A.C.-10.05.2025
Appendix-91

POST GRADUATE DIPLOMA IN CYBER SECURITY AND LAW(PGDCSL)

PREAMBLE

Cyber-security is a niche subject of modern studies wherein this diploma is an advanced Penetration Testing & Information Security Program. The course provides intensive practical sessions to prepare an individual with uncompromising practical knowledge in a simplified and easily graspable manner.

SESSION DURATION

	SEMESTER 1	SEMESTER 2
Course	15 weeks	15 weeks
Project	4 weeks	8 weeks
Exams	1	1
Total Academic course duration - 42 weeks excluding examination		

Ajay

COURSE CONTENT

Semester I	Semester II
• Fundamentals of Computer and Cyber Security • Networking Basics and Network Security • Fundamentals of Web Designing and Web Application Security • Cryptography • Cloud Fundamentals and Cloud Security • Project 1	• Mobile Eco System Security • Internet of Things Security (IoT) • Advanced Network Security • Cyber Laws and Forensics • Information Security Compliance Management • Project 2

EXAMINATION PATTERN: (40 Theory 40 Practical and 20 Internal Assessments)

EXAM: Diploma Certificate will be issued to participants only after clearing final examination of both the semesters conducted the end of the final semester. The span period of the course will be as per the University Policy.

EXAM DURATION: As per guidelines issued by University of Delhi.

DURATION OF COURSE: 1 year.

SPAN OF COURSE: 2 years.

DELIVERABLES: Each student will get:

- A toolkit containing tools as required in the curriculum
- Videos for referrals case studies and White papers
- Subject Wise E- Tutorials

The schedule of papers prescribed for two semesters shall be as follows:

Semester I

Papers		Hrs. For lectures and labs	Total marks	Marks		
Paper No.	Title			Internal assessment	Practical	Writte n Exam
1	Fundamentals of Computer and Cyber Security	60 lectures	100	20	40	40
2	Networking Basics and Network Security	60 lectures	100	20	40	40
3	Fundamentals of Web Designing and Web Application Security	60 lectures	100	20	40	40
4	Cryptography	60 lectures	100	20	40	40
5	Cloud Fundamentals and Cloud Security	60 lectures	100	20	40	40
6	Project 1	4 weeks	100			

Ajay

Semester II

Papers		Hrs. For lectures and labs	Total marks	Marks		
Paper No.	Title			Internal assessment	Practical	Written Exam
1	Mobile Eco System Security	60 lectures	100	20	40	40
2	Internet of Things Security	60 lectures	100	20	40	40
3	Advanced Network Security	60 lectures	100	20	40	40
4	Cyber Law & Forensics	60 lectures	100	20	40	40
5	Information Security Compliance Management	60 lectures	100	20	40	40
6	Project 2 + Internship	8 weeks	100			

Note: Each lecture will be 60 minutes in duration.

Semester - 1

Paper 101: Fundamentals of Computer and Cyber Security

Marks: 100 **Lectures 60**

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

Unit I: Fundamentals of Computer and Cyber Security

Introduction to Computers, Computer History, Software, Hardware, Classification, Computer Input-Output Devices, Windows, DOS Prompt Commands, Operating System Security(windows and Linux) terminal and Commands, Basic Computer Terminology, Computer Security models, Computer Security Terms, Computer Ethics, Business and Professional Ethics, Need for cyber security; Cyber Frauds and crimes, Digital Payments, Various Search Engines, Introduction to Auditing,.Deep Web, VAPT, Smartphone Operating systems, introduction to compliances ,Globalization and border less world.

Unit II: Python Scripting and PHP Basics

Python and PHP Basics, Variables and Types, Lists, Basic Operators, String Formatting, Basic String Operations, Conditions, Loops, Functions, Classes and Objects, Dictionaries, Modules and Packages. Web Development with Python Introduction to web frameworks: Flask, Django
Creating RESTful APIs Handling forms, templates, and sessions Advanced PHP Programming, Object-oriented programming: classes and objects, inheritance, polymorphism, Exception handling, File handling and I/O operations, Common security threats (e.g., SQL injection, XSS, CSRF)

Unit III: Cyber Laws

Need for Cyber Regulations; Scope and Significance of Cyber laws: Information Technology Act 2000; Network and Network Security, Access and Unauthorized Access, Data Security, E Contracts and E Forms. Penal Provisions for Phishing, Spam, Virus, Worms, Malware, Hacking, Trespass and Stalking; Human rights in cyberspace, International Co-operation in investigating cybercrimes. Incident Response and Disaster Recovery: Incident response process: detection, analysis, containment, eradication, and recovery. Disaster recovery planning and business continuity. Legal and ethical considerations in incident response.

