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 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 student in the ACES (Advanced Cybersecurity Experience for Students) Living-Learning Program.

HACS102 Foundations in Cybersecurity II (3 Credits)
Second interdisciplinary foundational course of the ACES program. Through lectures and project work, students will learn and practice cybersecurity. Students will work in teams to develop a honeypot project, and work on this project throughout the course. Weekly lectures will supplement project work, focusing on types of computer attacks and protections, data collection and analysis, and other foundational cybersecurity concepts.
Prerequisite: HACS100.
Restriction: Must be a 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 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 and HACS102).

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.

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.

HACS204 Cybersecurity Experience for Students (Minor Program)
Minor Program for students who have completed the ACES Living-Learning Program or taken CMSC216.
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.

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.

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.