Kumaun University, Nainital, Uttarakhand

Post Graduate Diploma in Cyber Security & Information System Security

w.e.f Session 2021-2022

Syllabus for Post Graduate Diploma in Cyber Security & Information System Security

Semester	Paper Code	Title of Paper	Internal	External	Total Marks
I	CS 711	Cyber Law and Ethical Hacking	25	75	100
	CS 712	Cyber Anonymity	25	75	100
	CS 713	System of Cyber Security	25	75	100
	CS 714	Cryptography Basics and Network Security	25	75	100
	CS L:715	LAB 1	25	75	100
II	CS 721	Footprinting and Social Engineering	25	75	100
	CS 722	Web Hacking and Security	25	75	100
	CS 723	Device Hacking and Security	25	75	100
	CS 724	Security Auditing	25	75	100
	CS L:725	LAB 2	25	75	100
	CS 726	Project Work	GRADE		

Kumaun University, Nainital, Uttarakhand

Post Graduate Diploma in Cyber Security & Information System Security

w.e.f Session 2021-2022

CS 711: Cyber Law and Ethical Hacking

Unit I

Introduction to Ethical Hacking: Information Security Overview, Threats to Information Security, Attack Vectors Overview, Ethical Hacking, Scope and Limitation to Ethical hacking.

Unit II

Information Security Concepts: Hacking Concepts, Types of Hacking, Phases of Hacking, Information Assurance, Defence-in-Path, Security Policies, Physical Security, Risk Management, Threat Modelling.

Unit III

Security Testing Methodology: Penetration Testing Process, Planning and Preparation, Reconnaissance, Discovery.

Unit IV

Cyber Laws: Information Technology Law (Cyber Law), Evolution of the IT Act, Genesis and Necessity, Salient features of the IT Act, 2000, various authorities under IT Act and their powers, Penalties & Offences.

UNIT V

Basics of Cryptocurrency: Introduction to Cryptocurrency, Various Cryptocurrency Systems – Bitcoin, Ethereum, Blockchain, Impact of Cryptocurrency in Cyber Security.

Recommended Books:

1. Information Security and Cyberlaws by Sarika Gupta, Gaurav Gupta.
2. Mastering Bitcoin: Unlocking Digital Cryptocurrencies by Andreas Antonopoulos

Kumaun University, Nainital, Uttarakhand

Post Graduate Diploma in Cyber Security & Information System Security

w.e.f Session 2021-2022

CS 712: Cyber Anonymity

Unit I

Introduction: Introduction to Anonymity, Importance of Privacy and Anonymity, Types of anonymity, - Ture Anonymity, Pseudo-Anonymity, Anonymity in Penetration Testing.

UNIT II

TOR: Introduction to The Onion Routing, History of The Onion Routing, TOR for anonymity, Installing and Configuring TOR Browser.

UNIT III

ProxyChain: Introduction to Proxychains, Usage of Proxychains for Anonymity, Proxychains Features, ProxyChain Syntax, setting up and Using Proxychains.

UNIT IV

VPN: Introduction to VPN, Difference between VPN and Proxy, VPN and it's Legality. Importance of VPN in Penetration Testing.

UNIT V

Managing VPN Service: Introduction to AWS, Introduction to OpenVPN software stack, setting up and Configuring AWS and OpenVPN for a private VPN Server.

Recommended Books:

1. Practical Anonymity by Peter Loshin
2. OpenVPN: Building and Integrating Virtual Private Networks Kindle Edition by Markus Feilner

Kumaun University, Nainital, Uttarakhand

Post Graduate Diploma in Cyber Security & Information System Security

w.e.f Session 2021-2022

CS 713: System of Cyber Security

Unit I

Linux Basics: Introduction to Linux, History of Unix and Linux, Installation of Kali Linux, Directory Structure, Basic Commands, VI editor, Permissions, User and Groups.

Unit II

Advanced Linux: I/O redirectors, Hardlink and Softlink, Compression/Decompression, Backup and Scheduling Tasks, Disk Recovery using Foremost and ddrescue, Filter Commands, Finding and processing Files, Process Commands, analysing logs, Exploring Virtual File System (Proc)

Unit III

Managing Services using Linux: Configuring SSH Server, Configuring DNS Server, Configuring Web Server with Virtual Hosting, Configuring FTP Server, Configuring Database Server (MySQL).

Unit IV

System Hacking Process: CEH System Hacking Process, hacking tools – keyloggers, spywares and rootkits, etc., System Hacking Prevention, Penetration testing Steps.

