MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

DETAILED LAB TOOLKIT · 2026 EDITION

OSINT & Recon Toolkit
Authorized Automation Workflows

A scope-first approach to passive discovery, asset normalization, validation, change tracking, evidence, and defensive attack-surface management.

18	10	1
Detailed pages	Workflow modules	Safe pipeline

mnatech.in @mna_tech_academy +91 9216110094

MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

How to use this guide

This resource supports authorized attack-surface inventory and defensive OSINT. It intentionally emphasizes scope, rate limits, provenance, and validation over indiscriminate scanning.

> **Professional-use notice:** Security testing must stay within systems you own or have explicit written authorization to assess. Standards summaries are educational aids, not certification, legal, or audit advice.

Inside this resource

01 **Scope Manifest & Guardrails**
Represent approved roots, exclusions, methods, ownership, and rate limits as data.

02 **Passive Source Planning**
Choose sources based on purpose, terms, freshness, and privacy.

03 **Domain & DNS Inventory**
Normalize names and resolve records without treating every result as owned.

04 **Certificate Transparency Review**
Use public certificate metadata to find candidate names and lifecycle issues.

05 **Repository & Secret Exposure Review**
Inspect organization-owned repositories and public references without collecting secrets.

06 **Web Service Validation**
Confirm approved candidate hosts conservatively and capture minimal metadata.

07 **Port & Service Validation**
Use targeted service checks only where active scanning is authorized.

08 **JavaScript & Endpoint Inventory**
Review client assets for documented routes and accidental disclosures.

09 **Normalization, Deduplication & Diffing**

Turn noisy observations into an owned asset dataset.

10 **Reporting & Remediation Workflow**

Convert exposure data into ownership and closure.

11 **Authorization, Ethics & Lab Boundaries**

Keep every tool and experiment inside systems you own or are explicitly authorized to assess.

12 **Troubleshooting Playbook**

Diagnose failures systematically instead of reinstalling or changing many variables at once.

13 **Documentation & Evidence**

Turn lab work into reproducible notes that another learner can safely follow.

14 **Maintenance & Update Routine**

Keep a working lab trustworthy through controlled updates and backups.

15 **Capstone & Quality Gate**

Demonstrate an end-to-end outcome without relying on copied screenshots.

Scope Manifest & Guardrails

Represent approved roots, exclusions, methods, ownership, and rate limits as data.

Purpose: Represent approved roots, exclusions, methods, ownership, and rate limits as data.

Working checklist

01 · Manifest
Record domains, CIDRs, cloud tenants, repositories, brands, and explicit exclusions.

02 · Enforcement
Make automation refuse targets not derived from approved roots.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Passive Source Planning

Choose sources based on purpose, terms, freshness, and privacy.

Purpose: Choose sources based on purpose, terms, freshness, and privacy.

Working checklist

01 · Sources
Certificate transparency, DNS, registries, owned cloud inventory, and approved search.

02 · Provenance
Store source and observed time for every candidate asset.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Domain & DNS Inventory

Normalize names and resolve records without treating every result as owned.

Purpose: Normalize names and resolve records without treating every result as owned.

Working checklist

01 · Records
Review A/AAAA, CNAME, MX, NS, TXT, and authoritative relationships.

02 · Ownership
Validate through internal inventory or responsible contacts.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Certificate Transparency Review

Use public certificate metadata to find candidate names and lifecycle issues.

Purpose: Use public certificate metadata to find candidate names and lifecycle issues.

Working checklist

01 · Filtering
Normalize wildcards, remove noise, and respect source limits.

02 · Findings
Flag expired certificates, unexpected issuers, and unmanaged candidates for validation.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Repository & Secret Exposure Review

Inspect organization-owned repositories and public references without collecting secrets.

Purpose: Inspect organization-owned repositories and public references without collecting secrets.

Working checklist

01 · Search
Use approved organization/code search and dependency manifests.

02 · Response
Do not validate live credentials; notify owner and rotate through incident process.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Web Service Validation

Confirm approved candidate hosts conservatively and capture minimal metadata.

Purpose: Confirm approved candidate hosts conservatively and capture minimal metadata.

Working checklist

01 · Requests
Use low concurrency, clear user agent, timeouts, and HEAD/GET where appropriate.

02 · Metadata
Record URL, status, title, server hints, certificate, and timestamp.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Port & Service Validation

Use targeted service checks only where active scanning is authorized.

