

UNIVERSITY OF MYSORE
Established: 1916

Vishwavidyanilaya Karyasoudha
Crawford Hall, Mysore-570 005

No.AC.2(S)/151/2021-22

Dated: 18.08.2021

NOTIFICATION

Sub: Introducing PG Diploma in Network and Cyber security (Two semesters) Programme from the academic year 2021-22.

Ref: 1. Decision of Board of Studies in Information Technology and Multimedia (CIST) (PG) meeting held on 27.11.2020.

2. Decision of the Faculty of Science & Technology Meeting held on 08.02.2021.


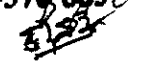
3. Decision of the Academic Council meeting held on 07.04.2021.

The Board of Studies in Information Technology and Multimedia (CIST) (PG) which met on 27.11.2020 has approved the regulations and the syllabus of two semesters Post Graduation Diploma in network and Cyber Security Programme at CIST from the academic year 2021-22.

The Faculty of Science and Technology and Academic Council meeting held on 08.02.2021 and 07.04.2021 respectively have approved the above said proposal and the same is hereby notified.

The detailed Syllabus and Regulations Information Technology and Multimedia (CIST) (PG) course is annexed. The contents may be downloaded from the University Website i.e., www.uni-mysore.ac.in.

DRAFT APPROVED BY THE REGISTRAR


DEPUTY REGISTRAR (ACADEMIC)
Deputy Registrar (Academic)
University of Mysore
Mysore-570 005


To:

1. The Registrar (Evaluation), University of Mysore, Mysore.
2. The Dean, Faculty of Science & Technology, DoS in Psychology, MGM.
3. The Chairperson, BoS in Information Technology and Multimedia (CIST) (PG), Manasagangotri, Mysore.
4. The Director, Centre for Information Science & Technology (CIST), MGM.
5. The Deputy/Assistant Registrar/Superintendent, AB and EB, UOM, Mysore.
6. The P.A. to the Vice-Chancellor/Registrar/Registrar (Evaluation), UOM, Mysore.
7. Office file.

UNIVERSITY OF MYSORE

REGULATIONS

for

**Post Graduate Diploma in Network & Cyber
Security (PGDNCS)**

Choice based Credit System

Effective from the Academic Year 2021-22

UNIVERSITY OF MYSORE
Regulations for the Post Graduate Diploma in Network & Cyber Security (PGDNCS)
(Choice based Credit System)
(Effective from the academic year 2021-22)

The program shall be called Post Graduate Diploma in Network & Cyber Security (PGDNCS). It is one-year duration consisting of two semesters in the Faculty of Science and Technology with a provision to study on a full-time basis. The course shall be governed by the following regulations:

1. ELIGIBILITY FOR ADMISSION

- 1.1.** A candidate who has passed B.C.A/ B.Tech/ B.E/ B.Sc degree with Computer Science or Mathematics as one of the optional/ any Bachelor's degree with one-year diploma in Computer Application/ PGDSD/ with a minimum of 45% marks in aggregate (40% in case of SC/ST and Cat-1) from a recognized University is eligible for admission to the first semester of the program.
- 1.2.** There shall be two streams; Stream-1: From 10 a.m. to 5 p.m., In case there are vacant seats in Stream 2, such seats shall be filled by other students in accordance to roster system. In the case of high demand, depending on the availability of faculty and infrastructure, more than one section can be formed.

2. INTAKE

- 2.1.** There shall be an intake of maximum or minimum of seats in accordance to University norms.
- 2.2.** The merit of the candidate is the aggregate percentage of marks of all years of the Bachelor's degree examination.
- 2.3.** The selection of eligible candidates for admission to course shall be based on merit-cum reservation policy of the government of Karnataka from time to time.

3. COURSE OF STUDY

- 3.1.** The course of study for the Post Graduate Diploma in Network & Cyber Security (PGDNCS) shall extend over a period of one year consisting of two semesters. Each semester shall be of sixteen weeks duration. The academic calendar shall be as notified by the university from time to time. However, a candidate can take a maximum of two years for completion as per double the duration norms of the University of Mysore.
- 3.2.** The medium of instruction shall be English.
- 3.3.** There shall be five papers of theory with practical in the first semester. There shall be four papers with practical and one project work in the second semester. The hours of instruction shall be two hours/week for each theory paper and four hours (two hours duration Two times a week) for each practicals.

4. ATTENDANCE, PROGRESS AND CONDUCT

- 4.1.** Each semester shall be taken as a unit to calculate attendance.

4.2. The students shall attend practicals and theory classes as prescribed by the University during each semester.

4.3. A student shall be considered to have completed a semester, if the student has attended not less than 75% of number of working periods of the course during the said semester.

4.4. The student who fails to complete the course in the manner stated in 4.3 above shall not be permitted to appear for the University examinations. Such a candidate shall enroll himself/herself in the coming two years. However, the admission is subject to the availability of the seats.

4.5. If the conduct/ behaviour of the student is not found to be satisfactory, action will be initiated as per the University regulations.

5. CREDIT PATTERN & SCHEME OF EXAMINATION

5.1 There shall be a University examination at the end of each semester. The duration of theory and practical examination shall be two hours duration.

