CODELIVLY OFFENSIVE SERIES

Enterprise Network Penetration Testing

The Complete Guide to Enterprise Network Reconnaissance, Internal Penetration Testing, Active Directory Assessments, Network Protocol Security, and Professional Security Assessments

Codelivly

www.codelivly.com

Authorized Testing · Blue-Team Aware

Beginner → Advanced

Enterprise Network Penetration Testing

The Complete Guide to Enterprise Network Reconnaissance, Internal Penetration Testing, Active Directory Assessments, Network Protocol Security, and Professional Security Assessments

Author: Codelivly · **Website:** www.codelivly.com

© Codelivly. All Rights Reserved.

No part of this publication may be reproduced, distributed, or transmitted in any form without prior written permission of the publisher, except for brief quotations used in reviews and certain non-commercial educational uses permitted by copyright law.

Responsible-Use Notice. This book is written for defenders and for security professionals who conduct *authorized* assessments. Every technique in this book assumes documented, signed authorization and a defined scope. The material emphasizes methodology, configuration review, detection, and remediation. It deliberately does not provide instructions for unauthorized intrusion, malware development, credential theft, or evasion of security controls. Performing any of these activities against systems you do not own or lack written permission to test may be a criminal offense.

Disclaimer. The information is provided "as is." The author and Codelivly assume no liability for misuse or for damages arising from the use of this material. Always operate within the law and your rules of engagement.

Edition 1.0 · Codelivly Offensive Series · Codelivly • www.codelivly.com

Table of Contents

Part I Network Pentesting Foundations 7

1 Introduction to Network Penetration Testing 8
2 Rules of Engagement, Authorization, Ethics & Law 13
3 Scoping, Methodology, and the Reporting Mindset 17

Part II Networking Fundamentals 22

4 The OSI and TCP/IP Models for Assessors 23
5 Addressing, Subnetting, Routing & Switching 27
6 Core Protocols: TCP, UDP, ARP, DNS, DHCP & ICMP 31
7 Firewalls, NAT, VPNs & Load Balancers 35

Part III Reconnaissance & Asset Discovery 39

8 Passive Reconnaissance 40
9 Active Reconnaissance: Host Discovery & Network Mapping 43
10 Service Identification, Banner Grabbing & OS Fingerprinting 47
11 DNS & SNMP Enumeration 50
12 Consolidating the Attack Surface & Asset Inventory 53
13 OSINT & External Footprinting 55

Part IV Network Service Assessment 58

14 SMB & Windows File Services 59
15 SSH & FTP 63
16 HTTP & HTTPS Services 65
17 DNS Services & Mail (SMTP) 68
18 LDAP & Directory Services 70
19 Kerberos Architecture & Assessment 73
20 Remote Access & Databases: RDP, WinRM, VNC & DB 76
21 SNMP & Network Device Assessment 78
22 VPN & Remote-Access Service Assessment 80

Part V Windows Enterprise Networks & Active Directory 83

23 Active Directory Fundamentals 84
24 Enterprise Enumeration Methodology 87
25 Group Policy, Delegation & Administrative Shares 90
26 BloodHound CE & PowerView: Assessment and Visualization 92
27 Active Directory Certificate Services (AD CS) Assessment 95
28 Domain & Forest Trust Security 97

29 Kerberos & NTLM Attack Surface: Assessment and Defense 99

Part VI Linux Network Security 102

30 Linux Services, NFS & Samba 103
31 Cron, Systemd, Permissions & Linux Hardening 105
32 Linux Authentication, PAM & Centralized Identity 107
33 Container & Virtualization Host Security 109

Part VII Network Vulnerability Assessment 112

34 Vulnerability Scanning & Manual Validation 113
35 Prioritization, Risk Rating & CVSS 115
36 Legacy Protocols & Insecure Services 117

