Laboratory Manual

Subject: Network Cloud Security (CE664A)

School of Computer Engineering & Mathematical Sciences
DEFENCE INSTITUTE OF ADVANCED TECHNOLOGY
(Deemed to be University)
Pune 411 025 India

For
M.Tech. (Computer Science and Engineering) Students

Faculty Incharge:
Dr CRS Kumar
Professor, School of Computer Engineering and Mathematical Sciences, DIAT (DU), Pune

Year: 2023-2024

Student Name	
Reg No	

Course Plan

Department: Computer Science and Engineering	***Course Type: Professional Core***
Course Title: **Network and Cloud Security**	***Course Code:*** **CE664A**
L-T-P: 3-0-2	***Credits:*** *4*
Semester: I	***Specialization: Cyber security***
*Total Lectures : 48**L** + 2P(per week)*	
EndSem Marks*: 50*	***Internal Marks: 30(Quiz)+20(Lab)***

Prerequisites: Basic computer networking, operating systems and computer programming knowledge is required.

Course Objectives:
Understanding basic issues, concepts, principles and mechanisms in Network Security.

- Basic Security concepts
- Authentication
- Access Control
- IPSec and Internet Key Management
- SSL/TLS Protocol
- Firewall/UTM
- Malicious Software
- Intruder Detection Systems

Be able to determine appropriate mechanisms for protecting networked systems.
Security Laboratory.
1. To facilitate individual in gaining knowledge on Network Security Protocols, Appliances and systems.
2. To facilitate individual in gaining hands on experience on various attacks and countermeasures

Course outcome (CO):

On completion of this course, the students will be able to:

Course Outcomes	Description	Blooms Taxanomy Level Targeted	No. of Contact Hours	Marks
CO1	Students will be able to understand and apply Network and cloud security Concepts along with various countermeasures. (PO1, PO3, PSO1)	Level 2: Remembering, Understanding	16	10
CO2	Students will be able to understand and apply Network and cloud Security concepts, hardware, software, standards and policies	Level 3: Remembering,	19	10

	required for an organization. (PO1,PO2, PO3, PSO1)	Understanding, Analysing		
CO3	Students will be able to understand the importance of implementation of Network and cloud Security protocols, Devices, policies. (PO1, PO3, PSO1)	Level 2: Remembering, Understanding,	13	10
CO4	Students will be capable of applying their knowledge and skills to solve engineering problems in Network and cloud Security. (PO1, PO2, PO3, PSO1, PSO2)	Level 4: Applying, Analysing	2Hrs/Week (LAB)	20
CO1-CO3	Endsem			50
Total Marks				100

Assessment Plan

Components	**Test**	**Lab-Assignments/ Project/seminar**	**End semester exam**
Duration	**30 minutes**	**2Hrs/week**	**180 minutes**
Weightage	**30% (3x10 marks)**	**20% (20 marks)**	**50% (1x50 marks)**
Typology of Questions	**Understanding , Applying, Analyzing**	**Understanding , Applying, Analyzing**	**Understanding , Applying, Analyzing**
Pattern	**Answer all Questions in form of MCQs/short answers/Descriptive Answers**	**Lab-Assignments/ Project/seminar presentation**	**Answer all 5 Questions**
Schedule	**As notified by Dy registrar Academics.**	**Calendared activity**	**Calendared activity**
Topics Covered	**Test1(Unit1) (CO1)**	**Lab-Assignments/ Project/seminar Presentation (CO4)**	**Comprehensive examination covering full syllabus. Students are expected to answer all questions (CO1-CO3)**
	Test2 (Unit3 and Unit4) (CO2)		
	Test3 (Unit4) (CO3)		

Lesson Plan

L.No/T.No	**Topic**	**CO**	**PO**
L0	**Introduction about the course and evaluation schemes**		
L1-L15	**Unit I**	**CO1**	**PO1,PO3,PSO1**
L16-L28	**Unit II**	**CO3**	**PO1,PO3,PSO1**
L29-L37	**Unit III**	**CO2**	**PO1,PO2, PO3, PSO1**
L38-L47	**Unit V**	**CO2**	**PO1,PO2, PO3, PSO1**

	List of Experiments	**CO4**	**PO1,PO2, PO3, PSO1, PSO2**

Hardware and Software: Core i-5 machines, Kali Linux, windows VM

Detailed Syllabus

Subject Code	**CE-664A**
Subject Title	**Network and Cloud Security**
Credit	**04**
Teaching Scheme	Lectures: 03 hours/week Tutorial/Practical: 02 hours/week Total Contact hours 05 per week.
Evaluation Pattern	03 monthly tests + 01 final evaluation + assignments for internal assessment
Total Marks	100
Prerequisite	Basic computer networking, operating systems and computer programming knowledge is required.

