COURSE STRUCTURE AND DETAILED SYLLABUS

M.Tech (Cyber Security)

For

Two Year PG Course

(Applicable for batches admitted from 2016)

UNIVERSITY COLLEGE OF ENGINEERING KAKINADA (A)
JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY KAKINADA
KAKINADA - 533 003, Andhra Pradesh, India

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY COLLEGE OF ENGINEERING (A): JNTU KAKINADA

COURSE STRUCTURE

M.Tech. -CYBER SECURITY - I -SEMESTER

S.NO	SUBJECT	L	P	C
1	APPLIED CRYPTOGRAPHY	4	—	3
2	OPERATING SYSTEMS: ADMINISTRATION AND SECURITY	4	—	3
3	INFORMATION SECURITY MANAGEMENT	4	—	3
4	TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL	4	—	3
5	**ELECTIVE 1** BIOMETRIC SECURITY WEB SECURITY SOFTWARE VULNERABILITY ANALYSIS	4	—	3
6	CRYPTOGRAPHY AND SECURITY LAB		3	2
7	INFORMATION SECURITY MANAGEMENT LAB	—	3	2
8	**MINI PROJECT -1**			1
	TOTAL			20

M.Tech. -CYBER SECURITY – II- SEMESTER

S.NO	SUBJECT	L	P	C
1	PRINCIPLES OF SECURE CODING	4	—	3
2	CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS	4	—	3
3	CLOUD ARCHITECTURES AND SECURITY	4	—	3
4	ETHICAL HACKING	4	—	3
5	**ELECTIVE 2** PENETRATION TESTING AND VULNERABILITY ASSESSMENT. CYBER LAWS AND SECURITY POLICIES MALWARE ANALYSIS	4	—	3
6	DIGITAL FORENSICS LAB		3	2
7	ETHICAL HACHING LAB	—	3	2
8	**MINI PROJECT - 2**			1
	TOTAL			20

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY COLLEGE OF ENGINEERING (A): JNTU KAKINADA

COURSE STRUCTURE

III —SEMESTER

S.NO	SUBJECT	L	P	C
1	COMPREHENSIVE VIVA	—	—	**2**
2	SEMINAR-I	—	—	**2**
3	THESIS WORK PART – I	—	—	**16**
	TOTAL			**20**

IV— SEMESTER

S.NO	SUBJECT	L	P	C
1	SEMINAR-II	—	—	**2**
2	THESIS WORK PART – II	—	—	**18**
	TOTAL			**20**

IMPORTANCE OF CYBER SECURITY PROGRAMME

The technological growth, the internet, and availability and sharing of information have tremendously increased information threats to organizations and individuals making it a challenge for users and system administrators to preserve security. Due to the requirement of sophisticated knowledge and tools to keep systems secure, there is a big need in India and around the world for information security professionals who are well educated about the various aspects of information security.

The main **objective** of this programme is to create security professionals who will be handling the real-life problems and challenges the industry is facing today in connection to cyber security.

- This program prepares students to head teams of technologists who are responsible for information security assessments, architectures, operations, monitoring, auditing, and lead information security programs.
- The programme is designed to take students through the wider aspects of security threats, challenges and associated strategies for solving such problems.
- Three verticals that have been identified for specialization are the following – threat intelligence, application security and security analytics.
- During the programme, students are exposed to various tools for secure communications, analytics and threat management.
- The two-year curriculum is aligned with the demand of the industry.
- The unique design of the Programme focuses on providing a high degree of industry exposure, by academic and functional experts from the industry in this domain.
- This programme offers a brilliant career pathway to those who are passionate about knowing more about security challenges and solutions as well as practicing cyber security, security analytics and related tools and technologies.

Eligibility: The course is beneficial for experienced professionals with bachelor's degrees in Information technology, computer science, and information systems. If they already hold a major security certification, then it can provide knowledge to move more quickly through the required subject area assessments.

Employability: According to NASSCOM Cyber Security Task Force, India has a great opportunity to create a workforce of one million cyber security professionals to provide security solutions and services to clients in India and abroad by 2020. The world faces a projected shortfall of 1.5 million Cyber Security experts today.

Employment Areas: Government Departments, Colleges & Universities, Financial Service Institutions, Local Authorities, Security Consultancy Services, IT Companies

Cyber Security Job Types: Senior Security Administrator, Information Systems Security Manager, Senior Security Analyst, Information Systems Security Officer, Information Security Manager, Chief Information Security Officer

M Tech I Sem – R17

APPLIED CRYPTOGRAPHY

Course Outcomes:

By the end of the course students will

- Know the methods of conventional encryption.
- Understand the concepts of public key encryption and number theory
- Understand various applications of cryptography and security issues practically.

SYLLABUS:

UNIT I:

Foundations – Protocol Building Blocks - Basic Protocols - Intermediate Protocols - Advanced Protocols -Zero-Knowledge Proofs - Zero-Knowledge Proofs of Identity -Blind Signatures - Identity-Based Public-Key Cryptography - Oblivious Transfer - Oblivious Signatures - Esoteric Protocols

UNIT II:

Key Length - Key Management - Electronic Codebook Mode - Block Replay - Cipher Block Chaining Mode - Stream Ciphers - Self-Synchronizing Stream Ciphers - Cipher-Feedback Mode – Synchronous Stream Ciphers - Output-Feedback Mode - Counter Mode - Choosing a Cipher Mode - Interleaving -Block Ciphers versus Stream Ciphers - Choosing an Algorithm - Public Key Cryptography versus Symmetric Cryptography - Encrypting Communications Channels - Encrypting Data for Storage - Hardware Encryption versus Software Encryption - Compression, Encoding, and Encryption – Detecting Encryption – Hiding and Destroying Information.

UNIT III:

Information Theory - Complexity Theory - Number Theory - Factoring - Prime Number Generation - Discrete Logarithms in a Finite Field - Data Encryption Standard (DES) – Lucifer -Madryga - NewDES -GOST – 3 Way – Crab – RC5 - Double Encryption - Triple Encryption - CDMF Key Shortening - Whitening.

