. If attackers know the programming language, the framework, the database or the operating system used by a web application, they can inject code via text input fields to force the webserver to do what they want.

These types of injection attacks are possible on applications that lack input data validation. If a text input field lets users enter whatever they want, then the application is potentially exploitable. To prevent these attacks, the application needs to restrict as much as it can the input users are allowed to enter.

For example, it needs to limit the amount of expected data, to check the data format before accepting it, and to restrict the set of allowed characters.

The code injection vulnerabilities can be easy to find, just by testing the text input of a web application with different types of content. When found, the vulnerabilities are moderately hard to exploit. But when an attacker manages to exploit one of these vulnerabilities, the

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

impact could include loss of confidentiality, integrity, availability, or application functionality.

SQL injection

In a similar fashion to code injection, this attack inserts an SQL script –the language used by most databases to perform query operations– in a text input field. The script is sent to the application, which executes it directly on its database. As a result, the attacker could pass through a login screen or do more dangerous things, like read sensitive data directly from the database, modify or destroy database data, or execute admin operations on the database.

PHP and ASP applications are prone to SQL injection attacks (Links to an external site.) due to its older functional interfaces. J2EE and ASP.Net apps are usually more protected against these attacks. When an SQL injection vulnerability is found –and they could be easily found–the magnitude of the potential attacks will only be limited by the attacker's skill and imagination. Thus, the impact of an SQL injection attack is undoubtedly high.

Year: 2

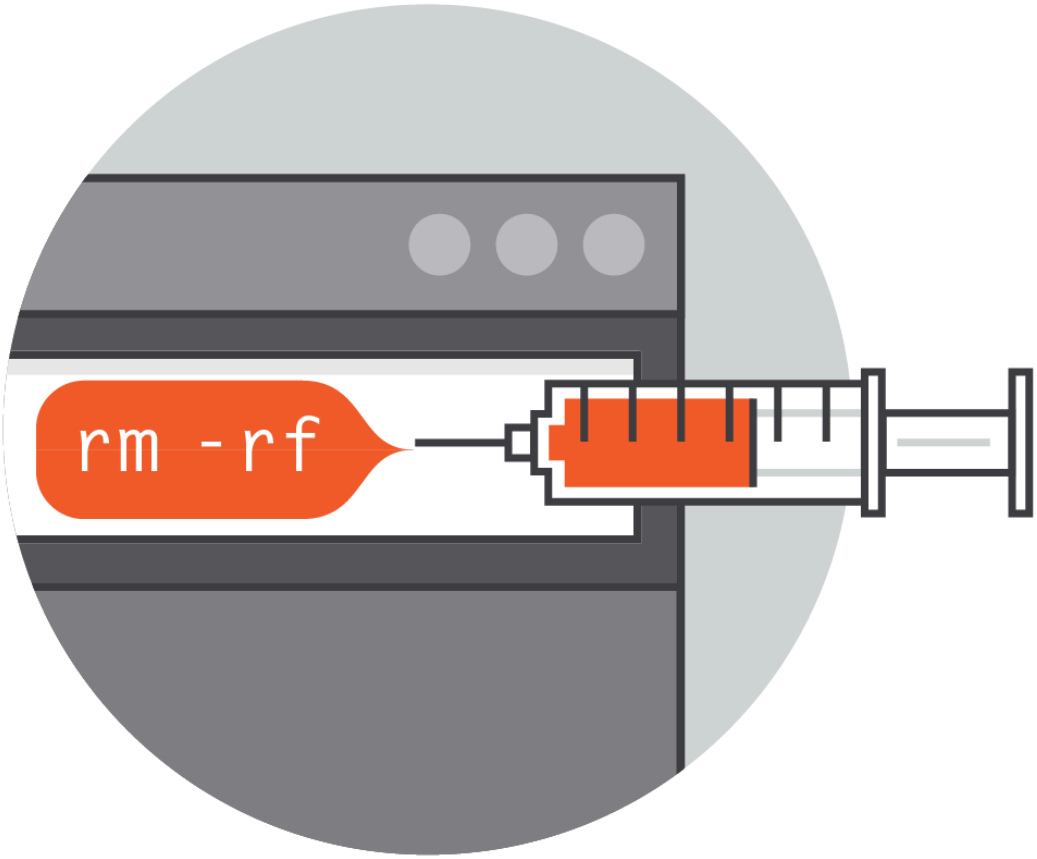
Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917
7. Course : Cybersecurity L: 0
8. Program : MCA T: 0
9. Target : 70% P: 3