5.2 The duration and maximum marks and minimum marks for pass in each of the theory and practical shall be as given below:

PGDNCS PROGRAM

First Semester

Paper	Theory Papers and Practicals	Credits in LTP pattern			Total Credits
		Lesson(L) (2hrs /week)	Tutorial(T)	Practical(P) (4hrs /week)	
PGDMT -1.1	Operating System & Network Concepts	2	0	2	4
PGDMT -1.2	Cyber Security	2	0	2	4
PGDMT -1.3	Network Programming using Python	2	0	2	4
PGDMT -1.4	Infrastructure Security	2	0	2	4
PGDMT -1.5	Ethical Hacking	2	0	2	4

Second Semester

Paper	Theory Papers and Practicals	Credits in LTP pattern			
		Lesson(L) (2hrs /week)	Tutorial(T)	Practical(P) (4hrs /week)	Total Credits
PGDMT -2.1	Cyber Law	2	0	2	4
PGDMT -2.2	Cryptography & Data Security	2	0	2	4
PGDMT -2.3	Social Network Analysis	2	0	2	4
PGDMT -2.4	Digital Forensics	2	0	2	4
PGDMT -2.5	PROJECT	2	0	2	4

SCHEME OF EXAMINATION

For each Paper	Marks Allocation						Total	
	IA		Theory		Practical			
	Max.	Min.	Max.	Min.	Max.	Min.	Max.	Min.
	20	7	50	18	30	11	100	40

5.3 In the Practical examination each student should execute one question out of the specified practical questions approved in the syllabus. Change of program during lab examinations is not permitted because all the Programmes are given from the predefined list from the syllabus only.

*In case of practical examination, the following scheme shall be followed: Writing procedure – **05 marks, Execution -12 marks, Viva-voce – 8 record-05 marks**

**In case of Project, the following scheme shall be followed:

Project Demonstration/execution: 30 marks, Viva-voce: 20 marks, Dissertation: 30 marks

5.4 The internal assessment marks in each theory paper shall be awarded by the concerned course teacher based on (i) two class tests, each of one-hour duration, conducted by him/ her during the semester, (ii) Assignment, and (iii) one seminar. Average of the two tests to be considered as the final internal assessment marks. Internal assessment: 20 marks Test1: 15 marks Test2: 15 marks Assignment: 5 marks Seminar: 5 marks

5.5 Candidate shall submit two copies of the dissertation along with CD/DVD on project work during the second semester for evaluation. The project viva shall be conducted by one internal examiner and one external examiner approved by the Registrar (Evaluation).

6 DECLARATION OF RESULTS AND CLASSIFICATION OF SUCCESSFUL CANDIDATES

6.1 The candidate who obtains a minimum of 35% of marks in each of the theory and practical examination and a minimum of 40% of marks of theory/practical/Project examination and Internal Assessment marks put together shall be declared to have passed in the respective paper. The candidate is declared to have passed the semester if he/she passes in all the papers. The candidate who fails to get such minimum marks in any paper(s) shall repeat the theory / practical examination of that paper. The Internal Assessment marks once

awarded is final and there is no provision for improvement. Minimum Credits for getting the Diploma: 20 credits from 2 semesters.

6.2 The Grades shall be declared based on aggregate marks obtained by the candidate, who has completed both semesters of the course.

6.3 The classification of credits of successful candidates shall be as under:

Grades in each paper:

1. Marks secured in the paper is 90% and above - A Grade
2. Marks secured in the paper is 80% and above but less than 90% - B Grade
3. Marks secured in the paper is 70% and above but less than 80% - C Grade
4. Marks secured in the paper is 60% and above but less than 70% - D Grade
5. Marks secured in the paper is 50% and above but less than 60% - E Grade
6. Marks secured in the paper is 40% and above but less than 50% - F Grade
7. Marks secured in the paper is less than 40% - Dropped

SYLLABUS

FIRST SEMESTER

PGDNCS-1.1- Operating System & Network Concepts

UNIT-1

Operating System- An Introduction, Operating System Architecture, Process Management, Introduction to Operating Systems :(Microsoft Windows, UNIX and Linux on the Network Setup and Management including-Hardware/Software configuration of Gateway, Overview of Network Services: Remote Administration and Access Services, Directory Services, Other NOS Services. Routers, and Switches. Desktop, Network Operating Systems Overview). Introduction to Network Operating Systems :(Characteristics of a Network Operating System. Windows NT/2000 and Linux. Software Requirements for a Linux NOS).

UNIT-2

Network Models, Client-Server Applications, Network Hardware, The Seven-Layer OSI Model , Safety Procedures and Policies, Network Infrastructure and Documentation-Components of Structured Cabling, Network Documentation , Change Management, Addressing on Networks-Addressing Overview, MAC Addresses, IP Addresses, Ports and Sockets, Domain Names and DNS (Domain Name System)

Network Protocols and Routing: TCP/IP Core Protocols, Routers and How They Work, Network Cabling, Transmission Basics, Copper Cable and its types, Fiber-Optic Cable and its types

UNIT-3

Wireless Networking: Characteristics of Wireless Transmissions, Wireless Standards for the IoT (Internet of Things), 802.11 WLAN Standards, Implementing a Wi-Fi Network, Wi-Fi Network Security

UNIT-4

Virtualization and Cloud Computing: Virtualization, Cloud Computing, Encryption Protocols, Remote Access, Network Risk Management-Security in Network Design, Network Performance and Recovery, Wide Area Networks

References:

1. *Operating Systems with Windows NT Lab Exercises and Solutions.pdf*. (n.d.).
2. *Linux Administration A Beginners Guide 6/E Book Online at Low Prices in India*
3. *Practical Guide to Linux Commands, Editors, and Shell Programming, A, 3rd Edition*. (n.d.).