UNIT IV:

Pseudo-Random-Sequence Generators and Stream Ciphers – RC4 - SEAL - Feedback with Carry Shift Registers - Stream Ciphers Using FCSRs - Nonlinear-Feedback Shift Registers - System-Theoretic Approach to Stream-Cipher Design - Complexity-Theoretic Approach to Stream-Cipher Design - N- Hash- MD4 - MD5 - MD2 - Secure Hash Algorithm (SHA) - One Way Hash Functions Using Symmetric Block Algorithms - Using Public-Key Algorithms - Message Authentication Codes

UNIT V:

RSA - Pohlig-Hellman - McEliece - Elliptic Curve Cryptosystems -Digital Signature Algorithm (DSA) - Gost Digital Signature Algorithm - Discrete Logarithm Signature Schemes - Ongchnorr-Shamir – CellularAutomata - Feige-Fiat-Shamir -Guillou-Quisquater - Diffie-Hellman - Station-to-Station Protocol -ShamirsThree-Pass Protocol - IBM Secret-Key Management Protocol - MITRENET - Kerberos - IBM Common Cryptographic Architecture. (subject may be taught with implementation through JAVA)

REFERENCES:

1. Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C" John Wiley &Sons, Inc, 2nd Edition, 1996.
2. Wenbo Mao, "Modern Cryptography Theory and Practice", Pearson Education, 2004
3. Atul Kahate, "Cryptography and Network Security", Tata McGrew Hill, 2003.
4. William Stallings, "Cryptography and Network Security, Prentice Hall, New Delhi, 2006.
5. Bernard Menezes, "Network Security and Cryptography", Cengage Learning, New Delhi, 2010.

M Tech I Sem – R17

OPERATING SYSTEMS: ADMINISTRATION AND SECURITY

Course Outcomes:

By the end of the course students will

- Become knowledgeable in the concepts of various functions of operating systems.
- Gain hands-on experience in the basic administration of a Linux system.
- Understand the concepts of securing operating systems.

SYLLABUS:

UNIT I - INTRODUCTION TO COMPUTER ARCHITECTURE AND OPERATING SYSTEMS:

Introduction- Computer system Organization and Architecture- Operating System structure and operations- Protection and Security- Process Management- Process Scheduling – Inter process communication- Multi threading models Memory Management: Swapping, Segmentation, Page replacement algorithms- File Systems: File system mounting and sharing, File system implementation and allocation methods- Device management: Disk structure, scheduling and management, I/O hardware and kernel I/O subsystem.- Semaphores- Deadlocks- Mutexes- Critical Section problem. (basics of all these topics to be covered)

UNIT II – SYSTEM ADMINISTRATION:

Standard "best practices" for system administration: documentation, backup and restore, logging automating repetitive tasks using scripting, conservative, incremental change, use of policy in network administration

Administering Windows operating systems: basic issues: overview: comparison between Windows systems, file system model, basic security model: accounts, permissions, support for TCP/IP, support utilities for system administration: net commands; ipconfig; arp, backup

UNIT III - LINUX ADMINISTRATION AND OTHER SERVICES:

Open source operating system- Linux Kernel architecture- User administration in Linux- Services offered by Linux OS- Configuration of email service, web service, NFS, DNS in Linux- Syntactical Interpretation of various files related to different services in Linux.

UNIT IV - TRUST IN SECURE OPERATING SYSTEMS:

Secure operating systems- Security goals- Trust model- Threat model- Access Control fundamentals: Lampson"s access matrix, mandatory protection systems, Reference monitor- Secure operating system definition- Assessment criteria

UNIT V - OPERATING SYSTEM SECURITY:

Security in Windows and Unix: Protection system, authorization, security analysis and vulnerabilities-The security kernel- Secure communications processor – Retrofitting security into operating systems

REFERENCES:

1. Abraham Silberschatz, Peter Baer Galvin and Greg Gagne, "Operating System Concepts", John Wiley & Sons , Inc., 9th Edition, 2012.

2. William Stallings, “Operating System: Internals and Design Principles”, Prentice Hall, 7th Edition,2012.
3. Tom Adelstein and Bill Lubanovic, “Linux System Administration”, O'Reilly Media, Inc., 1st Edition, 2007.
4. Trent Jaeger, “Operating Systems Security”, Morgan & Claypool Publishers, 2008.
5. Michael J.Palmer, “Guide to Operating Systems Security”, Thomson/Course Technology, 2004.
6. The Practice of System and Network Administration (2nd Ed.), Thomas A. Limoncelli, Christina J. Hogan, and Strata R. Chalup, Addison-Wesley, 2007, ISBN 0-321-49266-8.
7. Frisch, A., Essential System Administration, 2nd Edition, c. 1995, O’Reilly Ivens, K,. Managing Windows NT Logons, c. 2000, O’Reilly
8. Leber, J., Windows NT Backup and Restore, c. 1999, O’Reilly
9. Lowe-Norris, A., Windows 2000 Active Directory, c. 2000, O’Reilly
10. Meggitt, A., and Ritchey, T., Windows NT User Administration, c. 1997, O’Reilly
11. UNIX and Linux System Administration Handbook (4th Ed.), Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, Prentice Hall, 2011, ISBN-10: 0-13-148005-7.
12. Linux Administration A Beginners Guide (6th Ed.), Wale Soyinka, McGraw Hill, 2012, ISBN-10: 0-07-176758-4
13. Essential System Administration (3rd Ed.), A. Frisch, O'Reilly, 2002, ISBN-10: 0-596-00343-9
14. Microsoft Windows Server Administration Essentials, Tom Carpenter, Sybex, 2011, ISBN-10: 1- 11-801686-6

M Tech I Sem – R17

INFORMATION SECURITY MANAGEMENT

Course Outcomes:

By the end of the course students will

- Know principles of applied information security management
- Understand of security management in medium to large organizations.

SYLLABUS:

UNIT I :

Information Security Management : Information Security Overview, Threats and Attack Vectors, Types of Attacks, Common Vulnerabilities and Exposures (CVE), Network Security Attacks, Fundamentals of Information Security, Computer Security Concerns, Information Security Measures

UNIT II :

Fundamentals of Information Security: Key Elements of Networks, Logical Elements of Network, Critical Information Characteristics, Information States

UNIT III :

Data Leakage: What is Data Leakage, Statistics, Data Leakage Threats, Reducing the risk of data loss, Key Performance Indicators (KPI), Database Security etc.,

UNIT IV :

Information Security Policies, Procedures and Audits: Information Security Policies: - Necessity - Key Elements – Characteristics, Security Policy Implementation, Configuration, Security Standards, Security Guidelines and Frameworks etc.,

UNIT V :

Information Security Management - Roles & Responsibilities: Security Roles and Responsibilities, Accountability, Roles and Responsibility of Information Security Management, Team responding to emergency situation, Risk Analysis Process

REFERENCES:

1. Andy Taylor(ed.) ; David Alexander; Amanda Finch; David Sutton; Andy Taylor, "Information Security Management Principles", BCS Learning & Development Limited; June 2013

* Additional resources NASSCOM

M Tech I Sem – R17

TRANMISSION CONTROL PROTOCOL/INTERNET PROTOCOL

Course Outcomes:

By the end of the course students will

- Learn about the protocols which are using in the current scenario.
- Learn client server relations and OSI programming Implementation of the socket and IPC.

