MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

DETAILED LAB TOOLKIT · 2026 EDITION

Home SOC & SIEM Lab
Wazuh & ELK Blueprint

An architecture-first defensive lab for collecting endpoint and network telemetry, building detections, triaging alerts, and documenting incidents.

18	10	5
Detailed pages	Build modules	Detection cases

mnatech.in @mna_tech_academy +91 9216110094

MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

How to use this guide

Build a small defensive lab that prioritizes telemetry quality and investigation skills. Product requirements change, so confirm current official installation documentation before deployment.

> **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 **SOC Lab Architecture**
Design manager, index/search, dashboard, endpoints, network, and time synchronization.

02 **Safe Network Segmentation**
Prevent simulations from reaching personal, production, or public systems.

03 **Wazuh Deployment Planning**
Prepare supported OS, versions, certificates, storage, and administrator access.

04 **Endpoint Agent Onboarding**
Enroll Windows and Linux endpoints with ownership and telemetry purpose.

05 **Windows Telemetry & Sysmon**
Collect high-value process, network, registry, and file events responsibly.

06 **Linux Telemetry & Audit**
Collect authentication, process, privilege, service, and integrity evidence.

07 **ELK/Kibana Investigation Views**
Design searchable fields, saved queries, dashboards, and time filters.

08 **Detection Engineering Basics**
Write hypotheses, required telemetry, logic, tests, severity, and response guidance.

09 **Alert Triage Playbooks**

Make every alert answer who, what, when, where, how, and what next.

10 **Five Defensive Scenarios**

Practise failed login spikes, suspicious process trees, new persistence, DNS anomalies, and file integrity changes.

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.

SOC Lab Architecture

Design manager, index/search, dashboard, endpoints, network, and time synchronization.

Purpose: Design manager, index/search, dashboard, endpoints, network, and time synchronization.

Working checklist

01 · Sizing
Match components to RAM and storage; begin small and set retention limits.

02 · Diagram
Show data sources, management flows, analyst access, and trust boundaries.

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

Safe Network Segmentation

Prevent simulations from reaching personal, production, or public systems.

Purpose: Prevent simulations from reaching personal, production, or public systems.

Working checklist

01 · Segments
Separate management, monitored endpoints, and simulation targets.

02 · Egress
Restrict outbound traffic and test isolation before generating events.

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

Wazuh Deployment Planning

Prepare supported OS, versions, certificates, storage, and administrator access.

Purpose: Prepare supported OS, versions, certificates, storage, and administrator access.

Working checklist

01 · Official path
Follow current Wazuh quickstart or distributed deployment guidance.

02 · Validation
Confirm service health, dashboard access, TLS, time, and index status.

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

Endpoint Agent Onboarding

Enroll Windows and Linux endpoints with ownership and telemetry purpose.

Purpose: Enroll Windows and Linux endpoints with ownership and telemetry purpose.

Working checklist

01 · Inventory
Record agent ID, host, owner, OS, IP, policy, and last seen.

02 · Quality
Validate authentication, process, file, and system events without overcollection.

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

Windows Telemetry & Sysmon

Collect high-value process, network, registry, and file events responsibly.

Purpose: Collect high-value process, network, registry, and file events responsibly.

Working checklist

01 · Configuration
Use a reviewed Sysmon configuration and understand included/excluded events.

02 · Mapping
Connect event IDs and fields to questions analysts must answer.

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

Linux Telemetry & Audit

Collect authentication, process, privilege, service, and integrity evidence.

Purpose: Collect authentication, process, privilege, service, and integrity evidence.

Working checklist

01 · Sources
Review journald, auth logs, auditd, package, service, and Wazuh FIM.

02 · Noise
Start with critical paths and privileged actions; tune based on measured volume.

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

ELK/Kibana Investigation Views

Design searchable fields, saved queries, dashboards, and time filters.

Purpose: Design searchable fields, saved queries, dashboards, and time filters.

Working checklist

01 · Normalization
Keep host, user, process, source/destination, action, outcome, and timestamp consistent.

02 · Dashboard
Show coverage and investigation context, not only alert counts.

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

Detection Engineering Basics

Write hypotheses, required telemetry, logic, tests, severity, and response guidance.

Purpose: Write hypotheses, required telemetry, logic, tests, severity, and response guidance.

Working checklist

01 · Rule design
Define behavior, data source, condition, exclusions, and known false positives.

02 · Testing
Use benign simulations and compare expected events with actual ingestion.

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

Alert Triage Playbooks

Make every alert answer who, what, when, where, how, and what next.

Purpose: Make every alert answer who, what, when, where, how, and what next.

Working checklist

01 · Enrichment
Add asset criticality, identity context, prevalence, history, and related events.

02 · Disposition
Document true positive, benign positive, false positive, or insufficient data.

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

Five Defensive Scenarios

Practise failed login spikes, suspicious process trees, new persistence, DNS anomalies, and file integrity changes.

Purpose: Practise failed login spikes, suspicious process trees, new persistence, DNS anomalies, and file integrity changes.

Working checklist

01 · Simulation
Generate only controlled, non-destructive events on owned endpoints.

02 · Report
Build timeline, scope, conclusion, containment suggestion, and tuning action.

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.