

Advanced Penetration Testing: A CEH Professional's Field Guide

Dinh Ngoc Dung

Advanced Penetration Testing: A CEH Professional's Field Guide

Dinh Ngoc Dung

This book is available at <https://leanpub.com/advanced-pentest-ceh-guide>

This version was published on 2026-07-29



This is a [Leanpub](#) book. Leanpub empowers authors and publishers with the Lean Publishing process. [Lean Publishing](#) is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

© 2026 Dinh Ngoc Dung

Contents

Advanced Penetration Testing: A CEH Professional's Field Guide	1
Practical Methodology for Authorized Security Assessments	1
About the Author	1
Preface	1
Part One: Foundations and Methodology	1
Part Two: Reconnaissance	2
Part Three: Vulnerability Analysis and Exploitation	4
Part Four: Post-Exploitation	7
Part Five: Specialized Testing Domains	9
Part Six: Reporting and Professional Practice	11
Conclusion: The Path Forward for the CEH Professional	12
References	13
Writing in Markua	14
Section One	14
Including a Chapter in the Sample Book	14
Links	14
Images	14
Lists	19
Page Breaks	20
Code Samples	21
Tables	22
Math	22
Headings	23
Block quotes, Asides and Blurbs	24
Good luck, have fun!	26

Advanced Penetration Testing: A CEH Professional's Field Guide

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Practical Methodology for Authorized Security Assessments

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

About the Author

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Preface

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Part One: Foundations and Methodology

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 1: The Penetration Testing Execution Standard (PTES)

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Overview

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

The Seven Phases of PTES

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Applying PTES in Practice

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 2: Legal and Ethical Framework for Penetration Testing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Authorization as the Foundation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Key Legal Frameworks

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

The Rules of Engagement

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Ethical Obligations of the Penetration Tester

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Part Two: Reconnaissance

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 3: Passive Reconnaissance and OSINT

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Principles of Passive Reconnaissance

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

DNS Reconnaissance

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

WHOIS and Registration Data

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Search Engine Reconnaissance (Google Dorking)

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Social Media and LinkedIn Intelligence

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Code Repository Mining

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Shodan, Censys, and Internet-Wide Scanning Data

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 4: Active Reconnaissance and Network Mapping

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Transitioning from Passive to Active

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Network Scanning with Nmap

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Web Application Fingerprinting

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Directory and File Enumeration

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Part Three: Vulnerability Analysis and Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 5: Vulnerability Scanning and Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

The Role of Vulnerability Scanning

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Nessus Professional

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

OpenVAS / Greenbone

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Manual Vulnerability Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 6: Exploitation with the Metasploit Framework

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Metasploit Architecture

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Working with Metasploit: Core Workflow

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

EternalBlue (MS17-010): A Case Study

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

PrintNightmare (CVE-2021-1675 / CVE-2021-34527)

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 7: Web Application Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Web Application Testing Methodology

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

SQL Injection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Cross-Site Scripting (XSS)

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Server-Side Request Forgery (SSRF)

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 8: Network Protocol Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

SMB Protocol Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Active Directory Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Part Four: Post-Exploitation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 9: Privilege Escalation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

The Significance of Privilege Escalation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Windows Privilege Escalation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Linux Privilege Escalation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 10: Lateral Movement Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Lateral Movement as Attacker Behavior

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Pass-the-Hash and Pass-the-Ticket

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Remote Service Execution

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Living Off the Land (LOLBins)

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 11: Persistence Mechanisms

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Why Persistence Matters in Penetration Testing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Windows Persistence

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Linux Persistence

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 12: Data Exfiltration Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Simulating Data Exfiltration

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Exfiltration Channels

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Egress Filtering Assessment

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Part Five: Specialized Testing Domains

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 13: Wireless Network Security Testing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Wireless Testing Scope

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

WPA2-Personal Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

WPA2/WPA3-Enterprise Attacks

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Rogue Access Point Detection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 14: Cloud Penetration Testing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Cloud Security Assessment Framework

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

AWS Penetration Testing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Azure Penetration Testing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 15: Mobile Security Testing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

iOS and Android Security Models

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

OWASP Mobile Top 10 Testing

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Frida and Dynamic Instrumentation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Part Six: Reporting and Professional Practice

