G.VENKATASWAMY NAIDU COLLEGE (AUTONOMOUS)

(Re-Accredited with "A" Grade by NAAC)

Department of PG Diploma in Cyber Security

P26DCS101 - Fundamentals of Cyber Security

Code	Category	Course Title	Lecture Hours	Tutorial Hours	Practical Hours	Credits
P26DCS101	Core–1	Fundamentals of Cyber Security	2	0	0	4

Year	Semester	Internal Marks(CIA)	External Marks(ESE)	Total Marks
I	I	40	60	100

Course Objectives

- This course deals with the fundamental concepts of cyber security and information protection, including cyber threats, vulnerabilities, and attack mechanisms
- It develops awareness of network security principles, safe computing practices, and basic cryptographic techniques for protecting digital information
- It familiarizes students with cyber laws, ethical practices, and security policies related to information security and data protection

Course Outcomes

Upon completion of the Course, students will be able to

CO	Course Outcome	Knowledge Level(RBT)
CO1	understand fundamental concepts of cyber security, threats, and vulnerabilities.	K1,K2,K3,K4,K5
CO2	identify common network attacks and apply basic security measures.	K1,K2,K3,K4,K5
CO3	analyze system security issues and malware threats.	K1,K2,K3,K4,K5
CO4	apply basic cryptographic techniques for securing data.	K1,K2,K3,K4,K5
CO5	understand cyber laws, ethics, and adopt safe digital practices.	K1,K2,K3,K4,K5

(K1-Remember, K2-Understand, K3-Apply, K4-Analyze, K5-Evaluate, K6-Create)

CO - PO & PSO Mapping

CO	POs							PSOs		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2	PSO3
CO1	3	2	2	2	3	2	2	3	3	2
CO2	2	3	2	3	3	2	2	3	2	3
CO3	2	2	3	3	2	2	3	2	3	2
CO4	3	2	3	3	2	2	2	3	3	3
CO5	2	3	2	2	3	3	2	3	3	2
Total	12	12	12	13	13	11	11	14	14	12

(3-Strong, 2-Medium, 1-Weak, 0-No Correlation)

Course Content

Unit-I Introduction to Cyber Security **(L-6 hrs)**

Introduction to cyber security – Cyber threats and attacks – Types of hackers – Security principles

(Confidentiality, Integrity, Availability) – Risk, vulnerability and threat concepts – Need for cyber security in digital world.

Unit-II Network Security Basics **(L-6 hrs)**

Introduction to networks – Common network attacks (Phishing, Malware, DoS, Man-in-the-Middle) – Firewalls – Intrusion Detection Systems (IDS) – Intrusion Prevention Systems (IPS) – Secure network practices

Unit-III System Security and Malware **(L-6 hrs)**

Operating system security – User authentication methods – Password security – Types of malware – Antivirus and security tools – Safe browsing practices – System vulnerabilities and patch management.

Unit-IV Cryptography and Data Security **(L-6 hrs)**

Introduction to cryptography – Encryption and decryption – Symmetric and asymmetric encryption – Digital signatures – Hashing – Data protection techniques – Secure data transmission – Basics of Public Key Infrastructure (PKI).

Unit-V Cyber Laws and Ethical Practices **(L-6 hrs)**

Introduction to cyber laws – IT Act – Digital rights and responsibilities – Cyber ethics – Privacy and data protection – Cyber security policies – Incident response basics – Career opportunities in cyber security.

Text Books

1. Stallings, W. (2017). Cryptography and Network Security. Pearson.
2. Whitman, M., & Mattord, H. (2018). Principles of Information Security. Cengage Learning.

Reference Books

1. Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards. Auerbach Publications.
2. Andress, J. (2014). The Basics of Information Security. Syngress.
3. Easttom, C. (2018). Computer Security Fundamentals. Pearson.

