HACS - ACES-CYBERSECURITY

HACS100 Foundations in Cybersecurity I (2 Credits)
Interdisciplinary foundational course of the ACES program. Through lectures, lab activities, and discussions, students will learn and practice various aspects of cybersecurity. Weekly technical lectures will introduce students to the operating system UNIX. Students will partner with the Division of Information Technology in a project to engage the University of Maryland community in a cyber- hygiene and cyber-ethics campaign based on the concepts learned in class.
Restriction: Must be a first-semester student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program.

HACS101 Applied Cybersecurity Foundations (2 Credits)
Prepares students for team research that will be conducted in HACS 200. Students gain an understanding across the breadth of cybersecurity including system monitoring, networking basics and penetration testing. An applied approach to statistics is also included to prepare students to assess the data collected for their research projects. The course is conducted with a hands-on approach applying virtual environments to practice the concepts learned in the technical lectures each week.
Prerequisite: Minimum grade of C- in HACS100.
Restriction: Must be a second-semester student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program.

HACS200 Applied Cybersecurity Foundations II (2 Credits)
Students will apply the skills learned in HACS 100 and 101 to practice cybersecurity research through team led projects employing honeypots, carrying that project through all stages - proposal, implementation, and analysis. Weekly lectures will supplement project work by addressing trends observed in honeypot attacks and protections needed, along with data collection and analysis tools, and other foundational cybersecurity concepts.
Prerequisite: Minimum grade of C- in HACS101.
Restriction: Must be a third-semester student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program.

HACS201 Introduction to UNIX (1 Credit)
Introduction to the operating system UNIX through lectures and hands-on assignments.
Restriction: Must be a first-year student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.
Credit Only Granted for: HACS201 or CMSC216.
Additional Information: Required course for students who have not completed the ACES Living-Learning Program or taken CMSC216.

HACS202 Group Project in Cybersecurity (3 Credits)
The group project in this course will combine technical, analytical, and communication skills, further engaging students in the practice of cybersecurity. Students will learn about design concepts and data analysis as they engage in a team project designing, deploying, and collecting and analyzing data from a honeypot. The hands-on nature of the course will give students experiential insight about how and why attackers attack and how to engage in protective measures to prevent attacks.
Restriction: Must be a first-year student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program; and cannot have been an ACES Living-Learning Program student (i.e., have taken HACS100, HACS101 and HACS200).

HACS208 Seminar in Cybersecurity (3 Credits)
Explores various lenses of cybersecurity in order to promote an interdisciplinary understanding of the field. Although each section may focus on a different topic, each integrates active student engagement, communication, critical communication, critical thinking, and teamwork.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program.
Repeatable to: 6 credits if content differs.

HACS208A Accounting and Economic Aspects of Cybersecurity (3 Credits)
In today's interconnected digital world, cybersecurity has become one of the most important issues confronting organizations in both the private and public sectors of an economy. Indeed, cybersecurity is a national and economic security priority in countries throughout the world. This is an interdisciplinary Honors Seminar offered as part of UMD's ACES program. The primary objective of this course is to discuss the relationships among accounting, economics and cybersecurity, with a focus on the important roles of accounting and economics in understanding the issues related to cybersecurity. A basic framework for assessing the interactions among accounting, economics, and cybersecurity will be developed and discussed. A secondary objective of the course is to assist ACES students in developing their ability to conduct original and applied research on topics related to "accounting and economic aspects of cybersecurity."
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program.

HACS208E Introduction to Reverse Engineering (3 Credits)
An introduction to software reverse engineering tools and methodologies. Fundamental topics will be introduced: compilers, linkers, loaders, assembly language, as well as static and dynamic analysis tools. We will motivate some reasons for software reverse engineering and examine the background material necessary for an understanding of the subject. This will include computer architecture and low-level systems programming, as well as an introduction to x86_64 assembly language. We will apply this newly acquired knowledge while learning about static and dynamic analysis tools used by practitioners of software reverse engineering.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program.

HACS208I Security Incident Handling and Management (3 Credits)
Examines the many roles, capabilities, organizations, and objectives involved in security incident handling and management. Core course content includes three major components: learning about the skill sets that people use, participating in role playing exercises that increasingly build upon this knowledge, and finally conducting exercises in a lab environment simulating security incident discovery, handling, and management.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program.

