

10/4/12

FORMAT 1

Submit original with signatures + 1 copy + electronic copy to Faculty Senate (Box 7500).
See <http://www.uaf.edu/uafgov/faculty-senate/curriculum/course-degree-procedures/> for a complete description of the rules governing curriculum & course changes.

TRIAL COURSE OR NEW COURSE PROPOSAL

SUBMITTED BY:

Department	CITS	College/School	CRCO
Prepared by	Keith Swarner	Phone	455-2820
Email Contact	keith.swarner@alaska.edu	Faculty Contact	Keith Swarner

1. ACTION DESIRED (CHECK ONE):

Trial Course	<input type="checkbox"/>	New Course	<input checked="" type="checkbox"/>
--------------	--------------------------	------------	-------------------------------------

2. COURSE IDENTIFICATION:

Dept	CITS	Course #	F263	No. of Credits	3
------	------	----------	------	----------------	---

Justify upper/lower division status & number of credits:

This course will build upon the skills and knowledge developed in CITS F261. Students will learn how to conduct penetration tests to verify the validity of vulnerabilities identified within an enterprise's network and information systems and to make recommendations about security improvements that should be considered to better protect an organization's digital assets. This course is appropriate for students who are entering their second or third semester of the IT Specialist associate degree program.

3. PROPOSED COURSE TITLE: Network Security Penetration Testing

4. To be CROSS LISTED? YES/NO

No	If yes, Dept: NA	Course #	NA
----	------------------	----------	----

(Requires approval of both departments and deans involved. Add lines at end of form for additional required signatures.)

5. To be STACKED? YES/NO

No	If yes, Dept: NA	Course #	NA
----	------------------	----------	----

Stacked course applications are reviewed by the (Undergraduate) Curricular Review Committee and by the Graduate Academic and Advising Committee. Creating two different syllabi—undergraduate and graduate versions—will help emphasize the different qualities of what are supposed to be two different courses. The committees will determine: 1) whether the two versions are sufficiently different (i.e. is there undergraduate and graduate level content being offered); 2) are undergraduates being overtaxed?; 3) are graduate students being undertaxed? In this context, the committees are looking out for the interests of the students taking the course. Typically, if either committee has qualms, they both do. More info online - see URL at top of this page.

6. FREQUENCY OF OFFERING: As Demand Warrants

Fall, Spring, Summer (Every, or Even-numbered Years, or Odd-numbered Years) — or As Demand Warrants

7. SEMESTER & YEAR OF FIRST OFFERING (AY2013-14 if approved by 3/1/2013; otherwise AY2014-15)

Spring 2014 (AY2013-14)

8. COURSE FORMAT:

NOTE: Course hours may not be compressed into fewer than three days per credit. Any course compressed into fewer than six weeks must be approved by the college or school's curriculum council. Furthermore, any core course compressed to less than six weeks must be approved by the core review committee.

COURSE FORMAT: (check all that apply)

<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input checked="" type="checkbox"/> 6 weeks to full semester
----------------------------	----------------------------	----------------------------	----------------------------	----------------------------	--

OTHER FORMAT (specify)

NA
Mode of delivery (specify lecture, field trips, labs, etc)
Lecture

9. CONTACT HOURS PER WEEK:	3	LECTURE hours/weeks	0	LAB hours /week	0	PRACTICUM hours /week
-----------------------------------	----------	------------------------	----------	--------------------	----------	--------------------------

Note: # of credits are based on contact hours. 800 minutes of lecture=1 credit. 2400 minutes of lab in a science course=1 credit. 1600 minutes in non-science lab=1 credit. 2400-4800 minutes of practicum=1 credit. 2400-8000 minutes of internship=1 credit. This must match with the syllabus. See <http://www.uaf.edu/uafgov/faculty-senate/curriculum/course-degree-procedures-/guidelines-for-computing-/> for more information on number of credits.

