

BEST Penetration Testing Foundations



Course syllabus

Course outline for review. Your enrolled course keeps its assigned version.

At a glance

Format	Self-paced text lessons, formative checks, staged practice and evidence reporting
Level	Beginner. No prior penetration testing experience required
Modules	10 (Orientation through Independent Skills Assessment)
You need	A desktop or laptop, a current browser, and space to save text or JSON evidence
Price	\$349 standard course price
Access	6 months, with usage limits
Enroll at	https://best-training.co
Completion time	No reliable estimate yet
Syllabus	Public. Lessons and practice materials require enrollment or an authorized access entitlement

About this course

You begin with the BEST B-CID method (Baseline, Change, Compare, Interpret, Document), then investigate networks and web applications within an authorized scope. Along the way you compare observations, test secure controls and document what the evidence supports.

Practice combines lessons, supplied-record worksheets, local simulations and assigned isolated labs. Availability varies by activity; the practice inventory below lists the status of each one.

Who it is for

- Beginners exploring ethical hacking, penetration testing or web application testing
- Defenders who want to understand how offensive observations inform defensive work

Prerequisites

- You are comfortable opening web pages, managing files and reading short instructions.
- No prior penetration testing experience is needed. Introductory network and browser concepts are taught in the course.
- No paid cloud account, arbitrary scanning target or real customer account is required.
- You use only assigned targets and fictional accounts.

Course outcomes

By the end of the course you will be able to:

1. Define an authorized scope and apply B-CID to an investigation.
2. Distinguish reachability, port state and observed service behavior from assumptions.
3. Interpret requests, sessions and common web trust boundaries using positive and negative controls.
4. Write reproducible evidence notes with limitations, remediation and retest steps.

How the course works

The learning cycle is: learn the concept, see an example, investigate with guidance, repeat with fewer hints, try unfamiliar practice and document the evidence. Save your observations, negative controls, limitations and restoration checks.

Types of practice

- **Formative questions** check understanding. They do not establish practical mastery.
- **Supplied records and simulations** are preparation, not verified live observations.
- **Assigned isolated labs** are real environments allocated to your account.
- **Integrated practice** combines earlier skills.
- **Blind practice** is preparation, not independent demonstration.

Independent assessment

The final module uses separate, unfamiliar materials and review criteria. It excludes AI tutoring, RAG assistance, structured hints and correctness-driven retries, with server-side assistance restrictions. Current preparation does not activate a sitting. Juniper preparation is inactive and ungraded.

A worksheet or saved report does not award course completion, certification or demonstrated skill.

AI-assisted learning

- Use the course AI tutor to clarify concepts, understand errors, review your reasoning, and get hints during lessons and guided practice.

- You remain responsible for checking its answers. AI may provide incorrect or incomplete information.
- During independent assessments, use AI only when the assessment instructions expressly allow it. Do not submit AI-generated work as evidence of independently demonstrated skills.

Privacy and authorized use

- Use only assigned labs or systems you have explicit permission to test.
- Do not submit passwords, API keys, access tokens, personal information, employer/client data, or confidential material. Use sanitized examples.
- Do not use the tutor to attack real targets, steal credentials, evade course safeguards, or generate activity outside the authorized lab scope.

Usage and abuse

- Access is for the enrolled learner only. Account sharing, resale, automated prompting, bulk content extraction, and attempts to bypass usage limits are prohibited.
- Repeated questions, requests for simpler explanations, and accessibility-related support are legitimate learning uses.
- Excessive automated activity or activity that disrupts service may be throttled or temporarily suspended. Learners should receive an explanation and a way to request review; immediate restrictions may be necessary for security incidents.

Equipment and setup

Basics

- Use a desktop or laptop with a current browser and a keyboard for browser inspection and workstation activities.
- Browser practice introduces the built-in developer tools. A proxy is optional, not a starting requirement.
- Text lessons and worksheets can be read on a phone.
- Compatibility with every mobile device or assistive technology is not established.

