Air Force Institute of Technology
Graduate School of Engineering and Management
Department of Electrical and Computer Engineering

CSCE 629
Cyber Attack
Course Syllabus

Winter Quarter 2019

Meeting times Class	1400-1600 Tuesday & Thursday
Lab	1600-1700 Tuesday & Thursday
Location	Building 646, Room 204 (GECO Lab)
Instructor	Dr. Barry E. Mullins
Office location	Building 642, Room 209
Office hours	By appointment or as available. Please feel free to drop in anytime that I'm in the office. If I don't have time to meet with you then, we can at least set a time to meet. I prefer you make appointments via email.
Contact information	barry.mullins@afit.edu / (937) 255-3636 ext 7979

Course Description

Course provides an introduction to cyber attack. Students learn to apply exploitation and attack methods to design and execute a viable attack strategy against computer systems/networks and humans using tools and techniques via hands-on labs and projects. Topics include identifying targets, reconnaissance, enumeration and scanning, gaining unauthorized access, denial of service attacks, maintaining access, and hiding attack evidence.

Credits	4
Prerequisites	CSCE 560 or permission of instructor

Student Learning Objectives

1	Understand the basic concepts, terminology and resources used in information security.
2	Understand cyber attack methodologies based on stated policies, requirements and threats.
3	Apply structured exploitation and attack methods to design a viable attack strategy.
4	Demonstrate the ability to identify target computer systems.
5	Demonstrate the ability to perform basic enumeration and scanning of computer systems.
6	Demonstrate the ability to gain unauthorized access to a computer system.
7	Demonstrate the ability to attack confidentiality (cracking, sniffing), authenticity (spoofing), availability (denial-of-service) and integrity (buffer-overflows/Trojan-horse).
8	Demonstrate the ability to gather information from a target computer system.
9	Demonstrate the ability to hide attack occurrence and assess attack success.

Required Books and Resource Materials

- *Counter Hack Reloaded - A Step-by-Step Guide to Computer Attacks and Effective Defenses*, 2nd edition (January 2, 2006; most current is 9th printing), by Ed Skoudis and Tom Liston, Prentice Hall, ISBN 0131481045

Recommended/Optional Books and Resource Materials

- *RTFM: Red Team Field Manual*, Clark 2014
- *BTFM: Blue Team Field Manual*, White 2017
- *BackTrack 5 Wireless Penetration Testing Beginners Guide*, Vivek Ramachandran, 2011.
- *Hacking The Art of Exploitation*, 2nd ed, Erickson, 2008.
- *Metasploit: The Penetration Tester's Guide*, David Kennedy et al., 2011.
- *Hacking Exposed*, 7th ed by Stuart McClure et al., 2012, .
- *Hacking Web Applications Exposed*, Joel Scambray and Mike Shema, 3rd ed., 2010.
- *Gray Hat Hacking: The Ethical Hacker's Handbook*, Daniel Regalado, et al., 2015.

Grading Scheme/Policy

Grading:	Exam (week 8)	25%
	Final Project (weeks 7-10)	35%
	Homework/Labs (6)	30%
	Class Project (Python tools)	10%

Examinations: One exam will be given for this course. This exam is tentatively scheduled for week eight. The exam is to be worked solely by the individual. There is to be no collaboration of work on the exam. Whether the exam will be in-class or take-home is TBD. Quizzes may also be given throughout the quarter.

Final project: The final project ties together (synthesizes) everything you learned during the quarter. It assesses how well you understand exploitation using various techniques and tools in an attempt to compromise an organization to harvest information and gain unauthorized access. It also assesses how well you document the attack methodology and results.

Homework/Labs: The homework, labs and class projects are intended to have the students apply principles discussed in class and to gain familiarity with cyber attack tools and techniques. You may collaborate to complete the homework assignments, but the work you submit must not be copied from anyone. Submit a hardcopy during class unless told otherwise. Please do not email your work. Please do not "drop off" your work at my office.