PGDNCS-1.2- CYBER SECURITY

UNIT 1

Cyber Crime- Overview, Internal and External Attacks, Attack Vectors. Cybercrimes against Individuals – E-mail spoofing and online frauds, Phishing and its forms, Spamming, Cyber-defamation, Cyberstalking, Cyber Bullying and harassment, Computer Sabotage, Pornographic offenses, Password Sniffing. Keyloggers and Screenloggers. Cyber Crimes against Women and Children.

UNIT 2

Cybercrime against the organization – Unauthorized access of a computer, Password Sniffing, Denial-of-service (DOS) attack, Backdoors and Malware, and its types, E-mail Bombing, Salami attacks, Software Piracy, Industrial Espionage, Intruder attacks. Security policies violations, Crimes related to Social Media, ATM, Online, and Banking fraud. Intellectual Property Frauds. Cyber Crimes against Women and Children

UNIT 3

Introduction to Cyber Security

Overview of Cyber Security, Internet Governance – Challenges and Constraints, Cyber Threats:- Cyber Warfare-Cyber Crime-Cyber terrorism-Cyber Espionage, Need for a Comprehensive Cyber Security Policy, Need for a Nodal Authority, Need for an International Convention on Cyberspace.

UNIT 4

Cyber Security Vulnerabilities and Cyber Security Safeguards:Cyber Security Vulnerabilities-Overview, vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Unprotected Broadband communications, Poor Cyber Security Awareness. Cyber Security Safeguards- Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, Firewalls, Intrusion Detection Systems, Response, Scanning, Security policy, Threat Management.

TEXTBOOKS

1. Balkin, J. M. (2007). *Cybercrime: Digital Cops in a Networked Environment* (K. Eddan, J. Grimmelmann, N. Kozlovski, S. Wagman, & T. Zarsky, Eds.). NYU Press.
2. Loundy, D. J. (2003). *Computer Crime, Information Warfare & Economic Espionage*. Carolina Academic Pr.

REFERENCES

1. *Cybercrime: The Investigation, Prosecution and Defense of a Computer-related Crime:*

- Ralph D. Clifford: 9781594608537: Amazon.com: Books.* (n.d.).
2. *Kerr's Computer Crime Law: (American Casebook Series): Orin S. Kerr: 9780314144003: Amazon.com: Books.* (n.d.).
 3. *Secrets of Computer Espionage: Tactics and Countermeasures: McNamara, Joel: 9780764537103: Amazon.com: Books.* (n.d.).
 4. Stephenson, P., & Gilbert, K. (1999). *Investigating Computer-Related Crime* (1st edition). CRC Press.
 5. *Understanding And Managing Cybercrime: McQuade, Samuel C., III: 9780205439737: Amazon.com: Books.* (n.d.).
 6. Nina Godbole and Sunit Belapore; "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley Publications, 2011.
 7. Shon Harris, "All in One CISSP, Exam Guide Sixth Edition", McGraw Hill, 2013.
 8. Bill Nelson, Amelia Phillips and Christopher Steuart; "Guide to Computer Forensics and Investigations" – 3 rd Edition, Cengage, 2010 BBS.
 9. William Stallings; "Cryptography and Network Security: Principles and Practices", Fifth Edition, Prentice Hall Publication Inc., 2007.
 10. Atul Jain; "Cyber Crime: Issues, Threats and Management", 2004.
 11. Majid Yar; "Cybercrime and Society", Sage Publications, 2006.
 12. Michael E Whiteman and Herbert J Mattord; "Principles of Information Security", Vikas Publishing House, New Delhi, 2003.
 13. Matt Bishop, "Computer Security Art and Science", Pearson/PHI, 2002.
 14. *Web Application Security, A Beginner's Guide Book Online at Low Prices in India*
 15. *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity (Advanced Sciences and Technologies for Security Applications): Jahankhani, Hamid, Kendzierskyj, Stefan, Chelvachandran, Nishan, Ibarra, Jaime: 9783030357450: Amazon.com: Books.* (n.d.).
 16. *Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, 2nd Edition: Diogenes, Yuri, Ozkaya, Erdal: 9781838827793: Amazon.com: Books.* (n.d.).
 17. *Guide to Intrusion Detection and Prevention Systems (IDPS): Nist: 9781494758813: Amazon.com: Books.* (n.d.).
 18. M, L. (n.d.). *Top 7 Cyber Security Books To Read For Beginners in 2020.* BitDegree.Org Online Learning Platforms.
 19. *Network Intrusion Detection and Prevention—Concepts and Techniques | Ali A. Ghorbani | Springer.* (n.d.).
 20. *Securing Web Applications [Book].* (n.d.).
 21. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy: Engebretson, Patrick: 9780124116443*

PGDNCS-1.3-Network Programming using Python

UNIT 1

Sockets, Ipv4, And Simple Client/Server Programming: Introduction Printing The Machine's Name And Ipv4 Address, Retrieving A Remote Machine's IP Address, Converting An Ipv4 Address To Different Formats, Finding A Service Name, Given The Port And Protocol, Converting Integers To And, Rom Host To Network Byte Order, Setting And Getting The Default Socket Timeout, Handling Socket Errors Gracefully, Modifying A Socket's Send/Receive Buffer Size, Changing A Socket To The Blocking/Non-Blocking Mode, Reusing Socket Addresses, Printing

The Current Time, Rom The Internet Time Server, Writing A SNTP Client, Writing A Simple Echo Client/Server Application.