Workstation command walkthrough

- Uses Linux Bash on an already approved local workstation. Open its Terminal application and select Bash.
- BEST does not provide a browser terminal.
- Do not paste these commands into the browser address bar or Windows PowerShell.
- No installation or elevated privileges are required.
- If you do not have approved Linux Bash access, use the supplied-output rehearsal and ask your instructor or workstation administrator before execution.

Command-boundary and file-boundary fixtures

- Require an approved copy of the supplied application files and Python 3.10 or later. The command-boundary fixture also requires a POSIX shell at `/bin/sh`.

- A public syllabus or browser lesson does not supply this checkout.
- Without the approved files or tools, use the supplied-record rehearsal. Do not substitute arbitrary commands or targets.

Network socket exercises

- Require a separately approved isolated host, with confirmation that it is available and authorized before execution.
- Without one, use supplied records and do not run network probes.

Assigned isolated labs

- Require sign-in, existing course/lab access and completed safety orientation.
- Setup requirements differ by lab. Reading a guide does not allocate or reset a lab.

Module outline

Administrative orientation comes first. BEST B-CID is the first instructional module and is applied throughout practice and reporting. Each module builds on the one before it.

#	Module	Focus	Practice
1	Orientation	Prepare for authorized learning before touching a target	Text/formative
2	BEST B-CID Method	Use B-CID as the method for every investigation	Text/formative
3	Penetration Testing Methodology	Turn an authorized scope into a small, ordered testing plan	Text/formative
4	Network Foundations	Build the addressing and transport vocabulary to reason about connectivity	FND-LAB-13, LOCAL-NETWORK
5	Reconnaissance & Enumeration	Investigate scoped reachability, ports and services without treating guesses as observations	FND-LAB-11
6	Web Application Foundations	Read browser requests and follow fictional login and cookie state	FND-LAB-01, 08, 14
7	Common Web Vulnerabilities	Compare controlled trust-boundary weaknesses with repaired and ambiguous cases	13 activities (see inventory)
8	Evidence & Reporting	Write a finding another reviewer can reproduce and challenge	Text/formative
9	Integrated Guided Pentest	Combine network, web and reporting practice in one fictional engagement	FND-LAB-12, WILLOW-MAPLE, ASSIGNED-ENGAGEMENT
10	Independent Skills	Unfamiliar-transfer and review stage	Separate

#	Module	Focus	Practice
	Assessment		independent materials

Module 1. Orientation

Topics: Learner journey · Authorization and scope · Lab safety · Assessment orientation

Outcomes:

- Identify permitted targets, stop rules and assistance boundaries.
- Explain how to retain evidence without exposing credentials or other learners.

Module 2. BEST B-CID Method

Before this module: Orientation

Topics: Baseline · Change · Compare · Interpret · Document

Outcomes:

- Record a baseline before changing one input.
- Compare and repeat observations, then separate interpretation from documented fact.

Module 3. Penetration Testing Methodology

Before this module: BEST B-CID Method

Topics: NIST SP 800-115 · PTES · MITRE ATT&CK as a reference model

Outcomes:

- Explain the difference between a testing methodology and a reference model.
- Prepare a workstation and evidence plan using fixed local activities.

Module 4. Network Foundations

Before this module: Penetration Testing Methodology

Topics: TCP/IP · IP addressing · Routing · TCP/UDP · Common services and ports · DNS · HTTP/HTTPS · SSH · SMB · Open/closed/filtered

Outcomes:

- Identify an address, subnet, route and service endpoint.
- Explain why TCP, UDP and a missing response require different interpretations.

Practice: FND-LAB-13, LOCAL-NETWORK

Module 5. Reconnaissance & Enumeration

Before this module: Network Foundations

Topics: Host discovery · Port enumeration · Service identification · DNS enumeration · HTTP discovery · Nmap workflows

Outcomes:

- Distinguish open, closed and ambiguous observations and corroborate service identity.
- In campus preparation, separate ticket-approved administrator changes from read-only tester rights and application access.

