ETHICAL HACKING

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

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. The participants are encouraged to try and replicate the demonstration experiments that will be discussed as part of the course.

ABOUT INSTRUCTOR

Prof. Indranil Sengupta has obtained his B.Tech., M.Tech. and Ph.D. degrees in Computer Science and Engineering from the University of Calcutta. He joined the Indian Institute of Technology, Kharagpur, as a faculty member in 1988, in the Department of Computer Science and Engineering, 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 has over 28 years of teaching and research experience. He has guided 22 PhD students, and has more than 200 publications to his credit in international journals and conferences. His research interests include cryptography and network security, VLSI design and testing, and mobile computing.

He is a Senior Member of IEEE. He had been the General Chairs of Asian Test Symposium (ATS-2005), International Conference on Cryptology in India (INDOCRYPT-2008), International Symposium on VLSI Design and Test (VDAT-2012), International Symposium on Electronic System Design (ISED-2012), and the upcoming Conference on reversible Computation (RC-2017). He had delivered invited and tutorial talks in several conferences in the areas of VLSI design and testing, and network security.

COURSE PLAN

Week 1: Introduction to ethical hacking. Fundamentals of computer networking. TCP/IP protocol stack.

Week 2: IP addressing and routing. TCP and UDP. IP subnets.

Week 3: Routing protocols. IP version 6.

Week 4: Installation of attacker and victim system. Information gathering using advanced google search, archive.org, netcraft, whois, host, dig, dnsenum and NMAP tool.

Week 5: Vulnerability scanning using NMAP and Nessus. Creating a secure hacking environment. System Hacking: password cracking, privilege escalation, application execution. Malware and Virus. ARP spoofing and MAC attack.

Week 6: Introduction to cryptography, private-key encryption, public-key encryption.

Week 7: Cryptographic hash functions, digital signature and certificate, applications.

Week 8: Steganography, biometric authentication, network-based attacks, DNS and Email security.

Week 9: Packet sniffing using wireshark and burpsuite, password attack using burp suite. Social engineering attacks and Denial of service attacks.

Week 10: Elements of hardware security: side-channel attacks, physical inclinable functions, hardware trojans.

Week 11: Different types of attacks using Metasploit framework: password cracking, privilege escalation, remote code execution, etc.Attack on web servers: password attack, SQL injection, cross site scripting.

Week 12: Case studies: various attacks scenarios and their remedies.