

SREENIVASA INSTITUTE of TECHNOLOGY and MANAGEMENT STUDIES

III MCA - I Semester

L	P	C
4	0	4

16MCA315C

ETHICAL HACKING

Course Objectives:

- To learn about how systems vulnerabilities manifest themselves and why hackers continue to enjoy success breaking into systems, despite increasing attention paid to cyber defense.
- To gain experience with a systematic hacking methodology.
- To learn about and experiment with hacking tools that can be applied at different stages of the hacking process.

Syllabus:

UNIT I: Introduction to Ethical Hacking, Ethics, and Legality:

Ethical Hacking Terminology, Different Types of Hacking Technologies, Different Phases Involved in Ethical Hacking and Stages of Ethical Hacking: Passive and Active Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks, Hacktivism, Types of Hacker Classes, Skills Required to Become an Ethical Hacker, Vulnerability Research, Ways to Conduct Ethical Hacking, Creating a Security Evaluation Plan, Types of Ethical Hacks, Testing Types, Ethical Hacking Report

Footprinting and Social Engineering: Footprinting , Information Gathering Methodology, Competitive Intelligence ,DNS Enumeration Who is and ARIN Lookups, Types of DNS Records, Traceroute, E- Mail Tracking , Web Spiders, Social Engineering, Common Types Of Attacks, Insider Attacks, Identity Theft, Phishing Attacks, Online Scams, URL Obfuscation, Social-Engineering Countermeasures.

UNIT II : Scanning and Enumeration

Scanning, types of Scanning , CEH Scanning Methodology ,Ping Sweep Techniques, Nmap Command Switches, SYN, Stealth, XMAS, NULL, IDLE, and FIN Scans, TCP Communication Flag Types, War-Dialing Techniques, Banner Grabbing and OS Fingerprinting Techniques, Proxy Servers, Anonymizers , HTTP Tunneling Techniques, IP Spoofing Techniques, Enumeration, Null Sessions, SNMP Enumeration, Windows 2000 DNS Zone Transfer, Steps Involved in Performing Enumeration.

System Hacking

Understanding Password - Cracking Techniques, Understanding the LAN Manager Hash Cracking Windows 2000 Passwords, Redirecting the SMB Logon to the Attacker SMB Redirection, SMB Relay MITM Attacks and Countermeasures NetBIOS DoS Attacks, Password - Cracking Countermeasures, Understanding Different Types of Passwords Passive Online Attacks, Active Online Attacks, Offline Attacks Nonelectronic Attacks, Understanding Keyloggers and Other Spyware Technologies Understand Escalating Privileges, Executing Applications, Buffer Overflows, Understanding Rootkits Planting Rootkits on Windows 2000 and XP Machines, Rootkit Embedded TCP/IP Stack Rootkit Countermeasures, Understanding How to Hide Files, NTFS File Streaming NTFS Stream Countermeasures, Understanding Steganography Technologies, Understanding How to Cover Your Tracks and Erase Evidence, Disabling Auditing, Clearing the Event Log

UNIT III : Trojans, Backdoors, Viruses, and Worms

Trojans and Backdoors, Overt and Covert Channels, Types of Trojans, Reverse-Connecting Trojans, Netcat Trojan, Indications of a Trojan Attack, Wrapping, Trojan Construction Kit and Trojan Makers, Countermeasure Techniques in preventing Trojans, Trojan - Evading Techniques, System File Verification Sub-objective to Trojan Countermeasures Viruses and Worms, Difference between a Virus and a Worm, Types of Viruses, Understand Antivirus Evasion Techniques, Understand Virus Detection Methods

Sniffers

Protocols Susceptible to Sniffing, Active and Passive Sniffing, ARP Poisoning, Ethereal Capture and Display Filters, MAC Flooding, DNS Spoofing Techniques, Sniffing Countermeasures **Denial of Service and Session Hijacking**

MCA -R13 Regulations 87 Denial of Service, Types of DoS Attacks, DDoS Attacks, BOTs/BOTNETs, "Smurf" Attack, "SYN" Flooding, DoS/DDoS Countermeasures, Session Hijacking, Spoofing vs. Hijacking, Types of Session Hijacking, Sequence Prediction, Steps in Performing Session Hijacking, Prevention of Session Hijacking.

UNIT IV : Hacking Web Servers, Web Application Vulnerabilities, and Web- Based Password Cracking Techniques

Hacking Web Servers, Types of Web Server Vulnerabilities, Attacks against Web Servers, IIS Unicode Exploits, Patch Management Techniques, Web Server Hardening Methods Web Application Vulnerabilities, Objectives of Web Application Hacking, Anatomy of an Attack, Web Application Threats, Google Hacking, Web Application Countermeasures Web_Based Password Cracking Techniques, Authentication Types, Password Cracker, Password Attacks: Classification ,Password-Cracking Countermeasures

SQL Injection and Buffer Overflows

SQL Injection, Steps to Conduct SQL Injection, SQL Server Vulnerabilities, SQL Injection Countermeasures Buffer Overflows, Types of Buffer Overflows and Methods of Detection, Stack- Based Buffer Overflows, Buffer Overflow Mutation Techniques

UNIT V : Linux Hacking

Linux Basics, Compile a Linux Kernel, GCC Compilation Commands, Install Linux Kernel Modules, Linux Hardening Methods Penetration Testing Methodologies Security Assessments, **Penetration Testing Methodologies,**

Penetration Testing Steps, Pen - Test Legal Framework, Automated Penetration Testing Tools Pen_Test Deliverables

Course Outcomes:

- Able to defend hacking attacks and protect data assets.
- Able to defend a computer against a variety of different types of security attacks using a number of hands-on techniques.
- Able to defend a LAN against a variety of different types of security attacks using a number of hands on techniques.
- Practice and use safe techniques on the World Wide Web.

TEXT BOOK:

1. CEH official Certified Ethical Hacking Review Guide, Wiley India Edition

REFERENCE BOOKS:

1. Kenneth C.Brancik “Insider Computer Fraud” Auerbach Publications Taylor & Francis Group–2008.
2. Ankit Fadia “ Ethical Hacking” second edition Macmillan India Ltd, 2006

3. Ethical Hacking & Network Defense, Michael T. Simpson edition3. Hacking Exposed Windows, Joel Scambray, cissp, Stuart McClure, Cissp, Third Edition, Tata Mc Graw hill edition
4. Hacking Exposed Window server 2003, Joel Scambray Stuart McClure, Tata Mc Graw hill edition

Dr. S .Jyothi

Professor, Dept. of Computer Science,
Sri Padmavathi Mahila University,
Tirupathi

University BOS Member

Dr. N. Ch. S. N. Iyengar

Sr. Professor,
School of SCSE,
VIT University,
Vellore, T.N.

Academic Expert member

Dr. A. Rama Mohan Reddy

Professor,
Dept. of Computer Science & Engineering,
S.V. University,
Tirupathi.

Academic Expert member

Mr. D. Babu Rao,

Director of Engineering,
Aricent Technologies,
Bangalore

Industrial Expert member

Mr. M. Nagarjun

Sr. Software Engineer
Cognizent Technology Solution, Bangalore

Alumni member

Prof. M. E. Palanivel

Professor,
MCA Department
SITAMS
Chittoor

BOS Chairman