Ethical Hacking

Module – 3

- **What are the different types of hacking methods? Ethical Hacking**
  - ✓ Phishing. ...
  - ✓ Bait and Switch Attack.
  - ✓ Key Logger.
  - ✓ Denial of Service (DoS\DDoS) Attacks.
  - ✓ Click Jacking Attacks.
  - ✓ Fake W.A.P.
  - ✓ Cookie Theft. ...
  - ✓ Viruses and Trojans.

- **Explain Types of Password Attacks**

Brute Force Attack

If a password is equivalent to using a key to open a door, a brute force attack is using a battering ram. A hacker can try 2.18 trillion password/username combinations in 22 seconds, and if your password is simple, your account could be in the crosshairs.

Phishing

Phishing is when a hacker posing as a trustworthy party sends you a fraudulent email, hoping you will reveal your personal information voluntarily. Sometimes they lead you to fake "reset your password" screens; other times, the links install malicious code on your device. We highlight several examples on the OneLogin blog.

Man-in-the-Middle Attack

Man-in-the middle (MitM) attacks are when a hacker or compromised system sits in between two uncompromised people or systems and deciphers the information they're passing to each other, including passwords. If Alice and Bob are passing notes in class, but Jeremy has to relay those notes, Jeremy has the opportunity to be the man in the middle. Similarly, in 2017, Equifax removed its apps from the App Store and Google Play store because they were passing sensitive data over insecure channels where hackers could have stolen customer information.

Dictionary Attack

A type of brute force attack, dictionary attacks rely on our habit of picking "basic" words as our password, the most common of which hackers have collated into "cracking dictionaries." More sophisticated dictionary attacks incorporate words that are personally important to you, like a birthplace, child's name, or pet's name.

Credential Stuffing

If you've suffered a hack in the past, you know that your old passwords were likely leaked onto a disreputable website. Credential stuffing takes advantage of accounts that never had their passwords changed after an account break-in. Hackers will try various combinations of former usernames and passwords, hoping the victim never changed them.

Keyloggers

Keyloggers are a type of malicious software designed to track every keystroke and report it back to a hacker. Typically, a user will download the software believing it to be legitimate, only for it to install a keylogger without notice.

- **Explain Password Cracking Tools: pwdump7**

PwDump7:

This utility was created by Tarasco. This utility dumps the system's SAM file's credentials after extracting it. Simply enter the following line on the command prompt after downloading to use this tool:

PwDump7.exe

As a result, it will spill all the hashes kept in the SAM file. The next step is to use the commands below to save the registry values for the SAM file and system file in a system file:

reg save hklm\sam c:\sam

reg save hklm\system c:\system

With the aforementioned command, we stored the values to get the data from the SAM file.

Usage:

pwdump7.exe (Dump system passwords)

pwdump7.exe -s <samfile> <systemfile> (Dump passwords from files)

pwdump7.exe -d <filename> [destination] (Copy filename to destination)

pwdump7.exe -h (Show this help)

- **Explain Types of Steganography with QuickStego**

Text Steganography

There is steganography in text files, which entails secretly storing information. In this method, the hidden data is encoded into the letter of each word.

Image Steganography

The second type of steganography is image steganography, which entails concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography.

Since the computer description of an image contains multiple bits, images are frequently used as a cover source in digital steganography.

The various terms used to describe image steganography include:

- ✓ Cover-Image - Unique picture that can conceal data.
- ✓ Message - Real data that you can mask within pictures. The message may be in the form of standard text or an image.
- ✓ Stego-Image − A stego image is an image with a hidden message.
- ✓ Stego-Key - Messages can be embedded in cover images and stego-images with the help of a key, or the messages can be derived from the photos themselves.

Audio Steganography

It is the science of hiding data in sound. Used digitally, it protects against unauthorized reproduction. Watermarking is a technique that encrypts one piece of data (the message) within another (the "carrier"). Its typical uses involve media playback, primarily audio clips.

Video Steganography

Video steganography is a method of secretly embedding data or other files within a video file on a computer. Video (a collection of still images) can function as the "carrier" in this scheme. Discrete cosine transform (DCT) is commonly used to insert values that can be used to hide the data in each image in the video, which is undetectable to the naked eye. Video steganography typically employs the following file formats: H.264, MP4, MPEG, and AVI.

Network or Protocol Steganography

It involves concealing data by using a network protocol like TCP, UDP, ICMP, IP, etc., as a cover object. Steganography can be used in the case of covert channels, which occur in the OSI layer network model.

Steganography Examples Include

- ✓ Writing with invisible ink
- ✓ Embedding text in a picture (like an artist hiding their initials in a painting they've done)
- ✓ Backward masking a message in an audio file (remember those stories of evil messages recorded backward on rock and roll records?)
- ✓ Concealing information in either metadata or within a file header
- ✓ Hiding an image in a video, viewable only if the video is played at a particular frame rate
- ✓ Embedding a secret message in either the green, blue, or red channels of an RRB image

Steganography can be used both for constructive and destructive purposes. For example, education and business institutions, intelligence agencies, the military, and certified ethical hackers use steganography to embed confidential messages and information in plain sight.