

**OUTLINES OF TESTS,
SYLLABI AND COURSES OF READING**

FOR

B.Voc. (CYBER SECURITY)

**Third Year
(FIFTH AND SIXTH SEMESTER)
FOR
2021-22, 2022-23 and 2023-24 Sessions**

**PUNJABI UNIVERSITY
PATIALA**

B.VOC(Cyber Security) 3rd Year (5th and 6th Semester)

2021-22, 2022-23 and 2023-24 Sessions

Code	Title of Paper	Component	Credits	University Examination	Internal Assessment	Max. Marks	Exam. Duration Hours
B.VCS-311	Presentation Skills and Personality Development	General	4.5	60	40	100	3
B.VCS-312	Ethical Hacking- Level 3	General	4.5	60	40	100	3
B.VCS-313	Penetration Testing	Skill	4.5	60	40	100	3
B.VCS-314	Cloud Computing	Skill	4.5	60	40	100	3
B.VCS-315	Software Lab – IX	General	4.0	50	50	100	3
B.VCS-316	Software Lab – X	Skill	4.0	50	50	100	3
B.VCS-317	Software Lab – XI	Skill	4.0	50	50	100	3
Total			30	390	310	700	

1. The breakup of marks for the practical will be as under:

i.	Internal Assessment	50 Marks
ii.	Viva Voce (External Evaluation)	20 Marks
iii.	Lab Record Program Development and Execution(External Evaluation)	30 Marks

1. The breakup of marks for the internal assessment for theory Subjects will be as under:

i.	Average of Both Mid Semester Tests / Internal Examinations	24 Marks
i.	Attendance	8 Marks
i.	Written Assignment/Project Work etc.	8Marks

**SYLLABUS
FOR**

B.VOC(Cyber Security) Third Year(6th Semester)

2021-22, 2022-23 and 2023-24 Sessions

CODE	TITLE OF PAPER	INTERNAL ASSESSMENT	EXTERNAL	MAXIMUM MARKS
B.VCS-321	PROJECT	150	250	400

6-month Industrial Training

Credit: 18

Semester-V

B.VCS-311 Presentation Skills and Personality Development

Max. Marks: 60 Marks

Min. Pass Marks: 35%

Min. Time: 3hrs

Lectures to be delivered: 55-65

INSTRUCTIONS FOR THE PAPER SETTER

The question paper will consist of three sections A, B and C. Each of sections A and B will have four questions from the respective sections of the syllabus and each question carry 9 marks. Section C will consist of one compulsory question having 12 parts of short-answer type covering the entire syllabus uniformly and each question will carry 2 marks.

INSTRUCTIONS FOR THE CANDIDATES

Candidates are required to attempt two questions each from section A and B and the entire section C.

Section – A: Literature

Prescribed Text: Popular Short Stories.

From the prescribed text the following stories are to be read: A Cup of Tea – Katherine Mansfield.

The Open Window – H.H. Munro (“Saki”)

The Gift of the Magi – O. Henry

The Ant and the Grasshopper – W. Somerset

Maugham The Necklace – Guy De Maupassant

Section B: Grammar and Writing Skills Tenses

- Voice
- Narration
- Letter Writing – Formal
- Resume/C.V. Writing
- Report Writing
- Note making, Summarizing and Abstracting

Books Recommended:

- The Written Word by Vandana R. Singh: Oxford University Press.
- Popular Short Stories: Oxford University Press
- Oxford Practice Grammar by John Eastwood : Oxford University Press
- Oxford Advanced Learner’s Dictionary.

B.VCS- 312 Ethical Hacking-Level 3

Max Marks: 60
Min Pass Marks: 35%

Maximum Time: 3 Hrs.
Lectures to be delivered: 55-65

INSTRUCTIONS FOR THE PAPER SETTER

The question paper will consist of three sections A, B and C. Each of sections A and B will have four questions from the respective sections of the syllabus and each question carry 9 marks. Section C will consist of one compulsory question having 12 parts of short-answer type covering the entire syllabus uniformly and each question will carry 2 marks.

INSTRUCTIONS FOR THE CANDIDATES

Candidates are required to attempt two questions each from section A and B and the entire section C.

