

BEST Training / Penetration Testing Foundations

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

Syllabus foundations-syllabus-3 / curriculum 2.0-draft.2

Overview foundations-public-1 / labs foundations-public-labs-1

Begin with the BEST B-CID method, then investigate networks and web applications within an authorized scope. 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.

Audience and prerequisites

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

Be comfortable opening web pages, managing files and reading short instructions. No prior penetration testing experience is required. Use only assigned targets and fictional accounts; introductory network and browser concepts are taught in the course.

Course outcomes

Define an authorized scope and apply B-CID to an investigation.

Distinguish reachability, port state and observed service behavior from assumptions.

Interpret requests, sessions and common web trust boundaries using positive and negative controls.

Write reproducible evidence notes with limitations, remediation and retest steps.

Equipment and format

Use a desktop or laptop with a current browser, keyboard and space to save text or JSON evidence. 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. Use a desktop or laptop for browser inspection and workstation activities. Compatibility with every mobile device or assistive technology is not established.

The 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. If you do not have approved Linux Bash access, use the supplied-output rehearsal and ask your instructor or workstation administrator before execution. No installation or elevated privileges are required for this walkthrough.

The separate 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 and confirmation that the host is available and authorized before execution. No paid cloud account, arbitrary scanning target or real customer account is required.

Assigned isolated labs require sign-in, existing course/lab access and completed safety orientation. Availability and setup requirements differ by lab; reading a guide does not allocate or reset a lab.

Self-paced text lessons and formative checks, staged practice and evidence reporting. Supplied records and simulations are preparation, not verified live observations. Independent assessment uses separate unfamiliar materials and excludes AI/RAG assistance.

Module outline

Administrative orientation precedes instruction. BEST B-CID is the first instructional module and is applied throughout practice and reporting.

1. Orientation

Prepare for authorized learning before touching a target.

Before this module: No prior module; begin here.

Topics

Learner journey

Authorization and scope

Lab safety

Assessment orientation

Learning outcomes

Identify permitted targets, stop rules and assistance boundaries.

Explain how to retain evidence without exposing credentials or other learners.

Associated practice: Text/formative or separate independent materials; see policy.

2. BEST B-CID Method

Use BEST B-CID as the first instructional method and carry it through every investigation.

Before this module: Orientation

Topics

Baseline

Change

Compare

Interpret

Document

Learning outcomes

Record a baseline before changing one input.

Compare and repeat observations, then separate interpretation from documented fact.

Associated practice: Text/formative or separate independent materials; see policy.

3. Penetration Testing Methodology

Turn an authorized scope into a small, ordered testing plan.

Before this module: BEST B-CID Method

Topics

NIST SP 800-115

PTES

MITRE ATT&CK as a reference model

Learning outcomes

Explain the difference between a testing methodology and a reference model.

Prepare a workstation and evidence plan using fixed local activities.

Associated practice: Text/formative or separate independent materials; see policy.

4. Network Foundations

Build the addressing and transport vocabulary needed to reason about connectivity.

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

Learning outcomes

Identify an address, subnet, route and service endpoint.

Explain why TCP, UDP and a missing response require different interpretations.

Associated practice: FND-LAB-13, LOCAL-NETWORK

5. Reconnaissance & Enumeration

Investigate scoped reachability, ports and services without treating guesses as observations.

Before this module: Network Foundations

Topics

Host discovery

Port enumeration

Service identification

DNS enumeration

HTTP discovery

Nmap workflows

Learning 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.

Associated practice: FND-LAB-11

6. Web Application Foundations

Read browser requests and follow fictional login and cookie state.

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

Learning outcomes

Identify method, path, parameters, headers and response evidence.

Distinguish Set-Cookie from Cookie, preference persistence from authentication and logout appearance from invalidation.

Associated practice: FND-LAB-01, FND-LAB-08, FND-LAB-14

7. Common Web Vulnerabilities

Compare controlled web trust-boundary weaknesses with repaired and ambiguous cases.

Before this module: Web Application Foundations

Topics

SQL injection

Reflected XSS

Stored XSS

Command injection

File inclusion/path behavior

Authentication weaknesses

Session weaknesses

Redirects

Learning 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.

