Security Enterprise

2015 training catalog

Summer Edition

1-800-418-6789
www.learnsmartsystems.com

For more information about LearnSmart training contact us toll-free at 1-800-418-6789.

EDURISER
www.eduriser.com
Official India Partner

LearnSmart™

Mile2 Certified Digital Forensics Examiner (CDFE) Series

Digital Incidents, Investigating Computer Crimes, OS Disk Storage Concepts and Digital Acquisition

Course Number: 1475
Time: 165 Minutes
Number of Quizzes: 2 Quizzes

You will go through instruction on the methodology for conducting a computer forensic examination. Begin with an introduction to computer forensic incidents as you learn about the legal system, criminal incidents, computer fraud, internal threats, investigative challenges, and media volume. Then you'll dig into digital acquisition and analysis, and computer crime investigations. In the computer crime investigations section, you will go over the roles involved in computer forensics, how to form your team, risk assessment, forensic investigation toolkit, investigation methodology, forensic photography, and other investigation elements. There's also a section dedicated to operating system disk storage concepts, which concentrates on disk-based operating systems, and file and disk storage concepts. All in all, these topics will help prepare for the CDFE certification exam.

Introduction & Course Overview ..... 1475_001
Computer Forensics Incidents ..... 1475_002
Investigative Process ..... 1475_003
OS Disk Storage Concepts ..... 1475_004
Digital Acquisition and Analysis ..... 1475_005

Forensic Examination and Digital Evidence Protocols, Computer Forensics Investigative Theory and Digital Evidence Presentation

Course Number: 1476
Time: 130 Minutes
Number of Quizzes: 2 Quizzes

The following topics are essential to anyone encountering digital evidence while conducting an investigation. To start, you'll look at forensic examination protocols and forensic examination. From there, you'll focus on digital evidence protocols as you study digital evidence concepts and categories, learn the computer forensic investigative theory, and prepare for the digital evidence presentation. In the digital evidence presentation section, you'll train in compiling digital evidence, dealing with hearsay, and a summary of digital evidence. Gain an in-depth understanding of these topics to prepare for the CDFE certification exam.

Forensic Examination Protocols ..... 1476_001
Digital Evidence Protocols ..... 1476_002
Computer Forensics Investigative Theory .... 1476_003
Digital Evidence Presentation ..... 1476_004

Computer Forensics Laboratory Protocols and Processing Techniques, Digital Forensics Reporting and Specialized Artifact Recovery

Course Number: 1477
Time: 130 Minutes
Number of Quizzes: 1 Quiz

You will gain the skills and knowledge needed to perform forensically sound computer examinations, and to clearly and accurately report the findings. To report the findings of your investigation, you will need to run tests and reviews of the evidence through labs. To conduct those labs, you need to know computer forensics lab protocols. After the lab, you can then form an analysis report, which requires having an understanding of computer sciences, and knowing the laws of good report writing and the parts of a report. Another topic you need to be familiar with is specialized artifact recovery, which highlights file signatures, image file databases, the Windows registry, Windows Recycle Bin, and historical files. Utilize these topics to prepare for the CDFE certification exam.

Computer Forensic Laboratory Protocols .... 1477_001
Computer Forensics Processing Techniques 1477_002
Digital Forensics Reporting ..... 1477_003
Specialized Artifact Recovery ..... 1477_004

eDiscovery, Cell Phone Forensics, USB Forensics and Incident Handling

Course Number: 1478
Time: 180 Minutes
Number of Quizzes: 1 Quiz

Government or investigative agencies need proper training to succeed in cases involving acts of fraud, computer misuse, illegal pornography, counterfeiting, and so forth. Learn the tools, techniques, and knowledge to conduct an investigation. This training focuses on eDiscovery, cell phone forensics, USB forensics, and incident handling. The eDiscovery section provides you with details on discoverable ESI material, eDiscovery notification,

preserving information, eDiscovery products, metadata, data retention architecture, and tools for eDiscovery. In the incident handling section, you will learn about common security events of interest, incident handling steps, the incident response plan, identifying an incident, and more. There are also appendix sections discussing PDA forensics and investigating harassment. Studying these topics will help ready you for the CDFE certification exam.

■ Mile2 Certified Information Systems Security Officer (CISSO)

Risk and Security Management

Course Number: 1479
Time: 180 Minutes

Topics covered in the risk management section highlight control effectiveness, risk management and assessment, types of risk assessment, and the qualities of an asset, a threat source or agent, vulnerabilities, controls, likelihoods, and impacts. The security management section describes an enterprise security program, how to plan horizon components, control types, the security roadmap, senior management's role in security, security program components, human factors in security, employee management, human resources issues, recruitment issues, termination of employment, and enforcement. Upon completing this training, you will have actively learned the risk management mind-set. Gain an understanding of all these topics while preparing for the CISSO certification exam.

Authentication and Access Control

Course Number: 1480
Time: 180 Minutes
Number of Quizzes: 1 Quiz

Authentication covers access control terminology and administration, the trusted path, authentication mechanisms, authorization, fraud controls, biometrics technology and enrollment process, passwords and PINs, cryptographic keys, single sign-on technology, Kerberos components, federated authentication, and IDS. The access control section goes into detail on the role of access control, layers of access control, access control mechanisms and characteristics, preventive control types, information classification, enforcing a DAC policy, RBAC, the access control matrix, RADIUS, TACACS+ and Diameter characteristics, and control administration. Overall, in this training, you will hear theory discussed, and observe techniques demonstrated in an effort to prepare you for the CISSO certification exam.

Security Models and Operation Security

Course Number: 1481
Time: 180 Minutes
Number of Quizzes: 1 Quiz

You will learn both the theory and the requirements for practical implementation of core security concepts, practices, monitoring and compliance. You will specifically focus on security models, evaluation criteria, and operations security. Security models and evaluation criteria make up one portion of the course where you'll train in system protection, gain an understanding of the different security modes of operation, as well as study ITSEC ratings, common criteria components, and sets of requirements. And then through the operations security discussions, you will solidify your understanding of the role of operations, records management and change control, system controls, backup types, penetration testing, and threats to operations. Delve into these topics to thoroughly prepare for the CISSO certification exam.

Cryptography and Network Connections

Course Number: 1482
Time: 270 Minutes
Number of Quizzes: 2 Quizzes

The CISSO addresses the broad range of industry best practices, knowledge, and skills expected of a security leader. As you study cryptographic concepts, you will learn about symmetric cryptography, asymmetric cryptography, hashing, and PKI. And then in the network connections section, you'll dive into network connections, network protocols and devices. In addressing these two

topics, there are so many details to immerse yourself in and information to internalize. So take your time going through these presentations as you prepare for the CISSO certification exam.

Symmetric Cryptography and Hashing ..... 1482_001
Asymmetric Cryptograpy and PKI..... 1482_002
Network Connections..... 1482_003

Telephony, VPNs, Wireless and Security Architecture

Course Number: 1483
Time: 180 Minutes
Number of Quizzes: 1 Quiz

You'll spend time learning the concepts associated with telephony, VPNs, and wireless. The wireless section describes different wireless technologies, Wi-Fi network types, wireless network topologies, WEP, TKIP, network based attacks, and countermeasures to common wireless technology attacks. Additionally, the other topic covered in this course is security architecture. In discussing security architecture, you'll go over architectural models, how security functions on virtual machines and cloud computing, memory management, system functionality, and types of compromises. As you study the components and design of the security architecture, you will also be exposed to the different kinds of attacks you might encounter.

Telephony, VPNs and Wireless ..... 1483_001
Security Architecture..... 1483_002

Software Development Security, Database Security and System Development

Course Number: 1484
Time: 180 Minutes
Number of Quizzes: 1 Quiz

Go through discussions on software development security, where you'll learn the difference between device and software security, the trends associated with security, where to implement security, different development methodologies, security issues, module characteristics, ActiveX security, cookies, PCI requirements, and virtualization. The next portion of the course concentrates on database security and system development. The database security section covers different database models, the components in a database, database data integrity controls, add-on security, controlling access, and database security issues. Along with these topics, you will get into malware and software attacks, and business continuity. Gain an in-depth understanding of all these topics to ready yourself for the CISSO certification exam.

Software Development Security..... 1484_001
Database Security
and System Development..... 1484_002

Disaster Recovery and Physical Security Threats

Course Number: 1485
Time: 180 Minutes
Number of Quizzes: 2 Quizzes

Through the use of a risk-based approach, the CISSO is able to implement and maintain cost-effective security controls that are closely aligned with business requirements. Start out in the disaster discovery section as you go over proper planning, preventive measures to avoid a disaster, backup and redundancy options, disk shadowing, serial lines, the recovery plan, emergency response, and types of tests. You'll also go over incident management, security laws, and ethical practices. The last portion of this course explores physical security, which includes discussions on different types of threats and planning, facility site selection, controlling access, external boundary protection, lock types, perimeter protection, types of physical IDS, volumetric sensors, and environmental considerations. Learn all the ins and outs of security to prepare for the CISSO certification exam.

Disaster Recovery ..... 1485_001
Physical ..... 1485_002

Mile2 Certified Penetration Testing Engineer (CPTE)

(CPTE) Business and Technical Logistics of Penetration Testing and Linux Fundamentals

Course Number: 1486
Time: 120 Minutes

Mile2 certified individuals keep abreast of their expertise. So ensure that you're aware of the latest technologies and advances by learning the fundamentals of Linux and about business and technical logistics of penetration testing. Start out in the business and technical logistics of penetration testing section, which includes discussion on recent attacks and breaches, the cost of an attack, zombies, the evolving threat, penetration testing types, hacking methodology, reviewing a website, and seven management errors. As for Linux fundamentals, you will learn user account management, the steps to changing a password for a user, how to configure network interface, tarballs and zips, Linux boot CDs, and demonstrations of passwd/shadow files, BackTrack AddUser, and BackTrack

Passwd. Cover these topics to prepare for the CPTE certification exam.

