

LATE BHAUSAHEB HIRAY S.S. TRUST'S INSTITUTE
OF COMPUTER APPLICATION, MUMBAI

Ethical Hacking Lab Manual

**DR. RASHMITA PRADHAN,
PRAKASH SAKHARKAR**

Faculty, Master of Computer Application (M.C.A.)

Late Bhausaheb Hiray S.S. Trust's Institute of Computer Application



ETHICAL HACKING LAB MANUAL

ETHICAL HACKING LAB MANUAL

LATE BHAUSAHEB HIRAY S.S. TRUST'S INSTITUTE OF COMPUTER
APPLICATION BANDRA, EAST MUMBAI-51

Dr. Rashmita Pradhan

Co-Authors: Asst. Prof. Prakash Sakharkar

Faculty, Master of Computer Application (M.C.A.)

Late Bhausaheb Hiray S.S. Trust's Institute of Computer Application



First Edition, 2023

Copyright © Late Bhausaheb Hiray S.S.Trust's Institute Of Computer Application, Bandra (E), Mumbai-51, 2023

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the author, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. For permission requests, write to the publisher at the address below.

This book can be exported from India only by the publishers or by the authorized suppliers. Infringement of this condition of sale will lead to Civil and Criminal prosecution.

Paperback ISBN: 978-81-19221-44-8

eBook ISBN: 978-81-19221-52-3

WebPDF ISBN: 978-81-19221-53-0

Note: Due care and diligence has been taken while editing and printing the book; neither the author nor the publishers of the book hold any responsibility for any mistake that may have inadvertently crept in.

The publishers shall not be liable for any direct, consequential, or incidental damages arising out of the use of the book. In case of binding mistakes, misprints, missing pages, etc., the publishers' entire liability, and your exclusive remedy, is replacement of the book within one month of purchase by similar edition/reprint of the book.

Printed and bound in India by

16Leaves

2/579, Singaravelan Street

Chinna Neelankarai

Chennai - 600 041, India

info@16leaves.com

www.16Leaves.com

Call: 91-9940638999

Contents

1. Use software tools/commands to perform foot printing/information gathering and generate analysis report	1
2. Use software tools/commands to perform network scanning and sniffing and generate analysis report	7
3. Use software tools/commands to perform malware attacks and other cyber-attacks and generate analysis report	21
4. Implementation of keyloggers, viruses and trojans	31
5. Use of software tools/commands for web servers and web applications hacking and generate analysis report	35
6. Use of software tools/commands for performing SQL injection and session hijacking and generate analysis report	43
7. Use of software tools/commands to encrypt and decrypt password, implement encryption and decryption using Ceaser Cipher	49
8. Using Metasploit and metasploitable for penetration testing	55

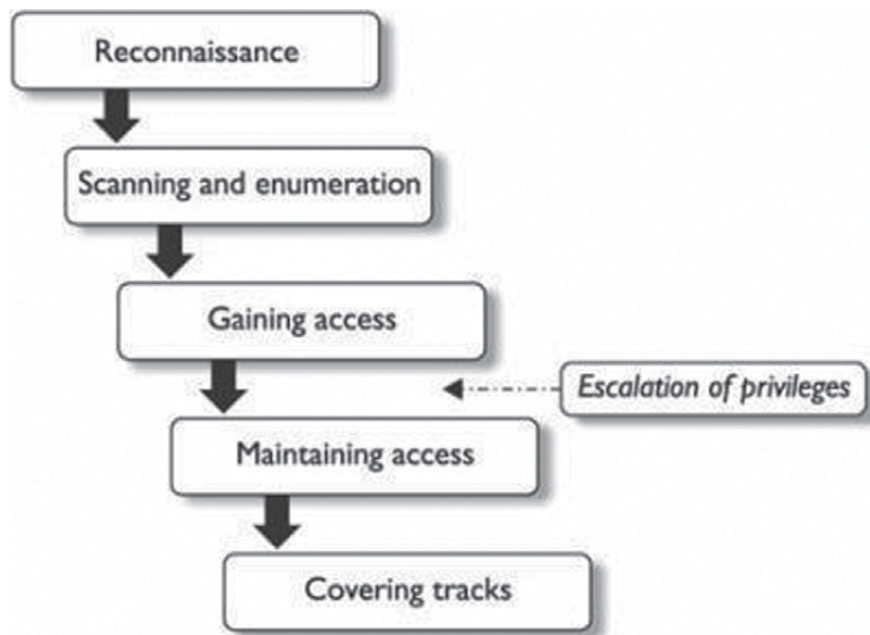
Chapter 1 Use software tools/commands to perform foot printing/ information gathering and generate analysis report