OTHER HOURS (specify type)	NA
----------------------------	----

10. COMPLETE CATALOG DESCRIPTION including dept., number, title, credits, credit distribution, cross-listings and/or stacking (50 words or less if possible):

Example of a complete description:

FISH F487 W, O Fisheries Management
3 Credits Offered Spring
 Theory and practice of fisheries management, with an emphasis on strategies utilized for the management of freshwater and marine fisheries. *Prerequisites: COMM F131X or COMM F141X; ENGL F111X; ENGL F211X or ENGL F213X; ENGL F414; FISH F425; or permission of instructor. Cross-listed with NRM F487. (3+0)*

CITS F263 Network Security Penetration Testing
3 Credits Offered As Demand Warrants
 This course focuses on network and information systems security from an offensive point of view. Students will learn technical testing and examination techniques used to identify, validate and assess technical vulnerabilities within an enterprise. Topics include penetration testing methodology, footprinting and reconnaissance, scanning and enumeration, vulnerability validation, data collection and reporting. *Prerequisite: CITS F261 or equivalent skills. (3+0)*

11. COURSE CLASSIFICATIONS: Undergraduate courses only. Consult with CLA Curriculum Council to apply S or H classification appropriately; otherwise leave fields blank.

H = Humanities ☐ S = Social Sciences ☐

Will this course be used to fulfill a requirement for the baccalaureate core? If YES, attach form.	YES:	<input type="checkbox"/>	NO:	<input checked="" type="checkbox"/>
--	------	--------------------------	-----	-------------------------------------

IF YES, check which core requirements it could be used to fulfill:

O = Oral Intensive, Format 6 <input type="checkbox"/>	W = Writing Intensive, Format 7 <input type="checkbox"/>	Natural Science, Format 8 <input type="checkbox"/>
---	--	--

11.A Is course content related to northern, arctic or circumpolar studies? If yes, a "snowflake" symbol will be added in the printed Catalog, and flagged in Banner.

YES <input type="checkbox"/>	NO <input checked="" type="checkbox"/>
------------------------------	--

12. COURSE REPEATABILITY:

Is this course repeatable for credit?	YES <input type="checkbox"/>	NO <input checked="" type="checkbox"/>
---------------------------------------	------------------------------	--

Justification: Indicate why the course can be repeated (for example, the course follows a different theme each time).

NA

How many times may the course be repeated for credit?	NA	TIMES
If the course can be repeated for credit, what is the maximum number of credit hours that may be earned for this course?	NA	CREDITS
If the course can be repeated with variable credit, what is the maximum number of credit hours that may be earned for this course?	NA	CREDITS

13. GRADING SYSTEM: Specify only one. Note: Later changing the grading system for a course constitutes a Major Course Change.

LETTER: <input checked="" type="checkbox"/>	PASS/FAIL: <input type="checkbox"/>
---	-------------------------------------

RESTRICTIONS ON ENROLLMENT (if any)**14. PREREQUISITES**

CITS F261 or equivalent skills

These will be required before the student is allowed to enroll in the course.

Reference the registration implications below due to Banner coding of these terms:

Prerequisite: Course completed and grade of "C" (2.0) or higher prior to registering for the course that requires it.

Concurrent: Course may be taken simultaneously (and allows for a course to have been previously completed).

Co-requisite: Courses MUST be taken simultaneously and does NOT allow for fact that a course was previously completed!

15. SPECIAL RESTRICTIONS, CONDITIONS

None

16. PROPOSED COURSE FEES

None

Has a memo been submitted through your dean to the Provost for fee approval?

Yes/No

NA

17. PREVIOUS HISTORY

Has the course been offered as special topics or trial course previously?

Yes/No

No

If yes, give semester, year, course #, etc.:

NA

18. ESTIMATED IMPACT

WHAT IMPACT, IF ANY, WILL THIS HAVE ON BUDGET, FACILITIES/SPACE, FACULTY, ETC.

The IT Specialist program currently has sufficient resources (budget, facilities/space and faculty) to teach this proposed course and incorporate it into the IT Specialist program.