SYLLABUS:

UNIT I:

Introduction to Networks: OSI model, Unix standards, TCP and UDP & TCP connection establishment and Format, Buffer sizes and limitation, standard internet services, Protocol usage by common internet application Real time apps, High speed networks-types of N/W's, Switching & Routing

UNIT II:

TCP client server: Introduction, TCP Echo server functions, Normal startup, terminate and signal handling server process termination, Crashing and Rebooting of server host shutdown of server host.

UNIT III:

Sockets: Address structures, value – result arguments, Byte ordering and manipulation function and related functions Elementary TCP sockets – Socket, connect, bind, listen, accept, fork and exec function, concurrent servers. Close function and related function.

I/O Multiplexing and socket options: I/O Models, select function, Batch input, shutdown function, poll function, TCP Echo server, getsockopt and setsockopt functions. Socket states, Generic socket option IPV6 socket option ICMPV6 socket option IPV6 socket option and TCP socket options.

UNIT IV:

Elementary UDP sockets: Introduction UDP Echo server function, lost datagram, summary of UDP example, Lack of flow control with UDP, determining outgoing interface with UDP.

Elementary name and Address conversions: DNS, gethost by Name function, Resolver option, Function and IPV6 support, uname function, other networking information.

UNIT V:

IPC : Introduction, File and record locking, Pipes, FIFOs streams and messages, Name spaces, system IPC, Message queues, Semaphores. **Remote Login:** Terminal line disciplines, Pseudo-Terminals, Terminal modes, Control Terminals, rlogin Overview, RPC Transparency Issues.

TEXTBOOKS:

1. UNIX Network Programming, Vol. I, SocketsAPI, 2nd Edition. - W.Richard Stevens, Pearson Edn. Asia.
2. UNIX Network Programming, 1st Edition, - W.Richard Stevens. PHI.

REFERENCES:

1. UNIX Systems Programming using C++ T CHAN, PHI.
2. UNIX for Programmers and Users, 3rd Edition Graham GLASS, King abls, Pearson Education
3. Advanced UNIX Programming 2nd Edition M. J. ROCHKIND, Pearson Education

M Tech I Sem – R17

BIOMETRIC SECURITY

Course Outcomes:

By the end of the course students will

- Demonstrate knowledge of the basic physical and biological science and engineering principles underlying biometric systems.
- Understand and analyze biometric systems at the component level and be able to analyze and design basic biometric system applications.
- Be able to work effectively in teams and express their work and ideas orally and in writing.
- Identify the sociological and acceptance issues associated with the design and implementation of biometric systems.
- Understand various Biometric security issues.

SYLLABUS:

UNIT I:

Biometrics- Introduction- benefits of biometrics over traditional authentication systems - benefits of biometrics in identification systems-selecting a biometric for a system – Applications - Key biometric terms and processes - biometric matching methods -Accuracy in biometric systems.

UNIT II:

Physiological Biometric Technologies: Fingerprints - Technical description –characteristics - Competing technologies - strengths – weaknesses – deployment - Facial scan - Technical description - characteristics - weaknesses-deployment - Iris scan - Technical description – characteristics - strengths – weaknesses – deployment - Retina vascular pattern

UNIT III:

Technical description – characteristics - strengths – weaknesses –deployment - Hand scan - Technical description-characteristics - strengths – weaknesses deployment – DNA biometrics. Behavioral Biometric Technologies: Handprint Biometrics - DNA Biometrics.

UNIT IV:

signature and handwriting technology - Technical description – classification – keyboard / keystroke dynamics- Voice – data acquisition - feature extraction - characteristics - strengths – weaknesses-deployment.

UNIT V:

Multi biometrics and multi factor biometrics - two-factor authentication with passwords - tickets and tokens – executive decision - implementation plan.

TEXT BOOKS:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi : “Biometrics -Identity verification in a network”, 1st Edition, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul : “Implementing Biometric Security”, 1st Edition, Wiley Eastern Publication, 2005.

REFERENCES:

1. John Berger: "Biometrics for Network Security", 1st Edition, Prentice Hall, 2004.
2. Jain, Anil K.; Flynn, Patrick; Ross, Arun A. (Eds.), Handbook of Biometrics, Springer, 2008.
3. Benjamin Muller, Security, Risk and the Biometric State: Governing Borders and Bodies, 1st Edition, Routledge, 2010.

M Tech I Sem – R17

WEB SECURITY

Course Outcomes:

By the end of the course students will

- Understand about Web languages, different attacks on Web
- Understand different Cryptography methods and RSA
- Understand about web interfaces and different web application process.

SYLLABUS:

UNIT I:

Introduction- A web security forensic lesson, Web languages, Introduction to different web attacks. Overview of N-tier web applications, Web Servers: Apache, IIS, Database Servers.

UNIT II:

Review of computer security, Public Key cryptography, RSA. Review of Cryptography Basics, On-line Shopping, Payment Gateways

UNIT III:

Web Hacking Basics HTTP & HTTPS URL, Web Under the Cover Overview of Java security Reading the HTML source, Applet Security Servlets Security Symmetric and Asymmetric Encryptions, Network security Basics, Firewalls & IDS

UNIT IV:

Digital Certificates, Hashing, Message Digest, & Digital Signatures

UNIT V:

Basics, Securing databases, Secure JDBC, Securing Large Applications, Cyber Graffiti

TEXT BOOKS:

1. McClure, Stuart, Saumil Shah, and Shreeraj Shah. Web Hacking:attacks and defense. AddisonWesley. 2003.
2. Garms, Jess and Daniel Somerfield. Professional Java Security. Wrox. 2001.

