जम्मू केंद्रीय विश्वविद्यालय
Central University of Jammu
राया-सूचानी, जिला **सांबा -181143**,जम्मू **(जम्मू एवं कश्मीर)**
Rahya-Suchani, District Samba-181143, Jammu (J&K), India

Post Graduate Diploma in Cyber Forensic (PGDCF)

The 12-month Post Graduate Diploma in Cyber Forensic (PGDCF) with exit option after 6 months is designed to provide students with foundational knowledge and practical skills necessary to protect information systems from cyber threats. With a blend of theoretical understanding and hands-on experience, this program equips students to address real-world cyber security challenges and prepares them for entry-level roles in the rapidly evolving field of cyber security and digital forensic.

Fundamentals of Cyber Security

Rationale

This course serves as an entry point into the domain of cyber security, focusing on foundational principles, threat landscapes, and basic protection mechanisms. It is tailored for students with no prior background in the subject, providing them with a clear understanding of critical concepts such as the CIA triad, attack vectors, and the role of security tools. This course empowers students to comprehend the significance of cyber security in today's digital world.

Course Contents

Contents	**No. of Lectures**
Unit I **Overview of Cyber Security:** Definition and scope of cyber security, Importance in modern society, Threat landscape, Case studies on common attacks (Phishing, Malware, and Ransomware).	8
Unit II **Cyber Security Principles:** Confidentiality, Integrity, and Availability (CIA Triad); Principles of Authentication, Authorization, Non-repudiation; Importance of Accountability in systems	8
Unit III **Cyber Threats and Risks:** Classification of vulnerabilities (software, hardware, human); Exploit examples; Introduction to attack vectors (network, application, and social engineering); Basics of risk management, Risk assessment frameworks.	8
Unit IV **Security Mechanisms:** Firewalls: Types and configurations; Antivirus software: Role and updates; Access control: Methods and levels; Security policies: Creating, enforcing, and auditing policies.	8
Unit V **Introduction to Security Tools:** Introduction to Wireshark (packet capture and analysis); Overview of Nessus (vulnerability scanning); Basic usage of security tools for system analysis and protection.	8

Course Outcomes

Upon successful completion of this course, students will be able to:

1. Grasp the foundational principles and importance of cyber security in modern contexts.
2. Identify and categorize common cyber threats and their corresponding impacts.
3. Analyze cyber risks and vulnerabilities within software, networks, and human factors.
4. Apply fundamental security mechanisms to safeguard systems and data.
5. Use introductory security tools like Wireshark and Nessus to detect and analyze vulnerabilities effectively.
6. Develop a proactive approach to maintaining security through policies and updated defenses.

List of Books and References

- Bhushan, M., Singh Rathore, R., Jamshed, A. (2017). Fundamentals of Cyber Security: Principles, Theory and Practices. Germany: BPB Publications.
- Stallings, W. (2016). Network Security Essentials: Applications and Standards. United Kingdom: Pearson.
- Shinde, A. (2021). Introduction to Cyber Security: Guide to the World of Cyber Security. Notion Press.
- Gollmann, D. (2011). Computer Security. United Kingdom: Wiley.

Network Essentials for Cyber Security

Rationale

This course introduces students to essential networking concepts crucial for understanding the security of communication systems. It covers networking fundamentals, protocols, devices, and security mechanisms that form the backbone of secure digital communication. The course also emphasizes packet analysis techniques to identify potential threats within network traffic. The objective is to provide students with the necessary skills to understand and secure network infrastructures effectively.