C:3

Command injection

These attacks are also possible, mainly due to insufficient input validation. They differ from code injection attacks in that the attacker inserts system commands instead of pieces of programming code or scripts. Therefore, hacker doesn't need to know the programming language in which the application is based or the language used by the database. But they need to know the operating system used by the hosting server.



The inserted system commands are executed by the host operating system with the privileges of the application (Links to an external site.), which could allow for exposing the content of arbitrary files residing on the server, for showing the directory structure of a server, for changing user passwords, among other things.

These attacks can be prevented by a sysadmin, by limiting the system access level of the web applications running on a server.

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

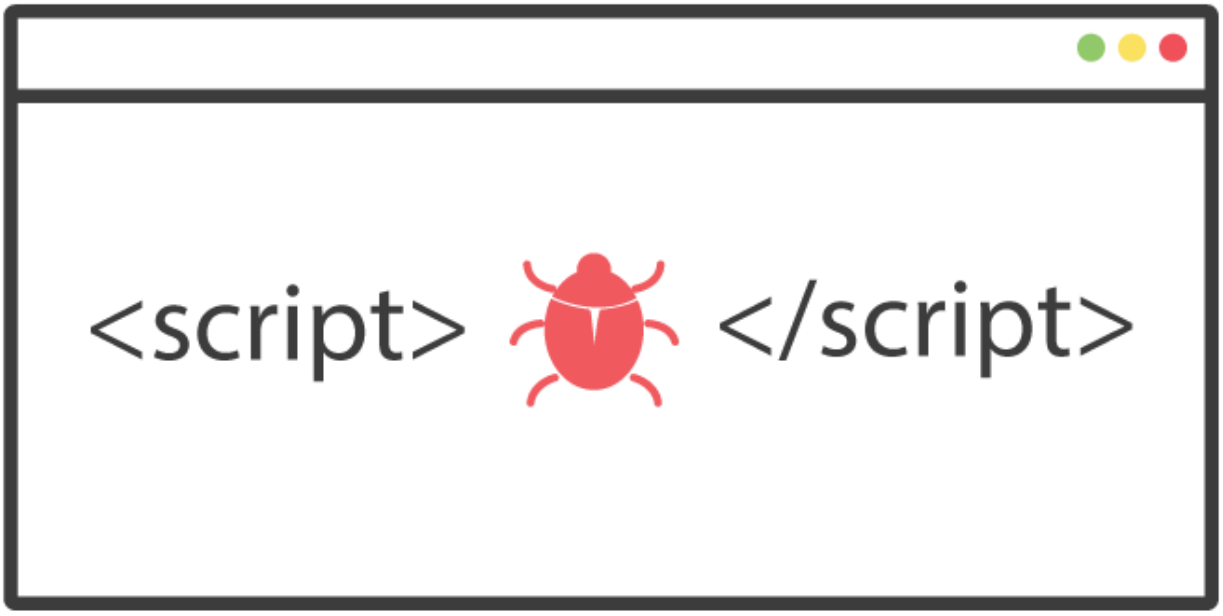
4.Target : 70% **P: 3**

C:3

Cross-site scripting

Whenever an application inserts input from a user within the output it generates, without validating or encoding it, it gives the opportunity to an attacker to send malicious code to a different end-user. Cross-Site Scripting (XSS) attacks take these opportunities to inject malicious scripts into trusted websites, which is ultimately sent to other users of the application, which become the attacker's victims.

