Course Syllabus

Course Prefix, Number, and Title:

CSC 436 – Offensive Network Security

Credits:

3

University name:

Dakota State University

Academic term/year:

Fall 2017

Last date to Drop and receive 100% refund:

8/31/2017

Last date to Withdraw and earn a grade of 'W':

11/3/2017

Course meeting time and location:

Section D01: TTH 11:00 – 12:15, Beacom Institute of Technology 231
Section D02: TTH 9:30 – 10:45, Beacom Institute of Technology 231

Instructor information:

Name:

Cody Welu

Office:

East Hall 6

Phone number(s):

(507) 828-8315

Email address:

Cody.Welu@dsu.edu

Office hours:

Please see the D2L site for the most up-to-date list of office hours.

I'm often in my office or on campus outside of scheduled office hours, feel free to drop me an email any time, and we can setup a time to meet that's convenient for both of us.

Approved course description:

Catalog description:

This course provides theoretical and practical aspects of Network Penetration Testing. The course includes in-depth details and hands on labs for each of the five distinct phases of an ethical hack including reconnaissance, scanning and vulnerability assessment, gaining access and exploitation, maintaining access, and covering tracks. An applied approach with a focus on current tools and methodologies will be stressed.

Prerequisites:

Course prerequisite(s):

CSC 328 + CIS 385

Technology skills:

Students should be comfortable with the basic operation of their computer, including Windows 10 and Microsoft Office. A DSU –issued tablet is required for on campus students. Those students who choose to opt out of the tablet program are solely responsible for meeting any technology requirements.

Students will need to have an in-depth understanding of networking, Windows and Linux operating systems, and virtualization. Students should also know of and be familiar with basic network services such as SSH, FTP, HTTP(S), DNS, etc.

Course materials:

Required textbook(s):

The Hacker Playbook 2: Practical Guide To Penetration Testing
Peter Kim
ISBN-10: 1512214566

Optional materials:

Basics of Hacking & Penetration Testing, 2nd Ed
Engebretson
ISBN-10: 0124116442

Required supplementary materials:

Students must have high-speed internet access and administrative permissions on their PC.

Course delivery and instructional methods:

Instructional methods will include the use of labs, lecture slides, notes, textbook, e-mail, and student presentation. Your instructor will serve as a mentor a guide. You will be responsible for keeping up with the course material.

Classroom policies:

IA Lab Policy

We will make DSU's IA lab available for use to all students of this class. The lab will be used to provide software in the event that you do not have the software available. The IA lab will have scheduled downtime from time to time. A schedule or notice of this downtime will be posted in advance (or at www.twitter.com/dsuia) . Missing an assignment due to difficulties accessing the lab is not an acceptable excuse.

Attendance and make-up policy:

It is expected that students attend and participate in the lecture. Assignments will largely be based on the material covered in the lectures. Assignments must be turned in on time. Late assignments will not be accepted, **no exceptions**.

Quizzes and exams are to be taken within the given/assigned time frame or PREVIOUSLY arranged with the instructor.

Students are expected to check their DSU email and the D2L course site daily to ensure important changes or assignment updates are communicated.

Note: It is the unfortunate truth that major life events (e.g. demise of a loved one) may pull us away from learning objectives and schedules. Please let me know as soon as possible if you are experiencing or expect to experience such an event and I will be more than happy to work with you. This communication needs to happen **before** deadlines of assignments, quizzes, tests, etc. to be able to accommodate your situation.

ADA Statement:

If you have a documented disability and/or anticipate needing accommodations (e.g., non-standard note taking, extended time on exams or a quiet space for taking exams) in this course, please contact the instructor. Also, please contact Dakota State University's Disabilities Office by calling 605-256-5121 or emailing Success.Center@dsu.edu as soon as possible. The DSU website contains additional information and the form to request accommodations found at https://portal.sdbor.edu/dsu-student/student-resources/disability-services/Pages/default.aspx/. (Students must log into the DSU portal to access this page.) You will need to provide documentation of your disability. The Disabilities Office must confirm the need for accommodations before officially authorizing them.

Academic Honesty Statement:

Cheating and other forms of academic dishonesty run contrary to the purpose of higher education and will not be tolerated in this course. Please be advised that, when the instructor suspects plagiarism, the Internet and other standard means of plagiarism detection will be used to resolve the instructor's concerns. DSU's policy on academic integrity (DSU Policy 03-22-00) is available online.

All forms of academic dishonesty will result in a zero for the assignment

Freedom in Learning Statement:

Students are responsible for learning the content of any course of study in which they are enrolled. Under Board of Regents and University policy, student academic performance shall be evaluated solely on an academic basis and students should be free to take reasoned exception to the data or views offered in any course of study. It has always been the policy of Dakota State University to allow students to appeal the decisions of faculty, administrative, and staff members and the decisions of institutional committees. Students who believe that an academic evaluation is unrelated to academic standards but is related instead to judgment of their personal opinion or conduct should contact the dean of the college which offers the class to initiate a review of the evaluation.

University Policy Regarding the Use of Tablets in the Classroom:

The Tablet PC platform has been adopted across the DSU campus for all students and faculty, and tablet usage has been integrated into all DSU classes to enhance the learning environment. Tablet usage for course-related activities, note taking, and research is allowed and encouraged by DSU instructors. However, inappropriate and distracting use will not be tolerated in the classroom. Instructors set policy for individual classes and are responsible for informing students of class-specific expectations relative to Tablet PC usage. Failure to follow the instructor's guidelines will hinder academic performance and may lead to disciplinary actions. Continued abuse may lead to increased tablet restrictions for the entire class.

Because tablet technology is an integral part of this course, it is the student's responsibility to ensure that his/her Tablet PC is operational prior to the beginning of each class period.

Communication and Feedback:

Preferred Email Contact Method:

Cody.Welu@dsu.edu
Do NOT use D2L email.

Email Response Time:

Usually within 24 hours, could be longer on weekends and holidays.

Feedback on Assignments:

Students will usually receive feedback within one week after the due date.

Course Goals:

Students will learn proper tools and techniques for conducting penetration testing and security audits. Students will be able to demonstrate an understanding of and apply skills in the following areas:

- Phases of penetration testing: reconnaissance, scanning, exploitation, post exploitation & maintaining access, and reporting.
- Gathering open source intelligence (OSINT) information from a variety of sources.
- Advanced search operators to find and profile information passively.
- Active port scanning techniques.
- Vulnerability scanning with multiple products and custom scripts, along with interpreting and understanding the results.
- Exploitation of systems using open source and custom developed scripts and code.
- Pivoting through a system to attain higher levels of access, privilege escalation, or a more favorable standpoint in the network.
- Maintaining access, installing backdoors, and establishing persistence in a network.
- Reporting and interpreting results to clearly demonstrate vulnerabilities within a framework.

Evaluation Procedures:

Assessments:

Labs
Research Assignments
Quizzes
Exams

Attendance checks/challenges

Final examination:

D01 – Thursday, December 7, 10:30 – 12:30
D02 – Tuesday, December 12, 10:30 – 12:30

Performance standards and grading policy:

Students are expected to successfully complete all assigned labs and assignments, and correctly respond to all examinations given.

Grading will be on a point-by-point basis. The final letter grade will be based on the following scale:

90% - 100%	"A"
80 - 89.9%	"B"
70 - 79.9%	"C"
60 - 69.9%	"D"
Less than 60%	"F"