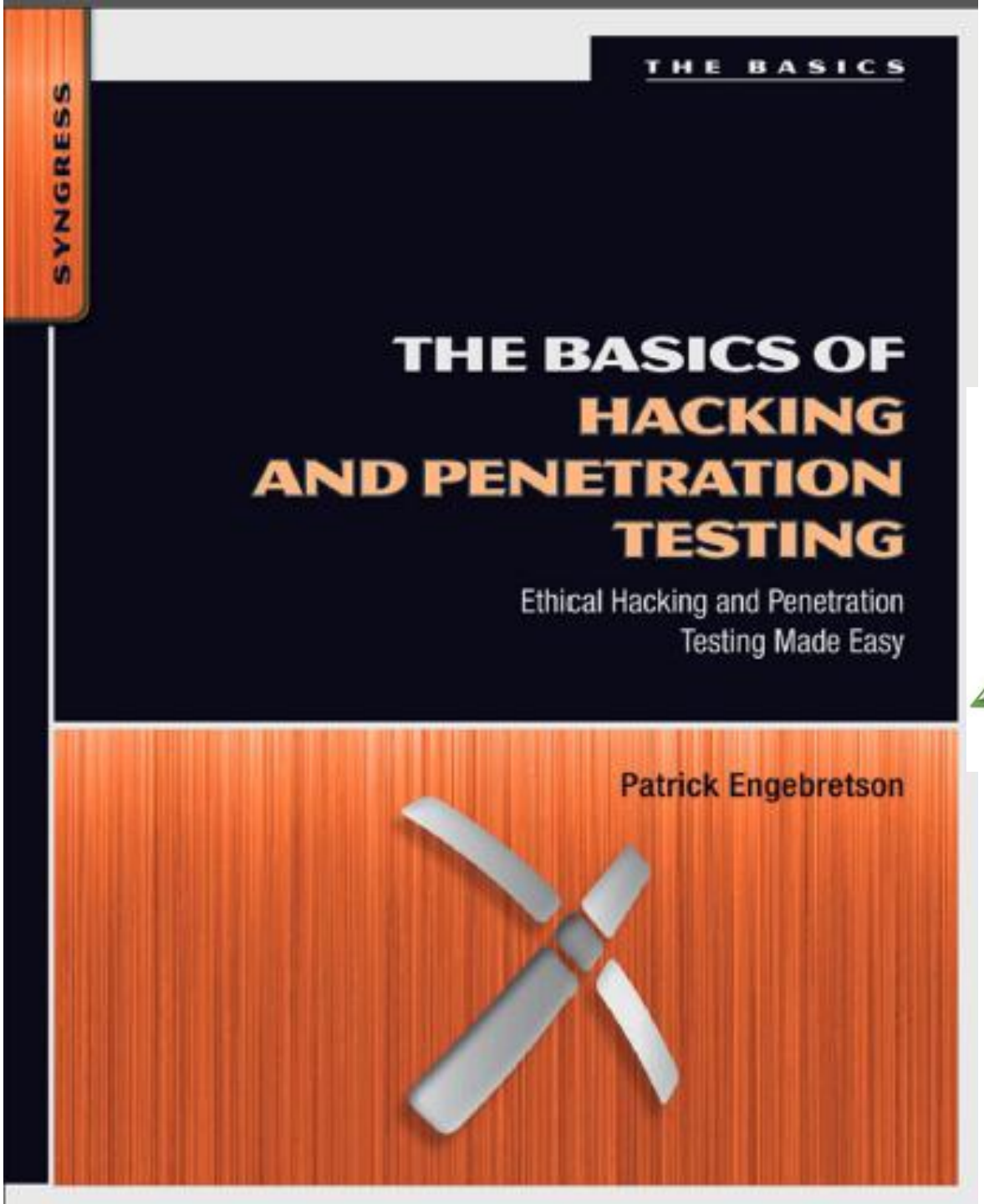
Book Review

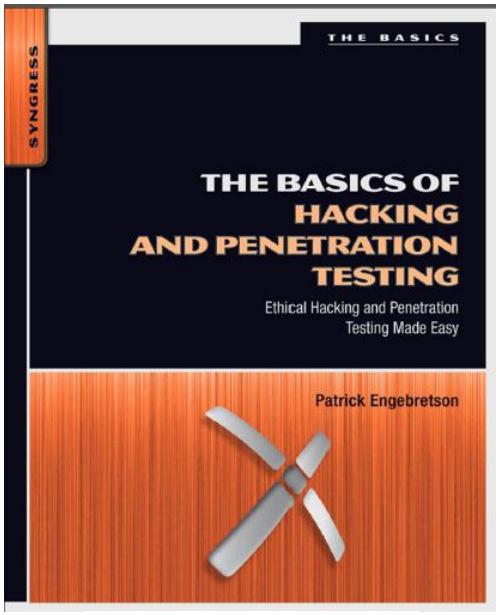


MY BOOK REVIEW

Anupam Tiwari

About the Book

Book Name	The basics of Hacking & Penetration Testing
Author	Patrick Engebretson
Technical Editor	James Broad
Publisher	Syngress
Pages	169



Who is this Author ?

AUTHOR

Dr Patrick Engebretson

Doctor of Science Degree with spl in Info Sec

Dakota State University

Asst Professor of Info Assurance

Senior Penetration Tester

Research ON penetration testing, hacking & malware

Why did I choose this Book?

Webinar in 2008 Apr conducted by Microsoft

Book published in 2011

Complimentary Copy

My own interest

Very Easy to assimilate and understand

Most of IT is Based on Open Source

Who is the Intended Audience?

New to HACKING ?

No experience ?

Frustrated ?

Expand Knowledge

Interested in Computer Security

Not sure where to begin?