19. LIBRARY COLLECTIONS

Have you contacted the library collection development officer (kljensen@alaska.edu, 474-6695) with regard to the adequacy of library/media collections, equipment, and services available for the proposed course? If so, give date of contact and resolution. If not, explain why not.

No

Yes

X

Karen Jensen, the collection development officer for the library, was contacted by email on 9/17/2012. We don't anticipate the need for any library acquisitions.

20. IMPACTS ON PROGRAMS/DEPTS

What programs/departments will be affected by this proposed action? Include information on the Programs/Departments contacted (e.g., email, memo)

The IT Specialist program is the only program that will be affected by this proposed action.

21. POSITIVE AND NEGATIVE IMPACTS

Please specify **positive** and **negative** impacts on other courses, programs and departments resulting from the proposed action.

Positive Impacts: This course will serve as a required course for the Network and Cybersecurity concentration of the IT Specialist A.A.S. degree program. The content of this course enables students to build on the skills and knowledge developed in CITS F261 Computer and Network Security. In CITS F261 students are introduced to fundamental concepts of computer and network security. In this course, CITS F263, students will develop the knowledge and skills necessary to validate vulnerabilities and make recommendations about security improvements that should be made to better protect an organization's digital assets. The offering of this course will result in a workforce that is better prepared to assess an organization's current security state and protect the digital assets that exist within the environments in which they work.

Negative Impacts: No negative impacts are foreseen.

JUSTIFICATION FOR ACTION REQUESTED

The purpose of the department and campus-wide curriculum committees is to scrutinize course change and new course applications to make sure that the quality of UAF education is not lowered as a result of the proposed change. Please address this in your response. This section needs to be self-explanatory. Use as much space as needed to fully justify the proposed course.


Cybersecurity has been identified as one of the most serious economic and national security challenges we face as a nation. The National Initiative for Cybersecurity Education (NICE) was established to help face this challenge head on with a strategy to build a cyber savvy nation through training, awareness, K through post-graduate educational programs, and professional development for federal security professionals. (<http://www.nist.gov/itl/csd/nice.cfm>. Retrieved September 14, 2012.)

NICE's Strategic Plan, which is currently in a draft format, states within the Executive Summary that: "Our nation is at risk. The cybersecurity vulnerabilities in our government and critical infrastructure are a risk to national security, public safety, and economic prosperity. Now is the time to begin a coordinated national initiative focused on cybersecurity awareness, education, training, and professional development. The United States must encourage cybersecurity competence across the nation and build an agile, highly skilled workforce capable of responding to a dynamic and rapidly developing array of threats."

(http://csrc.nist.gov/nice/documents/nicestratplan/Draft_NICE-Strategic-Plan_Aug2011.pdf. Retrieved September 14, 2012).

The addition of this course to the IT Specialist program curriculum is an effort to begin addressing the need identified by NICE to increase the skills and knowledge within the cybersecurity workforce. Also, as mentioned above under item 21, this course will serve as a required course for the Network and Cybersecurity concentration of the IT Specialist A.A.S. degree program and the topics delivered through this course will serve as an essential for the cybersecurity courses used within this concentration. Without this course, graduates from this concentration area will not possess the in-depth knowledge of how to validate security vulnerabilities that exist within information systems and network infrastructure in which they work. The addition of this course will enable the IT Specialist degree program to better prepare students to meet employer expectations of today's IT worker.

APPROVALS: Add additional signature lines as needed.

	Date	09/27/2012
Signature, Chair, Program/Department of:		Computer and Information Technology Systems

	Date	10/4/12
Signature, Chair, College/School Curriculum Council for:		College of Rural and Community Development

	Date	10/5/12
Signature, Dean, College/School of:		College of Rural and Community Development

Offerings above the level of approved programs must be approved in advance by the Provost.