Practice: FND-LAB-11

Module 6. Web Application Foundations

Before this module: Reconnaissance & Enumeration

Topics: HTTP requests/responses · Methods · Headers · Parameters · Cookies · Sessions · Authentication · Client vs server · HTML/JavaScript basics · Browser DevTools · Proxy concepts

Outcomes:

- Identify method, path, parameters, headers and response evidence.
- Distinguish Set-Cookie from Cookie, preference persistence from authentication, and logout appearance from invalidation.

Practice: FND-LAB-01, FND-LAB-08, FND-LAB-14

Module 7. Common Web Vulnerabilities

Before this module: Web Application Foundations

Topics: SQL injection · Reflected XSS · Stored XSS · Command injection · File inclusion/path behavior · Authentication weaknesses · Session weaknesses · Redirects

Outcomes:

- Investigate query, script, command and file boundaries without equating an error with execution.
- Compare record/role authorization, CSRF, upload and business-logic observations with secure controls, respecting each activity's availability.

Practice: FND-LAB-02 to FND-LAB-07, FND-LAB-09, FND-LAB-10, HARBOR-CATALOG, HARBOR-SEARCH, HARBOR-NOTES, LOCAL-COMMAND, LOCAL-FILE

Module 8. Evidence & Reporting

Before this module: Common Web Vulnerabilities

Topics: Observation vs finding · Evidence vs inference · Reproducibility · Limitations · Technical evidence notes · Severity concepts · Remediation · Technical vs executive reporting

Outcomes:

- Separate observation, inference, impact and uncertainty.

- Record baseline/change/repeat, counter-evidence, remediation and positive/negative retest criteria for technical and nontechnical readers.

Module 9. Integrated Guided Pentest

Before this module: Evidence & Reporting

Topics: Authorized fictional scope · Network discovery · Service analysis · Web investigation · Evidence collection · Structured report

Outcomes:

- Join separately scoped evidence without inventing a causal chain.
- Produce a structured report that preserves provenance, controls, limitations and restoration.

Practice: FND-LAB-12, WILLOW-MAPLE, ASSIGNED-ENGAGEMENT

Module 10. Independent Skills Assessment

Before this module: Integrated Guided Pentest

Topics: Transfer to an unfamiliar scenario · Finding, component/module, evidence · Skills results and recommended remediation

Outcomes:

- Explain independent evidence and the AI/RAG assistance exclusion.
- Prepare to submit reproducible evidence against a versioned rubric, without claiming an award from an ungraded candidate.

Practice inventory

Course lessons and practice materials require enrollment or an authorized access entitlement. Independent assessment is separate and not listed here.

Every activity is offered in **Guided, Semi-guided and Blind preparation** formats plus **Document** (ASSIGNED-ENGAGEMENT: Guided investigation and Document).

Availability key

Code	Meaning
Live	Runs in an isolated environment already assigned to your account. Requires existing access. Reading a guide does not start or allocate a lab.
Guide	Guide available. Live execution is not currently available, so this is not a verified live lab. Use the supplied records or simulation in the guide.
Local	Materials run on your approved workstation. No managed lab is started.

Code	Meaning
Local (host-gated)	Materials available. Socket execution needs a separately authorized isolated host. Without one, use supplied records and do not run network probes.
Records	Supplied-record rehearsal or worksheet. Preparation only, not live execution.

All activities, by module

Module	ID	Activity	Type	Availability
Network Foundations	LOCAL-NETWORK	Network workstation investigation: bounded TCP/UDP comparisons; retain original exports	Local workstation activity	Local (host-gated)
Network Foundations	FND-LAB-13	Campus paths and permissions: diagnose route/firewall faults with administrator tickets; keep tester rights and application permissions separate	Socket-free configuration simulation and supplied records	Local simulation, saved copies and reports available. Real campus network: coming soon
Reconnaissance & Enumeration	FND-LAB-11	Owned network service discovery: distinguish reachability, port state, silence and observed service identity	Supplied-record rehearsal and workstation preparation	Records. Managed network execution: coming soon
Web Application Foundations	FND-LAB-01	How a web request works: compare public products; identify request paths, parameters and responses	Assigned-lab browser guide	Live (use only the Harbor lab assigned to you)
Web Application Foundations	FND-LAB-08	Does logout end the session? Compare login messages and retained-session access after logout	Form-session simulation	Guide
Web Application Foundations	FND-LAB-14	Cookies and login sessions: compare	Supplied-record	Guide