SECTION-A

IDS/IPS and Honey pots: Rules for IDS/IPS, Honey pots Detection, Evasion Techniques, Security Measures for IDS, Unified Threat Management (UTM), Rules set for UTM, Virtual Private Network (VPN), Network Vulnerability Assessment Automated & Manually

Android Ethical Hacking & Security: Ethical Hacking Practical on Smartphone, Securing your Android mobile from being hacked, Cyber Threats for Mobile, Android Rooting and Testing for Exploits, Securing your family with Android Apps, Smartphone Data Recovery

Web Server Ethical Hacking: Types of Web servers and their Security, Web Server Enumeration, Attacking a Web server, Directory Traversal attack, Methodology for Web server attack, Using HTTrack to find backdoor in Web server, Testing the Payload on server, Brute force attack, Security and Defending against Web Server Attacks, Upgrading a Web server

Session Hijacking Ethical Hacking: Session Hijacking, Process of Session Hijacking, Types of Session Hijacking, Testing for Session Hijacking, Browser Hijacking, Coping with Session Hijacking, Coding Standards and Session Management, Evaluating the Cookies

Advance Google hacking: Advance Google hacking, Google Hacking Database, Google Dorks for SQL and Advance SQL Injection, Enumerating the Website's Security & Publicly Available Data, Deep Web vs Dark Web

SQL Injection: SQL Injection, Case Studies, SQL Injection Technologies, Types of SQL Injection, Steps to Perform SQL Injection, Advance SQL Injection, SQL Injection Tool-Kit, Security Methods against SQL Injection

SECTION-B

Web Application Ethical Hacking: Architecture of a Web Application, Hacking Threats for a Web Application, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), Data Storage and Functionality testing of a Web Application, Detecting a Web Application Attack, Vulnerability Testing Tools, Security against Web Application Attack

Shell: Shell Injection, Local File Inclusion (LFI) & Remote File Inclusion (RFI), Live Demonstration of Shell Injection on Web Server, Evaluating the Coding Standards

Tamper data: Intercepting between Server and Client Side, Understanding the GET and POST, Burp Suit & OWASP ZAP, Tampering Website's Data

Securing a Website: Web Application Firewall Introduction, AWS Web Application Firewall and Another Popular Firewall, Input Validations, Sanitisation the Input, Website Vulnerability Assessment Automated & Manually

Cloud Computing Ethical Hacking: Services of Cloud Computing, Loop Holes in Cloud Computing, Attack Methods for Cloud Services, Securing the Cloud (Manually and with Tools), Using Cloud Service for DDOS Protection and Session Hijacking

Practice Sets for Website Ethical Hacking: Bwap, Word Press Website Hacking, Dam Vulnerable Application, OWASP Top 10 Vulnerability

Reference Books:

1. Thomas Mathew, Ethical Hacking, 0571 Publisher, 2003. 13
2. Joel SeatnbraV and George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, Stuart McClure, McGraw-Hill, 2005

B.VCS- 313 Penetration Testing

Max Marks: 60
Min Pass Marks: 35%

Maximum Time: 3 Hrs.
Lectures to be delivered: 55-65

INSTRUCTIONS FOR THE PAPER SETTER

The question paper will consist of three sections A, B and C. Each of sections A and B will have four questions from the respective sections of the syllabus and each question carry 9 marks. Section C will consist of one compulsory question having 12 parts of short-answer type covering the entire syllabus uniformly and each question will carry 2 marks.

INSTRUCTIONS FOR THE CANDIDATES

Candidates are required to attempt two questions each from section A and B and the entire section C.

SECTION –A

Penetration Testing Process: Pre-engagement, Methodologies, Reporting,

Introduction to Web Applications: HTTP/S Protocol Basics, Encoding, Same Origin, Cookies, Sessions, Web Application Proxies

Information Gathering: Gathering information on your target, Infrastructure, Fingerprinting frameworks and applications, Fingerprinting custom applications, Enumerating resources, Relevant information through misconfigurations, Google hacking, Shodan HQ

Cross-Site Scripting: Cross-Site Scripting, Anatomy of an XSS Exploitation, The three types of XSS, Finding XSS, XSS Exploitation, Mitigation

SQL Injection: Introduction to SQL Injections, Finding SQL Injections, Exploiting In-band SQL Injections, Exploiting Error-based SQL Injections, Exploiting blind SQLi, SQL Map, Mitigation Strategies, From SQLi to Server Takeover.

Authentication and Authorization: Introduction, Common Vulnerabilities, Bypassing Authorization,

Session Security: Weaknesses of the session identifier, Session hijacking, Session Fixation, Cross-Site Request Forgeries

SECTION –B

Flash Security: Introduction, Flash Security Model, Flash Vulnerabilities, Pen testing Flash Applications

HTML5: Cross-Origin Resource Sharing, Cross-Window Messaging, Web Storage, Web Socket, Sandboxed frames

File and Resource Attacks: Path Traversal, File Inclusion Vulnerabilities, . Unrestricted File Upload,

Other Attacks: Click jacking, HTTP Response Splitting, Business Logic Flow, Denial of Services.