	Date	
Signature of Provost (if above level of approved programs)		

ALL SIGNATURES MUST BE OBTAINED PRIOR TO SUBMISSION TO THE GOVERNANCE OFFICE

	Date	
Signature, Chair		
Faculty Senate Review Committee: <input type="checkbox"/> Curriculum Review <input type="checkbox"/> GAAC		
<input type="checkbox"/> Core Review <input type="checkbox"/> SADAC		

ADDITIONAL SIGNATURES: (As needed for cross-listing and/or stacking)

	Date	
Signature, Chair, Program/Department of:		
	Date	
Signature, Chair, College/School Curriculum Council for:		
	Date	
Signature, Dean, College/School of:		

ATTACH COMPLETE SYLLABUS (as part of this application). The guidelines are online:

<http://www.uaf.edu/uafgov/faculty-senate/curriculum/course-degree-procedures-/uaf-syllabus-requirements/>

The Faculty Senate curriculum committees will review the syllabus to ensure that each of the items listed below are included. If items are missing or unclear, the proposed course (or changes to it) may be denied.

SYLLABUS CHECKLIST FOR ALL UAF COURSES

During the first week of class, instructors will distribute a course syllabus. Although modifications may be made throughout the semester, this document will contain the following information (as applicable to the discipline):

1. Course information:

☐ Title, ☐ number, ☐ credits, ☐ prerequisites, ☐ location, ☐ meeting time (make sure that contact hours are in line with credits).

2. Instructor (and if applicable, Teaching Assistant) information:

☐ Name, ☐ office location, ☐ office hours, ☐ telephone, ☐ email address.

3. Course readings/materials:

☐ Course textbook title, ☐ author, ☐ edition/publisher.
☐ Supplementary readings (indicate whether ☐ required or ☐ recommended) and
☐ any supplies required.

4. Course description:

☐ Content of the course and how it fits into the broader curriculum;
☐ Expected proficiencies required to undertake the course, if applicable.
☐ Inclusion of catalog description is *strongly* recommended, and
☐ Description in syllabus must be consistent with catalog course description.

5. ☐ Course Goals (general), and (see #6)

6. ☐ Student Learning Outcomes (more specific)

7. Instructional methods:

☐ Describe the teaching techniques (eg: lecture, case study, small group discussion, private instruction, studio instruction, values clarification, games, journal writing, use of Blackboard, audio/video conferencing, etc.).

8. Course calendar:

☐ A schedule of class topics and assignments must be included. Be specific so that it is clear that the instructor has thought this through and will not be making it up on the fly (e.g. it is not adequate to say "lab". Instead, give each lab a title that describes its content). You may call the outline Tentative or Work in Progress to allow for modifications during the semester.

9. Course policies:

☐ Specify course rules, including your policies on attendance, tardiness, class participation, make-up exams, and plagiarism/academic integrity.

10. Evaluation:

☐ Specify how students will be evaluated, ☐ what factors will be included, ☐ their relative value, and ☐ how they will be tabulated into grades (on a curve, absolute scores, etc.) ☐ Publicize UAF regulations with regard to the grades of "C" and below as applicable to this course. (Not required in the syllabus, but may be a convenient way to publicize this.) Faculty Senate Meeting #171:
<http://www.uaf.edu/uafgov/faculty-senate/meetings/2010-2011-meetings/#171>

11. Support Services:

☐ Describe the student support services such as tutoring (local and/or regional) appropriate for the course.

12. Disabilities Services: Note that the phone# and location have been **updated**.

The Office of Disability Services implements the Americans with Disabilities Act (ADA), and ensures that UAF students have equal access to the campus and course materials.

☐ State that you will work with the Office of Disabilities Services (208 WHITAKER BLDG, 474-5655) to provide reasonable accommodation to students with disabilities.

Course Syllabus
CITS F263 Network Security Penetration Testing
University of Alaska Fairbanks

Course Information

Course Number-Section, Title: CITS F263 Network Security Penetration Testing

Number of Credits: 3.0

Prerequisite: CITS 261 or permission of the instructor.

Class Location: CTC 604B, Room 316 (604 Barnette Street, Fairbanks AK)

Meeting Days & Time: Tuesday and Thursday, 3:40-5:10 PM, 8/30 – 12/14.