Part VIII Segmentation & Lateral-Movement Risk Assessment 120

37 Segmentation, Trust Boundaries & Lateral-Movement Risk 121

Part IX Wireless Network Security 125

38 Wireless Security: WPA2, WPA3 & Enterprise 802.1X 126
39 Wireless Segmentation, Guest Networks & Monitoring 128

Part X Cloud & Hybrid Network Security 131

40 Cloud & Hybrid Network Security 132
41 AWS Network Security in Depth 134
42 Azure Network Security in Depth 136

Part XI Detection & Defensive Operations 139

43 Detection Engineering, Logging & MITRE ATT&CK 140
44 Network Detection with Zeek & Suricata 143
45 Endpoint Detection with Sysmon & Sigma 145
46 SIEM, Correlation & Alert Engineering 147

Part XII Professional Reporting & Communication 150

47 Professional Reporting & Communication 151

Part XIII Advanced Topics & Continuous Assessment 155

48 IPv6 Security Considerations 156
49 Wired 802.1X & Network Access Control 158
50 Attack-Surface Management & Continuous Validation 160
51 Building an Assessment Lab 162

Part XIV Applied Case Studies 166

52 Case Study: An Internal Network Assessment 167

53 Case Study: Active Directory Hardening **169**

Appendices & Reference **173**

Cheat sheets · Checklists · Event IDs · MITRE ATT&CK · Templates · Glossary

PART I

Network Pentesting Foundations

- Introduction to Network Pentesting
- What a Network Assessment Delivers
- Rules of Engagement
- Authorization & Scoping
- The Assessment Lifecycle
- Evidence & Reporting
- Ethics & Professional Conduct
- Legal Considerations
- Building a Home Lab
- A Career Roadmap

CHAPTER 1

Introduction to Network Penetration Testing

LEARNING OBJECTIVES

- Define enterprise network penetration testing and distinguish it from vulnerability scanning and red teaming.
- Explain **why** organizations commission internal network assessments and what business risk they reduce.
- Describe the mindset and workflow of a professional assessor.
- Understand where this discipline sits alongside the blue team and detection engineering.
- Set expectations for the lab environment used throughout the book.

A network penetration test is not about "breaking in." It is a structured, authorized investigation that answers a business question: if a threat actor gained a foothold in our environment, how far could they get, how quickly, and what would stop them?

1.1 What Network Penetration Testing Is

Enterprise network penetration testing is the practice of methodically evaluating the hosts, services, protocols, and trust relationships that make up an organization's internal and perimeter networks, in order to identify weaknesses that a real adversary could exploit, and then communicating those weaknesses in a way that lets the organization fix them. The word *enterprise* matters: we are rarely testing a single server. We are testing a living system of thousands of endpoints, dozens of services, an identity fabric (usually Active Directory), segmentation controls, and the humans who administer all of it.

The deliverable is not a shell. The deliverable is **clarity**: a prioritized, evidence-backed picture of risk, paired with remediation and detection guidance that a defender can act on. A test that produces ten screenshots of compromised hosts but no actionable remediation has failed at its actual job.

WHY DEFENDERS CARE

Everything an assessor discovers is something the blue team can **detect, prevent, or monitor**. Throughout this book, each offensive concept is paired with the log source, event ID, or network signature that would reveal it. Reading this book as a defender is just as valuable as reading it as a tester.

1.2 Assessment Types and Where They Differ

"Penetration test" is used loosely in industry. Understanding the distinctions keeps your scope honest and your reporting accurate.

Table 1.1 — Comparing common offensive-security engagement types.

Engagement	Primary question	Depth	Stealth	Typical output
Vulnerability scan	What known weaknesses exist?	Broad, shallow	None	Scanner report, CVSS list
Vulnerability assessment	Which weaknesses are real and how severe?	Broad + manual validation	None	Validated findings, risk ratings
Penetration test	How far can a validated weakness be leveraged?	Deep on paths	Low–medium	Attack narrative + remediation
Red team	Can we achieve a specific objective undetected?	Objective-driven	High	Objective outcome + detection gaps
Purple team	How well do detections perform against known TTPs?	Collaborative	Transparent	Detection coverage matrix

This book centers on the **vulnerability assessment**-to-**penetration test** band with a strong Active-Directory awareness, because that is what most internal enterprise engagements require. We consistently fold in **purple-team thinking**: for every finding, we ask what a SOC would see.