Business and Technical
Logistics of Penetration Testing ..... 1486_001
Linux Fundamentals ..... 1486_002

Information Gathering and Detecting Live Systems

Course Number: 1487
Time: 120 Minutes
Number of Quizzes: 1 Quiz

For effective knowledge transfer, you must have a combination of theory and real world experience. In this training, you'll find these two elements utilized to instruct you in information gathering and detecting live systems. The detecting live systems section details the basics of scanning, how to port scan, countermeasures, and how to use tools like NMAP, Superscan, Unicornscan, auto scan, Amap, and fragrouter. And then the information gathering section provides you with discussions and demonstrations on the Leo Meta Text Editor, IHMC Cmap tools, social networks, digital access, passive versus active reconnaissance, Maltego, footprinting tools, DNS databases, people search engines, and footprinting countermeasures. Prepare for the CPTE certification exam.

Information Gathering ..... 1487_001
Detecting Live Systems ..... 1487_002

Enumeration and Vulnerability Assessments

Course Number: 1489
Time: 120 Minutes

On the network, vulnerabilities will be discovered using tried and true techniques based on five key elements. Explore vulnerability assessments and enumeration. The vulnerability assessments section provides you with demonstrations and details on vulnerability research sites, vulnerability scanners, dealing with assessment results, patch management options, and tools like Nessus, SAINT, RETINA, Qualys Guard, and MBSA. In the enumeration section, you'll learn about Web server banners, banner grabbing with Telnet and SuperScan, HTTPrint, DNS enumeration, zone transfers, SNMP insecurity and SNMP enumeration countermeasures, null sessions, Active Directory enumeration and countermeasures, NAT Directory attack tool, and THC-Hydra. With these topics, you will gain a deeper understanding of penetration testing concepts and will be further prepared for the CPTE exam.

Enumeration ..... 1489_001
Vulnerability Assessments ..... 1489_002

Malware, Windows and UNIX/Linux Hacking

Course Number: 1490
Time: 185 Minutes
Number of Quizzes: 1 Quiz

Ready yourself for the CPTE certification exam as you study malware, Windows hacking, and hacking UNIX/Linux. The malware section mostly covers the tools used to combat malware specifically Netcat, Restorator, and port monitoring. In the Windows hacking section, you will go over password guessing, syskey encryption, cracking techniques, precomputation detail, password sniffing, monitoring logs, hard disk security, tokens and smart cards, covering tracks, steganography, leaving no local trace, encrypted tunnel notes, and hacking tools like RootKit, NTPASWD, and Ophcrack. Then the hacking UNIX/Linux section describes the processes involved in hacking, the file system structure, Kernel, command assistance, accounts and groups, Link and UNIX permissions, auditing, common network services, attacks, countermeasures, salting, symbolic link, and file and directory permissions.

Malware ..... 1490_001
Windows Hacking ..... 1490_002
Hacking UNIX/Linux ..... 1490_003

Advanced Exploitation Techniques and Pen Testing Wireless Networks

Course Number: 1491
Time: 120 Minutes
Number of Quizzes: 1 Quiz

In studying advanced exploitation techniques, you'll look at format strings, race conditions, buffer and heap overflows, heap spraying, security code, stages of exploit development, and the Metasploit project. You'll also spend time learning how to implement penetration testing on wireless networks. This section explains how WPA improves on WEP, LEAP, a typical wired/wireless network, new age protection, and different tools. CPTE's foundation is built firmly upon proven hands-on Penetration Testing methodologies as utilized by the CWNP's international group of vulnerability consultants. Learn all the details, knowledge, and skills associated with exploitation techniques and penetration testing in wireless networks to deepen your understanding of Penetration Testing methodologies. Moreover, this training is designed to help prepare you for the CPTE certification exam.

Advanced Exploitation Techniques ..... 1491_001
Pen Testing Wireless Networks ..... 1491_002

Networks, Sniffing, IDS and Attacking Web Technologies

Course Number: 1492
Time: 120 Minutes
Number of Quizzes: 1 Quiz

Through this training, you will gain an in-depth understanding of networks, sniffing, IDS, and how to attack Web technologies. The attacking Web technologies section goes over finding and fixing un-validated input, attacks against IIS, unicode, IIS logs, NTOSpider, HTTrack Website Copier, paros and burp proxy, cookies, and the Acunetix Web Scanner. Most of the discussions involving networks, sniffing, and IDs centralizes on tools like Wireshark, packetyzer, OmniPeek, Cain and Abel, Ettercap, and DNS spoofing. Other discussions in this section are about session hijacking, Voice over IP, intercepting RDP, routing protocols analysis, evading the firewall and IDS, and new age protection. Immerse yourself in these topics to prepare for the CPTE certification exam.

Networks, Sniffing, IDS ..... 1492_001
Attacking Web Technologies..... 1492_002

Project Documentation and Financial Sector Regulations Pertaining to Pen Testing

Course Number: 1493
Time: 120 Minutes

You'll spend the majority of your time studying financial sector regulations. In this section, you'll cover things like IT governance best practices, IT risk management, types of risks, risk management, information security risk evaluation, improving security posture, risk evaluation activities, risk assessment, compliance, IT applications and security, IT issue for SOX, dirty dozen, change control and auditing, and total cost of compliance. The other topic covered in this training is project documentation. Project documentation explains how to analyze risk, the report results matrix, how to deliver the report, the executive summary, the technical report, the report table of contents, and how to format summary observations. All in all, these topics will prepare you to sit for the CPTE certification exam.

Project Documentation..... 1493_001
Financial Sector Regulations
Pertaining to Pen Testing..... 1493_002

Access Controls and Protocols

Course Number: 1494
Time: 120 Minutes
Number of Quizzes: 1 Quiz

Mile2 goes far beyond simply teaching you to "hack." You'll spend time training in access controls and protocols. In the protocols section, you will go through the OSI model layers and the protocols at each layer, the TCP/IP suite, the port and protocol relationship, the conceptual use of ports, the difference between UDP and TCP, and the SSH security protocol. Other protocol types that you'll study include ARP, ICMP, SNMP, and SMTP. Gain a thorough understanding of penetration testing using advanced persistent threat techniques along with the highest level ethical hacking methodologies in preparation for the CPTE certification exam.

Access Controls..... 1494_001
Protocols..... 1494_002

■ CCNA Security Series

Security and Cisco Routers

Course Number: 919
Time: 105 Minutes
Number of Quizzes: 5 Quizzes

You will find discussions on the common security threats within a network and take a look at network and information security basics. You will review some of the fundamental security principles. Go through descriptions of common security threats to Cisco devices, as well as all network devices and networks. You will also spend time studying how to secure the control, data and management planes on Cisco devices, including implementing security on Cisco routers. You will also take a look at Cisco Security Manager. There's also a section dedicated to IP version 6, along with the different types and formats of associated addresses. Deepen your understanding of these security concepts to prepare for the CCNA Security exam.

Common Security Threats..... 919_001
Cisco Security ..... 919_002
IPv4 to IPv6..... 919_003

AAA on Cisco Devices

Course Number: 920
Time: 45 Minutes
Number of Quizzes: 4 Quizzes

Gain an understanding of TACACS and RADIUS. You'll take a look at the differences between them regarding what they offer as an authentication type, and how to configure each one. You will also take some time to discuss AAA – looking at its definition, and then at some

design considerations for implementing it. You'll go over examples of ways in which you can configure AAA, via the Command Line Interface and Cisco Configuration Professional, along with some verification commands. All in all, the topics stem from the exam objective AAA on Cisco Devices, and will aid in preparing you for the CCNA Security exam.

TACACS versus RADIUS..... 920_001
AAA ..... 920_002

IOS ACLs

Course Number: 921
Time: 45 Minutes
Number of Quizzes: 4 Quizzes

With this training you are provided with an overview of Access Control Lists, or ACLs. ACLs help to mitigate threats against a network in a variety of ways. ACLs should be tested in a test environment prior to actually applying them. You will take a look at exactly what they are, what they do, and discuss the different types of ACLs and the role they play in security. The training progresses from teaching you the basics to showing you how to effectively work with ACLs in terms of security. Topics covered include types of attacks to ACLs, and details on standard access, extended access, and named access lists. Altogether, these topics will help prepare you to sit for the CCNA Security exam as you focus on the IOS ACLs exam topic.

IOS Access Control Lists ..... 921_001
Mitigating Threats ..... 921_002

Secure Network Management

Course Number: 922
Time: 45 Minutes
Number of Quizzes: 3 Quizzes

You will focus on securing the management plane. You will start off by learning to define the management plane, and learning some best practices that can be used to make it more secure, such as strong passwords, AAA, Role Based Access Control, Syslog, and NTP. Then, you will learn to identify and study demonstrations of the different configurations that can be implemented on the management plane. You will also concentrate on strong passwords, SNMP, and Cisco Resilient Configuration. The topics covered in this course are encompassed in the Secure Network Management exam objective, and will aid in preparing you for the CCNA Security certification exam.

Network Management..... 922_001
Course Review ..... 922_002

Common Layer 2 Attacks

Course Number: 923
Time: 90 Minutes
Number of Quizzes: 5 Quizzes

Common Layer 2 Attacks is an exam objective in the CCNA Security certification exam. In preparation for this exam, you are going to cover concepts like configuring VLANs, trunking, securing switches, and optimizing spanning tree. You will begin by taking a look at VLANs, or Virtual Local Area Networks. After taking some time to define VLANs and describe their purpose, you will find discussions on VTP, which is the VLAN Trunking Protocol, and then focus on trunking itself. You will also learn about InterVLAN routing and port security on switches. Learn how to identify security implementations that should be considered with designing a network, such as enable password access, authentication servers like RADIUS and TACACS+, and disabling IOS services that come standard on Cisco devices. Finally, you will learn the definition of spanning tree, and then you will look at ways in which you can implement and optimize it. Gain an in-depth understanding of these topics to determine how to best respond to layer 2 attacks.