Course Contents:

Contents	**No. of Lectures**
Unit I **Networking Fundamentals:** OSI Model layers and their functions; Introduction to TCP/IP Suite; IP addressing (IPv4 and IPv6) concepts; Subnetting techniques, Network Address Translation (NAT).	8
Unit II **Protocols and Services:** Overview of essential network protocols: DNS (Domain Name System), HTTP/HTTPS (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), and DHCP (Dynamic Host Configuration Protocol)	8
Unit III **Network Devices:** Role and operation of networking devices: Switches, Routers, Firewalls; Introduction to Intrusion Detection and Prevention Systems (IDS/IPS), their importance in network security.	8
Unit IV **Secure Network Design:** Secure network architecture design, understanding network topologies (star, mesh, etc.); DMZ (Demilitarized Zone) configuration; Virtual Private Networks (VPNs) for secure communications; Virtual LANs (VLANs) for network segmentation.	8
Unit V **Introduction to Packet Analysis:** Introduction to packet capturing and analysis using Wireshark; Basics of packet structures; Capturing network traffic and analyzing it to detect suspicious activities or vulnerabilities.	8

Course Outcomes

Upon successful completion of this course, students will be able to:

1. Understand and explain the basic networking concepts and protocols that form the foundation of network security.
2. Identify the role and operation of different network devices, including switches, routers, and firewalls, in ensuring network security.
3. Understand how network protocols like DNS, HTTP/HTTPS, FTP, and SMTP contribute to the overall network security.
4. Design and implement secure network architectures using concepts like VPNs, VLANs, and DMZs.
5. Use tools like Wireshark to capture and analyze network traffic for detecting potential security threats or anomalies.

List of Books and References

- Kurose, J. F. (2005). Computer Networking: A Top-Down Approach Featuring the Internet, 3/e. India: Pearson Education.
- Bragg, R., Rhodes-Ousley, M., Strassberg, K. (2004). Network Security: The Complete Reference. United Kingdom: McGraw-Hill Education.
- Bose, S., Vijayakumar, P. (2016). Cryptography and Network Security. India: Pearson.
- Kizza, J. M. (2008). Guide to Computer Network Security. Germany: Springer London.
- Stallings, W. (2007). Data and Computer Communications. India: Pearson Education.

Ethical Hacking and Penetration Testing

Rationale

This course provides students with a comprehensive introduction to the field of ethical hacking and penetration testing. Students will learn to identify vulnerabilities in systems through systematic techniques and tools used by ethical hackers. Emphasis is placed on hands-on practices, using industry-standard tools for reconnaissance, exploitation, and mitigation. By the end of the course, students will gain knowledge in performing ethical hacking activities while adhering to legal and ethical standards, and preparing thorough security reports.

Course Contents

Contents	**No. of Lectures**
Unit I **Introduction to Ethical Hacking:** Definition of ethical hacking and its importance in cyber security; Roles of ethical hackers in organizations; Legal and ethical considerations in hacking; Overview of hacker types (black hat, white hat, gray hat).	8
Unit II **Information Gathering:** Reconnaissance techniques: Passive vs. active methods; Footprinting: Gathering information from public sources; Scanning: Identifying live hosts and services using tools like Nmap and Netcat.	8
Unit III **Vulnerability Analysis:** Techniques for identifying vulnerabilities in systems and networks; Using tools like Nessus and OpenVAS for vulnerability scanning; Interpretation of vulnerability scan results and prioritization of threats.	8
Unit IV **Exploitation and Penetration Testing:** Exploit development: Understanding and creating exploits for known vulnerabilities; Penetration testing on networks and applications using tools like Metasploit; Attacking and defending against real-world attacks.	8
Unit V **Reporting and Mitigation:** Documenting findings in a penetration testing report; Writing clear and actionable	8

security recommendations; Mitigating vulnerabilities: Patching, firewall configurations, intrusion detection systems, and best practices.	

Suggested List of Lab Experiments

1. To understand and perform reconnaissance and footprinting techniques using industry-standard tools.
2. To conduct network scanning and enumeration to identify vulnerabilities in a system.
3. To exploit known vulnerabilities using frameworks like Metasploit to understand exploitation mechanisms.
4. To demonstrate password cracking techniques using brute force and dictionary attacks.
5. To simulate web application vulnerabilities like SQL Injection and XSS in a controlled environment.
6. To analyze and apply social engineering tactics to assess human vulnerabilities in security.
7. To perform wireless network analysis and identify potential threats in Wi-Fi security.
8. To assess system vulnerabilities by performing basic penetration testing on a network.
9. To learn how to use tools such as Nessus and OpenVAS for vulnerability assessment and management.
10. To understand and practice phishing attacks and learn countermeasures to prevent them.