REFERENCES:

1. Collection of Cryptography Web Sites, Publications, FAQs, and References: http://world.std.com/~franl/crypto.html
2. FAQ: What is TLS/SSL? http://www.mail.nih.gov/user/faq/tlsssl.htm
3. The Open SSL Project (SDKs for free download): http://www.openssl.org/
4. Windows & .NET security updates Web site: http://www.ntsecurity.net/

M Tech I Sem – R17

SOFTWARE VULNERABILITY ANALYSIS

Course Outcomes:

By the end of the course students will

- Understand the software vulnerabilities in the real software world.
- Understand different application level security
- Understand the malicious code actions and different protection techniques.

SYLLABUS:

UNIT-I:

Introduction to security & Authentication: Software Security **-** Dealing with Widespread Security Failures, Bugtraq, CERT Advisories, RISKS Digest, Technical Trends Affecting Software Security, the ilities, Beyond Reliability, Penetrate and Patch, On Art and Engineering, Security Goals, Prevention, Traceability and Auditing, Monitoring, Privacy and Confidentiality, Multilevel Security, Anonymity, Authentication, Integrity, Know Your Enemy – Common Software Security Pitfalls. Software Project Goals.

UNIT-II:

Application Security & Malicious Code: Managing Software Security Risk: An Overview Of Software Risk Management For Security, The Role Of Security Personnel, Software Security Personnel in the Life Cycle, Deriving Requirements, Risk Assessment, Design For Security, Implementation and Testing, ADose of Reality, Getting People To Think About Security, Software Risk Management In Practice, When Development Goes Astray, Code Review (Tools) - Architectural Risk Analysis - Penetration Testing -Risk-Based Security Testing - Abuse Cases - Security Requirements - Security Operations

UNIT-III:

Access Control & Physical Protection: The UNIX Access Control Model, Working of UNIX Permissions, Modifying File Attributes, Modifying Ownership, The umask, The Programmatic Interface, Setuid Programming, Access Control In Windows NT, Compartmentalization, Fine-Grained Privileges. Buffer Overflow & Rootkits: Buffer Overflows As Security Problems, Defending Against Buffer Overflow, Major Gotchas, Internal Buffer Overflows, More Input Overflows, Other Risks, Tools for handling buffer overflows, Smashing Heaps And Stacks, Heap Overflows, Stack Overflows, Decoding The Stack, To Infinity … Attack Code, A UNIX Exploit, Windows.

UNIT-IV:

Network Security & Intrusion: Brief Review of OSI Model, Sockets, Socket Functions, Socket Addresses, Network Byte Order, Internet Address Conversion, Simple Server and Web Clients, Tinyweb Server. Peeling Back the Lower Layers - Data-Link Layer - Network Layer-Transport Layer – Network Sniffing -Raw Socket Sniffer - libpcap Sniffer - Decoding the Layers - Active Sniffing - Denial of Service – SYN Flooding - The Ping of Death - Teardrop –

Ping Flooding - Amplification Attacks - Distributed DoS Flooding - TCP/IP Hijacking - RST Hijacking - Continued Hijacking - Port Scanning - Stealth SYN Scan -FIN, X-mas, and Null Scans - Spoofing Decoys - Idle Scanning - Proactive Defense (shroud) - Reach Out and Hack Someone - Analysis with GDB - Almost Only Counts with Hand Grenades - Port-Binding ,Shell code.

UNIT-V:

Counter Measures: Detection of System Daemons, Crash Course in Signals, Tinyweb Daemon, Tools of the Trade, tiny web Exploit Tool, Log Files, Blend In with the Crowd, Overlooking the Obvious, One Stepat a Time, Putting Things Back Together Again, Child Laborers, Advanced Camouflage, Spoofing theLogged IP Address, Log less Exploitation, The Whole Infrastructure, Socket Reuse, Payload Smuggling, String Encoding, How to Hide a Sled, Buffer Restrictions, Polymorphic Printable ASCII Shellcode. Hardening Countermeasures - Non executable Stack, ret2libc,Returning into system(). Randomized Stack Space - Investigations with BASH and GDB, Bouncing Off Linux-gate. Applied Knowledge, First Attempts, Paying the Odds

TEXTBOOKS:

1. John Viega & Gary McGraw: Building Secure Software: How to Avoid Security Problems the Right Way(Addison-Wesley Professional Computing Series) [Paperback]
2. Gary McGraw: Software Security: Building Security In (Addison-Wesley Professional Computing Series)[Paperback]

REFERENCES:

1. Michael Howard, David LeBlanc, John Viega: 19 Deadly Sins of Software Security: ProgrammingFlaws and How to Fix Them (Security One-off) (Addison-Wesley Professional Computing Series)[Paperback]
2. Jon Erickson: Hacking: The Art of Exploitation, 2nd Edition (No Starch Press, San Fransico) [Paperback]
3. Richard Sinn " Software Security , Theory Programming and Practice" Cengage Learning

M Tech I Sem – R17

CRYPTOGRAPHY AND SECURITY LAB

Course Outcomes:

By the end of this lab students will

1. Know the methods of conventional encryption.
2. Understand the concepts of public key encryption and number theory
3. Understand various applications of cryptography and security issues practically.

SYLLABUS:

1. Configure a mail agent to support Digital Certificates, send a mail and verify the correctness of this system using the configured parameters.

2. Configure SSH (Secure Shell) and send/receive a file on this connection to verify the correctness of this system using the configured parameters.

3. Configure a firewall to block the following for 5 minutes and verify the correctness of this system using the configured parameters:
   (a) Two neighborhood IP addresses on your LAN
   (b) All ICMP requests
   (c) All TCP SYN Packets

4. Configure S/MIME and show email-authentication.

5. Implement encryption and decryption with Open SSL.

6. Implement Using IP TABLES on Linux and setting the filtering rules.

7. Working with Sniffers for monitoring network communication (Ethereal)

8. Using IP TABLES on Linux and setting the filtering rules

M Tech I Sem – R17

INFORMATION SECURITY MANAGEMENT LAB

Course Outcomes:

By the end of this lab students will

- Get the knowledge about audit and information security management,
- Get the real world experience

SYLLABUS:

1. Audit security policy implementation in windows environment
2. Create a Demilitarized zone creation in Network environment for information security
3. Implement Resource harvesting attack and mitigation
4. Implement Window Patch management policy
5. Knowing the Behavior of Trojans and mitigation strategies
6. Create a metasploit and make it to implement.
7. Access control list creation and content filtering limiting the traffic.
8. Data leakage in a website database and preventive measures.
9. Password policy implementations and verification.
10. Patch management implementation using MBSA tool on windows machine.
11. Audit Policy management for users and computers log analysis.
12. Media handling policy implementation and event log analysis.
13. Installation of Trojan and study of different options.
14. Network DOS attack and proof of bandwidth utilization and preventive steps.