1.3 The Analyst's Mindset

Tools find *ports*; analysts find *risk*. The difference between a junior tester running Nmap and a principal consultant is not the tool — it is the questions asked of the output. A professional assessor works from hypotheses:

- "This host answers on 445 — is SMB signing enforced, and what does that imply for relay risk?"
- "This service banner claims an old version — is that patch level real, or a back-ported fix?"
- "This account can reach the DC on LDAP — is that expected for its role, or a segmentation gap?"
- "I found a finding — what is the *simplest* control that would have prevented it?"

> **COMMON MISTAKE**
>
> Treating scanner output as the finished product. A scanner reports symptoms; the analyst explains the disease, its impact in *this* environment, and the cure. Copy-pasting CVSS scores into a report without validation produces false positives, erodes client trust, and buries the findings that actually matter.

1.4 The Assessment Lifecycle at a Glance

Every engagement in this book follows the same repeatable lifecycle. We introduce it here and return to each phase in depth. The lifecycle is **iterative**: discovery feeds enumeration, which feeds validation, which frequently sends you back to discover more.

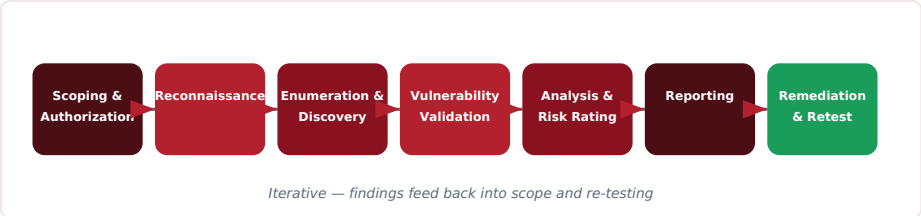


Figure 1.1. *The end-to-end assessment lifecycle. Authorization gates everything; reporting and retest close the loop.*

Table 1.2 — The seven phases used consistently throughout this book.

Phase	Goal	Representative activity	Key artifact
Scoping & Authorization	Define what, when, and rules	Signed RoE, target list	Authorization letter
Reconnaissance	Build a picture without touching (much)	Passive OSINT, DNS review	Target profile
Enumeration & Discovery	Map live hosts and services	Host discovery, port/service scan	Asset inventory
Vulnerability Validation	Confirm real, exploitable issues	Manual checks, config review	Evidence log
Analysis & Risk Rating	Turn findings into prioritized risk	CVSS, business context	Risk register
Reporting	Communicate to execs and engineers	Exec summary + technical detail	Final report
Remediation & Retest	Verify fixes hold	Re-test closed items	Retest addendum

1.5 The Lab You Will Build

Reading about assessments teaches vocabulary; running them teaches judgment. Part I closes with a full home-lab build. Every practical exercise in this book runs against machines **you own**, inside an isolated virtual network. The reference lab is:

- `Kali Linux` — assessor workstation.
- `Windows Server` (Domain Controller) + `Windows 11` clients — the `corp.local` Active Directory domain.
- `Ubuntu Server` — Linux services (SSH, NFS, Samba, web).
- `pfSense` — firewall and network segmentation between VLANs.
- Intentionally vulnerable targets (Metasploitable, OWASP BWA) for safe practice.
- Virtualized with `VirtualBox` or `VMware Workstation`; containers via `Docker` where useful.

> **GOLDEN RULE OF THE LAB**
>
> Keep the lab on a **host-only** or **internal** virtual network with no route to your home or corporate LAN. Snapshot every VM once built so you can revert after destructive exercises. Never point lab tooling at an address you cannot prove you own.

