MADHYA PRADESH BHOJ (OPEN) UNIVERSITY,
Raja Bhoj Marg Kolar Road, BHOPAL (M.P.)

DIPLOMA IN
CYBER SECURITY
(from Calendar Year 2023-24)

MADHYA PRADESH BHOJ (OPEN) UNIVERSITY,
Raja Bhoj Marg Kolar Road, BHOPAL (M.P.)

Fundamentals of Cyber Security

This course will be responsible for establishing a comprehensive understanding in the field of cyber security. With a view that incumbents in this diploma course are from varied disciplines, after studying this paper all the students would be able to come at par and move together as they must go deeper into hard-core cyber security topics during the course duration.

LEARNING OUTCOMES

After undergoing the subject, the students will be able to:

- Understand cyber security concepts.
- Learn different types of cyber-attacks.
- Categorise the types of cyber security.
- Learn the general procedures adopted for cyber-attacks.

DETAILED CONTENTS

Unit 1. Cyber Security **(10 Period)**

Introduction to cyber security, information security, network security, application and system security, Threats to Information Systems, Information Assurance, Security Risk Analysis, Security Principles or Security Goals (CIA Principle), Security Services. Security Mechanism, Security Technique: Cryptography & Steganography, Active & Passive Attacks. Hardware & network Basics, Basic terminologies in cyber security: Cloud, Software, Domain, VPN, IP Address, Exploit, Breach, Firewall, Malware, Virus, Ransomware, Trojan Horse, Worm, Bot/Botnet, Spyware, Rootkit, DDOS, Phishing/Spear Phishing, Encryption. Security Threats - Viruses, Worms, Trojan Horse, Bombs, Trapdoors, Spoofs, E-mail viruses, Macro viruses, Malicious Software, Network and Denial of Services Attack

Unit 2. System & Application security ***(06 Period)***

System Hacking Concepts: Gaining access, cracking passwords, vulnerability exploitation,escalating privileges, hiding files, clearing logs,
Data Security Considerations: Backups, Archival Storage and Disposal of Data
Security Technologies: Firewall and VPNs, Intrusion Detection, Access Control Security

Unit 3. Web Security ***(10 Period)***

Introduction- A web security forensic lesson, Introduction to different web attacks. Overview ofN-tier web applications, Web Hacking Basics HTTP & HTTPS URL, Web under the Cover,

Overview of Java security Reading the HTML source, Applet Security Servlets Security Symmetricand Asymmetric Encryptions

Unit 4. Cloud Security *(15 Period)*

Introduction to Cloud Computing, migrating into a Cloud, Enriching the 'Integration as a Service' Paradigm for the Cloud Era, The Enterprise Cloud Computing Paradigm.
Cluster: Admin Server & Managed Server
Infrastructure as a Service (IAAS) & Platform and Software as a Service (PAAS / SAAS) Virtual machines provisioning and Migration services, On the Management of Virtual machines forCloud Infrastructures, Enhancing Cloud Computing Environments using a cluster as a Service, Secure Distributed Data Storage in Cloud Computing, Aneka, Comet Cloud, T-Systems', Workflow Engine for Clouds, Understanding Scientific Applications for Cloud Environments.

Unit-5. General Procedure adopted for Cyber Attacks: *(15 Period)*

Reconnaissance: Foot printing concepts and methodology, foot printing using -search engines, web services, social networking sites, website, email, whois, DNS, network, foot printing by social engineering, foot printing tools, foot printing counter measures.
Scanning: concept, host discovery, OS discovery, scanning beyond IDS and Firewall, Drawing network diagram.
Enumeration: Concepts and Techniques, NetBIOS Enumeration.

List of Practical's

- Recovering the content of a virus infected storage media device.
- Password cracking using open-source tools.
- Learning different type of attacks.
- Study of firewall and implementation of protection mechanism.
- Service Development & usage over cloud using open source.
- Managing cloud computing resources
- Detecting Trojan Attacks using open-source tools.
- Implementing Foot printing using open-source tools.
- Implementing Fingerprinting using open-source tools.
- Implementing Poisoning & Exploitation using open-source tools.

INSTRUCTIONAL STRATEGY

The content of this course is to be taught on conceptual basis with real world examples. Since this subject is practice oriented, the teacher should demonstrate the capabilities of websites/Webpages to students while doing practical exercises for information security. The students should be made familiar with preventive measures for information and computer security.

