		DOMAIN		
CUTM		**Cyber Security**	**20**	6+10+4
	CUCS2045	**Linux Server Management and Security**	4	2-2-0
	CUCS2046	**Advanced Hacking Techniques**	4	2-2-0
	CUCS2047	**IT Networking and Network Security**	4	2-2-0
	CUCS2048	**Vulnerability Assessment & Penetration Testing**	4	0-0-4
	CUCS2049	**Project**	4	0-0-4

Objective

1.Develop skills to manage a Linux server and provide basic security to the server

2.Master hacking methodology to be used in penetration testing

3. Good understanding on network infrastructure and identify points of vulnerability in networks

4. Hands on experience on various tools & techniques of vulnerability assessment & penetration testing used in Linux and shall pursue a career in penetration testing domain

Course outcome

- Able to setup Linux server
- Able to do client and server side configuration of different services
- Able to provide security to the server
- Perform different type of attack and find the vulnerabilities
- Able to build networks and subnets
- Able to configure network devices for switching and routing
- Identify some of the factors driving the need for network security
- Aware of the various ways through which hackers' attempts to compromise an Application, Service, Desktop or a server and its countermeasures
- Establishing a methodology for vulnerability assessment and penetration testing

Course content

1. CUCS2045 - Linux Server Management and Security (50 HRs)

1.1 Access the command line, Recovery of the root user password
1.2 Managing files from the command line
1.3 Creating,Viewing,and Editing Text Files
1.4 Managing Local Linux Users and Groups
1.5 Linux File System Permissions
1.6 Monitoring and Managing Linux Processes
1.7 Archiving and Copying Files Between Systems
1.8 Installing and Updating Software Packages
1.9 Accessing Linux File Systems
1.10 Linux Networking
1.11 Analyzing and Storing Logs
1.12 Configuring and Securing OpenSSH Service
1.13 Using Regular Expressions with grep
1.14 Scheduling Future Linux Tasks
1.15 ACLs
1.16 SELinux Security
1.17 Adding Disks, Partitions, and File Systems to a Linux System
1.18 Managing Logical Volume Management (LVM) Storage
1.19 Boot Process
1.20 Managing different services using systemctl
1.21 Planning and Configuring Security Updates
1.22 Basics of System Auditing
1.23 Security guidelines during installation
1.24 Configuring firewalld
1.25 Compliance Policy and Vulnerability Scanning With OPENSCAP

2. CUCS2046 -Advanced Hacking Techniques (56 HRs)

2.1 What is zero day vulnerability and how it works.
2.2 Replay attack, pass the hash
2.3 Hijacking, Clickjacking, Session hijacking, URL hijacking
2.4 Typo squatting, Manipulating Driver, Shimming
2.5 Refactoring, Pivot, Initial exploitation, Persistence
2.6 Techniques of Penetration Testing, vulnerability scanning
2.7 Passively test Security Controls
2.8 Identifying vulnerability, lack of security control, common misconfigurations
2.9 Intrusive vs non intrusive, Credentialed vs non- credentialed, False positive
2.10Security using Firewall, ACL, Application based vs network based
2.11 Stateful vs Stateless, Implicit deny
2.12 Remote access vs site-to-site

2.13 IPSec, Tunnel mode, Transport mode, AH, ESP
2.14 Split tunnel vs full tunnel, TLS, Always-on VPN
2.15 HIDS/HIPS,Antivirus
2.16 File integrity check, Host based firewall
2.17 Application whitelisting, Removable media control
2.18 Advanced malware tools,Patch management tools
2.19 Data execution prevention, web application firewall
2.20 Network Segmentation, Blackholes, Sinkholes, and Honeypots
2.21 System Hardening
2.22 Google Dork
2.23 Proxy
2.24, Password Guessing
2.25 Browser Password Hacking
2.26 Application Password Hacking
2.27 OS Password Hacking
2.28 Server Password Hacking

3. CUCS2047 - IT Networking and Network Security (54 Hrs)

3.1 Network Fundamentals
3.2 OSI model
3.3 TCP/IP protocol suite
3.4 IP addressing- IPv4
3.5 IP addressing- IPv6
3.6 Subnetting
3.7 Wireshark
3.8 Packet capturing
3.9 Analysis of packet
3.10 DHCP
3.11 DNS
3.12 IP configuration
3.13 WAN connectivity
3.14 Authentication
3.15 Basic switching
3.16 Static routing
3.17 Dynamic routing
3.18 VLAN
3.19 IPSec
3.20 ACL
3.21 Firewall
3.22 SSL
3.23 VPN
3.24 NAT
3.25, AAA

4. CUCS2048 - Vulnerability Assessment & Penetration Testing (44 HRs)

4.1 To gain knowledge about how VAPT works, as well as network security protocols, devices, and controls.
4.2 Initiate and manage incidents, as well as do penetration testing.
4.3 Comprehend packet sniffing techniques.
4.4 Learn about network penetration testing models and procedures, security analysis
4.5 scanning and its types(network, port and vulnerability scanning)
4.6 Nmap and live scanning on ports and networks
4.7 Netcat usage on TCP/UDP ports
4.8 Wireshark basics and capturing data
4.9 NFS ,SMB ,SMTP enumeration
4.10 Vulnerability scanning overview
4.11 Different types of vulnerability scanning
4.12 Nessus installation and configuration
4.13 Vulnerability scanning with Nessus
4.14 Web application assessment with nikto, burp suite and Vega
4.15 Vulnerability analysis with Metasploit framework
4.16 Application security testing using acunetix
4.17 OWASP mobile vulnearibility
4.18 Tools for Mobile application vulnearibility
4.19 Identify and mitigate security issues using Microsoft TMT
4.20 Automated software testing using VAF tool
4.21 password security auditing and password recovery using John the Ripper
4.22 Penetration testing using BeEF tool

Text Books:

1. Soyinka Wale, Linux Administration A Beginners Guide ,Mcgrawhill HED, Sixth Edition
2. Jon Erickson , Hacking: The Art of Exploitation, No Starch Press, US, Second Edition
3. CCNA - Routing And Switching Study Guide by Todd Lammle

Reference Books:

1. *Patrick Engebretson,, The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration, Syngress Media,U.S, Second Edition*
2. *Designing Storage Area Networks – Second Edition – Tom Clark*
3. *http://ptac.ed.gov/sites/default/files/issue-brief-threats-to-your-data.pdf*

Sample Project

1. Password Security

2. System Auditing

2. Website vulnerabilities and counter measures

3. Secure application development

Course outline Prepared by: Suvendu Kumar Nayak ***Date:02-07-2022***

Courseware Link: http://courseware.cutm.ac.in/courses/**domain-track-cyber-security**/