1.6 How to Read This Book

Parts I–II build the foundation (process, law, and networking). Parts III–IV are the core craft: reconnaissance and per-service assessment. Part V dives into Active Directory, where most enterprise risk concentrates. Parts VI–X broaden into Linux, vulnerability management, segmentation, wireless, and cloud. Parts XI–XII make you effective on the other side of the table: detection and professional reporting. Appendices give you cheat sheets you will use on real engagements.

1.7 The People Behind an Engagement

A technical assessment is also a human project. Knowing who you are working with — and what each person needs from the engagement — is as important as knowing Nmap flags. The following roles recur on almost every enterprise engagement, and your report ultimately has to serve all of them.

Table 1.3 — Common engagement stakeholders and their needs.

Stakeholder	What they care about	What they need from you
Executive sponsor	Business risk, budget, outcomes	A clear, jargon-free risk story
IT / infrastructure lead	Uptime, remediation effort	Precise, prioritized, actionable fixes
Security team / SOC	Detection coverage, gaps	What each finding looks like in logs
Application / service owners	Their specific systems	Findings scoped to their assets
Compliance / GRC	Framework obligations	Evidence mapped to requirements

Identify these people during scoping and confirm your primary technical point of contact and an emergency contact. When a critical finding appears at 2 a.m. — an exposed database, a passwordless remote-desktop service — you must already know who to call and how.

1.8 A Guided First Engagement (Walkthrough)

To make the lifecycle concrete, here is how a small internal assessment actually unfolds, step by step. Do not worry about the specific tools yet — later chapters cover each in depth. The point is the *shape* of the work and the decisions at each stage.

1. **Kickoff.** You receive signed authorization scoping the internal 10.0.0.0/8 range, a testing window of 09:00–17:00, and an emergency-stop contact. You confirm what is explicitly *out* of scope (e.g., the production payment system) before anything else.
2. **Position.** You are given a network drop and a standard user account on the `corp.local` domain — the same starting point a compromised employee workstation would provide. This is a realistic, common assessment scenario.
3. **Baseline.** You confirm your own IP, gateway, and DNS, and run a small, list-only check to make sure every target you will touch is inside the authorized range. This reconciliation step prevents the single worst mistake in the field: scanning something you were not authorized to.
4. **Discovery.** You perform host discovery to learn what is alive, then service scans to learn what those hosts expose. You now have an asset inventory: the raw material of the assessment.
5. **Enumeration.** For each interesting service you ask focused questions — is SMB signing required? does this LDAP allow anonymous bind? — and you begin enumerating Active Directory with your authorized account.
6. **Validation.** Every candidate weakness is confirmed by hand before it becomes a finding. A scanner label is a lead, not a conclusion.
7. **Analysis.** You step back and look for the *story*: how do the individual weaknesses combine? Often a handful of root causes explains most of the risk.
8. **Reporting and retest.** You write for two audiences, brief them live, and later retest to confirm the fixes actually closed the issues.

> **FIELD NOTE — THE RECONCILIATION HABIT**
>
> Experienced assessors run a harmless, list-only pass (resolve and list targets without probing) before any active scanning, and diff it against the authorized scope. It takes two minutes and is the cheapest insurance you will ever buy against an out-of-scope incident.

Notice what did *not* appear in that walkthrough: no dramatic "break-in," no reckless exploitation.

Professional network assessment is deliberate, authorized, and documentation-driven from the first minute. The excitement is intellectual — piecing together how trust flows through an environment — not theatrical.

1.9 Common Pitfalls for New Assessors

Most early-career mistakes are not technical; they are process failures. Internalize these now and you will avoid the errors that most often damage engagements and reputations:

- **Scanning before confirming scope.** Always reconcile your target list against written authorization first.
- **Trusting tools blindly.** Validate every finding; a scanner is a starting point, not a verdict.
- **Collecting shells instead of insight.** The goal is prioritized, fixable risk — not a trophy wall of access.
- **Ignoring the defender.** If you cannot say how a finding would be detected, your analysis is only half done.
- **Poor evidence discipline.** Capture the command, output, target, and timestamp as you go; reconstructing evidence later is painful and error-prone.

