CTMTAIDS SI P2: Network Security and Forensics

Teaching Scheme					Evaluation Scheme									
					Theory							Practical		
L	T	P	C	TCH	Internal Exams					University Exams		University Exams (LPW)		Total
					TA-1		MSE		TA-2 *					
					Marks	Hrs	Marks	Hrs	Marks	Marks	Hrs	Marks	Hrs	
03	00	00	03	03	25	00:45	50	01:30	25	100	03:00	-	-	200

* Note: TA-2 will be in form of assignments or workshops.

Objectives

1. To understand the basics of network vulnerability assessment and penetration testing methodology.
2. To understand the important network communication protocols.
3. To understand the concept of encryption, public key cryptography, message authentication and hash functions.
4. To understand the basics of wireless network protocols and its security concepts.
5. To understand the basics of network forensics.

UNIT–I

ISO/OSI, TCP-IP, Networking devices: Host, Hub, Bridge, Switch, Router and its functioning, Perimeter devices: IDS, IPS, Firewall and its functioning. NOC, SOC, SIEM, Servers: DNS, DHCP, Proxy, Mail and Application servers. Threat, vulnerability, attack surface, attack vector, exploit. Common attacks and countermeasures: Phishing attack, ARP poising, MAC flooding, DoS and DDoS.

UNIT–II

Penetration testing life cycle: Scope, SOW, Reconnaissance, target enumeration, vulnerability identification, assessment, exploitation, and reporting. Information gathering starting at source scrutinizing key employees, Dumpster diving, War driving, analyzing the web, exploring domain ownership- whois, Regional internet registries, server location, Scanning: active and passive, ICMP (Ping), OS and server fingerprinting, scanning tools and port status, TCP and UDP scan. SNMP services enumeration, and countermeasures. Routing devices enumeration and countermeasures. Advanced enumeration: Password cracking, sniffing

password hashes and password protection. Vulnerability exploitation, Buffer overflow, vulnerability assessment tools, source code assessment tools, application assessment tools, system assessment tools, exploit tools.

UNIT–III

Introduction to Security: need for security, principle of security, security approaches. Encryption Techniques: plaintext, cipher text, substitution and transposition techniques, encryption and decryption, key range and size. Symmetric and Asymmetric encryption. Public Key Cryptography and Message Authentication: Public key cryptographic principles, digital signatures, key management, hash function and message digest. Types of attacks and countermeasures.

UNIT–IV

802.11 Protocols, WAP and inherent security issues, promiscuous and monitor mode, Sniffing wireless packets, management, control, and data frames, WLAN authentication and encryption, WEP, WPA and WPA 2. WLAN authentication and security flaws. WLAN based attacks and countermeasures. WLAN Pen testing tools.

UNIT–V

Digital evidence, Network based digital evidence, Network Forensic investigation methodology, Sources of network-based evidence, Evidence acquisition, Network traffic capture and analysis, Traffic capture and analysis tools, Event log aggregation, correlation, and analysis. Data in motion investigation

Reference Books: -

1. Stallings, W., Network Security Essentials: applications and standards. 3rd ed. Pearson Education India, 2007.
2. Stallings, W., Cryptography and Network Security: Principles and Practice. 6th ed. Pearson, 2004.
3. Forouzan, B.A., Cryptography and Network Security. Tata McGraw-Hill Education, 2010 2.
4. Kahate, A. Cryptography and Network Security. McGraw-Hill Higher Ed., 2009.
5. Michael Gregg, Build Your Own Security Lab: A Field Guide for

Networking Testing.

6. Sherri Davidoff and Jonathan Ham, Network Forensics Tracking Hackers through Cyberspace.
7. Mastering Wireless Penetration Testing for Highly Secured Environments by Aaron Johns