Multiplexing Socket I/O for Better Performance: Using, working MixIn in the socket server applications, Using Threading MixIn in the socket server applications, Writing a chat server using select, Multiplexing a web server using select. epoll, Multiplexing an echo server using Diesel concurrent library.

UNIT 2

IPv6, Unix Domain Sockets, and Network Interfaces: Forwarding a local port to a remote host, Pinging hosts on the network with ICMP, Waiting for a remote network service, Enumerating interfaces on the machine, Finding the IP address for a specific interface on the machine, Finding whether an interface is upon the machine, Detecting inactive machines on the network, Performing a basic IPC using connected sockets (socketpair), Performing IPC using Unix domain sockets, Finding out if the Python supports IPv6 sockets, Extracting an IPv6 prefix from an IPv6 address, Writing an IPv6 echo client/server.

Programming with HTTP for the Internet: Downloading data from an HTTP server, Serving HTTP requests from the machine, Extracting cookie information after visiting a website, Submitting web forms, Sending web requests through a proxy server, Checking whether a web page exists with the HEAD request, Spoofing Mozilla Firefox in the client code, Saving bandwidth in web requests with the HTTP compression, Writing an HTTP fail-over client with resume and partial downloading, Writing a simple HTTPS server code with Python and OpenSSL.

UNIT 3

E-mail Protocols, FTP, and CGI Programming: Listing the files in a remote FTP server, Uploading a local file to a remote FTP server, E-mailing the current working directory as a compressed ZIP file, Downloading the Google e-mail with POP3, Checking the remote e-mail with IMAP, Sending an e-mail with an attachment via the Gmail SMTP server, Writing a guestbook for the (Python-based) web server with CGI.

Screen-scraping and Other Practical Applications: Searching for business addresses using the Google Maps API, Searching for geographic coordinates using the Google Maps URL, Searching for an article in Wikipedia, Searching for Google stock quote, Searching for a source code repository at GitHub, Reading news feed from BBC, Crawling links present in a web page. **Programming Across Machine Boundaries:** Executing a remote shell command using telnet, Copying a file to a remote machine by SFTP, Printing a remote machine's CPU information, Installing a Python package remotely, Running a MySQL command remotely,

Transferring files to a remote machine over SSH, Configuring Apache remotely to host a website

UNIT 4

Working with Web Services – XML-RPC, SOAP, and REST: Querying a local XML-RPC server, Writing a multithreaded, multical XML-RPC server, Running an XML-RPC server with a basic HTTP authentication, Collecting some photo information from Flickr using REST, Searching for SOAP methods from an Amazon S3 web service, Searching Google for custom information, Searching Amazon for books through product search API

Network Monitoring and Security: Sniffing packets on the network, Saving packets in the pcap format using the pcap dumper, Adding an extra header in HTTP packets, Scanning the ports of a remote host, Customizing the IP address of a packet, Replaying traffic by reading from a saved pcap file, Scanning the broadcast of packets

References:

1. *GitHub—PacktPublishing/Python-Network-Programming-Cookbook-Second-Edition: Python Network Programming Cookbook – Second Edition, published by Packt.* (n.d.).
2. *Learning Python Network Programming—Google Search.* (n.d.).
3. *Mastering Python Networking—Google Search.* (n.d.).
4. *Practical Network Automation: Leverage the Power of Python and Ansible to Optimize Your Network—Google Search.* (n.d.).
5. *Python Network Programming Cookbook eBook: Sarker, Dr. M. O. Faruque: Amazon.in: Kindle Store.* (n.d.).
6. Sarker, D. M. O. F. (2014). *Python Network Programming Cookbook.* Packt Publishing.

PGDNCS-1.4- Infrastructure Security

UNIT-1

Introduction to Infrastructure security: internet infrastructure (internet, ISP, POP, NAP), Introduction to Network Infrastructure Security- LAN, Network of networks, Key components in the Internet infrastructure- Links, Routers, Addressing, Naming System. Internet infrastructure security- Network Information and Network Infrastructure Securities, Importance of Network Infrastructure Security, Difficulties of Securing the Infrastructure-

UNIT-2

Network Infrastructure Security 1 – Switching:- Overview on Layer 2 Functionality, Why Switch Security is Important, How Switches can be Attacked, MAC Flooding- Content Addressable Memory Table, MAC Flooding Attacks, Mitigation, ARP Spoofing, What is ARP, The ARP Poison Process, Limitations of ARP, Solutions (Static ARP Entries: Detection, No Cache Update), STP

attacks, How STP works, Topology Change, STP Attack Scenarios, Countermeasures, VLAN attacks: What is VLAN, How VLAN works, VLAN Hopping Attacks

UNIT-3

Network Infrastructure Security 2 – Routing, Routing basic, Routing protocol vulnerability, Overview of Internet Routing- Interior and Exterior routing protocols(AS, IGP and EGP), Classifications of routing protocol(Distance Vector, Link-State, Path Vector), Popular routing protocols, OSPF, BGP, External and internal attacks, Modification and fabrication, Replication-Internal Attacks, Breaking into router OS, Configure file exposure, Password cracking, Abusing password recovery, RIP Attacks and Countermeasures, Consistency Check Algorithm, Identify a correct update, Identify an incorrect update, Fail to identify an incorrect update, Advantages, and Disadvantages. Pivot-based Algorithm for Inconsistency Recovery, OSPF Attacks and Countermeasures, Cryptography solutions to link state, Hash Chains for Stable Link State, BGP Attacks and Countermeasures- BGP Countermeasure, Operations, Deployment Obstacles, Objectives achieved and its operations