M Tech II Sem – R17

PRINCIPLES OF SECURE CODING

Course Outcomes:

By the end of the course students will

- Understand the need for secure coding and proactive development process
- Learn secure coding practices
- Learn input issues related to database and web
- Understand the fundamental principles of software security engineering

SYLLABUS:

UNIT I – INTRODUCTION:

Need for secure systems- Proactive security development process- Security principles to live by and threat modeling.

UNIT II - SECURE CODING IN C:

Character strings- String manipulation errors – String Vulnerabilities and exploits – Mitigation strategies for strings- Pointers – Mitigation strategies in pointer based vulnerabilities – Buffer Overflow based vulnerabilities.

UNIT III - SECURE CODING IN C++ AND JAVA:

Dynamic memory management- Common errors in dynamic memory management- Memory managers-Double –free vulnerabilities –Integer security- Mitigation strategies.

UNIT IV - DATABASE AND WEB SPECIFIC INPUT ISSUES:

Quoting the Input – Use of stored procedures- Building SQL statements securely- XSS related attacks and remedies.

UNIT V – SOFTWARE SECURITY ENGINEERING:

Requirements engineering for secure software: Misuse and abuse cases- SQUARE process model-Software security practices and knowledge for architecture and design.

REFERENCES:

1. Michael Howard , David LeBlanc, “Writing Secure Code”, Microsoft Press, 2nd Edition, 2003.
2. Robert C.Seacord, “ Secure Coding in C and C++”, Pearson Education, 2nd edition, 2013.
3. Julia H. Allen, Sean J. Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, “Software Security Engineering : A guide for Project Managers”, Addison-Wesley Professional, 2008.

M Tech II Sem – R17

CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS

Course Outcomes:

By the end of the course students will

- Understand different crimes that are happening through the cyber world
- Understand the digital forensic tools and different digital techniques in the cyber digital world

SYLLABUS:

UNIT I:

INTRODUCTION: Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime,

Types of Cyber Crime: Social Engineering, Categories of Cyber Crime, Property Cyber Crime.

UNIT II:

CYBER CRIME ISSUES: Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses.

UNIT III:

INVESTIGATION: Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

UNIT IV:

DIGITAL FORENSICS: Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics.

UNIT V:

LAWS AND ACTS: Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies.

REFERENCES:

1. Nelson Phillips and Enfinger Steuart, “Computer Forensics and Investigations”, Cengage Learning,New Delhi, 2009.
2. Kevin Mandia, Chris Prosise, Matt Pepe, “Incident Response and Computer Forensics “, TataMcGraw -Hill, New Delhi, 2006.
3. Robert M Slade,” Software Forensics”, Tata McGraw - Hill, New Delhi, 2005.
4. Bernadette H Schell, Clemens Martin, “Cybercrime”, ABC – CLIO Inc, California, 2004.
5. ”Understanding Forensics in IT “, NIIT Ltd, 2005.

M Tech II Sem – R17

CLOUD ARCHITECTURES AND SECURITY

Course Outcomes:

By the end of the course students will

1. Understand the fundamentals of cloud computing.
2. Understand the requirements for an application to be deployed in a cloud.
3. Become knowledgeable in the methods to secure cloud.

SYLLABUS:

UNIT I- CLOUD COMPUTING FUNDAMENTALS:

Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public (vs) private clouds, role of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture.

UNIT II - CLOUD APPLICATIONS:

Technologies and the processes required when deploying web services-Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages-Development environments for service development; Amazon, Azure, Google App.

UNIT III – SECURING THE CLOUD:

Security Concepts - Confidentiality, privacy, integrity, authentication, nonrepudiation, availability, access control, defense in depth, least privilege- how these concepts apply in the cloud and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud.

UNIT IV – VIRTUALIZATION SECURITY:

Multi-tenancy Issues: Isolation of users/VMs from each other- How the cloud provider can provide this-Virtualization System Security Issues: e.g. ESX and ESXi Security, ESX file system security- storage considerations, backup and recovery- Virtualization System Vulnerabilities.

UNIT V - CLOUD SECURITY MANAGEMENT:

Security management in the cloud – security management standards- SaaS, PaaS, IaaS availability management- access control- Data security and storage in cloud.

REFERENCES:

1. Rajkumar Buyya, Christian Vecchiola, and Thamarai Selvi," Mastering Cloud Computing", International Edition: Morgan Kaufmann, ISBN: 978-0-12-411454-8, Burlington, Massachusetts, USA, May 2013; and Indian Edition: Tata McGraw Hill, ISBN-13: 978-1-25-902995-0, New Delhi, India, Feb 2013."
2. Gautam Shroff, “Enterprise Cloud Computing Technology Architecture Applications”, Cambridge University Press; 1 edition [ISBN: 978- 0521137355], 2010.
3. Toby Velte, Anthony Velte, Robert Elsenpeter, “Cloud Computing, A Practical Approach”, Tata McGraw-Hill Osborne Media; 1 edition 22, [ISBN: 0071626948], 2009.
4. Tim Mather, Subra Kumaraswamy, Shahed Latif, “Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance”, O'Reilly Media; 1 edition, [ISBN: 0596802765], 2009.
5. Ronald L. Krutz, Russell Dean Vines, “Cloud Security”, Wiley [ISBN: 0470589876], 2010.

M Tech I Sem – R17

ETHICAL HACKING

Course Outcomes:

By the end of the course students will

- Learn various hacking methods.
- Perform system security vulnerability testing.
- Perform system vulnerability exploit attacks.
- Produce a security assessment report
- Learn various issues related to hacking.

SYLLABUS:

UNIT I:

Hacking Windows: BIOS Passwords, Windows Login Passwords, Changing Windows Visuals, Cleaning Your Tracks, Internet Explorer Users, Cookies, URL Address Bar, Netscape Communicator, Cookies URL History, The Registry, Baby Sitter Programs.

UNIT II:

Advanced Windows Hacking: Editing your Operating Systems by editing Explorer.exe, The Registry, The Registry Editor, Description of .reg file, Command Line Registry Arguments, Other System Files, Some Windows & DOS Tricks, Customize DOS, Clearing the CMOS without opening your PC, The Untold Windows Tips and Tricks Manual, Exiting Windows the Cool and Quick Way, Ban Shutdowns: A Trick to Play, Disabling Display of Drives in My Computer, Take Over the Screen Saver, Pop a Banner each time Windows Boots, Change the Default Locations, Secure your Desktop Icons and Settings.