Web Resources

1. https://www.cisa.gov
2. https://www.kaspersky.com/resource-center
3. https://www.geeksforgeeks.org/cyber-security/

Course Designer

Dr.S.Suganthi, Assistant Professor, Department of Computer Science

G.VENKATASWAMY NAIDU COLLEGE (AUTONOMOUS)

(Re-Accredited with "A" Grade by NAAC)

Department of PG Diploma in Cyber Security

P26DCS102 - Networking & Operating System Basics

Code	Category	Course Title	Lecture Hours	Tutorial Hours	Practical Hours	Credits
P26DCS102	Core-2	Networking & Operating System Basics	2	0	0	4

Year	Semester	Internal Marks(CIA)	External Marks(ESE)	Total Marks
I	I	40	60	100

Course Objectives

- This course focuses on the core principles of computer networks and operating systems, including communication protocols, network models, and system functionalities
- It provides knowledge of operating system structures, process management, memory management, file systems, and system resource handling
- It familiarizes students with basic system administration practices and essential security concepts related to computer systems and networks

Course Outcomes

Upon completion of the Course, students will be able to

CO	Course Outcome	Knowledge Level(RBT)
CO1	understand basic networking concepts, models, and communication protocols.	K1,K2,K3,K4,K5
CO2	identify network components and explain data transmission methods.	K1,K2,K3,K4,K5
CO3	describe the structure and functions of operating systems.	K1,K2,K3,K4,K5
CO4	apply concepts of process and memory management in OS.	K1,K2,K3,K4,K5
CO5	understand file systems, system security, and basic administration practices.	K1,K2,K3,K4,K5

(K1-Remember, K2-Understand, K3-Apply, K4-Analyze, K5-Evaluate, K6-Create)

CO - PO & PSO Mapping

CO	POs							PSOs		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2	PSO3
CO1	3	2	2	2	2	2	2	3	2	2
CO2	2	3	2	3	3	2	2	3	3	2
CO3	2	2	3	3	2	2	3	2	3	2
CO4	3	2	3	3	3	2	2	3	3	3
CO5	2	3	3	3	3	3	2	3	3	2
Total	12	12	13	14	13	11	11	14	14	11

(3-Strong, 2-Medium, 1-Weak, 0-No Correlation)

Course Content

Unit-I Introduction to Computer Networks **(L-6 hrs)**

Basics of computer networks – Types of networks – Network topologies – Network devices – Transmission

media – Guided and unguided media – Introduction to Internet and its services.

Unit-II Network Models and Protocols **(L-6 hrs)**

OSI model – Layers and functions – TCP/IP model-Comparison of OSI and TCP/IP – IP addressing (IPv4 basics) - Domain Name System - Common protocols – Introduction to ports and sockets.

Unit-III Introduction to Operating Systems **(L-6 hrs)**

Definition and functions of operating system – Types of operating systems – Structure of OS – System calls – User interface – Overview of Linux and Windows operating systems.

Unit-IV Process and Memory Management **(L-6 hrs)**

Process concept – Process states – Process scheduling – Threads – Deadlock – Memory management – Paging and segmentation – Virtual memory – Performance and resource utilization.

Unit-V File System and System Security Basics **(L-6 hrs)**

File systems – File operations – Directory structures – Disk management – Access control –User authentication – Permissions – Basic system security practices – Backup and recovery – Introduction to system administration tasks.

Text Books

1. Tanenbaum, A. S., & Wetherall, D. (2011). Computer Networks. Pearson.
2. Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). Operating System Concepts. Wiley.

Reference Books

1. Kurose, J. F., & Ross, K. W. (2017). Computer Networking: A Top-Down Approach. Pearson.
2. Stallings, W. (2018). Operating Systems: Internals and Design Principles. Pearson.
3. Forouzan, B. A. (2013). Data Communications and Networking. McGraw-Hill.

Web Resources

1. https://www.coursera.org/learn/packt-operating-systems-and-networking-fundamentals-bokjh
2. https://www.geeksforgeeks.org/computer-networks/last-minute-notes-computer-network/
3. https://www.geeksforgeeks.org/operating-systems/operating-systems/

Course Designer

Dr.S.Suganthi, Assistant Professor, Department of Computer Science

G.VENKATASWAMY NAIDU COLLEGE (AUTONOMOUS)

(Re-Accredited with "A" Grade by NAAC)

Department of PG Diploma in Cyber Security

P26DCS1P1 - Cyber Security Lab (Linux & Tools)

Code	Category	Course Title	Lecture Hours	Tutorial Hours	Practical Hours	Credits
P26DCS1P1	Core Lab–1	Cyber Security Lab (Linux & Tools)	0	0	3	4

