COURSE TITLE : ETHICAL HACKING
COURSE CODE : 5135
COURSE CATEGORY : ELECTIVE
PERIODS/WEEK : 4
PERIODS/SEMESTER : 52
CREDITS : 4

TIME SCHEDULE

MODULE	TOPICS	PERIODS
1	Vulnerabilities and Attacks	**13**
2	Hacking Techniques	**13**
3	Operating System Vulnerabilities	**13**
4	Hacking Web Servers and Wireless Networks	**13**

Course General Outcomes:

Sl.	G.O	On completion of this course the student will be able :
1	1	Understand ethical hacking concepts
2	1	Understand the hacking techniques and tools
3	1	Understand the various vulnerabilities of Windows and Linux OSs
4	1	Understand the techniques to hack web servers and tools for it.

Specific outcomes:

MODULE – I: Vulnerabilities and attacks

1.1 Understand ethical hacking concepts
- 1.1.1 Explain the definition of ethical hacking
- 1.1.2 List any five malicious software
- 1.1.3 Explain any five malicious software
- 1.1.4 Explain how to protect against malware attacks
- 1.1.5 List any six network and system attacks
- 1.1.6 Explain any six network and system attacks

MODULE – II: Hacking Techniques

2.1Understand the hacking techniques and tools
- 2.1.1 Describe how web tools are used for footprinting
- 2.1.2 Explain competitive intelligence
- 2.1.3 Describe the use of other footprinting tools
- 2.1.4 Explain the method of DNS zone transfer
- 2.1.5 Explain the art of shoulder surfing
- 2.1.6 Explain the art of dumpster diving

2.1.7 Explain the art of piggy backing
2.1.8 Describe various types of port scans
2.1.9 Explain the use of port scanning tools such as Nmap, Unicornscan, Nessus and OpenVAS
2.1.10 Explain how to conduct ping sweeps
2.1.11 Describe about crafting IP packets

MODULE – III: Operating System Vulnerabilities

3.1 Understand various vulnerabilities of Windows and Linux
3.1.1 Explain Windows file system
3.1.2 Explain Windows RPC
3.1.3 Explain NetBIOS
3.1.4 Explain Server Message Block
3.1.5 Explain common Internet File System
3.1.6 Explain null sessions
3.1.7 Explain Web Services
3.1.8 Explain Buffer overflows
3.1.9 Explain Windows passwords and authentication
3.1.10 Explain the tools for identifying Windows vulnerabilities
3.1.11 Explain the best practices for hardening Windows systems
3.1.12 Explain Linux OS vulnerabilities
3.1.13 Explain the tools for identifying Linux vulnerabilities
3.1.14 Explain the countermeasures against Linux attacks

MODULE – IV: Hacking Web Servers and Wireless Networks

4.1Understand the techniques to hack web servers and tools for it.
4.1.1 Explain web server hacking
4.1.2 Explain about web applications and their components
4.1.3 Describe web application vulnerabilities and countermeasures
4.1.4 Identify the tools used by web attackers and hackers
4.1.5 Explain wireless hacking
4.1.6 Describe the components of a wireless network
4.1.7 Explain the working of wardriving
4.1.8 Explain the tools for wireless hacking
4.1.9 Explain the countermeasures against wireless attacks

CONTENT DETAILS:

MODULE – I: Vulnerabilities and attacks

Definition of ethical hacking, Malicious software – Viruses, Worms, Trojans programs, Spyware, Adware, protection methods, Network and system attacks - Denial of Service (DoS), Distributed Denial of Service (DDoS), Buffer overflow, Ping of death, Session Hijacking, Brute force attack, Man-in-the-middle, Dictionary attack, Replay attack

MODULE – II: Hacking Techniques

Footprinting - Web tools are used for footprinting, Competitive intelligence, Other footprinting tools, DNS zone transfer - Social engineering - Shoulder surfing, Dumpster diving, Piggy backing - Port scanning - Types of port scans, Port scanning tools - Nmap, Unicornscan, Nessus and OpenVAS - Ping sweeps - Crafting IP packets

MODULE – III: Operating System Vulnerabilities

Windows OS vulnerabilities - Windows file system, Windows RPC, NetBIOS, Server Message Block, common Internet File System, Null sessions, Web Services, Buffer overflows, Windows passwords and authentication, Tools for identifying Windows vulnerabilities, Hardening Windows systems

Linux OS vulnerabilities - Tools for identifying Linux vulnerabilities, Countermeasures against Linux attacks

MODULE – IV: Hacking Web Servers and Wireless Networks

Web server hacking - Web applications and their components - Web application vulnerabilities and countermeasures - Tools for web attackers and hackers

Wireless hacking - Wireless network technology - Components of a wireless network – Wardriving - Tools for wireless hacking - Countermeasures against wireless attacks

TEXT BOOK:

1.Hands-On Ethical Hacking and Network Defence - Simpson Michael, Backman Kent ,Corley James-2010

REFERENCES:

1. Official Certified Ethical Hacker Review Guide - DeFino Steven, Kaufman Barry, Valenteen Nick-Cengage Learning--2009

Engebret-sonyngress