

Oklahoma State University Institute of Technology
Online Common Syllabus
Summer 2018

ITD 3443 Network Security

Students will provide Cyber Defense while understanding Cyber Threats. Their attack types and their vulnerabilities. Topics include: applications of cryptography, malicious activity detection, trust relationships, advisories and targets, motivations and techniques, and the Adversary Model.

Course Purpose:

This course allows students to work with labs considered vital to Ethical Hacking. Uses the Ethical Hacking guidelines for lab development.

Type of Course: Theory/Lab

Credit Hours: 3; Total clock hours of theory per semester: 30;

Total clock hours of lab per semester: 45; Total clock hours of clinical per semester: 0.

Class Length: Full Semester

Class Days and Times: Fully Online

Prerequisites: ITD3253 – Server Administration OR ITD3533 – Secure Server Administration

Instructor Name: Dr. Fil Guinn

Instructor Phone: (918) 293-5428

Office: EET/IT, Room 15C

Instructor email: fil.guinn@okstate.edu

Contact: My preferred method of contact is **email**. Please allow 24-48 hours to return your correspondence during the normal work week.

Instructor's Office Hours: Tuesday and Wednesday 6:30 – 8:30 PM, Tuesday & Thursday 10:00 AM – 3:00 PM, (Online, Phone and Email) Central Time

School: Information Technologies

School's Main Phone: 918-293-5440

REQUIRED TEXT, REFERENCES, AND MATERIALS

Texts: N/A, Purchase set of labs from infoseclearning.com or Bookstore

References: *The Hacker Playbook 2: Practical Guide to Penetration Testing*, Peter Kim. Secure Planet, LLC, ISBN: 9781512214567

Materials: Access to a computer with broadband Internet Access (2Mbps upload preferred).

Uniform/Tools: N/A

Estimated Cost for Materials: \$ 88 from infoseclearning.com

Estimated Cost for Uniform/Tools: \$ 102.75 from the bookstore

Optional Resources: Assorted YouTube videos

Upon completion of the course, students should:

Course Objectives

Assessment of Competency

Evaluate and document IT security risks and make recommendations for mitigation	*Course Project	E.1
Conduct network administration, maintenance, diagnostics, or testing	Lab assignments	J.1
Demonstrate knowledge of industry standard network classifications, topologies or network communication models	Lab assignments	M.2

Aspects of the course objective assessments may be used in the university’s assessment of student learning. If applicable, an asterisk (*) above indicates this assignment is used in the university assessment program.

COURSE ACTIVITIES

In this course students will:

(Please list the specific activities in the course)

- Using network sniffing software to analyze network traffic.
- Perform foot printing, scanning and enumeration.
- Perform and mitigate advanced network intrusions techniques.
- Develop firewall rule set.
- Use vulnerability assessment tools to analyze network hosts.
- Configure and secure wireless network.
- Install, configure and monitor intrusion detection software.

EVALUATION - GRADES WILL BE BASED ON THE QUALITY AND COMPLETION OF THESE TASKS:

Discussion Questions	10%
Faculty Contact.....	5%
Hands-On Labs.....	40%
Writing Assignments	25%
*Final Project	15%
Portfolio.....	5%
Total.....	100%

OSUIT Grading Scale
A = 90%-100%
B = 80%-89%
C = 70%-79%
D = 60%-69%
F = 59% & below

*The student’s grade for this assignment will be used in the university’s assessment of student learning. A 70% competency or higher receives a Pass rating. This Pass/Fail rating is independent of the student’s course grade.

Daily and/or weekly quizzes, small weekly assignments and similar type projects: Normal return time to student by next class meeting or no later than one (1) week.

Extensive assignments, large lab projects, extensive quizzes, exams and similar type projects: Normal return time to students in one (1) to two (2) weeks.

RECOMMENDED STUDENT COMPETENCIES/SKILLS

Recommended student skills needed for success are the following:

- Ability to access a website (Infoseclearning) and use the site to run computer simulations
- Ability to read and follow step by step instructions within the course site
- Ability you attend class during the required time
- Working understanding of PowerPoint and screen capture software

AUTHORIZED TOOLS

Students may use any/all course materials, including books and notes, while participating in online classroom activities. All quizzes, labs, and written assignments are to be completed independently and any instance of collaboration will be considered academic dishonesty. Collaboration with classmates while studying concepts and network configurations is permitted and encouraged.

