EC-COUNCIL CERTIFIED ENCRYPTION SPECIALIST

DURATION: 3 DAYS

COURSE OVERVIEW

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:

1. Overview of other algorithms such as Blowfish, Twofish, and Skipjack
2. Hashing algorithms including MD5, MD6, SHA, Gost, RIPMD 256 and others.
3. Asymmetric cryptography including thorough descriptions of RSA, Elgamal, Elliptic Curve, and DSA.
4. Significant concepts such as diffusion, confusion, and Kerkchoff's principle.
5. Participants will also be provided a practical application of the following:
6. How to set up a VPN
7. Encrypt a drive
8. Hands-on experience with steganography
9. Hands on experience in cryptographic algorithms ranging from classic ciphers like Caesar cipher to modern day algorithms such as AES and RSA.

TARGET AUDIENCE

Anyone involved in selecting, implementing VPN's or digital certificates should attend this course first. 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.

COURSE OBJECTIVES

1. Introduction and History of Cryptography
2. Symmetric Cryptography and Hashes
3. Number theory and Asymmetric Cryptography
4. Applications of Cryptography part 1
5. Applications of Cryptography part 2

COURSE CONTENT

Introduction and History of Cryptography

What is Cryptography?

History

Mono-Alphabet Substitution

Caesar Cipher

Atbash Cipher

ROT 13

Scytale

Single Substitution Weaknesses

Multi-Alphabet Substitution

Cipher Disk

Vigenère Cipher

Vigenère Cipher: Example

Breaking the Vigenère Cipher

Playfair

The ADFGVX cipher

The Enigma Machine

CrypTool

Symmetric Cryptography and Hashes

Symmetric Cryptography

Information Theory

Information Theory Cryptography Concepts

Kerckhoffs's Principle

Substitution

Transposition

Substitution and Transposition

Binary M

ath

Binary AND

Binary OR

Binary XOR

Block Cipher vs. Stream Cipher

Symmetric Block Cipher Algorithms

Basic Facts of the Feistel Function

The Feistel Function

A Simple View of a Single Round

Unbalanced Feistel Cipher

DES

3DES

DESx

Whitening

AES

AES General Overview

AES Specifics

Blowfish

Serpent

Twofish

Skipjack

IDEA

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

Hash – Salt

MD5

The MD5 Algorithm

MD6

Secure Hash Algorithm (SHA)

Fork 256

RIPEMD – 160

GOST

Tiger

CryptoBench

Number theory and Asymmetric Cryptography

Asymmetric Encryption

Basic Number Facts

Prime Numbers

Co-Prime

Eulers Totient

Modulus Operator

Fibonacci Numbers

Birthday Problem

Birthday Theorem

Birthday Attack

Random Number Generators

Classification of Random Number Generators

Naor-Reingold and Mersenne Twister Pseudorandom Function

Linear Congruential Generator

Lehmer Random Number Generator

Lagged Fibonacci Generator

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 part 1

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)

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

Pretty Good Privacy (PGP)

PGP Certificates

Wife 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/VPN

Encrypting Files

Backing up the EFS key

Restoring the EFS Key

Bit locker

Bit locker: Screenshot

Disk Encryption Software: True crypt

Steganography

Steganography Terms

Historical Steganography

Steganography Details

Other Forms of Steganography

Steganography Implementations

Demonstration

Steg analysis

Steg analysis – Raw Quick Pair

Steg analysis - Chi-Square Analysis

Steg analysis - Audio Steg analysis

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

Applications of Cryptography part 2

Breaking Ciphers

Cryptanalysis

Frequency Analysis

Kasiski

Cracking Modern Cryptography

Cracking Modern Cryptography: Chosen Plaintext Attack

Linear Cryptanalysis

Differential Cryptanalysis

Integral Cryptanalysis

Cryptanalysis Resources

Cryptanalysis Success

Rainbow Tables

Password Cracking

Tools