VLANs and Trunking..... 923_001
Securing Switches ..... 923_002
Spanning Tree..... 923_003

Cisco Firewall Technologies

Course Number: 924
Time: 90 Minutes
Number of Quizzes: 5 Quizzes

Cisco Firewall Technologies explains the different firewall technologies and the strengths and weaknesses that surround them. The concept of a stateful firewall is introduced, as well as what it means when it comes to protecting your network. Zone based firewalls and the Cisco ASA series of firewall appliances and the ways in which these devices can be implemented within your network is discussed. Network Address Translation (NAT), and Port Address Translation (PAT) are introduced and the reasons for which they are both needed are explained in detail.

Firewall Technologies ..... 924_001
Types of Firewalls ..... 924_002
NAT and PAT..... 924_003

Cisco IPS

Course Number: 925
Time: 45 Minutes
Number of Quizzes: 2 Quizzes

Cisco IPS discusses the differences between a Cisco IPS and Cisco IDS device, and some options that you have when deploying them in your network. The type of traffic analysis and the actions that can be performed by each of these devices on malicious traffic that is detected in your network is described. The steps to configure Cisco IPS are demonstrated as well as some best practices to consider when deploying an IPS or IDS device. The topics covered will teach the fundamentals of Cisco IPS, and prepare you for the CCNA Security exam.

IPS Deployment ..... 925_001
Course Review ..... 925_002

VPN Technologies

Course Number: 926
Time: 60 Minutes
Number of Quizzes: 4 Quizzes

You will go through discussions on the basics of VPN technologies, and how IPSec works in a VPN tunnel setup. You will also look at the basics of cryptography in order to gain a better understanding of exactly what goes on behind the scenes of a VPN tunnel establishment. Finally, you will walk through different ways of implementing a site-to-site VPN and configured SSL VPN using the graphical device manager from an ASA.

Virtual Private Networks ..... 926_001
Site-to-Site VPN ..... 926_002

Test Me: Cisco Exam CCNA Security 640-554 IINS

Course Number: 1850
Time: 90 Minutes
Number of Quizzes: 1 Quiz

Test your knowledge and skills through this Test Me: Cisco Exam CCNA Security 640-554 IINS. Prove to yourself, and others, that you are ready for Cisco's Implementing Cisco IOS Network Security certification exam. You'll demonstrate your proficiency in the principles, techniques, and tools involved in working with routers, networks, and switches. The instruction period is over; this Test Me provides you with a collection of questions based on the exam domains contained in testing for the actual certification exam. Wrap up your exam preparation with this Test Me pulling questions from our Cisco IOS Network Security course series.

CISSP® 2013 Series

Telecommunications & Network Security 2013

Course Number: 836
Time: 195 Minutes

When it comes to information security, there are a range of concepts, skills, and issues to understand to properly administer network security. The CISSP exam assesses how thorough your knowledge is in the area of information security. Pick up the knowledge needed to prepare for this certification exam. Study the OSI model and layers to understand how communication flows across the network, see how to implement Remote Access, and look at media and LAN topologies like fiber optics, star topology, tree topology, and mesh topology. You will also learn about security elements that will protect the network through firewalls, security protocols, and various security techniques. At the conclusion of this course, you will understand how to implement network security and maintain telecommunications.

OSI Reference Model ..... 836_001
OSI Layers ..... 836_002
Media/LAN Topologies ..... 836_003
LAN/WAN/Remote Access ..... 836_004
Remote Access Security ..... 836_005
Network Devices ..... 836_006
Firewalls ..... 836_007
Security Protocols and Services ..... 836_008
Security Techniques ..... 836_009
Common Network Attacks ..... 836_010

Information Security Governance and Risk Management 2013

Course Number: 837
Time: 135 Minutes

The Certified Information Systems Security Professional (CISSP) designation is a recognized international standard for information security certifications. The CISSP series will provide certification candidates with an understanding of crucial security issues and solutions to address them. Start out with an overview of CISSP, its requirements, and the importance of confidentiality, integrity, and availability. You will then learn about security management training by studying information security governance, audit frameworks for compliance, security administration, physical and human risks, legal responsibilities, and risk assessment methodologies. The remainder of the course

looks at risk assessment, job policies and training, and security policies.

Software Development Security 2013

Course Number: 838
Time: 285 Minutes

Attention is given to software development security to deepen your understanding of information security. Topics covered include application issues, storage, development controls, malicious code, and methods of attack. The material you will study can be divided up into different categories: software development issues and storage, software development protection, and software development threats. The discussion on storage focuses on databases, warehouses, virtual memory, information retrieval, knowledge-based systems, and audits. With development controls, the two types focused on are system development controls and security development controls where you will learn about the isolation architecture, coding controls, and certification standards.

Cryptography 2013

Course Number: 839
Time: 105 Minutes

The Certified Information Systems Security Professional (CISSP) designation is a recognized international standard for information security certifications. You will specifically focus on the concept and implementation of cryptography. To solidify your understanding of cryptography, you will look at its history, its uses, and its role in confidentiality, integrity, and authentication. Some concepts associated with cryptography are transposition cipher, steganography, substitution cipher, digital signatures, asymmetric algorithms, and message authentication. You will also learn about the various methods of attack as in brute force, man-in-the-middle, chosen ciphertext, and replay.

Security Architecture and Design 2013

Course Number: 840
Time: 135 Minutes

The Certified Information Systems Security Professional (CISSP) designation is a recognized international standard for information security certifications. Obtaining your CISSP certification ensures that you're trained in information security concepts and skills. Explore the security architecture and design by studying its organization, machine operation, protection mechanisms, and security models. Additionally, you will also learn about security evaluation criteria, common flaws, and security issues in covert channels, the parameter, timing, EMR, and programming.

Operations Security 2013

Course Number: 841
Time: 120 Minutes

Once a network is set up and configured, it becomes the administrators responsibility to ensure that network operations, or day-to-day activities, are executed correctly and safely. Concentrating on network operations, you will learn about administrative management, operation controls, auditing, monitoring, intrusion detection, threats, and countermeasures. In the auditing and monitoring sections, you will take a closer look at audit procedures, audit reporting, sampling, keystroke monitoring, trend analysis, and failure recognition. Upon course completion, you will understand security concepts and issues concerning operations security in the CBK required for the CISSP exam.

Business Continuity and Disaster Recovery Planning 2013

Course Number: 842
Time: 90 Minutes

When a disaster occurs on a network due to attack or some other issue, network administrators must have a plan for restoring and re-securing the network. Creating a disaster recovery plan involves elements such as an emergency response, backup data, off-site storage, and logistics. Once you've create a plan, you have to know how to execute it by training all administrators involved in network security, walking through the checklist, and running scenarios. These are all topics covered in this training. It falls under the umbrella of Business Continuity Planning (BCP) to preserve the network. Additional topics that are encompassed in BCP include ensuring legislative compliance, establishing a planning team, understanding legal and resource requirements, as well as performing a business impact analysis. Maintaining network security is equally preventive measures as well as planning.

Legal, Regulations, Investigations & Compliance 2013

Course Number: 843
Time: 120 Minutes

Prepare for your CISSP certification by studying laws and regulations on security. Learn about the different types of computer crime as in grudge attacks, financial attacks, military attacks, fun attacks, and hacking. You will also spend time looking at the different categories of law, computer laws, types of incidents and how to respond to them, and the ethics behind information security. You will also find explanations on investigation practices and how evidence is gained. Altogether, your studies will deepen your understanding of how to be compliant, the laws behind security, and lessons learned through some example investigations.

Physical (Environmental) Security 2013

Course Number: 844
Time: 90 Minutes

Deepen your understanding of crucial CISSP security concepts and issues. Focus your attention on physical security by studying physical security threats, facility requirements as in security policies and a critical path analysis, physical security controls, environmental issue, and ways to implement physical security. In the discussion on threats, you will work through Threats 1-12. Additionally, some of the techniques concentrated on for implementing physical security are fire safety, physical access control, administrative controls, egress safety, and detective controls.

Access Control 2013

Course Number: 845
Time: 120 Minutes

Concentrate on Access Control. Start with the basics by studying the concepts of least privilege, accountability, and physical, logical, and administrative access. You will also explore the topics of data classification, Access Control techniques, Access Control Implementation, identification, authentication, attack, and monitor Access Control. Some of the topics covered in Access Control techniques are control types and categories, security labels, and Access Control lists. The information detailed will provide certification candidates with the skills and knowledge needed to prepare for the CISSP exam.

Test Me: (ISC)² Exam CISSP

Course Number: 1853
Time: 360 Minutes
Number of Quizzes: 1 Quiz

Test your knowledge and skills through this Test Me: (ISC)² Exam CISSP. Prove to yourself, and others, that you are ready for (ISC)²'s Certified Information Systems Security Professional (CISSP) certification exam. You'll demonstrate your proficiency in the principles, techniques, and tools involved in securing data that's collected and distributed within hardware and software systems. The instruction period is over; this Test Me provides you with a collection of questions based on the exam domains contained in testing for the actual certification exam. Wrap up your exam preparation with this Test Me pulling questions from our CISSP course series.