Practical No. 01 ◀◀◀

Aim: Use software tools/commands to perform foot printing /information gathering and generate analysis report

Solution:

Phases of Ethical Hacking



Footprinting is a part of Reconnaissance

Types of Footprinting

- 1) Passive
- 2) Active

During footprinting, a hacker can collect the

- 1) Domain Name
- 2) IP Address
- 3) Namespaces

- 4) Employee Information
- 5) Phone Numbers
- 6) E-mails
- 7) Job Information

Footprinting methods and tools

1) Search Engines

- Google Earth
- Google Maps
- Bing Maps

The above Search Engines provide Location Information

- LinkedIn.com
- Piple.com
- These sites are used to view the Personal Information
- www.netcraft.com
- **Performing footprinting using Google Hacking commands**

2) Google Hacking

Google Hacking involves Manipulating a Search String with addition of specific Operators to search for vulnerabilities.

Basic Examples

This Search	Find Pages Containing...
Biking Italy	The words biking and Italy
Recycle steel OR iron	Information on recycling steel or recycling iron
"I have a dream"	The exact phrase I have a dream
Salsa -dance	The word Salsa but NOT the word dance
Louis "I" France	Information about Louis the First (I), weeding out other kings of France
Castle ~glossary	Glossaries about Castles , as well as dictionaries , lists of terms , terminology , etc.
Fortune-telling	All forms of the term, whether spelled as a single word, a phrase, or hyphenated
define: imbrogio	Definitions of the word imbrogio from the Web

Calculator

Operators	Meaning	Type into Search Box (& Results)
+ - * /	Basic Arithmetic	12 + 34 - 56 * 7 / 8
% of	Percentage of	45% of 39
^ or **	Raise to a power	2 ^ 5 or 2 ** 5
Old units in new units	Convert units	300 Euros in USD, 130 lbs. in kg, or 31 in hex

Restrict Search

Operators	Meaning	Type into Search Box (& Results)
city1 city2	Book flights	SFO BOS (Book flights from San Francisco (SFO) to Boston (BOS))
site:	Search only one website or domain	Halloween site:www.census.gov (Search for information on Halloween gathered by the US Census Bureau.)
[#]..[#]	Search within a range of numbers.	Dave Barry pirate 2002..2006 (Search for Dave Barry articles mentioning pirates written in these years.)
filetype: (or ext:)	Find documents of the specified type	Form 1098-T IRS filetype: pdf (Find the US tax form 1098-T in PDF format.)
link:	Find linked pages, i.e., show pages that point to the URL	link:warriorlibrarian.com (Find pages that link to Warrior Librarian's website.)

Specialized Information Queries

Operators	Meaning	Type into Search Box (& Results)
book (or books)	Search full-text of books	book Ender's Game (Show book-related information Note: No colon needed after book .)
define, what is, what are	Show a definition for a word or phrase	Define monopsony, what is podcast (Show a definition for the words monopsony and podcast .)
define:	Provide definitions for words, phrases, any acronyms from the web.	define: kerning (Find definitions for kerning from the Web.)
movie:	Find reviews and showtimes	movie: traffic (Search for information about this movie, including reviews, showtimes, etc.)