MEANS OF ASSESSMENT

1. Assignments and quiz/class tests, mid-term and end-term written tests
2. Practical work, exercises and viva-voce
3. Software installation, operation and viva-voce

Reference Books:

- Security Analysis and Portfolio Management by Donald E. Fischer
- Professional Pen Testing for Web Applications by Andres Andreu
- Foundations of Security: What Every Programmer Needs to Know by by Christoph Kern (Author), Anita Kesavan (Author), Neil Daswani
- Cloud Computing by M N Rao, PHI Publication, 1st edition.
- Cloud Computing by Saurabh Kumar, Wiley Publication
- Cloud Computing Bible, Wiley Publication
- Social Media Security: Leveraging Social Networking While Mitigating Risk by Michael Cross
- Securing the Clicks Network Security in the Age of Social Media by by Gary Bahadur

Websites for Reference:

1. http://swayam.gov.in
2. http://spoken-tutorial.org
3. https://nptel.ac.in/
4. https://cloud.google.com/docs/get-started

SUGGESTED DISTRIBUTION OF MARKS

Unit No.	Time Allotted (Periods)	Marks Allotted (%)
1	10	20
2	06	10
3	10	20
4	15	25
5	15	25

Total	56	100

Networking Concepts & Security

RATIONALE

This course focuses on teaching students about the fundamentals and distinctions of network building along with setup of present-day networks in complex environments. The networks today are vulnerable to various attacks and this paper aims at acquainting students with the techniques used by hackers for network attacks and also the techniques adopted in order to guard the entire infrastructure against various attacks.

LEARNING OUTCOMES

After undergoing this course, the students will be able to:

- Understand the fundamentals and security concepts of networking.
- Learn and implement the Virtual private Networks.
- Learn the strategy behind different types of network attacks & their prevention by using open source tools.
- Understand the types of wireless attacks & their prevention by using open source tools.

DETAILED CONTENTS

Unit I: Introduction to Network Security **(14 Periods)**

Types of networks, IP Address, NAT, IP Subnets, DHCP Server, Ports, DNS, Proxy Servers, Virtual Private Networks, DNS Server, OSI and TCP/IP Model, TCP Vs. UDP, Routers, Switches, Endpoint solutions, Access Directory, TOR Network. Networking Devices (Layer1,2,3) - Different types of network layer attacks–Firewall (ACL, Packet Filtering, DMZ, Alerts and Audit Trails) – IDS, IPS and its types (Signature based, Anomaly based, Policy based, Honeypot based) and setup.

Unit II: Virtual Private Networks **(10 Periods)**

VPN and its types –Tunnelling Protocols – Tunnel and Transport Mode –Authentication Header Encapsulation Security Payload (ESP)- IPSEC Protocol Suite – IKE PHASE I, II Generic RoutingEncapsulation (GRE). Implementation of VPNs.

Unit III: Network Attacks Part 1 *(20 Periods)*

Sniffing concepts, Sniffing Techniques: MAC Attack, DHCP attack, ARP poisoning, Spoofing, DNS poisoning. Wireshark, packet analysis, display and capture filters. Ettercap, sniffing counter measures, sniffing protection tools.

Denial of service (DOS)/Distributed Denial of service (DDOS): Concepts, DOS/DDOSTechnique,Botnets, DDOS, DOS/DDOS attacking tools, DOS/DDOS counter Measures, DOS/DDOS protection tools.

Vulnerability scanning tools: Concepts, Scanning Techniques, Tools: Nessus, OpenVAS; Sparta, Nexpose, Nmap. Network Scanning Report Generation, Striping, Router attacks, VPN pentesting, VOIP pentesting, Enumeration techniques: SMTP, SNMP, IPsec, VOIP, RPC, Telnet, FTP, TFTP,SMP, IPV6 and BGP.

Unit IV: Network Attacks Part 2 *(20 Periods)*

Network Exploitation OS Detection in network, Scanning: nmap, open ports, filtered ports, servicedetection, metasploit framework, interface of metasploit framework, network vulnerability assessment, evade anti viruses and firewalls, metasploit scripting, exploits, vulnerabilities, payloads,custom payloads, nmap configuration, Social Engineering toolkit, Xero sploit Framework, exploitsdelivery, burp-suite, End Point Security.