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 16: Penetration Test Reporting

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

The Report as Primary Deliverable

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Report Structure

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Risk Rating Methodology

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 17: Purple Team Operations

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

From Red Team to Purple Team

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Purple Team Exercise Structure

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

MITRE ATT&CK Navigator

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Atomic Red Team

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Chapter 18: Setting Up a Penetration Testing Lab

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Lab Environment Philosophy

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

VirtualBox / VMware Lab Setup

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Vulnerable-by-Design Platforms

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Cloud Lab on a Budget

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Conclusion: The Path Forward for the CEH Professional

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

References

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/advanced-pentest-ceh-guide>.

Writing in Markua

Writing in Markua is easy! You can learn most of what you need to know with just a few examples.

To make *italic text* you surround it with single asterisks. To make **bold text** you surround it with double asterisks.

Section One

You can start new sections by starting a line with two # signs and a space, and then typing your section title.

Sub-Section One

You can start new sub-sections by starting a line with three # signs and a space, and then typing your sub-section title.

Including a Chapter in the Sample Book

At the top of this file, you will also see a line at the top:

```
1 {sample: true}
```

Leanpub has the ability to make a sample book, which interested readers can download or read online. If you add this line above a chapter heading, then when you publish your book, this chapter will be included in a separate sample book for these interested readers.

Links

You can add web links easily.

Here's a link to the [Leanpub homepage](#).

Images

You can add an image to your book in a similar way.

First, add the image to the “Resources” folder for your book. You will find the “Resources” folder under the “Manuscript” menu to the left.

If you look in your book’s “Resources” folder right now, you will see that there is an example image there with the file name “palm-trees.jpg”. Here’s how you can add this image to your book:



If you want to add a figure title, you put it in quotes:



Figure 1. Palm Trees

If you want to add descriptive alt text, which is good for accessibility, you put it between the square brackets:



Figure 2. Palm Trees

You can also set the alt text and/or the figure title in an attribute list:



Figure 3. Palm Trees

Finally, if no title is provided, and the `alt-title` document setting is the default of `all`, the alt text will be used as the figure title instead of as alt text.



Figure 4. Palm Trees

You can set the important document settings at Settings > Generation Settings.

Lists

Numbered Lists

You make a numbered list like this:

1. kale
2. carrot
3. ginger

Bulleted Lists

You make a bulleted list like this:

- kale

- carrot
- ginger

Definition Lists

You can even have definition lists!

term 1

definition 1a

definition 1b

term 2

definition 2

Page Breaks

We don't recommend that you manually break pages, since that is brittle and can lead to unexpected formatting if you edit text earlier in your chapter and forget about the manual page breaks. But if you really want to add a page break, you use the `{pagebreak}` directive on a line by itself, with blank lines above it and below it.

Code Samples

You can add code samples really easily. Code can be in separate files (a “local” resource) or in the manuscript itself (an “inline” resource).

Local Code Samples

Here’s a local code resource:

Figure 5. Hello World in Ruby

```
1 require 'time'
2
3 # This is just some pointless code so you can see the syntax highlighting...
4 def display_info
5   pi = Math::PI.round(10)
6   time_last_year = (Time.now - 365 * 24 * 60 * 60).getlocal("-08:00")
7   formatted_time = time_last_year.strftime("%Y-%m-%d %H:%M:%S")
8   puts "Pi to 10 decimal places: #{pi}"
9   puts "The time 1 year ago in Pacific Time: #{formatted_time}"
10 end
```

Inline Code Samples

Inline code samples can either be spans or figures.

A span looks like `puts "hello world"` this.

