AC - Applied Computing

Courses numbered 100 to 299 = *lower-division*; 300 to 499 = *upper-division;* 500 to 799 = *undergraduate/graduate*.

AC 121. Cybersecurity Awareness (3).
The ability to secure information and systems within a modern enterprise in this modern globalized environment is a growing challenge. Ever-present human threats are global, persistent and increasingly sophisticated. Natural threats are unpredictable but inevitable. Vulnerabilities within the complex and interdependent system of systems continue to be discovered with many more yet to become common knowledge. Exploited vulnerabilities can have a devastating impact on an organization or even a society. This course is designed to familiarize users with information, cyberspace and security principles needed to understand these threats. To this end, the course addresses a range of topics, including information infrastructures, social engineering, information system exploitation techniques and countermeasures to the threats discussed.

AC 201. Introductory Design Project (1).
The first of the three-course project design series. The course introduces students to project design, prototyping, engineering standards and professional reports. Students are part of teams, learn prototyping skills and have hands on experiences in a maker-space. Students learn project management tools, team working tools, how to perform market research and develop videos, and prototype development. Prerequisite(s): FYAP 102A, FYAP 102B, ENGR 302, ID 300 or instructor's consent.

AC 222. Applied Computing Fundamentals (3).
Information technology (IT) virtually connects people and businesses in the world. The daily operations of every organization in the public and private sector heavily rely on the internet. This course allows students to gain vital concepts on computer hardware, computer systems, networking and security to solve real-world computing challenges. This course is a key for anyone who wants to gain basic skills in the computing sector. Students collaborate effectively and think critically to develop skills in computing and networking. Students learn to use industry-standard tools through hands-on class projects.

AC 235. Tools and Techniques of Cybercrime (3).
Cross-listed as CJ 235, HLS 235. Introduces students to the basic cybercrime tools, techniques and concepts to better prepare for today’s information technology in criminal justice. Tools and techniques used by cybercriminals and cybercrime investigators, such as Tor, IP addresses, VPN, OSINT (Open-Source Intelligence), and data sharing and analysis, are discussed concerning cybercrime prevention, mitigation and investigations. Some concepts discussed include privacy, surveillance, artificial intelligence and biometrics. The course prepares students for further cybercrime and cybersecurity courses.

AC 301. Junior Project (2).
Second course in four-course project sequence. Introduces students to engineering design concepts with an entrepreneurial mindset. This includes customer discovery and value creation techniques as well as engineering design and project management tools. Prerequisite(s): AC 121.

AC 321. Applied Networking (3).
Information technology (IT) virtually connects people and businesses in the world. The daily operations of every organization in the public and private sector heavily rely on the internet. This course allows students to gain vital concepts on computer networking and security to solve real-world computing challenges. This course is a key for anyone who wants to gain advanced skills in the computing sector. Students collaborate effectively and think critically to develop skills in computer networking. Students learn to use industry-standard tools through hands-on class projects.

AC 322. Applied Programming and Scripting (3).
Good scripting skills are vital to IT experts in the fields of information security. This course is designed for cybersecurity professionals who are interested in learning basic coding skills to perform the cybersecurity tasks more efficiently. The course assists students in taking their cybersecurity career to the next level by teaching the vital skills needed to develop as well as customize applications that interact with file systems, databases, networks and websites. Covers command shell scripting (cmd, powershell, bash) in Windows and Linux operating systems. Emphasizes scripting cybersecurity tasks such as system configuration, system auditing and penetration testing. Also covers Arduino microcontrollers, coding Arduino in Python and coding TCP Traceroute. Python language is used in this course. Prerequisite(s): AC 222 with C- or better.

AC 324. Applied Web Applications and Database Development (3).
When browsing on a web application, look for two things: how user-friendly the web app is and how the information is stored, controlled and used. Each web application has a set of requirements such as financial transaction, customer information, etc. The course covers web and database technologies, services, protocols, design and operation. Students learn a variety of languages including HTML, CSS, Apache and MySQL. Course is designed to apply the languages through hands-on projects. Prerequisite(s): AC 222 or MIS 325 or CS 664, with a C- or better. Pre- or corequisite(s): ECON 201 or IME 255, with a C- or better.

AC 326. Cyber Operations (4).
Covers concepts related to cyber attack, penetration testing, cyber intelligence, cryptography and cyber defense. Students learn the attacker's perspective and how security infrastructure integrates with the rest of the business and IT infrastructure through the use of hands-on projects. Prerequisite(s): AC 121, AC 222, AC 321 and AC 322 .

AC 331. Introduction to Powershell for Hackers (1).
Cross-listed as CS 331. Students learn the basics of using Windows PowerShell and how to interact with Windows via the PowerShell command prompt. Course instruction includes: how to create and interact with Windows files and directories, how to interact with Windows processes and services, how to use PowerShell commands for basic digital forensics analysis, and how to create and use basic PowerShell scripts. Repeatable for credit.

AC 334. Go Language for Ethical Hackers (1).
Go Language or “Go” for short, is a flexible programming language developed by programmers at Google. It has been increasingly used as a language to build, test and analyze code due to its large library and ease of use. Go has become increasingly popular amongst ethical hackers as it is an effective way to script custom tools to defeat prebuilt or common cyber defense software. This class is designed for beginners that are unfamiliar with Go who wish to understand its application in the cybersecurity spectrum. Prerequisite(s): AC 121 or instructor's consent.