■ Securing and Managing XenApp 6.5 Series

Planning Policies and Administering Performance and Load in Citrix XenApp 6.5

Course Number: 1497
Time: 60 Minutes
Number of Quizzes: 3 Quizzes
Number of Labs: 2 Labs

Part of implementing security on XenApp 6.5 is working with policies and administering performance and load. To help you learn about policies, it is broken up into two section planning policies and creating policies. In the administering performance and load section, the discussions address sessions, monitoring sessions, maintaining connections, optimizing and customizing sessions, controlling application instances, and folder redirection. Delve into these topics to learn how to effectively secure Citrix XenApp 6.5.

Planning Policies ..... 1497_001
Creating Policies ..... 1497_002
Administering Performance and Load ..... 1497_003

Securing XenApp, Update and Patch Management, Zones and Server Management, User Profiles and Troubleshooting in Citrix XenApp 6.5

Course Number: 1498
Time: 105 Minutes
Number of Quizzes: 5 Quizzes
Number of Labs: 2 Labs

The majority of your time in this training will be spent looking at security options for XenApp 6.5. For the discussions on security, you will learn about failover options, high availability, site redirection, configuration, security settings, working with multiple farms, and configuring authentication. Then you'll shift your attention to managing XenApp as you look at update and patch management, zones and server management, and troubleshooting options concentrating on functionality and performance, and load evaluators. In the update and patch management section, you will get to work with Windows Server, hot fixes; while the zones and server management section covers servers, worker groups, and zones. Having covered these topics, you will be better skilled in securing and managing Citrix XenApp 6.5.

Securing XenApp ..... 1498_001
Update and Patch Management ..... 1498_002
Zones and Server Management ..... 1498_003
User Profiles ..... 1498_004
Troubleshooting ..... 1498_005

■ CEHv8 Series

Footprinting

Course Number: 1676
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Footprinting is the gathering of information related to a particular computer and its users and systems. In this course you will learn the various tools and techniques used in footprinting as well as prevention and countermeasures that you can take to protect yourself and your systems. We will pair this with in-depth demos on some of the tools and their uses.

Footprinting/Reconnaissance ..... 1676_001
Methodology ..... 1676_002
Tools ..... 1676_003
Countermeasures ..... 1676_004

Reconnaissance

Course Number: 1677
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Reconnaissance is an exploration that is conducted to gain information. In this course, you will be learning the tools and steps for assessing computers, computer systems, networks, and applications. We will include in-depth demos that go into further detail on the uses of many of these tools.

Reconnaissance ..... 1677_001
Footprinting ..... 1677_002
Scanning ..... 1677_003
Countermeasures ..... 1677_004

Banner Grabbing

Course Number: 1681
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Banner grabbing is a technique used to grab information about computer systems on a network and the services running its open ports. In the course Banner Grabbing, you will be learning the tools and techniques used in the process of banner grabbing. You will learn how to take inventory of the systems and services on your networks. You will be able to identify potential risks of banner grabbing and learn steps to take to protect your networks and systems from the potential threat of an intruder using banner grabbing. We will pair this course with demos on the tools you will be discussing.

Banner Grabbing ..... 1681_001
Countermeasures ..... 1681_002

Enumeration

Course Number: 1682
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Every system has its own services running on the network, in many cases those services can reveal sensitive information about network topology, users and groups, etc. services like LDAP or NTP can be enumerated to reveal such information. In this course you will be introduced to enumeration and the many different uses it has in computer systems. This course will include demos on the different tools and uses of enumeration.

Enumeration ..... 1682_001
Enumerating Services and Countermeasures 1682_002

Linux Fundamentals

Course Number: 1671
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Linux was developed as a free operating system for Intel x86 based personal computers. It is a leading operating system on servers. Linux runs on embedded systems. The most widely used operating system for mobile technology (tablets and smartphones) is built on top of the Linux kernel. In this course you will be learning the fundamentals of Linux. We will be pairing this course with demos with a more in-depth look into some of the fundamentals and tools of Linux.

Introduction to Linux ..... 1671_001
Working in Linux ..... 1671_002

Configuring Linux for Pentesting

Course Number: 1672
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Servers are primary targets for attackers. Pentesting is an attack on a system in hopes of finding security weaknesses. In the course Configuring Linux for Pentesting, you will be learning the steps to configure Linux for pentesting and tools used for pentesting on a Linux system. This course will be combined with demos that will delve deeper and give you real world examples of the tools and programs that Linux uses to accomplish pentesting.

Configuring Linux for Pentesting..... 1672_001
Pentesting on Linux..... 1672_002

System Hacking

Course Number: 1683
Time: 90 Minutes
Number of Quizzes: 4 Quizzes

Ensure that you know everything involved in securing a Windows system against attack. During this course you'll get into Windows passwords — how they're created, how they're stored, and different methods used to crack them. You'll discover different methods used for guessing passwords and breaking the different security methods used within the Windows operating system. You'll find discussions on responding to privilege escalation. You'll also spend some time going through a couple of scenarios demonstrating how to use key defense tools. Overall, the topics explored here will teach you how to increase security on your Windows machines, as well as show you required procedures and tools to prepare for different certification exams from EC-Council, CompTIA, Linux, and CISSP.

Windows Hacking ..... 1683_001
Password Attacks..... 1683_002
Alternate Data Streams ..... 1683_003
Steganography..... 1683_004
Rootkits ..... 1683_005
Course Summary ..... 1683_006

Spyware & Keyloggers

Course Number: 1684
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

You will take a good look at spyware, the activities it performs, different types of spyware, and the countermeasures needed in order to prevent hackers from utilizing these types of techniques against your company.

You will also spend time studying different types of keyloggers. There are three different types of keyloggers that we see used in today's environments: hardware, software, and kernel/driver keyloggers. A good pen tester or ethical hacker cannot perform his or her job properly without understanding the countermeasures for all of the hacking techniques used against today's computer systems. Overall, these topics will help prepare you for certification exams from vendors, such as Linux, CompTIA, and EC-Council.

Spyware Uncovered ..... 1684_001
Keyloggers ..... 1684_002

Viruses and Worms

Course Number: 1686
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

You will discover what viruses and worms are and how they can infect computers and systems. You'll study their nature, how they function, and their impact. You will also spend time going through discussions on varieties of each, along with some real life examples. Refine your understanding of viruses and worms to better your system. The knowledge you gain here will prepare you to be a more effective network administrator. Furthermore, the topics covered here will help with preparing you for security certification exams offered by EC-Council, CompTIA, and Linux.

Viruses ..... 1686_001
Worms ..... 1686_002

Denial-of-Service

Course Number: 1689
Time: 90 Minutes
Number of Quizzes: 4 Quizzes

Become familiar with the following concepts: denial-of-service, distributed denial-of-service, and how the denial-of-service and distributed denial-of-service attacks take place. You will also see what botnets are and how they are used to attack your system or network. You will find explanations on the tools that are used to attack, and how you can detect such attacks. You will be introduced to different countermeasures, so that you can plan, prepare, and establish the relevant countermeasures to protect your organization. You will also learn how DoS and DDoS can be used in penetration testing. You will go through discussions on how to protect your organization from the distributed denial-of-service attacks and denial-of-service penetration testing. Altogether, these topics focus on deepening your understanding of security concepts and practices, so that you're a more efficient network administrator. With the skills you gain here, you're equipped to pursue a number of security certifications from CompTIA, EC-Council, and CEH.

Denial-of-Service &
Distributed Denial-of-Service ..... 1689_001
Digital Attack Map ..... 1689_002
Botnets ..... 1689_003
DoS/DDoS Attack Tools and Detection ..... 1689_004
DoS/DDoS Countermeasures ..... 1689_005
DoS/DDoS in Penetration Testing ..... 1689_006

Vulnerability Assessment

Course Number: 1670
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Our course Vulnerability Assessment will introduced to the concepts of: Vulnerability Assessment, Vulnerability Assessment Tools, and Patch Management. It will offer demos on several of the vulnerability assessment tools that are available, as well as in-depth discussions on the benefits of these tools. We will discuss the process of analyzing the scan results that the vulnerability assessment tools provide. Finally, we will discuss patch management and some tools that are available for this process, and at the end of this course you will be able to create a comprehensive VA program, identify key vulnerabilities, and perform mitigation actions before those vulnerabilities can be exploited.

Testing Vulnerabilities ..... 1670_001
Results, Reports, and Remediation ..... 1670_002

Covering Tracks

Course Number: 1688
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

This course will be going over various ways that attackers have at their disposal to cover any tracks that may lead to their unwanted eviction or worse yet to an audit trail that would lead directly back to them. In this course we will be discussing, disabling auditing during or after an event, steps to take once it is disabled, and destroying any evidence. We will be going over various ways to avoid detection on Linux machines, and this will include several in-depth demos on various operations for the Linux machines.

Avoiding Detection on Windows Machines . 1688_001
Avoiding Detection on Linux Machines ..... 1688_002
Destroying the Evidence ..... 1688_003
Log Protection Techniques ..... 1688_004

Disaster Recovery and Risk Management

Course Number: 1668
Time: 30 Minutes
Number of Quizzes: 3 Quizzes

Since you are a part of IT operations in your enterprise, you could be involved in planning and applying policies related to Risk Management and/or Disaster Recovery. In our course Disaster Recovery and Risk Management, you will receive an introduction to the basics of Risk Management and Disaster Recovery. When you have completed the course, you will be able to identify a risk and the effect that it has on daily operations. You will gain an understanding of security measures and how they are implemented, as well as the importance and the process of managing risk in your environment. We will partner this with a detailed demo on the process of risk assessment. You will gain an understanding of Disaster Recovery, be able to define what a disaster is, rank a disaster, and create a plan that will define how to recover from a disaster, as well as successfully recovering your data.