Module	ID	Activity	Type	Availability
		preferences, header direction, login/logout and cookie-flag limitations	rehearsal and browser preparation	
Common Web Vulnerabilities	HARBOR-CATALOG	Catalog query investigation: compare query behavior; document SQL-injection evidence	Existing assigned Harbor lab	Live
Common Web Vulnerabilities	HARBOR-SEARCH	Search reflection investigation: compare reflected browser content and secure-control limits	Existing assigned Harbor lab	Live
Common Web Vulnerabilities	HARBOR-NOTES	Project-note investigation: compare stored note behavior with a safe rendering control	Existing assigned Harbor lab	Live
Common Web Vulnerabilities	FND-LAB-02	Who may read this order? Compare fictional order access with a server ownership control	Assigned-lab scenario	Guide
Common Web Vulnerabilities	FND-LAB-03	Where may a manual reader look? Compare fictional file disclosure with a root-confined reader	Virtual-file simulation	Guide
Common Web Vulnerabilities	FND-LAB-04	Customer versus staff access: compare navigation visibility with enforced role permissions	Form-session simulation	Guide
Common Web Vulnerabilities	FND-LAB-05	What does an error reveal? Compare controlled technical detail with a generic	Fixed-response simulation	Guide

Module	ID	Activity	Type	Availability
		error		
Common Web Vulnerabilities	FND-LAB-06	Who asked to change delivery? Compare unwanted preference updates with token controls and repeated state reads	Supplied-record rehearsal and browser preparation	Guide
Common Web Vulnerabilities	FND-LAB-07	What did the attachment check? Compare file labels, inert text validation and safe retrieval	Non-executable attachment experiment	Guide
Common Web Vulnerabilities	FND-LAB-09	Who calculates the cart total? Compare a display preview with a server-stored fictional receipt	Fictional cart simulation	Guide
Common Web Vulnerabilities	FND-LAB-10	Did an extra command run? Compare a harmless fixed-program marker with literal and unavailable controls	Fixed-program simulation	Guide
Common Web Vulnerabilities	LOCAL-COMMAND	Command investigation: run fixed authored programs in a disposable directory; retain controls and cleanup	Local workstation activity	Local
Common Web Vulnerabilities	LOCAL-FILE	File investigation: compare fictional file reads, disclosure and confined controls	Local workstation activity	Local (no host-file targets)
Integrated Guided Pentest	FND-LAB-12	Returns workflow, fix and retest: connect order ownership and price evidence; compare repairs and restore	Supplied-record rehearsal and workflow simulation	Guide

Module	ID	Activity	Type	Availability
Integrated Guided Pentest	WILLOW-MAPLE	Willow / Maple investigation: combine supplied observations; write a bounded evidence report	Supplied-record worksheet	Records (ungraded)
Integrated Guided Pentest	ASSIGNED-ENGAGEMENT	Assigned guided engagement: investigate only the isolated environment assigned to you	Existing assigned live lab	Live. Existing entry requirements apply; expanded scenarios are not automatically enabled

Career paths and workforce alignment

This course offers an introduction to security work through selected tasks from the National Initiative for Cybersecurity Education (NICE) framework. Coverage is partial and was inferred by the course author from existing materials. It is not a government equivalence or a test of career suitability.