Year	Semester	Internal Marks(CIA)	External Marks(ESE)	Total Marks
I	I	50	50	100

Course Objectives

- This course focuses on practical exposure to the Linux operating system and its applications in cyber security practices and system protection
- It develops skills in using cyber security tools and techniques for system monitoring, network analysis, vulnerability assessment, and security configuration
- It introduces real-time cyber security scenarios and safe computing practices using open-source security tools and environments

Course Outcomes

Upon completion of the Course, students will be able to

CO	Course Outcome	Knowledge Level(RBT)
CO1	work with Linux operating system and execute basic commands.	K1,K2,K3,K4,K5
CO2	configure users, permissions, and system settings securely.	K1,K2,K3,K4,K5
CO3	use basic cyber security tools for network scanning and monitoring.	K1,K2,K3,K4,K5
CO4	analyze network traffic and identify potential threats.	K1,K2,K3,K4,K5
CO5	perform simple vulnerability assessments and security practices.	K1,K2,K3,K4,K5

(K1-Remember, K2-Understand, K3-Apply, K4-Analyze, K5-Evaluate, K6-Create)

CO - PO & PSO Mapping

CO	POs							PSOs		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2	PSO3
CO1	3	2	2	2	3	2	2	3	2	2
CO2	2	3	2	3	3	2	2	3	3	2
CO3	2	2	3	3	2	2	2	3	3	2
CO4	3	2	3	3	2	2	2	3	3	3
CO5	2	3	3	3	3	2	2	3	3	3
Total	12	12	13	14	13	10	10	15	14	12

(3-Strong, 2-Medium, 1-Weak, 0-No Correlation)

Course Content

List of Practicals **(P-3 hrs)**

1. Basic Linux commands – File and directory operations (ls, cd, mkdir, rm, cp, mv).

2. User and permission management in Linux (chmod, chown, useradd).
3. Working with file systems and text editors (nano, vi).
4. Process management commands (ps, top, kill).
5. Network configuration commands (ifconfig/ip, ping, netstat, traceroute).

Text Books

1. Linux Command Line and Shell Scripting Bible, Richard Blum and Christine Bresnahan, Linux Command Line and Shell Scripting Bible, 4th Edition, Wiley Publishing, 2020.
2. The Linux Command Line, William E. Shotts Jr., The Linux Command Line: A Complete Introduction, 2nd Edition, No Starch Press, 2019.

Reference Books

1. Charles P. Pfleeger Shari Lawrence Pfleeger Jonathan Margulies (2015), Security in Computing, 5th Edition , Pearson Education .

Web Resources

1. https://www.geeksforgeeks.org/cybersecurity/what-is-cyber-security/
2. https://www.geeksforgeeks.org/linux-unix/linux-tutorial/
3. https://www.geeksforgeeks.org/ethical-hacking/kali-linux-tutorial/
4. https://www.w3schools.com/cybersecurity/
5. https://hackertarget.com/cyber-security-detectionlab/

Course Designer

Dr.S.Suganthi, Assistant Professor, Department of Computer Science

G.VENKATASWAMY NAIDU COLLEGE (AUTONOMOUS)

(Re-Accredited with "A" Grade by NAAC)

Department of PG Diploma in Cyber Security

P26DCS1P2 - Network & System Administration Lab

Code	Category	Course Title	Lecture Hours	Tutorial Hours	Practical Hours	Credits
P26DCS1P2	Core Lab-2	Network & System Administration Lab	0	0	3	4

Year	Semester	Internal Marks(CIA)	External Marks(ESE)	Total Marks
I	I	50	50	100

Course Objectives

- This course emphasizes practical training in configuring, managing, and maintaining computer networks and system environments
- It develops skills in system administration using Linux and Windows platforms, including network setup, troubleshooting, and maintenance activities
- It familiarizes students with server configuration, basic networking services, and essential security practices in network and system administration

Course Outcomes

Upon completion of the Course, students will be able to

CO	Course Outcome	Knowledge Level(RBT)
CO1	install and configure operating systems and manage system resources.	K1,K2,K3,K4,K5
CO2	perform user management and access control in different environments.	K1,K2,K3,K4,K5
CO3	configure and troubleshoot basic network settings.	K1,K2,K3,K4,K5
CO4	manage servers and network services at a basic level.	K1,K2,K3,K4,K5
CO5	apply security practices in system and network administration.	K1,K2,K3,K4,K5

(K1-Remember, K2-Understand, K3-Apply, K4-Analyze, K5-Evaluate, K6-Create)

