EC-Council

EC-COUNCIL NETWORKING SECURITY ADMINISTRATOR

This course looks at the network Security in defensive view. The ENSA program is designed to provide fundamental skills needed to analyse the internal and external security threats against a network, and to develop security policoes and firewall srategies. In addition they will learn how to expose system and network vulnerabilities and defend against them.

- Fundamentals of Computer Networking
- Network security
- IEEE standard
- Packet filtering and proxy servers
- Troubleshooting Networking
- Patch management
- E-mail Security
- Creating fault Tolerance
- Network Vulnerability Assessment
- Network Protocols
- Security standards organizations
- Network security threats
- Bastion host honeypots
- Hardening routers
- Log Analysis
- Authentication Encryption Cryptography & Digital signatures
- Protocol Analysis
- Security standards
- Intrusions detection systems (IDS) and intrusion prevention systems (IPS)
- Application Security
- Virtual private network
- Incident response
- Hardening Physical Security
- Security policy
- Firewalls
- Securing modems
- Hardening operating System
- Web security
- Wireless Network security
- Disaster recovery and planning

Who should Attends? System administrators, Network administrator and anyone who is interested in networks security technologies.

EC-COUNCIL CERTIFIED SECURITY SPECIALIST

The EC-Council certified security specialist (ECSS) program is designed primarily for students of academic institution. It covers the fundamental basics of information security, computer forensics and network security. The program will give a holistic overview of key components of informationsecurity. Students who complete the ECSS program, will be equipped with the adequate foundation knowledge, and should be able to progress onto the next level.

- Information Security Fundamentals
- Password Cracking
- Wireless Networks
- Hacking cycle
- Authentication
- Virtual Private Network
- Trademark, copyright, and patents
- Inside response and forences
- Steganography
- Introduction to Writing investigative
- Addressing Threats
- Cryptography
- Intrusion Detection system
- Introduction to Ethical Hacking
- Network Attacks
- Introduction to Wireless Network security
- Digital evidence
- Analyzing Logs
- Backdoors, Virus, and Worms
- Web Servers and Web Applications
- Networking Revisited
- Bastion Hosts and DMZ
- Voice over Internet protocol
- Network and router forensics fundamentals
- E-mail crime and computer forensics
- Introduction to the Linux Operating System
- Firewalls and honeypots
- Secure networking protocols
- Proxy server
- Computer forensics Fundamentals
- Understanding Windows, DOS, Linux, and Macintosh
- Computer Forensics as a Profession

EC-COUNCIL CERTIFIED SECURITY SPECIALIST

The EC-Council certified security specialist (ECSS) program is designed primarily for students of academic institution. It covers the fundamental basics of information security, computer forensics and network security. The program will give a holistic overview of key components of informationsecurity. Students who complete the ECSS program, will be equipped with the adequate foundation knowledge, and should be able to progress onto the next level.

- Information Security Fundamentals
- Password Cracking
- Wireless Networks
- Hacking cycle
- Authentication
- Virtual Private Network
- Trademark, copyright, and patents
- Inside response and forences
- Steganography
- Introduction to Writing investigative
- Addressing Threats
- Cryptography
- Intrusion Detection system
- Introduction to Ethical Hacking
- Network Attacks
- Introduction to Wireless Network security
- Digital evidence
- Analyzing Logs
- Backdoors, Virus, and Worms
- Web Servers and Web Applications
- Networking Revisited
- Bastion Hosts and DMZ
- Voice over Internet protocol
- Network and router forensics fundamentals
- E-mail crime and computer forensics
- Introduction to the Linux Operating System
- Firewalls and honeypots
- Secure networking protocols
- Proxy server
- Computer forensics Fundamentals
- Understanding Windows, DOS, Linux, and Macintosh
- Computer Forensics as a Profession

SECURITY 5

Security` is a buzz word that is catching up with diverse industry verticals relying on computing system to keep the operations and business wheels moving. Today, average office goers sign an `Acceptable Use Policy` that is part of `corporate Security policies` and are responsible for any misuse and damage caused on computing resources. Several companies offer in-house traning to raise the security awareness of its employees, while others prefer knowledgeable workers who here acquired security related credentials. However, there is a discemble need for knowledge workers who know the basics of Security. These employees bring greater value to the workplace in terms of better productivity and higher efficiency. There are lasser downtimes and security lapses by employees and hence greater cost saving and profits. Identify theft, credit card fraud, online banking Phishing scams, virus and backdoors email hoaxes sex offenders lurking online loss of confidentialinformtiuonand hackers are same off the threats you bell face on a daily basis. Are you prepared to face them and defend secure yourself? With security 5training take control of you information resources

- Foundations of security
- Desktop security
- security threats and attacks
- working on the internet
- Basic security configurations
- Administering Windows securit
- security internet access
- incident response

WHO SHOULD ATTEND? Office knowledge workers home users any non –IT person using computeres in their office