HACS208M Project Management Techniques for IT Professionals (3 Credits)
This course aims to build an in-depth understanding of project management methodologies for IT professionals. The course explores the application of Project Management Institute (PMI) guidelines for managing projects and PMP certification. Topics include an overview of PMI standards and project management, various roles in managing technical projects, work breakdown structures, security considerations, risk assessment, testing, and implementation. The students will have an opportunity to learn how to apply PMI guidelines in a real world software development project.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program.

HACS208N Digital Forensics (3 Credits)
Explores the various fields of digital forensics, such as memory, hard drive, and network traffic analysis. This course covers the legalities involved with forensic investigations and the wide variety of digital forensics tools, including both open source and proprietary. This course includes the different types of forensic artifacts that can be acquired and analyzed and review the careers and certifications relevant to the field.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program.

HACS208P Beyond Technology, the Policy Implications of Cyberspace (3 Credits)
Explores the key issues facing policy makers attempting to manage the problem of cybersecurity from its technical foundations to the domestic and international policy considerations surrounding governance, response, and critical infrastructure risk management. The course is designed for students with little to no background in information technology, and will provide the principles to understand the current debates shaping a rapidly evolving security landscape.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program.

HACS208Z Methods for Solving (And not Solving) Puzzles (3 Credits)
Surveys modern problems from different domains in computer science and cybersecurity to train our minds to appropriately approach puzzles we encounter in the future. This course covers graph theory, including what a graph is and the kinds of objects it can model, connectivity types, and vertex/edge covers algorithms. This course covers computer networks, including the models used for network stacks and what algorithms are used to solve difficult problems present in our current networks. This course covers algorithm analysis, including greedy algorithms, big O complexity, and how to analyze the capabilities and limitations of an algorithm. This course introduces cryptography, including the difference between public-key and symmetric-key cryptography, how RSA works, and the cryptanalysis of well-known cryptosystems.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program.

HACS279 Undergraduate Research in Cybersecurity (1-3 Credits)
The Advanced Cybersecurity Experience for Students (ACES) program encourages its students to engage in research in order to gain greater insight into a specific area within cybersecurity, obtain an appreciation for the subtleties and difficulties associated with the production of knowledge and fundamental new applications, and to prepare for graduate school and the workforce.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program; and permission of UGST-HCOL-ACES Cybersecurity Program.
Repeatable to: 6 credits if content differs.

HACS287 Undergraduate Research in Cybersecurity (3 Credits)
The Advanced Cybersecurity Experience for Students (ACES) program encourages its students to engage in research in order to gain greater insight into a specific area within cybersecurity, obtain an appreciation for the subtleties and difficulties associated with the production of knowledge and fundamental new applications, and to prepare for graduate school and the workforce.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program; and permission of UGST-HCOL-ACES Cybersecurity Program.

HACS297 Cybersecurity Experience Reflection (3 Credits)
Cybersecurity experience is defined as an experiential learning activity either with a University of Maryland entity (such as the Division of Information Technology, the ACES competition team or in an ACES outreach program), or with an external organization that will provide valuable, hands-on experience to supplement the knowledge learned in the other ACES coursework.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program; and permission of UGST-HCOL-ACES Cybersecurity Program.

HACS318 Cybersecurity Professionals Colloquium Series (1 Credit)
The Cybersecurity Professionals Colloquium Series explores various lenses of cybersecurity in order to promote an interdisciplinary understanding of the field. The colloquium series consists of guest lectures of cybersecurity professionals. In written assignments, students will not only summarize the lecture content but also reflect on the significance of the lecture content for the field of cybersecurity.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.
Repeatable to: 2 credits.

HACS402 Applied Security Analysis and Visualization (3 Credits)
Focuses on exploratory and statistical data analysis, data and information visualization, and the presentation and communication of analysis results. These topics will be presented and explored in the context of and with applications to cybersecurity related data.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.

HACS408 Advanced Seminar in Cybersecurity (3 Credits)
Explores various lenses of cybersecurity in order to promote an interdisciplinary understanding of the field. Although each section may focus on a different topic, each integrates active student engagement, communication, critical communication, critical thinking, and teamwork.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.
Repeatable to: 9 credits if content differs.

HACS408C Interpersonal Cyber Communications (3 Credits)
Designed to prepare students to participate in culturally responsible and environmentally appropriate communication in the workforce. Students will explore the industry standards for writing technical reports, as well as the variances between persuasive, team, written, and oral communication styles.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.

