MNA
TECH ACADEMY
LEARN • PRACTICE • SUCCEED

DETAILED STUDY NOTES · 2026 EDITION

Network Security & Packet Analysis
Study Notes

Layered protocols, packet reasoning, Wireshark filters, DNS, TLS, routing, segmentation, firewalls, detection, and investigation.

18	10	30+
Detailed pages	Protocol modules	Analysis checks

mnatech.in @mna_tech_academy +91 9216110094

MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

How to use this guide

Packet analysis is evidence-driven reasoning. Capture only on networks you own or are authorized to monitor, minimize sensitive data, and record timestamps and capture boundaries.

> **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 **OSI/TCP-IP Mental Models**
Use layers to localize failures without treating either model as a literal implementation map.

02 **Ethernet, ARP & Switching**
Understand local delivery, MAC learning, VLANs, and ARP trust.

03 **IPv4/IPv6 & Routing**
Read addresses, prefixes, TTL/hop limit, fragmentation, and route selection.

04 **TCP State & Reliability**
Analyze handshake, sequence, acknowledgment, windows, retransmissions, and teardown.

05 **UDP & ICMP**
Interpret connectionless traffic and control/error signaling.

06 **DNS Analysis**
Investigate queries, answers, recursion, caching, record types, and anomalies.

07 **TLS & Certificates**
Observe handshake metadata while respecting encrypted application content.

08 **Wireshark Workflow & Filters**
Create focused display filters and preserve the original capture.

09 **Firewalls & Segmentation**

Reason about policy direction, state, zones, identity, and logging.

10 **Packet-Based Investigation**

Build timelines and correlate network evidence with endpoint, identity, and application logs.

11 **Concept Review Questions**

Use explanation-first questions to expose gaps before attempting a lab.

12 **Defensive Lab Exercises**

Practise with synthetic data and isolated environments.

13 **Investigation Worksheet**

Structure technical reasoning so conclusions remain auditable.

14 **Exam & Interview Revision**

Convert notes into concise explanations and practical examples.

15 **Further Study & References**

Prefer official documentation and repeatable practice over unverified shortcuts.

OSI/TCP-IP Mental Models

Use layers to localize failures without treating either model as a literal implementation map.

Purpose: Use layers to localize failures without treating either model as a literal implementation map.

Working checklist

01 · Encapsulation
Relate application data, transport segments, network packets, and link frames.

02 · Troubleshooting
Move layer by layer and distinguish name, route, transport, TLS, and application failures.

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

Ethernet, ARP & Switching

Understand local delivery, MAC learning, VLANs, and ARP trust.

Purpose: Understand local delivery, MAC learning, VLANs, and ARP trust.

Working checklist

01 · Observation
Review broadcasts, ARP request/reply, duplicate addresses, and VLAN context.

02 · Defense
Segmentation, DHCP snooping, dynamic ARP inspection, monitoring, and static critical mappings where appropriate.

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

IPv4/IPv6 & Routing

Read addresses, prefixes, TTL/hop limit, fragmentation, and route selection.

Purpose: Read addresses, prefixes, TTL/hop limit, fragmentation, and route selection.

Working checklist

01 · Path
Record source, destination, gateway, interface, MTU, and asymmetric routes.

02 · Hardening
Filter spoofed ranges, control router advertisements, and maintain IPv6 parity.

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

TCP State & Reliability

Analyze handshake, sequence, acknowledgment, windows, retransmissions, and teardown.

Purpose: Analyze handshake, sequence, acknowledgment, windows, retransmissions, and teardown.

Working checklist

01 · Baseline
Identify client/server, initial handshake, timing, and negotiated options.

02 · Diagnosis
Separate loss, delay, reset, application close, and capture artifacts.

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

UDP & ICMP

Interpret connectionless traffic and control/error signaling.

Purpose: Interpret connectionless traffic and control/error signaling.

Working checklist

01 · UDP
Use application semantics, request/response correlation, and timeout behavior.

02 · ICMP
Understand reachability, TTL exceeded, fragmentation needs, and filtering effects.