Ajay

Unit IV: Encoding

Encoding: Charset, ASCII, UNICODE, URL Encoding, Base64, Illustration: ISBN/ QR Code/ Barcode, Binary hamming codes and Binary Reedmuller codes.

Unit V: Web Application Architecture

HTML Basics, XAMPP Server Setup, Hosting Websites Linux, Apache, Virtualizations, Server Configurations, Web Application Firewalls. Security in Web Applications OWASP Top Ten Security Risks, Secure Authentication and Authorization (OAuth2, JWT), Secure data transmission (TLS/SSL) Cross-site Scripting (XSS), SQL Injection, CSRF Prevention

Recommended Practical Questions

Fundamentals of Computer Security

1. **Virus and Malware Analysis**:
   - Analyze a given malware sample and document its behavior, including file system changes, network activity, and registry modifications.
   - Identify the type of malware (e.g., virus, worm, Trojan) and explain its propagation method.
2. **Firewall Configuration**:
   - Configure a firewall to block all incoming traffic except for HTTP and HTTPS. Verify that other services are inaccessible.
   - Set up a firewall rule to allow traffic from a specific IP address and block all others. Test the configuration with different IP addresses.
3. **Security Auditing**:
   - Perform a security audit on a Windows system using built-in tools (e.g., Event Viewer, Audit Policy). Identify any potential security issues.
   - Conduct a vulnerability assessment on a Linux server using tools like Lynis. Provide a report detailing the findings and recommended actions.

Suggested Readings:

1. Langtangen, H.P. (2012). *Python Scripting for Computational Science* (4th Ed.). Springer
2. Behrouz A. Forouzan (2004). *Data communication and Networking*. Tata McGraw-Hill.

3. Kurose, James F. & Ross, Keith W. (2003). *Computer Networking: A Top-Down Approach Featuring the Internet* (3rd Ed.). Pearson Education.
4. Shklar, L. & Rosen, R. (2009). *Web Application Architecture: Principles, Protocols and Practices* (2nd Ed.). John Wiley & Sons.
5. Craig, B. (2012). *Cyber Law: The Law of the Internet and Information Technology.* Pearson.
6. Sharma J. P. & Kanojia S. (2016). *Cyber Laws.* New Delhi: Ane Books Pvt Ltd.
7. Paintal, D. *Law of Information Technology.* New Delhi: Taxman Publications Pvt. Ltd.
8. Forbes, A. (2015). *The Joy of PHP: A Beginner's Guide to Programming Interactive Web Applications with PHP and MySQL* (4th Ed.). Plum Island Publishing LLC.
9. Shema, M. (2012). *Hacking Web Apps: Detecting and Preventing Web Application Security Problems.*
10. Peterson. W.W, (1972), Error *Correcting Codes,* MIT Press
11. https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf
12. MacWilliams F J and Sloane N J A, (2013), Theory *of Error Correcting Codes*, North Holland Elsevier Science Ltd

Semester - 1
Paper 102: Network Basics and Network Security

Marks: 100 **Lectures 60**

Objective: This course aims at 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 the course 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 varied attacks.

Unit I: Introduction to Network Security

Types of networks, IP Address, NAT, IP Subnets, DHCP Server, Ports, DNS, Proxy Servers, Virtual Private Networks, DNS Server, OSI and TCP IP Model, 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).

Unit II: Virtual Private Networks

VPN and its types –Tunneling 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

Network Sniffing, Wireshark, packet analysis, display and capture filters, Ettercap, DNS Poisoning, ARP Poisoning, Denial of services, Vulnerability scanning, Nessus, Network Policies, Open VAS, Sparta, Network Scanning Report Generation, System hardening, secure system configurations, SSL Striping, Setup network IDS/IPS, Router attacks, VPN Pentesting, VOIP Pentesting,

Unit IV: Network Attacks Part 2

Network Exploitation OS Detection in network, 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 sploi. Framework exploits delivery. End Point Security.

