CS466/566 Principles and Practices of Cyber Defense

Instructor: Dr. Danella Zhao, E&CS Rm 3313, E-mail: dzhao@odu.edu
Office Hours: TR 11:30am-1:00pm or by Email appointment
Lecture: TR 9:30am-10:45pm, VAB 1033  https://www.blackboard.odu.edu

Course Description:
This course is to help students gain a thorough understanding of vulnerabilities and attacks in systems and networks and learn cyber defense best practices. It covers fundamental security design principles and defense strategies and security tools used to mitigate various cyber attacks. It provides hands-on experience with security software and network systems in a live laboratory environment, and gain an understanding of real-world threats. The course will focus on attacks, hacking fundamentals, and offensive and defensive techniques. Students are expected to finish intensive lab assignments that use real-world malware, exploits, and defenses.

Topics:
• Identification of reconnaissance operations
• Anomaly/intrusion detection and identification
• Identification of command and control operations
• data exfiltration detection and prevention
• Identifying malicious code based on signatures, behavior and artifacts,
• Network security techniques and components
• Cryptography in cybersecurity
• Malicious activity detection
• System security architectures and concepts
• Defense in depth
• Trust relationships
• Distributed/Cloud and virtualization

Hands on Labs:
• Reconnaissance & exploitation Lab (hacking fundamentals)
• Intrusion detection system Lab (defense)
• Buffer-overrun malicious code attack Lab (SW security)
• SQL injection attack Lab (Web security)
• TCP attacks Lab (Network security)
• Public key infrastructure lab (Cryptography)
• DNS attack Lab (Network security)
• Android rooting attack lab (Mobile security)

Textbook:
No textbooks are required. Required and supplemental reading materials have been collected specifically for CS466/566, and will be distributed throughout the semester via Blackboard.

Prerequisites:
Students will need to have basic knowledge of programming, computer architecture, computer networks and operating systems as covered in such courses as CS250, CS270 and CS455. No prior knowledge of computer security is necessary.

Grading: Attendance 10%, Lab assignments 60%, Quizzes 30%
**Grade Scale:** A, 92% and above; A-, 90-92%; B+, 87-90%; B, 82-87%; B-, 80-82%; C+, 77-80%; C, 72-77%; C-, 70-72%; D+, 67-70%; D, 62-67%; D-, 60-62%; F, below 60%

**Assignment Policy:**

Assignments and quizzes are to be submitted as instructed - typically via Blackboard, on or before the due date. Any assignment submitted after its deadline is considered late. Assignments that are submitted late by one day - 15% off penalty, 2 days - 30% off, 3 days - 50%, 4 days and beyond - not graded and no credit be awarded. Quizzes are administered via Blackboard. Quizzes expire on the due date, and cannot be taken after they have expired and become unavailable.

Make-ups for graded activities may be possible only with a valid written medical or university excuse, and then only at the instructors discretion. It is the student’s responsibility to give the instructor the written excuse beforehand and to arrange for any makeup work to be done.

**Academic Integrity:**

By attending Old Dominion University you have accepted the responsibility to abide by the honor code:

“I pledge to support the Honor System of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member of the academic community it is my responsibility to turn in all suspected violations of the Honor Code. I will report to a hearing if summoned.”

Students may still provide legitimate assistance to one another. You are encouraged to form study groups to discuss course topics. Students should avoid discussions of solutions to ongoing assignments and should not, under any circumstances, show or share solutions for an ongoing assignment.

Please see the ODU Honor Council’s webpage at [https://online.odu.edu/policies-and-student-responsibilities](https://online.odu.edu/policies-and-student-responsibilities) for concrete examples of what constitutes cheating, plagiarism, and unauthorized collaboration. All students are responsible for knowing the rules.

**Disability Services:**

In compliance with PL94-142 and more recent federal legislation affirming the rights of disabled individuals, provisions will be made for students with special needs on an individual basis. The student must have been identified, as “special needs” by the university and an appropriate letter must be provided to the course instructor. Provisions will be made based upon written guidelines from the University’s Special Needs Students Resource Office. All students are expected to fulfill all course requirements.