COURSE DESCRIPTION (with prerequisites):
This course is an introduction to the principles and practices of network and system penetration testing, and techniques to defend against attacks that exploit system vulnerabilities. CIS 1352 prepares students for the EC-Council Certified Ethical Hacking industry certification. This course includes both lecture and structured lab experiences. Prerequisite: CTS 1120 or equivalent certifications or consent of department. 3 semester hours credit.

NAME(S) OF INSTRUCTORS:
Marcus Dabai

REQUIRED TEXTBOOKS AND INSTRUCTIONAL MATERIALS:

GRADING POLICY:
The standing of a student in each course is expressed by one of the following letters and corresponding grading system:
A – 90 – 100
B – 80 – 89
C – 70 – 79
D – 60 – 69
F – 59 or less
The Chipola Catalog provides policies and procedures regarding the grading system. A student’s Grade Point Average is derived from the grading system/quality point scale.

ATTENDANCE AND WITHDRAWAL POLICIES:
Chipola College expects regular attendance of all students, and all instructors record attendance daily. Students who are absent from classes for any reason other than official college activities must satisfy the instructor concerned that the absence was due to illness or other clearly unavoidable reasons. Otherwise, the student may suffer grade loss at the discretion of the instructor. Chipola policy allows each instructor to specify in the Instructor First Day Handout whether or not an absence is excusable and what affect the absence or tardy may have on the grade.
A student is allowed to repeat a course a maximum of three (3) times. **On the third attempt a student (1) must bear the full cost of instruction (unless waived by Student Services), (2) cannot withdraw, and (3) must receive a grade.**

**MAKE-UP POLICY:**  
Chipola allows each instructor to specify in the Instructor First Day Handout the makeup policy.

**ACADEMIC HONOR CODE POLICY:**  
Students are expected to uphold the Academic Honor Code. Chipola College’s Honor Code is based on the premise that each student has the responsibility to (1) uphold the highest standards of academic honesty in his/her own work; (2) refuse to tolerate academic dishonesty in the college community; and (3) foster a high sense of honor and social responsibility on the part of students. Further information regarding the Academic Honor Code may be found in the Chipola Catalog, Student Governance section.

**STUDENTS WITH DISABILITIES POLICY:**  
Chipola College is committed to making all programs and facilities accessible to anyone with a disability. Chipola’s goal is for students to obtain maximum benefit from their educational experience and to effectively transition into the college environment. Students with disabilities are requested to voluntarily contact the Office of Students with Disabilities to complete the intake process and determine their eligibility for reasonable accommodations.

**NOTICE OF EQUAL ACCESS/EQUAL OPPORTUNITY AND NONDISCRIMINATION:**  
Chipola College does not discriminate against any persons, employees, students, applicants or others affiliated with the college with regard to race, color, religion, ethnicity, national origin, age, veteran’s status, disability, gender, genetic information, marital status, pregnancy or any other protected class under applicable federal and state laws, in any college program, activity or employment.

Karan Davis, Associate Vice President of Human Resources, Equity Officer and Title IX Coordinator, 3094 Indian Circle, Marianna, FL 32446, Building A, Room 183A, 850-718-2205, davisk@chipola.edu.

**LIBRARY AND ON-LINE REFERENCE MATERIALS:**  
The library is a comprehensive learning resource center providing information in print, electronic, and multimedia format to support the educational objectives of the College. On-line catalogs, e-books and electronic databases can be accessed by using the LINCCWeb icon on the Chipola Library website at [www.chipola.edu/library](http://www.chipola.edu/library). If you have questions about database usage consult the “How to Use the Chipola Databases” on the Library website or call the Library at 850/718-2274 during regular hours. Library hours are posted each semester at the building entrance and on the Library website. See your Instructor First Day Handout for individual instructor recommendations and resources.
TECHNOLOGY RESOURCES:
The college’s learning management system is Canvas. Classes become available on Canvas on the first day of the semester. It is the student’s responsibility to log onto the Canvas system the first day of class to establish the first day of attendance and to check announcements. All official class communication must be through Canvas. For further information, contact your instructor or the Director of eLearning. The Canvas support hotline is available online in live chat and on the phone, toll-free, at 855-308-2812 for any issues in accessing or utilizing Canvas. The Technology Center, located in the library, is equipped with computer workstations. Lab hours are posted each semester at the building entrance and on the Library website.

FREE TUTORING RESOURCES:
The Academic Center for Excellence (ACE) Lab, located in Building L, offers free tutoring from 8 a.m. to 5 p.m. and is equipped with computer workstations. ACE lab hours are posted each semester at the room entrance and on the website. Additionally, Chipola College has contracted Smarthinking, a Pearson Company, for online tutoring services, accessible especially from 5 p.m. to 8 a.m. and weekends. Smarthinking can be accessed through Canvas.

ELECTRONIC DEVICE USAGE STATEMENT:
Classrooms should be free of all unnecessary distractions from the task of learning. Therefore, as a general rule, students should silence and avoid use of all electronic devices (laptops, phones, tablets, etc.) not being used for coursework. Consult first-day handouts for any specific policies related to the use of electronic devices in the classroom, as they may vary depending upon the nature of the course or the guidelines of the instructor. Faculty reserve the right to regulate the use of electronic devices and their accessories in class.