Objective:

Understanding basic issues, concepts, principles and mechanisms in Network and Cloud Security.

- Basic Security concepts
- Authentication
- Access Control
- IPSec and Internet Key Management
- SSL/TLS Protocol
- Firewall/UTM
- Malicious Software
- Intruder Detection Systems
- Cloud Computing and Security

Be able to determine appropriate mechanisms for protecting networked systems. Network and Cloud Security Laboratory.

- To facilitate individual in gaining knowledge on Network and Cloud Security Protocols, Appliances and systems.
- To facilitate individual in gaining hands on experience on various attacks and countermeasures

Course Outcomes:

CO1: Students will be able to understand and apply Network and Cloud security Concepts along with various countermeasures. (PO1, PO3, PSO1)

CO2: Students will be able to understand and apply Network and Cloud Security concepts, hardware, software, standards and policies required for an organization. (PO1, PO2, PO3, PSO1)

CO3: Students will be able to understand the importance of implementation of Network and Cloud Security protocols, Devices, policies. (PO1, PO3, PSO1)

CO4: Students will be capable of applying their knowledge and skills to solve engineering problems in Network and Cloud Security. (PO1, PO2, PO3, PSO1, PSO2)

Syllabus:

Syllabus Details		**Text Book**	**Hours**	**Outcome**
Unit 1	Introduction, OSI security Architecture, Security Principles, Attacks and Threats, Model of Network Security Security at Application Layer: Email Architecture, PGP, S/MIME	Text book 1 Chap 1, & 8	6	CO1
Unit 2	Security at Transport Layer: SSL Architecture, TLS, SET, HTTPS protocols Security at Network Layer, IPSec, VPN, ISKMP Firewall: Types of Firewalls, Firewall configuration, DMZ, UTMs	Text Book1, Chap 6 & 9**, 12**	12	CO1
Unit 3	Intrusion Detection and Intrusion Prevention Systems, Honeypots, Distributed IDS, Password Management Authentication: kerberos, X509, Authentication, PKI	Text Book 1 Chap 11 & 4	7	CO2
Unit 4	Wireless Security: Wireless LAN, 802.11 Standards, Security of WLAN Cloud Security: Cloud Computing, Security Issues and Challenges, Applications	Text Book 1 Chap 5, 7	9	CO2
Unit 5	DDoS : Direct, Reflector and Amplifier Attacks, TCP Syn Flooding, Countermeasures, Digital Attack Maps Malicious Software: Viruses, Worms, Ransomware etc, Anti-virus Architecture, Generation of Anti-Virus, Types of Viruses in network and cloud Network and cloud Reconnaissance, Traceroute, Port Scanning, ICMP Scanning, Sniffing, Probing Routers in cloud	Text Book 1 Chap 10 Text Book 2,3	9	CO3
Unit 6	Game Theory applications in Network Security Miscellaneous topics and current developments, Dark Web Network Security Observatory: Monitoring Networks	Research Papers & Ref 1	11	CO3

Text Book:

1. William Stallings, “Network Security Essentials”, 6th Edition, Pearson Education, 2019.
2. B. Menezes, “Network Security and Cryptography”, Cengage, 2013.
3. W. Du, “Computer and Internet Security: A Hands On Approach”, 3rd Edition, 2022.

Reference Books:

1. T.Alpcan and T. Basar, “Network Security: A Decision and Game-Theoritic Apparoach”, Cambridge University Press, 2010.
2. Bragg et al. “Network Security: The complete Reference”, McGraw Hill, 2004
3. Seedlabs: https://seedsecuritylabs.org/ (last accessed on 12th June 2022).

Lab Assignments

Sl No	**Lab Experiment**	**Unit**	**Hours**	**Outcome**
1	Packet Sniffing and Spoofing Lab	1	2	CO1, CO4
2	TCP attacks Lab	2	2	CO1, CO4
3	Firewall Exploration Lab	2	2	CO1, CO4
4	VPN Lab	2	2	CO1, CO4
5	Wireshark Lab	5	2	CO3, CO4
6	Snort: Intrusion Detection Lab	3	2	CO2, CO4
7	CyberCiege Lab	1	2	CO1, CO4

8	OpenSSL Exploration Lab	2	2	CO1, CO4
9	Digital Attack Maps DOS lab	5	2	CO3, CO4
10	Cloud Computing Lab	4	2	CO2, CO4

Mini-Projects

Sl No	Topic	Reference
1	Deep Learning based Intrusion Detection System	
2	Firewall with Machine Learning	
3	BloomFilter for Password Rejection	
4	Network Security Observatory	
5	Private Cloud infrastructure	

Experiment No. 1

Packet Sniffing and Spoofing Lab

Aim	students will write simple sniffer and spoofing programs, and gain an in-depth understanding of the technical aspects of these programs.
Objectives	This lab covers the following topics: • How the sniffing and spoofing work • Packet sniffing using the pcap library and Scapy • Packet spoofing using raw socket and Scapy • Manipulating packets using Scapy
Outcomes	learning to use the tools and understanding the technologies underlying these tools
Hardware/Software	This lab has been tested on the SEED Ubuntu 20.04 VM. You can download a pre-built image from the SEED website, and run the SEED VM on your own computer. However, most of the SEED labs can be conducted on the cloud, and you can follow our instruction to create a SEED VM on the cloud.