Web Services: Introduction, Web Services Implementations, The WSDL Language, and Attacks.

X Path: XML Documents and Databases, X Path, Detecting X Path Injection, Exploitation, Best Defensive Techniques.

Reference Books :

1. Georgia Weidman, "Penetration Testing".
2. Patrick Engebretson, "The Basics of Hacking and Penetration Testing", Ethical Hacking and Penetration Testing Made Easy.

B.VCS- 314 Cloud Computing

Max Marks: 60

Maximum Time: 3 Hrs.

Min Pass Marks: 35%

Lectures to be delivered: 55-65

INSTRUCTIONS FOR THE PAPER SETTER

The question paper will consist of three sections A, B and C. Each of sections A and B will have four questions from the respective sections of the syllabus and each question carry 9 marks. Section C will consist of one compulsory question having 12 parts of short-answer type covering the entire syllabus uniformly and each question will carry 2 marks.

INSTRUCTIONS FOR THE CANDIDATES

Candidates are required to attempt two questions each from section A and B and the entire section C.

SECTION –A

Introduction: Definition of Cloud, Basics of Cloud Computing, Characteristics of Cloud, Benefits of Cloud, Driving factors towards the use of Cloud Computing, Comparing Cloud with Grid Computing Systems, Workload Patterns for the Cloud, Selection criteria for migrating into Cloud, Application of Cloud Computing.

Basic Concepts and Virtualization: Cloud Computing Evolution, Big Data Concept, Elasticity and scalability, Virtualization: characteristics of virtualization, Benefits of virtualization, Forms of CPU virtualization, Hypervisors, VMWare, Multitenancy, Application programming interfaces (API), Billing and metering of Cloud services, Economies of scale, Management, Tooling, and automation in Cloud Computing, SLA in Cloud Computing.

Cloud Computing Service Delivery Models: Cloud service delivery models, Cloud Reference Model, Infrastructure as a service (IaaS) architecture, details, examples and applications, Platform as a service (PaaS) architecture, details, examples and applications, Software as a service (SaaS) architecture, details, examples and applications, NIST architecture.

SECTION –B

Cloud Deployment Models: Cloud deployment models, Private Clouds, Public Clouds, Hybrid Clouds, Community, Virtual private Clouds, Heterogeneous and Homogenous Clouds, Vertical and special purpose Clouds, Migration paths for Cloud, Selection criteria for Cloud deployment.

Cloud Security: Cloud Security challenges and risks, Principal Characteristics of Cloud Computing security, Cloud Computing Security Reference Model, How security gets integrated, Principal security dangers to Cloud Computing, Virtualization and Multitenancy, Internal security breaches, Data corruption or loss, User account and service hijacking, Steps to reduce Cloud Security breaches, Identity and access management, Cloud forensics, Digital signature, SSL.

Reference Books:

1. Barrie Sosinsky, Cloud Computing Bible, Wiley.
2. Michael Miller, Cloud Computing, QUE Publications.
3. Judith Hurwitz, Robin Bloor, Marcia Kaufman, Fern Halper, Cloud Computing for Dummies, Wiley.

B.VCS – 315 Software Lab – IX (Based on B.VCS- 312)

Max Marks: 50

Maximum Time: 3 Hrs.

Min Pass Marks: 35%

This laboratory course will comprise as exercises to supplement what is learnt under paper
B.VCS- 312: Ethical Hacking-Level 2

*Maximum Marks for Continuous Assessment: 50

Maximum Marks for University Examination: 50

B.VCS – 316 Software Lab – X (Based on B.VCS- 313)

Max Marks: 50

Maximum Time: 3 Hrs.

Min Pass Marks: 35%

This laboratory course will comprise as exercises to supplement what is learnt under paper B.VCS- 313: Penetration Testing

*Maximum Marks for Continuous Assessment: 50

Maximum Marks for University Examination: 50

B.VCS – 317 Software Lab – XI (Based on B.VCS- 314)

Max Marks: 50

Maximum Time: 3 Hrs.

Min Pass Marks: 35%

This laboratory course will comprise as exercises to supplement what is learnt under paper B.VCS- 314: Cloud Computing

*Maximum Marks for Continuous Assessment: 50

Maximum Marks for University Examination: 50

iii. One or two nominee(s) of Dean, Academic Affairs

iv. External Examiner

Quorum will be of any three members.