

**Oklahoma State University Institute of Technology**  
**Online Common Syllabus**  
**Fall 2017**

**ITD 3533 Secure System Administration**

Students learn to secure systems and networks from threats and vulnerabilities. Topics include IDP/IDS and firewall implementation, defense in depth, network monitoring and traffic analysis, DMZs and Proxy servers, policy development and enforcement, networking hardening and attacks.

**Course Purpose:**

Focuses on the security of Windows and Linux servers using native security tools. Designed to give students experience using these different tools.

**Type of course:** Theory/Lab.

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

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

**Class length** - Full Semester

**Class format** - Fully Online

**Class Days and Times:** N/A

**Prerequisites:** ITD 1243, ITD 2223

**Instructor Name:** Dr. Fil Guinn

**Instructor Phone:** (918) 293-5428

**Office:** EET/IT, Room 15C

**Instructor email:** [fil.guinn@okstate.edu](mailto: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:** Monday and Wednesday 6:30 – 8:30 PM (Online, Phone and Email), Tuesday & Thursday 9:30 – 11:30 AM (On Campus) PLUS should be available in my office during the Study Hall, Monday-Thursday, 3-4PM, Central Time

**School Name:** Information Technologies

**School's Main Phone:** 918-293-5440

**REQUIRED TEXT, REFERENCES, AND MATERIALS**

**Texts:** *Getting Started with Windows Server Security*, Santhosh Sivarajan, Packet Publishing ISBN-13: 978-1-78439-872-9 AND *Linux Server Security, Hack and Defend*, Chris Binne, Wiley ISBN-13: 978-1-119-27765-1

**References:** Assorted Subject Videos

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

**Uniform/Tools:** None

**Estimated Cost for Materials:** \$ 113.75

**Estimated Cost for Uniform/Tools:** \$ None

**Optional Resources:** Assorted YouTube videos

Upon completion of the course, students should:

Course Objectives	Assessment of Objectives	
Evaluate and document IT security risks and make recommendations for mitigation	*Course Project	E.1
Implement systems integration practices for specific processes on enterprise IT system components	*Course Project	L.1
Create a comprehensive security plan, set of policies or procedures to protect the IT assets of an organization	*Course Project	L.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:

- Participate in online discussions and activities
- Use a virtual network environment to use software
- Reply to chapter questions and definitions
- View course specific video presentation
- Complete chapter quizzes
- Complete a Final Exam
- Complete a course project
- Compile a portfolio of work produced

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

Discussions .....	10%
Faculty Contact.....	5%
Hands-on Projects .....	45%
Research Questions .....	20%
*Course Project .....	15%
Portfolio .....	5%
<b>Total</b> .....	<b>100%</b>

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 OSUIT vSphere environment
- Ability to run virtual computers
- Ability to read and follow step by step instructions within the course site
- Ability you complete all required assignments within the allotted time
- Ability to research related topics and use MLA formatted in-text citations
- Ability to build a MLA formatted Work Cited page for all research cited

## **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**

N/A

## **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](http://osuit.edu/center/student_syllabus_information)

## Course Schedule

Schedule	Topic	Assignment	Due Date
Week 1	<b>Getting Started</b> Online Orientation Partner Selection	Reading assignment – Preface. Online Orientation. Assignment –Partner selection	<b>9/10/2017</b>
Week 2	<b>Module One</b> Chapter 1 – Operating System & Baseline Security	Assignments – Chapter Labs Discussion responses Assessments: Research Questions	<b>9/17/2017</b>
Week 3	<b>Module Two</b> Chapter 2 – Native MS Security Tools and Configuration	Assignments – Chapter Labs Required Faculty Contact Assessments: Research Questions	<b>9/24/2017</b>
Week 4	<b>Module Three</b> Chapter Three – Server Roles and Protocols	Assignments – Chapter Labs Discussion responses. Assessments: Research Questions	<b>10/1/2017</b>
Week 5	<b>Module Four</b> Chapter Four – Application Security	Assignments – Chapter Labs Discussion responses. Assessments: Research Questions	<b>10/8/2017</b>
Week 6	<b>Module Five</b> Chapter Five – Network Service Security	Assignments – Chapter Labs Required Faculty Contact Assessments: Research Questions	<b>10/15/2017</b>
Week 7	<b>Module Six</b> Chapter Six – Access Control	Assignments – Chapter Labs Discussion responses. Assessments: Research Questions	<b>10/22/2017</b>
Week 8	<b>Module Seven</b> Chapter Seven – Patch Management	Assignments – Chapter Labs Discussion responses. Assessments: Research Questions	<b>10/29/2017</b>
Week 9	<b>Module Eight</b> Chapter Eight – Auditing and Monitoring	Assignments – Chapter Labs Required Faculty Contact Assessments: Research Questions	<b>11/5/2017</b>
Week 10	<b>Module Nine</b> Chapter One – Invisibility Cloak & Chapter Two – Digitally Fingerprint Your Files	Assignments – Chapter Labs Discussion responses. Assessments: Research Questions	<b>11/12/2017</b>
Week 11	<b>Module Ten</b> Chapter Three – Twenty-First-Century Netcat & Chapter Four – Denying Service	Assignments – Chapter Labs Discussion responses. Assessments: Research Questions	<b>11/19/2017</b>
Week 12	<b>Module Eleven</b> Chapter Five – Nping & Chapter Six – Logging Reconnoiters	Assignments – Chapter Labs Discussion responses. Assessments: Research Questions	<b>11/26/2017</b>

Week 13	<b>Module Twelve</b> Chapter Seven – Nmap's Prodigious NSE & Chapter Eight – Malware Detection	Assignments – Chapter Labs Discussion responses. Assessments: Research Questions	<b>12/3/2017</b>
Week 14	<b>Module Thirteen</b> Chapter Nine – Password Cracking with Hashcat & Chapter Ten – SQL Injection Attacks	Assignments – Chapter Labs Discussion responses. Assessments: Research Questions	<b>12/10/2017</b>
Week 15	<b>Module Fourteen</b> Final Project & Portfolio	<b>Final Project</b> <b>Course Portfolio</b>	<b>12/12/2017</b> <b>12/14/2017</b>

Schedule is subject to change at instructor discretion.