North Central State College
MASTER SYLLABUS
2019-2020

A.   <u>Academic Division</u>: Business, Industry, and Technology

B.   <u>Discipline</u>: Information Technology – Cyber Security

C.   <u>Course Number and Title</u>: ITEC1430 – Certified Ethical Hacker (CEH)

D.   <u>Course Coordinator</u>: Mohamed Ghonimy
                 <u>Assistant Dean</u>: Toni Johnson, PhD

            <u>Instructor Information</u>:
- Name: Click here to enter text.
- Office Location: Click here to enter text.
- Office Hours: Click here to enter text.
- Phone Number: Click here to enter text.
- E-Mail Address Click here to enter text.

E.   <u>Credit Hours</u>: 3
             Lecture: 2 hours
             Laboratory: 3 hours

F.   <u>Prerequisites</u>: ITEC1640 (minimum grade of C-), ITEC1650 (minimum grade of C-), ITEC1840 (minimum grade of C-), ITEC2420c (minimum grade of C-)

G.   <u>Syllabus Effective Date</u>: Fall 2019

H.   <u>Textbook(s) Title</u>:

CEH Vol 1: Ethical Hacking Concepts and Methodology Version 10 eBook with iLabs
- Authors: EC Council
- Copyright Year: 2018
- Edition: 1st
- ISBN: 9781635672169

CEH Vol 2: Attach Vectors and Countermeasures Version 10 eBook with iLabs
- Authors: EC Council
- Copyright Year: 2018
- Edition: 1st
- ISBN: 9781635672176

<u>Workbook(s) and/or Lab Manual</u>: None

J.   <u>Course Description</u>: This ethical hacking and countermeasures course prepares students for EC-Council's Certified Ethical Hacker (CEH) exam. The course focuses on hacking techniques and technology from an offensive perspective. The student will learn to scan, test, hack and secure systems. Students will learn the five phases of ethical hacking: reconnaissance; gaining access; enumeration; maintaining access; and covering their tracks. Throughout the course, students will be immersed in a hacker's mindset, evaluating not just logical, but physical security exploring every possible point of entry to find the weakest link in an organization.

K.   College-Wide Learning Outcomes:

College-Wide Learning Outcome	Assessments - - How it is met & When it is met
Communication – Written	
Communication – Speech	
Intercultural Knowledge and Competence	
Critical Thinking	
Information Literacy	
Quantitative Literacy	

L.   Course Outcomes and Assessment Methods:

Upon successful completion of this course, the student shall:

Outcomes	Assessments – How it is met & When it is met
1. Describe security issues affecting networks and network security	Weeks 1-2 labs, midterm/final exam
2. List the various types of Footprinting and Footprinting tools	Weeks 3-4 labs, midterm/final exam
3. Compare and contrast network scanning and sniffing techniques and associated countermeasures	Weeks 5-6 labs, midterm/final exam
4. Explain social engineering, identity theft, and associated social engineering techniques	Weeks 7-8 labs, midterm/final exam
5. Demonstrate DOS/DDOS, botnets, DDOS attacks and DOS/DDOS countermeasures for a given set of conditions	Weeks 9-10 labs, final exam
6. Demonstrate wireless hacking methodologies using a variety of tools for a given set of conditions	Weeks 11-12 labs, final exam
7. Explain Public Key Infrastructure, cryptography attacks, and cryptanalysis tools	Weeks 13-14 labs, final exam
8. Demonstrate various types of penetration testing for a given set of conditions	Weeks 15-16 labs, final exam

M.   Topical Timeline (Subject to Change):

Week 1: Introduction to Ethical Hacking
Week 2: Footprinting and Reconnaissance
Week 3: Scanning Networks
Week 4: Enumeration
Week 5: System Hacking
Week 6: Malware Threats
Week 7: Sniffing/Social Engineering
Week 8: Denial of Service/Session Hijacking
Week 9: Hacking Webservers
Week 10: Hacking Web Applications/SQL Injection
Week 11: Hacking Wireless Networks/Hacking Mobile Platforms
Week 12: Evading IDS, Firewalls, and Honeypots
Week 13: Cloud Computing
Week 14: Cryptography
Week 15: Review, Term Project (optional)
Week 16: Practice Exams, Makeup Labs, Final Exam

N.   Course Assignments:

1. Labs
2. Tests
3. Midterm Exam
4. Final Exam
5. Final Project (optional)

O.   Recommended Grading Scale:

NUMERIC	GRADE	POINTS	DEFINITION
93–100	A	4.00	Superior
90–92	A-	3.67	Superior
87–89	B+	3.33	Above Average
83–86	B	3.00	Above Average
80–82	B-	2.67	Above Average
77–79	C+	2.33	Average
73–76	C	2.00	Average
70-72	C-	1.67	Below Average
67–69	D+	1.33	Below Average
63-66	D	1.00	Below Average
60-62	D-	0.67	Poor
00-59	F	0.00	Failure

P.   Grading and Testing Guidelines:

Click here to enter text.

Q.   Examination Policy:

Click here to enter text.

R.   Class Attendance and Homework Make-Up Policy:

Click here to enter text.

S.   Classroom Expectations:

Click here to enter text.

T.   College Procedures/Policies:

Important information regarding College Procedures and Policies can be found on the syllabus supplement located at https://sharept.ncstatecollege.edu/committees/1/curriculum/SiteAssets/SitePages/Home/SYLLABUS%20SUPPLEMENT.pdf

The information can also be found Choose an item.