UNIT-4

Network Infrastructure Security 3 - Address Configuration and Naming: DHCP Attack: Basic, DHCP Operations, Attacks, Denial of Service Attack using Address Starvation, Man-in-the-middle Attack using Rogue DHCP server, DNS Redirection Attack using Rogue DHCP server, DNS Attack- DNS Basic, DNS Space, DNS Components, DNS packet format and valid response, Zone transfer, Name Resolution and Caching, DNS Vulnerabilities, Cache Poisoning Attack, Buffer Overflow Attack, Zone Transfer Attack, Dynamic Update Attack, DNSSEC: DNSSEC background, Public-key Cryptography in DNSSEC, New Resource Record (RR) Types in DNSSEC, DNSKEY, RRSIG, NSEC, DS, Example of the use of the DS and DNSKEY records, Example of address resolution with the chain of trust, Cache Poisoning and Compromise of Zone Files, Zone Transfer, Dynamic Update, and DoS, Limitations of DNSSEC

References:

1. *Infrastructure Security—Cloud Security and Privacy [Book]*. (n.d.).
2. Birkholz, E. P., Kenyon, B., & Andrés, S. (2004). *Security Sage's Guide to Hardening the Network Infrastructure* (1st edition). Syngress.
3. Maiwald, E. (2012). *Network Security: A Beginners Guide* (Third edition). McGraw Hill Education.
4. *Network Infrastructure Security | Angus Wong | Springer*. (n.d.).
5. *SANS Institute: Reading Room - Security Basics*. (n.d.).
6. Weaver, R. (n.d.). *Network Infrastructure Security*.
7. Wong, A., & Yeung, A. (2009a). Experiments for Illustrating Network Infrastructure Attacks. In A. Yeung & A. Wong (Eds.), *Network Infrastructure Security* (pp. 181–218). Springer US. https://doi.org/10.1007/978-1-4419-0166-8_5
8. Wong, A., & Yeung, A. (2009b). Introduction to Network Infrastructure Security. In A. Yeung & A. Wong (Eds.), *Network Infrastructure Security* (pp. 1–18). Springer US.
9. Wong, A., & Yeung, A. (2009c). Network Infrastructure Security ' Address Configuration and Naming. In A. Yeung & A. Wong (Eds.), *Network Infrastructure Security* (pp. 137–179). Springer US. https://doi.org/10.1007/978-1-4419-0166-8_4

10. Wong, A., & Yeung, A. (2009d). Network Infrastructure Security – Routing. In A. Yeung & A. Wong (Eds.), *Network Infrastructure Security* (pp. 59–135). Springer US.
https://doi.org/10.1007/978-1-4419-0166-8_3
11. Wong, A., & Yeung, A. (2009e). Network Infrastructure Security ’ Switching. In A. Yeung & A. Wong (Eds.), *Network Infrastructure Security* (pp. 19–58). Springer US.
https://doi.org/10.1007/978-1-4419-0166-8_2
12. Wong, A., & Yeung, A. (2009f). Protecting Network Infrastructure – A New Approach. In A. Yeung & A. Wong (Eds.), *Network Infrastructure Security* (pp. 219–262). Springer US.
https://doi.org/10.1007/978-1-4419-0166-8_6
13. Wong, A., & Yeung, A. (2009g). *Network Infrastructure Security* (2009th edition). Springer.

PGDNCS-1.5- Ethical Hacking

UNIT-1

Hacking: the purpose behind the hacking, hacker, cracking, cracker, hacking as destructive tool- identify theft, email access, website security. **Hacking as a Political Statement, Hacking through Worm Exploits, Hacking as a Learning Tool, Possible Protection from Hackers- Firewalls, routers, updates,** Classification various Kind of hacking: white-hat hacker, black hat hacker, grey hat hacker, blue hat, elite hacker, script kiddie, Neophyte “newbie”, Hactivist, Nation-state, Organized criminal gangs, bots. Computer Security-Computer Crime and Intelligence Agency:- Computer Security, Cybersecurity, computer Threats, Computer Crime, Topology of computer crime, cyber Terrorism, top 10 intelligence agencies of the world

Network systems and DNS working:- Computer Network, Networks are used to types of networks, including LAN, WAN, MAN, HAN, intranet, extranet, internet, VPN, Benefits of networking: File Sharing, Resource Sharing, Program Sharing. Network Host, Network Protocol, IP Address, Types of IP Address, How to Find the IP Address of a Computer?, HTTP, FTP, SMTP, Telnet, WWW, SSH, SSH port forwarding, network port, Domain Name System, Structure of a DNS, Authority, Delegation, and Zone, Resource Records, DNS Queries, Proxy server, Proxy Server – Types

UNIT-2

Various Types of Hacking attacks: Active attacks and its types. Passive Attack. Hacking Tools: Password Cracker Software, Wireless Hacking Tools, Packet Crafting to Exploit Firewall Weaknesses, Traffic Monitoring for Network Related Hacking, Packet Sniffers to Analyze Traffic, Rootkit Detectors to Hack File System, Fuzzers to Search Vulnerabilities, Forensic, Hacking Operating Systems, Encryption Tools, Intrusion Detection System, and the IDs Tools, Hacking Vulnerability Exploitation Tools, Vulnerability Scanners, Web Vulnerability Scanners.

