



InfoSec Academy Pen Testing & Hacking Track

Fundamental Courses	Foundational Courses	Foundational Courses	Specialized Courses	Advanced Courses	Certification Preparation Courses
Texas Security & Policy Assurance Soft Skills	Certified Security Sentinel C)SS & Certified Vulnerability Assessor C)VA	Certified Information Systems Security Officer	Certified Penetration Testing Engineer C)PTE	Certified Penetration Testing Consultant C)PTC	Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM) Certified Information Systems Auditor (CISA) Certified Ethical Hacker (CEH)



InfoSec Academy

Pen Testing & Hacking Track

Course Details

Course Name	Description	Professional Roles	Modules/Labs
Texas Security Policy & Assurance Course	Upon successful completion of this course, the participant will be prepared to apply the state rules regarding information security in the state of Texas within their agency.	ISOs & CISOs	Module 1: Texas Rules and Legislation Modules 2: Data Classification Module 3: Security Framework Module 4: Agency Security Plans Modules 5: Reports Modules 6: Security Services
Soft Skills Course (examples): Team Building Without Time Wasting Helping Employees Use Their Time Wisely Everybody Wins: How to Turn Conflict into Collaboration	A variety of soft skills courses are available covering a wide range of topics.	Dependent on the course	N/A



InfoSec Academy

Pen Testing & Hacking Track

Course Details

Course Name	Description	Professional Roles	Modules/Labs
Certified Security Sentinel - C)SS	<p>The Certified Security Sentinel certification course is intended for anyone that uses a computer on the internet. Attendees will not only understand security threats and attacks but also be prepared with countermeasures for these attacks. The weakest link in any companies' security program is a poorly trained employee. Once a student understands what can happen, they will know what to look for. And with that understanding, be able to keep the information they have been entrusted with as safe as possible.</p> <p>The social engineering portion of the class is designed to teach the participants the skills used by social engineers to facilitate the extraction of information from an organization using technical and non-technical methods. Computer fraud, black-hat hacking, and cyber-terrorism are all phrases that describe crimes that use over-the-wire technology to attack, steal, and terrorize their victims. The key to most of these over-the-wire attacks being successful is information they receive through social engineering. Does it work? Can smart people be easily deceived? Kevin Mitnick, who served five years in prison for repeated hacking said in testimony before Congress on the subject of Social Engineering: "I was so successful with that attack that I rarely had to resort to a technical attack." If you're afraid of having your identity, credit card credentials, or business information compromised, then this is the training you have been looking for.</p> <p>The Certified Security Sentinel certification course trains students on how attacks are performed, how to identify an attack, and how to secure information. One of the most valuable skill sets of a C)SS is that they understand how to train others on security as well.</p>	Employees who need to learn the basics of security.	Module 1: Basic Computer Security Module 2: User Awareness Module 3: Implementation Countermeasures Module 4: Essential Security Awareness Module 5: Using the Internet at Work Module 6: Accessing the Network Locally Module 7: Accessing the Network Remotely Module 8: Social Engineering Module 9: Understanding and Interacting with our Target Module 10: Researching Our Target Module 11: Methods of Deception



InfoSec Academy

Pen Testing & Hacking Track

Course Details

Course Name	Description	Professional Roles	Modules/Labs
Certified Vulnerability Assessor C VA	<p>The Certified Vulnerability Assessor course trains students to be proficient in conducting vulnerability assessments by:</p> <ol style="list-style-type: none"> 1. Teaching the risk associated with information technology and why a vulnerability assessment is crucial to the continuing operations of a business. 2. Preparing students with the tools and knowledge of how to perform a vulnerability assessment. 3. Instructing students on how to summarize and report on their findings from a vulnerability assessment. <p>This is accomplished by having students perform in-depth labs that focus recognizing prominent threats with industry proven tools, learn our proven methodology by using real world examples, and study what vulnerabilities hackers look for when trying to hack into systems. After completing the course, students will be able to sit for the Certified Vulnerability Assessor exam. Upon passing the exam, students will be able to use the C VA certification.</p>	IT Professionals	<p>Module 1: Why Vulnerability Assessment Module 2: Vulnerability Types Module 3: Assessing the Network Module 4: Assessing Web Servers & Applications Module 5: Assessing Remote & VPN Services Module 6: Vulnerability Assessment Tools Module 7: Output Analysis</p>