Unit V: Wireless Attacks

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

Recommended Practical Questions

1. **Network Topology Design:**
   - Design a network topology for a small office, including routers, switches, and end devices. Create a diagram and explain the choice of devices.
   - Simulate the designed network topology using network simulation software (e.g., Cisco Packet Tracer) and verify connectivity.
2. **Packet Sniffing and Analysis:**
   - Use Wireshark to capture network traffic on a local network. Identify and analyze packets related to common protocols (e.g., HTTP, DNS).
   - Capture and analyze a packet containing a login attempt to a web application. Identify the username and any potential security issues.
3. **Secure Socket Layer (SSL) Configuration:**
   - Configure SSL on a web server and verify the SSL certificate using a browser. Explain the process of obtaining and installing the certificate.
   - Test the SSL configuration for vulnerabilities (e.g., Heartbleed) using tools like SSL Labs. Provide a report on the findings.

Suggested Readings:

1. Kaufman, C, Perlman, R., & Speciner, M. (2002). *Network Security, Private communication in the public world* (2nd Ed.). PHI

2. Monte, M. (2015). *Network Attacks and Exploitation: A Framework.* Wiley.

3. Perez, Andre. (2014). *Network Security.* Wiley.

4. Stallings, W. (2006). Cryptography and Network Security: Principles and Practice (8th Ed.). Prentice Hall
5. "Wireless Network Security: A Beginner's Guide" by Tyler Wrightson
   A practical guide to securing wireless networks, covering both basics and advanced topics.

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester - 1

Paper 103: Fundamentals of Web Designing and Web Application Security

Marks: 100 **Lectures 60**

Objective: Moving from networks the most important component of any technology stack is the software which is positioned at the top of infrastructure. We will start with the necessities of how software applications are built, where students will understand and build their applications to have the real world feel on how the internet stack is working, along with showing them real loopholes while coding himself so that they understand the real world attacks which are possible on applications, and simulate them so that they can themselves come to conclusions and understand the best practices involved in application security.

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. Introduction to Voice Search Optimization.

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. 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.

Unit IV: Web Application Attacks Part II

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, 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.

Practical: This paper will have 30 lectures for the practical work.

Recommended Practical Questions

1. **HTML and CSS Basics:**
    - Create a simple webpage with HTML and CSS that includes a header, navigation bar, main content area, and footer. Ensure it is responsive.
    - Implement a contact form using HTML and CSS, including fields for name, email, and message. Validate the input fields.
2. **JavaScript Security:**
    - Write JavaScript code to validate user input on a form (e.g., email address format) and prevent submission of invalid data.
    - Implement measures to prevent common JavaScript vulnerabilities such as Cross-Site Scripting (XSS) in a sample web application.
3. **Web Application Vulnerability Scanning:**
    - Perform a vulnerability scan on a provided web application using OWASP ZAP. Identify and report any found vulnerabilities.
    - Demonstrate how to exploit a found vulnerability and then implement a fix. Re-scan the application to ensure the vulnerability is resolved.

Suggested Readings:

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.

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester - 1
Paper 104: Cryptography

Marks: 100 **Lectures 60**

Objective: After infrastructure and software, the communication in between multiple devices using applications and securing them become most important, cryptography is the mechanism using which we hide the information in public eye site from anybody and is something which is used very popularly almost anything across the internet. So, we start with fundamentals of what cryptography is and how cryptography algorithms work and then come to real world scenarios on how currently our data processed on the internet is secured from the eyes of an intruder. Further, the paper enables the students to use cryptography in the most extensive and elaborate manner.

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 and Bitcoins

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

Unit IV: 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.

Ajay

Recommended Practical Questions

1. **Symmetric Key Encryption:**
    - Implement AES encryption in a programming language of your choice. Encrypt and decrypt a given plaintext message.
    - Compare the performance and security of different modes of AES (e.g., ECB, CBC) using sample data.
2. **Asymmetric Key Encryption:**
    - Generate a pair of RSA keys using a cryptographic library. Encrypt a message with the public key and decrypt it with the private key.
    - Explain the process of key generation, encryption, and decryption in RSA and discuss its applications.
3. **Digital Signatures:**
    - Create a digital signature for a given document using a private key. Verify the signature using the corresponding public key.
    - Explain the importance of digital signatures in ensuring data integrity and authenticity. Provide an example use case.

Suggested Readings:

1. Delfs, H. & Knebl, H. (2001). *Introduction to Cryptography: Principles and Applications*. Springer-Verlag Berlin and Heidelberg GmbH & Co.