Unit V

Malware Threats: Malware Introduction, Malware Propagation Techniques, Working of Trojans and Viruses, Static and Dynamic Malware analysis process, Methods of Virus Detection

Recommended Books:

1. CEH v10 Certified Ethical Hacker Study Guide by Ric Messier
2. Hacking: The Art of Exploitation by Jon Erickson
3. The Hacker Playbook 2: Practical Guide to Penetration Testing by Peter Kim
4. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski, Andrew Honig

Kumaun University, Nainital, Uttarakhand

Post Graduate Diploma in Cyber Security & Information System Security

w.e.f Session 2021-2022

CS 714: Cryptography Basics and Network Security

Unit I

Introduction to Cryptography Concepts, Types of Cryptography, Ciphers and its types

Various Encryption Algorithms: Introduction to Encryption, Symmetric and Asymmetric Encryption, AES, Blowfish, RSA Encryption Algorithms, Attacks on Encryption Algorithms.

Various Hashing Algorithms: Intro to Hashing, Hash Function, Usage of Hashing Algorithms, Various Hashing Algorithms like md5, SHA-family, Attacks on Hashing Algorithms.

Unit II

Public Key Infrastructure: Intro to PKI, Key Management, Digital Certificate, Certifying Authority, Key Functions of Certifying Authority, Registration Authority, Certificate Management System, CA Hierarchy.

Cryptographic Attacks: Email Encryption, Disk Encryption, Cryptography Attacks, Cryptanalysis, Cryptanalysis Methods, Cryptanalysis Tools, Defence against Cryptographic Attacks.

Unit III

Basic Networking: Introduction to Networking, Types of Network, OSI Model, Client/Server Configuration, Topologies, Media, Ip Address (ipv4, ipv6), Protocols.

Basic Network Devices: Cabling, Addressing, Managing Basic Switches, Managing Advanced Switches, Managing Basic Routers.

Unit IV

Scanning Networks using Nmap: Network Scanning Concepts, Live Systems and ports scanning Techniques, Identifying Services, Banner Grabbing/OS Fingerprinting, Drawing Network Diagram of Vulnerable Hosts.

Python for Network Security: Introduction to Python, Python Basics, Network Programming in Python, Making a port scanner in Python.

Unit V

Sniffing using Ettercap and Wireshark: Sniffing Concepts, Various Types of Sniffing, Sniffing Techniques, MAC Attack, DHCP attack, ARP Poisoning, DNS Poisoning etc., Prevention against Sniffing.

Recommended Books:

1. CEH v10 Certified Ethical Hacker Study Guide by Ric Messier
2. Hacking: The Art of Exploitation by Jon Erickson
3. The Hacker Playbook 2: Practical Guide to Penetration Testing by Peter Kim
4. Applied Cryptography by Bruce Shnenier
5. Modern Cryptography and Elliptic Curves by Thomas R. Shemanske

Kumaun University, Nainital, Uttarakhand

Post Graduate Diploma in Cyber Security & Information System Security
w.e.f Session 2021-2022

CS 721: Footprinting and Social Engineering

Unit I

Footprinting Terminologies: Footprinting Basics, Intelligence Gathering, Web Services, Countermeasures to defend against footprinting attacks.

Unit II

Footprinting Techniques: Footprinting through search engines, social networking sites, social engineering, website and email footprinting, whois footprinting, DNS footprinting.

Unit III

Vulnerability Analysis: Vulnerability Assessment Concepts, Vulnerability Scanning Solutions, Tools used for Vulnerability Assessment, Generating and Analysing Vulnerability Assessment Report.

Unit IV

Intro to Social Engineering: Intro to Social Engineering, Various attack Phases, Types of Social Engineering, Types of Insider Threats, Anti-Phishing tools to detect phishing websites and Emails

Unit V

Social Engineering Techniques using SET Tool: Social Engineering Techniques such as Phishing, Impersonation, Whaling, Watering Hole, Baiting and Quid Pro Quo attacks.

