SYLLABUS

POST GRADUATE DIPLOMA IN CYBER SECURITY

ENLIGHTENMENT TO PERFECTION

2018-19

University of North Bengal

OUTLINE OF COURSE STRUCTURE

Post Graduate Diploma in Cyber Security

(Session: 2024-25)

SEMESTER-I

Course Code	Name of the module	Marks	Credit	Hours/ Week
Course (Theoretical)				
CYSPGD 101	Networking Concepts & Security	40	2	4
CYSPGD 102	Operating System & Security	40	2	4
CYSPGD 103	Web Application & Security	40	2	4
Course (Practical)				
CYSPGD 104	Networking Security	40	2	5
CYSPGD 105	Operating Security	40	2	5
CYSPGD 106	Web Application Penetrations	40	2	5
Continuing Evaluation				
CYSPDG 107	Exam	15	2	2
CYSPGD 108	Project	45	2	1
Total Marks & Credits in the Semester I		300	16	30

Semester-II

Course Code	Name of the module	Marks	Credit	Hours/ Week
Course (Theoretical)				
CYSPGD 101	Cryptography	40	2	4
CYSPGD 102	Mobile Concept & Security	40	2	4
CYSPGD 103	IOT Security	40	2	4
Course (Practical)				
CYSPGD 204	Cryptrography	40	2	5
CYSPGD 205	Mobile Security	40	2	5

CYSPGD 206	IOT Security		40	2	5
Continuing Evaluation					
DBI-207	Exam		15	2	1
DBI-208	Project		15	1	1
DBI-209	Internship		30	1	1
Total Marks & Credits in the semester II			300	16	30
		Grand Total	600	32	60

Detailed Syllabus
Semester-I

Course Code	Name of the module	Marks
CYSPGD (101)	Networking Concept & Security	40

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 1, II – Generic Routing Encapsulation (GRE). Implementation of VPNs.

Unit III: Network Attacks Part 1

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

Network Exploitation OS Detection in network, Scanning: nmap, open ports, filtered ports, service detection, 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, exploits delivery, burp-suite, End Point Security.

Unit V: Wireless Attacks

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

Unit I: File System & Data Recovery

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

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

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

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

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 signature analysis, executable file analysis, Event log analysis.

Unit I: Web Designing and Penetration Testing

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, php forms, form handling, validation, form input page with database attachment, XAMPP Server Setup.

Unit II: Web Application and Information Gathering

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:

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:

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

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

- 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.

CYSPGD(105) **Operating System & Security (Practical)** **40**

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

CYSPGD(106) **Web Security (Practical)** **40**

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.

CYSPGD (107)	**Continuing Evaluation** Seminar from a bunch of topics to be offered by the teachers	**15**
CYSPGD (108)	**Continuing Evaluation** Class tests	**45**

Semester -II

Course Code	Name of the module	Marks
CYSPGD (101)	Cryptography	40

Unit I: - Classical Ciphers

Ceaser Cipher, Vegnere Cipher, Rail-fence Cipher, Row Transposition Cipher. Requirement and Basic Properties, Main Challenges, Confidentiality, Integrity, Availability, Non-Repudiation,

Unit II: Secret Key Cryptography

Data Encryption Standard-Symmetric Ciphers (Stream Cipher &Block cipher) Advanced Encryption Standard (AES)-Triple DES-Blowfish, RC4, RC5/RC6 family.

Unit III: Public Key Cryptography

Principles of public key cryptosystems-The RSA algorithm-Key management -Diffie Hellman Key exchange, Elgamal Algorithm, Polynomial Arithmetic, Elliptic curve arithmetic-Elliptic curve cryptography, cryptanalysis.

Unit IV: Cryptocurrency

Bitcoin introduction, working, blockchain crucial to bitcoin, block chain operation with bitcoins, bitcoin glossary, bitcoin wallets, setup for bitcoin payments, bitcoin mining.