Associated practice: FND-LAB-02, FND-LAB-03, FND-LAB-04, FND-LAB-05, FND-LAB-06, FND-LAB-07, FND-LAB-09, FND-LAB-10, HARBOR-CATALOG, HARBOR-SEARCH, HARBOR-NOTES, LOCAL-COMMAND, LOCAL-FILE

8. Evidence & Reporting

Write a finding that another reviewer can reproduce and challenge.

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

Learning outcomes

Separate observation, inference, impact and uncertainty.

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

Associated practice: Text/formative or separate independent materials; see policy.

9. Integrated Guided Pentest

Combine network, web and reporting practice within one fictional engagement brief.

Before this module: Evidence & Reporting

Topics

Authorized fictional scope

Network discovery

Service analysis

Web investigation

Evidence collection

Structured report

Learning outcomes

Join separately scoped evidence without inventing a causal chain.

Produce a structured report that preserves provenance, controls, limitations and restoration.

Associated practice: FND-LAB-12, WILLOW-MAPLE, ASSIGNED-ENGAGEMENT

10. Independent Skills Assessment

Understand the separate unfamiliar-transfer and review stage; current preparation does not activate a sitting.

Before this module: Integrated Guided Pentest

Topics

Transfer to an unfamiliar scenario

Finding, component/module, evidence

Skills results and recommended remediation

Learning 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.

Associated practice: Text/formative or separate independent materials; see policy.

Complete practice inventory (independent assessment is separate)

The syllabus is public. Course lessons and practice materials require enrollment or an authorized access entitlement.

FND-LAB-01: How a web request works

Compare public products and identify request paths, parameters and responses.

Module: Web Application Foundations

Type: Assigned-lab browser guide

Availability: Guide available; use only the Harbor lab already assigned to your account. Reading the guide does not start a lab.

Prerequisites: B-CID, HTTP and browser tools

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /practice/harbor/requests

FND-LAB-02: Who may read this order?

Compare fictional order access with a server ownership control.

Module: Common Web Vulnerabilities

Type: Assigned-lab scenario

Availability: Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Prerequisites: Request basics and authentication

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /practice/harbor/orders

FND-LAB-03: Where may a manual reader look?

Compare fictional file disclosure with a root-confined reader.

Module: Common Web Vulnerabilities

Type: Virtual-file simulation

Availability: Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Prerequisites: Request basics and file boundaries

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /practice/harbor/manuals

FND-LAB-04: Customer versus staff access

Compare navigation visibility with enforced role permissions.

Module: Common Web Vulnerabilities

Type: Form-session simulation

Availability: Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Prerequisites: Request basics and authentication

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /practice/harbor/staff

FND-LAB-05: What does an error reveal?

Compare controlled technical detail with a generic error.

Module: Common Web Vulnerabilities

Type: Fixed-response simulation

Availability: Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Prerequisites: Request basics and file boundaries

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /practice/harbor/errors

FND-LAB-06: Who asked to change delivery?

Compare unwanted preference updates with token controls and repeated state reads.

Module: Common Web Vulnerabilities

Type: Supplied-record rehearsal and browser preparation

Availability: Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Prerequisites: Request basics and cookies

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /practice/harbor/csrf-runtime

FND-LAB-07: What did the attachment check?

Compare file labels, inert text validation and safe retrieval.

Module: Common Web Vulnerabilities

Type: Non-executable attachment experiment

Availability: Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Prerequisites: Request basics and browser tools

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /practice/harbor/uploads

FND-LAB-08: Does logout end the session?

Compare login messages and retained-session access after logout.

Module: Web Application Foundations

Type: Form-session simulation

Availability: Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Prerequisites: Request basics and authentication

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /practice/harbor/authentication

FND-LAB-09: Who calculates the cart total?

Compare a display preview with a server-stored fictional receipt.

Module: Common Web Vulnerabilities

Type: Fictional cart simulation

Availability: Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Prerequisites: Request basics

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /practice/harbor/cart

FND-LAB-10: Did an extra command run?

Compare a harmless fixed-program marker with literal and unavailable controls.

Module: Common Web Vulnerabilities

Type: Fixed-program simulation

Availability: Guide available; live execution is not currently available for this

activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Prerequisites: Request basics and command boundaries

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /practice/harbor/diagnostics

FND-LAB-11: Owned network service discovery

Distinguish reachability, port state, silence and observed service identity.