Zero entry Hacking

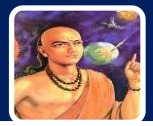
How is the Book Different from rest ?

Quality of Text

Will not make you go haywire

Based on Open source

Precise and to the point - 169



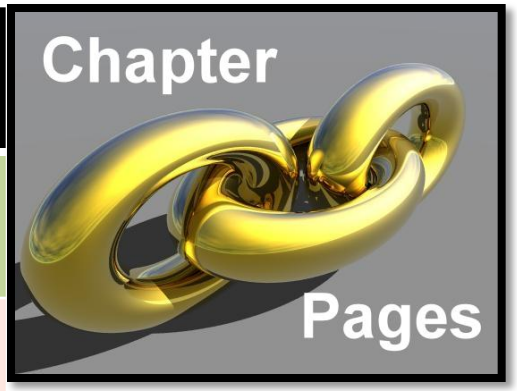
Zero Entry

Tools with screen shots

Creates and Solves Challenges

CHAPTERS

CHAPTER	NAME OF CHAPTER	PAGES
CHAPTER 1	What is Penetration Testing?	1
CHAPTER 2	Reconnaissance	15
CHAPTER 3	Scanning	43
CHAPTER 4	Exploitation	65
CHAPTER 5	Web Based Exploitation	107
CHAPTER 6	Maint Access with Back Doors & RootKits	127
CHAPTER 7	Wrapping up	145



What is Penetration Testing ?

Sandboxed Environment

PRACTISE & INTRO

CREATION OF PEN TEST LAB

4 STEP METHODOLGY

RECONNAISSANCE

SCANNING

EXAMPLES & PRACTICALS

EXPLOITATION

MAINT ACCESS

Chapter

RECONNAISSANCE

HTTrack	GOOGLE DIRECTIVES	HARVESTER	NETCRAFT	HOST	METAGooFI

Google UK
bing
YAHOO!

