EC-Council Certified Encryption Specialist (ECES)

Duration: 3 days

Course Description

The EC-Council Certified Encryption Specialist (ECES) program introduces professionals and students to the field of cryptography. The participants will learn the foundations of modern symmetric and key cryptography including the details of algorithms such as Feistel Networks, DES, and AES. Other topics introduced:

- Overview of other algorithms such as Blowfish, Twofish, and Skipjack
- Hashing algorithms including MD5, MD6, SHA, Gost, RIPMD 256 and others.
- Asymmetric cryptography including thorough descriptions of RSA, Elgamal, Elliptic Curve, and DSA.
- Significant concepts such as diffusion, confusion, and Kerkchoff' s principle.

Participants will also be provided a practical application of the following:

- How to set up a VPN
- Encrypt a drive
- Hands-on experience with steganography
- Hands on experience in cryptographic algorithms ranging from classic ciphers like Caesar cipher to modern day algorithms such as AES and RSA.

Who Should Attend

Anyone involved in the selection and implementation of VPN' s or digital certificates should attend this course. Without understanding the cryptography at some depth, people are limited to following marketing hype. Understanding the actual cryptography allows you to know which one to select. A person successfully completing this course will be able to select the encryption standard that is most beneficial to their organization and understand how to effectively deploy that technology.

This course is excellent for ethical hackers and penetration testing professionals as most penetration testing courses skip cryptanalysis completely. Many penetration testing professionals testing usually don' t attempt to crack cryptography. A basic knowledge of cryptanalysis is very beneficial to any penetration testing.

What you will learn

- Types of Encryption Standards and their differences
- How to select the best standard for your organization

- How to enhance your pen-testing knowledge in encryption
- Correct and incorrect deployment of encryption technologies
- Common mistakes made in implementing encryption technologies
- Best practices when implementing encryption technologies

Course Outline

Introduction and History of Cryptography

- What is Cryptography?
- History of Cryptography
- Mono-Alphabet Substitution
    - Caesar Cipher
    - Atbash Cipher
    - Affine Cipher
    - ROT13 Cipher
    - Scytale
    - Single Substitution Weaknesses
- Multi-Alphabet Substitution
    - Cipher Disk
    - Vigenère Cipher
        - Vigenère Cipher: Example
        - Breaking the Vigenère Cipher
    - Playfair Cipher
    - ADFGVX Cipher
- Homophonic Substitution
- Null Ciphers
- Book Ciphers
- Rail Fence Ciphers
- The Enigma Machine
- CrypTool

Symmetric Cryptography & Hashes

- Symmetric Cryptography

- Information Theory
    - Information Theory Cryptography Concepts
- Kerckhoffs' s Principle
- Substitution
- Transposition
- Binary Math
    - Binary AND
    - Binary OR
    - Binary XOR
- Block Cipher vs. Stream Cipher
- Symmetric Block Cipher Algorithms
    - Basic Facts of the Feistel Function
        - The Feistel Function
        - Unbalanced Feistel Cipher
    - Data Encryption Standard (DES)
    - 3DES
        - DESx
        - Whitening
    - Advanced Encryption Standard (AES)
        - AES General Overview
        - AES Specifics
    - Blowfish
    - Serpent
    - Twofish
    - Skipjack
    - International Data Encryption Algorithm (IDEA)
    - CAST
    - Tiny Encryption Algorithm (TEA)
    - SHARK

- Symmetric Algorithm Methods
    - Electronic Codebook (ECB)
    - Cipher-Block Chaining (CBC)
    - Propagating Cipher-Block Chaining (PCBC)
    - Cipher Feedback (CFB)
    - Output Feedback (OFB)
    - Counter (CTR)
    - Initialization Vector (IV)
- Symmetric Stream Ciphers
    - Example of Symmetric Stream Ciphers: RC4
    - Example of Symmetric Stream Ciphers: FISH
    - Example of Symmetric Stream Ciphers: PIKE
- Hash Function
    - Hash – Salt
    - MD5
        - The MD5 Algorithm
    - MD6
    - Secure Hash Algorithm (SHA)
    - FORK-256
    - RIPEMD-160
    - GOST
    - Tiger
    - MAC and HMAC
- CryptoBench