InfoSec Academy

Pen Testing & Hacking Track

Course Details

Course Name	Description	Professional Roles	Modules/Labs
Certified Vulnerability Assessor C)VA	<p>The Certified Vulnerability Assessor course trains students to be proficient in conducting vulnerability assessments by:</p> <ol style="list-style-type: none"> 1. Teaching the risk associated with information technology and why a vulnerability assessment is crucial to the continuing operations of a business. 2. Preparing students with the tools and knowledge of how to perform a vulnerability assessment. 3. Instructing students on how to summarize and report on their findings from a vulnerability assessment. <p>This is accomplished by having students perform in-depth labs that focus recognizing prominent threats with industry proven tools, learn our proven methodology by using real world examples, and study what vulnerabilities hackers look for when trying to hack into systems. After completing the course, students will be able to sit for the Certified Vulnerability Assessor exam. Upon passing the exam, students will be able to use the C)VA certification.</p>	IT Professionals	<p>Module 1: Why Vulnerability Assessment Module 2: Vulnerability Types Module 3: Assessing the Network Module 4: Assessing Web Servers & Applications Module 5: Assessing Remote & VPN Services Module 6: Vulnerability Assessment Tools Module 7: Output Analysis</p>



InfoSec Academy

Pen Testing & Hacking Track

Course Details

Course Name	Description	Professional Roles	Modules/Labs
Certified Penetration Testing Engineer C)PTE	<p>The Certified Penetration Testing Engineer course trains students on the 5 key elements of penetration testing: information gathering, scanning, enumeration, exploitation and reporting. Ethical hacking is the art of using these penetration testing techniques to identify and repair the latest vulnerabilities in a system to make sure it is secure. Malicious hackers use these same techniques to find the same vulnerabilities except they exploit the vulnerabilities giving them access to the businesses' network. Once inside, hackers can access private information, such as usernames, passwords, credit card numbers, and social security numbers of clients and employees. It's very likely this data will be held for ransom or sold off on a black market. Hackers are constantly looking for new companies they can exploit; when they come across yours, will they be able to gain access? Certified Penetration Testing Engineers are the solution to prevent this from happening to businesses they serve.</p> <p>With our proprietary penetration testing lab exercises, students will spend about 20 hours getting real-world penetration testing experience. They'll know what they are learning and they'll know how to use it after course. Our instructors will also provide real life examples of when to use the techniques that are being taught. There is no better way to learn the art of penetration testing.</p> <p>This course also enhances the business skills needed to identify protection opportunities, justify testing activities and optimize security controls appropriate to the business needs in order to reduce business risk.</p>	Ethical Hacker Security Consultant System Administrator Chief Security Officer	Module 0: Course Overview Module 1: Logistics of Pen Testing Module 2: Linux Fundamentals Module 3: Information Gathering Module 4: Detecting Live Systems Module 5: Enumeration Module 6: Vulnerability Assessments Module 7: Malware Goes Undercover Module 8: Windows Hacking Module 9: Hacking UNIX/Linux Module 10: Advanced Exploitation Techniques Module 11: Pen Testing Wireless Networks Module 12: Networks, Sniffing and IDS Module 13: Injecting the Database Module 14: Attacking Web Technologies Module 15: Project Documentation Lab 1: Getting Set Up Lab 2: Linux Fundamentals Lab 3: Information Gathering Lab 4: Detecting Live Systems Lab 5: Reconnaissance Lab 6: Vulnerability Assessment Lab 7: Malware Lab 8: Windows Hacking Lab 9: UNIX/Linux Hacking Lab 10: Advanced Vulnerability and Exploitation Lab 11: Attacking Wireless Networks Lab 12: Network Sniffing and IDS Lab 13: Database Hacking Lab 14: Hacking Web Applications



InfoSec Academy

Pen Testing & Hacking Track

Course Details

Course Name	Description	Professional Roles	Modules/Labs
Certified Penetration Testing Consultant C)PTC	<p>The Certified Penetration Testing Consultant course is our advanced course in our penetration testing track. The C)PTC is designed for cyber security professionals and IT network administrators who are interested in conducting Penetration tests against large network infrastructures, such as large corporate networks.</p> <p>The training starts with capturing and analyzing basic packets and continues with Layer2 attack vectors; Layer3 based attacks, including both IPv4 and IPv6 stacks, routing protocol attacks (OSPF, BGP, etc); Service Provider level attacks related with very common used MPLS; how to use relays and pivots; VPN attacks including IPSEC protocol suite; SSL attacks; and finally covers NIDS/NIPS evasion and implementation techniques.</p> <p>At the completion of each module, students are going to be able to practice their knowledge with the lab exercises that are specifically prepared for the covered materials during the theory.</p>	Security Consultant Ethical Hacker IT Management Chief Security Officer	Module 1: Packet Capturing Module 2: Layer 2 Attacks Module 3: Layer 3 Attacks on Cisco Based Infrastructures Module 4: Pivoting and Relays Module 5: IPv6 Attacks Module 6: VPN Attacks Module 7: Defeating SSL Module 8: IDS/IPS Evasion Lab 1: Working with Captured Files Lab 2: Layer 2 Attacks Lab 3: Attacking Routing Protocols Lab 4: Using Pivot Machines Lab 5: IPv6 Attacks Lab 6: VPN attack Lab 7: Defeating SSL, Decrypting Traffic and man-in-the-middle attacks Lab 8: NIDS/NIPS