Unit V: Message authentication code and Hash Functions

Message authentication code Authentication functions, Hash functions- Hash Algorithms (MD5, Secure Hash Algorithm), Digital signatures (Authentication protocols, Digital signature Standard). Digital Certificate and Public Key Infrastructure

CYSPGD (102)	Mobile Concepts & Security	40

Unit I: Introduction to Mobile Concepts & Security

Mobile Security Model, Enterprise Mobile Environment, Mobile Crypto Algorithm.

Unit II: Mobile System Technology

Mobile Devices - features and security concerns, Platforms, Applications - development, testing and delivery.

Unit III: Mobile Networks

Cellular Network - baseband processor and SIM card, GSM encryption and authentication and other attacks, VoLTE and its working, WIFI Networks - public hotspots and enterprise WLANs, SSL/TLS, Web Technologies - server-side and client-side web applications.

Unit IV: Mobility Management

Enterprise Mobility Program, Transactions Security, File Synchronization and Sharing, Vulnerability Assessments, BYOD Device Backup, Data Disposal/Sanitization, NAC for BYOD, Container Technologies, Exchange ActiveSync (EAS), Mobile Authentication, Mobile Management Tools.

Unit V: Scenario Testing

Cellular Attacks, Attacking Web Interface, Wireless Attacks, SSL attacks, Android, iOS

CYSPGD(103) **IOT Security (Theoretical)** **40**

Unit 1: IOT - What is the Internet of Things(IOT) and why is it important? How does the Internet of Things (IOT) affect our everyday lives? How does IOT work? Describe the different parts or components of IOT Elements of an IOT Ecosphere, Technology. Trends of IOT and implications, Overview of Governance, Privacy and Security Issues.

Unit 2: IOT Protocols are utilized to associate low-power IOT gadgets. They give correspondence equipment on the client side - without the requirement for any web association. The availability in IOT information conventions and norms is through a wired or cell organization.

Unit 3: Introduction to Arduino

Overview, Board description, Installation, Pin configuration and architecture, Device and platform features., Concept of digital and analog ports, Familiarizing with Arduino Interfacing Board, Introduction to Embedded C and Arduino platform.

Unit 3: Arduino Functions:

Pins Configured as INPUT, Pull-up Resistors, Pins Configured as OUTPUT, pin Mode() Function, digital Write() Function, analog Read() function, Arduino Interrupts

Unit 4: Arduino Time:

Incorporating Arduino time, delay () function, delay Microseconds () function, millis () function, micros () function .

CYSPGD(104) **Cryptography (Practical)** **40**

List of Practical's

- To create a simple digital signature by using open-source software/website.
- To understand the process of creating simple digital certificate.
- To understand Public Key Cryptosystem (PKCS v1.5) scheme.

- To implement the following Substitution & Transposition Techniques concepts:

    a) Caesar Cipher
    b) Playfair Cipher
    c) Hill Cipher
    d) Vigenere Cipher
    e) Rail fence – Row & Column Transformation

- To implement the following algorithms

    a) DES
    b) RSA Algorithm
    c) Diffiee-Hellman
    d) MD5
    e) SHA-1

CYSPGD (205) **Mobile Concept & Security (Practical)** **40**

List of Practical's

- To understand various types of Cellular Attacks
- To identify WEP/WPA attacks.
- To understand mobile crypto algorithms.
- To use mobile management tools.
- To implement the mobile backup & data recovery using open-source tools.
- To use mobile vulnerability assessment tools.
- To do mobile testing using open source tools like Monkey Talk, Appium, Katalan Studio.
- To use the container technologies.

CYSPGD (206) **IOT Security (Practical)** **40**

LIST OF PRACTICALS:

1. Installation of Arduino IDE
2. Programming exercise in C language.
3. Programming exercise on Arduino with C language.
4. Programming exercise on Arduino-I/O function.

CYSPGD (207)	**Continuing Evaluation** Educational Trip along with submission of a final tour report	**15**
CYSPGD (208)	**Continuing Evaluation** Class Tests	**15**
CYSPGD (209)	**Continuing Evaluation** *Project/Dissertation Work:* The students will be assigned with a practical project at the end of the first semester which they will have to complete by the end of second semester to the following themes (which is not an exhaustive list): - Phylogenetic Analyses - Construction of databases - Comparative genome analysis - Developing Bioinformatics tools/software	**30**