The victims' browser will execute the malicious script without knowing it should not be trusted. Therefore, the browser will let it access session tokens, cookies, or sensitive information stored by the browser. If properly programmed, the scripts could even rewrite the contents of an HTML file.



XSS attacks can be generally divided into two different categories: stored and reflected.

In **stored** XSS attacks, the malicious script resides permanently on the target server, in a message forum, in a database, in a visitor log, etc. The victim gets it when its browser requests the stored information. In **reflected** XSS attacks, the malicious script is reflected in a response that includes the input sent to the server. This could be an error message or a search result, for example.

XPath injection

This type of attack is possible when a web application uses information provided by a user to build an XPath query for XML data. The way these attack works is similar to SQL injection (Links to an external site.): attackers send malformed information to the application in order to find out how the XML data is structured, and then they attack again to access that data.

XPath is a standard language with which, like SQL, you can specify the attributes you want to find. To perform a query on XML data, web applications use user input to set a pattern the data should match. By sending malformed input, the pattern can turn into an operation that the attacker wants to apply to the data.

Unlike what happens with SQL, in XPath, there are no different versions. This means that XPath injection can be done on any web application that uses XML data, regardless of the implementation. That also means that the attack can be automated; therefore, unlike SQL injection, it has the potential to be fired against an arbitrary number of objectives.

Mail command injection

This attack method can be used to exploit email servers and applications that build IMAP or SMTP statements with improperly validated user input. Occasionally, IMAP and SMTP servers don't have strong protection against attacks, as it would be the case with most web servers, and therefore could be more exploitable. Entering through a mail server, attackers could evade restrictions such as captchas, a limited number of requests, etc.

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

To exploit an SMTP server, attackers need a valid email account to send messages with injected commands. If the server is vulnerable, it will respond to the attackers' requests, allowing them, for example, to override server restrictions and use its services to send spam.

IMAP injection could be done mainly on webmail applications, exploiting the message reading functionality. In these cases, the attack can be performed by simply entering, in the address bar of a web browser, a URL with the injected commands.

CRLF injection

The insertion of carriage return and line feed characters –combination known as CRLF– in web form input fields represents an attack method called CRLF injection. These invisible characters indicate the end of a line or the end of a command in many traditional internet protocols, such as HTTP, MIME, or NNTP.

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917
7. Course : Cybersecurity L: 0
8. Program : MCA T: 0
9. Target : 70% P: 3
C:3

For example, the insertion of a CRLF into an HTTP request, followed by some certain HTML code, could send custom web pages to the visitors of a website.

This attack can be performed on vulnerable web applications that don't apply the proper filtering to the user input. This vulnerability opens the door to other types of injection attacks, such as XSS and code injection, and could also derive in a website being hijacked.

Host Header injection

In servers that host many websites or web applications, the host header becomes necessary to determine which of the resident websites or web applications –each of them known as a virtual host– should process an incoming request. The value of the header tells the server to which of the virtual hosts to dispatch a request. When the server receives an invalid host header, it usually passes it to the first virtual host in the list. This constitutes a vulnerability that attackers can use to send arbitrary host headers to the first virtual host in a server.

Manipulation of the host header is commonly related to PHP applications, although it can also be done with other web development technologies. Host header attacks work as enablers for other types of attacks, such as web-cache poisoning. Its consequences could include the execution of sensitive operations by the attackers, for example, password resets.

LDAP injection

LDAP is a protocol designed to facilitate the search of resources (devices, files, other users) in a network. It is very useful for intranets, and when used as part of a single sign-on system, it can be used to store usernames and passwords. LDAP queries involve the use of special control characters that affect its control. Attackers can potentially change the intended behavior of an LDAP query if they can insert control characters in it.