Mapping: foundations-workforce-2 · NICE 2.2.0 · checked 2026-10-04 **Role:** Vulnerability Analysis (PD-WRL-007), category PROTECTION and DEFENSE **Official source:** [NICE v2.2.0 components](#)

Task	Coverage	What the course practices
T1118 Identify vulnerabilities	Practiced in preparation; not independently assessed	Comparing suspected web, command and file weaknesses with secure controls; distinguishing service observations and session behavior from proven vulnerabilities
T1119 Recommend vulnerability remediation strategies	Practiced in preparation; not independently assessed	Explaining a boundary repair; defining positive and negative retest criteria without expanding configuration authority
T1279 Prepare audit reports	Practiced in preparation; not independently assessed	Writing technical and executive accounts with scope, reproducible evidence and limitations

Related practice by task

Task	Activities
T1118	HARBOR-SEARCH, FND-LAB-02, LOCAL-NETWORK, LOCAL-COMMAND, LOCAL-FILE, FND-LAB-14
T1119	LOCAL-COMMAND, LOCAL-FILE, FND-LAB-03, FND-LAB-12, FND-LAB-13
T1279	WILLOW-MAPLE, LOCAL-NETWORK, FND-LAB-13

Remaining gaps

- **T1118:** No accepted enterprise vulnerability program, broad scanner coverage or independent live transfer is established. Supplied records and host-gated network materials do not establish learner execution. Browser session effects need actual browser evidence.
- **T1119:** The practice does not establish independently demonstrated skill or verified live-system performance.
- **T1279:** A fictional penetration-test report is only partial preparation. Compliance audit planning, standards and independent audit acceptance are not covered.

Optional practice questions

Use named activities when available and keep writing in your own notebook or local draft. This public syllabus saves nothing.

T1118

- **LOCAL-NETWORK:** Compare one permitted service over TCP and UDP. What replied, what stayed silent, and which application observation supports the service name? *Keep the claim bounded:* silence does not prove absence and a port number does not prove service identity. Label supplied records if no authorized socket host is available.
- **LOCAL-COMMAND:** Compare the ordinary input, harmless marker and literal-argument control. Which observed effect supports a command-boundary conclusion? *Keep the claim bounded:* error text alone is not execution. Use only the fixed disposable scenario; do not test other hosts or add outbound callbacks.
- **FND-LAB-14:** Compare login, logout and later access. Which record shows the server decision, and what do the cookie flags tell you? *Keep the claim bounded:* separate browser sending rules from application access. Flags alone do not prove that logout invalidated a session.

T1119

- **LOCAL-FILE:** Write a retest that allows the intended manual and denies an outside-root fictional file. What evidence distinguishes disclosure from inclusion? *Keep the claim bounded:* a filename or denied request does not prove disclosed content or executable inclusion. Stay inside the disposable file activity.
- **FND-LAB-13:** For an administrator ticket, predict one narrow route or firewall change, a permitted check, an unrelated denied check and restoration. How would a tester without that

ticket proceed? *Keep the claim bounded*: this is simulation. Do not change real routes or firewalls; reachability does not grant payroll or grades access.

T1279

- **WILLOW-MAPLE**: Choose one supplied observation. Write a technical reproduction and a short executive explanation, then add counter-evidence, an unknown and a retest criterion. *Keep the claim bounded*: mark the packet as supplied records, not your live observations. This supports reporting preparation, not compliance audit competence.

What this course does not claim

- No official DoD 8140 approval, DCWF crosswalk, certification, employment eligibility or full work-role qualification.
- No independent work-role competence is established.
- SOC monitoring, incident response and cloud defensive administration need additional training. Specialist courses and career bundles are planned, not included.

Accessibility and support

- Use the HTML syllabus for headings, links and labeled controls. The PDF export is untagged and has accessibility limitations.
- Compatibility with every browser, PDF reader or assistive technology, and accessibility conformance, have not been established.
- If you hit an access barrier, use the contact link below and describe the page, task, browser or assistive technology. Do not send passwords or private evidence.

Contact: <https://best-training.co>

Price and access

- **Standard course price:** \$349
- Study at your own pace. A reliable completion-time estimate is not yet available.
- Course access lasts 6 months, and usage limits apply. Check the current account terms before purchasing.
- Partner proposals and career bundles are not available offers.

Open protected training: <https://best-training.co>