Ref: https://seedsecuritylabs.org/Labs_20.04/Files/Sniffing_Spoofing/Sniffing_Spoofing.pdf

Lab 1: Student Observations and Comments

Sl No	Observations	Remarks
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Experiment No. 2

TCP Attacks Lab

Aim	The learning objective of this lab is for students to gain first-hand experience on vulnerabilities, as well as on attacks against these vulnerabilities
Objectives	, students will conduct several attacks on TCP. This lab covers the following topics: • The TCP protocol • TCP SYN flood attack, and SYN cookies • TCP reset attack • TCP session hijacking attack • Reverse shell • A special type of TCP attack, the Mitnick attack, is covered in a separate lab
Outcomes	studying these vulnerabilities help students understand the challenges of network security and why many network security me
Hardware/Software	This lab has been tested on the SEED Ubuntu 20.04 VM. You can download a pre-built image from the SEED website, and run the SEED VM on your own computer. However, most of the SEED labs can be conducted on the cloud, and you can follow our instruction to create a SEED VM on the cloud

Ref: https://seedsecuritylabs.org/Labs_20.04/Files/TCP_Attacks/TCP_Attacks.pdf

Lab 2: Student Observations and Comments		
Sl No	**Observations**	**Remarks**
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Experiment No. 3

Firewall Exploration Lab

Aim	
Objectives	
Outcomes	
Hardware/Software	

Ref: https://seedsecuritylabs.org/Labs_20.04/Files/Firewall/Firewall.pdf

Lab 3: Student Observations and Comments		
Sl No	**Observations**	**Remarks**
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Experiment No. 4

VPN Lab

Aim	
Objectives	
Outcomes	
Hardware/Software	

Ref: https://seedsecuritylabs.org/Labs_20.04/Files/VPN/VPN.pdf

Lab 4: Student Observations and Comments		
Sl No	**Observations**	**Remarks**
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Experiment No. 5

WireShark Lab

Aim	
Objectives	
Outcomes	
Hardware/Software	

Ref: http://www-net.cs.umass.edu/wireshark-labs/Wireshark_SSL_v8.0.pdf

Lab 5: Student Observations and Comments

Sl No	Observations	Remarks
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Experiment No. 6

Snort: Intrusion Detection Lab

Aim	
Objectives	
Outcomes	
Hardware/Software	

Ref : http://webpages.eng.wayne.edu/~fy8421/16sp-csc5991/labs/lab8-instruction.pdf

Lab 6: Student Observations and Comments

Sl No	Observations	Remarks
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Experiment No. 7

CyberCiege Lab

Aim	
Objectives	
Outcomes	
Hardware/Software	

Ref : https://nps.edu/web/c3o/cyberciege

Lab 7: Student Observations and Comments		
Sl No	Observations	Remarks
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Experiment No. 8

OpenSSL Exploration Lab

Aim	
Objectives	
Outcomes	
Hardware/Software	

Ref : www.openssl.org

Lab 8: Student Observations and Comments		
Sl No	**Observations**	**Remarks**
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Experiment No. 9

Digital Attack Maps DOS Lab

Aim	
Objectives	
Outcomes	
Hardware/Software	

Ref: https://www.digitalattackmap.com/

Lab 9: Student Observations and Comments

Sl No	Observations	Remarks
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Experiment No. 10

Cloud Computing Lab

Aim	
Objectives	
Outcomes	
Hardware/Software	

Ref: https://openstack.org/software/start/

- http://cloudsim-setup.blogspot.com/2013/01/running-and-using-cloud-analyst.html

Lab 10: Student Observations and Comments

Sl No	Observations	Remarks
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Network Security Tools, Libraries and Resources

Sl No	Description	Link
1	SEEDLabs	https://seedsecuritylabs.org/
2	CyberCiege	https://nps.edu/web/c3o/cyberciege
3	OpenStack	Openstack.org
4	OpenSSL	Openssl.org
5	Digital Attack Maps	Digitalattackmap.org
6	SNORT	Snort.org
7	Network Security Essentials	http://williamstallings.com/NetworkSecurity/
8		
9		
10		