ETHICAL HACKING
23ICOE311

(COURSE HANDBOOK)

Department of CSE (IoT & Cyber Security with Blockchain Technology)

COURSE FACULTY:

Mr. Aneesh Kumar A

1. GENERAL INFORMATION

Ethical hacking

This Ethical Hacking course provides a structured, step-by-step exploration of the key methodologies used to identify and fix security vulnerabilities across computer networks and systems. Beginning with foundational concepts, legal implications, and reconnaissance techniques, students learn how to gather crucial target intelligence using WHOIS, DNS, and search tools. The curriculum then moves into active network probing and service discovery, covering TCP handshake protocols, port scanning, OS fingerprinting, proxy-based anonymization, and vulnerability assessment tools like OpenVAS and Nikto. Building on these discoveries, the course details deep system enumeration techniques across Windows and UNIX environments—focusing on Null Session, SNMP, LDAP, and SMTP vulnerabilities—before delving into full system hacking topics such as password cracking, privilege escalation, rootkit installation, steganography, and covering tracks. Finally, the syllabus synthesizes these technical domains into practical penetration testing frameworks, teaching students how to manage risk and execute every phase of a pentest using industry-standard security platforms like Nessus, SAINT, and Metasploit.

1.1. Course Objectives

This course is designed to:

- Equip students with a comprehensive understanding of the ethical implications, legal considerations, and best practices associated with ethical hacking.
- Teach students various methodologies for conducting penetration tests, including reconnaissance, enumeration, and exploitation, to assess system security effectively.
- Introduce industry-standard tools such as Nmap and Metasploit for vulnerability assessment,network scanning, and exploitation techniques.
- Cover documentation and presentation of penetration testing results through detailed reports and presentations.

1.2.. Course Outcomes

CO1 Explain security fundamentals, ethical hacking, attack methods, and footprinting for ethical information gathering.

CO2 Perform network scanning, vulnerability assessment, and anonymization for risk identification and countermeasures.

CO3 Analyze the role of enumeration in identifying system vulnerabilities and apply appropriate mitigation techniques.

CO4 Examine system hacking techniques and implement corresponding defense mechanisms to secure systems.

CO5 Analyze penetration-testing methodologies for effective vulnerability assessment and mitigation.

1.3. Set Text and Suggested Sources

The concepts mentioned in the syllabus is taken from the following book:

The Experts: EC-Council, “Ethical Hacking and Countermeasures Attack Phases”, Course Learning, Cengage Learning.

Students can also refer to the following textbooks.

1. James S. Tiller, “The Ethical Hack: A Framework for Business Value Penetration Testing”, Auerbach Publications, CRC Press.
2. Michael Simpson, Kent Backman, James Corley, “Hands-On Ethical Hacking and Network Defense”, Cengage Learning.
3. Gray Hat Hacking - The Ethical Hackers Handbook, Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams, 3rd Edition, Tata McGraw-Hill

Weblinks:

1. Ethical Hacking in 12 Hours - Full Course - Learn to Hack!: https://www.youtube.com/watch?v=fNzpcB7ODxQ
2. Ethical Hacking Full Course 2024 | Live: https://www.youtube.com/watch?v=uHU2uajL1EE
3. Ethical Hacking Full Course - Learn to Hack Fast!: .: https://www.youtube.com/watch?v=K6V7fc5Hj2s
4. Ethical Hacking: https://archive.nptel.ac.in/courses/106/105/106105217/

2. THE COURSE

2.1. Course Description

ETHICAL HACKING			
Semester	**V**	CIE Marks	**50**
Course Code	**23ICOE311**	SEE Marks	**50**
Teaching Hours/Week (L:T:P)	**3:0:0**	Exam Hrs	**3**
Total Hours	**42**	Credits	**3**

The course will run for 14 weeks during Semester 5 and consists of 5 modules that cover essential topics in Ethical Hacking. Each week includes 3 lectures, delivered by Mr. Aneesh Kumar A. These lectures focus on theoretical concepts,and course-related activities. Spanning a total of 42 hours, this 3-credit course is assessed through Continuous Internal Evaluation (CIE) for 50 marks and a Semester-End Examination (SEE) for 50 marks in the form of 3-hour exam duration. This structure ensures a balanced and engaging learning experience for students.

2.2. Initiating Contact with Staff and Other Students

We encourage open communication and welcome your questions regarding the course. However, given the large number of students enrolled, we request that you use email, office-hour appointments, and other forms of correspondence thoughtfully. Before contacting the course team with administrative queries, please check whether your question has already been addressed in previous communications, the course handbook, or the course website. Additionally, we encourage you to engage with your peers for discussion and collaborative learning, as this will enhance your understanding of the course content and help foster a supportive academic community.

2.3. Resources

Resources go beyond just books; they include dynamic tools like digital libraries, e-learning platforms, and research databases. These modern learning environments offer anytime, anywhere access to academic materials, interactive courses, and cutting-edge research, empowering students to explore knowledge and excel in their fields.