Course Outcomes

Upon successful completion of this course, students will be able to:

1. Understand the legal and ethical aspects of ethical hacking and how to conduct hacking activities responsibly.
2. Use industry-standard tools to identify and analyze vulnerabilities in both network and application layers.
3. Develop and conduct penetration testing on systems and networks, simulating real-world attack scenarios.
4. Document and report security findings with clarity and accuracy, providing appropriate security recommendations.
5. Apply security mitigations effectively to resolve identified vulnerabilities and enhance system resilience.

List of Books and References

- Engebretson, P. (2013). The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. Netherlands: Elsevier Science.Cyber Forensics.
- Baloch, R. (2017). Ethical Hacking and Penetration Testing Guide. United States: CRC Press.
- Sabih, Z. (2018). Learn Ethical Hacking from Scratch: Your Stepping Stone to Penetration Testing. Germany: Packt Publishing.
- Weidman, G. (2014). Penetration Testing: A Hands-On Introduction to Hacking. United States: No Starch Press.
- GRAHAM, D. (2021). Ethical Hacking: A Hands-on Introduction to Breaking In. United Kingdom: No Starch Press.

Web Application Security

Rationale

This course focuses on understanding web application vulnerabilities and teaches students secure coding practices, along with testing techniques to protect web platforms from various attacks. Web applications are increasingly targeted by attackers due to their ubiquitous nature. By learning how to identify common vulnerabilities such as SQL injection, XSS, and CSRF, students will be equipped with the skills to develop and test secure applications. The course also emphasizes hands-on learning with industry-standard tools to scan, identify, and fix security flaws, ensuring that students are well-prepared for real-world challenges.

Course Contents

Contents	**No. of Lectures**
Unit I **Web Application Basics:** Introduction to web architecture: Client-server model, web application layers (front-end, back-end, database); Understanding HTTP/HTTPS protocols, cookies, and sessions: How data is transmitted and stored on the web.	8
Unit II **Web Security Overview:** Theory-based unit focusing on key security principles and their applications in web applications. Topics include secure communication protocols, protection against man-in-the-middle attacks, securing web storage, and advanced session management strategies.	8
Unit III **OWASP Top 10 Vulnerabilities:** Overview of OWASP (Open Web Application Security Project); In-depth exploration of the top 10 web vulnerabilities: SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Insecure Deserialization, and others.	8
Unit IV **Secure Coding Practices:** Best practices in secure coding: Input validation, Output encoding to prevent injection attacks, Secure authentication and authorization techniques; Designing secure web applications from the ground up.	8
Unit V	

Vulnerability Scanning Tools: Introduction to web application vulnerability scanning tools: Burp Suite, OWASP ZAP Proxy, Acunetix; How these tools work, their key features, and how to use them to identify common security vulnerabilities.	8

Suggested List of Lab Experiments

1. To analyze the basic structure of a web application and understand the functioning of HTTP/HTTPS protocols.
2. To understand the working of cookies and sessions in web applications and their potential vulnerabilities.
3. To identify and exploit basic SQL injection vulnerabilities in a web application.
4. To identify and exploit reflected Cross-Site Scripting (XSS) vulnerabilities in web applications.
5. To understand the workings of Cross-Site Request Forgery (CSRF) attacks and explore preventive measures.
6. To learn about insecure deserialization vulnerabilities and how to exploit them in web applications.
7. To gain hands-on experience in using Burp Suite for web application security testing and vulnerability scanning.
8. To understand the process of using OWASP ZAP for scanning and identifying vulnerabilities in web applications.
9. To perform a session fixation attack and understand the importance of proper session management.
10. To implement input validation techniques in web forms to prevent injection attacks like SQL injection and XSS.