UNIT III:

Getting Past the Password: Passwords: An Introduction, Password Cracking, Cracking the Windows Login Password, The Glide Code, Windows Screen Saver Password, XOR, Internet Connection Password, Sam Attacks, Cracking Unix Password Files, HTTP Basic Authentication, BIOS Passwords, Cracking Other Passwords.

UNIT IV:

The Perl Manual: Perl: The Basics, Scalars, Interacting with User by getting Input, Chomp() and Chop(), Operators, Binary Arithmetic Operators, The Exponentiation Operator(**), The Unary Arithmetic Operators, Other General Operators, Conditional Statements, Assignment Operators. The : Operator, Loops, The While Loop, The For Loop, Arrays, THE FOR EACH LOOP: Moving through an Array, Functions Associated with Arrays, Push() and Pop(), Unshift() and Shift(), Splice(), Default Variables, $_, @ARGV, Input Output, Opening Files for Reading, Another Special Variables.

UNIT V:

Virus Working, Boot Sector Viruses (MBR or Master Boot Record), File or Program Viruses, Multipartite Viruses, Stealth Viruses, Polymorphic Viruses, Macro Viruses, Blocking Direct Disk Access, Recognizing Master Boot Record (MBR) Modifications, Identifying Unknown Device Drivers, making own Virus, Macro Viruses, Using Assembly to Create your own Virus, Modifying a Virus so Scan won't Catch it, Creating New Virus Strains, Simple Encryption Methods.

TEXT BOOKS:

1. Patrick Engbreston: "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy",1st Edition, Syngress publication,2011.
2. Ankit Fadia : "Unofficial Guide to Ethical Hacking", 3rd Edition , McMillan India Ltd,2006.

REFERENCES:

1. Simpson/backman/corley, "HandsOn Ethical Hacking & Network Defense International", 2nd Edition,Cengageint,2011.

M Tech II Sem – R17

PENETRATION TESTING AND VULNERABILITY ASSESSMENT

Course Outcomes:

By the end of the course students will

- Identify security vulnerabilities and weaknesses in the target applications.
- Identify how security controls can be improved to prevent hackers gaining access to operating systems and networked environments.
- Able to test and exploit systems using various tools.
- Understand the impact of hacking in real time machines.

SYLLABUS:

UNIT I – INTRODUCTION:

Ethical Hacking terminology- Five stages of hacking- Vulnerability Research- Legal implication of hacking- Impact of hacking.

UNIT II - FOOT PRINTING & SOCIAL ENGINEERING:

Information gathering methodologies- Competitive Intelligence- DNS Enumerations- Social Engineering attacks.

UNIT III - SCANNING & ENUMERATION:

Port Scanning-Network Scanning- Vulnerability Scanning- NMAP scanning tool- OS Fingerprinting-Enumeration.

UNIT IV - SYSTEM HACKING:

Password cracking techniques- Key loggers- Escalating privileges- Hiding Files- Steganography technologies- Countermeasures.

UNIT IV - SNIFFERS & SQL INJECTION:

Active and passive sniffing- ARP Poisoning- Session Hijacking- DNS Spoofing- Conduct SQL Injection attack - Countermeasures.

REFERENCES:

1. Kimberly Graves, “CEH: Official Certified Ethical Hacker Review Guide”, Wiley Publishing Inc., ISBN: 978-0-7821-4437-6, 2007.
2. Shakeel Ali &Tedi Heriyanto, “Backtrack -4: Assuring security by penetration testing”, PACKT Publishing., ISBN: 978-1-849513-94-4, 2011.

M Tech II Sem – R17

CYBER LAWS AND SECURITY POLICIES

Course Outcomes:

By the end of the course students will

- Understand the cyber laws and different security policies
- Understand different ethical responsibilities in the present world
- Understand role of cyber law employ will
- Understand the different organization and human adoption rights

SYLLABUS:

UNIT I:

Introduction to Computer Security: Definition, Threats to security, Government requirements, Information Protection and Access Controls, Computer security efforts, Standards, Computer Security mandates and legislation, Privacy considerations, International security activity.

UNIT II:

Secure System Planning and administration, Introduction to the orange book, Security policy requirements, accountability, assurance and documentation requirements, Network Security, The Redbook and Government network evaluations.

UNIT III:

Information security policies and procedures: Corporate policies- Tier 1, Tier 2 and Tier3 policies - process management-planning and preparation-developing policies-asset classification policy-developing standards.

UNIT IV:

Information security: fundamentals-Employee responsibilities- information classification-Information handling- Tools of information security- Information processing-secure program administration.

UNIT V:

Organizational and Human Security: Adoption of Information Security Management Standards,Human Factors in Security- Role of information security professionals.

REFERENCES:

1. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)", 2ndEdition, OReilly Media, 2006.
2. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004.
3. Kenneth J. Knapp, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", IGI Global, 2009.
4. Thomas R Peltier, Justin Peltier and John blackley, "Information Security Fundamentals", 2ndEdition, Prentice Hall, 1996
5. Jonathan Rosenoer, "Cyber law: the Law of the Internet", Springer-verlag, 1997
6. James Graham, " Cyber Security Essentials" Averbach Publication T & F Group.

M Tech II Sem – R17

MALWARE ANALYSIS

Course Outcomes:

By the end of the course students will

- Understand the purpose of computer infection program.
- Implement the covert channel and mechanisms.
- Be able test and exploit various malware in open source environment.
- Be able to analyze and design the famous virus and worms.

SYLLABUS:

UNIT I - INTRODUCTION

Computer Infection Program- Life cycle of malware- Virus nomenclature- Worm nomenclature- Tools used in computer virology.

UNIT II - IMPLEMENTATIONOF COVERT CHANNEL

Non self-reproducing Malware- Working principle of Trojan Horse- Implementation of Remote access and file transfer- Working principle of Logical Bomb- Case Study: Conflicker C worm.

UNIT III - VIRUS DESIGN AND ITS IMPLICATIONS

Virus components- Function of replicator, concealer and dispatcher- Trigger Mechanisms- Testing virus codes- Case Study: Brute force logical bomb.