The numerical to letter grade distribution is as follows:

Grade	Grade Point Equivalent	Percent Equivalent
A	4.0	93.0-100.0
A-	3.7	90.0-92.9
B+	3.3	87.1-89.9
B	3.0	83.0-87.0
B-	2.7	80.0-82.9
C+	2.3	77.1-79.9
C	2.0	73.0-77.0
C-	1.7	70.0-72.9
D+	1.3	67.1-69.9
D	1.0	60.0-67.0
F	0.0	below 60.0

Policies

1. **Attendance**: Attendance at all class sessions and exams is mandatory for military and civilians assigned to AFIT as full-time students except for extenuating circumstances. Scheduled classes and exams are defined by the instructor and they are documented in the course schedule. Part-time students are expected to attend scheduled classes, and absences should be explained to the instructor. The student should provide advance notice, if possible. (References: Student Handbook, Graduate School Catalog)

2. **Academic Integrity**: All students must adhere to the highest standards of academic integrity. Students are prohibited from engaging in plagiarism, cheating, misrepresentation, or any other act constituting a lack of academic integrity. Failure on the part of any individual to practice academic integrity is not condoned and will not be tolerated. Individuals who violate this policy are subject to adverse administrative action including disenrollment from school and disciplinary action. Individuals subject to the Uniform Code of Military Justice may be prosecuted under it. Violations by government civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. (References: Student Handbook, ENOI 36 – 107, Academic Integrity)

3. **Academic Grievance**: AFIT and the Graduate School of Engineering and Management affirm the right of each student to resolve grievances with the Institution. Students are guaranteed the right of fair hearing and appeal in all matters of judgment of academic performance. Procedures are detailed in ENOI 36 – 138, Student Academic Performance Appeals.

4. **Late Assignments and Make-ups**: The late penalty for work not submitted on time is as follows:

1 business day	-10%
2 business days	-30%
3 business days	-60%
4 business days	-100%

5. **Recording Lectures:** You may not record the lectures. Non-Attribution – What you say in class will not be attributed to you if and when your thoughts or ideas are repeated outside of class --AFIT Faculty Handbook 2014 and AU Instruction 36-2305

Tentative Schedule

This schedule is tentative and is subject to (and probably will) change.

CSCE 629 Schedule - Winter 2019

Class number	Date	Text Chapter	Topic	Slide set
1,2	3-Jan		Course Overview	0 - Course Overview
		1	Intro to Cyber Attack	1 - Intro
3,4	8-Jan	5	Reconnaisance	2 - Reconnaissance
5,6	10-Jan	6	Network Mapping Nmap Finding Open Ports Vulnerability Scanning Nexpose	3 - Scanning
7,8	15-Jan	6	IDS / IPS Evasion Shares	3 - Scanning
9,10	17-Jan	7	Buffer Overflows Metasploit	4 - Exploit - OS-App attacks
11		7	Maneuver / Pivoting Armitage	4 - Exploit - OS-App attacks
12	22-Jan	7	Password Guessing Password Cracking	5 - Exploit - Password attacks
13,14	24-Jan	7	Password Storage Retrieving Passwords Cain John the Ripper Pass the Hash Windows Tokens	5 - Exploit - Password attacks
15,16	29-Jan	7	Session Tracking Burp Proxy SQL Injection Command Injection WebGoatClient-Side Attacks Browser Exploitation Framework SET Heartbleed	6 - Exploit - Web app attacks
17,18	31-Jan	8	Sniffing ARP cache poisoning IP Address Spoofing Session Hijacking Ettercap Ncat	7 - Exploit - Network attacks
		8	Proxy Chains	7 - Exploit - Network attacks
19,20	5-Feb		Wardriving Kismet	8 - Exploit - Wireless attacks
21,22	7-Feb		WEP Cracking WEP	8 - Exploit - Wireless attacks
23,24	12-Feb		Cracking WEP WPA Attacking WPA	8 - Exploit - Wireless attacks

25		9	Malformed Packet Attacks SYN Floods Distributed DoS	9 - Exploit - DoS attacks
26	14-Feb	10	Trojan Horses Backdoor Factory Rootkits	10 - Maintain Access
			Event Logs Hidden Files Covert Channels Steganography	11 - Covering Tracks
27,28	19-Feb			**Exam**
29,30	21-Feb			Final Project
31,32	26-Feb			Final Project
33,34	28-Mar			Final Project
35,36	7-Mar			Final Project
37,38	7-Mar			Final project due - 8 March 2018, 1700

The course syllabus is a general plan for the course; deviations announced to the class by the instructor may be necessary.