Unit V: Wireless Attacks *(20 Periods)*

Wireless concept, wireless encryption, wireless threats, wireless hacking methodology, wireless hacking and security tools, Bluetooth hacking, countermeasures to wireless threats. Protocols, MAC Filtering, Packet Encryption, Packet Sniffing, Types of authentications, ARP Replay attack, Fake Authentication Attack, De authentication, Attacks on WEP, WPA and WPA-2 Encryption, fake hotspots, evil twin attack, fluxion framework

List of Practical's

- Brute force attack using open-source tools.
- Identifying network attacks using Nmap, Metasploit.
- Selecting a Capture Interface and creating the first pcap file using Wireshark.
- Using Capture filters in Wireshark.
- Finding a Text String in a Trace File using Wireshark.
- Understanding Packet Loss and Recovery process.
- Identifying DOS & DDOS Attack.
- VPN & VOIP pentesting using open-source tools.
- Demonstration of IDS using snort or any other open-source tool.
- Demonstration of IPS using snort or any other open-source tool.

INSTRUCTONAL STRATEGY

The content of this course is to be taught on conceptual basis with real world examples. Since this subject is practice oriented, the teacher should demonstrate the capabilities of websites/Webpages to students while doing practical exercises for information security. The students should be made familiar with preventive measures for information and computer security.

MEANS OF ASSESSMENT

- Assignments and quiz/class tests, mid-term and end-term written tests
- Practical work, exercises and viva-voce
- Software installation, operation and viva-voce

Reference Books:

- Computer Networks by Tanenbaum; Prentice Hall of India, New Delhi
- Data Communications and Networking by Forouzan, (Edition 2nd and 4th); Tata McGraw Hill Education Pvt Ltd , New Delhi
- Data and Computer Communication by William Stallings; Pearson Education, New Delhi
- Information Security: The Complete Reference, Second Edition by Mark Rhodes-Ousley
- Principles of Information Security by Whitman
- Cryptography and Network Security: Principles and Practice by William Stallings
- Cryptography Theory & Practice by Douglas Stinson
- Understanding Cryptography: A Textbook For Students And Practitioners by Paar
- Information Security by Pankaj Sharma
- Charles P. Pfleeger, Shari Lawerance Pfleeger, "Analysing Computer Security "
- V.K. Pachghare, "Cryptography and information Security".

Websites for Reference:

1. http://swayam.gov.in
2. http://spoken-tutorial.org
3. https://wiresharklabs.com
4. https://www.snort.org/

SUGGESTED DISTRIBUTION OF MARKS

Unit No.	Time Allotted (Periods)	Marks Allotted (%)
I	14	20

This paper introduces students about threats and vulnerabilities in an operating system. It also makesthem able to understand the installation and features of Kali Linux and how to establishthe security in various operating systems. It focuses on the study of different tools & techniques used for OS Security along with protection systems, Information flow and OS Forensics.

LEARNING OUTCOMES

- After undergoing this course, the students will be able to:
- Understand the fundamentals of operating system.
- Implement the process of securing an OS.
- Understand the principles of trusted systems, Information flow integrity and Harding OS.
- Understand the Kali Linux OS, its administration & security.
- Learn the operating system forensics

DETAILED CONTENTS

Unit I: File System & Data Recovery **(12 Periods)**

File System Concept, File Structure, Attributes of a file, File Access method, Directory Structure, aspects of file systems, Types of file systems, File systems & operating systems, Data Backup & Recovery Solutions.

Unit II: Linux OS: Kali Linux ***(14 Periods)***

Installation of Kali Linux, boot process, Basic Linux commands, Configuring the GRUB boot loader, Disk partition, Managing Kali Linux Services, Searching, Installing, and Removing Tools, Bash Scripting, Piping & Redirection, File and command monitoring, Network related commands.

Unit III: Linux OS Administration and Security **(24 Periods)** Repository configuration, User administration of Linux, Network Configuring. Load balancing, SSH, VNC, Network Authentication, Perform System Management, Package management, configuring the Apache web server, SE LINUX, Basic Service Security, Log Management and NTP, BIND and DNS Security, Network Authentication: RPC, NIS and Kerberos, LDAP, LDAP Enumeration Technique, Apache security (SSL).

- Automate Task Using Bash Script, Security patches, IP Tables.

Unit IV: OS Security *(14 Periods)*

Introduction: Secure OS, Security Goals, OS Security Vulnerabilities, updates and patches, OS integrity checks, Anti-virus software, Design of secure OS and OS hardening, configuring the OS for security, Trusted OS, Threat Model, OS authentication mechanisms, Verifiable security goals: Information flow, information flow integrity model

Unit V: OS Forensics *(20 Periods)*

Types of digital media, booting process, types of information: volatile & non-volatile information, memory analysis, registry analysis, cache, cookie & history analysis in web browser, MD5 calculation for checking integrity of files, recycle bin/trash file analysis, prefetch files, file signatureanalysis, executable file analysis, Event log analysis.