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

DNS Analysis

Investigate queries, answers, recursion, caching, record types, and anomalies.

Purpose: Investigate queries, answers, recursion, caching, record types, and anomalies.

Working checklist

01 · Fields
Name, type, response code, answers, TTL, server, latency, and transport.

02 · Detection
Rare domains, long labels, high entropy, unusual volume, NXDOMAIN patterns, and unauthorized resolvers.

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

TLS & Certificates

Observe handshake metadata while respecting encrypted application content.

Purpose: Observe handshake metadata while respecting encrypted application content.

Working checklist

01 · Handshake
Versions, cipher negotiation, SNI, ALPN, certificate chain, and alerts.

02 · Diagnosis
Name mismatch, expiry, trust chain, protocol mismatch, interception, and time errors.

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

Wireshark Workflow & Filters

Create focused display filters and preserve the original capture.

Purpose: Create focused display filters and preserve the original capture.

Working checklist

01 · Workflow
Set time/reference, filter progressively, follow streams, annotate, and export minimal evidence.

02 · Examples
ip.addr, tcp.port, dns, http, tls.handshake, tcp.analysis.retransmission.

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

Firewalls & Segmentation

Reason about policy direction, state, zones, identity, and logging.

Purpose: Reason about policy direction, state, zones, identity, and logging.

Working checklist

01 · Rule review
Source, destination, service, action, order, owner, expiry, and log behavior.

02 · Validation
Test allowed and denied flows from correct segments and confirm logs.

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

Packet-Based Investigation

Build timelines and correlate network evidence with endpoint, identity, and application logs.

Purpose: Build timelines and correlate network evidence with endpoint, identity, and application logs.

Working checklist

01 · Questions
Who communicated, when, how often, using what protocol, and with what outcome?

02 · Limits
Packet absence is not proof of absence; document capture point, loss, encryption, and clock issues.

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

Concept Review Questions

Use explanation-first questions to expose gaps before attempting a lab.

Purpose: Use explanation-first questions to expose gaps before attempting a lab.

Working checklist

01 · Explain
Describe the concept in your own words without tool names.

02 · Differentiate
Compare it with the closest related concept and common confusion.

03 · Predict
State expected behavior before observing traffic or logs.

04 · Defend
Name preventive, detective, and recovery controls.

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

Defensive Lab Exercises

Practise with synthetic data and isolated environments.

Purpose: Practise with synthetic data and isolated environments.

Working checklist

01 · Baseline
Capture normal behavior before introducing a controlled change.

02 · Generate
Create one safe, observable event in the lab.

03 · Detect
Locate evidence across endpoint, application, identity, and network layers.

04 · Improve
Tune a control and show the before/after result.

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

Investigation Worksheet

Structure technical reasoning so conclusions remain auditable.

Purpose: Structure technical reasoning so conclusions remain auditable.

Working checklist

01 · Question
Write the precise question being answered.

02 · Evidence
Record source, timestamp, timezone, integrity, and limitations.

03 · Hypotheses
List multiple plausible explanations before deciding.

04 · Conclusion
Separate facts, inferences, unknowns, and next actions.

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

Exam & Interview Revision

Convert notes into concise explanations and practical examples.

Purpose: Convert notes into concise explanations and practical examples.

Working checklist

01 · One-minute answer
Define the concept, risk, example, and control.

02 · Diagram
Draw the data flow or trust boundary from memory.

03 · Scenario
Explain how you would investigate a realistic event.

04 · Mistakes
List common false assumptions and how to verify them.

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

Further Study & References

Prefer official documentation and repeatable practice over unverified shortcuts.

Purpose: Prefer official documentation and repeatable practice over unverified shortcuts.

Working checklist

01 · Primary sources
Read vendor, standards, protocol, and project documentation.

02 · Version awareness
Record edition, product version, and publication date.

03 · Lab notes
Link each claim to evidence or a trusted reference.

04 · Learning loop
Plan the next topic from observed gaps, not social-media trends.

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.