LEARNING PLAN

Information Security Concepts & Practices

Master the practical steps you can take to meet security threats to your corporate data head on. Learn about the tools to protect data, monitor environments, and recover in the event of a security breach.

Areas of focus

- Monitoring and tools for protecting from attacks
- Inside the mind of a hacker
- Data protection techniques

Curriculum

VIDEOS FROM COURSE

CompTIA Security+ SY0-401 Videos 11-39  13 hours

- Forensics  20 min
- Incident Response  11 min
- Security Awareness  31 min
- Physical and Environmental Security  25 min
- Risk Management  36 min
- The Correct Controls for CIA  39 min
- Malware  31 min
- Attack Types  51 min
- Social Engineering  25 min
- Wireless Attacks  17 min
- Application Attacks  31 min
- Mitigation and Deterrent Techniques  30 min
- Discovery Tools  37 min
- Penetration Testing  14 min
- App. Security Controls and Techniques  27 min
- Security for Mobile  20 min
- Host Security  26 min
- Data Security  25 min
- Static Environment Security  15 min
- Authentication Services & Protocols  34 min
- Authentication Methods  33 min
- Authorization Models  18 min
- Account Management  21 min
- Crypto Concepts  43 min
- Crypto Protocols  41 min
- PKI  29 min
- ACL Case Study  16 min
- NAT Case Study  12 min
- Layered Security Case Study  10 min

Prerequisite Plans

FUNDAMENTAL LEVEL

Understanding the End-User
Information Security Fundamentals

Current Plan

ASSOCIATE LEVEL

Information Security Concepts & Practices

Possible Next Plans

EXPERT LEVEL

Advanced Cloud Computing
Advanced Server Technologies
Depth Security for Corporate Information
VIDEOS FROM COURSE
(ISC)² CISSP 2015
Videos 2-9, 15-34, 36-39

- CIA Concepts 4 min
- Policies 13 min
- Risk 13 min
- Control Types 17 min
- Security Awareness Training 6 min
- Ethical Hacking 13 min
- Symmetric Cryptography 19 min
- Asymmetric Cryptography 24 min
- Firewalls 21 min
- VPNs 27 min
- Attacks 21 min
- Authentication Concepts 9 min
- Multifactor Authentication 15 min
- Centralized Management 17 min
- SSO and Security Threats 25 min
- Computing System Evaluations 15 min
- Security Model Details 11 min
- Availability and Integrity Design 14 min
- IDS and IPS 17 min
- Controls for Operational Security 19 min
- Separation of Duties 18 min
- Backups and Media 16 min
- DR and BC 20 min
- Malware 14 min
- Evidence 12 min
- Laws and Liability 10 min
- Incident Response 15 min
- System and Software Security 16 min
- 2700x 6 min
- Federated Identities 11 min
- EPA 16 min
- Monitoring and More 12 min

VIDEOS FROM COURSE
EC Council Certified Ethical Hacker v9.0 (cont.)

- Windows Evaluations 7 min
- Deploy Windows 8.1 15 min
- Deploy Windows 2012 11 min
- Deploy Windows 10 7 min
- Deploy Windows 2016 7 min
- Ethics and Hacking 10 min
- Hacking Vocabulary 6 min
- InfoSec Concepts 5 min
- Attack Categories, Types, and Vectors 5 min
- Five Phases of Hacking 5 min
- Footprinting and Reconnaissance Concepts 11 min
- Search Engine Tools 8 min
- Hacking using Google 12 min
- Website Recon Tools 13 min
- Metagoofil Metadata Tool 3 min
- Email Headers for Footprinting 5 min
- Using WHOIS for Recon 4 min
- DNS Tools 12 min
- Network Scanning Overview 3 min
- Network Scanning Methodology 9 min
- Port Discovery 11 min
- Network Scanning Tools 3 min
- Stealth Idle Scanning 10 min
- OS and Application Fingerprinting 10 min
- Vulnerability Scanning 8 min
- Network Mapping Tools 5 min
- Proxy Servers 8 min
- Using Public Proxy Services 6 min
- Enumeration Concepts 5 min
- NetBIOS Enumeration 11 min
- SNMP Enumeration Concepts 10 min
- SNMP Enumeration Tools 10 min
- LDAP Enumeration Concepts 5 min
- LDAP Enumeration Example 7 min
- NTP Enumeration 7 min
- SMTP Enumeration 8 min
- System Hacking Overview 9 min
- Password Cracking Concepts 10 min
- Password Attack Example: MITM and Sniffing 13 min
- Rainbow Crack Lab Setup 8 min
- Rainbow Crack Demonstration 8 min
- Password Reset Hacking 8 min
- DHCP Starvation 10 min
**EC Council Certified Ethical Hacker v9.0 (cont.)**

- Remote Access
- Spyware
- NTFS Alternate Data Streams Exploit
- Steganography with OpenPuff
- Steganography with SNOW
- Covering Tracks
- Malware Overview
- Trojan Overview
- Creating a Trojan
- Virus Overview
- Virus Creation
- Detecting Malware
- Malware Analysis
- Hash File Verification
- Sniffing Overview
- CAM Table Attack and Port Security
- DHCP Snooping
- Dynamic ARP Inspection (DAI)
- Social Engineering
- Denial of Service (DoS) Attacks
- Session Hijacking
- Hacking Web Servers
- Buffer Overflow
- OWASP Broken Web Application Project
- Shellshock
- SQL Introduction
- SQL Injection
- Web App Vulnerabilities: WordPress
- Wireless Hacking
- Using an Android VM
- Malware for Mobile
- Mobile Device Risks and Best Practices
- Firewall Evasion
- Firewall ACL Example
- NAT and PAT fundamentals
- IDS/IPS Evasion
- Honeypots
- Cloud Computing

**EC Council Certified Ethical Hacker v9.0 (cont.)**

- CIA: Confidentiality, Integrity, and Availability
- Policies
- Quantifying Risk
- Separation of Duties
- Symmetrical Encryption Concepts
- Asymmetrical Encryption Concepts
- Control Types
- Multifactor Authentication
- Centralized Identity Management
- Kerberos and Single Sign On (SSO)
- Backups and Media Management
- Operations Security Controls
- Physical Security Controls
- Incident Response
- VPNs
- Disaster Recovery Planning
- Pen Testing Tips
- Useful Tools
- Case Study
- Additional Resources and Exam Prep