UNIT IV - MALWARE DESIGN USING OPEN SOURCE

Computer Virus in Interpreted programming language- Designing Shell bash virus under Linux-Fighting over infection- Anti –antiviral fighting – Polymorphism- Case study: Companion virus.

UNIT V VIRUS AND WORM ANALYSYS

Klez Virus- Clone Virus- Doom Virus- Black wolf worm- Sassar worm- Happy worm 99.

REFERENCES:

1. ErciFiliol, “Computer Viruses: from theory to applications”, Springer, 1st edition, ISBN 10: 2-287-23939-1, 2005.
2. Mark.A .Ludwig, “The Giant black book of computer viruses, Create Space Independent Publishing Platform, 2nd edition, ISBN 10**:** 144140712X, 2009.

M Tech II Sem – R17

DIGITAL FORENSICS LAB

Course Outcomes:
By the end of the course students will Be able to work on different Forensic Tools

SYLLABUS:

Evidence Collection
1. Linux: Capturing RAM dump using fmem
a. https://github.com/NateBrune/fmem
2. Linux: Capturing Disk using ddd
3. Windows: Capture RAM dump of a windows system
a. Hint: FTK Imager or RAMCapture
4. Windows: Capture Disk Image of a windows system
a. Hint: FTK Imager

Disk Analysis
1. List all files in a directory from a disk image
a. FTK Imager
2. Export a particular file from a disk image
a. FTK Imager
3. Recover a deleted file from a disk image
a. FTK Imager

Memory Analysis
1. List all running processes from a memory image
2. List all network connections from a memory image
3. Find out whether a firewall is set by analysing a memory image
Hint: volatility

Live Incident Response
1. Perform live incident response on a system
2. View all browser history in a computer
3. List out all established network connections in a computer
Hint: Triage Incident Response

Stegnography
1.Do analysis on the images
2.Remove the author details and other functions with files

Exploring:
Explore on the below tools
Oxygen Forensic Suite
Cyber Check Suite
FAT32 Format

Explore on web forensics

Forensics Acquisition of Websites

***Analyze on different forensic tools in given tools list .If time permits

*** Make literature survey on all the tools given.

M Tech II Sem – R16

ETHICAL HACKING LAB

Course Outcomes:
By the end of the course students will be able work on Hacking related issues using various software tools/utilities

SYLLABUS:

1. Web Based Email Attacks & Security Working of Email
E-mail Server: E-mail Server Setup ,· Sending mails through Email, Server E-mail Forgery, E-mail Forgery – Fake Mail, Sending fake E-mails Analyzing E-mail Header , Tracing E-mail Defensive-measures Electronic Transaction Security, Using Websites Using Scripts E-mail Bombing Attacking E-mail password .
Introduction to Various Attacks Phishing: Desktop Phishing Cookies Stealing Non-Technical Attacks Social Engineering Shoulder Surfing Investigating an E-mail

2. Windows OS Hacking /Linux
Cracking Windows Login Password – Various Attacks, Password Guessing, Dictionary Attack, Brute-force Attack, Rainbow Table Attack, Creating Backdoors , Bootkits
Hidden User Account in Windows
Bypassing the Login Screen Introduction to Steganography Hiding Files behind an Image Creating File and Folder Locks Defensive measures, Restricting Files & Folders Access, Strong Password Configuration, BIOS Boot Order, BIOS Security Options, Physical Security
Windows Tips & Tricks: Account Privilege Escalation, Browser Hacks, Registry Tweaks Customizing Login Screen, Multiple GTalk & Yahoo Messenger

3. Understanding Malwares Working & Detection
Trojan Working Methods, Direct Connection ,Reverse Connection, Viruses Working, Virus creation
Introduction to Batch Programming, Viruses through Batch Programming Spyware Working
Introduction to Keyloggers, Password Cracking using Keylogger, Types of Keyloggers
Detection & Removal of Malwares: Automatic Process,Using Anti-Malware Software
Manual Process Using TCP View Monitoring Process

4. Networking Attacks & Security Tips & Tricks, Netstat , Tracert, Telnet Firewall & IDS

5. Wi-Fi Attacks & Security
Accessing Wireless Network ,WEP Key Cracking Wireless Attack Methods:
War Driving, War Walking, MAC Address Spoofing, Creating Rouge Wireless Access Point Defensive-measures, MAC Filtering, Configuring Strong Key, Setting up a Proxy Server

6. Web Server Attacks & Security: Web Server Attack Vectors,
Breaking into Database using SQL Injection, Web Ripping, Directory Traversal attack
PHP Remote Code Execution Defensive Measures, Input Validation, Controlling Directory Access · Monitoring of Web Server

7. Hacking Using Google : Google as a Hacking Tool. · Digging Websites Defensive Measures, Restricting Google to Website

8. Software Reverse Engineering Software Assembly Code Analysis Software Disassembling Software Key Phishing Software Patching:
Generating Patch ,Executing the Patch Software Manipulation ,Finding the Decisive Code, Modifying the Software Code Defensive Measures, Encrypting Application, Setup Encrypters

VOIP & Mobile Hacking: Call Forgery, Making Fake Calls SMS Forgery
Sending,Fake SMSs to Any Phone

***Learn all these tools and perform mitigation techniques on all the tools and hack techniques listed above

MINI PROJECT WORK 1

In the project period the student has to undergo the servers and routers so that the student get enriched knowledge in servers which helps him to know the behavior of servers which makes him expert in the servers so that he can easily guess how to hack the server and how to mitigate it.