REVIEW QUESTIONS

1. In one sentence, what is the true deliverable of a network penetration test?
2. How does a vulnerability assessment differ from a red-team engagement in question and stealth?
3. Why is copying scanner CVSS scores straight into a report considered a mistake?
4. Name three components of the reference lab and the role each plays.
5. Why is authorization drawn as the gate in front of the entire lifecycle?

HANDS-ON EXERCISES

1. Write a one-paragraph "mission statement" for a fictional internal assessment of a 500-person company.
2. Draw the assessment lifecycle from memory and annotate each phase with one artifact it produces.
3. List five hypotheses (in the style of §1.3) you would ask about a host that only exposes ports 22 and 443.

CHAPTER 2

Rules of Engagement, Authorization, Ethics & Law

LEARNING OBJECTIVES

- Explain why written authorization is the single non-negotiable prerequisite of any test.
- Draft the core sections of a Rules of Engagement (RoE) document.
- Scope an engagement precisely, including exclusions and emergency contacts.
- Apply a professional code of ethics to ambiguous field situations.
- Recognize the major legal frameworks that govern security testing.

There is exactly one activity in this book that is never optional and never delegated: obtaining and verifying written authorization. Skill without authorization is not penetration testing — it is a crime.

2.1 Authorization: The Only Thing That Makes This Legal

The difference between a penetration tester and an intruder is a signed document. Authorization must be explicit, in writing, granted by someone with the authority to grant it, and specific about what may be tested, when, and how. A verbal "sure, go ahead" from a friendly sysadmin is not authorization — that person almost certainly cannot consent on behalf of the organization that owns the assets.

VERIFY THE SIGNER'S AUTHORITY

Confirm that the person signing owns the risk. For third-party-hosted assets (cloud, SaaS, co-located hardware), the client may not have the right to authorize testing at all. Get the hosting provider's authorization too, or exclude those assets.

Table 2.1 — Minimum elements of a valid authorization.

Element	What it establishes	Example
Signatory	Who authorizes the test	CISO / VP of IT with delegated authority
Target scope	Exactly what may be tested	10.20.0.0/16 internal, corp.local domain
Exclusions	What must not be touched	SCADA VLAN, prod payment gateway
Time window	When testing may occur	Weekdays 18:00–06:00, 4-week window
Techniques	Permitted and forbidden methods	No DoS, no destructive exploits, no social engineering
Data handling	How findings/evidence are stored	Encrypted, deleted 30 days post-report

2.2 The Rules of Engagement (RoE)

The RoE operationalizes the authorization. Where the authorization letter says "you may test," the RoE says "here is precisely how." A strong RoE prevents the two failure modes of field work: causing an outage you were not permitted to risk, and being blamed for one you did not cause.

2.2.1 Core sections

- **Scope & exclusions** — CIDR ranges, hostnames, domains, and explicit out-of-scope items.
- **Testing windows** — dates/times, and whether production hours are permitted.

- **Rules on impact** — is exploitation permitted, or validation only? Are DoS conditions forbidden?
- **Emergency contacts** — 24/7 names and numbers for both sides, plus a stop-work procedure.
- **Evidence handling** — where data lives, encryption, retention, and destruction.
- **Reporting cadence** — daily check-ins, critical-finding escalation path.
- **De-confliction** — how the client distinguishes your traffic from a real attacker.

THE "CRITICAL FINDING" CLAUSE

Always agree in advance what happens if you find something catastrophic (e.g., an exposed domain-admin credential or an internet-facing unauthenticated RCE). The RoE should require you to **stop and notify immediately** rather than continue exploiting. This protects the client and you.