AC 346. Introduction to Computer Networks (3).
Cross-listed as CS 346, ECE 346. Introductory course on computer networking. Introduces concepts, protocols and security in various network layers with emphasis on applications, transport layer (TCP, UDP), network layer (ICMP), and link layer. All concepts in the course are reinforced though hands-on assignments. Prerequisite(s): CS 211.

AC 352. Competitive Ethical Hacking (3).
Cross-listed as CS 352. Presents fundamental concepts of competitive ethical hacking in computer and network security. The course

introduces the command line interface, open-source intelligence, cryptography, digital forensics, web application security, software reverse engineering, secure programming and log analysis. Assignments include participating in capture the flag competitions. Prerequisite(s): CS 211 or (AC 121 and AC 322), with a C- or better.

AC 362. Basic Python for OSINT (1).
Open Source Intelligence (OSINT) is a critical part of both cybersecurity offensive reconnaissance process and threat analysis for defensive security specialists. While there are many tools that are prebuilt to assist the practitioner in both target and systems OSINT, a background in basic Python can create and develop even more choices for finding, gathering and organizing critical information. Prerequisite(s): AC 121.

AC 363. Human Threats to Cybersecurity (3).
Kevin Mitnick, who popularized the term “social engineering,” explained that it is much easier to trick someone into revealing a password for a system than to exert the effort of hacking into the system. Mitnick claims that this social engineering tactic was the single-most effective method in his arsenal. This course covers human threats to cybersecurity in political, social and economic contexts. It includes targeted exploitation/manipulation of individuals, small groups and larger groups through social engineering, marketing, propaganda, psychological operations by personal contact, email, social networking, web and RF transmission. Prerequisite(s): AC 121 and PHIL 125.

AC 401. Senior Project I (3).
The third of the four-course project design series. In this intermediate course, students learn the importance of the voice of the customer, the customer/product market fit through using the business model canvas, and engineering design tools. Students learn and practice customer interview techniques and, through the feedback, help to develop appropriate solutions and prototypes. Students perform individual observations to discover unmet needs in industry and, after refining the needs, teams form to solve these needs. Comprehensively covers the student’s concentration in applied computing and its applications. Students work with faculty and external consultants and industry to refine their team based senior project. Prerequisite(s): AC 301 and PHYS 213. Pre- or corequisite(s): PHIL 354.

AC 402. Senior Project II (3).
Comprehensively covers the student’s concentration in applied computing and its applications. Students continue to work in their teams with faculty and external consultants and industry to refine and develop a final solution for their team based senior project. Prerequisite(s): AC 401.

AC 452. Advanced Competitive Ethical Hacking (3).
Cross-listed as CS 452. Advanced capture the flag players take the knowledge built from AC 352/CS 352 and participate in a more challenging capture the flag competition as a team based on real world scenarios as opposed to the Jeopardy style questions of National Cyber League. These competitions could include but are not limited to the Collegiate Cyber Defense Competition and National Center of Academic Excellence Competition. Repeatable for up to 6 credit hours. Prerequisite(s): AC 352/CS 352 with a grade of A, a minimum score of 1500 on individual National Cyber League games, and instructor's consent.

AC 461. Digital Forensics (3).
Covers concepts related to hardware and software forensics, incident response, cyber crime and cyber law enforcement. Students learn different aspects of computer and cyber crime and ways to uncover, protect, exploit and document digital evidence. Students are exposed to different types of tools (both software and hardware), techniques and procedures, and are able to use them to perform rudimentary forensic investigations. Focuses on the entire life cycle of incident response including preparation, data collection, data analysis and remediation. Real world case studies reveal the methods behind and remediation strategies for today's most insidious attacks. Prerequisite(s): AC 326 .

AC 462. Cyber Physical Systems (4).
Focuses on trustworthy and resilient CPS, starting with NIST's CPS Framework. Students learn about common IoT infrastructures, integrate CPS into organizational risk management, and conduct cybersecurity risk assessments for critical cyber physical systems. Prerequisite(s): ENGR 220 and AC 326, or instructor’s consent.

AC 463. Cyber Risk Management (3).
This course covers application of risk and information security management to improve organizational resilience. Concepts include business impact analysis, incident response planning, disaster recovery planning, business continuity planning and security auditing. Prerequisite(s): AC 326.

AC 464. Web Application Security (3).
Develops an understanding of common web-based vulnerabilities and their impacts. Concepts include development and management of secure web-based systems, security mitigation strategies and penetration testing. Prerequisite(s): AC 324 and AC 326 .

AC 668. Geopolitical Strategy in Cyber Operations (3).
Geopolitical strategy drives the actions of nation-states, and cyber is a large part of the engine, increasingly so with advances in technology and its interoperability with other instruments of power. From disinformation to satellite hacks to current use of artificial intelligence, the course examines how history has shaped the cyber strategy in regions of the world, what the current state of affairs are in selected countries, and what the future may hold in this ever changing dynamic. This course is for students who are a current or otherwise eligible SFS Scholar, residing or planning to reside within commuting distance of WSU, and a U.S. citizen due to NSA and CAE standards. Students who have a desire to work at some level of government in the U.S. may also be eligible to take this course. Prerequisite(s): instructor's consent.