COURSE TITLE	**ADVANCED NETWORK SECURITY**
COURSE CODE	**01CY2102**
COURSE CREDITS	**4**

Objective:

1 The objective of this course is to equip students with a comprehensive understanding of network security by covering key areas such as the working architecture of OSI and TCP/IP models, and the fundamental principles of wireless architecture and network creation. Students will explore various aspects of Vulnerability Assessment and Penetration Testing (VAPT) along with its relevant domains, gain insights into different network attack methods, and develop practical knowledge of advanced security tools and techniques. Additionally, the course emphasizes defensive strategies and mitigation techniques essential for advanced network security.

Course Outcomes: After completion of this course, student will be able to:

1 Understand the fundamental concepts of network security and advance network security, including the threat landscape, risk assessment, and implementing cryptography protocols.

2 Identify and analyze common network vulnerabilities, such as insecure communication, insecure network blue print, and weak authentication and authorization mechanisms.

3 Analyze and implement secure cryptography practices for network communication, including protocol security, end point detection, and secure storage of sensitive data.

4 Analyze and implement secure cryptography practices for network communication, including protocol security, end point detection, and secure storage of sensitive data.

5 Design and implement effective security controls for network, such as encryption, access controls, and secure user authentication.

6 Will Understand OWASP top 10 concept and able to defend Advance network security as per the Blue teaming

Pre-requisite of course: Basic Understanding of Topologies, Operating System Fundamentals, Basic Networking Concepts

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
3	0	2	50	30	20	25	25

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
1	**Introduction to Networking Fundamentals** Learning OSI & TCP/IP model with security aspects, Risks and Threats associated with LAN, WAN & Wireless area Network, Understand the concepts of VPN, Proxy, DHCP, IPV4, IPV6, Port, Router & Switch, Understand the concepts of Transmission mode, Transmission media & Topologies, Peer to Peer network with security aspects and working flow	8
2	**Network Security Fundamentals** Importance of Network security and threats associated with network security, Network security attack vectors & risk matrix, Networking Security policies and procedures, Risk assessment and management in network security, Role of network security in modern computing and cyber security	5
3	**Network protocols and Secure Authentication Protocols** Networking Protocols (Basics to advance protocols) BGP, RIP, OSPF, RADIUS (Remote Authentication Dial-In User Service), TACACS+ (Terminal Access Controller Access Control System Plus), LDAP (Lightweight Directory Access Protocol), Kerberos, OAuth and OpenID Connect, Secure Socket Layer/Transport Layer Security (SSL/TLS), Secure Shell (SSH) for remote access, IPsec and PGP, Extensible Authentication Protocol (EAP), OAuth 2.0 and OpenID Connect, Security Assertion Markup Language (SAML), Carrier Sense Multiple Access with Collision Detection & Avoidance	9
4	**Cryptography Algorithm for Secure communication** Public & Private key Cryptography, Certificate Authority hierarchy and it's Key roles, 3 Key distribution & Management, Digital signature, RSA, AES, DES, 3DES, SHA Algorithms.	8
5	**Network Perimeter Security & Wireless Security** Basic IDS, IPS Fundamentals and firewall types, Advance firewall detection security, End point detection security, DMZ, WEP, WPA, WPA2, WPA3 standards & differences, Authentication mechanism in wireless area network Access Point Security	6
Total Hours		**36**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Capture Network Traffic in order to Analyse packets and identify Username & Password using Wire-shark tool Tools Required:Wireshark	2
2	**Practical 2** Create a LAN & WAN network inside Cisco Packet Tracer in order to understand about how to create network & detecting packets movements Tools Required:Cisco Packet Tracer (CPT)	2

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
3	**Practical 3** Create & configure the Firewall network using Cisco Packet tracer in order to understand how to filter packets Tools Required:Cisco Packet Tracer (CPT)	2
4	**Practical 4** Use CPT to Configuration in DNS server and Configure Telnet Tools Required:Cisco Packet Tracer (CPT)	2
5	**Practical 5** Perform ARP Poisoning attack in order to understand ARP working flow in Router Tools Required: 1 Ettercap 2 Metapsloittable2 3 Kali linux	2
6	**Practical 6** Use hping3 tool for DDos attack in order to understand server response architecture Tools Required: 1 Kali Linux 2 Hping3 Tool	2
7	**Practical 7** Configure AAA in the Cisco packet tracer in order to understand RADIUS server architecture Tools Required:Cisco Packet Tracer (CPT)	2
8	**Practical 8** Configure firewalls (stateful vs. stateless, packet filtering, proxy firewalls) on routers or Security appliances in Packet Tracer. Tools Required:Cisco Packet Tracer (CPT)	2
9	**Practical 9** Implement network security measures such as Access Control Lists (ACLs), firewall rules, and port security on routers and switches in Packet Tracer. Tools Required:Cisco Packet Tracer (CPT)	2
10	**Practical 10** Perform DNS spoofing attack in order to understand DNS architecture and MITM attack Tools Required: 1 Dnsmasq 2 Ettercap 3 Kali Linux	2
Total Hours		**20**

Textbook :

1 “Cryptography and Network Security - Principles and Practice, William Stallings, Pearson Education, 2006

References:

1 Cryptography and Network Security, Cryptography and Network Security, Atul Kahate, McGraw Hill, 2013

2 Introduction to Network Security, Introduction to Network Security, Neal Krawetz, CENGAGE Learning, 2007

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
0.00	0.00	30.00	30.00	30.00	10.00

Instructional Method:

1. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz,brainstorming, MOOCs etc.
2. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.
3. Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.
4. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1. http://nptel.ac.in/courses/106104128/
2. http://nptel.ac.in/courses/106106133/
3. https://cse02-iiith.vlabs.ac.in/
4. https://www.learn-c.org/

DR. KRUNAL NARUMAL VAGHELA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)