Malware: A hackers Henchman, Types of Malware- Adware, Spyware, Bot, Bug, Ransomware, Rootkit, Trojan Horse, Virus, Worm, Key logger, Zombie Computer, Drive-by-Download, Scareware, Web beacon or web bug, Backdoors, Malware Symptoms, Vulnerability to Malware, Insecure design or user error, Over-privileged users and over-privileged code, Malware prevention and removal, Website Security scans, “air gap” isolation or “parallel Network”, Grayware.

UNIT-3

Common Attacks and Viruses: identification of theft, How does identify theft work? How can one protect them from identity theft?, Spoofing Attacks, Address Resolution Protocol(ARP), DNS server spoofing attacks, Spoofing attack prevention and mitigation(Packet filtering, Avoid trust relationships, Use spoofing detection software, Use cryptographic network protocols), Phishing Attacks, Type of Phishing Attacks, Social Engineering, Shoulder Surfing, Dumpster Diving, Trojan Horses, How to avoid getting infected in the future? How to get rid of trojans? Computer Virus, How Do Viruses Spread, Types of Virus, Some Famous & Worst Computer Virus, Anti-Virus Software, How can you protect yourself?

UNIT-4

Password cracking and hack an Email password: Password cracking and its types. Password cracking Strategy, Penetration Testing, Pen-Testing vs. Vulnerability Assessment, identification of Vulnerabilities, Penetration Testing - its strategies, services. PENETRATION TESTING TOOL:- Reconnaissance, Packet Manipulation, and Password Cracking Tools, Exploitation tool, Manual Penetration Test, Penetration Testing Methodology.

References:

1. Erickson, J. (2008). *Hacking: The Art of Exploitation, 2nd Edition* (2nd edition). No Starch Press.
2. Kim, P. (n.d.). *The Hacker Playbook 2: Practical Guide To Penetration Testing*.
3. Smith, K. (Ed.). (2015). ***Hacking: The Ultimate Hacking for Beginners : How to Hack : Hacking Intelligence : Certified Hacking Book. Kevin Smith.***
4. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy eBook: Engebretson, Patrick: Amazon.in: Kindle Store.* (n.d.).
5. Weidman, G. (2014). *Penetration Testing: A Hands-On Introduction to Hacking* (1st edition). No Starch Press.

SYLLABUS

SECOND SEMESTER

PGDNCS-2.1- CYBER LAW

UNIT 1

Introduction Computers and its Impact in Society, Overview of Computer and Web Technology, Need for Cyber Law, Cyber Jurisprudence at International and Indian Level,

UNIT 2

Cyber Law - International Perspectives UN, & International Telecommunication Union (ITU) Initiatives Council of Europe - Budapest Convention on Cybercrime, Asia-Pacific Economic Cooperation (APEC), Organization for Economic Co-operation and Development (OECD), World Bank, Commonwealth of Nations.

UNIT 3

Constitutional & Human Rights Issues in Cyberspace Freedom of Speech and Expression in Cyberspace, Right to Access Cyberspace – Access to Internet, Right to Privacy, Right to Data Protection

Cyber Crimes & Legal Framework Cyber Crimes against Individuals, Institution and State, Hacking, Digital Forgery, Cyber Stalking/Harassment, Cyber Pornography, Identity Theft, & Fraud Cyber terrorism, Cyber Defamation, Different offenses under IT Act, 2000,

UNIT 4

Cyber Torts Cyber Defamation, Different Types of Civil Wrongs under the IT Act, 2000, Intellectual Property Issues in Cyber Space Interface with Copyright Law, Interface with Patent Law, Trademarks, & Domain Names Related issues Module VII E-Commerce Concept, E-commerce-Salient Features, Online approaches like B2B, B2C, & C2C Online contracts, Click Wrap Contracts, Applicability of Indian Contract Act, 1872

Dispute Resolution in Cyberspace 1. Concept of Jurisdiction 2. Indian Context of Jurisdiction and IT Act, 2000. 3. International Law and Jurisdictional Issues in Cyberspace. 4. Dispute Resolutions

REFERENCES

1. *A Comprehensive Study of Cyber Security And E- Surveillance.* (n.d.).
2. *Computer Law Book Online at Low Prices in India | Computer Law Reviews & Ratings—Amazon.in.* (n.d.).
3. *CyberLaw: The Law of the Internet (eBook, 1996) [WorldCat.org].* (n.d.).
4. Dudeja, V. D. (2003). *Cyber Crimes and Law Enforcement* (2017 edition). Commonwealth

Publishers.

5. *Law*. (n.d.). Indiamart.Com.
6. *The Right to Information Act 2005—Sudhir Naib—Oxford University Press*. (n.d.).

PGDNCS-2.2- Cryptography & Data Security

UNIT-1

Introduction to Cryptography and Data Security: Overview of Cryptology, Symmetric Cryptography, Basics, Simple Symmetric Encryption: The Substitution Cipher. , Cryptanalysis, General Thoughts on Breaking Cryptosystems, How Many Key Bits Are Enough, Modular Arithmetic and More Historical Ciphers, Modular Arithmetic, Integer Rings, Shift Cipher (or Caesar Cipher, Affine Cipher.

UNIT-2

Stream Ciphers: Introduction, Stream Ciphers vs. Block Ciphers, Encryption and Decryption with Stream Ciphers. , Random Numbers and an Unbreakable Stream Cipher, Random Number Generators, The One-Time, Towards Practical Stream Ciphers, Shift Register-Based Stream Ciphers, Linear Feedback Shift Registers (LFSR, Known-Plaintext Attack Against Single LFSRs, Trivium.