CO - PO & PSO Mapping

CO	POs							PSOs		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2	PSO3
CO1	3	2	2	2	3	2	2	3	2	2
CO2	2	3	2	3	3	2	2	3	3	2
CO3	2	2	3	3	2	2	2	3	3	2
CO4	3	2	3	3	2	2	2	3	3	3
CO5	2	3	3	3	3	2	2	3	3	3
Total	12	12	13	14	13	10	10	15	14	12

(3-Strong, 2-Medium, 1-Weak, 0-No Correlation)

Course Content

List of Practicals **(P-3 hrs)**

1. Disk partitioning and file system management.

3. User account creation and management in Windows
4. Configuring user permissions and access control.
5. Basic network setup – IP addressing and subnetting (manual configuration).
6. Network troubleshooting using ping, traceroute, ipconfig/ifconfig.
7. Sharing files and printers over network (Windows/Linux).

Text Books

1. Windows Server Administration Fundamentals, Andrew Warren, Windows Server Administration Fundamentals, 2nd Edition, Microsoft Press, 2016.
2. Mastering Windows Server, Jordan Krause, Mastering Windows Server 2019, 1st Edition, Packt Publishing, 2019.

Web Resources

1. https://www.geeksforgeeks.org/computer-networks/computer-network-tutorials/
2. https://www.udemy.com/course/ultimate-network-administrator-course/?utm_campaign=Search_Keyword_Beta_Prof_la.ES_cc.ROW-Spanish&utm_source=google&utm_medium=paid-search&portfolio=ROW-Spanish&utm_audience=mx&utm_tactic=nb&utm_term=_._ag_167955721111_._ad_762942519356_._kw_unix%20tutorial&utm_content=g&funnel=&test=&gad_source=1&gad_campaignid=21487757259&gbraid=0AAAADROdO0suhch1OHjzkyziUV-d4BGj&gclid=CjwKCAjw4ufOBhBkEiwAfuC7-aGUBS5jA4AT0x4g__WkBT_yScxRowQ9rZbL9LIbp3ca9ffHxnq0mhoCNb4QAvD_BwE
3. https://www.wiley.com/en-in/terms-of-use/

Course Designer

Dr.S.Suganthi, Assistant Professor, Department of Computer Science

G.VENKATASWAMY NAIDU COLLEGE (AUTONOMOUS)

(Re-Accredited with "A" Grade by NAAC)

Department of PG Diploma in Cyber Security

P26DCS203 - Ethical Hacking & Penetration Testing

Code	Category	Course Title	Lecture Hours	Tutorial Hours	Practical Hours	Credits
P26DCS203	Core–3	Ethical Hacking & Penetration Testing	2	0	0	4

Year	Semester	Internal Marks(CIA)	External Marks(ESE)	Total Marks
I	II	40	60	100

Course Objectives

- This course focuses on the concepts and methodologies of ethical hacking and penetration testing, including common cyber attacks and system vulnerabilities
- It develops knowledge of various tools and techniques used in ethical hacking for identifying and assessing security weaknesses in controlled environments
- It enables students to perform basic security testing while creating awareness about the legal and ethical aspects of cyber security practices

Course Outcomes

Upon completion of the Course, students will be able to

CO	Course Outcome	Knowledge Level(RBT)
CO1	understand ethical hacking concepts, phases, and legal issues.	K1,K2,K3,K4,K5
CO2	perform basic scanning and enumeration to identify vulnerabilities.	K1,K2,K3,K4,K5
CO3	analyze system hacking techniques and malware threats.	K1,K2,K3,K4,K5
CO4	identify common web and network attacks.	K1,K2,K3,K4,K5
CO5	apply penetration testing methodology and recommend security measures.	K1,K2,K3,K4,K5

(K1-Remember, K2-Understand, K3-Apply, K4-Analyze, K5-Evaluate, K6-Create)

CO - PO & PSO Mapping

CO	POs							PSOs		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2	PSO3
CO1	3	2	2	2	3	2	2	3	3	2
CO2	2	3	2	3	3	2	2	3	2	3
CO3	2	2	3	3	2	2	3	2	3	2
CO4	3	2	3	3	2	2	2	3	3	3
CO5	2	3	2	2	3	3	2	3	3	2
Total	12	12	12	13	13	11	11	14	14	12

(3-Strong, 2-Medium, 1-Weak, 0-No Correlation)

Course Content

Unit-I Introduction to Ethical Hacking **(L-6 hrs)**

Ethical hacking concepts – Types of hackers – Phases of ethical hacking – Footprinting and reconnaissance –

Information gathering techniques – Introduction to penetration testing – Legal and ethical considerations.