This course will consist of two 90 minute class lectures delivered to students twice a week for 14 weeks. Students can expected to spend an additional six to nine hours per week, outside of scheduled classroom lecture, studying lecture materials and completing reading assignments and homework. A final exam will be given during the 15th week.

Instructor Information

Name: Keith Swarner

Office Location: CTC 604B, Room 326 (604 Barnette Street, Fairbanks AK)

Student Office Hours: 2:00 pm – 4:30 pm Monday, Tuesday and Thursday or by appointment

Telephone: 455-2820

Email: keith.swarner@alaska.edu

Course Readings/Materials

Required textbook/materials:

Title: Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide

Author(s): Lee Allen

Publisher: Packt Publishing

ISBN13: 978-1849517744

Title: SP 800-115: Technical Guide to Information Security Testing and Assessment

Author(s): Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh

Publisher: US Department of Commerce, National Institute of Standards and Technology

Recommended textbook/materials: None

Course Description

This course focuses on network and information systems security from an offensive point of view. Students will learn technical testing and examination techniques used to identify, validate and assess technical vulnerabilities within an enterprise. Topics include penetration testing methodology, footprinting and reconnaissance, scanning and enumeration, vulnerability validation, data collection and reporting.

Course Goals

Upon successful completion of this course, the student will be able to define, explain, or perform tasks related to the following:

- 1.0 Penetration Testing and Assessment Methodology
- 2.0 Footprinting and Reconnaissance
- 3.0 Scanning and Enumeration
- 4.0 Vulnerability Validation Techniques
- 5.0 Maintaining Access
- 6.0 Data Collection and Reporting

Student Learning Outcomes

Upon successful completion of this course, the student will be able to:

- 1.1 Define penetration testing and the types of tests performed by a penetration tester (Black Box tests, White Box tests, and Grey Box tests).
- 1.2 Describe legal issues related to penetration testing and how the concepts of authorization, motivation and intent differentiate activities of a penetration tester from malicious attacker.
- 1.3 Identify and summarize important legal statutes and laws related to cyber crime and discuss their relevance to working as a penetration tester.
- 1.4 Identify the basic tools used to perform penetration testing.
- 1.5 Setup and configure a testing environment for penetration testing.
- 1.6 Describe the phases of a penetration test (reconnaissance, scanning and enumeration, vulnerability validation, maintaining access).
- 2.1 Explain the importance of gathering information about a target.
- 2.2 Describe techniques that can be used to passively gather information about a target.
- 2.3 Provide examples of first party sources of information and methods that can be used to obtain this information.
- 2.4 Demonstrate how to use Google and other search engines to obtain relevant information.
- 2.5 Provide examples of third party sources of information and methods that can be used to obtain this information.
- 2.6 Explain how to obtain information from DNS and the Regional Internet Registrars and how this information will be used as a part of the penetration test.
- 2.7 Use tools such as *Dig* and *Nslookup* to acquire system and address information about a target's network.
- 3.1 Explain what port scanning is and what can be learned from port scanning.
- 3.2 Identify the TCP Flags used within a TCP header and explain how these flags are used in different combinations during a communication session.
- 3.3. Explain the three-way handshake that occurs when TCP is used to establish a connection and the TCP Flags used during the three-way handshake.
- 3.4 Use discovery and scanning tools such as *Ping*, *Traceroute*, *Nmap* and *Hping* to enumerate systems and services available on a target network.
- 3.5 Use *Nmap* to perform different types of network scans and interpret the results; including, connect scans, UDP scans, SYN or half-open scans, FIN scans, Christmas scans, null scan, and ACK scans.
- 3.6 Explain how *Firewalking* can be used to determine which ports on a firewall are open.
- 3.7 Use the SNMP protocol to discover information about the devices running on a target network.
- 3.8 Identify tools and methods that can be used to fingerprint operating systems and services.
- 3.9 Use banner grabbing to fingerprint services running on a target system.
- 4.1 Describe password security and vulnerabilities associated with password security.
- 4.2 Describe the four primary methods used to compromise password security (Manual Guessing, Automated Dictionary Attack, Brute Force Attack, and Hybrid Attack).
- 4.3 Explain methods used by different operating systems and devices to store passwords.
- 4.4 Explain hashing and how it relates to password storage.
- 4.5 Explain the significance of the *SAM* file on a Windows system and methods that can be used to compromise the contents of this file.