UNIT-3

The Data Encryption Standard (DES) and Alternatives: Introduction to DES, Confusion, and Diffusion, Overview of the DES Algorithm, Internal Structure of DES, Initial and Final Permutation, The f-, Key, Security of DES, Exhaustive Key Search, Analytical Attacks, Implementation in Software and Hardware, DES Alternatives, The Advanced Encryption Standard (AES) and the AES Finalist Ciphers, Triple DES (3DES) and DESX, Lightweight Cipher PRESENT, Block Ciphers, Introduction to Public-Key Cryptography, The RSA Cryptosystem, Digital Signatures, Hash Functions, Message Authentication Codes (MACs)

UNIT-4

Attacks on Computer Security: Introduction, the need of security, security approaches, types of attacks, -Internet digital certificate and public key, security protocols-internet security protocols, user authentication, and Kerberos, basics of cryptography in java,.net and operating system.

References:

1. *Introduction to Cryptography: Principles and Applications, 2nd Edition*. (n.d.).
2. *Cryptography and Network Security | 4th Edition Book Online at Low Prices in India*
3. *Understanding Cryptography: A Textbook for Students and Practitioners Book*
4. *Cryptography & network security by atul kahate—PDF Drive*. (n.d)
5. Kahate, A. (2019). *Cryptography and Network Security | 4th Edition* (Fourth edition). McGraw-Hill.

6. Preneel, B., Paar, C., & Pelzl, J. (2011). *Understanding Cryptography: A Textbook for Students and Practitioners* (1st ed. 2010 edition). Springer.

Textbook

1. *D. Stinson Cryptography, Theory and Practice (Third Edition)—Google Search.* (n.d.).
2. *A Comprehensive Study of Cyber Security And E- Surveillance.* (n.d.).
3. *CS 178: Introduction to Cryptography.* (n.d.).

REFERENCES

1. *M. Bellare Introduction to Modern Cryptography—Google Search.* (n.d.).
2. *O. Goldreich. The Foundations of Cryptography—Google Search.* (n.d.).
3. *A Course in Cryptography.* (n.d.).
4. *CSE 526: Cryptography.* (n.d.).
5. Katz, J., & Lindell, Y. (2008). *Introduction to modern cryptography.* Chapman & Hall/CRC.

PGDNCS-2.3- SOCIAL NETWORK ANALYSIS

UNIT 1

Introduction to social network analysis, Descriptive network analysis, Network structure
 Introduction to Web - Limitations of current Web – Development of Semantic Web – Emergence of the Social Web – Statistical Properties of Social Networks -Network analysis - Development of Social Network Analysis - Key concepts and measures in network analysis - Discussion networks - Blogs and online commUNITies - Web-based networks. Node centralities and ranking on a network, Network communities, Affiliation networks

UNIT 2

MODELING AND VISUALIZATION: Visualizing Online Social Networks - A Taxonomy of Visualizations - Graph Representation - Centrality- Clustering - Node-Edge Diagrams - Visualizing Social Networks with Matrix- Based Representations- Node-Link Diagrams - Hybrid Representations - Modelling and aggregating social network data – Random Walks and their Applications –Use of Hadoop and Map Reduce - Ontological representation of social individuals and relationships

UNIT 3

Evolution in Social Networks – Framework - Tracing Smoothly Evolving Communities - Models and Algorithms for Social Influence Analysis - Influence Related Statistics - Social Similarity and Influence - Influence Maximization in Viral Marketing - Algorithms and Systems for Expert Location in Social Networks - Expert Location without Graph Constraints - with Score Propagation

– Expert Team Formation - Link Prediction in Social Networks - Feature-based Link Prediction – Bayesian Probabilistic Models - Probabilistic Relational Models.

UNIT 4

APPLICATIONS

A Learning-Based Approach for Real-Time Emotion Classification of Tweets, A New Linguistic Approach to Assess the Opinion of Users in Social Network Environments, Explaining Scientific and Technical Emergence Forecasting, Social Network Analysis for Biometric Template Protection

Recommended Reading Books

1. Kolaczyk, E. D., & Csárdi, G. (2014). *Statistical Analysis of Network Data with R: 65* (2014 edition). Springer Nature.
2. *Social Network Analysis [1994].pdf*. (n.d.).
3. *Social Network Analysis: Methods and Applications (Structural Analysis in the Social Sciences)* | Stanley Wasserman, Katherine Faust | download. (n.d.).
4. Ajith Abraham, Aboul Ella Hassanien, Václav Snášel, —*Computational Social Network Analysis: Trends, Tools and Research Advances*||, Springer, 2012
5. Borko Furht, —*Handbook of Social Network Technologies and Applications*||, Springer, 1 st edition, 2011
6. Charu C. Aggarwal, —*Social Network Data Analytics*||, Springer; 2014
7. Giles, Mark Smith, John Yen, —*Advances in Social Network Mining and Analysis*||, Springer, 2010.
8. Guandong Xu , Yanchun Zhang and Lin Li, —*Web Mining and Social Networking – Techniques and applications*||, Springer, 1st edition, 2012
9. Peter Mika, —*Social Networks and the Semantic Web*||, Springer, 1st edition, 2007.
10. Przemyslaw Kazienko, Nitesh Chawla,||*Applications of Social Media and Social Network Analysis*||, Springer,2015

Supplementary Reading

1. (PDF) *Securing the Cloud* | Djumhadi, ST.,M.Kom—*Academia.edu*. (n.d.).
2. *Read Securing the Cloud Online* by Vic (J.R.) Winkler | *Books*. (n.d.).
3. Tsvetovat, M., & Kouznetsov, A. (2011). *Social network analysis for startups*. O'Reilly Media Inc.
4. Winkler, V. (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics* (1st edition). Syngress.
5. Zafarani, R. (2014). *Social Media Mining*. Cambridge University Press.
6. Zafarani, R., Abbasi, M. A., & Liu, H. (2014). *Social Media Mining: An Introduction* (1st edition). Cambridge University Press.