Year: 2
Semester: III

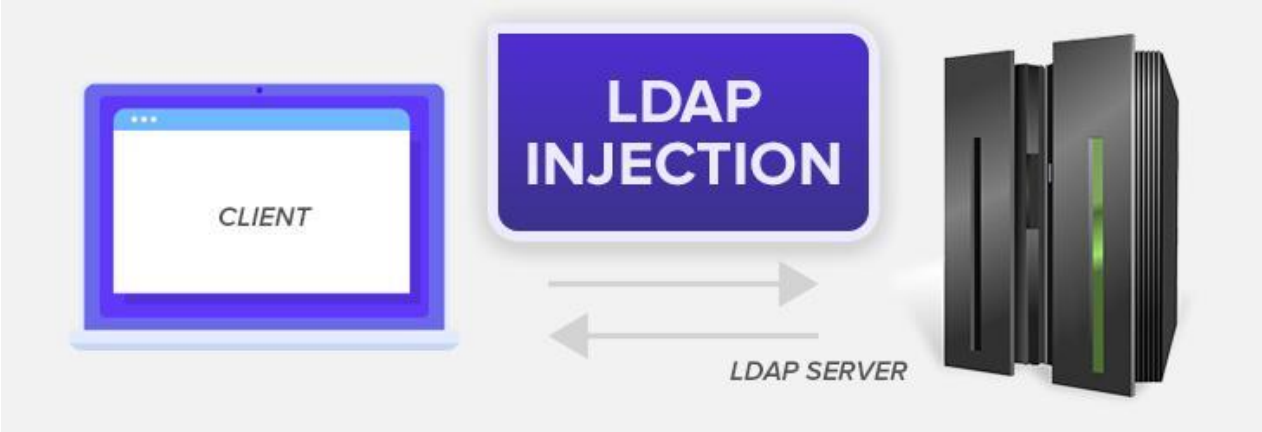
1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3



Again, the root problem that allows for LDAP injection attacks is improperly validated user input. If the text a user sends to an application is used as part of an LDAP query without sanitizing it, the query could end up retrieving a list of all users and showing it to an attacker, just by using an asterisk (*) in the right place inside an input string.

Preventing injection attacks

As we saw in this article, all injection attacks are directed towards servers and applications with open access to any internet user. The responsibility to prevent these attacks is distributed among application developers and server administrators.

Application developers need to know the risks involved in the incorrect validation of user input and learn best practices to sanitize user input with risk prevention purposes. Server administrators need to audit their systems periodically to detect vulnerabilities (Links to an external site.) and correct them as soon as possible. There are many options to perform these audits, either on-demand or automatically.

UNIT IV

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917
7. Course : Cybersecurity L: 0
8. Program : MCA T: 0
9. Target : 70% P: 3

C:3

Packet Filter Firewall and Application Level Gateway

Packet Filter Firewall and Application Level Gateway

No one can deny the fact that the dynamic rise of the Internet has brought the world closer. But at the same time, it has left us with different kinds of security threats. To ensure the confidentiality and integrity of valuable information of a corporate network from the outside attacks, we must have some robust mechanism. This is where the **Firewall** comes into picture.

It can be compared with a security guard standing at the entrance of a minister's home. He keeps an eye on everyone and physically checks every person who wishes to enter the house. It won't allow a person to enter if he/she is carrying a harmful object like a knife, gun etc. Similarly, even if the person doesn't possess any banned object but appears suspicious, the guard can still prevent that person's entry.

The firewall acts as a guard. It guards a corporate network acting as a shield between the inside network and the outside world. All the traffic in either direction must pass through the firewall. It then decides whether the traffic is allowed to flow or not. The firewall can be implemented as hardware and software, or a combination of both.

Packet Filters –

Packet filter firewall

- It works in the network layer of the OSI Model. It applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.
- Packet filter firewall controls access to packets on the basis of packet source and destination address or specific transport protocol type. It is done at the OSI (Open Systems Interconnection) data link, network and transport layers. Packet filter firewall works on the network layer of the OSI model.
- Packet filters consider only the most basic attributes of each packet, and they don't need to remember anything about the traffic since each packet is examined in isolation. For this reason they can decide packet flow very quickly.

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

- Example : Filter can be set to block all UDP segments and all Telnet connections. This type configuration prevents outsiders from logging onto internal hosts using Telnet and insider from logging onto external hosts using Telnet connections.

