

Understanding Cybersecurity

Protecting People, Data and Systems in a Connected World

1

What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, programs and data from digital attacks.

2

Why is it Important?

Helps maintain confidentiality, integrity and availability of information and services.

3

Common Threats

Malware, phishing, ransomware, unauthorized access and insider threats.

4

Real-World Impact

Cyberattacks can cause financial loss, operational disruption and damage to reputation.



Key Takeaway: Cybersecurity is essential for a safe, trustworthy and resilient digital world.

Ethical Hacking in Practice



Course:

Ethical Hacking — One-Day Seminar



Focus Areas:

Footprinting • Scanning • Enumeration •
Wireless • IDS/Firewalls • Pentesting • Malware • Sniffing



Presented by:

Priyank Mistry



What You Will Learn Today

From reconnaissance to reporting – a complete ethical-hacking workflow in one day.

1

Footprinting & Scanning

Collect public information, then find hosts, ports, services and operating systems.

2

Enumeration

Extract users, shares, records and configuration from SNMP, SMB, LDAP, SMTP and DNS.

3

Wireless, Mobile & Defenses

WLAN and mobile security, IDS, IPS, firewalls and honeypots.

4

Assessment & Pentesting

Vulnerability assessment, the penetration-testing lifecycle and reporting.

5

Malware, Sniffing & Labs

Safe lab analysis, packet capture and the 10-lab sequence.



Every technique today is taught for authorized laboratory use only.

One-Day Agenda

Fourteen blocks — theory, lab, evidence, remediation.



1 Footprinting & Reconnaissance

2 Network Ranges & Active Hosts

3 Port Scanning

4 OS Fingerprinting

5 Attack Surface Mapping

6 Enumeration

7 Wireless & Mobile Security

8 IDS, IPS, Firewalls & Honeypots

9 Vulnerability Assessment

10 Penetration Testing

11 System Hacking & Malware Concepts

12 Network Sniffing & Traffic Analysis

13 Practical Tools & Labs

14 Recap, Quiz & Q&A



Theory → Lab → Evidence → Remediation: the rhythm of every session.

SAFETY FIRST

The Authorized-Lab Rule



Run scanning, enumeration, wireless testing, sniffing, malware analysis or system-hacking exercises only against systems, networks, files and wireless equipment that you own or have explicit permission to test.



Isolated VMs

Use host-only or isolated NAT networks.



Simulated targets

Metasploitable, OWASP Juice Shop or purpose-built labs.



Explicit permission

No authorization means no testing.



Ethical hacking is only ethical when it is authorized.

SECTION 1

Footprinting & Reconnaissance

Collecting information about an authorized target before active testing.

1

Passive vs Active Reconnaissance

Public sources versus direct interaction.

2

Footprinting Data Categories

Organization, DNS, network, technology, people, exposure.

3

Footprinting Workflow

Six steps from scope to attack-surface inventory.

4

Lab: Recon Tools

dig, whois and traceroute on a lab domain.



Good reconnaissance minimizes unnecessary interaction with the target.

Passive vs Active Reconnaissance

Passive

NO DIRECT PROBING

Uses information already available without directly probing the target.



Examples:

- ✓ WHOIS/RDAP
- ✓ DNS records
- ✓ Search engines
- ✓ Certificate transparency
- ✓ Public documentation

Active

CAN BE LOGGED OR DETECTED

Interacts with target-controlled infrastructure and can be logged or detected.



Examples:

- ✓ DNS queries
- ✓ Traceroute
- ✓ Service discovery
- ✓ Host discovery
- ✓ Controlled banner collection



Collect passive intelligence first — go active only when authorized and necessary.

What Footprinting Collects



Organization

Legal name, subsidiaries, domains, business units, public contacts, geographic presence.



Domain / DNS

Name servers, MX and TXT records, SPF/DKIM/DMARC indicators, subdomains, DNSSEC status.



Network

Public IP ranges, ASN ownership, routing information, exposed gateways, hosting providers.



Technology

Web-server banners, certificate metadata, software families, cloud/SaaS providers.



People / Process

Public roles, contact formats, job postings, security and compliance information.



Physical / External

Public facilities, remote-access portals, wireless references, third-party integrations.