List of Practical's

- Identifying the file system of an operating system
- Step by step Implementation of OS Hardening.
- Working with Information Gathering tools in Kali Linux: NMAP & ZENMAP
- Identifying vulnerabilities of an operating system
- Working with Vulnerability Analysis Tools in Kali Linux
- Working with Exploitation Tools in Kali Linux
- Working with Forensics Tools in Kali Linux
- Working with password cracking tools in kali Linux
- Use of keyloggers & anti keyloggers
- Implementation of IP tables in Linux

INSTRUCTONAL STRATEGY

This subject is both theory and practical oriented. Therefore, stress must be given on practical's along with theory. Concepts of O.S. must be taught practically.

MEANS OF ASSESSMENT

- Assignments and quiz/class tests, mid-term and end-term written tests
- Actual laboratory and practical work, exercises and viva-voce
- Software installation, operation, development and viva-voce

Reference Books:

- Operating System Concepts (2012) by Silber Schatz, Galvin and Gagne.
- Operating Systems (2003) by Deitel, Deitel, and Choffnes
- Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition (Information Security) by Albert Marcella Jr. , Doug Menendez
- Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspective by Raghu Santanam (Arizona State University, USA), M. Sethumadhavan (Amrita University, India) and Mohit Virendra (Brocade Communications Systems, USA)

- Operating System Security by Trent Jaeger
- Operating System Forensics by Ric Messier

Websites for Reference:

1. http://swayam.gov.in
2. http://spoken-tutorial.org
3. https://www.kali.org/
4. https://nmap.org/
5. https://nmap.org/book/zenmap.html

SUGGESTED DISTRIBUTION OF MARKS

Unit No.	Time Allotted (Periods)	Marks Allotted (%)
1	12	15
2	14	15
3	24	30
4	14	20
5	20	20
Total	84	100

Fundamentals of Web Application and Security

RATIONALE

Moving beyond the network the most important component any technology stack is the software that lies on top of the infrastructure. We will start with the requirements of how software applications are built, where students need to understand and build their applications to give the real world feel for how the internet stack is working, as well as

coding itself. along with showing them real loopholes while coding himself so that they understand the real-world attacks which are possible onapplications, and simulate them so that they can come to conclusions and understand the best practices involved in web application security.

LEARNING OUTCOMES

After undergoing this course, the students will be able to:

- Understand the basics of web development using PHP.
- Setup the XAMPP Server environment and vulnerability assessment.
- Understand the strategy behind web-based attacks and their prevention.
- Learn web application penetration testing and ethical hacking.
- Web application penetration testing is comprised of four main steps including information gathering, research and exploitation.
- Learn Advanced MySQL and MS SQL Exploitation along with basic web-based attacks using open-source tools.

DETAILED CONTENTS

Unit I: Web Designing and Penetration Testing (20 Periods)

Process Scope Understanding, Liabilities and Responsibilities, Allowed Techniques, Deliverables, OWASP Top 10 Attack Testing Guidelines, Reporting- Executive Summary, Risk Exposure over time, Successfully Attacks by whom, Vulnerability causes, Vulnerability report, Remediation report, Report Design Guidelines, Malware Analysis. PHP Basics: Variables, data types, strings, constants, operators, if else, else if statements, switch, while loops, for loops, functions, arrays, phpforms, form handling, validation, form input page with database attachment, XAMPP Server Setup.

Unit II: Web Application and Information Gathering *(14 Periods)*

HTTP Request, Response, Header Fields and HTTPS, Understanding Same Origin, Cookies, Sessions, Web Application Proxies, Information Gathering: whois, nsLookup, netcraft, web server fingerprinting, subdomain enumeration, fingerprinting frameworks, hidden resource enumeration, security misconfigurations, google hacking database, Shodan HQ.

Unit III: Web Application Attacks Part I: *(15 Periods)*

SQL Injections & Cross Site Scripting SQL Statements, Finding SQL Injections, Exploiting SQL Injections, Bypass Authentication, Xpath Injection, Error Based Injection, Double Query Injection, Time Based injections, Union Based Injections, SQL Map, Mitigation plans, SQLi to Server Rooting, Advance MY-SQL and MS-SQL Exploitation.

Unit IV: Web Application Attacks Part II: *(15 Periods)*

Cross Site Scripting: Anatomy of an XSS Exploitation, Reflected XSS, Persistent XSS, DOM based XSS, Browsers and XSS, Cookie Stealing, Defacements, Advanced Phishing attacks, BeEF Framework, Mitigation, Single factor and two factor authentication, dictionary and brute force attacks, storing hashes, blocking malicious request, user enumeration, random password guessing, remember me functionality, no limit attempts, password reset feature, logout flaws, CAPTCHA.