1. **Network Essentials**

- Networking Concepts, History of Server OS
- Introduction to windows server 2008 & 2012
- Features of Windows Server 2012
- Installation of Windows Server 2012
- Introduction and Creation of Users account RODC & Physical Structure of AD-DS
- Introduction & Configuration of Read-Only Domain Controller
- Sites and Global Catalog
- Replication between the Domain Controllers
- AD-DS Partitions
- Configuring A.D.C using Install From Media [IFM]

2. **Active Directory - Domain Services**

- IP Addressing
- Logical Topologies - Peer-Peer & Domain Models
- Introduction to Directory Services
- Evolution of Active Directory Services - LDAP Protocol
- Features of Active Directory
- Installing Active Directory – Domain Controller
- Dynamic Host Configuration Protocol (DHCP)
- Introduction and Configuration of DHCP Server
- DHCP Client Configuration
- Reservations
- DHCP Backup

3. **Member Servers, Clients, User Configuration**

- Configuring Member Servers and Clients
- Creating Users in AD-DS
- User Logon policies
- Password policies
- Account Lockout policies
- User properties
- Domain Name System (DNS)
- Internet Basics, Host & LM Host Files
- DNS Naming Hierarchy
- Lookup Zones - Forward and Reverse lookup Zones Types of Zones – Primary, Secondary & Stub Zone Resource Records, Integration with ADS, SRV Records Forwarders, Dynamic Updates

4. **Permissions/Access Control Lists**
- File Systems
- Security and Sharing Permissions - Folders & Files
- Access Based Enumeration
- Internet Information Services(IIS)
- IIS 8.0 Configuration
- Hosting Websites, Virtual Directories
- Redirecting Web Sites
- Backup & Restoring Sites
- FTP Sites

5. Profiles and File Server Resource Manager [FSRM]
- Types of Profiles – Local & Roaming
- Home Folder
- Configuring Quotas using FSRM
- Implementing File Screening using FSRM Windows Deployment Services Introduction and Configuration of WDS Server Attended and Unattended Installation

6. Distributed File System
- Creating Organizational Unit
- Delegating Control to a User
- DFS Namespace
- DFS Folders
- Routing & Remote Access
- Routing Configuration - Static Routes
- Dynamic routes (RIP)
- NAT
- Remote Access Server Configuration
- VPN - PPTP

7. Logical Structure of AD - DS
- Configuring ADC
- Tree Structure - Child Domain
- Forest Structure
- Remote Desktop Services
- Remote Administration Mode(Terminal services)

8. FSMO Roles of AD - DS

- Roles of AD - DS
- Transferring of Roles
- Seizing of Roles
- Storage Technologies
- Introduction to various data backup technologies, Tape drives (LTO,SAN,NAS) Introduction to RAID and RAID LELVELS Configuring Simple Volume (RAID – 0)
- Configuring Mirror Volume (RAID – 1)
- Configuring Parity Volume (RAID – 5)

9. Active Directory Trusts

- Introduction to Trust Relationship
- Categories, Directions & Types of Trusts
- Functional Levels
- Configuring Forest Trusts between 2012 Forests.
- Active Directory Recycle Bin
- Backup & Restore
- Windows Server Backup & Restore
- Upgrading Windows Server 2008 to 2012 TO 2016

MINI PROJECT WORK 2

In the project period the student has to undergo the routers so that the student get enriched knowledge in routers which helps him to know the behavior of routers which makes him expert in the routers so that he can easily guess how to hack the router and how to mitigate it.

1. **Network Fundamentals**
   - Compare & contrast OSI & TCP/IP models Firewalls, Access points, Wireless controllers
   - Compare & contrast collapsed core and three-tier architecture Select the appropriate cabling type (Straight & Cross)
   - Configure, verify & troubleshoot IPv4 addressing & subnetting & supernetting Compare & contrast IPv4 address types Unicast, Broadcast, Multicast
   - Describe the need for private IPv4 addressing,Static and Auto Configuration

2. **LAN Switching Technologies**
   - Describe & verify switching concepts
   - MAC learning & aging, Frame switching, Frame flooding, MAC address table
   - Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches
   - Access ports , Default VLAN
   - Configure, verify, and troubleshoot interswitch connectivity Trunk ports, Add & remove VLANs on a trunk
   - VTP (v1&v2), and 802.1Q Native VLAN Configure, verify, & troubleshoot STP protocols
   - STP mode (PVST+ and RPVST+), STP root bridge selection Configure, verify & troubleshoot STP related optional features
   - PortFast, BPDU guard
   - Configure & verify Layer 2 protocols
   - Cisco Discovery Protocol, LLDP

3. **WAN Technologies**
   - Configure, verify, & troubleshoot GRE tunnel connectivity Describe WAN topology options
   - Point-to-point
   - Describe WAN access connectivity options
   - MPLS, Metro Ethernet, Broadband PPPoE, Internet VPN (DMVPN, site-to-site VPN, client VPN)

4. Routing Technologies

- Describe the routing concepts
- Packet handling along the path through a network
- Forwarding decision based on route lookup
- Frame rewrite
- Interpret the components of a routing table
- Prefix, Network mask, Next hop, Routing protocol code Administrative distance, Metric Gateway of last resort & Admin distance
- Configure, verify, & troubleshoot inter-VLAN routing Router on a stick & SVI
- Compare & contrast static routing & dynamic routing
- Compare & contrast distance vector and link state routing protocols
- Compare & contrast interior and exterior routing protocols
- Configure, verify & troubleshoot IPv4 static and dynamic route
- Default route, Network route, Host route, Floating static
- Configure, verify & troubleshoot single area & multi-area OSPFv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub, virtual-link, and LSAs)
- Configure, verify & troubleshoot EIGRP for IPv4
- Configure, verify, and troubleshoot RIPv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution) Troubleshoot basic Layer 3 end-to-end connectivity issues

5. Infrastructure Services

- Describe DNS lookup operation
- Troubleshoot client connectivity issues involving DNS
- Configure and verify DHCP on a router (excluding static reservations) Server, Relay, Client, TFTP, DNS, & gateway options Troubleshoot client- and router-based DHCP connectivity issues Configure, verify, and troubleshoot basic HSRP Priority, Pre-emption, Version
- Configure, verify, and troubleshoot inside source NAT NAT Static, Pool, PAT

6. Infrastructure Services

- ACL Standard, Extended, Named
- Configure, verify, and troubleshoot basic device hardening
- Local authentication, Secure password, Access to device (Source address & Telnet/SSH)
- Login banner

7. Infrastructure Management

- Configure and verify device-monitoring protocols SNMPv2, SNMPv3 & Syslog
- Configure and verify initial device configuration Perform device maintenance
- Cisco IOS upgrades and recovery (TFTP)
- Password recovery and configuration register & File system management Use Cisco IOS tools to troubleshoot and resolve problems
- Ping & trace route with extended option

8. Layer 3 switch concepts

- Introduction Layer 3 switch
- VLAN routing with layer 3 switch
- Real-time scenario with combination of layer 3 and layer 2 switch configurations

9. Introduction ISP

- Introduction to ISP switches
- Introduction to fiber cables and splicing
- Real time exposure on ISP service.

By undergoing this the Student is able to know the basics of the Hardware Networking and having knowledge on Servers and Routers. So it is Possible for him/her to Know more about Hacking and Mitigation