Risk Management..... 1668_001
Disaster Recovery ..... 1668_002

Trojans and Backdoors

Course Number: 1685
Time: 90 Minutes
Number of Quizzes: 4 Quizzes

As an ethical hacker, there are times when you need to hide software from the company that you are performing the test against in order to verify that the defensive strategy is able to find your software. Trojans and Backdoors is the course where our software is going to be going undercover. In this course we are going to define malware and take a look at how a payload is delivered. We will overview the various Trojan tools, and tools used to generate Trojan programs, as well as learning about Netcat. We will spend time going over countermeasures and various anti-Trojan software and hardware, and preventive methods that can be used to prevent attacks. We will also be incorporating several demos on the many tools that we will be discussing in this course.

Defining Malware..... 1685_001
Malware..... 1685_002
Tools of the Trade..... 1685_003
Countermeasures ..... 1685_004
Course Summary ..... 1685_005

Introduction to Ethical Hacking

Course Number: 1667
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

Ethical hacking is testing the resources for a good cause and for the betterment of technology. In our course Introduction to Ethical Hacking, you will be introduced to various concepts on ethical hacking. We will be talking about vulnerabilities, exploits, defense strategy, penetration testing, pentest types and methodology, vulnerability management, incident management, and security policy development, and at the end of this course we hope you will have a basic understanding of the various concepts involved in ethical hacking.

Introduction to Hacking ..... 1667_001
Security Management..... 1667_002

Penetration Testing

Course Number: 1669
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

Pentesting is an intentional attack on a system to discover security weaknesses. These can be left either by the security officer or the security controls. Penetration Testing is our course that covers security, vulnerabilities, different types of tests, and when to test as a pen tester. We have paired this with an in-depth demo on vulnerability assessment using the tool Nexpose. At the end of this course we will have reviewed security and vulnerability assessment, and the differences between automatic and manual testing.

Penetration Testing Introduction ..... 1669_001
Organizational Considerations ..... 1669_002

Port Scanning

Course Number: 1680
Time: 105 Minutes
Number of Quizzes: 3 Quizzes

When a port is scanned on a server, the port returns a response indicating that the port is open and a service is listening. In our course Port Scanning, you will learn how ports can be scanned, how a hacker can break into your network through the ports, and the countermeasures you can take to protect your device or network. Our course will offer in-depth discussions on port scanning methods and techniques, port scanning tools, and port scanning countermeasures. We will partner this with detailed demos on Ping, Ping tester, and Netstat.

Port Scanning ..... 1680_001
Advanced Techniques..... 1680_002

Sniffers

Course Number: 1687
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

Sniffers is our course where we take a look at Network Sniffing. We will be covering the basics of packet sniffing, ARP cache poisoning, DNS spoofing, SSL sniffing, VoIP phone calls and sniffing remote desktop connections. This will be coupled with demos on Wireshark, ARP poisoning, and XARP.

Network Sniffing ..... 1687_001
Security Measures ..... 1687_002

Advanced Exploitation Techniques

Course Number: 1870
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

Exploit is a common term in the computer security community that refers to a piece of software that takes advantage of a bug or glitch. In our course Advanced Exploitation Techniques, you will learn what advanced exploitation techniques are and how you can use them in your penetration testing. You will also learn how to use Metasploit to exploit vulnerabilities. This will be coupled with in-depth demos on using Metasploit, and other Metasploit tools, such as, Meterpreter, Armitage, and Armitage-mimikatz.

Advanced Exploiting Techniques..... 1870_001
Penetration Testing..... 1870_002
Exploits ..... 1870_003

Cryptography

Course Number: 1673
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Traditional cryptography uses a secret key for encrypting and decrypting a message. This is also known as symmetric keys. Public key cryptography, the CA creates private and public keys using the same algorithm, it functions asymmetrically. In the course Cryptography, you will discuss Public Key Infrastructures, Certificate Authorities, and Certificate management. We will combine that with in-depth demos on PKI Installation, Config-complete, CRL, Enroll Certificate, and CA Management. We will discuss the steps to create and manage a public key infrastructure, and the relationship between public key infrastructures and certificate authority, as well as, both traditional cryptography and public key cryptography, the implementation of certificates, and managing certificates.

Certificates..... 1673_001
Using Secure Certificates ..... 1673_002

Scanning Networks

Course Number: 1679
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

Network scanning is the scanning of public or private networks to find out which systems are running, their IP addresses, and which services they are running. In our course Network Scanning, you will learn techniques for private and public network scanning using various tools. Accompanied with in-depth demos and discussions on how to use Angry IP, Nmap, Hping, and Zmap network scanners. Through this, you will learn the steps to network scanning, how to draw a network map, and plan an attack accordingly.

Private and Public Network Scanning..... 1679_001
Using Zmap..... 1679_002

Hacking Web and App Servers

Course Number: 1690
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Hacking Web and Application Servers, is a course that will give us a good idea about vulnerabilities and attacks available for web servers and web applications. This course includes in-depth demos on several of the tools used for hacking web servers and application servers. These tools include Apache2, Netcraft, Website Mirroring, W3AF, and WMAP. By the end of this course we will have discussed various ways to collect information from web servers, application server attacks, and finding vulnerabilities in a server.

Web Server Attacks ..... 1690_001
Web Application Attacks..... 1690_002

SQL Injections

Course Number: 1691
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

SQL injection is the most used of all attacks. In this course, SQL Injections, you will be learning how SQL injections can be initiated, cause damage or loss, prevention against such attacks, and discussing detection tools. This course includes demos demonstrating BSQL tool as well as SQL Injection Username and Password. By the end of this course you will have covered SQL injection methodology, attacks, buffer overflow exploit, testing for SQL injection, countermeasures and detection tools.

SQl Injections..... 1691_001
Protecting Against SQL Injections..... 1691_002

Session Hijacking

Course Number: 1692
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

Have you heard the words session hijacking? Simply put, it is defined as an intruder taking over a genuine session between two computers and using if for sinister purposes. In the course Session Hijacking, you will learn details about session hijacking, well-known techniques employed by aggressors, the steps involved in session hijacking, various types of session hijacking, tools for hijacking sessions, ways you can protect yourselves from session hijacking, and how pentesting can be used to identify vulnerabilities.

Session Hijacking ..... 1692_001
Countermeasures ..... 1962_002

Buffer Overflows

Course Number: 1693
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Buffer overflow occurs when you try to store more data than what the allocated buffer or storage area can hold. In this course you will be introduced to the concepts of buffer overflows, how they happen, and how attackers take advantage of them. You will also learn how to defend against buffer overflow attacks, and what security measures you can take to protect your data. We will accompany this with several demos that will delve deeper and help you understand some of the specific topics that will be discussed.

Buffer Flow ..... 1693_001
Program and Application Vulnerability ..... 1693_002
Defense, Countermeasures, and Security ..... 1693_003

Hacking Wireless Networks

Course Number: 1695
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

Wireless attacks have become easy; even unskilled people with little computer literacy can accomplish them. This is because of the many automated tools available to perform this hack. In our course Hacking Wireless Networks, we will not be focusing on weaknesses of your wireless networks or how to protect them, instead, we will focus on showing you how to gain access to a wireless network.

Hacking Wireless Networks ..... 1695_001
Hacking Windows ..... 1695_002

Social Engineering

Course Number: 1678
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

Social engineering is the art of extorting employees for information. It can take the form of human-based or digital. In our course Social Engineering, you will learn what social engineering is, who's at risk, and how to protect and educate your employees against social engineering. You will learn the importance of creating a security policy, and how to deal with the threat of human-based attacks from both outside and inside the company. You will learn what kind of risks computer-based attacks, and social media present. We will couple this with in-depth demos on phishing email, SET-webTemplate, SET-spear phishing, SET-trojan, and SET SMS Spoofing.

Social Engineering ..... 1678_001
Social Engineering Demos ..... 1678_002

Authentication Systems

Course Number: 1674
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

Whenever we login to a computer system, we provide information it identify ourselves. We refer to this as authentication. Authentication has been developed to contain more than just username and password because we are looking for added layers of security. In this course we will be covering authentication factors, forms of authentication, and authentication protocols. We will also be going over RADIUS, LDAP, and SSO. We will pair this with several demos depicting practical uses of the many tools that we will discuss in this course.

Introduction ..... 1674_001
Authentication Protocols ..... 1674_002
RADIUS, LDAP, and SSQ ..... 1674_003

Cryptography Weaknesses

Course Number: 1675
Time: 75 Minutes
Number of Quizzes: 4 Quizzes

Cryptography is the science of writing in secret code and is considered an ancient art. The first documented use of cryptography dates back to circa 1900 B.C. In our course Cryptography Weaknesses, we will discuss weaknesses in cryptography and ways to improve your security. We will also cover the use of symmetric and asymmetric keys and the use of hybrid keys, as well as, the use of hashing algorithms and digital signatures. We will pair this with

several demos to show you how each of these works in practical situations.

Encryption ..... 1675_001
Symmetric Encryption ..... 1675_002
Asymmetric Encryption ..... 1675_003
Hashing Algorithms ..... 1675_004
Digital Signatures ..... 1675_005

Cross-Site Scripting

Course Number: 1694
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

As a security tester or security analyst, it is important that you are aware of cross-site scripting vulnerabilities and how they may be exploited by attackers. In our course Cross-site Scripting, you will gain a comprehensive understanding of cross-site scripting, you will learn how to prevent it, and how you can test to identify cross-site scripting vulnerabilities. You will also learn what cross-site scripting is and the different types of cross-site scripting you may come across. This course will also be paired with several demos that give you a real world view of what we have and will cover in this course.

Cross-Site Scripting ..... 1694_001
Types of Cross-Site Scripting ..... 1694_002
Preventing Cross-Site Scripting ..... 1694_003

Mobile Hacking Basics

Course Number: 1697
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

Mobile hacking can be anything from searching for unlocked Wi-Fi networks, to the hacking of Android OS or IOS systems. In our course Mobile Hacking Basics, we will give you a basic introduction of the tools and concepts behind mobile hacking with demos giving you a look at some of these tools in action.

