Chapter 3.2

Password Cracking Mechanism

Aim

To enable the students to elucidate the process and practices of password cracking related to corporate marketing communications through the use of computer forensics

Instructional Objectives

After completing this chapter, you should be able to:

- Outline crucial aspects of steganography
- Elaborate on common tools for password cracking
- Explain the concept of email tracking
- Explain the concept of password cracking

Introduction to Password Mechanism

Introduction to Password Mechanism

To secure document or any information, the general practice is to protect it with the password.

In digital forensic investigation we come across the password protected documents or data during the investigation of digital evidence.

One of the most common ways of overcoming password protection is password cracking.

Introduction to Password Mechanism

- Passwords, along with their corresponding usernames, are used as a method of authentication. Authentication means verification of the fact that the user wishing to gain access is who he or she claims to be.
- During forensic investigations, a variety of items might be password protected.
- These items could include operating systems, CMOS, various files or documents (for example Microsoft Word documents and even compressed files), and even software.

Steganography

Definition of Steganography

Steganography is the art and science of communicating in a manner where a message cannot be detected. Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in electronic format new techniques for information hiding have been discovered.

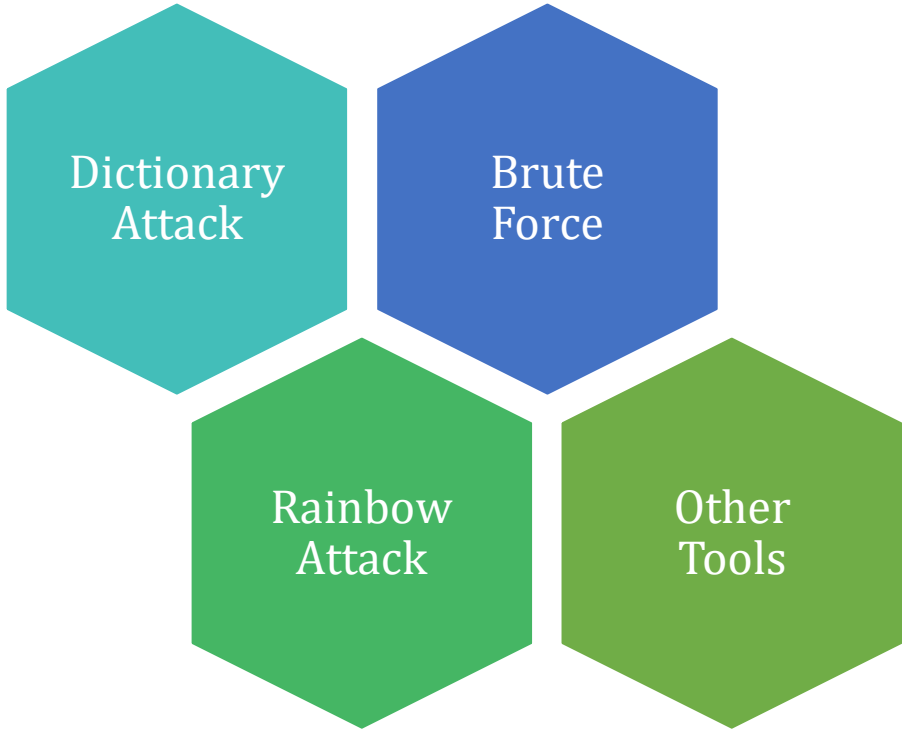
Steganography in detail

Steganography includes the following:

Common Tools for Password Cracking

Common Tools for Password Cracking

The common tools for password cracking mechanism are as follows:



Quiz / Assessment

1) Dictionary attacks is a common tool of _____.

a. Password cracking
b. Email tracking
c. Steganography
d. Digital cracking

Quiz / Assessment

2) Information hiding is a part of _____.

a. Evidence
b. Tracking
c. Steganography
d. Investigation

Quiz / Assessment

3) In the digital realm, steganography, involves _____in digital files.

a. Hiding data or message
b. Estimating data or plan
c. Tracking email or data
d. Forensic evidence or file

Email Tracking

Concept of Email Tracking – Internet Standard Protocols

SMTP

- Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission. SMTP by default uses TCP port25.