LATE WORK

Turning in your properly-executed work early is always acceptable. All exams, assignments, papers and projects must be completed and submitted by the specified due date; late work will not be accepted after the due date unless prior authorization is given.

If the faculty member grades an assignment you have submitted before the due date, you do not have the ability to modify the assignment to increase your grade. Any additional submissions will not be opened, so make sure you are ready to submit your assignments and accept the grade you are given.

TESTING

Quizzes may be timed or proctored during this course.

OTHER LAB AND CLASSROOM POLICIES

No food or drink is allowed in the computer labs

ONLINE COURSE INTERACTION

OSUIT requires all online courses to include interaction between students, peers and instructors. Our online courses use a variety of tools to build a community of learners and strengthen engagement between students and their peers, as well as between students and the instructor. Communication tools used in courses may include Discussion, News, and Email. Read the syllabus completely to determine which of these methods you, your classmates and your instructor will use for interaction. General guidelines for student conduct while interacting within an online course include: (1) Use proper language in all communications; (2) Harassment of any type will not be tolerated; (3) No jokes, insults or threats of an offensive nature.

For more information, go to: <http://osuit.edu/center/netiquette>

SYLLABUS ATTACHMENT

View the Syllabus Attachment, which contains other important information, by visiting http://osuit.edu/center/student_syllabus_information

Course Schedule			
Schedule	Topic	Assignment	Due Date
Week 1	Module One Performing Reconnaissance from the WAN	Assignments: Labs on infoseclearning.com Assessments Research Questions	5/6/2018
Week 2	Module Two Scanning the Network on the LAN	Assignments: Labs on infoseclearning.com Assessments Research Questions	5/13/2018
Week 3	Module Three Enumerating Hosts Using Wireshark, Windows, and Linux Commands	Assignments: Labs on infoseclearning.com Assessments Research Questions	5/20/2018
Week 4	Module Four Remote and Local Exploitation	Assignments: Labs on infoseclearning.com Assessments Research Questions	5/27/2018
Week 5	Module Five Using the Dark Comet Remote Access Trojan (RAT)	Assignments: Labs on infoseclearning.com Assessments Research Questions	6/3/2018
Week 6	Module Six Capturing and Analyzing Network Traffic Using a Sniffer	Assignments: Labs on infoseclearning.com Assessments Research Questions	6/10/2018
Week 7	Module Seven Using SET (Social Engineering Toolkit)	Assignments: Labs on infoseclearning.com Assessments Research Questions	6/17/2018
Week 8	Module Eight Performing a Denial of Service Attack from the WAN	Assignments: Labs on infoseclearning.com Assessments Research Questions	6/24/2018
Week 9	Module Nine Using Browser Exploitation to Take Over a Host's Computer	Assignments: Labs on infoseclearning.com Assessments Research Questions	7/15/2018
Week 10	Module Ten Attacking Webservers from the WAN & Exploiting a Vulnerable Web Application	Assignments: Labs on infoseclearning.com Assessments Research Questions	7/22/2018
Week 11	Module Eleven Breaking WEP and WPA and Decrypting the Traffic	Assignments: Labs on infoseclearning.com Assessments Research Questions	7/29/2018

Week 12	Module Twelve Attacking the Firewall and Stealing Data Over an Encrypted Channel	Assignments: Labs on infoseclearning.com Assessments Research Questions	8/5/2018
Week 13	Module Thirteen Using Public Key Encryption to Secure Messages	Assignments: Labs on infoseclearning.com Assessments Research Questions	8/12/2018
Week 14	Module Fourteen Performing SQL Injection to Manipulate Tables in a Database	Assignments: Labs on infoseclearning.com Assessments Research Questions	8/19/2018
Week 15	Module Fifteen Final Project & Portfolio	Final Project Portfolio (with copy of Project)	8/21/2018 8/23/2018

Schedule is subject to change at instructor discretion.