Every public detail is a clue — defenders should know what they expose.

The Footprinting Workflow

1

Define scope

Domains, IP ranges, subsidiaries, cloud assets, applications and exclusions.



2

Collect passively

Gather passive intelligence first.



3

Correlate

Link names, domains, IPs, certificates, DNS data and organizational relationships.



4

Validate

Perform only authorized active checks needed to confirm findings.



5

Record

Source, timestamp, confidence and ownership for every finding.



6

Build inventory

Turn validated assets into an attack-surface inventory.



Footprinting ends with an inventory — not with an attack.

Lab: Footprinting Tools

Legacy Tool	Modern Alternative	Safe Practical
 3D Traceroute	traceroute / tracert / mtr	Trace an owned lab server; record hops and latency
 Alchemy Eye	Uptime Kuma, Zabbix, native monitoring	Monitor a lab VM; observe availability events
 DNS Tools	dig, nslookup, host	Query A, AAAA, MX, NS and TXT for a lab domain
 Network Solutions WHOIS	RDAP / WHOIS services	Use public registration data as a recon source

EXAMPLE COMMANDS

```
$ dig example.lab A
$ dig example.lab MX
$ dig example.lab NS
$ whois <authorized-domain>
$ traceroute <authorized-lab-host>
```



Outcome: asset table with domain, IP, DNS records, routing observations and evidence source.
Mark each item: **verified** • **inferred** • **unverified**.



Every finding needs a source, a timestamp and a confidence level.

Identifying Network Ranges

Which address space is in scope — and which hosts respond?

1

CIDR notation

Network address, prefix length, usable host space and subnet boundaries.



2

ASN & route information

Identifies organization-associated public prefixes; cloud and CDN ownership can complicate attribution.



3

Host discovery

ICMP echo, TCP-based probes, ARP on local networks and controlled service probes.



An allocated address is not a reachable host — and a reachable host is not a service.

Host Discovery: False Negatives & False Positives

False negatives

Firewalls may block ICMP.
A non-responsive host is not necessarily inactive.



False positives

Load balancers, anycast services, NAT and shared hosting can make one IP represent multiple services.



Treat discovery results as evidence, not proof.

Lab: Host Discovery

EXAMPLE COMMAND

```
$ nmap -sn 192.168.56.0/24
# Use only on an isolated lab subnet you own.
```

Legacy Tool	Modern Alternative	Learning Objective
 Advanced Port Scanner	Nmap, RustScan (where appropriate)	Host and port discovery
 Colasoft Ping Tool	ping, fping, native monitoring	ICMP reachability, latency and packet loss



Student task

Compare discovered hosts with the VMs you know are running.



Compare scan results with what you know is running — that is how you learn.

Port Scanning Concepts

Finding transport-layer endpoints that may accept connections.

Scan Concept	Purpose	Interpretation
 TCP connect	Establish a full TCP connection.	Useful when raw-packet privileges are unavailable; more visible in logs.
 SYN scan	Probe TCP state without completing the application connection.	Common discovery technique; requires appropriate privileges.
 UDP scan	Identify UDP services.	Slower and harder to interpret; many UDP services do not respond predictably.
 Service/version detection	Identify application protocols and versions.	Builds a technology inventory and helps correlate with vulnerabilities.



Different scans trade visibility, speed and certainty.

Scan Progressively

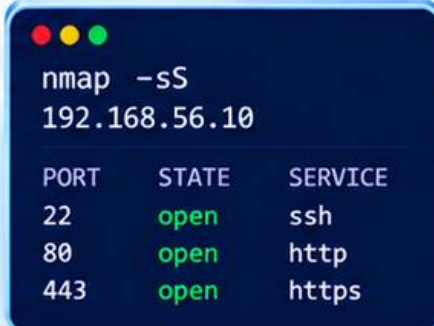
1 Host discovery

Identify which hosts are alive and reachable.



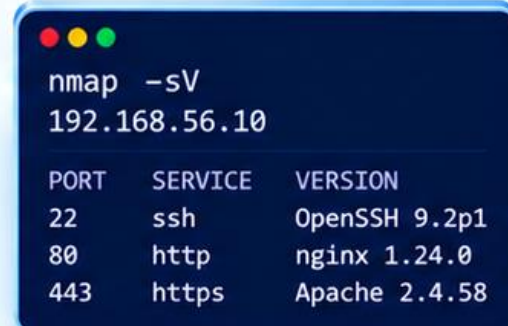
2 Port scan

Identify open ports on discovered hosts.



