

**RARITAN VALLEY COMMUNITY COLLEGE
COURSE OUTLINE**

NTWK 290 – Ethical Hacking and Penetration testing

I. Basic Course Information

- A. Course number and Title: NTWK 290 – Ethical Hacking and Penetration Testing
- B. New or Modified Course: New
- C. Date of Proposal: Semester: Fall Year: 2018
- D. Effective Term: Fall 2019
- E. Sponsoring Department: Mathematics & Computer Science
- F. Semester Credit Hours: 3
- G. Weekly Contact Hours: Lecture: 2
Lab 2
Out of class student work per week: 5
- H. Prerequisites: NTWK 271-Routing and Switching Essentials or permission of the Instructor
- I. Laboratory Fees: Yes
- J. Name and Telephone Number or E-Mail Address of Department Chair and Divisional Dean at time of approval: Lori Austin –
Lori.Austin@raritanval.edu (Chair), Sarah Imbriglio –
Sarah.Imbriglio@raritanval.edu (Divisional Dean)

II. Catalog Description

(Prerequisite/s: NTWK 271-Routing and Switching Essentials or permission of the Instructor) The course is based on the industry performance-based EC-Council CEH certification. Students will acquire solid foundation and relevant hands-on experience in hacking and pen-testing. Students will learn the tools, technologies, methods, and skills needed to earn EC-Council's certified Ethical Hacker certification. Software packages such as Kali Linux will be used to attain the skills needed to become a professional ethical hacker.

III. Statement of Course Need

- A. Ethical hackers, or penetration testers, have been around for a long time, but because of the increases in cybercrime and regulations over the last decade, they have become more popular than in the past. The realization is that finding weaknesses and deficiencies in systems and addressing them proactively is less costly than dealing with the fallout that comes after the fact. In response, organizations have sought to create their own penetration testing teams internally as well as contract with outside experts when and if they are needed.
- B. This course does have a lab component. Students are expected to use computers in the lab to work with various operating systems. A regular Computer Lab is sufficient.
- C. This course generally transfers as a Computer Science Elective.

IV. Place of Course in College Curriculum

- A. Free Elective
- B. This course meets a program requirement for:
 - a. Computer Networking and Cybersecurity, AAS and Certificate programs
- C. Computer Elective from the Computer and Programming Electives List
- D. Course Transferability: for New Jersey schools go to the NJ Transfer website, www.njtransfer.org . For all other colleges and universities, go to their individual websites.

V. Outline of Course Content

This course addresses the following topics:

- A. Cryptography
- B. Footprinting
- C. Scanning
- D. Enumeration
- E. System Hacking
- F. Malware
- G. Sniffers
- H. Social Engineering
- I. Denial of Service
- J. Session Hacking
- K. Web Servers and Applications
- L. SQL Injections

- M. Hacking Wi-Fi and Bluetooth
- N. Mobile Device Security
- O. Evasion
- P. Cloud Technologies and Security
- Q. Physical Security

VI. General Educational and Course Learning Outcomes

A. General Education Learning Outcomes:

After completion of this course, the student will be able to:

1. Analyze complex system attacks and specify Network and Host security features to meet them. (GE-NJ 4)

B. Course Learning Outcomes:

At the conclusion of the course, students will be able to:

1. Analyze systems to gain information from a target
2. Probe various services present on a given host
3. Use the information gained from footprinting, scanning, and earlier examinations to secure a network.
4. Describe the varieties of malware
5. Use packet sniffers to gather information that is flowing across the network.
6. Analyze attacks that are designed to temporarily or permanently shut down a target.
7. Analyze disrupt and shut down wireless networks and mobile devices
8. Describe how physical security can protect assets from being stolen, lost, or otherwise compromised.

C. Assessment Instruments:

1. Quizzes
2. Lab exercises
3. Homework Assignments
4. Research Projects
5. Exams

VII. Grade Determinants

- A. Individual homework and projects
- B. Class participation
- C. Quizzes
- D. Exams
- E. Final Exam

Modes of Teaching and Learning

- A. Lecture/Discussion
- B. Laboratory

VIII. Text and Materials

Suggested Textbook – CEHv9 Certified Ethical Hacker Version 9 Study Guide, Sean-Phillip Oriyano, SYBEX, a Wiley Brand, 2016.

(Please Note: The course outline is intended only as a guide to course content and resources. Do not purchase textbooks based on this outline. The RVCC Bookstore is the sole resource for the most up-to-date information about textbooks.)

IX. Resources

- A. Computer Lab for classroom instruction and exercises
 - a. Technology Support: Oracle Virtual Box
 - b. Software: Kali Linux

X. Honors Option

N/A