Application Gateways –

Application level gateway

- Application level gateway is also called a bastion host. It operates at the application level. Multiple application gateways can run on the same host but each gateway is a separate server with its own processes.
- These firewalls, also known as application proxies, provide the most secure type of data connection because they can examine every layer of the communication, including the application data.
- Example : Consider FTP service. The FTP commands like get file, put file, list files and position the process at a particular point in a directory tree. Some system admin blocks puts command but permits gets command, list only certain files or prohibit changing out of a particular directory. The proxy server would simulate both sides of this protocol exchange. For example the proxy might accepts get commands and reject put commands.

It works as follows:

Step-1: User contacts the application gateway using a TCP/IP application such as HTTP.

Step-2: The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.

Step-3: After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.

Year: 2
Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917
7. Course : Cybersecurity L: 0
8. Program : MCA T: 0
9. Target : 70% P: 3

C:3

Difference :

Packet filter	Application level
Simplest	Even more complex
Screens based on connection rules	Screens based on behaviour or proxies
Auditing is difficult	Activity can audit
Low impact on network performance	High impact on network performance
Network topology can not hide	Network topology can hide from attacker
Transparent to user	Not transparent to user
See only addresses and service protocol type	Sees full data portion of packet

What is a Firewall?

What is a Firewall?

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet (Links to an external site.) in infected computers.

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

Firewall: Hardware or Software

This is one of the most problematic questions whether a firewall is a hardware or software. As stated above, a firewall can be a network security device or a software program on a computer. This means that the firewall comes at both levels, i.e., hardware (Links to an external site.) and software (Links to an external site.), though it's best to have both. Each format (a firewall implemented as hardware or software) has different functionality but the same purpose. A hardware firewall is a physical device that attaches between a computer network (Links to an external site.) and a gateway. For example, a broadband router. On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software.

Apart from that, there are cloud-based firewalls. They are commonly referred to as FaaS (firewall as a service). A primary advantage of using cloud-based firewalls is that they can be managed centrally. Like hardware firewalls, cloud-based firewalls are best known for providing perimeter security.

Why Firewall

Firewalls are primarily used to prevent malware and network-based attacks. Additionally, they can help in blocking application-layer attacks. These firewalls act as a gatekeeper or a barrier. They monitor every attempt between our computer and another network. They do not allow data packets to be transferred through them unless the data is coming or going from a user-specified trusted source.

Firewalls are designed in such a way that they can react quickly to detect and counter-attacks throughout the network. They can work with rules configured to protect the network and perform quick assessments to find any suspicious activity. In short, we can point to the firewall as a traffic controller.

Some of the important risks of not having a firewall are:

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917
7. Course : Cybersecurity L: 0
8. Program : MCA T: 0
9. Target : 70% P: 3

C:3

Open Access

If a computer is running without a firewall, it is giving open access to other networks. This means that it is accepting every kind of connection that comes through someone. In this case, it is not possible to detect threats or attacks coming through our network. Without a firewall, we make our devices vulnerable to malicious users and other unwanted sources.

Lost or Comprised Data

Without a firewall, we are leaving our devices accessible to everyone. This means that anyone can access our device and have complete control over it, including the network. In this case, cybercriminals can easily delete our data or use our personal information for their benefit.

Evaluation Sheet – Internal Assessment

Roll Number	Registration Number	Name of the Student	Internal Assessment (30)				
			Assignment [10]	Class Test [20]	Case Study	etc.	Total
AU/2020/0004456	PG/02/MCA/2020/001	NAMRATA SAMANTA	7	14			21
AU/2020/0004545	PG/02/MCA/2020/003	Deepika Barua	8	19			27
AU/2020/0004585	PG/02/MCA/2020/006	Oliva Roy	9	20			29
AU/2020/0004594	PG/02/MCA/2020/009	Ankit Kumar shah	7	18			25
AU/2020/0004534	PG/02/MCA/2020/002	SAYANI DAS	6	17			23
AU/2020/0004590	PG/02/MCA/2020/007	Ujjal Dey Sarkar	7	15			22
AU/2020/0004599	PG/02/MCA/2020/010	soham Das	6	14			20