Module: Reconnaissance & Enumeration

Type: Supplied-record rehearsal and workstation preparation

Availability: Supplied-record rehearsal available; managed network execution Coming soon. Interpret the provided records without scanning a target.

Prerequisites: B-CID, addressing and transport

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required:
/course/network-captures#service-discovery-rehearsal

FND-LAB-12: Returns workflow: fix and retest

Connect order ownership and price evidence; compare repairs and restore.

Module: Integrated Guided Pentest

Type: Supplied-record rehearsal and workflow simulation

Availability: Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Prerequisites: Order and cart practice

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /practice/harbor/returns-workflow

FND-LAB-13: Campus paths and permissions

Diagnose route/firewall faults with administrator tickets; keep tester rights and application permissions separate.

Module: Network Foundations

Type: Socket-free configuration simulation and supplied records

Availability: Local simulation, saved copies and reports available; real campus network Coming soon.

Prerequisites: Addressing, routing and introductory service discovery

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /practice/campus-editor

FND-LAB-14: Cookies and login sessions

Compare preferences, header direction, login/logout and cookie-flag limitations.

Module: Web Application Foundations

Type: Supplied-record rehearsal and browser preparation

Availability: Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Prerequisites: HTTP, browser tools and sessions

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /practice/harbor/cookies-browser

HARBOR-CATALOG: Catalog query investigation

Compare query behavior and document SQL-injection evidence.

Module: Common Web Vulnerabilities

Type: Existing assigned Harbor lab

Availability: Assigned-lab practice requires existing access and an assigned Harbor environment. Follow its scope and setup instructions; this page allocates no lab.

Prerequisites: B-CID, HTTP and relevant SQL/XSS lessons

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: </practice/harbor/catalog>

HARBOR-SEARCH: Search reflection investigation

Compare reflected browser content and secure-control limits.

Module: Common Web Vulnerabilities

Type: Existing assigned Harbor lab

Availability: Assigned-lab practice requires existing access and an assigned Harbor environment. Follow its scope and setup instructions; this page allocates no lab.

Prerequisites: B-CID, HTTP and relevant SQL/XSS lessons

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: </practice/harbor/search>

HARBOR-NOTES: Project-note investigation

Compare stored note behavior with a safe rendering control.

Module: Common Web Vulnerabilities

Type: Existing assigned Harbor lab

Availability: Assigned-lab practice requires existing access and an assigned Harbor environment. Follow its scope and setup instructions; this page allocates no lab.

Prerequisites: B-CID, HTTP and relevant SQL/XSS lessons

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: </practice/harbor/notes>

LOCAL-COMMAND: Command investigation

Run fixed authored programs in a disposable directory and retain controls and cleanup.

Module: Common Web Vulnerabilities

Type: Local workstation activity

Availability: Local materials available; no managed lab is started.

Prerequisites: Command boundaries and safe workstation preparation

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /course/command-practice

LOCAL-FILE: File investigation

Compare fictional file reads, disclosure and confined controls.

Module: Common Web Vulnerabilities

Type: Local workstation activity

Availability: Local materials available; no host-file targets or managed lab.

Prerequisites: File boundaries and safe workstation preparation

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /course/file-practice

LOCAL-NETWORK: Network workstation investigation

Prepare bounded TCP/UDP comparisons and retain original exports.

Module: Network Foundations

Type: Local workstation activity

Availability: Materials available; socket execution requires a separately authorized isolated host. Without one, use supplied records and do not run network probes.

Prerequisites: Addressing, transport and approved disposable scope

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /course/network-plan

WILLOW-MAPLE: Willow / Maple investigation

Combine supplied observations and write a bounded evidence report.

Module: Integrated Guided Pentest

Type: Supplied-record worksheet

Availability: Preparation available and ungraded; not live execution.

Prerequisites: Introductory lessons and evidence reporting

Format: Guided, Semi-guided and Blind preparation; Document

Access practice - enrollment required: /course/integrated-rehearsal

ASSIGNED-ENGAGEMENT: Assigned guided engagement

Investigate only the isolated environment assigned to your account.

Module: Integrated Guided Pentest

Type: Existing assigned live lab

Availability: Existing entry requirements apply; no lab allocated by this inventory.
Expanded scenarios are not automatically enabled.

