

CSC 562 – ATTACK, DEFENSE AND PENETRATION TESTING

CREDIT HOURS: 3

PREREQUISITES: CSC 241 or 331, 455 or 447; or Instructor Permission.

GRADE REMINDER: Must have a grade of C or better in each prerequisite course

CATALOG DESCRIPTION

Examination of the techniques and technologies for the penetration of networks, detection of attacks, and prevention of attacks. Addresses the techniques, technologies, and methodologies used by cyber intruders (hackers) to select a target and launch an attack. Assesses the various countermeasures to keep the system out of the “sights” of the hacker and to keep the hacker out of the perimeter of the target network. Explores the laws and the legal considerations in prosecuting computer crime.

PURPOSE OF COURSE

To study techniques and technologies to detect cyber attacks even while the attack is in progress. To permit early detection of system vulnerabilities, permitting an administrator to track the movements of the hacker and to discover the intent and goals of the hacker, and thereby provide a good defense. To study and understand the mind and psyche of the hacker is essential to anticipating the actions and reactions of the hacker and to design effective countermeasures. Covers penetration testing to aid in discovery or prevention of cyber attacks.

EDUCATIONAL OBJECTIVES

Upon successful completion of the course, students should be able to:

1. Explain how attackers map organizations, and be able to describe common port scanning techniques
2. Identify some of the tools used to perform enumeration
3. Explain the significance of wireless security
4. List the issues facing Web servers
5. Describe the characteristics of malware, and be able to explain an understanding of the ways of detecting Trojans
6. Describe the process of DoS attacks
7. Describe the benefits of automated assessment tools, and be able to list the components of incident response
8. List the detective methods of defense

CONTENT

Hours

Introduction.....	3
Classes of hackers	
Attack detection	
Defense against attacks	
Penetration Testing	
Footprinting.....	9

Footprinting Tools and Techniques
Ports and Port Scanning
NMAP lab

Web and Database Attacks	12
Viruses	
Malware	
Worms	
SQL Injection	
Trojans and backdoors	
Session hijacking	
DOS (Denial of Service) Attacks	
Prevention	6
Linux, PC and OSX prevention	
Live CDs	
Bootable USBs	
Automated and on-demand assessment tools	
Penetration Testing	9
Ethical Penetration Testing	
Methods and techniques	
Exams (plus final)	6
	TOTAL 45

REFERENCES

Sean Philip and Michael Gregg, Hacker Techniques, Tools, and Incident Handling, Jones & Bartlett Learning, 2011

George Weidman, Penetration Testing: A Hands-On Introduction to Hacking, No Starch Press, 2014

James Patterson, Hacking: Beginner to Expert Guide to Computer Hacking, Basic Security and Penetration Testing, Amazon Digital Services, 2016

Edward Skoudis and Tom Liston, Computer Hack Reloaded: A Step by Step Guide to Computer Attacks and Effective Defenses, 2nd Ed, Prentice Hall, 2007