Course Outcomes

Upon successful completion of this course, students will be able to:

1. Identify and mitigate web application vulnerabilities using secure coding techniques and best practices.
2. Apply secure coding methods such as input validation and output encoding to protect against injection attacks, XSS, and other common vulnerabilities.
3. Use industry-standard web vulnerability scanning tools like Burp Suite and OWASP ZAP effectively to identify and resolve security issues in web applications.
4. Understand the security risks associated with web protocols, cookies, and sessions, and take steps to secure them.
5. Conduct hands-on penetration testing on web applications to identify vulnerabilities and generate detailed security reports.

List of Books and References

- Hoffman, A. (2024). Web Application Security: Exploitation and Countermeasures for Modern Web Applications. China: O'Reilly Media.
- Shema, M. (2012). Hacking Web Apps: Detecting and Preventing Web Application Security Problems. Netherlands: Syngress.
- Sullivan, B., Liu, V. (2011). Web Application Security, A Beginner's Guide. United States: McGraw Hill LLC.
- Cross, M. (2011). Developer's Guide to Web Application Security. Ukraine: Syngress.
- Harwood, M. (2015). Internet Security: How to Defend Against Attackers on the Web. United States: Jones & Bartlett Learning.

Cyber Forensic: Laws and Regulations

Rationale

The course will explore the knowledge of cybercrime and related laws, related policies, and compliances. It will focus on understanding primarily legal aspects related by cyber laws and cybercrimes and whenever necessary on cyber forensic aspects. Indian Information Technology Act along with certain criminal laws will be analyzed in detail to understand the law framework in this regard. The course will also cover Intellectual property issues in cyberspace.

Course Contents

Contents	**No. of Lectures**
Unit I Introduction Cyberspace, Cybersecurity, Nature of threats, Cybercriminals, Cybersecurity Policy, Current cybercrime scenario and challenges.	8
Unit II Cyber Offenses Categories of Cybercrimes – Active and Passive attacks, Tools and Methods used in cybercrime, Social Engineering, Classification of the cybercrimes	8
Unit III Cybercrime Legal Perspective, Introduction to the Legal Perspectives of Cybercrimes and Cybersecurity, Cybercrime, and the Legal Landscape around the World, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Digital Signatures and the Indian IT Act, Cybercrime and Punishment, Cyberlaw, Technology and Students: Indian Scenario	8
Unit IV Digital Ethics, Privacy & Legislation Computer ethics, moral and legal issues, descriptive and normative claims, Professional Ethics, code of ethics and professional conduct. Privacy, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT, Negotiable Instruments Act 1881(Amended), IPC and CrPC, Electronic Communication Privacy ACT	8
Unit V Intellectual property issues in cyberspace Introduction to	8

intellectual property, WIPO, computer software copyrights, copyright in databases and electronic publishing, the law of confidence, product designs, international law, Copyright, Trade Secrets, Trademarks, Patents, Design, protection of intellectual property, Protection options – Encryption, copyright on web-content, copyright on software.	

Course Outcomes

Upon successful completion of this course, students will be able to:

1. Classify various cybercrimes, the motivation behind them and the overall global perspective of cybercrime.
2. Differentiate modern cyber-attacks along with the need for digital forensic.
3. Analysis of cyber laws and interpretation.
4. Apply diverse viewpoints to ethical dilemmas in the information technology field and recommend appropriate actions..
5. Ensure the Intellectual property issues in the cyberspace.

List of Books and References

- Sunit Belapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India Pvt. Ltd, 2011.
- Mark F Grady, Fransesco Parisi, "The Law and Economics of Cyber Security", Cambridge University Press, 2006
- Understanding Cybercrime: Phenomena, and Legal Challenges Response, ITU 2012 4. Jonathan Rosenoer, "CyberLaw: The law of the Internet", Springer-Verlag, 1997.

Cyber Forensics and Investigations

Rationale

Digital forensic is needed when cybercrime is reported. It is a process to identify the true reasons behind cybercrime by systematic and scientifically investigation of various collected digital pieces of evidence. Digital forensics refers to the process of collection, acquisition, preservation, analysis, and presentation of electronic evidence for intelligence purposes and/or use in investigations and prosecutions of various forms of crime, including cybercrime.