HACS408L Analytical and Forensic Techniques for Cybersecurity (3 Credits)
Explores forensic artifacts contained in digital devices, security mechanisms available to protect digital devices and mechanisms available to cybersecurity professionals for analysis of digital devices. Topics include file structure and recovery of IoT and cell phone forensic data, network data capture and analysis, enterprise mobile device management analysis and forensic investigation of digital devices (IoT, telematics systems, etc.) that interact with cell phone and other devices. Incident response, timeline analysis, and detection and analysis of artifacts will be explored in a hands-on and lab-centric course using a variety of open-source tools and commercial cloud services.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.

HACS408M Introduction to Cyber Threats and Risk Management (3 Credits)
Provides an exploration of cyber risk management and present-day cyber threats, their impacts, and their mitigations. Students will take a multi-disciplinary approach to understanding threats and risks including the technical, policy, and social aspects. This course is guided by real-world cyber threats and examples.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.

HACS408O Internet of Things Security (3 Credits)
This increasingly interconnected world brings a need for understanding cybersecurity challenges associated with embedded devices and systems. This course will expose students to topics in Internet of Things (IoT) and Cyber Physical System (CPS) device types, IoT/CPS threat categories, security services, distributed networking, activity privacy, and intrusion detection for embedded environments. In addition to individual homework assignments, students will participate in a semester long group project involving research, design, and implementation.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.

HACS408T Penetration Testing (3 Credits)
A hands-on, technically rigorous experience that prepares students for real-world work in penetration testing and offensive security. This course will allow students to gain proficiency and become comfortable using the tools, techniques, and methodologies that represent the state of the art in penetration testing today. Students should be comfortable on the command line, and a technical exposure to networking and basic proficiency in some scripting language (Bash, Ruby, or Python) is expected.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.

HACS408V Data Analysis and Visualization for Cybersecurity (3 Credits)
Focuses on exploratory and statistical data analysis, data and information visualization, and the presentation and communication of analysis results. These topics will be presented and explored in the context of and with applications to cyber security related data. Examples and illustrations will often involve the R programming language, but prior experience with R is not required and submitted work may involve the use of other languages and tools at times.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program.

HACS479 Undergraduate Research in Cybersecurity (1-3 Credits)
The Advanced Cybersecurity Experience for Students (ACES) program encourages its students to engage in research in order to gain greater insight into a specific area within cybersecurity, obtain an appreciation for the subtleties and difficulties associated with the production of knowledge and fundamental new applications, and to prepare for graduate school and the workforce.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program; and permission of UGST-HCOL-ACES Cybersecurity Program.
Repeatable to: 6 credits if content differs.

HACS487 Undergraduate Research in Cybersecurity (3 Credits)
A semester-long, individualized academic research project. Students work with a faculty supervisor to design and research an original topic. Students engage in research to gain greater insight into a specific area within cybersecurity, obtain an appreciation for the subtleties and difficulties associated with the production of knowledge and fundamental new applications, and prepare for graduate school and/or the workforce.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program; and permission of UGST-HCOL-ACES Cybersecurity Program.

HACS497 Cybersecurity Experience Reflection (3 Credits)
Cybersecurity experience is defined as an experiential learning activity either with a University of Maryland entity or with an external organization that will provide valuable, hands-on experience to supplement the knowledge learned in other ACES coursework. This course is intended to help students reflect on their cybersecurity experience and to learn from others' cybersecurity experiences. It is also intended to help students gain professional skills that will aid in their future career.
Prerequisite: Students may enroll concurrently with or after completing a cybersecurity related internship experience of at least 135 hours.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program; and must not have taken HACS297.
Credit Only Granted for: HACS297 or HACS497.

HACS498 Cybersecurity Group Problem Solving (3 Credits)
The Advanced Cybersecurity Experience for Students (ACES) program encourages its students to engage in team problem solving activities in order to gain greater insight into a specific area within cybersecurity and to obtain an appreciation for the subtleties and difficulties associated with these activities in order to prepare students for graduate school and the workforce. Students engage in a semester long problem solving or development project under the mentorship of a industry specialist and with the guidance of university faculty. Through the exercise the students will develop teamwork experience and professional communication skills in addition to experience of the project itself. The project might be evaluation, creation, testing or analysis of some area of cybersecurity as needed by the mentor-sponsor. A contract of what will be accomplished is required must be agreed upon by the mentor, the student and the ACES leadership before the project can begin.
Restriction: Must be a student in the ACES (Advanced Cybersecurity Experience for Students) Minor Program; and permission of UGST-HCOL-ACES Cybersecurity Program.
Repeatable to: 6 credits.