Course Type	Course Code	Name of Course	L	T	P	Credit
DE	OCSD603	Ethical Hacking	3	0	0	3

Course Objective
Ethical hacking is a subject that has become very important in present-day context, and can help individuals and organizations to adopt safe practices and usage of their IT infrastructure. Starting from the basic topics like networking, network security and cryptography, the course will cover various attacks and vulnerabilities and ways to secure them.
Learning Outcomes
There will be hands-on demonstrations that will be helpful to the participants. The participants are encouraged to try and replicate the demonstration experiments that will be discussed as part of the course.

Unit No.	Topics To be covered	No of Lecture Video	Video Time (Minutes)	Learning Outcome
1	Introduction to ethical hacking. Fundamentals of computer networking. TCP/IP protocol stack.	5	140	Understand the foundational principles, legal boundaries, and core methodologies of ethical hacking and vulnerability assessment. Master essential computer networking concepts, including network architectures, media types, and data transmission models. Analyze the TCP/IP protocol stack layer-by-layer to evaluate packet structures, protocol interactions, and network-level attack vectors.
2	IP addressing and routing TCP and UDP. IP subnets	5	134	Apply IP addressing schemes and subnet masking techniques to calculate logical subnets, network boundaries, and host address allocations. Analyze IP routing principles and packet forwarding mechanisms to direct traffic efficiently across interconnected subnetworks. Evaluate transport layer protocols by contrasting connection-oriented, reliable data delivery in TCP against connectionless, low-latency transmission in UDP.
3	Routing protocols. IP version 6 Deepen the understanding with the knowledge of various routing protocols and Ipv6 technological superiority.	5	152	Analyze the operational mechanics, metric calculations, and convergence properties of distance-vector, link-state, and path-vector routing protocols. Examine the 128-bit architectural framework, address hierarchy, and header structure optimizations of IP version 6 (IPv6). Evaluate the technological superiority of IPv6 over IPv4, focusing on stateless autoconfiguration (SLAAC), built-in IPsec support, simplified headers, and improved routing efficiency.
4	Installation of attacker and victim system Information gathering using advanced google search, archive.org, netcraft, whois, host, dig, dnsenum and NMAP tool.	5	178	Deploy and configure isolated attacker and victim environments to establish a controlled laboratory setup for ethical hacking and security testing. Conduct passive reconnaissance using open-source intelligence (OSINT) tools—including advanced Google dorks, Archive.org, Netcraft, and WHOIS—to gather target domain metadata. Execute active network reconnaissance and DNS enumeration using tools like host, dig, dnsenum, and Nmap to discover live hosts, open ports, and running services.
5	Vulnerability scanning and security scanning Hands-on: using NMAP and Nessus. Creating a secure hacking environment System Hacking: password cracking privilege escalation application execution Malware and Virus ARP spoofing MAC attack.	5	166	Conduct comprehensive vulnerability and security scanning using Nmap and Nessus within a secure, isolated hacking environment. Master system hacking techniques—including password cracking, local privilege escalation, application execution, and malware behavior analysis. Analyze and execute Data Link layer attack vectors, specifically ARP spoofing and MAC flooding, to evaluate traffic interception and man-in-the-middle risks.
6	Cryptography How private-key encryption, public-key encryption play pivotal role in security and its hacking perspective.	5	130	Analyze the fundamental mechanics and trade-offs of private-key (symmetric) and public-key (asymmetric) cryptosystems within modern security architectures. Evaluate how hybrid cryptographic frameworks leverage

				symmetric encryption for data privacy and asymmetric encryption for secure key exchange and authentication. Examine cryptographic primitives from an offensive security perspective to identify implementation flaws, key recovery attack vectors, and protocol-level vulnerabilities.
7	Application of cryptography Cryptographic hash functions, digital signature and certificate	5	124	Apply cryptographic hash functions to ensure data integrity, password security, and message authentication across real-world applications. Evaluate digital signature mechanisms to achieve non-repudiation, origin verification, and tamper detection in digital transactions. Construct and manage Public Key Infrastructure (PKI) architectures utilizing X.509 digital certificates to establish trusted communications across untrusted networks.
8	Authentication and Network based attacks Steganography, biometric authentication, network-based attacks, DNS and Email security	5	130	Examine biometric authentication systems, multi-factor mechanisms, and steganographic data-hiding techniques for identity verification and covert communication analysis. Analyze common network-based attack vectors—including denial-of-service, packet sniffing, and session hijacking—to evaluate perimeter defenses and traffic anomalies. Evaluate core infrastructure security controls for DNS and Email systems (such as DNSSEC, SPF, DKIM, and DMARC) to mitigate domain spoofing, cache poisoning, and phishing attacks.
9	Authentication and Network based attacks – Part 2 Packet sniffing using wireshark and burpsuite, password attack using burp suite. Social engineering attacks and Denial of service attacks.	5	125	Execute network traffic capture and HTTP/S payload analysis using Wireshark and Burp Suite to conduct controlled credential auditing and automated password attacks. Examine human-centric social engineering attack vectors—including phishing, pretexting, and baiting—to assess organizational vulnerabilities and implement defense controls. Analyze network- and application-layer Denial of Service (DoS/DDoS) attack mechanisms to evaluate rate-limiting, traffic scrubbing, and infrastructure resilience strategies.
10	Hardware security side-channel attacks physical inclinable functions hardware trojans.	5	122	Analyze physical side-channel attacks—including power analysis, timing measurements, and electromagnetic emanations—to identify information leakage in cryptographic hardware implementations. Evaluate Physical Unclonable Functions (PUFs) and silicon fingerprinting techniques for generating secure keys, chip authentication, and hardware root-of-trust. Examine hardware Trojan classification, malicious modification mechanisms, and supply-chain detection methodologies to safeguard integrated circuits (ICs).
11	Types of attacks Web Server Attacks Using Metasploit framework: password cracking privilege escalation, remote code execution, Attack on web servers: password attack, SQL injection, cross site scripting.	5	183	Analyze web server attack classifications and vector models to identify common vulnerabilities across application architectures. Evaluate web application security flaws—including SQL Injection (SQLi), Cross-Site Scripting (XSS), and credential-based attack mechanisms. Assess post-exploitation and penetration testing methodologies using frameworks like Metasploit to analyze remote code execution and privilege escalation vectors.
12	Case studies Various attacks scenarios and their remedies. Relook on Nmap Tool Network analysis using Wireshark Course summarization	5	145	Analyze real-world cyberattack case studies to evaluate multi-stage threat scenarios, system vulnerabilities, and actionable mitigation strategies. Master advanced network analysis and host discovery techniques using Nmap and Wireshark to inspect packet-level traffic and identify security anomalies. Synthesize end-to-end security concepts, attack paradigms, and defensive tools into a holistic ethical hacking and network security framework.
Total No of video lectures & Video time		**60**	**1729**	

Text books

1. Data and Computer Communications -- W. Stallings.
2. Data Communication and Networking -- B. A. Forouzan
3. TCP/IP Protocol Suite -- B. A. Forouzan
4. UNIX Network Programming -- W. R. Stallings

Reference books:

1. Introduction to Computer Networks and Cybersecurity -- C-H. Wu and J. D. Irwin
2. Cryptography and Network Security: Principles and Practice -- W. Stallings
3. ** Various web resources **

Link of NPTEL Course:

https://nptel.ac.in/courses/106105217