

CSIS 3758 - Ethical Hacking

Fall 2026 Syllabus, Section 01, CRN 43951,

Credit hours: 3

Instructor

Todd Jones

Email: tajones01@ysu.edu

Public Instructor Information

Instructor Title: Senior Lecturer

Instructor Professional Qualifications: Master of Computing Information Systems, Youngstown State University, 2019

Instructor Office Location: Meshel Hall 308

Instructor Office Phone: 330-941-1341

Course Description

3758. Ethical Hacking. Application of tools and methodologies used in cyber security. Analysis of threat actors' methods and how to defend against them. Methods and tools on securing enterprise infrastructure including network access and communication security. Prereq.: CSIS 3755. 3 s.h.

Course Readings

Group	Title	Author	ISBN
Optional	o CompTIA PenTest+ Guide to Penetration Testing	Robert S. Wilson	9780357950654

The course readings are subject to change in the event of extenuating circumstances, research developments, current events, and/or to ensure better learning.

Tentative Course Schedule

Week of	Reading(s)	Proposed Topic	Due/To Prepare for Class
8/24	Module 1	Introduction to Ethical Hacking and Penetration Testing.	• Research Pentesting Career Paths and Certifications • Set up the VM • Module 1 Exam
8/31	Module 2	Planning and Scoping a Penetration Testing Assessment	• Compliance Requirements and Local Restrictions Lab • Pre-Engagement, Scope and Planning
9/7	Module 2 and 3	Module 2: Planning and Scoping a Penetration Testing Assessment Module 3: Information Gathering and Vulnerability Scanning	• Pentesting Agreement • Codes of Conduct • Module 2 Exam • Module 3 Labs: OSINT Tools, DNS Lookups, Employee Intelligence Gathering
9/14	Module 3	Information Gathering and Vulnerability Scanning	• Module 3 Labs: File Meta Data, SSL Certificates, Shodan Searches, NMAP, Network Sniffing, Packet Crafting with Scapy
9/21	Module 3	Information Gathering and Vulnerability Scanning	• Module 3 Labs: Vulnerability Scans, How to deal with Vulnerability • Module 3 Exam
9/28	Module 4	Social Engineering Attacks	• Labs: Explore SET and use the BeEF tool • Module 4 Exam
10/5	Module 5	Exploiting Wired and Wireless Networks	• Labs: Server Message Block Vulnerability scans with enum4linux, Attacks with Ettercap



10/12	Module 5 and Review	: Exploiting Wired and Wireless Networks	Module 5 Exam, Midterm
10/19	Module 6	Exploiting Application-Based Vulnerabilities https://www.offsec.com/kali-training/?utm_source=kali&utm_medium=web&utm_campaign=t	• Labs: Website Vulnerabilities, Greenbone Vulnerability Manager. Injection Attacks • Create an account at this link: https://www.offsec.com/kali-training/?utm_source=kali&utm_medium=web&utm_campaign=t
10/26	Module 6	Exploiting Application-Based Vulnerabilities	• Labs: Password Tools, Cross Site Scripting, OWASP Web Security Guide • Module 6 Exam
11/2	Module 7	Cloud, Mobile, and IoT Security	• Lab: IoT Vulnerabilities • Module 7 exam
11/9	Module 8	Performing Post-Exploitation Techniques	• Lab: Steganography • Module 8 Exam
11/16	Module 9	Reporting and Communication	• Labs: Explore PenTest Reports, Expert Recommendation for Remediation • Module 9 Exam
11/23	Module 10	Tools and Code Analysis	• Labs: Analyze Exploit and Automation Code
11/30	Module 10	Tools and Code Analysis	• Module 10 Exam
12/7	Review	Final	Final Exam

The course schedule, policies, procedures, and assignments in this course are subject to change in the event of extenuating circumstances, by mutual agreement, and/or to ensure better learning.