Securing Mobile Basics ..... 1697_001
Mobile Security Considerations ..... 1697_002
Hardening Mobile Devices ..... 1697_003

Physical Security

Course Number: 1699
Time: 75 Minutes
Number of Quizzes: 4 Quizzes

What kind of security measures do you take to protect your facilities, equipment, resources, personnel, and property from damage caused by unauthorized access? In this course, Physical Security, these are questions that we will be answering. You will be learning how to recognize the potential risks of unauthorized access to your business and personnel, and how to counteract these risks by learning the steps to creating a security policy for you and your personnel to implement. We will included demos that will help you better understand the concepts that will be discussed in this course.

Physical Security ..... 1699_001
Internal Support Systems ..... 1699_002
Perimeter Security ..... 1699_003
Audits, Testing & Drills ..... 1699_004

Evading Firewalls and Honeypots

Course Number: 1700
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Evading Firewalls and Honeypots, is the course where we will not only discuss what firewalls and honeypots are, but how attackers get around these preventive programs. You will learn about the different types of firewalls and how they may be evaded. You will also learn what honeypots are and how they are set-up to divert any would be attackers attention. You will be learning how attackers anticipate honeypots and how penetration testing can help you in dealing with these attackers. We have paired this course with several demos that will cover more in-depth the topics that we will be discussing and help you gain a broader understanding of those topics.

Working with Firewalls ..... 1700_001
Working with Honeypots ..... 1700_002

Evading IDS

Course Number: 1701
Time: 75 Minutes
Number of Quizzes: 4 Quizzes

Intrusion Detection System (IDS) is a device or software that monitors network activities and system activities. While monitoring, it looks for suspicious activities and security policy violations. In this course Evading IDS we will be discussing the vulnerabilities in an IS, types of IDS, types of evasion, techniques used to evade IDS, IDS tools, and how to carry out penetration testing so you can put a prevention plan in place. We will combine this with an in-depth demo on how to avoid an IDS.

Introduction to IDS ..... 1701_001
Evading IDS ..... 1701_002
Points of Vulnerability in IDS ..... 1701_003
Desynchronization ..... 1701_004
Intrusion Detection Tools ..... 1701_005
IDS Evading Tools ..... 1701_006

Wireless Types and Vulnerabilities

Course Number: 1696
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Wireless types, such as WLAN, are also known as Wi-Fi networks and they are susceptible to security lapses that wired networks are exempt from. In this course you will learn about different wireless types and their vulnerabilities. You will learn about several different tools that will help you take countermeasures against these vulnerabilities. We will complete this course with demos on different tools that we will be discussing.

Test Me: EC-Council Exam CEHv8 (312-50)

Course Number: 1890
Time: 240 Minutes
Number of Quizzes: 1 Quiz

Test your knowledge and skills through this Test Me: Cisco Exam CCNA Security 640-554 IINS. Prove to yourself, and others, that you are ready for Cisco's Implementing Cisco IOS Network Security certification exam. You'll demonstrate your proficiency in the principles, techniques, and tools involved in working with routers, networks, and switches. The instruction period is over; this Test Me provides you with a collection of questions based on the exam domains contained in testing for the actual certification exam. Wrap up your exam preparation with this Test Me pulling questions from our Cisco IOS Network Security course series.

■ Security+ (SY0-401) Series

Security Incidents

Course Number: 1871
Time: 30 Minutes
Number of Quizzes: 3 Quizzes

Handling incidents often needs preparation. There are plans and procedures to be taken, and drills to prepare the team. A successful handling team can prevent loss of money for an organization in case of incident. It is an investment rather than a cost if it is done correctly. In the course Incident Handling, you will learn how to recognize what an incident is and where they potentially come from. You will then learn the steps to handling incidents and implementing those steps into your everyday policies and procedures.

Business Continuity

Course Number: 1872
Time: 30 Minutes
Number of Quizzes: 3 Quizzes

Business continuity plans are important if the organization wishes to continue its normal operations in disasters, whether it is man-made or natural. Business continuity plans study all kinds of threats and estimates the damage resulting from those threats. In the course Business Continuity, you will learn the different categories that the events that threaten your business are classified under. You will also learn the steps in creating a business continuity plan. You will also delve further into the development process for a business continuity plan, and learn all the necessary steps that are involved in initiating the plan as well.

Network Design and Security Controls

Course Number: 1873
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

Today's threats and cyber intelligence have made it mandatory for us to use devices for protection. Threats can come from inside our network and the Internet. This makes it so that a firewall alone is not sufficient. We need to design a secure network. In Network Design and Security Controls, you will learn the steps and the tools to designing a secure network. You will also learn of the many security devices that you have at your disposal, with an in-depth discussion on firewalls and their uses. Included in this course will be detailed demos on Firewall and proxy-nat, DMZ, and IDS-IPS.

System Hacking

Course Number: 1683
Time: 90 Minutes
Number of Quizzes: 4 Quizzes

Ensure that you know everything involved in securing a Windows system against attack. During this course you'll get into Windows passwords — how they're created, how they're stored, and different methods used to crack them. You'll discover different methods used for guessing passwords and breaking the different security methods used within the Windows operating system. You'll find discussions on responding to privilege escalation. You'll also spend some time going through a couple of scenarios demonstrating how to use key defense tools. Overall, the topics explored here will teach you how to increase security on your Windows machines, as well as show you required procedures and tools to prepare for different certification exams from EC-Council, CompTIA, Linux, and CISSP.

Windows Hacking ..... 1683_001
Password Attacks..... 1683_002
Alternate Data Streams ..... 1683_003
Steganography..... 1683_004
Rootkits ..... 1683_005
Course Summary..... 1683_006

Spyware & Keyloggers

Course Number: 1684
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

You will take a good look at spyware, the activities it performs, different types of spyware, and the countermeasures needed in order to prevent hackers from utilizing these types of techniques against your company. You will also spend time studying different types of keyloggers. There are three different types of keyloggers that we see used in today's environments: hardware, software, and kernel/driver keyloggers. A good pen tester or ethical hacker cannot perform his or her job properly without understanding the countermeasures for all of the hacking techniques used against today's computer systems. Overall, these topics will help prepare you for certification exams from vendors, such as Linux, CompTIA, and EC-Council.

Spyware Uncovered ..... 1684_001
Keyloggers ..... 1684_002

Viruses and Worms

Course Number: 1686
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

You will discover what viruses and worms are and how they can infect computers and systems. You'll study their nature, how they function, and their impact. You will also spend time going through discussions on varieties of each, along with some real life examples. Refine your understanding of viruses and worms to better your system. The knowledge you gain here will prepare you to be a more effective network administrator. Furthermore, the topics covered here will help with preparing you for security certification exams offered by EC-Council, CompTIA, and Linux.

Viruses..... 1686_001
Worms ..... 1686_002

Denial-of-Service

Course Number: 1689
Time: 90 Minutes
Number of Quizzes: 4 Quizzes

Become familiar with the following concepts: denial-of-service, distributed denial-of-service, and how the denial-of-service and distributed denial-of-service attacks take place. You will also see what botnets are and how they are used to attack your system or network. You will find explanations on the tools that are used to attack, and how you can detect such attacks. You will be introduced to different countermeasures, so that you can plan, prepare, and establish the relevant countermeasures to protect your organization. You will also learn how DoS and DDoS can be used in penetration testing. You will go through discussions on how to protect your organization from the distributed denial-of-service attacks and denial-of-service penetration testing. Altogether, these topics focus on deepening your understanding of security concepts and practices, so that you're a more efficient network administrator. With the skills you gain here, you're equipped to pursue a number of security certifications from CompTIA, EC-Council, and CEH.

Denial-of-Service &
Distributed Denial-of-Service ..... 1689_001
Digital Attack Map..... 1689_002
Botnets..... 1689_003
DoS/DDoS Attack Tools and Detection ..... 1689_004
DoS/DDoS Countermeasures..... 1689_005
DoS/DDoS in Penetration Testing..... 1689_006

Vulnerability Assessment

Course Number: 1670
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Our course Vulnerability Assessment will introduced to the concepts of: Vulnerability Assessment, Vulnerability Assessment Tools, and Patch Management. It will offer demos on several of the vulnerability assessment tools that are available, as well as in-depth discussions on the benefits of these tools. We will discuss the process of analyzing the scan results that the vulnerability assessment tools provide. Finally, we will discuss patch management and some tools that are available for this process, and at the end of this course you will be able to create a comprehensive VA program, identify key vulnerabilities, and perform mitigation actions before those vulnerabilities can be exploited.

Testing Vulnerabilities..... 1670_001
Results, Reports, and Remediation ..... 1670_002

Covering Tracks

Course Number: 1688
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

In Covering Tracks we will be going over various ways that attackers have at their disposal to cover any tracks that may lead to their unwanted eviction or worse yet to an audit trail that would lead directly back to them. In this course we will be discussing, disabling auditing during or after an event, steps to take once it is disabled, and destroying any evidence. We will be going over various ways to avoid detection on Linux machines, and this will include several in-depth demos on various operations for the Linux machines.

Avoiding Detection on Windows Machines. 1688_001
Avoiding Detection on Linux Machines ..... 1688_002
Destroying the Evidence ..... 1688_003
Log Protection Techniques..... 1688_004

Disaster Recovery and Risk Management

Course Number: 1668
Time: 30 Minutes
Number of Quizzes: 3 Quizzes

Since you are a part of IT operations in your enterprise, you could be involved in planning and applying policies related to Risk Management and/or Disaster Recovery. In our course Disaster Recovery and Risk Management, you will receive an introduction to the basics of Risk Management and Disaster Recovery. When you have completed the course, you will be able to identify a risk and the effect that it has on daily operations. You will gain an understanding of security measures and how they are implemented, as well as, the importance and the process of managing risk in your environment. We will partner this with a detailed demo on the process of risk assessment. You will gain an understanding of Disaster Recovery, be able to define what a disaster is, rank a disaster, and create a plan that will define how to recover from a disaster, as well as, successfully recovering your data.