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

AU/2020/0004551	PG/02/MCA/2020/004	J SAGAR SINGH	6	13			19
AU/2020/0004573	PG/02/MCA/2020/005	Santanu Soo	7	14			21
AU/2020/0004592	PG/02/MCA/2020/008	Sumita Choubey	8	19			27

Signature of HOD/Dean **Signature of Faculty**

Date: **Date:**

Evaluation Sheet – Mid Semester

Roll Number	Registration Number	Name of the Student	Marks (20)

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

AU/2020/0004456	PG/02/MCA/2020/001	NAMRATA SAMANTA	
AU/2020/0004545	PG/02/MCA/2020/003	Deepika Barua	
AU/2020/0004585	PG/02/MCA/2020/006	Oliva Roy	
AU/2020/0004594	PG/02/MCA/2020/009	Ankit Kumar shah	
AU/2020/0004534	PG/02/MCA/2020/002	SAYANI DAS	
AU/2020/0004590	PG/02/MCA/2020/007	Ujjal Dey Sarkar	
AU/2020/0004599	PG/02/MCA/2020/010	soham Das	
AU/2020/0004551	PG/02/MCA/2020/004	J SAGAR SINGH	
AU/2020/0004573	PG/02/MCA/2020/005	Santanu Soo	
AU/2020/0004592	PG/02/MCA/2020/008	Sumita Choubey	

Signature of HOD/Dean **Signature of Faculty**

Date: **Date:**

Planning for Remedial Classes – Mid Semester

Sl. No.	Name of Student	Roll No.	Reg. No.	Mid Sem Marks	Remedial Classes Held	Class test on the basis of	End Sem Marks	Improvement (Y/N)

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

												Remedial Classes		
					Date									
					Venue									
					Time									
1.														
2.														

Signature of HOD/ Dean **Signature of Faculty**

Date: **Date:**

COURSE END SURVEY

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

INDIRECT ASSESSMENT

Sample format for Indirect Assessment of Course outcomes:

NAME:
ROLL NO.:
REG. NO..:
COURSE:
PROGRAM:

Please rate the following aspects of course outcomes of

Use the scale 1-5 (Poor – Excellent)

Course Outcomes	Statement	1	2	3	4	5
CO1						
CO2						
CO3						
CO4						
CO5						

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

INDIRECT ASSESSMENT CONSOLIDATION

ADAMAS UNIVERSITY, KOLKATA **SCHOOL OF** **DEPARTMENT OF** **CO Indirect Assessment**		
Programme: **Academic Year:2020-21** **Batch: 2020-22**		
Course Code & **Name:**		
Course Outcome	**Students Feed Back (5)**	**Attainment (100)**
CO1		
CO2		
CO3		
CO4		
CO5		
etc.		
Signature of HOD/Dean **Date:**		**Signature of Faculty** **Date:**

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917
7. Course : Cybersecurity L: 0
8. Program : MCA T: 0
9. Target : 70% P: 3

C:3

Evaluation Sheet (End Semester)

Roll Number	Registration Number	Name of the Student	Marks (50)

Signature of HOD/Dean

Date:

Signature of Faculty

Date:

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

Planning for Remedial Classes – End Semester

Sl. No.	Name of Student	Roll No.	Reg. No.	End Sem Marks	Remedial Classes Held							Class test on the basis of Remedial Classes	Supple Exam Marks	Improvement (Y/N)
					Date									
					Venue									
					Time									
1.														

Year: 2

Semester: III

6. Name of the Faculty: Subhasish Mohapatra Course Code: CSE21917
7. Course : Cybersecurity L: 0
8. Program : MCA T: 0
9. Target : 70% P: 3

C:3

2.														