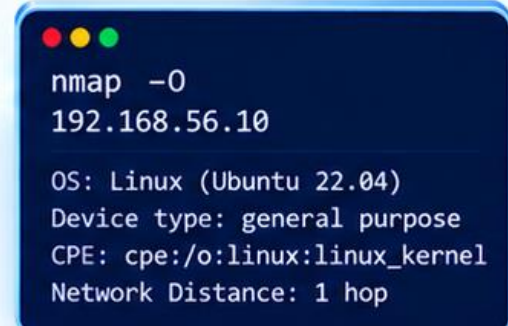
3 Service / version detection

Identify application protocols and versions.



4 OS detection

Estimate the operating system and device type.



A port number alone does not prove what software is running.



Interpret scan results together with service/version detection and application context.



Hosts → ports → services → OS: build the picture step by step.

Lab: Port & Service Scanning

EXAMPLE COMMANDS

```
$ nmap -sS --top-ports 100 192.168.56.10
$ nmap -sS -sV --top-ports 100 192.168.56.10
# Lab-only example.
```



Record

Open ports, services and versions.



Compare

Results against the known services on the target VM.



Note

TCP connect is more visible in logs than SYN scanning.



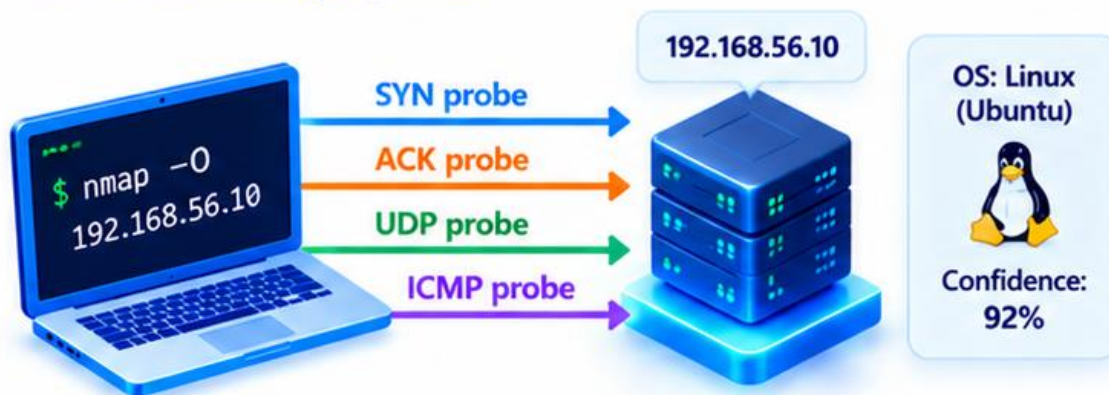
Scan only the isolated lab target you own.

Active vs Passive OS Fingerprinting

Estimating the operating-system family from network-stack behavior.

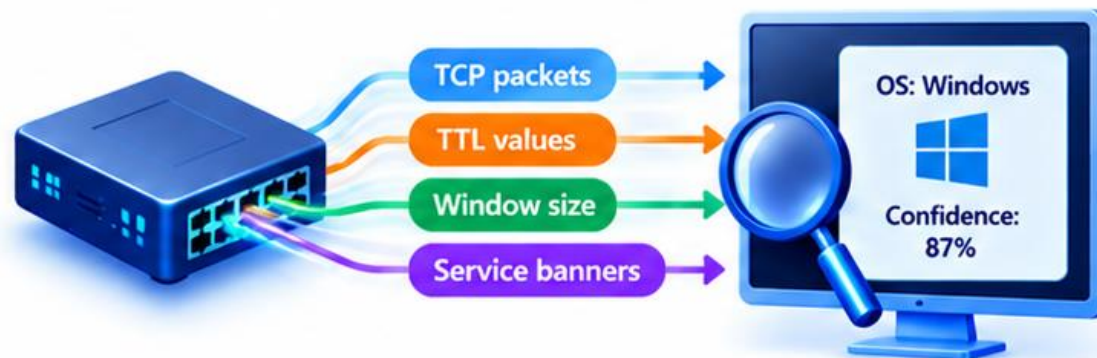
Active fingerprinting

Sends probes and compares responses with known fingerprints.