PGDNCS-2.4- Digital Forensics

Unit-1

Understanding Digital Forensics; meaning of Digital Forensics, goals of Digital Forensics, Cybercrime, Cybercrime Attack Mode, How Are Computers Used in Cybercrimes?, Malware Distribution, Ransomware Distribution, CryptoJacking, Hacking, SQL Injections, Pharming, Phishing, E-mail Bombing and Spamming, Identity Theft Cyberstalking, DDoS Attacks, Digital Forensics Categories- Digital Forensics Users, Intelligence and Counterintelligence, Digital Forensics Investigation Types, The Importance of Forensic Readiness for Organizations, Electronic Discovery Reference Model (EDRM), Digital Evidence and its Types, Machine/Network-Created Data, Locations of Electronic Evidence, Challenge of Acquiring Digital Evidence, Who Should Collect Digital Evidence, Chain of Custody, Digital Forensics Examination Process, Digital Forensics Process Official Guides, Digital Forensics Certifications, Digital Forensics vs. Other Computing Domain.

Unit-2

Essential Technical Concepts: Data Representation, Computer Character Encoding Schema, File Structure, Digital File Metadata, Timestamps Decoder (Tool), Hash Analysis, Memory Types, Types of Computer Storage: primary and secondary, Data Recovery Considerations, Computing Environment:- Personal Computing Environment, Client Server Computing Environment, Distributed Computing Environment, Cloud Computing, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Windows Version Variations.

Unit-3

Initial Response and First Responder Tasks: Search and Seizure, Consent to Search, Subpoena, Search Warrant, First Responder Toolkit, First Responder Tasks, Order of Volatility, Documenting the Digital Crime Scene, Packaging and Transporting Electronic Devices, Conducting Interview, Witness Interview Questions, Witness Signature, Acquiring Digital Evidence, Forensic Image File Format- Raw Format, AFF, Expert Witness (EnCase), Forensics Image File Validation, Acquiring Volatile Memory (Live Acquisition), Virtual Memory (Swap Space), The Challenges of Acquiring RAM Memory, Capturing RAM Using the DumpIt Tool, Belkasoft Live RAM Capturer, Capture RAM with Magnet, Capture RAM with FTK Imager, Acquiring Nonvolatile Memory (Static Acquisition), Hard Drive Acquisition Methods- physical, logical, Sparse, Using FTK Imager to Capture Hard Drive, Hard Drive Imaging Risks and Challenges, Encrypted Hard Drive, Cloud Data Acquisition, Network Acquisition, Forensic Tool Limitations.

Unit-4

Analyzing Digital Evidence: Analyzing Hard Drive Forensic Images, Arsenal Image Mounter, OSFMount, Autopsy, Launching the Wizard and Creating the First Case, duration to Finish the Data Source Analysis Process, Importing a Hash Database, Analyzing RAM Forensic Image, Volatility Framework, Windows Forensics Analysis: Timeline Analysis, Creating a Timeline Using Autopsy, Generate a Timeline Report Using Autopsy, File Recovery, Attributing an Action to Its Associated User Account, Windows Registry Analysis, Acquiring Windows Registry, Registry Examination, Automatic Startup Locations, Network Analysis, Deleted Registry Key Recovery, File Format Identification, Windows Features Forensics Analysis, Windows Thumbnail Forensics,

Jump Lists Forensics, LNK File Forensics, Windows File Analyzer (WFA), Windows 10 Forensics, Web Browser and E-mail Forensics: Microsoft Edge Web Browser, Google Chrome, Cookies, Web Browser Investigation Tools, E-mail Forensics, Determine Sender Geographic Location Using Sender's Time Zone, Antiforensics Techniques

References:

1. *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives: I (Advances in Digital Crime, Forensics, and Cyber Terrorism)*
2. *Digital Forensics Basics: A Practical Guide Using Windows OS Book Online at Low Prices in India | Digital Forensics Basics: A Practical Guide Using Windows OS Reviews & Ratings—Amazon.in.* (n.d.).
3. *Python Digital Forensics Cookbook: Effective Python recipes for digital investigations Book Online at Low Prices in India*
4. *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics Book Online at Low Prices in India | The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics Reviews & Ratings—Amazon.in.* (n.d.).
5. *Computer Forensics & Digital Investigation with EnCase Forensic v7 by Suzanne Widup—PDF Drive.* (n.d.).
6. Hassan, N. A. (2019). *Digital Forensics Basics: A Practical Guide Using Windows OS* (1st ed. edition). Apress.
7. Kävrestad, J. (2018). *Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications* (1st ed. 2018 edition). Springer.
8. Lakhani Joseph, M. (2018). *CISCO | Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer| Cyber Security | First Edition | By Pearson* (First edition). Pearson Education.
9. Sridhar C. Iyer, C. R. (2018). *Understanding Digital Forensics and Incident Response in a simplified manner* (1st edition). Blue Rose Publishers.

PGDNCS-2.5- PROJECT