2. Stallings, W. (2010). *Cryptography and network security: Principles and practice* (5th ed.) Boston: Prentice Hall.

3. Menezes, A.J., Oorschot, P. Van & Vanstone, S.A. (1997). *The Handbook of Applied Cryptography*. CRC Press.

4. Schneier, B. (1995). *Applied cryptography, Protocols, algorithms and source code in C* (2nd ed.). New York: John Wiley & Sons.

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester - 1

Paper 105: Cloud Fundamentals and Cloud Security

Marks: 100 **Lectures 60**

Objective: The purpose of the course is to make students understand and comprehend the revolutionizing concept of CLOUD in the cyber world with a view to enable them with achieving cloud security. It also aims at developing expertise amongst students with cloud architecture as well as the security concerns for organizations planning a move towards Cloud or planning to enhance their cloud security.

Unit I: Introduction to Cloud Computing

Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vsprivateclouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture. Application availability, performance, security and disaster recovery; next generation Cloud Applications.

Unit II: Cloud Application Architecture

Technologies and the processes required when deploying web services, Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages.

Unit III: Cloud Services Management

Reliability, availability and security of services deployed from the cloud.

Performance and scalability of services, tools and technologies used to manage cloud services deployment; Cloud Economics: Cloud Computing infrastructures available for implementing cloud-based services. Economics of choosing a Cloud platform for an organization, based on application requirements, economic constraints and business needs. Discuss industry cases including open sources.

Unit IV: Cloud Application Development

Service creation environments to develop cloud-based applications. Development, for service development; Amazon, Azure, Google App. Applicability of laws to data stored outside the nation's boundary.

Unit V: Cloud IT Model

Analysis of Cases while deciding to adopt secure cloud computing architecture. Appropriate cloud requirements. Secure Cloud based service, Applications and development platform deployment so as to improve the total cost of ownership (TCO), Compliance and Governance in Cloud: Ensuring adherence to regulations and standards

Ajay

Recommended Practical Questions

1. **Cloud Service Deployment:**
   - Deploy a simple web application (e.g., a static website) on a cloud platform like AWS S3 or Azure Blob Storage. Verify its accessibility.
   - Set up a virtual machine in a cloud environment (e.g., AWS EC2) and deploy a web server. Secure the instance by configuring security groups.
2. **Cloud Storage Security:**
   - Configure access controls for a cloud storage bucket to allow public read access to certain objects while keeping others private.
   - Implement encryption for data at rest in a cloud storage service and verify that the data is encrypted.
3. **Identity and Access Management (IAM):**
   - Create IAM users and groups in AWS or Azure. Assign appropriate permissions to ensure least privilege access for a given task.
   - Implement multi-factor authentication (MFA) for an IAM user and demonstrate the login process.

Suggested Readings:

1. Rittenhouse, J.W. & Ransome, J.F.(2010). *Cloud Computing: Implementation, Management, and Security*. CRC Press.
2. Rountree, D. & Castrillo, I. (2013). *The Basics of Cloud Computing: Understanding The Fundamentals Of Cloud Computing in Theory And Practice*. Syngress, Elsevier
3. Stallings (2016). *Cryptography & Network Security*. Paperback.
4. Vacca, J. (2016). *Cloud Computing Security: Foundations and Challenges*. CRC Press

Latest research papers from refereed journals discussed by the faculty may also be referred.

Semester 2

Paper 201: Mobile Eco- System Security

Marks: 100 **Lectures 60**

Objective: At a time when companies are looking at not only a mobile first approach but a mobile only approach, the cell phone revolution has hit both the enterprise and the consumer market in a massive way. Its entire eco system needs to be very carefully understood, and the various attacks which can be possible at each stage needs to be carefully, practically performed in order to understanding how to protect the entire mobility ecosystem, which is going to be one of the most important pillars of transforming an organization into a digital organization.

Unit I: Introduction to Mobile Eco-System Security
Mobile Security Model, Enterprise Mobile Environment, Mobile Crypto Algorithm.

Unit II: Mobile Eco-System Technology
Mobile Devices - features and security concerns, Platforms, Applications - development, testing and delivery

Unit III: Mobile Eco-System Networks
Cellular Network - baseband processor and SIM card, GSM encryption and authentication and other attacks, WIFI Networks - public hotspots and enterprise WLANs, SSL/TLS, Web Technologies - server-side and client-side web applications

Unit IV: 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

Recommended Practical Questions

1. **Mobile Application Security Testing:**
   - Perform a security assessment on a provided Android application using MobSF. Identify vulnerabilities related to insecure data storage and suggest remediation.
   - Test an iOS application for common security flaws such as improper platform usage and insecure communication. Use tools like Xcode and iOS Security Suite for the assessment.