Risk Management..... 1668_001
Disaster Recovery ..... 1668_002

Trojans and Backdoors

Course Number: 1685
Time: 90 Minutes
Number of Quizzes: 4 Quizzes

As an ethical hacker, there are times when you need to hide software from the company that you are performing the test against in order to verify that the defensive strategy is able to find your software. Trojans and Backdoors is the course where our software is going to be going undercover. In this course we are going to define malware and take a look at how a payload is delivered. We will overview the various Trojan tools, and tools used to generate Trojan programs, as well as, learning about Netcat. We will spend time going over countermeasures and various anti-Trojan software and hardware, and preventive methods that can be used to prevent attacks. We will also be incorporating several demos on the many tools that we will be discussing in this course.

Defining Malware..... 1685_001
Malware..... 1685_002
Tools of the Trade..... 1685_003
Countermeasures ..... 1685_004
Course Summary ..... 1685_005

Introduction to Ethical Hacking

Course Number: 1667
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

Ethical hacking is testing the resources for a good cause and for the betterment of technology. In our course Introduction to Ethical Hacking, you will be introduced to various concepts on ethical hacking. We will be talking about vulnerabilities, exploits, defense strategy, penetration testing, pentest types and methodology, vulnerability management, incident management, and

security policy development, and at the end of this course we hope you will have a basic understanding of the various concepts involved in ethical hacking.

Introduction to Hacking ..... 1667_001
Security Management..... 1667_002

Penetration Testing

Course Number: 1669
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

Pentesting is an intentional attack on a system to discover security weaknesses. These can be left either by the security officer or the security controls. Penetration Testing is our course that covers security, vulnerabilities, different types of tests, and when to test as a pen tester. We have paired this with an in-depth demo on vulnerability assessment using the tool Nexpose. At the end of this course we will have reviewed security and vulnerability assessment, and the differences between automatic and manual testing.

Penetration Testing Introduction ..... 1669_001
Organizational Considerations ..... 1669_002

Port Scanning

Course Number: 1680
Time: 105 Minutes
Number of Quizzes: 3 Quizzes

When a port is scanned on a server, the port returns a response indicating that the port is open and a service is listening. In our course Port Scanning, you will learn how ports can be scanned, how a hacker can break into your network through the ports, and the countermeasures you can take to protect your device or network. Our course will offer in-depth discussions on port scanning methods and techniques, port scanning tools, and port scanning countermeasures. We will partner this with detailed demos on Ping, Ping tester, and Netstat.

Port Scanning ..... 1680_001
Advanced Techniques..... 1680_002

Sniffers

Course Number: 1687
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

Sniffers is our course where we take a look at Network Sniffing. We will be covering the basics of packet sniffing, ARP cache poisoning, DNS spoofing, SSL sniffing, VoIP phone calls and sniffing remote desktop connections. This will be coupled with demos on Wireshark, ARP poisoning, and XARP.

Network Sniffing ..... 1687_001
Security Measures ..... 1687_002

Advanced Exploitation Techniques

Course Number: 1870
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

Exploit is a common term in the computer security community that refers to a piece of software that takes advantage of a bug or glitch. In our course Advanced Exploitation Techniques, you will learn what advanced exploitation techniques are and how you can use them in your penetration testing. You will also learn how to use Metasploit to exploit vulnerabilities. This will be coupled with in-depth demos on using Metasploit, and other Metasploit tools, such as, Meterpreter, Armitage, and Armitage-mimkatz.

Advanced Exploiting Techniques..... 1870_001
Penetration Testing ..... 1870_002
Exploits ..... 1870_003

Cryptography

Course Number: 1673
Time: 75 Minutes

Traditional cryptography uses a secret key for encrypting and decrypting a message. This is also known as symmetric keys. Public key cryptography, the CA creates private and public keys using the same algorithm, it functions asymmetrically. In the course Cryptography, you will discuss Public Key Infrastructures, Certificate Authorities, and Certificate management. We will combine that with in-depth demos on PKI Installation, Config-complete, CRL, Enroll Certificate, and CA Management. We will discuss the steps to create and manage a public key infrastructure, and the relationship between public key infrastructures and certificate authority, as well as, both traditional cryptography and public key cryptography, the implementation of certificates, and managing certificates.

Certificates..... 1673_001
Using Secure Certificates ..... 1673_002

Scanning Networks

Course Number: 1679
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

Network scanning is the scanning of public or private networks to find out which systems are running, their IP addresses, and which services they are running. In our course Network Scanning, you will learn techniques for private and public network scanning using various tools. Accompanied with in-depth demos and discussions on how to use Angry IP, Nmap, Hping, and Zmap network scanners. Through this, you will learn the steps to network scanning, how to draw a network map, and plan an attack accordingly.

Private and Public Network Scanning ..... 1679_001
Using Zmap ..... 1679_002

Hacking Web and App Servers

Course Number: 1690
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Hacking Web and Application Servers course, is a course that will give us a good idea about vulnerabilities and attacks available for web servers and web applications. This course includes in-depth demos on several of the tools used for hacking web servers and application servers. These tools include Apache2, Netcraft, Website Mirroring, W3AF, and WMAP. By the end of this course we will have discussed various ways to collect information from web servers, application server attacks, and finding vulnerabilities in a server.

Web Server Attacks ..... 1690_001
Web Application Attacks ..... 1690_002

SQL Injections

Course Number: 1691
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

SQL injection is the most used of all attacks. In this course, SQL Injections, you will be learning how SQL injections can be initiated, cause damage or loss, prevention against such attacks, and discussing detection tools. This course includes demos demonstrating BSQL tool as well as SQL Injection Username and Password. By the end of this course you will have covered SQL injection methodology, attacks, buffer overflow exploit, testing for SQL injection, countermeasures and detection tools.

SQl Injections ..... 1691_001
Protecting Against SQL Injections ..... 1691_002

Session Hijacking

Course Number: 1692
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

Have you heard the words session hijacking? Simply put, it is defined as an intruder taking over a genuine session between two computers and using if for sinister purposes. In the course Session Hijacking, you will learn details about session hijacking, well-known techniques employed by aggressors, the steps involved in session hijacking, various types of session hijacking, tools for hijacking sessions, ways you can protect yourselves from session hijacking, and how pentesting can be used to identify vulnerabilities.

Session Hijacking ..... 1692_001
Countermeasures ..... 1962_002

Buffer Overflows

Course Number: 1693
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Buffer overflow occurs when you try to store more data than what the allocated buffer or storage area can hold. In this course you will be introduced to the concepts of buffer overflows, how they happen, and how attackers take advantage of them. You will also learn how to defend against buffer overflow attacks, and what security measures you can take to protect your data. We will accompany this with several demos that will delve deeper and help you understand some of the specific topics that will be discussed.

Buffer Flow ..... 1693_001
Program and Application Vulnerability ..... 1693_002
Defense, Countermeasures, and Security ..... 1693_003

Hacking Wireless Networks

Course Number: 1695
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

Wireless attacks have become easy; even unskilled people with little computer literacy can accomplish them. This is because of the many automated tools available to perform this hack. In our course Hacking Wireless Networks, we will not be focusing on weaknesses of your wireless networks or how to protect them, instead, we will focus on showing you how to gain access to a wireless network.

Hacking Wireless Networks ..... 1695_001
Hacking Windows ..... 1695_002

Social Engineering

Course Number: 1678
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

Social engineering is the art of extorting employees for information. It can take the form of human-based or digital. In our course Social Engineering, you will learn what social engineering is, who's at risk, and how to protect and educate your employees against social engineering. You will learn the importance of creating a security policy, and how to deal with the threat of human-based attacks from both outside and inside the company. You will learn what kind of risks computer-based attacks, and social media present. We will couple this with in-depth demos on phishing email, SET-webTemplate, SET-spear phishing, SET-trojan, and SET SMS Spoofing.

Social Engineering ..... 1678_001
Social Engineering Demos ..... 1678_002

Authentication Systems

Course Number: 1674
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

Whenever we login to a computer system, we provide information to identify ourselves. We refer to this as authentication. Authentication has been developed to contain more than just username and password because we are looking for added layers of security. In this course we will be covering authentication factors, forms of authentication, and authentication protocols. We will also be going over RADIUS, LDAP, and SSO. We will pair this with several demos depicting practical uses of the many tools that we will discuss in this course.

Introduction ..... 1674_001
Authentication Protocols ..... 1674_002
RADIUS, LDAP, and SSQ ..... 1674_003

Cryptography Weaknesses

Course Number: 1675
Time: 75 Minutes
Number of Quizzes: 4 Quizzes

Cryptography is the science of writing in secret code and is considered an ancient art. The first documented use of cryptography dates back to circa 1900 B.C. In our course Cryptography Weaknesses, we will discuss weaknesses in cryptography and ways to improve your security. We will also cover the use of symmetric and asymmetric keys and the use of hybrid keys, as well as, the use of hashing algorithms and digital signatures. We will pair this with several demos to show you how each of these works in practical situations.