Recommended Books:

1. Social Engineering: The Art of Human Hacking by Christopher Hadnagy
2. The Art of Deception: Controlling the Human Element of Security by Kevin D. Mitnick
3. Hacking: The Art of Exploitation by Jon Erickson
4. Foot printing and Reconnaissance: Part 2 of CEH by Dr. Haidaia Mahmood Alssouli

Kumaun University, Nainital, Uttarakhand

Post Graduate Diploma in Cyber Security & Information System Security

w.e.f Session 2021-2022

CS 722: Web Hacking and Security

Unit I

DDos Attacks and Prevention: This module explains DoS/DDoS attacks, the classification of DoS/DDoS attacks, and various attack techniques, Discusses Botnets, the types of bots, and how they infect the system, demonstrates various tools to perform DoS and DDoS attacks, discusses various techniques to detect, prevent, and mitigate DoS/DDoS attacks, Briefs about various post-attack forensic methods

Unit II

Session Hijacking: Session hijacking concepts, discusses about network and application-level session hijacking, explains various session hijacking tools, explains various session hijacking detection methods and tool, explains countermeasures to prevent session hijacking attacks

Unit III

Evading IDS, Firewalls and Honeypots: Introduction to IDS, firewall and honeypot concepts and types, demonstrates various IDS, firewall and honeypot solutions, describes various IDS and firewall evasion techniques, explains various techniques to detect and defeat honeypots, lists various IDS/firewall evasion tools and honeypot detection tools, Discusses the countermeasures to defend against IDS/firewall evasion

Unit IV

Hacking Web Servers: Open-source web server and IIS architecture, discusses various reasons why web servers are compromised, demonstrates various key web server attack techniques and tools, discusses about web server attack methodology and tools, discusses various methods to detect web server hacking attempts, explains countermeasures to prevent web server attacks

Unit V

Hacking Web Application: Lists and explains various web application threats and attacks, explains web application hacking methodology, demonstrates various web application hacking tools, SQL Injection Discusses countermeasures to defend against web application attacks, Demonstrates various web application security tools

Recommended Books:

1. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws by Dafydd Stuttard
2. The Basics of Web Hacking: Tools and Techniques to Attaack the Web by Josh Pauli
3. Hacking: The Art of Exploitation by Jon Erickson

Kumaun University, Nainital, Uttarakhand

Post Graduate Diploma in Cyber Security & Information System Security

w.e.f Session 2021-2022

CS 723: Device Hacking and Security

Unit I

Wireless Hacking: Wireless terminologies, types, standards, etc., Types of wireless encryption and their working, various wireless threats, wireless hacking methodology, various wireless hacking tools, Bluetooth hacking, threats, and Bluetooth hacking tools, discusses how to defend against wireless attacks, Illustrates various wireless security tools

Unit II

Android Hacking: Mobile platform attack vectors in detail and explores app sandboxing issues, Discusses Android OS architecture briefly and demonstrates hacking android OS using various tools, illustrates working of various Android Trojans and guidelines for securing Android devices

Unit III

iOS Hacking: Jailbreaking iOS, its types, techniques and tools required for jailbreaking, illustrates various iOS Trojans and guidelines for securing iOS devices.

Unit IV

IoT Hacking: IoT Concepts, IoT Security Challenges, IoT Threats and Attack Surface Area, IoT Hacking Tools, Countermeasures to prevent IoT hacking, IoT Security Tools.

Unit V

Threats to Cloud Computing: Cloud Computing Concepts, Virtualization in Cloud Computing, Various Cloud Computing Attacks, Security Considerations, Best Practices for Security Cloud, Cloud Security Tools.

Recommended Books:

1. Android Security Internals: An In-Depth Guide to Android's Security Architecture
2. Hacking Exposed Mobile: Security Secrets & Solutions
3. iOS Application Security: The Definitive Guide for Hackers and Developers
4. IoT Security Issues by Alasdair Gilchrist
5. CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security

Kumaun University, Nainital, Uttarakhand

Post Graduate Diploma in Cyber Security & Information System Security
w.e.f Session 2021-2022

CS 723: Security Auditing

Unit I

Introduction to Security Auditing – Roles, Objectives and Scope, Digital Asset Protection, Lines of Defence.

Unit II

Cybersecurity Roles and Responsibilities, Security Frameworks, Security Organization Goals, Cybersecurity Policy and Standards, Cybersecurity Risk Assessments

Unit III

Cybersecurity Awareness Training and Education, Social Media – Risk and Control, Third Party Assessment, Supply Chain Risk Managements

Unit IV

Cybersecurity Operations, Thread and Vulnerability Management, Enterprise Identity and Access Management, Configuration Management, Change Management

Unit V

Client Endpoint Protection, Application Security, Data Backup and Recovery, Security Compliance, Secure Build and Deploy.

Recommended Books:

1. The Complete Guide to Cybersecurity Risks and Controls by Anne Kohnke, Dan Shoemaker, Ken Sigler
2. Cyber Security and Privacy Control by Robert R. Moeller
3. Auditor's Guide to IT Auditing" by Richard E. Cascarino