- 4.6 Explain how tools such as *L0phtCrack* and *Cain and Able* can be used to compromise passwords on a Windows system.
- 4.7 Explain the significance of the *passwd* and *shadow* files on a Linux system and methods that can be used to compromise the contents of these files.
- 4.8 Explain how to use tools such as *John the Ripper* to compromise passwords on a Linux system.
- 4.9 Explain privilege escalation and methods that can be used to elevate privileges on a system.
- 4.10 Explain what a vulnerability assessment is and describe how it should and shouldn't be used as part of a penetration test.
- 4.11 Identify the tools that can be used to perform vulnerability assessments
- 4.12 Describe methods that can be used by a penetration tester to exploit vulnerabilities found on a target system.
- 4.13 Explain how to research, locate, and compile source code that can be used to exploit vulnerabilities found on a target system.
- 4.14 Explain how *Metasploit* is used to exploit vulnerabilities found on a target system.
- 4.15 Update the *Metasploit* framework
- 4.16 Explain how Trojan horses are used as a delivery mechanism for malicious code (rootkits, illicit servers, viruses, worms).
- 4.17 Explain how packfiles are created by combining together legitimate and illicit server binaries into a believable application.
- 4.18 Describe methods that can be used to compromise web servers and web applications; including, SQL injections, cross-site scripting (XSS), buffer overflows, and cookie editing.
- 5.1 Describe methods that can be used by a penetration tester to maintain access to a target system.
- 5.2 Explain how tools such as *netcat* and *cryptcat* can be used to establish and maintain communication sessions.
- 5.3 Explain how programs such as *Netbus* can be used to maintain access to a target system.
- 5.4 Explain how rootkits such as *Hacker Defender* can be used to maintain access to a target system.
- 6.1 Explain data collection methodologies and advantages and disadvantages of each methodology.
- 6.2 Identify data collection tools that can be used during a penetration test.
- 6.3 Identify key system data that should be collected during a penetration test.
- 6.4 Identify the minimum sections that should be included in any penetration testing report.
- 6.5 Create a well written executive summary, a well written detailed report that includes findings and an analysis of findings, and present raw output that includes log files and other evidence collected during the penetration test.

Instructional Methods

This course teaches students through lectures, demonstrations, and instructor-led discussions. Students are expected to complete required reading assignments prior to each lecture. Students are expected to complete assigned homework during the week that follows that topic's lecture and to arrive prepared to discuss homework at the beginning of the following week's class.

Course Policies

Attendance: You are expected to attend classes regularly; unexcused absences may result in a failing grade. You are responsible for coordinating absences and the possibility of arranging to make up missed work with the instructor prior to the absence.

If an unforeseen circumstance prevents you from attending class you are expected to contact the instructor via email or phone prior to the start of the next class.

Assignment Due Dates: Check the Course Schedule at the end of the class syllabus for assignment due dates. Assignments are due at 3:30 PM on the due date specified for the assignment.

Late Assignments: Assignments submitted after 3:30 PM on the assignment due date will be considered late. Late assignments will receive a 10% deduction for every day (24-hour period) past the assignment due date. Students must also notify the course instructor through email that the late assignment has been submitted or it will not be graded.

Missed Exams: There will be no opportunity to make exams except for absences that have been pre-arranged with the instructor. Make-up exams must be completed prior the next class meeting from which the exam was given.

