GUJARAT TECHNOLOGICAL UNIVERSITY

BRANCH: CYBER SECURITY (59)
SUBJECT NAME- SECURITY TOOLS
SUBJECT CODE- 2735902
SEMESTER-III

Type of course: NA

Prerequisite: Basic fundamental knowledge of Network security, Ethical hacking, Malware analysis, Digital forensics.

Rationale: NA.

Teaching and Examination Scheme:

Teaching Scheme				Theory Marks				Tutorial/Practical Marks		Total Marks
						ESE(V)		PA(I)		
Theory	Tutorial/ Presentation	Practical	Credits	ESE (E)	PA (M)	ESE	OEP	PA	RP	
0	0	4	2	0	0	50	30	20	0	100

UNIT-I

Information Security and OpenSource Software

Securing the Perimeter, The Practice of Information-Security, Confidentiality, Integrity, Availability. The State of Computer Crime, Info-Security Business Risks, Open Source History, Open Source Advantages, When Open Source May Not Fit YourNeeds, Windows and Open Source, Open Source Licenses- The GNU General Public License, The BSD License.

UNIT-II

Operating System Tools

Hardening Your Security Tool- System, Installing Bastille Linux, Running Bastille Linux, traceroute (UNIX) or tracert (Windows): Network DiagnosticTools, Considerations for Hardening

Windows- Installing and Using Sam Spade for Windows, Installing and Running PuTTY

UNIT-III

Port Scanners and Vulnerability Scanners

Overview of Port Scanners, Considerations for Port Scanning, Uses for Port Scanners,Creating Your Own NlogExtensions, Interesting Uses for Nlog andNmap. Identifying Security Holes in Your Systems, Vulnerability Scanners to theRescue, Considerations for Vulnerability Scanning, What Vulnerability Testing Doesn't Find.

UNIT- IV

Network Sniffers and Intrusion Detection Systems

A Brief History of Ethernet, Considerations for Network Sniffing, TCP/IP Packet Headers.NIDS Signature Examples, The Problem of NIDS FalsePositives, Getting the Most Out of Your IDS, Configuring Snort for MaximumPerformance, Host-Based Intrusion Detection

UNIT-V

Analysis and Management Tools

Installing Swatch, Configuring and Running Swatch, The Swatch ConfigurationFile, Using Databases and Web Servers to Manage Your Security Data -Setting Up a MySQL Server, Setting Up the Apache WebServer, Setting Up PHP, ADOdb, PHPLOT, JpGraph, GD, Configuring Snort for MySQL, Installing and Configuring ACID, Introduction to Using ACID, Using ACID to Tune and Manage Your NIDS, Other Ways to Analyze Alert Data Using ACID, Using ACID on a Daily

Basis, Graphing ACID Data, Maintaining Your ACIDdatabase, Installing NPI, Importing Nessus Scans into NPI, Using NPI.

UNIT – VI

Encryption Tools

Types of Encryption - Encryption Algorithms, Encryption Applications, Encryption Protocols, Encryption Applications, Installing PGP and Generating Your Public/Private KeyPair, Using PGP

PGP Options, Installing GnuPG, Creating Key Pairs, creating a RevocationCertificate, Publishing Your Public Key, Encrypting Files with GnuPG, Decrypting Files, Signing Files, The PGP/GnuPG Web of TrustModel, Signing Keys and Managing Your Key Trusts, Installing and Starting theOpenSSH Server, Port Forwarding withOpenSSH, Virtual Private Networks - Installing and Starting FreeSWAN, Using FreeS/WAN, Windows Installation, UNIX Installation, Using John the Ripper

UNIT – VII

Wireless Tools

Wireless LAN Technology – Overview, Wi-Fi Terms. Dangers of Wireless LANs – Eavesdropping, Access to Wireless PCs, Access to the LAN, Anonymous Internet Access, 802.11-Specific Vulnerabilities, The "War-Driving" Phenomenon, Performing a Wireless Network - Security Assessment, Equipment Selection, Installing NetStumbler, Using NetStumbler, NetStumbler Options, Saving NetStumbler Sessions, Installing StumbVerter, Using StumbVerter, Installing Your Network Interface, Card and Drivers, Installing Kismet, Using Kismet Wireless, Kismet GPS Support, Kismet IDS, Uses for AirSnort, Installing AirSnort, Running AirSnort, Steps for More Secure WirelessLANs - Turn On WEP, Use Wireless Equipment with an Improved EncryptionProtocol, Require Wireless Users to Comein Via a VPN Tunnel, Treat Your Wireless Network asUntrusted, Audit Your Wireless Perimeter ona Regular BasisMove Your Access PointsConfigure Your Wireless NetworkProperly.

UNIT – VIII

Forensic Tools

Uses for Computer ForensicTools, Building an Incident Response Plan, Preparing for Good Forensic Data, Tenets of Good Forensic Analysis, Forensic Analysis Tools - Installing Fport, Using Fport, Installinglsof, Using lsof. Reviewing Log Files, Making Copies of ForensicEvidence - Installing dd, Using dd, Installing Sleuth Kit, Installing Autopsy ForensicBrowser, Using Sleuth Kit and Autopsy Forensic Browser, Creating and Logging Into aCase, Adding a Host, Adding an Image, Analyzing Your Data, Installing Forensic Toolkit, Using Forensic Toolkit.

COURSE OUTCOME:

After successful completion of the course, the students should be able to,

- Practice hands on experiments using different types of security tools.
- Understand cyber-attack as well as its mitigation techniques.
- Learn how to protect them self and ultimately society from such attacks.
- Assess how the digital evidences will be handled in any crime scene.

OPEN ENDED PROBLEMS:

1. Case Study on "A Solution to Selecting CyberSecuritySoftware Tools for anOrganization Using SecurityControls".

MAJOR EQUIPMENTS:

Desktop/Laptop with high configuration, Mobile, etc.

BOOKS RECOMMENDED:

1. Tony Howlett, "Open SourceSecurity Tools -Practical Applications for Security", Prentice Hall; [ISBN 0-321-19443-8], 2004.
2. Anti-Hacker Tool Kit (Indian Edition) by Mike Shema, Publication Mc Graw Hill.
3. Krutz, Ronald L.and Russell Dean Vines. 2001. The CISSP Prep Guide. New York: John
   Wiley & Sons.
4. Lammle, Todd. 2003. CCNA Cisco Certified Network Associate Study Guide, FourthEdition. Location: San Francisco: Sybex.