Course Contents

Contents	**No. of Lectures**
Unit I **Introduction to Cyber Forensics:** Definition of cyber forensics and its importance in the digital age; Principles of forensics: Integrity, reliability, and admissibility; Chain of custody and its role in preserving evidence; Types of digital evidence (files, logs, network traffic, etc.).	8
Unit II **Data Acquisition:** Methods of data acquisition: Imaging and cloning techniques; Preservation of evidence to avoid data tampering; Tools for data acquisition: Disk and memory acquisition.	8
Unit III **Analysis Techniques:** File recovery techniques: Identifying and restoring deleted files; Log analysis: Detecting suspicious activities from system logs; Memory forensics: Analyzing volatile data from RAM for traces of malicious activity.	8
Unit IV **Tools for Cyber Forensics:** Overview of popular forensic tools: FTK (Forensic Toolkit), Autopsy, EnCase; Tool functionalities: Data imaging, analysis, reporting; Practical applications of these tools in investigations.	8
Unit V **Legal and Ethical Aspects:** Legal admissibility of digital evidence in courts; Understanding of cybercrime laws and regulations; Ethical concerns in cyber forensics; Case studies of real-world cybercrime investigations.	8

Suggested List of Lab Experiments

1. Simulate a mock crime scene involving digital evidence.
2. Create an investigative plan for handling the simulated crime scene.
3. Write a detailed investigative report based on the findings.
4. Practice data acquisition techniques using various tools such as FTK
5. Imager, EnCase, or dd command in Linux.
6. Capture and analyze volatile evidence from a running system.
7. Set up a network capture environment using Wireshark and analyze captured traffic.
8. Perform forensic analysis on a Windows system using tools like Autopsy or Sleuth Kit.
9. Analyze artifacts specific to DOS systems and recover relevant evidence.
10. Explore Windows registry forensics and its significance in investigations

Course Outcomes

Upon successful completion of this course, students will be able to:

1. Understand the process of collecting, preserving, and analyzing digital evidence in a forensically sound manner.
2. Apply various forensic tools to perform cyber investigations, including the recovery of data and the analysis of system logs and memory.
3. Evaluate and interpret forensic evidence in line with the relevant legal and ethical standards.
4. Understand the chain of custody and its significance in maintaining the integrity of evidence.
5. Assess the legal admissibility of digital evidence and apply cybercrime laws in the context of forensic investigations.

List of Books and References

- Murugan, S. (2018). Cyber Forensics. Canada: Oxford University Press.
- Marcella Jr., A., Menendez, D. (2010). Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition. United States: CRC Press.
- Wiles, J., Reyes, A. (2011). The Best Damn Cybercrime and Digital Forensics Book Period. United Kingdom: Syngress.
- Critical Concepts, Standards, and Techniques in Cyber Forensics. (2019). United States: IGI Global.
- Britz, M. (2013). Computer Forensics and Cyber Crime: An Introduction. Netherlands: Pearson.

Cryptography in Cybersecurity

Rationale

This course introduces students to the fundamental principles and techniques of cryptography, which are essential for securing data and communication systems. It covers both symmetric and asymmetric encryption algorithms, key exchange protocols, hash functions, and cryptographic applications. Students will learn how to use these techniques in real-world security applications like digital signatures, secure emails, and Public Key Infrastructure (PKI). The course is designed to provide students with the theoretical understanding and practical skills to apply cryptographic methods to protect information.

Course Contents

Contents	**No. of Lectures**
Unit I **Basics of Cryptography:** Definition of Cryptography, Importance in Cyber Security; Basic cryptographic goals: Confidentiality, Integrity, Authentication, Non-repudiation; Overview of symmetric and asymmetric encryption techniques.	8
Unit II **Symmetric Key Algorithms:** Detailed study of Data Encryption Standard (DES), Advanced Encryption Standard (AES); Modes of Operation in block ciphers: ECB, CBC, CFB, OFB, CTR. Differences between symmetric encryption and asymmetric encryption.	8
Unit III **Asymmetric Key Algorithms:** RSA algorithm (Key generation, encryption, decryption); Diffie-Hellman Key Exchange (Theory and application); Digital signatures and their significance in data integrity and authentication.	8
Unit IV **Hash Functions:** Hashing concepts: MD5, SHA-1, SHA-256; Properties of hash functions: Collision resistance, Pre-image resistance; Application of hash functions in Digital Signatures and data verification.	8
Unit V **Cryptographic Applications:** Use of cryptography in	8

securing communications: Secure Email (PGP, S/MIME); Role of Digital Certificates, Public Key Infrastructure (PKI) in authenticating communications and ensuring data integrity.	