GOOGLE FU

- Strong
- Search Engine Directives

SEAT

- Search Engine Assessment Tool
- SEAT

JOHNNY LONG

- Single Repository
- Most Feared Google Hack

PATREVA's MALETEGO

- Aggregates info from public data base

Chapter 3

SCANNING

BRIEF OVER VIEW OF PINGS & PING SWEEPS

PORTs

VULNERABILITY

Chapter

EXPLOITATION

- Remote services

MEDUSA

METASPOLIT

- Hugh jackman style

- Powerful
- Proven

JOHN : THE RIPPER

DSNIFF

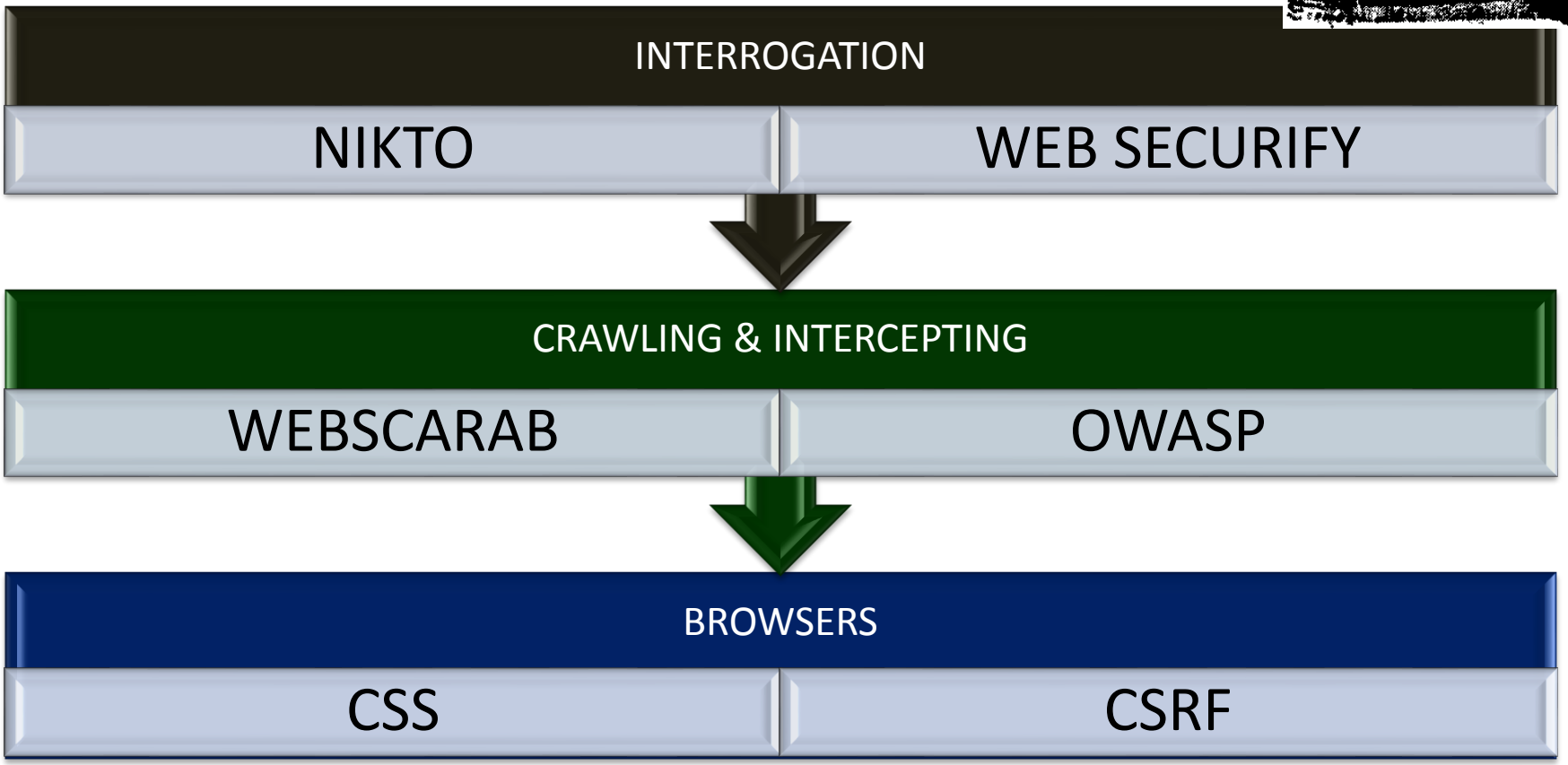
- Collection of tools

- Security Testing

FAST TRACK AUTOPWN

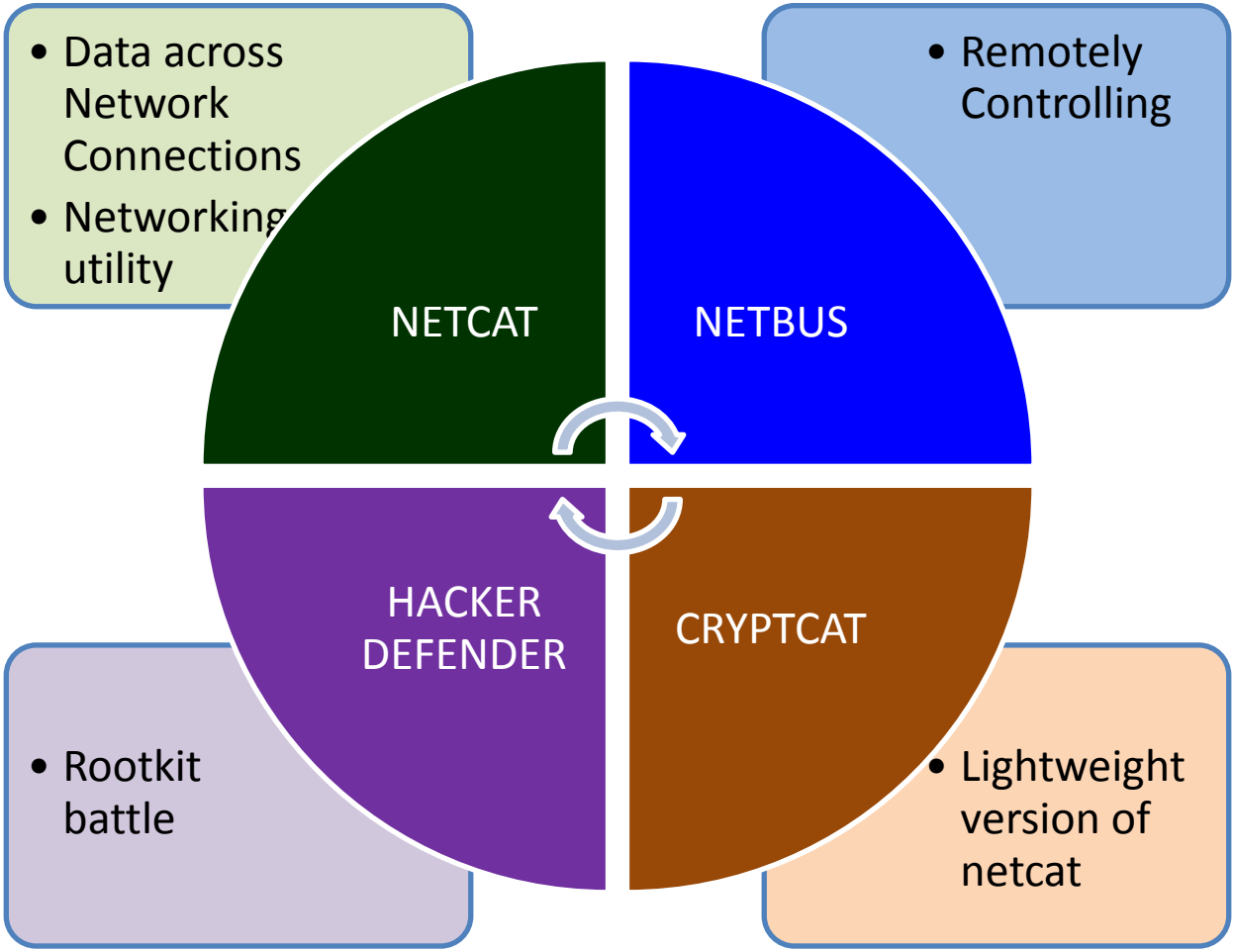
Chapter 5

WEB BASED EXPLOITATION



Chapter 6

MAINT ACCESS



Chapter 7

WRAPPING UP

WRAPPING UP THE PEN TEST

PEN TEST REPORT

EXEC SUMMARY

DETAILED REPORT

RAW OUTPUT

TRUE CRYPT

7 ZIP

WRAP UP