Other Important Dates: Check the UAF Academic Calendar for important dates related to fee payment and the last day to drop or withdraw from courses. The calendar can be viewed online at: http://www.uaf.edu/catalog/current/acad_calendar.html

Plagiarism/Academic integrity: Plagiarism and cheating are serious offenses and may result in failure on exams, papers, projects, or courses. The standards in this class will follow the *Student Code of Conduct* policy stated in the current UAF Catalog.

Email: Students are expected to be able to receive email sent to their UAF email address and are expected to check email sent to this email address regularly. This expectation can be met by students either regularly checking their UAF email account or by forwarding their UAF email to an email address that they do regularly check. Information about email and email forwarding can be found online at www.uaf.edu/google/faqs/general/#mail. Further assistance can be obtained by contacting the Help Desk at 450-8300.

Support Services

The UAF Community and Technical College Student Assistance and Advising Center provides registration, placement assessments and financial aid services. Services are available on a walk-in basis at the, 604 Barnette Street, room 110. Appointments can be scheduled by calling 455-2800.

Disability Services

The UAF Office of Disability Services implements the Americans with Disabilities Act (ADA), and insures that UAF students have equal access to the campus and course materials. The instructor will work the Office of Disability Services to provide reasonable accommodations to students with disabilities documented through the UAF Office of Disability Services. Information is available online at www.uaf.edu/disability/. Their office can be reached by phone at 474-5655.

Evaluation:

Final grades are calculated from the points earned in the following areas:

Assignments250 pts

Assignments are intended to provide an opportunity to complete and receive instructor feedback on tasks and questions that will be tested on the mid-term and final exams.

Quizzes200 pts

Quizzes will be available on the class Blackboard site and will be completed outside of class. See the class schedule for quiz due dates.

Midterm Exam 100 pts

The midterm exam will provide an assessment of the students use and retention of course material covered in weeks 1-7.

Scenario Project250 pts

The scenario project will provide students to an opportunity to apply the skills and knowledge developed throughout the entire course. Students will be given a virtual environment in which they will need to perform a penetration test write up a report of findings.

Final Exam200 pts

The Final Exam is a comprehensive assessment of the student's use and retention of course material covered in weeks 1-15. Exam will consist of both short answer and scenario-based multiple choice questions designed to measure student competency in the student learning outcomes defined for this class.

Letter grades for the course will be determined as follows and will reflect the *Grading System and Grade Point Average Computation* policy stated in the current UAF Catalog.

A+ 1000–970 pts	A 969–930 pts	A- 929–900 pts
B+ 899–870 pts	B 869–830 pts	B- 829–800 pts
C+ 799–770 pts	C 769–730 pts	C- 729–700 pts
D+ 699–670 pts	D 669–630 pts	D- 629–600 pts
	F less than 600 pts	

Grade Required to Satisfy Degree Requirements – To use this course to satisfy requirements in the IT Specialist certificate or associate degree program, students must earn a course grade of C or better. A grade of "C-" is not sufficient to meet degree requirements.

Withdrawal – Course withdrawals may be either student-initiated or faculty-initiated. A faculty-initiated withdrawal will be initiated if you don't meet prerequisites for a course or if you haven't participated substantially in the course. An attempt will be made to contact students prior to initiating a faculty-initiated withdrawal. It is the responsibility of the student to maintain current contact information (phone number and email address) within UA Online system.

The deadline for student- or faculty-initiated withdrawals is Friday, October 26th.

Incomplete - An incomplete is a temporary grade used to indicate that the student has satisfactorily completed (C or better) the majority of work in a course but for personal reasons beyond the student's control, such as sickness, has not been able to complete the course during the regular semester. An incomplete will only be assigned in a case when the student is current in the class until at least the last three weeks of the course. Negligence or indifference is not acceptable reasons for an "I" grade. If a grade of incomplete is assigned, it must be made up within one year or it will automatically be changed to a grade of "F".

Course Calendar:

The following course calendar provides a schedule of major course topics, reading assignments, homework assignments, and quizzes and exams.