Unit-II Scanning and Enumeration **(L-6 hrs)**

Network scanning concepts – Port scanning – Vulnerability scanning – Tools (Nmap basics) – Enumeration techniques – DNS enumeration – NetBIOS enumeration – Identifying active hosts and services.

Unit-III System Hacking and Malware **(L-6 hrs)**

Password cracking techniques – Authentication attacks – Privilege escalation – Malware concepts – Keyloggers – Backdoors – Countermeasures for system attacks.

Unit-IV Web and Network Attacks **(L-6 hrs)**

Web application attacks – SQL injection (basic concept) – Cross-site scripting (XSS) – Phishing attacks – Denial of Service (DoS/DDoS) – Session hijacking – Wireless network attacks (basics).

Unit-V Penetration Testing and Security Measures **(L-6 hrs)**

Penetration testing methodology – Planning and reconnaissance – Scanning and exploitation – Post-exploitation – Reporting and documentation – Security tools overview (Metasploit, Burp Suite basics) – Preventive measures and best practices.

Text Books

1. Vakul Sharma (2011). Information Technology Law and Practice. Universal Law Publishing.
2. Whitman, M., & Mattord, H. (2018). Principles of Information Security. Cengage Learning.

Reference Books

1. Allen, J. (2012). The Hacker Playbook. CreateSpace.
2. Erickson, J. (2008). Hacking: The Art of Exploitation. No Starch Press.
3. Scarfone, K., & Souppaya, M. (2011). Guide to Penetration Testing. NIST.

Web Resources

1. https://owasp.org
2. https://www.kali.org/tools/
3. https://www.eccouncil.org

Course Designer

Dr.S.Suganthi, Assistant Professor, Department of Computer Science

G.VENKATASWAMY NAIDU COLLEGE (AUTONOMOUS)

(Re-Accredited with "A" Grade by NAAC)

Department of PG Diploma in Cyber Security

P26DCS204 - Cyber Laws, Risk & Security Management

Code	Category	Course Title	Lecture Hours	Tutorial Hours	Practical Hours	Credits
P26DCS204	Core-4	Cyber Laws, Risk & Security Management	2	0	0	4

Year	Semester	Internal Marks(CIA)	External Marks(ESE)	Total Marks
I	II	40	60	100

Course Objectives

- This course provides an understanding of the legal and regulatory framework governing cyberspace, digital activities, and information security practices
- It develops awareness of cyber risks, threats, and security management techniques, including risk identification and assessment methods
- It familiarizes students with cyber laws, IT Act provisions, security policies, standards, regulatory compliance, and incident management procedures

Course Outcomes

Upon completion of the Course, students will be able to

CO	Course Outcome	Knowledge Level(RBT)
CO1	understand cyber laws, IT Act, and legal aspects of digital activities.	K1,K2,K3,K4,K5
CO2	identify different types of cyber crimes and legal procedures.	K1,K2,K3,K4,K5
CO3	analyze risks and apply risk management strategies.	K1,K2,K3,K4,K5
CO4	develop and implement basic information security policies.	K1,K2,K3,K4,K5
CO5	understand security governance, compliance, and incident management.	K1,K2,K3,K4,K5

(K1-Remember, K2-Understand, K3-Apply, K4-Analyze, K5-Evaluate, K6-Create)

CO - PO & PSO Mapping

CO	POs							PSOs		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2	PSO3
CO1	3	2	2	2	3	2	2	3	3	2
CO2	2	3	2	3	3	2	2	3	2	3
CO3	2	2	3	3	2	2	3	2	3	2
CO4	3	2	3	3	2	2	2	3	3	3
CO5	2	3	2	2	3	3	2	3	3	2
Total	12	12	12	13	13	11	11	14	14	12

(3-Strong, 2-Medium, 1-Weak, 0-No Correlation)

Course Content

Unit-I Introduction to Cyber Laws **(L-6 hrs)**

Cyber law – Definition and scope – Need for cyber laws – Overview of Information Technology (IT) Act – Digital

signatures – Electronic records – Legal recognition of electronic transactions – Cyber law issues in India.