Encryption ..... 1675_001
Symmetric Encryption ..... 1675_002
Asymmetric Encryption ..... 1675_003
Hashing Algorithms ..... 1675_004
Digital Signatures ..... 1675_005

Cross-Site Scripting

Course Number: 1694
Time: 60 Minutes
Number of Quizzes: 3 Quizzes

As a security tester or security analyst, it is important that you are aware of cross-site scripting vulnerabilities and how they may be exploited by attackers. In our course Cross-Site Scripting, you will gain a comprehensive understanding of cross-site scripting, you will learn how to prevent it, and how you can test to identify cross-site scripting vulnerabilities. You will also learn what cross-site scripting is and what the different types of cross-site scripting you may come across. This course will also be paired with several demos that give you a real world view of what we have and will cover in this course.

Cross-Site Scripting ..... 1694_001
Types of Cross-Site Scripting ..... 1694_002
Preventing Cross-Site Scripting ..... 1694_003

Mobile Hacking Basics

Course Number: 1697
Time: 90 Minutes
Number of Quizzes: 3 Quizzes

Mobile hacking can be anything from searching for unlocked Wi-Fi networks, to the hacking of Android OS or IOS systems. In our course Mobile Hacking Basics, we will give you a basic introduction of the tools and concepts behind mobile hacking with demos giving you a look at some of these tools in action.

Securing Mobile Basics ..... 1697_001
Mobile Security Considerations ..... 1697_002
Hardening Mobile Devices ..... 1697_003

Physical Security

Course Number: 1699
Time: 75 Minutes
Number of Quizzes: 4 Quizzes

What kind of security measures do you take to protect your facilities, equipment, resources, personnel, and property

from damage caused by unauthorized access? In this course, Physical Security, these are questions that we will be answering. You will be learning how to recognize the potential risks of unauthorized access to your business and personnel, and how to counteract these risks by learning the steps to creating a security policy for you and your personnel to implement. We have included demos that will help you better understand the concepts that will be discussed in this course.

Physical Security ..... 1699_001
Internal Support Systems ..... 1699_002
Perimeter Security ..... 1699_003
Audits, Testing, & Drills ..... 1699_004

Evading Firewalls and Honeypots

Course Number: 1700
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Evading Firewalls and Honeypots is the course where we will not only discuss what firewalls and honeypots are, but how attackers get around these preventive programs. You will learn about the different types of firewalls and how they may be evaded. You will also learn what honeypots are and how they are set-up to divert any would be attackers attention. You will be learning how attackers anticipate honeyports and how penetration testing can help you in dealing with these attackers. We have paired this course with several demos that will cover more in-depth the topics that we will be discussing and help you gain a broader understanding of those topics.

Working with Firewalls ..... 1700_001
Working with Honeypots ..... 1700_002

Evading IDS

Course Number: 1701
Time: 75 Minutes
Number of Quizzes: 4 Quizzes

Intrusion Detection System (IDS) is a device or software that monitors network activities and system activities. While monitoring, it looks for suspicious activities and security policy violations. In this course Evading IDS we will be discussing the vulnerabilities in an IS, types of IDS, types of evasion, techniques used to evade IDS, IDS tools, and how to carry out penetration testing so you can put a prevention plan in place. We will combine this with an in-depth demo on how to avoid an IDS.

Introduction to IDS ..... 1701_001
Evading IDS ..... 1701_002
Points of Vulnerability in IDS ..... 1701_003
Desynchronization ..... 1701_004
Intrusion Detection Tools ..... 1701_005
IDS Evading Tools ..... 1701_006
Countermeasures ..... 1701_007

Wireless Types and Vulnerabilities

Course Number: 1696
Time: 75 Minutes
Number of Quizzes: 3 Quizzes

Wireless types, such as WLAN, are also known as Wi-Fi networks and they are susceptible to security lapses that wired networks are exempt from. In this course you will learn about different wireless types and their vulnerabilities. You will learn about several different tools that will help you take countermeasures against these vulnerabilities. We will complete this course with demos on different tools that we will be discussing.

Wireless Authentication ..... 1696_001
Authentication Systems ..... 1696_002

Test Me: CompTIA Exam Security+ (SY0-401)

Course Number: 1891
Time: 90 Minutes
Number of Quizzes: 1 Quiz

Test your knowledge and skills through this Test Me: Security+ (SY0-401) Exam. Prove to yourself, and others, that you are ready for the Security+ (SY0-401) certification exam. You'll demonstrate your proficiency in the principles, techniques, and tools involved in being an IT security administrator for your company, including monitoring the system and understanding how hackers gain access. The instruction period is over; this Test Me provides you with a collection of questions based on the exam domains contained in testing for the actual certification exam. Wrap up your exam preparation with this Test Me pulling questions from our Security+ course series.

[BP] Security+ (SY0-401) Series

Recuperação de Desastres e Gestão de Riscos

Número do Curso: 1950
Tempo: 60 Atas
Número de Testes: 3 Teste

Desde que você é uma parte das operações de TI na sua empresa, você poderia estar envolvido no planejamento e as políticas aplicáveis relacionadas com a gestão de

riscos e/ou recuperação de falhas. Em nosso curso de Recuperação de Desastres e Gestão de Riscos, você receberá uma introdução aos conceitos básicos de Gestão de Riscos e Recuperação de Desastres. Quando tiver concluído o curso, você será capaz de identificar um risco eo efeito que tem sobre as operações diárias. Você vai ganhar uma compreensão das medidas de segurança e como eles são implementados, bem como, a importância e o processo de gerenciamento de riscos em seu ambiente. Seremos parceiros isso com uma demonstração detalhada sobre o processo de avaliação de riscos. Você vai ganhar uma compreensão de Recuperação de Desastres, ser capaz de definir o que é um desastre, classificar um desastre, e criar um plano que irá definir a forma de recuperar de um desastre, bem como, se recuperando com sucesso os seus dados.

Gestão de Riscos ..... 1950_001
Disaster Recovery ..... 1950_002

Avaliação de Vulnerabilidades

Número do Curso: 1985
Tempo: 90 Atas
Número de Testes: 3 Teste

Nosso curso Avaliação de Vulnerabilidades introduzirá os conceitos de: Avaliação de Vulnerabilidades, Ferramentas de Avaliação de Vulnerabilidades y Gerenciamento de patches. O curso oferecerá demos de diversas ferramentas de avaliação de vulnerabilidades que estão disponíveis, bem como debates aprofundados sobre os benefícios daquelas ferramentas. Nós iremos debater o processo de análise dos resultados verificados que as ferramentas de avaliação de vulnerabilidade proporcionam. Finalmente, iremos debater sobre o Gerenciamento de patches e sobre algumas outras ferramentas que estão disponíveis para este processo. No final deste curso, você poderá criar um programa amplio de AV, identificar vulnerabilidades chaves e realizar ações de reparação antes que aquelas vulnerabilidades possam ser exploradas.

Avaliação de Vulnerabilidade ..... 1985_001
Resultados, Relatórios, e Reparação ..... 1985_002

Hacking de Sistema

Número do Curso: 1965
Tempo: 105 Atas
Número de Testes: 4 Teste

Garantir que você saiba tudo que está relacionado com segurança de um sistema Windows contra ataques. Durante este curso, você vai ver senhas de Windows — como é que foram geradas, como é que são armazenadas, e diferentes métodos usados para craquear-as. Você descobrirá os diferentes métodos usados para adivinhar senhas e violar os diferentes métodos de segurança usados dentro do sistema operativo Windows. Você encontrará debates ao respeito de resposta a aumento de privilégios. Também passará algum tempo pesquisando através de um par de cenários, demonstrando como utilizar ferramentas importantes de defesa. Em geral, os tópicos estudados aqui, vão lhe ensinar como aumentar a segurança nos seus equipamentos Windows, e vão lhe mostrar os procedimentos e ferramentas necessários para preparar diversas provas de certificação do EC-Council, de CompTIA, Linux e CISSP.

Hacking do Windows ..... 1965_001
Ataques de Senhas..... 1965_002
Fluxos de Dados Alternativos..... 1965_003
Esteganografia ..... 1965_004
Rootkits ..... 1965_005
Resumo do Curso ..... 1965_006

Trojans e Backdoors

Número do Curso: 1967
Tempo: 90 Atas
Número de Testes: 4 Teste

Como um hacker ético, tem momentos em que você precisa esconder um software da empresa na qual você está realizando o teste, a fim de verificar se a estratégia de defesa não pode encontrar o seu software. Trojans e backdoors é o curso aonde nosso software vai estar encoberto. Neste curso iremos definir malware e dar uma olhada em como é a entrega da carga. Nós iremos ter uma visão geral nas diversas ferramentas de Trojan e ferramentas utilizadas para gerar programas de Trojan, assim como também aprender acerca de Netcat. Nós iremos passar tempo vendo contramedidas e vários softwares anti-Trojan e hardware, e métodos de prevenção que podem ser usados para prevenir ataques. Nós também estaremos incorporando várias demonstrações ao respeito das muitas ferramentas que iremos debater neste curso.

Definindo Malware..... 1967_001
Malware..... 1967_002
Ferramentas de Comércio ..... 1967_003
Contramedidas..... 1967_004
Resumo do Curso ..... 1967_005

Spyware e Keyloggers

Número do Curso: 1966
Tempo: 75 Atas
Número de Testes: 3 Teste

Você vai dar uma boa olhada no spyware, as atividades que realiza, diferentes tipos de spyware, e as contramedidas necessárias, a fim de impedir que os hackers utilizem estes tipos de técnicas contra sua empresa. Você também vai passar um tempo estudando diferentes tipos de keyloggers. Existem três tipos diferentes de keyloggers que vemos usados em ambientes de hoje em dia: hardware, software e keyloggers do driver / kernel. Um bom testador de penetração ou um hacker ético não pode executar o seu trabalho corretamente, sem compreender as contramedidas para todas as técnicas de hacking usadas contra sistemas de computadores de hoje em dia. Geralmente, estes temas ajudarão a se preparar para os exames de certificação de fornecedores, tais como Linux, CompTIA, e EC-Council.