Suggested List of Lab Experiments

1. To explain and apply a substitution algorithm for encryption of a plain text message.
2. To explain and apply a transposition technique for encryption of a plain text message.
3. To apply the Data Encryption Algorithm (DES) for encryption of plain text.
4. To apply the Advance Encryption standard (AES) for encryption of plain text.
5. To analyze the working of MD5 for data integrity.
6. To analyze the Hashing algorithm SHA for data authenticity.
7. To analyze the following attacks in a simulated environment.
   (a) Brute Force attack
   (b) Dictionary attack
8. Evaluation of signature validation in a simulated environment.
9. Analysis of Network Vulnerability by cracking SHA.
10. Analysis of Network Vulnerability by cracking MD5.

Course Outcomes

Upon successful completion of this course, students will be able to:

1. Understand the foundational principles of cryptography and its significance in cyber security.
2. Analyze and compare symmetric and asymmetric encryption algorithms, identifying their strengths and weaknesses.
3. Implement and apply cryptographic techniques such as AES, RSA, and Diffie-Hellman to secure data and communications.
4. Understand and apply hash functions like MD5, SHA-1, and SHA-256 in securing data integrity and generating digital signatures.
5. Apply cryptographic methods to real-world applications, including secure email communication, digital certificates, and PKI.

List of Books and References

- Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. United Kingdom: Pearson Education.
- Menezes, A. J., van Oorschot, P. C., Vanstone, S. A. (2018). Handbook of Applied Cryptography. United States: CRC Press.
- Cryptography and Network Security. (2016). India: Pearson Education India.
- Cryptography and Network Security. (2012). Krishna Prakashan.
- Paar, C., Pelzl, J. (2009). Understanding Cryptography: A Textbook for Students and Practitioners. Germany: Springer Berlin Heidelberg.
- Stinson, D. R., Paterson, M. (2018). Cryptography: Theory and Practice. United Kingdom: CRC Press.
- Stinson, D. R., Paterson, M. (2018). Cryptography: Theory and Practice. United Kingdom: CRC Press.

Artificial Intelligence in Cyber Security

Rationale

Learners should be made aware of artificial intelligence-based methods for problem-solving. They will also be able to understand different cybersecurity threats. Artificial Intelligence-based methods for detecting and preventing cybersecurity threats is the main objective of this course.

Course Contents

Contents	**No. of Lectures**
Unit I Artificial Intelligence Core Concepts and Tools Evolution of AI: from expert systems to data mining, Types of machine learning, Algorithm training and optimization, AI in the context of cyber security, Setting up AI for cyber security arsenal, Python for AI and cyber security	8
Unit II Detecting Cyber Security Threats with AI Detecting spam with perceptron, Spam detection with SVMs, Phishing detection with logistic regression and decision trees, Spam detection with Naïve Bayes.	8
Unit III Protecting Sensitive Information and Assets Authentication abuse prevention, account reputation scoring, User authentication with keystroke recognition, Biometric authentication with facial recognition, introducing fraud detection algorithm, Predictive analytics for credit card fraud detection, Evaluating the quality of predictions	8
Unit IV Evaluating and Testing AI Arsenal Best practising for featuring engineering, evaluating a detector's performance with ROC, using cross-validation for algorithms, Evading ML detectors, Challenging 10 25 Wef-AY-2021-22 ML anomaly detection, Testing for data and model quality, Ensuring securing and reliability	8
Unit V Malware analysis at glance, Decision tree malware detectors, detecting metamorphic malware with HMMs, Advanced malware detection with deep learning, Network Anomaly	8

detection techniques, Network attack classification, Detecting botnet topology, Different ML algorithms for botnet detection	