Unit-II Cyber Crimes and Legal Framework **(L-6 hrs)**

Types of cyber crimes – cyber stalking – Cyber crime investigation basics – Digital evidence – Cyber crime reporting procedures – Role of law enforcement agencies – Penalties and offences under IT Act.

Unit-III Risk Management in Cyber Security **(L-6 hrs)**

Risk concepts – Threat, vulnerability, risk – Risk assessment and analysis – Risk management process – Risk mitigation strategies – Business continuity planning (BCP) – Disaster recovery planning (DRP).

Unit-IV Information Security Management **(L-6 hrs)**

Information security management concepts – Security policies and procedures – Access control models – Identity and access management – Security awareness and training.

Unit-V Security Governance and Incident Management **(L-6 hrs)**

Security governance – Compliance and auditing – Incident response process – Handling security breaches – Logging and monitoring – Privacy and data protection – Emerging trends in cyber law and security.

Text Books

1. CEH v11 Study Guide, Walker, M. (2021). Certified Ethical Hacker Study Guide. Wiley.
2. Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press.

Reference Books

1. Godbole, N. (2017). Information Systems Security. Wiley India.
2. Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards. Auerbach Publications.
3. Easttom, C. (2018). Computer Security Fundamentals. Pearson.

Web Resources

1. https://www.meity.gov.in
2. https://cybercrime.gov.in
3. https://www.iso.org

Course Designer

Dr.S.Suganthi, Assistant Professor, Department of Computer Science

G.VENKATASWAMY NAIDU COLLEGE (AUTONOMOUS)

(Re-Accredited with "A" Grade by NAAC)

Department of PG Diploma in Cyber Security

P26DCS2P3 - Ethical Hacking Lab

Code	Category	Course Title	Lecture Hours	Tutorial Hours	Practical Hours	Credits
P26DCS2P3	Core Lab–3	Ethical Hacking Lab	0	0	3	4

Year	Semester	Internal Marks(CIA)	External Marks(ESE)	Total Marks
I	II	50	50	100

Course Objectives

- This course emphasizes practical exposure to ethical hacking tools and techniques for assessing the security of systems and networks
- It develops skills in vulnerability identification, penetration testing, threat analysis, and the application of appropriate security countermeasures in controlled environments
- It enables students to apply ethical hacking methodologies and security practices for protecting real-world computing systems and network infrastructures

Course Outcomes

Upon completion of the Course, students will be able to

CO	Course Outcome	Knowledge Level(RBT)
CO1	implement basic ethical hacking tools for reconnaissance and scanning.	K1,K2,K3,K4,K5
CO2	perform network and system vulnerability assessment.	K1,K2,K3,K4,K5
CO3	apply penetration testing techniques on systems and web applications.	K1,K2,K3,K4,K5
CO4	analyze security threats such as malware, sniffing, and spoofing attacks.	K1,K2,K3,K4,K5
CO5	evaluate system security and recommend mitigation strategies.	K1,K2,K3,K4,K5

(K1-Remember, K2-Understand, K3-Apply, K4-Analyze, K5-Evaluate, K6-Create)

CO - PO & PSO Mapping

CO	POs							PSOs		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2	PSO3
CO1	3	2	2	2	3	2	2	3	2	2
CO2	2	3	2	3	3	2	2	3	3	2
CO3	2	2	3	3	2	2	2	3	3	2
CO4	3	2	3	3	2	2	2	3	3	3
CO5	2	3	3	3	3	2	2	3	3	3
Total	12	12	13	14	13	10	10	15	14	12

(3-Strong, 2-Medium, 1-Weak, 0-No Correlation)

Course Content

List of Practicals **(P-3 hrs)**

1. Familiarization with basic Linux commands and environment.
3. Footprinting using WHOIS, nslookup, and traceroute tools.

4. Network scanning using Nmap.
5. Port scanning techniques (TCP, SYN, UDP scans).
6. Enumeration using NetBIOS, SNMP, and SMB tools.

Text Books

1. AMARA Hawthorn, Ethical Hacking 101: Hands-On Labs for Beginners: Learn penetration testing ,Kindle Edition.
2. Linux Basics for Hackers, OccupyTheWeb, Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali Linux, 1st Edition, No Starch Press, 2018.
3. Nmap Network Scanning, Gordon “Fyodor” Lyon, Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning, 1st Edition, Insecure.Com LLC, 2009.