2. Securing Mobile Devices:

- Configure MDM policies on an Android device to enforce encryption, remote wipe, and app management. Demonstrate the application and effectiveness of these policies.
- Implement biometric authentication on a mobile device and analyze its security compared to traditional PIN/password methods. Test scenarios where the biometric system could be bypassed.

3. Analyzing Mobile Malware:

- Use static analysis tools to dissect a provided mobile malware APK file. Document its permissions, embedded URLs, and potential malicious behavior.
- Conduct dynamic analysis by running the malware in a sandboxed environment. Capture and analyze the network traffic generated by the malware.

Suggested Readings:

1. Fried, S. (2010). *Mobile device security: A comprehensive guide to securing your information in a moving world.* Boca Raton, FL: Auerbach Publications.
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. Dwivedi, H., Clark, C., & Thiel, D. (2010). *Mobile application security.* New York: McGraw-Hill Companies.

Semester 2
Paper 202: Internet of Things Security (IoT)

Marks: 100 **Lectures 60**

Objective: The human race is going to go through a major transformation in the next ten years thanks to the internet of thing , when such a transformation happens, where internet and technology are going to touch possibly every aspect of our life , the security of the same would be of highest importance , here we will dwell with most popular IoT devices available in the market at present and their security concerns along with potential hacks that can be performed on such devices and to ensure its security according to best global practices.

Unit I: Introduction
Requirement and Basic Properties in Internet of Things, Primary challenges in security maintenance, Confidentiality, Integrity, Availability, Non-Repudiation.

Unit II: Architecture of Internet of Things
Device - device, Device - Cloud, Device - Gateway, Gateway - Cloud, Cloud – Backend - Applications

Unit III: Security Classification and Access Control
Data classification (Public and Private), Internet of Things Authentication and Authorization, Internet of Things Data Integrity

Unit IV: Attacks and Implementation of Internet of Things
Denial of Service, Sniffing, Phishing, DNS Hijacking, Pharming, Defacement, Firmware of the device, Web Application Dashboard, Mobile Application Used to Control, Configure and Monitor the Devices

Unit V: Security Protocols and Management
Firmware of the device, Web Application Dashboard, Mobile Application Used to Control, Configure and Monitor the Devices, Identity and Access Management, Key Management

Recommended Practical Questions

1. **Securing IoT Devices:**
    - Implement MQTT with TLS for an IoT device communication. Demonstrate the secure exchange of messages between the device and the server.
    - Set up an access control mechanism for an IoT network, ensuring only authorized devices can join and communicate. Test the setup with both authorized and unauthorized devices.

2. **IoT Vulnerability Assessment**:
   - Use Shodan to discover IoT devices on the internet. Select a device and perform a security assessment to identify open ports, services, and potential vulnerabilities.
   - Assess the security of a smart home IoT device using IoT Inspector. Identify weaknesses such as default credentials and outdated firmware and suggest mitigation steps.
3. **IoT Data Encryption**:
   - Implement AES encryption for data stored on an IoT device. Encrypt and decrypt a sample dataset to verify the implementation.
   - Secure the data transmission from an IoT sensor to the cloud using HTTPS. Capture the network traffic to confirm the data is encrypted.

Suggested Readings:

1. Russell, B. (2016). *Practical Internet of Things Security*. Packet Publishing Limited
2. FeiHu (2016). *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations*. CRC Press
3. Hersent, O., Boswarthick, D., & Elloumi, O. (2015). The Internet of Things: Key Applications and Protocols. Wiley
4. Pfister, C. (2011). *Getting Started with the Internet of Things*. Shroff Publisher.

Ajay

Semester 2

Paper 203: Advanced Network Security

Marks: 100 **Lectures 60**

Objective: To provide a deep understanding of contemporary network security measures, focusing on advanced concepts and practical implementations to secure modern network infrastructures against sophisticated threats.

Unit I: Introduction

Network Segmentation and Segregation , Boundary Protection, Firewalls , Logically Separated Control Network , Network Segregation, Recommended Defence-in-Depth Architecture, General Firewall Policies for ICS , Recommended Firewall Rules for Specific Services , Network Address Translation (NAT), Specific ICS Firewall Issues , Unidirectional Gateways , Single Points of Failure , Redundancy and Fault Tolerance , Preventing Man-in-the-Middle Attacks , Authentication and Authorization , Monitoring, Logging, and Auditing, Monitoring, Logging, and Auditing , Response, and System Recovery, Using tools such as Wireshark, Metasploit, Splunk etc.