Unit V: Web Application Attacks Part III *(20 Periods)*

Insecure direct object reference and security, missing function level access control, unvalidated redirects and forwards, Session ID, LFI and RFI ,Session Attacks via packet sniffing or accessing via web server and Fixation, CSRF (Cross Site Request Forgery), Pentesting Flash -based applications, HTML 5, Cross Origin Resource Sharing Policy, Cross Windows Messaging, Web Storage, Web Sockets, Sandbox, Path Traversal, Arbitrary file uploading, Clickjacking, HTTP Response Splitting, Business Logic Flaws, denial of services attacks.

List of Practical's

- Vulnerability assessment using OpenVAS.
- Vulnerability testing using Nikto.
- Setting up a XAMPP Server.
- Scripting Exercises using PHP.
- Cross-site scripting using OWASP.
- Broken Authentication & Session Management using OWASP.
- Understanding & Preventing SQL Injection.
- Identifying Authentication Bypass.
- Understanding Malicious File Execution Protection.

INSTRUCTONAL STRATEGY

- Since this subject is practical oriented, the teacher should demonstrate the capabilities of different security techniques to students while doing practical exercises. The students should be made familiar with web application attacks and related security & prevention tools and techniques.

MEANS OF ASSESSMENT

- Assignment & Quiz,
- Mid-Term and End-Term written test,
- Actual Lab & Practical Work, Viva-voce

Reference Books:

1. Shema, M. & Adam. (2010). Seven deadliest web application attacks. Amsterdam: Syngress Media.

2. Stuttard, D. & Pinto, M. (2011). The web application hacker's handbook: Discovering and exploiting security flaws (2nd ed). Indianapolis, IN: Wiley, John & Sons.

3. Heiderich, M., Nava E.A.V., Heyes, G., & Lindsay, D. (2011). Web application obfuscation. Amsterdam: Syngress Media,U.S.

4. Sullivan, Bryan (2012). Web Application Security, A Beginner's Guide. McGraw- Hill Education.

Websites for Reference:

- http://swayam.gov.in
- http://spoken-tutorial.org
- https://www.kali.org/tools/nikto/
- https://openvas.org/
- https://owasp.org/www-community/Free_for_Open_Source_Application_Security_Tools

SUGGESTED DISTRIBUTION OF MARKS

Unit No.	Time Allotted (Periods)	Marks Allotted (%)
1	20	20
2	14	20
3	15	20
4	15	20
5	20	20
Total	**84**	**100**

Project-I

➢ **Rules for the Project:**

- The students would develop their project individually and get the topic approved.
- The students have to report to the guide for at least three times during the project lifespan with the progress report duly signed by the internal guide. Moreover, they have to submit the progress reports with the final project report at the time of external examination.
- The students will write project proposal and literature survey report in this semester.
- Students will learn various tools used in cyber security and forensics and they will write a report on tools/language learned for final project implementation in second semester.

Tools: NET Tools, KALI, Recuva, Test disk, TOR, Wireshark, Metaspoilt, Cain & Able and other open-source tools used for cyber security.

म0प्र0 भोज (मुक्त) विश्वविद्यालय

राजा भोज मार्ग, (कोलर रोड)–462016 (म0प्र0)

दिनांक 04/09/2023 समय 11.30 बजे

: कार्यसूची :

Department of Technology से संबंधित अध्ययन मण्डल की बैठक दिनाँक 04/09/2023 को प्रात 11.30 बजे कक्ष क्रमांक–16 में आयोजित की गयी है।

बिन्दु क्रमांक–(1)

वि0वि0 में रोजगार उन्मुखी एवं नवीन तकनीकी आधारित डिप्लोमा /प्रमाण पत्र पाठ्यक्रमो का संचालन किये जाने हेतु इन पाठ्यक्रमो के सिलेबस तैयार किये गये है । जिसे वि0वि0 में प्रारम्भ किया जाना प्रस्तावित है ।

- **Diploma in Cyber Security**
- **Diploma in Data Science**
- **Diploma in AI & Data Science**

कुलसचिव

DIPLOMA IN
CYBER SECURITY
(from Calendar Year 2023-24)

Sr.No.	Title of the Paper	Credits
1.1	Fundamentals of Cyber Security	6
1.2	Networking Concepts & Security	6
1.3	Operating System Security &Forensics	6
1.4	Fundamentals of Web Applicationand Security	6
1.5	Project-I	6
#Student Centred Activities-Assignments		4