A figure looks like this:

```
1 require 'time'
2
3 # This is just some pointless code so you can see the syntax highlighting...
4 def display_info
5   pi = Math::PI.round(10)
6   time_last_year = (Time.now - 365 * 24 * 60 * 60).getlocal("-08:00")
7   formatted_time = time_last_year.strftime("%Y-%m-%d %H:%M:%S")
8   puts "Pi to 10 decimal places: #{pi}"
9   puts "The time 1 year ago in Pacific Time: #{formatted_time}"
10 end
```

You can also add a figure title using the title attribute:

Figure 6. Hello World in Ruby

```
1 require 'time'
2
3 # This is just some pointless code so you can see the syntax highlighting...
4 def display_info
5   pi = Math::PI.round(10)
6   time_last_year = (Time.now - 365 * 24 * 60 * 60).getlocal("-08:00")
7   formatted_time = time_last_year.strftime("%Y-%m-%d %H:%M:%S")
8   puts "Pi to 10 decimal places: #{pi}"
9   puts "The time 1 year ago in Pacific Time: #{formatted_time}"
10 end
```

Tables

You can insert tables easily inline, using the GitHub Flavored Markdown (GFM) table syntax:

Header 1	Header 2
Content 1	Content 2
Content 3	Content 4 Can be Different Length

Tables work best for numeric tabular data involving a small number of columns containing small numbers:

Central Bank	Rate
JPY	-0.10%
EUR	0.00%
USD	0.00%
CAD	0.25%

Definition lists are preferred to tables for most use cases, since reading a large table with many columns is terrible on phones and since typing text in a table quickly gets annoying.

Math

You can easily insert math equations inline using either spans or figures.

Here’s one of the kinematic equations $d = v_i t + \frac{1}{2} a t^2$ inserted as a span inside a sentence.

Here’s some math inserted as a figure.

$$\left| \sum_{i=1}^n a_i b_i \right| \leq \left(\sum_{i=1}^n a_i^2 \right)^{1/2} \left(\sum_{i=1}^n b_i^2 \right)^{1/2}$$

Figure 7. Something Involving Sums

Headings

Markua supports both of Markdown’s heading styles.

The preferred style, called atx headers, has the following meaning in Markua:

```
1 {class: part}
2 # Part
3
4 This is a paragraph.
5
6 # Chapter
7
8 This is a paragraph.
9
10 ## Section
11
12 This is a paragraph.
13
14 ### Sub-section
15
16 This is a paragraph.
17
18 #### Sub-sub-section
19
20 This is a paragraph.
21
22 ##### Sub-sub-sub-section
23
```

```

24 This is a paragraph.
25
26 ##### Sub-sub-sub-sub-section
27
28 This is a paragraph.

```

Note the use of three backticks in the above example, to treat the Markua like inline code (instead of actually like headers).

The other style of headers, called Setext headers, has the following headings:

```

1 {class: part}
2 Part
3 ====
4
5 This is a paragraph.
6
7 Chapter
8 =====
9
10 This is a paragraph.
11
12 Section
13 -----
14
15 This is a paragraph.

```

Setext headers look nice, but only if you're only using chapters and sections. If you want to add sub-sections (or lower), you'll be using atx headers for at least some of your headers. My advice is to just use atx headers all the time. (The `{class: part}` attribute list on a chapter header to make a part header does actually work with Setext headers, but it's really ugly.)

Note that while it is confusing and ugly to mix and match using atx and Setext headers for chapters and sections in the same document, you can do it. However, please don't.

Block quotes, Asides and Blurbs

Block quotes are really easy too.

—Peter Armstrong, *Markua Spec*

Asides are useful for longer text.
But typing them like this isn't fun.

Asides can be written this way, since adding a bunch of A> stuff at the beginning of each line can get annoying with longer asides.

Blurbs are useful

Blurbs are useful

There are many types of blurbs, which will be familiar to you if you've ever read a computer programming book.



This is a discussion.

You can also specify them this way:



This is a discussion



This is an error.



This is information.



This is a question. (Not a question in a Markua course; those are done differently!)



This is a tip.



This is a warning.



This is an exercise. (Not an exercise in a Markua course; those are done differently!)

Good luck, have fun!

If you've read this far, you're definitely the right type of person to be here!

Our last piece of advice is simple: once you have a couple chapters completed, publish your book in-progress!

This approach is called Lean Publishing. It's why Leanpub is called Leanpub.

If you want to learn more about Lean Publishing, read [this](#) or watch [this](#).