Unit II: Zero Trust Architecture (ZTA)

Principles of Zero Trust: Trust nothing, verify everything. Micro segmentation: Segmenting networks to minimize attack surfaces. Zero Trust Networks (ZTN): Implementing ZTA in corporate environments. Identity and Access Management (IAM): Ensuring proper authentication and authorization. Case Studies and Best Practices: Real-world implementations and lessons learned.

Unit III: Advanced Threat Protection (ATP)

Understanding ATP: Components and functionalities. Threat Intelligence Integration: Leveraging threat intelligence in ATP solutions. ATP Techniques: Sandboxing, behavioral analysis, and more. Case Studies: Successful ATP implementations. Introduction to Cyber Threat Intelligence (CTI) Threat Intelligence Lifecycle: Understanding the stages from data collection to dissemination. Types of Threat Intelligence: Strategic, tactical, operational, and technical. Threat Intelligence Platforms (TIPs): Tools and techniques for managing threat data. Indicators of Compromise (IoCs): Identifying and utilizing IoCs for threat detection. Case Studies: Real-world examples of threat intelligence applications.

Ajay

Unit IV Information Hiding Techniques

Introduction to Steganography and Watermarking. Differences between Watermarking and Steganography, A Brief History. Digital Steganography, Applications of Steganography, Covert Communication, Techniques of Steganography (for Text and Image). Steganographic Software: S-Tools, StegoDos, EzStego, Jsteg-Jpeg.

Unit V: Intrusion Detection and Prevention Systems (IDPS)

Types of IDPS: Network-based, host-based, and hybrid systems. Detection Techniques: Signature-based, anomaly-based, and hybrid detection. Implementation: Best practices for deploying IDPS in various environments. Response Strategies: Automated and manual response techniques.

Recommended Practical Questions

1. **Intrusion Detection and Prevention Systems (IDPS):**
   - Deploy Snort as an IDPS in a virtual network environment. Create and test custom rules to detect a simulated SQL injection attack.
   - Configure Suricata to monitor network traffic for signs of a DDoS attack. Test its effectiveness by generating controlled traffic and analyzing the alerts.
2. **Network Segmentation:**
   - Design and implement VLANs in a simulated enterprise network. Configure inter-VLAN routing and apply access control lists (ACLs) to control traffic between VLANs.
   - Test the security of the segmented network by attempting to access resources across different VLANs. Verify the ACLs effectively restrict unauthorized access.
3. **Secure Network Design:**
   - Design a secure network architecture for a medium-sized business, including the placement of firewalls, VPN gateways, and intrusion detection systems.
   - Simulate the network using GNS3 or Packet Tracer. Test the security controls by attempting to penetrate the network from an external attacker's perspective.

Suggested Readings

1. "Network Security Essentials: Applications and Standards" by William Stallings
   A comprehensive guide covering the essentials of network security, including cryptography, network-based attacks, and secure network applications.

2. "Zero Trust Networks: Building Secure Systems in Untrusted Networks" by Evan Gilman and Doug Barth
   Focuses on the principles and implementation of Zero Trust architecture to secure modern network environments.

3. Katzenbeisser, S. & Fabien A P. (2000). *Information Hiding Techniques for*

Steganography and Digital Watermarking. Petitcolas, Artech House.

4. Unit V: Advanced Threat Protection (ATP)"Cyber Threat Intelligence: From Data to Actions" by Henry Dalziel Provides insights into threat intelligence and its role in ATP.

Latest research papers from refereed journals discussed by the faculty may also be referred.

Ajay

Semester 2

Paper 204: Cyber Law and Forensic Evidence

Marks: 100 **Lectures 60**

Objective: The paper aims to create the basic clarity and understanding of cybercrimes and cyber security laws to the professionals learning the ethical hacking programme. The paper would address and emphasise the activities leading to infringement of individual or organisational privacy. Further, the paper intends to create highly sensitised professionals who can be responsible for handling cyber security issues pertaining to varied domains and dealing in forensics diligently.