Signature of HOD/ Dean **Signature of Faculty**

Date **Date**

Consolidated Mark Statement

Roll Number	Registration Number	Name of the Student	Total Marks			
			Mid Semester (20)	Internal Assessment (30)	End Semester (50)	Total (100)
AU/2020/0004456	PG/02/MCA/2020/001	NAMRATA SAMANTA				
AU/2020/0004545	PG/02/MCA/2020/003	Deepika Barua				
AU/2020/0004585	PG/02/MCA/2020/006	Oliva Roy				
AU/2020/0004594	PG/02/MCA/2020/009	Ankit Kumar shah				
AU/2020/0004534	PG/02/MCA/2020/002	SAYANI DAS				
AU/2020/0004590	PG/02/MCA/2020/007	Ujjal Dey Sarkar				

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

AU/2020/0004599 AU/2020/0004551 AU/2020/0004573	PG/02/MCA/2020/010 PG/02/MCA/2020/004 PG/02/MCA/2020/005	soham Das J SAGAR SINGH Santanu Soo				
AU/2020/0004592	PG/02/MCA/2020/008	Sumita Choubey				

Signature of Dean/HOD **Signature of Faculty**

Date: **Date:**

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

CO ATTAINMENT – GAP ANALYSIS & REMEDIAL MEASURES

ADAMAS UNIVERSITY, KOLKATA
SCHOOL OF
DEPARTMENT OF
CO ATTAINMENT - GAP ANALYSIS & REMEDIAL MEASURES

Batch :	**2020-22**			**Academic Year:**	**2020-21**	
Course Code & Name		**Name of the Coordinator**		**Year & Semester**		
CSE21917 CYBER SECURITY		**SUBHASISH MOHAPATRA**		**I & I**		
CO	**Direct Assessment**	**Indirect Assessment**	**CO Attainment**	**Target**	**CO Attainment Gaps**	**Action for Bridge the Gap**	**Target Modification**
CO1							
CO2							
CO3							
CO4							

Year: 2

Semester: III

6. Name of the Faculty: Subhasis Mohapatra Course Code: CSE21917
7. Course : Cybersecurity L: 0
8. Program : MCA T: 0
9. Target : 70% P: 3

C:3

CO5							

Signature of HOD/Dean

Date:

Signature of Faculty

Date:

CO-PO ATTAINMENT

ADAMAS UNIVERSITY, KOLKATA

SCHOOL OF

DEPARTMENT OF

CO-PO ATTAINMENT

Programme: MCA	Year & Sem: II& III	Academic Year: 2020-21	Batch:2020-22

Course Code	Course Name	CO-PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO 10	PO 11	PO 12	PSO 1	PS
CSE21917	CYBERSECURITY	Relationship	CO2, CO3, CO4, CO5	CO1, CO2, CO3	CO1,CO2, CO3, CO4, CO5	NA	CO4	NA	NA	NA	NA	NA	CO5	CO3,CO4	CO5	N

Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

		Mapping Value	3	3	2	NA	2	NA	NA	NA	NA	NA	2	3	2	N
		Attainment	2.4	2.4	1.6	NA	1.6	NA	NA	NA	NA	NA	1.6	2.4	1.6	

Signature of HOD/Dean

Date:

Signature of Faculty

Date:

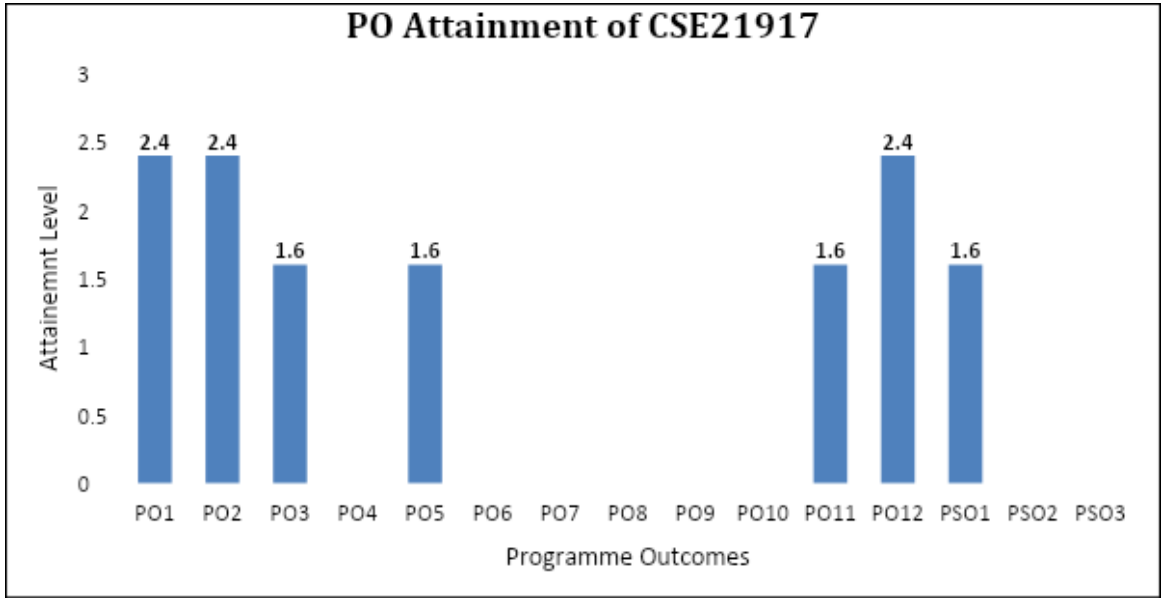
PO ATTAINMENT OF THE COURSE

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3



Year: 2
Semester: III

1Name of the faculty: Subhasish Mohapatra **Course Code: CSE21917**

2Course : Cybersecurity **L: 0**

3.Program : MCA **T: 0**

4.Target : 70% **P: 3**

C:3

Signature of HOD/Dean **Signature of Faculty**

Date: **Date:**

Year: 2

Semester: III

6. **Name of the Faculty: Subhasish Mohapatra** **Course Code: CSE21917**
7. **Course : Cybersecurity** **L: 0**
8. **Program : MCA** **T: 0**
9. **Target : 70%** **P: 3**

C:3

INSTRUCTIONS FOR FACULTY

Instructions for Faculty

- Faculty should keep track of the students with low attendance and counsel them regularly.
- Course coordinator will arrange to communicate the short attendance (as per University policy) cases to the students and their parents monthly.
- Topics covered in each class should be recorded in the table of RECORD OF CLASS TEACHING (Suggested Format).
- Internal assessment marks should be communicated to the students twice in a semester.
- The file will be audited by respective Academic Monitoring and Review Committee (AMRC) members for theory as well as for lab as per AMRC schedule.
- The faculty is required to maintain these files for a period of at least three years.
- This register should be handed over to the head of department, whenever the faculty member goes on long leave or leaves the Colleges/University.
- For labs, continuous evaluation format (break-up given in the guidelines for result preparation in the same file) should be followed.
- Department should monitor the actual execution of the components of continuous lab evaluation regularly.
- Instructor should maintain record of experiments conducted by the students in the lab weekly.
- Instructor should promote students for self-study and to make concept diary, due weightage in the internal should be given under faculty assessment for the same.
- Course outcome assessment: To assess the fulfilment of course outcomes two different approaches have been decided. Degree of fulfillment of course outcomes will be assessed in different ways through direct assessment and indirect assessment. In Direct Assessment, it is measured through quizzes, tests, assignment, Mid-term and/or End-term examinations. It is suggested that each examination is designed in such a way that it can address one or two outcomes (depending upon the course completion). Indirect assessment is done through the student survey which needs to be designed by the faculty (sample format is given below) and it shall be conducted towards the end of course completion. The evaluation of the achievement of the Course Outcomes shall be done by analyzing the inputs received through Direct and Indirect Assessments and then corrective actions suggested for further improvement.
- **Submission Targets of Course Contents:**
  - **S. No. 1 to 8 : Before Starting the Course**
  - **S. No. 9 & 10 : After Mid Semester Examination**
  - **S. No. 11 to 18 : Immediately After End Semester Examination**
  - **S. No. 19 to 22 : After Declaration of Result of the Course**