Students can access a variety of resources through the college website. These include the VTU Consortium, e-learning platforms, and additional sources like open-access repositories, government portals (e.g., NPTEL, NDLI), and these digital tools provide access to e-books, research papers, video lectures, and interactive tutorials, offering flexible and comprehensive learning environments.

E-learning and digital library can be accessed via the college website https://mite.ac.in/ (Campus Life section > Library > VTU Consortium/e-learning platforms/additional sources).

2.4. Staff

Course Convenor: Aneesh Kumar A
Cabin: Ground floor, PG Block
Email: aneesh@mite.ac.in

2.5. Topics and Reading materials for each module

Module 1	**No. of Hours: 08**
Topic: Introduction to Ethical hacking and Foot printing	
Introduction, Importance of Security, Elements of Security, Phases of an Attack: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks. Types of Hacker Attacks, Hacktivism, Ethical Hackers, Vulnerability Research, Conducting Ethical Hacking, Computer Crimes and Implications. Introduction to Footprinting, Information-Gathering Methodology, Footprinting Tools, WHOIS Tools, DNS Information Tools, Network Range Locator Tools, Email spiders, Locating Network Activity, Meta Search Engines.	
Module 2	**No. of Hours: 09**
Topic: Scanning	
Introduction to Scanning: Scanning Definition, Objectives of Scanning, Scanning Methodology: Checking for live systems, Check for open ports: Three-Way Handshake, TCP Communication Flags, Scanning Methods, War Dialing, Active Banner Grabbing Using Telnet. Fingerprint the operating system: Active stack fingerprinting, Passive stack fingerprinting Scan for vulnerability: OpenVAS and Nikto, Probing the network: Preparing Proxies, Anonymizers. Surfing Anonymously: HTTP Tunneling, Spoofing IP Addresses, Detecting IP Spoofing, Scanning Countermeasures. Tools: Live System Scanning Tools, Port Scanning Tools.	
Module 3	**No. of Hours: 09**
Topic: Enumeration	
Introduction to Enumeration, Enumeration Techniques: Null Session Enumeration-Windows Session Establishment, Null Sessions, Null Session Vulnerabilities, Null	

Session Enumeration Techniques, Null Session Countermeasures. SNMP Enumeration-SNMP, SNMP Service Enumeration, SNMP Enumeration Countermeasures, SNMP UNIX Enumeration, SNMP UNIX Countermeasures. UNIX Enumeration- Showmount, Finger, Rpcinfo, LDAP Enumeration, NTP Enumeration, SMTP Enumeration, Web Enumeration, Web Application Directory Enumeration, Default Password Enumeration, Enumeration Procedure. Tools: Null Session Tools-DumpSec, enum. User Account Tools-GetAcct. Null Session Countermeasure Tools-PsTools: PsExec, PsKill, PsList, SNMP Enumeration Tools-Snmputil,Solar Winds. LDAP Enumeration Tools- JXplorer, Ldap Miner. SMTP Enumeration Tools- SMTPscan. General Enumeration Tools- NB Tscan, Unicornscan.
Module 4 **No. of Hours: 08** **Topic: System Hacking** Introduction to System Hacking: Cracking Passwords, Four Types of Password Attacks: Passive online attacks, Active online attack, offline attacks and Non-Technical Attacks: Shoulder Surfing, Keyboard Sniffing, Social Engineering, Password Guessing. Password Cracking Tools: LCP, ophcrack, Crack, Password Cracking Countermeasures, Escalating Privileges, Executing Applications, Keyloggers and Spyware, Key logger and Spyware Countermeasures, Hiding Files, Rootkits, Rootkit Detection Tools, Steganography, Hiding the Data, Steganography Tools, Steganography Detection, Steganalysis Tools, Covering Tracks-Tools.
Module 5 **No. of Hours: 08** **Topic: Penetration Testing** Introduction to Penetration Testing, Security Assessments, Types of Penetration Testing, Phases of Penetration Testing: Planning Phase: Risk Management, Pretest Dependencies, Enumerating Devices, Threats, Pre Attack Phase: Passive Reconnaissance, Active Reconnaissance, Network Mapping, Attack Phase, Postattack Phase, Tools: Nessus, SAINT, Metasploit.

3. ASSESSMENT

The assessment for the Ethical Hacking is divided into two components: Continuous Internal Evaluation (CIE) and Semester End Examination (SEE), each accounting for 50% of the total marks.

Continuous Internal Evaluation (CIE) comprises two internal tests, scheduled for 8th and 14th week, which together contribute 30% of the total marks. Additionally, students can earn 20% through the completion of two assignments (10 marks for each assignment).

Semester End Examination (SEE) constitutes the remaining 50% of the total marks. Key information regarding examination dates and related details can be accessed via the college website (Academics and Courses section > Calendar of Events > B.E-Odd Sem.)