Unit I: Introduction to Cyberspace, Cybercrime and Cyber Law

The World Wide Web, Web Centric Business, E Business Architecture, Models of E Business, E Commerce, Threats to virtual world. Cyber Crimes& social media, Cyber Squatting, Cyber Espionage, Cyber Warfare, Cyber Terrorism, Cyber Defamation. Online Safety for women and children, Misuse of individual information. Objectives, Applicability, Non applicability and Definitions of the Information Technology Act, 2000.

Unit II: Regulatory Framework of the Information Technology Act, 2000

Digital Signature, Electronic Signature, Reliable Electronic Signature, Secured Electronic Signature, Electronic Records, and Electronic Governance. Controller, Certifying Authority, Adjudicating Officer and Appellate Tribunal. (Rules announced under the Act); Electronic Evidence – Power to investigate and Examiner for expert opinion (IT Act), Admissibility (The BSA, 2023).

Unit III: Offences and Penalties

Offences under the Information and Technology Act 2000, Penalty and adjudication. Punishments for contraventions under the Information Technology Act 2000; Role of Intermediaries and their liabilities; Power of Government to give directions under the Information Technology Act, 2000 – Blocking, Interception, Collecting traffic data, Critical Infrastructure Protection, Computer Emergency Response Team (Cert-In) and its functions-(Case Laws, Rules and recent judicial pronouncements to be discussed). Limitations of Cyber Law.

Security Policies, Standards, and Compliance: Development and implementation of security policies and standards. Compliance frameworks (e.g., GDPR, HIPAA, PCI DSS) and regulatory requirements. Auditing, assessment, and compliance monitoring.

Unit IV: Fundamentals of Cyber Forensics

Cyber Forensic Basics- Introduction to Cyber Forensics, Storage Fundamentals, File System Concepts, Data Recovery, Operating System Software and Basic Terminology Data and Evidence Recovery- Introduction to Deleted File Recovery, Formatted Partition Recovery

Unit V: Data Recovery Tools, Data Recovery Procedures and Ethics Gathering Evidence- Precautions, Preserving and safely handling original media for its admissibility, Document a Chain of Custody and its importance, Complete time line analysis of computer files based on file creation, file modification and file access, Recover Internet Usage Data, Data Protection and Privacy, Recover Swap Files/Temporary Files/Cache Files, Introduction to Encase Forensic Edition, Forensic Toolkit etc., Use computer forensics software/tools to cross validate findings in computer evidence-related cases.

Unit VI: Cyber Forensics Investigation

Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deleted evidence, Password Cracking, Cracking with GPU Systems, Hashcat. Work on open Source, Commercial tools and Cyber range, Digital Identity and Authentication

E-Signatures and Digital Identities: Legal recognition of digital identities and e-signatures, enabling more secure and efficient online transactions.

Biometric Data Protection: Laws and regulations governing the collection, use, and storage of biometric data, ensuring privacy and security.

Recommended Practical Questions

1. **Digital Forensics Investigation:**
   - Perform a forensic analysis on a provided disk image using Autopsy. Recover deleted files and analyze file metadata to determine the sequence of events.
   - Use FTK Imager to create a forensic image of a provided USB drive. Analyze the image for evidence of unauthorized access and data exfiltration.
2. **Incident Response:**
   - Simulate a ransomware attack on a virtual machine. Perform an incident response exercise, documenting the steps taken to contain, eradicate, and recover from the attack.
   - Develop an incident response plan for a small business. Include procedures for detection, containment, eradication, recovery, and lessons learned.
3. **Legal Aspects of Cybersecurity:**
   - Review a recent cybercrime case study and identify the laws that were violated. Discuss the potential legal consequences for the perpetrators.
   - Create a compliance checklist for an organization to ensure adherence to GDPR. Include measures for data protection, breach notification, and data subject rights.

Suggested readings

1. Craig, B. *Cyber Law: The Law of the Internet and Information Technology.* Pearson Education

Ajay

2. Paintal, D. *Law of Information Technology*. New Delhi: Taxmann Publications Pvt. Ltd.

3. Lindsay, D. (2007). *International domain name law: ICANN and the UDRP*. Oxford: Hart Publishing.

4. Sharma J. P, & Kanojia S. (2016). *Cyber Laws*. New Delhi: Ane Books Pvt. Ltd.

5. Duggal, P. *Cyber Laws*. (2016) Universal Law Publishing.

6. Kamath, N. (2016). *Law relating to computers, internet and e-commerce: A guide to Cyber Laws and the Information Technology Act, 2000 with rules, regulations and notifications (5th ed.)*. Delhi: Universal Law Publishing Co.