Reference Books

1. Computer Networking: A Top-Down Approach, James F. Kurose and Keith W. Ross, Computer Networking: A Top-Down Approach, 8th Edition, Pearson Education, 2021.
2. UNIX and Linux System Administration Handbook, Evi Nemeth, Garth Snyder, Trent R. Hein, and Ben Whaley, UNIX and Linux System Administration Handbook, 5th Edition, Pearson Education, 2017.

Web Resources

1. https://www.geeksforgeeks.org/ethical-hacking/ethical-hacking-tutorial/
2. https://www.udemy.com/course/kali-linux-hacking/?srsltid=AfmBOoqCy83HwdZTVodhYRuiaH7JiBwOnK7Stvw27F7hTJatGEQmmK4d
3. https://www.netacad.com/courses/ethical-hacker?courseLang=en-US

Course Designer

Dr.S.Suganthi, Assistant Professor, Department of Computer Science

G.VENKATASWAMY NAIDU COLLEGE (AUTONOMOUS)

(Re-Accredited with "A" Grade by NAAC)

Department of PG Diploma in Cyber Security

P26DCS2P4 - Security Tools Lab (Wireshark, Metasploit)

Code	Category	Course Title	Lecture Hours	Tutorial Hours	Practical Hours	Credits
P26DCS2P4	Core Lab-2	Security Tools Lab (Wireshark, Metasploit)	0	0	3	4

Year	Semester	Internal Marks(CIA)	External Marks(ESE)	Total Marks
I	II	50	50	100

Course Objectives

- This course provides practical exposure to network security and penetration testing tools used for analyzing and securing computer networks
- It develops skills in capturing, monitoring, and analyzing network traffic using Wireshark, as well as identifying vulnerabilities through the Metasploit Framework
- It enables students to perform basic exploitation techniques in controlled environments and apply security tools to detect, analyze, and mitigate cyber threats

Course Outcomes

Upon completion of the Course, students will be able to

CO	Course Outcome	Knowledge Level(RBT)
CO1	capture and analyze network packets using Wireshark.	K1,K2,K3,K4,K5
CO2	identify network protocols and detect suspicious traffic patterns.	K1,K2,K3,K4,K5
CO3	use Metasploit Framework for vulnerability scanning and exploitation.	K1,K2,K3,K4,K5
CO4	perform basic penetration testing using security tools.	K1,K2,K3,K4,K5
CO5	analyze security issues and recommend mitigation techniques.	K1,K2,K3,K4,K5

(K1-Remember, K2-Understand, K3-Apply, K4-Analyze, K5-Evaluate, K6-Create)

CO - PO & PSO Mapping

CO	POs							PSOs		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PSO1	PSO2	PSO3
CO1	3	2	2	2	3	2	2	3	2	2
CO2	2	3	2	3	3	2	2	3	3	2
CO3	2	2	3	3	2	2	2	3	3	2
CO4	3	2	3	3	2	2	2	3	3	3
CO5	2	3	3	3	3	2	2	3	3	3
Total	12	12	13	14	13	10	10	15	14	12

(3-Strong, 2-Medium, 1-Weak, 0-No Correlation)

Course Content

List of Practicals **(P-3 hrs)**

1. Installation of Wireshark and Metasploit Framework.

2. Introduction to network interfaces and packet capture in Wireshark.
3. Capturing live network traffic using Wireshark.
4. Filtering packets using Wireshark filters (IP, TCP, HTTP).
5. Identifying suspicious packets and network anomalies.
6. Password capture and analysis in a controlled environment.

Text Books

1. METASPLOIT. 2011 by David Kennedy, Jim O\'Gorman, Devon Kearns, and Mati Aharoni
2. Jessey Bullock with Jeff T. Parker , Wireshark® for Security Professionals, Wiley.

Reference Books

1. Practical Packet Analysis, Chris Sanders, Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems, 3rd Edition, No Starch Press, 2017.
2. Wireshark Network Analysis, Laura Chappell, Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide, 2nd Edition, Chappell University, 2012.

Web Resources

1. https://docs.metasploit.com/?utm_source=chatgpt.com
2. https://docs.metasploit.com/?utm_source=chatgpt.com

Course Designer

Dr.S.Suganthi, Assistant Professor, Department of Computer Science