Prerequisites: Existing orientation, diagnostic and guided-entry requirements

Format: Guided investigation and Document

Access practice - enrollment required: /integrated-lab

Practice, assessment and AI assistance

Learn the concept, see an example, investigate with guidance, repeat with fewer hints, try unfamiliar practice and document the evidence. B-CID connects a baseline with a controlled comparison, interpretation and defensible documentation. Blind practice is preparation, not independent demonstration. Save your observations, negative controls, limitations and restoration checks.

Formative questions check understanding; they do not establish practical mastery. Integrated practice combines earlier skills. Independent assessment uses separate unfamiliar materials and review criteria. Juniper preparation is inactive and ungraded. A worksheet or saved report does not award course completion, certification or demonstrated skill.

Contextual help and any configured formative AI review are practice assistance, not an answer validator or skill award. A live provider is not verified by this syllabus; unavailable help must leave the lesson and notes usable. AI tutoring, RAG assistance, structured hints and correctness-driven retries are excluded during independent assessment, with server-side assistance restrictions.

Career paths and workforce alignment

Explore introductory security work through selected tasks from the National Initiative for Cybersecurity Education (NICE) framework. This is partial coverage, not a complete qualification. The course does not confer official Department of Defense 8140 qualification, certification or employment eligibility.

Explore penetration testing and application security testing through evidence comparisons, secure controls and reporting. Use the optional practice questions below to connect course work with three tasks associated with the NICE Vulnerability Analysis role. This is partial preparation inferred by the author from existing artifacts, not a government equivalence or a test of career suitability.

Mapping foundations-workforce-2 / NICE 2.2.0 / checked 2026-10-04

Vulnerability Analysis (PD-WRL-007)

NICE category: PROTECTION and DEFENSE

Official NICE source: https://csrc.nist.gov/csrc/media/Projects/cprt/documents/nice/v2-2-0_nf_components.json

T1118: Identify vulnerabilities

Coverage: Practiced in preparation; Not independently assessed

Course outcome: Compare suspected web, command and file weaknesses with secure controls; distinguish service observations and session behavior from proven vulnerabilities.

Relevant lessons: Apply BEST B-CID; Separate observations, inferences, and findings; Build a bounded SQL injection evidence comparison; Separate TCP and UDP observations; Corroborate service names and version evidence; Bound a command-injection conclusion to its observed effect; Separate path traversal, file disclosure, and inclusion claims; Observe cookie and session lifecycle

Evidence offered: B-CID comparisons, fixed command/file programs and staged session records rehearse narrow claims. The network workbook practices corroboration and ambiguous-response interpretation; an open port or timeout is not itself a

vulnerability. Current practice availability is listed separately.

Remaining gap: 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.

Practice: Search reflection investigation (HARBOR-SEARCH); Existing assigned Harbor lab. Assigned-lab practice requires existing access and an assigned Harbor environment. Follow its scope and setup instructions; this page allocates no lab.

Practice: Who may read this order? (FND-LAB-02); Assigned-lab scenario. Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Practice: Network workstation investigation (LOCAL-NETWORK); Local workstation activity. Materials available; socket execution requires a separately authorized isolated host. Without one, use supplied records and do not run network probes.

Practice: Command investigation (LOCAL-COMMAND); Local workstation activity. Local materials available; no managed lab is started.

Practice: File investigation (LOCAL-FILE); Local workstation activity. Local materials available; no host-file targets or managed lab.

Practice: Cookies and login sessions (FND-LAB-14); Supplied-record rehearsal and browser preparation. Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Optional practice questions: use named activities when available; keep writing in your existing notebook or local draft. This public syllabus saves nothing.

Network workstation investigation (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: Use supplied records if an authorized socket host is unavailable. Label their source; silence does not prove absence and a port number does not prove service identity.

Command investigation (LOCAL-COMMAND): Compare the ordinary input, harmless marker and literal-argument control. Which observed effect supports a command-boundary conclusion?

Keep the claim bounded: Use only the fixed disposable scenario. Error text alone is

not execution; do not test other hosts or add outbound callbacks.

Cookies and login sessions (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. Supplied headers are rehearsal; flags alone do not prove that logout invalidated a session.