DISCIPLINE SPECIFIC COMPETENCIES / LEARNING OUTCOMES:
Associate in Science degree in Computer Information Technology Learning Outcomes:
CIT-1 Understand, install, configure, monitor, use, and troubleshoot computer hardware and software. [1.0, 2.0, 3.0, 4.0, 6.0, IT Support 12.0, 13.0]  
CIT-2 Understand, install, configure, monitor, use, and troubleshoot network hardware and software. [8.0, 9.0]  
CIT-3 Demonstrate general computing workplace competencies, including employability skills, interpersonal & customer service skills, and user support skills. [11.0, IT Support 12.0, 13.0, 14.0, 15.0]  
CIT-4 Demonstrate project management skills. [10.0]  
CIT-5 Perform database management and design tasks. [7.0]  

Associate in Science degree in Network Systems Technology Learning Outcomes:
NST-1 Understand, install, configure, monitor, use, and/or troubleshoot computer hardware and software. [1.0, 3.0]
NST-2 Understand, install, configure, monitor, use, and troubleshoot network hardware and software. [2.0, 4.0]
NST-3 Demonstrate general computing workplace competencies, including employability skills, interpersonal & customer service skills, and user support skills. [5.0, Server Admin 18.0]
NST-4 Demonstrate project management skills. [6.0]
NST-5 Depends on Specialization:
   A) Server Administration (Program Code 2181): Demonstrate advanced understanding of networked environments and perform network administration activities. [Server Admin Specialization 7.0-8.0]
   B) Network/Cybersecurity (Program Code 2182): Demonstrate proficiency in securing networks and data, including performing penetration testing and responding to cybersecurity incidents. [Network/Cybersecurity Specialization 7.0-9.0]
   C) Digital Forensics (Program Code 2183): Demonstrate understanding of forensic casework procedures and perform computer and mobile device forensic investigations. [Digital Forensics Specialization 7.0-14.0]

---

### LINKING COURSE-LEVEL STUDENT LEARNING OUTCOMES WITH DISCIPLINE-SPECIFIC COMPETENCIES, ASSESSMENT METHODS, AND ARTIFACTS

<table>
<thead>
<tr>
<th>COURSE-LEVEL STUDENT LEARNING OUTCOMES FOR CIS 1352</th>
<th>DISCIPLINE-SPECIFIC GENERAL EDUCATION COMPETENCIES</th>
<th>ASSESSMENT METHODS FOR COURSE LEVEL STUDENT LEARNING OUTCOMES</th>
<th>LEARNING ARTIFACTS FOR AA PROGRAM ASSESSMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upon completion of this course, the student will be able to:</td>
<td>CIT-1 CIT-2 CIT-3 NST-1 NST-2 NST-3</td>
<td>H or Proj. or Q or T</td>
<td>H or Proj. or T</td>
</tr>
<tr>
<td>1. Describe Ethical Hacking, Ethics, and Legality</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Explore Cryptography and Encryption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Gather Network and Host Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Explore System Hacking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Recognize and Deal with Trojans, Backdoors, Viruses, and Worms</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Gather Data from Networks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Explore Web Site Hacking and Network and Protection Systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Attacking Applications and Wireless Networks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Understand Methods used to Bypass Physical Site Security and Network Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Perform a Penetration Test</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Assessment Codes**

| T = Tests | RPT = Report/Presentation | Proj. = Projects | BO = Behavioral Observation |
| Pre/Post = Pre- and Post-Tests | SP = Skills Performance | Exp. = Experiments | Clin. = Clinicals |
| OT = Objective Tests | SD = Skills Demonstration | Cap. Proj. = Capstone Project | CS = Case Study |
| U = Unit Tests | W = Writing Assignments | Cap. Course = Capstone Course | CP = Case Plan |
| Q = Quizzes | E = Essays | Pract. = Practicum | Port. = Portfolio |
| F = Final Examination | DE = Documented Essays | Intern. = Internship | Obs. = Teacher Observation |
| CF = Cumulative Final | RP = Research papers | H = Homework | Sk. Check = Skills Check-off |
| EX = Departmental Exam | J = Jury | PS = Problem Solving | Curriculum Frameworks |
| SE = Nat’l or State Standardized Exam | R = Recital | DB = Discussion Board | JP = Judged |

**MEANS OF ACCOMPLISHING STUDENT LEARNING OUTCOMES:**

1. Attend and participate in class regularly.
2. Read all assigned material before class.
3. Study in-class notes and online (Canvas) materials.
4. Complete assigned projects in a timely manner to enable reflections and revisions on the final product.
5. Participate in discussions.
6. Demonstrate your mastery of the required skills on quizzes, exams, etc.
7. Complete all assignments with promptness and accuracy.
8. All written documents as well as online assignments must be completed using correct grammar, spelling, and structure.

The grading breakdown is subject to change at the discretion of the instructor.

- Quizzes up to 40%
- Test (which includes Midterm and Final) up to 60%
- Assignments, Projects and/or Labs up to 40%
- Participation up to 20%

Please see your first day handout for individual instructor grading schemes.

Academic Honesty: Do not attempt to get assistance on exams from any other individual; or to complete assignments or gain answers for quiz questions or assignments dishonestly. Please refer to the Chipola College Catalog and the Chipola College Student Handbook for information on the Academic Honor Code and the Academic Honor Code – Consequences. Academic dishonesty includes but is not limited to plagiarism, cheating, and misrepresentation on assignments, quizzes and/or exams.

**ASSIGNMENT AND/OR COURSE OUTLINE**

The following topics will be covered in this course at the discretion of the instructor:

- Ethical Hacking Overview
- TCP/IP Concepts Review
- Network and Computer Attacks
- Footprinting and Social Engineering
- Port Scanning
- Enumeration
- Programming for Security Professionals
- Desktop and Server OS Vulnerabilities
Embedded Operating Systems: The Hidden Threat
Hacking Web Servers
Hacking Wireless Networks
Cryptography
Network Protection Systems

See your Instructor First Day Handout for individual instructor assignment schedule.