ETHICAL HACKING

PROF. INDRANIL SENGUPTA
Dept. of Computer Science and Engineering
IIT Kharagpur

TYPE OF COURSE : Rerun | Elective | UG/PG
COURSE DURATION : 12 Weeks (24 Jan' 22 - 15 Apr' 22)
EXAM DATE : 23 Apr 2022

INTENDED AUDIENCE : Computer Science and Engineering / Information Technology / Electronics and Communication Engineering / Electrical Engineering
PREREQUISITES : Basic concepts in programming and networking
INDUSTRIES APPLICABLE TO : TCS, Wipro, CTS, Google, Microsoft, Qualcomm

COURSE OUTLINE

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. There will be hands-on demonstrations that will be helpful to the participants.

ABOUT INSTRUCTOR

Prof. Indranil Sengupta has obtained his B.Tech., M.Tech. and Ph.D. degrees in Computer Science from the University of Calcutta. He joined the Indian Institute of Technology, Kharagpur, as a faculty member in 1988, in the Department of CSE, where he is presently a full Professor. He had been the former Heads of the Department of Computer Science and Engineering and also the School of Information Technology of the Institute. He was also the Managing Director of Science and Technology Entrepreneurship Park (STEP), and the Professor-in-Charge of a Centre of Excellence in Information Assurance funded by the Ministry of Defense.

COURSE PLAN

Week 1 : Introduction to ethical hacking. Fundamentals of computer networking. TCP/IP protocol stack.
Week 2 : IP addressing and routing. Routing protocols.
Week 3 : Introduction to network security. Information gathering: reconnaissance, scanning, etc.
Week 4 : Vulnerability assessment: OpenVAS, Nessus, etc. System hacking: password cracking, penetration testing, etc.
Week 5 : Social engineering attacks. Malware threats, penetration testing by creating backdoors.
Week 6 : Introduction to cryptography, private-key encryption, public-key encryption.
Week 7 : Key exchange protocols, cryptographic hash functions, applications.
Week 8 : Steganography, biometric authentication, lightweight cryptographic algorithms.
Week 9 : Sniffing: Wireshark, ARP poisoning, DNS poisoning. Hacking wireless networks, Denial of service attacks.
Week 10 : Elements of hardware security: side-channel attacks, physical unclonable functions.
Week 11 : Hacking web applications: vulnerability assessment, SQL injection, cross-site scripting.
Week 12 : Case studies: various attacks scenarios and their remedies.