COMMON MISTAKE

Beginning work on "day one of the window" before the countersigned RoE is in hand. "It was about to be signed" is not a defense. No signature, no packets.

2.3 Ethics and Professional Conduct

Authorization makes testing legal; ethics makes you trustworthy. Professional bodies (e.g., (ISC)² and EC-Council codes) converge on the same principles: act with integrity, protect client confidentiality, avoid unnecessary harm, stay within scope, and disclose responsibly. In the field these principles become concrete decisions:

- You discover employee personal data during testing — you note its exposure as a finding but do not read, copy, or retain the contents.
- You find a path into an out-of-scope system — you stop, document the boundary crossing, and seek written scope expansion before proceeding.
- A client asks you to test a competitor "just to see" — you decline; you can only test assets the client is authorized to authorize.

2.4 Legal Considerations

Laws vary by jurisdiction, and this section is orientation, not legal advice — always consult counsel. Broadly, unauthorized access to computer systems is criminalized under statutes such as the U.S. Computer Fraud and Abuse Act (CFAA), the UK Computer Misuse Act, and equivalent laws worldwide. Data-protection regimes (e.g., GDPR) add obligations when testing touches personal data. The practical takeaways:

Table 2.2 — Recurring legal concerns in network assessments.

Concern	Practical guidance
Authorization scope	Never exceed the written scope, even accidentally-reachable systems.
Cross-border data	Testing that moves personal data across borders may trigger privacy law.
Third-party assets	Cloud/hosted targets may need the provider's authorization too.
Evidence & privacy	Minimize collection of personal data; store encrypted; destroy on schedule.
Incident overlap	If a real breach is suspected mid-test, pause and notify immediately.

KEEP THE PAPERWORK WITH YOU

On engagements, keep a copy of the signed authorization and RoE accessible. If network defenders or law enforcement question your activity, you must be able to produce proof of authorization instantly.

2.5 Verifying Authorization: A Practical Checklist

Before a single packet leaves your machine, walk this verification checklist. It takes minutes and has saved countless assessors from career-ending mistakes. Treat any "no" as a hard stop until resolved.

1. Is the authorization **in writing** and **countersigned** by both parties?
2. Does the signer have the **authority** to consent for the organization that owns the assets?
3. Does the scope list **exact** ranges, hostnames, and domains — and explicit **exclusions**?
4. Are the **testing windows** and any production-hours rules unambiguous?
5. Are **forbidden techniques** (DoS, destructive exploitation, social engineering) named?
6. Do you have **24/7 emergency contacts** and a written **stop-work** procedure?
7. For any **third-party-hosted** assets, is the provider's authorization included or the asset excluded?
8. Is **evidence handling** (encryption, retention, destruction) defined?

TURN THE CHECKLIST INTO A ONE-PAGE COVER SHEET

Keep a standard authorization cover sheet that captures each item above with the signed date and contacts. Attach it to every engagement folder. When the checklist is a habit, the "about-to-be-signed" temptation disappears.

2.6 Handling Boundary Situations in the Field

Real engagements produce ambiguous moments that the paperwork did not foresee. Professionalism is measured by how you handle them. The following decision guide covers the most common ones:

Table 2.3 — A field decision guide for boundary situations.

Situation	Correct action
You can reach an out-of-scope host	Stop, document the boundary, request written scope change
You find a critical, catastrophic issue	Invoke the critical-finding clause: stop, notify, don't exploit further
You encounter personal/sensitive data	Note exposure as a finding; do not read, copy, or retain contents
You suspect a real, active breach	Pause testing and notify the client immediately
A control blocks you and you could bypass destructively	Do not; note the control and its limits, and consult the RoE

The through-line is simple: when in doubt, **stop and communicate**. No finding is worth exceeding authorization, damaging production, or mishandling sensitive data. Clients remember how you handled the hard moments far longer than they remember your cleverest finding.