

Subject Code: 1ET2030107	Subject Title: ETHICAL HACKING (Elective – I)
Pre-requisite	Fundamentals of Computer Networks, Cryptography, Programming and Operating Systems

Course Objective:

Course Objectives defines to locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers. And also they get knowledge about hacking skills for defensive purposes on behalf of the owners of information systems.

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture	Tutorial	Practical	Credit	Theory		Practical		Total
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
2	-	2	4	60	40	30	20	150

Subject Contents			
Sr. No	Topic	Total Hours	Weight (%)
1	Overview of Information Security and Introduction of Ethical Hacking Case Study, The Security, Functionality, and Usability Triangle, Information Security Threats and Types of Attacks, The Technical Foundation of Hacking, The Business aspect of Penetration Testing, Hacking Concepts, Hacking Types, Hacking Phases	4	17
2	Reconnaissance, Information Gathering Methodology: Footprinting, and Social Engineering, Scanning and Enumeration: Footprinting Methodology - Using Google to Gather Information, Understanding Who is and ARIN Lookups, Email and Website, Footprinting, Footprinting Tools – Whois, Nslookup, Sam Spade, Types of Social Engineering Attacks and Countermeasures.	4	17
3	Malware Threats and Sniffers: Trojans, Backdoors, Viruses, and Worms, Sniffing Concepts, MAC Attacks, ARP Spoofing, DNS Spoofing, Spoofing Countermeasure, Sniffing tools – Wireshark, Steel Central Packet Analyzer, Tcpdump/Windump	4	17
4	Denial of Service and Session Hijacking, Web Application Vulnerabilities, SQL Injection and Buffer Overflows	3	13
5	Evading IDSs, Honeypots, and Firewalls	3	13
6	Hacking Linux System: Linux Basics, Compiling a Linux Kernel, Installing Linux Kernel Modules, Linux Hardening Methods	3	13
7	Wireless Network Hacking Wireless Concept, Wireless Encryption, Wireless Hacking Methodology and Tools, Countermeasures	3	13

Review Presentation: The student is expected to spend minimum 2 hours per week (as mentioned in the teaching and evaluation scheme) to refer at least two peer reviewed journal papers related to this domain/subject. The student is expected to identify issues/challenges and emerging trends in the domain/subject. Student is supposed to explore various video lectures (E.g. NPTEL) available in the domain/subject. Student is required to make a review-presentation on the work carried out for the same.

Recommended sites for journal papers are (1) dl.acm.org (2) springer.com (3) sciencedirect.com (4) elsevier.com (5) ieeexplore.ieee.org (6) scholar.google.co.in (7) scopus.com or others of similar repute.

Course Outcome:

After learning the course, the students would be able to

- Understand the Security Triad – Confidentiality, Integrity, and Availability, learn about various types of hacking attacks
- Understanding tools and techniques for a penetration testing
- aware about cyber-crime laws of IPC

List of References:

1. Kimberly Graves “CEH Certified Ethical Hacker Study Guide” Wiley Publication
2. Allen Harper, Shon Harris “Gray Hat Hacking: The Ethical Hackers Handbook” McGraw Hill
3. C.K punia “Cyber Laws” Sumit Enterprises

E-Resources / Web Links:

1. <http://williamstallings.com/ComputerSecurity/>
2. <http://williamstallings.com/Cryptography/>
3. <http://williamstallings.com/NetworkSecurity/>

List of Experiments:

Note: The experiment list provided beneath is for reference only. The course teacher may change/formulate it as per his/her methodology and requirement.

1. Download the tool samspace and explore *whois* on any of the domains.
2. Port and TCP Scanning using Nmap.
3. Explore any three information gathering exercises, using google hacks /dorks.
4. Explore information gathering using FOCA.
5. Create a Filter to capture only FTP traffic, using Wireshark.
6. Explore vulnerability scanning using Nessus and assess the report.
7. Using wireshark, identify the version of SSL protocol used (SSLv1, SSLv2, SSLv3, TLSv1, TLSv2, etc) in any HTTPS web portal of your choice.
8. Install Reanimator in your Windows Machine and scan the system for malware and prepare one report for the same.
9. Explore an email header and document the identified information.
10. Explore routing table, ARP tables, IP addresses, TCP and UDP Open ports, user accounts and shares using SNMP tools.(SNMPUtil).
11. Download the tool OmniPeek Network Analyzer and analyze network traffic on any of the domain.
12. Download the tool ZAP and performs session Hijacking between two machines.
13. Implement SQL Injection attack on MySQL Database.