Course Outcomes

Upon successful completion of this course, students will be able to:

1. Understand the core concepts and practical aspects of artificial intelligence in the context of cyber security..
2. Apply the artificial intelligence-based methods for detecting cyber security threats.
3. Apply the artificial intelligence-based methods for providing secure authentication mechanisms.
4. Analyse the artificial intelligence-based detection and prevention methods for cyber security.
5. Evaluate the performance of artificial intelligence-based cyber security methods.

List of Books and References

- Machine Learning and Security by Clarence Chio and David Freeman, O'Reilly Media, Inc., ISBN: 9781491979907, February 2018.
- 2. AI in Cybersecurity by Leslie F. Sikos Springer International Publishing
- 3. Artificial Intelligence For Cyber Security Methods Issues And Possible Horizons Or Opportunities by Misra S.

Malware Analysis

Rationale

The course will focus on the fundamentals of malware and set up a protected static and dynamic malware analysis environment. • The course will focus on the learning of various malware behaviour monitoring tools and actionable detection signatures from malware indicators. • The course will focus on learning how to track malware into exhibiting behaviour that only occurs under special conditions.

Course Contents

Contents	**No. of Lectures**
Unit I Introduction to malware, OS security concepts, Malware threats, Evolution of malware, Malware types, Malware analysis types.	8
Unit II Virtual Machines and Emulators, Benefits of virtualization, Oracle Virtual Box, VMware Player, Virtual PC, Open-source Alternatives: Bochs, QEMU, KVM.	8
Unit III Static Analysis: X86 Architecture- Main Memory, Instructions, Opcodes and Endian-ness, Operands, Registers, Simple Instructions, Stack, Conditionals, Branching, Rep Instructions, C Main Method and Offsets, Anti-virus Scanning, Fingerprint for Malware, Portable Executable File Format, The PE File Headers and Sections.	8
Unit IV Dynamic Analysis: Live Mal-ware analysis, dead Malware analysis, analyzing traces of Malware System-calls, API-calls, registries, network activities. Antidynamic analysis techniques: anti-vm, runtime-evasion techniques, Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark,	8
Unit V Malware Detection Techniques: Signature-based techniques:	8

Malware signatures, packed Malware signature, metamorphic and polymorphic Malware signature non signature-based techniques: similarity-based techniques, machine learning methods, invariant inferences.	

Course Outcomes

Upon successful completion of this course, students will be able to:

1. Understand the concept of the nature of malware, its capabilities and concepts of the virtual environment of the operating system.
2. Apply the tools and methodologies used to perform static and dynamic analysis on the unknown executable.
3. Execute techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples.
4. Analyze how malware interacts with any associated networks or devices, identifying the type of information being targeted.
5. Monitor the Indicators of Compromise (IoCs) from malware samples to aid in threat intelligence efforts.

List of Books and References

- Practical malware analysis The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig ISBN-10: 159327-290-1, ISBN-13: 978-1-59327-290-6, 2012
- "Anti-Hacker Tool kit" by Mike Shema, Mcgraw Hill Education (India) Fourth Edition, 2014
- "Hacking: The Art of Exploitation, 2nd Edition" by Jon Erickson.
- "The IDA PRO Book: The Unofficial Guide to the World's Most Popular Disassembler, 2nd Edition" by Chris Eagle (published by No Starch Press, 2011).
- "The GHIDRA Book: The Definitive Guide" by Chris Eagle and Kara Nance (Penguin Random House Publisher Services, 2020)
- Computer viruses: from theory to applications by Filiol, Eric Springer Science & Business Media, 2006
- Android Malware by Xuxian Jiang and Yajin Zhou, Springer ISBN 978-1-4614-7393-0, 2005
- Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by Michael Davis, Sean Bodmer, Aaron Lemasters, McGraw-Hill, ISBN: 978-0-07-159119-5, 2010
- Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2015

****