POP3

- The Post Office Protocol (POP) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.

Concept of Email Tracking - Internet Standard Protocols (contd.)

IMAP

- Internet Message Access Protocol (IMAP) is an Internet standard protocol used by e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection.

Quiz / Assessment

1) SMTP stands for _____.

a. Simple Mode Transfer Process
b. Simple Mail Transfer Protocol
c. Simple Machine Troll Process
d. Simple Method Target Procedure

Quiz / Assessment

2) _____ supports simple download-and-delete requirements for access to remote mailboxes.

a. POS
b. POD
c. POP
d. POC

Quiz / Assessment

3) IMAP is defined by _____.

a. RFC 3501
b. RFC 3509
c. RFS 3501
d. RCF 3502

Concept of Password Cracking

Concept of Password Cracking

Cryptanalysis	• Cryptanalysis and computer security systems have password cracking as a process of retrieving passwords from data which is saved in or transmitted by a computer system.
Common methods of Password cracking	• Pattern checking, word list substitution, dictionary attacks , etc.
Brute force attack	• A common approach (brute-force attack) is to attempt as many guesses as possible repeatedly for the password and use the available cryptographic hash of the password to check them.

Concept of Password Cracking

Steganography

- Steganography is derived from the Greek word, which means secret writing or covered.
- The intention of steganography is to hide the message in such a way that no one apart from the intended receiver even comes to know that the message has been sent.
- Higher the password bit strength, higher the number of candidate passwords that need to be verified, to recover the password and reduces the chances of the password to be found in any cracking dictionary.

Quiz / Assessment

1)The _____ the most common methods used in password cracking.

a) Rainbow
b) Dictionary
c) THC Hydra
d) Password strength

Quiz / Assessment

2) Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. State true or false.

a) True
b) False

Quiz / Assessment

3) Steganography is derived from the Greek word, which means _____.

a) Code wording
b) secret writing
c) short form writing
d) sky writing

Activity

Offline/Online Activity

Offline/Online Activity
(40 min)

- Explain the working of DES algorithm in steganography
- Using steganography, hide information in an image

Note: Refer Table of Content for the activities

Summary

- ✓ There are numerous programs accessible for password attack (or even auditing and recovery by systems personnel) such as L0phtCrack ,John the Ripper, and Cain; some of which use password design vulnerabilities (as found in the Microsoft LAN Manager system) to increase competency.
- ✓ The network security is becoming more important as the amount of data being exchanged on the Internet increases.
- ✓ Higher the password bit strength, exponentially high will be the number of candidate passwords that need to be checked, to recover the password; it reduces the possibility that the password will be found by cracking a dictionary.
- ✓ Well known email applications such as Microsoft Office Outlook and the convenient Mozilla Thunderbird, opt for a read-receipt tracking mechanism.

e-References

- (2016). Retrieved 15 June 2016, from https://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.pdf

- Popular Tools for Brute-force Attacks - InfoSec Resources. (2015). InfoSec Resources. Retrieved 15 June 2016, from http://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/

- 10 Most Popular Password Cracking Tools - InfoSec Resources. (2014). InfoSec Resources. Retrieved 15 June 2016, from http://resources.infosecinstitute.com/10-popular-password-cracking-tools/

- (2016). Retrieved 15 June 2016, from http://airccse.org/journal/nsa/1111nsa17.pdf

External Resources

- Hayes, D. D. *A Practical Guide to Computer Forensics Investigations.* US: Pearson Education, Inc. (2015).
- Nelson, B., Phillips, A., & Steuart, C. *Guide to Computer Forensics and Investigations, Fourth Edition*. USA: Cengage Learning. (2010).
- Philipp, A., Cowen, D., & Davis, C.*Hacking Exposed Computer Forensics, Second Edition*. New York: McGraw-Hill. (2010).