Wk No.	Class No.	Topic	Textbook Chapters	Assignment and Quiz Due Dates
1	1	<ul style="list-style-type: none">• Introduction to Penetration Testing• Determining Scope and Setting Limits	SP-800 115, Sec. 2 and 3 Chapter 1	
2	2	<ul style="list-style-type: none">• Installing and Exploring BackTrack	Chapter 1	
	3	<ul style="list-style-type: none">• Managing Test Results• Introduction to the Dradis Framework	Chapter 1	
3	4	<ul style="list-style-type: none">• Setting up a Virtual Environment for Penetration Testing	Chapter 10	<ul style="list-style-type: none">• Quiz 1 due• Assignment 1 due
	5	<ul style="list-style-type: none">• Setting up a Virtual Environment for Penetration Testing	Chapter 10	
4	6	<ul style="list-style-type: none">• Introduction to Reconnaissance• DNS Recon	Chapter 2	
	7	<ul style="list-style-type: none">• Gathering and Validating Ddomain and IP Information• Using Search Engines to Perform Recon	Chapter 2	
5	8	<ul style="list-style-type: none">• Network Discovery Techniques• Using Nmap to Scan Target Networks	SP-800 115, Section 4 Chapter 3	<ul style="list-style-type: none">• Quiz 2 due• Assignment 2 due
	9	<ul style="list-style-type: none">• Collecting Information with SNMP	Chapter 3	
6	10	<ul style="list-style-type: none">• Creating Network Baselines• Enumeration Avoidance Techniques	Chapter 3	
	11	<ul style="list-style-type: none">• Value of Exploitation as Part of a Pen Test• Manual Exploitation• Moving Files To and From Target Systems	Chapter 4	<ul style="list-style-type: none">• Quiz 3 due• Assignment 3 due
7	12	<ul style="list-style-type: none">• Compromising Passwords	SP-800 115, Section 5 Chapter 4	
	13	<ul style="list-style-type: none">• Using Metasploit	Chapter 4	
8	14	<ul style="list-style-type: none">• Midterm Exam		<ul style="list-style-type: none">• Quiz 4 due• Assignment 4 due
	15	<ul style="list-style-type: none">• Web Application Exploitation	Chapter 5	
9	16	<ul style="list-style-type: none">• SQL Injection; Cross-site Scripting (XSS), Cookie Editing	Chapter 5	
	17	<ul style="list-style-type: none">• Compromising Client Systems• Buffer Overflows	Chapter 6	

Course Syllabus: CITS 263 Network Security Penetration Testing

Wk No.	Class No.	Topic	Textbook Chapters	Assignment and Quiz Due Dates
10	18	<ul style="list-style-type: none"> Malware: Trojans, Rootkits, Backdoors, Viruses and Worms 	Chapter 6	<ul style="list-style-type: none"> Quiz 5 due Assignment 5 due
	19	<ul style="list-style-type: none"> Data gathering, Network Analysis, and Data Exfiltration 	Chapter 7	
11	20	<ul style="list-style-type: none"> Dradis Framework for Collaboration 	Chapter 7	<ul style="list-style-type: none"> Quiz 6 due Assignment 6 due
	21	<ul style="list-style-type: none"> Scanning Through the Firewall 	Chapter 8	
12	22	<ul style="list-style-type: none"> IDS Avoidance 	Chapter 8	<ul style="list-style-type: none"> Quiz 7 due Assignment 7 due
	23	<ul style="list-style-type: none"> Data Collection Methodologies Data Collection Tools 	SP-800 115, Sec. 6 and 7 Chapter 9	
13	24	<ul style="list-style-type: none"> Writing Penetration Reports 	SP-800 115, Section 8 Chapter 9	<ul style="list-style-type: none"> Quiz 8 due Assignment 8 due
	25	<ul style="list-style-type: none"> Scenario Project 		
14	26	<ul style="list-style-type: none"> Scenario Project 		
	27	<ul style="list-style-type: none"> Scenario Project 		<ul style="list-style-type: none"> Quiz 9 due Assignment 9 due
15	28	<ul style="list-style-type: none"> Final Exam 		