Purpose: Use targeted service checks only where active scanning is authorized.

Working checklist

01 · Plan
Start with explicit hosts and required ports; avoid internet-wide patterns.

02 · Output
Capture tool version, command, source, target, time, and service confidence.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

JavaScript & Endpoint Inventory

Review client assets for documented routes and accidental disclosures.

Purpose: Review client assets for documented routes and accidental disclosures.

Working checklist

01 · Collection
Limit to assets loaded by approved applications.

02 · Analysis
Extract route candidates, source maps, domains, and configuration indicators; validate manually.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Normalization, Deduplication & Diffing

Turn noisy observations into an owned asset dataset.

Purpose: Turn noisy observations into an owned asset dataset.

Working checklist

01 · Schema
Use asset, type, value, source, first/last seen, owner, status, and confidence.

02 · Change
Alert on new, removed, certificate, DNS, and technology changes.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Reporting & Remediation Workflow

Convert exposure data into ownership and closure.

Purpose: Convert exposure data into ownership and closure.

Working checklist

01 · Prioritization
Consider internet exposure, sensitivity, authentication, age, and ownership uncertainty.

02 · Closure
Assign owner, validate disposition, record remediation, and confirm disappearance.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Authorization, Ethics & Lab Boundaries

Keep every tool and experiment inside systems you own or are explicitly authorized to assess.

Purpose: Keep every tool and experiment inside systems you own or are explicitly authorized to assess.

Working checklist

01 · Scope record
Write targets, exclusions, permitted methods, time window, and stop conditions.

02 · Isolation
Use snapshots, host-only/NAT networks, test accounts, and synthetic data.

03 · Rate and impact
Start conservatively, monitor resources, and stop on instability.

04 · Evidence care
Exclude credentials and personal data from screenshots and public repositories.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Troubleshooting Playbook

Diagnose failures systematically instead of reinstalling or changing many variables at once.

Purpose: Diagnose failures systematically instead of reinstalling or changing many variables at once.

Working checklist

01 · Reproduce
Record the smallest repeatable failure and exact timestamp.

02 · Observe
Check process state, logs, ports, DNS, routes, certificates, disk, and memory.

03 · Compare
Separate configuration, dependency, permission, and network causes.

04 · Recover
Return to a known snapshot, then reapply changes individually.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Documentation & Evidence

Turn lab work into reproducible notes that another learner can safely follow.

Purpose: Turn lab work into reproducible notes that another learner can safely follow.

Working checklist

01 · Context
State goal, architecture, versions, assumptions, and boundaries.

02 · Method
Record commands and important configuration without secrets.

03 · Result
Include expected versus observed output and interpretation.

04 · Review
Add remediation, cleanup, references, and lessons learned.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Maintenance & Update Routine

Keep a working lab trustworthy through controlled updates and backups.

Purpose: Keep a working lab trustworthy through controlled updates and backups.

Working checklist

01 · Monthly review
Check disk, snapshots, package state, certificates, integrations, and stale accounts.

02 · Update safely
Snapshot first, review release notes, update in stages, and validate.

03 · Secrets
Rotate lab tokens and remove them from shell history and repositories.

04 · Retirement
Export evidence, revoke credentials, destroy data, and document closure.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact

Capstone & Quality Gate

Demonstrate an end-to-end outcome without relying on copied screenshots.

Purpose: Demonstrate an end-to-end outcome without relying on copied screenshots.

Working checklist

01 · Design
Create a small architecture diagram and measurable goal.

02 · Build
Implement from clean instructions and record deviations.

03 · Test
Validate normal, failure, and recovery paths.

04 · Present
Publish a sanitized report with findings and improvements.

Practical workflow

Stage	Action	Evidence / output
Prepare	Confirm scope, prerequisites, versions, access, and a rollback path.	Written scope and baseline
Execute	Apply the smallest safe change or test, one variable at a time.	Commands, screenshots, or notes
Validate	Compare expected and observed outcomes; investigate uncertainty.	Result with timestamps
Improve	Document lessons, ownership, maintenance, and the next measurable action.	Reusable playbook or portfolio artifact



Keep learning. Keep building.

Use this guide as a working plan: practise, document evidence, review outcomes, and improve the next iteration.

mnatech.in @mna_tech_academy +91 9216110094

© 2026 MNA Tech Academy. Original educational resource. Product names and trademarks belong to their respective owners. Verify standards and product details against official sources before production use.