Lab Module 20 Cryptography

With the increasing adoption of the Internet for business and personal communication, securing sensitive information such as credit-card and personal identification numbers (PINs), bank account numbers, and private messages is becoming increasingly important, and yet, more difficult to achieve. Today’s information-based organizations extensively use the Internet for e-commerce, market research, customer support, and a variety of other activities. Thus, data security is critical to online businesses and privacy of communication.

Cryptography and cryptographic (“crypto”) systems help in securing data from interception and compromise during online transmissions. Cryptography enables one to secure transactions, communications, and other processes performed in the electronic world, and is additionally used to protect confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, etc.

As an ethical hacker or penetration tester, you should suggest to your client proper encryption techniques to protect data, both in storage and during transmission. The labs in this module demonstrate the use of encryption to protect information systems in organizations.

Lab 1: Encrypt the Information using Various Cryptography Tools

As a professional ethical hacker and penetration tester, you should use various cryptography techniques or tools to protect confidential data against unauthorized access. Cryptography protects confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, and many other kinds of communication. Encrypted messages can at times be decrypted by cryptanalysis (code breaking), although modern encryption techniques are virtually unbreakable.

The labs in this exercise demonstrate how you can use various cryptography tools to encrypt important information in the system

System administrators use cryptography tools to encrypt system data within their network to prevent attackers from modifying the data or misusing it in other ways. Cryptography tools can also be used to calculate or decrypt hash functions available in MD4, MD5, SHA-1, SHA-256, etc.

Cryptography tools are used to convert the information present in plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme. The converted data are in the form of a scrambled code that is encrypted and sent across a private or public network.

Task 1: Perform Multi-layer Hashing using CyberChef

CyberChef enables a wide array of «cyber» tasks directly in browser. It offers a wide range of operations and transformations, from basic text manipulation to complex cryptographic functions which include various hashing techniques such as MD5, SHA-1, SHA-256, SHA-512, etc., and encoding techniques such as text to hexadecimal, binary, Base64, or URL encoding.

A multi-layer hash typically refers to a hierarchical or nested structure of hash functions applied successively to data. Instead of just applying a single hash function to a piece of data, multiple hash functions are employed in layers or stages, with the output of one hash function serving as the input to the next one.

Task 2: Perform File and Text Message Encryption using CryptoForge

Lab 2: Create a Self-signed Certificate

Task 1: Create and Use Self-signed Certificates

Lab 3: Perform Disk Encryption

Disk encryption is a technology that protects the confidentiality of the data stored on a disk by converting it into an unreadable code using disk encryption software or hardware, thus preventing unauthorized users from accessing it. Disk encryption provides confidentiality and privacy using passphrases and hidden volumes. As a professional ethical hacker or pen tester, you should perform disk encryption in order to prevent sensitive information from unauthorized access.

Disk encryption works in a manner similar to text-message encryption and protects data even when the OS is not active. By using an encryption program for the user's disk (Blue Ray, DVD, USB flash drive, External HDD, and Backup), the user can safeguard any or all information burned onto the disk and thus prevent it from falling into the wrong hands. Disk-encryption software scrambles the information burned on the disk into an illegible code. It is only after decryption of the disk information that one can read and use it.

This lab will demonstrate the use of various disk encryption tools to perform this technique.

Disk encryption is useful when the user needs to send sensitive information through email. In addition, disk encryption can prevent the real-time exchange of information from threats. When users exchange encrypted information, it minimizes the chances of compromising the data; the only way an attacker could access the information is by decrypting the message. Furthermore, encryption software installed on a user's system ensures the security of the system. Install encryption software on any systems that hold valuable information or on those exposed to unlimited data transfer.

Task 1: Perform Disk Encryption using VeraCrypt

VeraCrypt is a software used for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved, and decrypted just after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

Lab 4: Perform Cryptography using AI

Task 1: Perform Cryptographic Techniques using ShellGPT