T1119: Recommend vulnerability remediation strategies

Coverage: Practiced in preparation; Not independently assessed

Course outcome: Explain a boundary repair and define positive and negative retest criteria without expanding configuration authority.

Relevant lessons: Turn findings into a useful report; Define remediation and retest acceptance criteria; Separate path traversal, file disclosure, and inclusion claims; Read subnets, gateways, and routes

Evidence offered: Fixed command/file controls, product-manual comparisons and the guided integration workflow support repair and retest planning. Campus simulation adds narrow administrator-ticket changes, unrelated-path denial and restoration; network permission remains separate from application ownership.

Remaining gap: This practice does not establish independently demonstrated skill or verified live-system performance.

Practice: Command investigation (LOCAL-COMMAND); Local workstation activity. Local materials available; no managed lab is started.

Practice: File investigation (LOCAL-FILE); Local workstation activity. Local materials available; no host-file targets or managed lab.

Practice: Where may a manual reader look? (FND-LAB-03); Virtual-file simulation. Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Practice: Returns workflow: fix and retest (FND-LAB-12); Supplied-record rehearsal and workflow simulation. Guide available; live execution is not currently available for this activity. Not a verified live lab. Use supplied records or simulation from the guide where provided.

Practice: Campus paths and permissions (FND-LAB-13); Socket-free configuration simulation and supplied records. Local simulation, saved copies and reports available; real campus network Coming soon.

Optional practice questions: use named activities when available; keep writing in your existing notebook or local draft. This public syllabus saves nothing.

File investigation (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: Keep tests inside the disposable file activity. A filename or denied request does not prove disclosed content or executable inclusion.

Campus paths and permissions (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: Use the socket-free model as simulation. Do not change real routes or firewalls; reachability does not grant payroll or grades access.

T1279: Prepare audit reports

Coverage: Practiced in preparation; Not independently assessed

Course outcome: Write technical and executive accounts with scope, reproducible evidence and limitations.

Relevant lessons: Write a reproducible and appropriately redacted evidence note; Write technical and executive accounts of the same finding; Explain severity, confidence, and remediation priority; Rehearse a scoped multi-service network investigation

Evidence offered: Willow/Maple supplied-record reporting, the network evidence workbook and campus simulation reports practice source references, audience-aware claims and recovery of historical writing. Preserve source type, generation, limitations and original evidence when revising.

Remaining gap: A fictional penetration-test report is only partial preparation for audit reporting; compliance audit planning, standards and independent audit acceptance are not covered.

Practice: Willow / Maple investigation (WILLOW-MAPLE); Supplied-record worksheet. Preparation available and ungraded; not live execution.

Practice: Network workstation investigation (LOCAL-NETWORK); Local workstation activity. Materials available; socket execution requires a separately authorized isolated host. Without one, use supplied records and do not run network probes.

Equivalent HTML: <https://hackermartin.com/courses/foundations/syllabus>

Practice: Campus paths and permissions (FND-LAB-13); Socket-free configuration simulation and supplied records. Local simulation, saved copies and reports available; real campus network Coming soon.

Optional practice questions: use named activities when available; keep writing in your existing notebook or local draft. This public syllabus saves nothing.

Willow / Maple investigation (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 or independently assessed mastery.

No official 8140 approval, DCWF crosswalk, certification, employment eligibility or full work-role qualification is claimed. This course does not establish independent work-role competence. SOC monitoring, incident response and cloud defensive administration need additional training; specialist courses and career bundles remain planned, not included delivery.

Accessibility and support

Use the HTML syllabus for headings, links and labeled controls. Compatibility with every browser or assistive technology, and accessibility conformance, have not been established. If you encounter an access barrier, use the contact link below and describe the page, task, browser or assistive technology. Do not send passwords or private evidence.

This untagged PDF has accessibility limitations. Compatibility with every PDF reader or assistive technology is not established. Use the equivalent HTML syllabus for native headings and navigation.

Contact information: <https://hackermartin.com>

Price and access

Study at your own pace. A reliable completion-time estimate is not yet available. This syllabus does not promise an access duration or lab allowance; check the current account terms and available access before purchasing. The displayed standard course price is \$349; partner proposals and career bundles are not available offers.

Open protected training: <https://hackermartin.com/course>

Equivalent HTML syllabus: <https://hackermartin.com/courses/foundations/syllabus>