IT601: Cybersecurity Foundation

This course provides fundamental overview of cybersecurity and lays a foundation for subsequent topical courses in the area of cybersecurity systems Topics covered include: Cyber Security Fundamentals, Microsoft Windows Security Principles, Attacker Techniques, Exploit Tools, Self-Replicating Malicious Code, Evading Detection, Virtual Machine Detection, Stealing Information, Exploitation and Defense and Analysis Techniques, Memory Forensics, Intrusion Detection System.

IT602: Digital Forensics Technology & Practices

This course provides overview of digital forensic. Topics covered includes, introduction to digital forensic, digital forensic process, digital forensic tools, investigative methodology, current techniques and tools for forensic examinations & Analysis, Digital investigations, Electronic Discovery, Intrusion Investigation, Antiforensics, Windows Forensic Analysis, Embedded Systems Analysis &Network Evidence and Investigations.

IT603: Information Security Law, Policy, and Ethics

This course provides in depth analysis of information security laws in many jurisdictions and needs to understand the overall framework of legal security requirements, so it can evaluate how local law fits in, and what it might do to become generally legally compliant in many jurisdictions and under many laws. This course also provides a concise overview of the traditional ethical frameworks that can guide our analysis of the moral dilemmas and social problems that rise in cyberspace. Discussions on Saudi securities laws are also appended.

IT 604: Cybersecurity Technology and Management

This course provides issues in cyber security technology and practice. This course explores practical solutions to a wide range of cyber-physical and IT infrastructure protection issues. This course also aims at managing the cyber-attacks on the critical IT infrastructure computer networks.

IT 605: Research Methods and Engineering Statistics

Study of the research methods and processes applicable to engineering/technology Emphasis on defining research problems, collecting, analyzing, recording, and interpreting data. Students will be required to conduct a research project.

IT611: Network and System Security

This course includes basic concepts of network and system security, with an emphasis on the threats and countermeasures relevant to computer programs and Internet applications. Students will be prepared to evaluate the security of real network systems, and to develop strategies to detect and defend against attacks. In additional to the traditional security technologies, this course will also include discussions on problems of current research in network and system security.

IT612: Malware and Vulnerability Analysis

This Course provides important aspects of malicious codes and the technical skills required to identify, analyze, and exploit software vulnerabilities, focusing on application-level issues which includes Code auditing, reversing, memory corruption, fuzzing, Post-Exploitation, Web app Hacking, Reversing, Reverse Engineering, Client-side attacks and Web Hacking on android and smart devices. This will form the basis of a methodological approach for identifying and analyzing software vulnerabilities and to design secure systems and defend against intrusion.

IT613: Cryptography and Cryptanalysis

This course provides fundamental overview of Cryptography & cryptanalysis and lays a foundation for subsequent topical courses in the area of Computer Security. Topics covered include; Security Concepts, Attacks, Block Ciphers, Block Cipher Operation, Cryptanalysis, Number Theory, Public-Key Cryptography, Factoring and Discrete Algorithms, Linear Cryptanalysis. &Differential Cryptanalysis, Cryptographic Hash and MAC Functions, User Authentication Protocols.

IT614: Software Security

This course will provide students to understand the theories and tools used for secure software design, threat analysis, secure coding, and vulnerability analysis. Students will study, in-depth, vulnerability classes to understand how to protect software and how to develop secure software. This course will also cover various analysis and design techniques for improving software security. We will also discuss the technical trends affecting software security.

IT615: Penetration Testing and Ethical Hacking

Students will learn the ethical hacking techniques commonly used to breech and exploit corporate networks and can identify how and when they are used. This course enables students to uncover vulnerabilities in operating systems, applications and IT networks and provides advice in applying appropriate countermeasures. This course teaches penetration testing techniques that quickly,

efficiently and most importantly methodically uncover vulnerabilities in operating systems, applications and networks.

Students will learn core skills and techniques that every pentester needs. Using a virtual machine-based lab that includes Kali Linux and vulnerable operating systems, they will run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite

IT616: Special Topics in Cyber security

This course will focus on future trends in technology in the field of cyber security; as well discuss contemporary Cybersecurity policy problems, economy and politics, and how those are affecting Cybersecurity policy. Topics may include Routing security and next-generation Internet, Privacy and Anonymous communication: attacks and designs, Cloud security, End-to-end (E2E) security: practical attacks and defenses etc.

IT621: Computer Forensics and Investigations

This course gives students a solid foundation to the methods of computer forensics and investigations. It provides an in-depth knowledge of the criminal justice system, Computer hardware and software systems, investigative and evidence gathering protocols. The topics covered will enable the students to possess the knowledge, skills and experience to conduct complex, data-intensive forensic examinations involving various operating systems, platforms and file types

IT622: Advance Computer Forensics

This course is designed as an advanced course in computer forensics, focusing on Windows systems. It is estimated that Windows comprises over 85% of the operating systems used worldwide. This course focuses on advanced topics in Windows operating system analysis, including advanced file system analysis, web and email, as well as a comprehensive final case involving a moot court exercise

IT623: Mobile Network and Forensics

This course aims to provide mobile and network forensic investigations that are legal, ethical, and highly effective using the detailed information contained in this practical guide. This course will explain the latest tools and methods along with features, examples, and real-world case studies. Students will find out how to assemble a mobile and network forensics lab, collect prosecutable evidence, uncover hidden files, and lock down the chain of custody. This comprehensive resource shows not only how to collect and analyze mobile device and network data but also how to accurately document your investigations to deliver court-ready documents.

IT 624: Malware Development and Counter measurement

This course aims to provide malware development strategies such as delivery mechanisms, self-protection and malicious framework engagement. In addition to these this course also provides defense strategies against malware development such as threat modelling, static application security testing, Dynamic application security testing and benefits of the 360 approach

IT625: Forensics Management of Digital Evidence

This course covers digital evidence as it applies to any crime and its management. It includes forensic examination methods of computer components and computer networks within the legal framework. It covers wide ranging topics such as legal issues relating to digital evidence and computer crime, language of computer crime investigation, court room dealings of digital evidence and forensic examinations.