7. "Cyber Law: Indian Perspective" by Pavan Duggal

8. Prosise, C. & Mandia, K. (2014). Incident response & computer forensics (3rd ed.). New York, NY: McGraw-Hill Companies.
9. "Computer Forensics: Cybercriminals, Laws, and Evidence" by Marie-Helen Maras

Latest Editions of the Suggested Readings along with discussion material by the faculty.

Ajay

Semester 2
Paper 205: Information Security Compliance Management

Marks: 100 **Lectures 60**

Objective: In view of providing technical superiority essentially be complimented with the appropriate compliance advancement to maintain hygiene from the point of view of cyber security Compliances have increasingly coming up not in just financial or aviation space but also in conventional industries like manufacturing, real estate among others and hence its of tremendous importance for a cyber-security professional to have comprehensive knowledge of the most important compliances and the modus operandi from people, process and technology to get through a compliance check.

Unit I: Introduction to Information Security Management System (ISMS) - ISO/IEC 27001
Critical Appraisal of ISO 9000, Normative, regulatory and legal framework related to information security Fundamental principles of information securities/IEC 27001 certification process, Information Security Management System (ISMS), detailed presentation of the clauses 4 to 8 of ISO/IEC 27001

Unit II: Planning and Initiating an ISO/IEC 27001 audit
Fundamental audit concepts and principles, Audit approach based on evidence and on risk, Preparation of an ISO/IEC 27001 certification audit, ISMS documentation audit, Conducting an opening meeting

Unit III: Conducting an ISO/IEC 27001 audit
Communication during the audit, Audit procedures: observation, document review, interview, sampling techniques, technical verification, corroboration and evaluation, Audit test plans, Formulation of audit findings, Documenting nonconformities

Unit IV: Concluding and ensuring the follow-up of an ISO/IEC 27001 audit.
Audit documentation, Quality review, Conducting a closing meeting and conclusion of an ISO/IEC 27001 audit, Evaluation of corrective action plans, ISO/IEC 27001 Surveillance audit, internal audit management program

Unit V: PCI DSS, HIPPA
Security Management Process, Risk Analysis Risk Management, Information System Activity Review, Assigned Security Responsibility, Authorization and/or Supervision, Termination Procedures, Access Authorization, Access Establishment and Modification, Protection from Malicious Software, Log-in Monitoring, Password Management, Response and Reporting,

Contingency Plan Evaluation, Facility Access Control and Validation Procedures, Unique User Identification, Emergency Access Procedure, Automatic Logoff Encryption and Decryption, Audit Controls, Data Integrity, Person or Entity Authentication, Integrity Controls Encryption

Unit VI Intellectual Property Rights
Intellectual Property Rights: Types and Issues related to IPR, Policy framework in India and Abroad, Bitcoin and law enforcement.

Recommended Practical Questions

1. **Compliance Audit:**
   - Conduct a compliance audit for a provided organization based on ISO 27001 standards. Identify areas of non-compliance and suggest corrective actions.
   - Perform a GDPR compliance assessment for a company. Evaluate their data protection practices and provide recommendations to address any gaps.
2. **Risk Assessment and Management:**
   - Perform a risk assessment for a fictitious company. Identify potential threats, vulnerabilities, and impacts on critical assets. Prioritize the risks and suggest mitigation strategies.
   - Develop a risk management plan that includes risk identification, assessment, treatment, and monitoring. Implement the plan for a given scenario and evaluate its effectiveness.
3. **Policy Development:**
   - Develop a comprehensive information security policy for a small business. Include sections on access control, data protection, incident response, and employee responsibilities.
   - Implement the developed policy in a simulated environment. Conduct a tabletop exercise to test the policy's effectiveness in responding to a security incident.

Suggested Readings:

1. Godbole, N. *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*. Wiley

2. Calder, A. (2009*). Implementing Information Security Based on ISO 27001/ISO 27002: A Management Guide* (2nd Ed.). Van Haren Publishing

3. Humphreys, E. (2016). Implementing the ISO/IEC 27001 Information Security Management System Standard. Artech House Publishers.

4. Watkins, S. G. (2022). *An Introduction to Information Security and ISO 27001: 2022 A Pocket Guide*. IT Governance Publishing.

5. https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf

Ajay

Latest research papers from refereed journals discussed by the faculty may also be referred.

Ajay