Number Theory and Asymmetric Cryptography

- Asymmetric Encryption
- Basic Number Facts
    - Prime Numbers
    - Co-Prime Numbers
    - Euler' s Totient
    - Modulus Operator

    - Fibonacci Numbers
- Birthday Theorem
    - Birthday Paradox
        - Birthday Paradox: Probability
    - Birthday Attack
- Random Number Generator
    - Classification of Random Number Generator
    - Traits of a Good PRNG
    - Naor-Reingold and Mersenne Twister Pseudorandom Function
    - Linear Congruential Generator
    - Lehmer Random Number Generator
    - Lagged Fibonacci Generator (LFG)
    - Blum Blum Shub
    - Yarrow
    - Fortuna
- Diffie-Hellman
- Rivest Shamir Adleman (RSA)
    - RSA – How it Works
    - RSA Example
- Menezes–Qu–Vanstone
- Digital Signature Algorithm
    - Signing with DSA
- Elliptic Curve
    - Elliptic Curve Variations
- Elgamal
- CrypTool

Applications of Cryptography

- FIPS Standards
- Digital Signatures

- What is a Digital Certificate?
    - Digital Certificates
        - X.509
        - X.509 Certificates
        - X.509 Certificate Content
        - X.509 Certificate File Extensions
- Certificate Authority (CA)
    - Certificate Authority – Verisign
- Registration Authority (RA)
- Public Key Infrastructure (PKI)
- Digital Certificate Terminology
- Server-based Certificate Validation Protocol
- Digital Certificate Management
- Trust Models
- Certificates and Web Servers
- Microsoft Certificate Services
- Windows Certificates: certmgr.msc
- Authentication
    - Password Authentication Protocol (PAP)
    - Shiva Password Authentication Protocol (S-PAP)
    - Challenge-Handshake Authentication Protocol (CHAP)
    - Kerberos
        - Components of Kerberos System
        - Kerberos Authentication Process
- Pretty Good Privacy (PGP)
    - PGP Certificates
- Wi-Fi Encryption
    - Wired Equivalent Privacy (WEP)
    - WPA – Wi-Fi Protected Access
    - WPA2

- SSL
- TLS
- Virtual Private Network (VPN)
    - Point-to-Point Tunneling Protocol (PPTP)
        - PPTP VPN
    - Layer 2 Tunneling Protocol VPN
    - Internet Protocol Security VPN
    - SSL/TLS VPN
- Encrypting Files
    - Backing up the EFS key
    - Restoring the EFS Key
- BitLocker
    - BitLocker: Screenshot
- Disk Encryption Software: VeraCrypt
- Common Cryptography Mistakes
- Steganography
    - Steganography Terms
    - Historical Steganography
    - Steganography Details
    - Other Forms of Steganography
    - How to Embed?
    - Steganographic File Systems
    - Steganography Implementations
    - Demonstration
- Steganalysis
    - Steganalysis – Raw Quick Pair
    - Steganalysis – Chi-Square Analysis
    - Steganalysis – Audio Steganalysis
- Steganography Detection Tools

- National Security Agency and Cryptography
    - NSA Suite A Encryption Algorithms
    - NSA Suite B Encryption Algorithms
    - National Security Agency: Type 1 Algorithms
    - National Security Agency: Type 2 Algorithms
    - National Security Agency: Type 3 Algorithms
    - National Security Agency: Type 4 Algorithms
- Unbreakable Encryption

Cryptanalysis

- Breaking Ciphers
- Cryptanalysis
- Frequency Analysis
- Kasiski
- Cracking Modern Cryptography
    - Cracking Modern Cryptography: Chosen Plaintext Attack
    - Cracking Modern Cryptography: Ciphertext-only and Related-key Attack
- Linear Cryptanalysis
- Differential Cryptanalysis
- Integral Cryptanalysis
- Cryptanalysis Resources
- Cryptanalysis Success
- Rainbow Tables
- Password Cracking
- Tools

Quantum Computing and Cryptography

- Quantum Computing and Cryptography
- Timeline
- Issues for QC
- Two Branches
    - Quantum Key Distribution (QKD)
        - QKD

        - What do we need?
        - Qubits
        - Trends
    - Quantum Computers
        - The Problem
        - Why?
- NIST
- Major Approaches
- Lattice-Based Crypto
- Learning with Errors
- GGH
- NTRU