Passive fingerprinting

Infers characteristics from observed traffic without actively probing.



Clues:



TCP/IP behavior



response patterns



service evidence



A fingerprint is an estimate — never absolute proof.

Attack Surface Mapping

Turning raw reconnaissance into an asset graph.



A useful map connects domains, subdomains, IPs, ports, services, applications, identities, cloud resources, third parties and trust relationships.

External assets

Domains, public IPs, VPN portals, mail gateways, web applications, APIs, cloud endpoints.



Internal assets

Servers, workstations, network devices, directory services, file shares, printers, IoT/OT devices.



You cannot defend — or test — what you have not mapped.

Trust Paths

How access flows between assets.

1

Remote Access Path

From external access to internal applications.



2

User to File Access

From an endpoint to internal data.



3

Application Data Path

From an application to its backend data.



Trust relationships reveal how one weakness can reach another asset.

Exposure Scoring and Evidence



Keep evidence



Screenshots, command output, timestamps and source references — for reproducibility.



Prioritize by exposure — and keep evidence you can reproduce.

SECTION 6

Enumeration

Learning structured information from the services you discovered.

1

Scanning vs Enumeration

Finding services versus extracting information.



2

SNMP, NetBIOS/SMB & LDAP

Risks and countermeasures.



3

SMTP & DNS

Mail and name-service exposure.



4

Enumeration Lab Objectives

Safe checks in a test environment.



Enumeration is more targeted than scanning.

Scanning vs Enumeration

Scanning

Discovers hosts, ports and services.



Enumeration

After a service is found, the tester learns structured information from it: users, groups, hostnames, shares, directory objects, mail configuration or DNS data.



Scanning asks what is open — enumeration asks what it reveals.

Enumeration: SNMP, NetBIOS/SMB, LDAP

Protocol	Typical Information	Security Concern	Defensive Control
 SNMP	System name, interfaces, counters, device information (depends on MIB/access).	 Weak community strings or excessive read access.	 SNMPv3, strong authentication/privacy, ACLs, disable unused SNMP.
 NetBIOS/SMB	Hostnames, workgroup/domain context, shares and related metadata.	 Information disclosure and excessive share exposure.	 Disable legacy protocols, restrict SMB, least privilege, segmentation.
 LDAP	Directory structure, users/groups and attributes where access permits.	 Anonymous or over-permissive queries can disclose directory data.	 Require authenticated access, minimize attributes, ACLs, signing/channel binding where applicable.



Every protocol that answers questions needs an access policy.

Enumeration: SMTP and DNS

Protocol	Typical Information	Security Concern	Defensive Control
 SMTP	Mail server identity, accepted domains, configuration, sometimes user-validation behavior.	 User enumeration and mail infrastructure disclosure.	 Disable unnecessary information disclosure, rate-limit, secure relay configuration.
 DNS	A/AAAA, MX, NS, TXT, CNAME and other records; sometimes zone data.	 Subdomain discovery, information leakage, misconfiguration.	 Restrict zone transfers, review records, DNSSEC where appropriate, monitor unusual queries.



Restrict what each service tells an anonymous visitor.

Lab: Protocol Enumeration Objectives

SNMP



Is it enabled? Is access appropriately restricted?

NetBIOS/SMB



Identify host and share exposure; confirm least privilege.

LDAP



Query only a test directory; compare unauthenticated vs authenticated visibility.

SMTP



Inspect server identity, accepted domains and relay policy — without sending unsolicited mail.

DNS



Inspect records; verify unauthorized zone transfer is blocked.



Default Password List

— audit a lab device you own against vendor documentation.
Never test credentials against third parties.



Test only what you own — and fix what you find.

SECTION 7

Wireless & Mobile Security

Radio, authentication, encryption, configuration and device controls.

1

802.11 Fundamentals

APs, stations, SSID, BSSID, channels.



2

WEP to WPA3 & 802.1X

Security generations and enterprise authentication.



3

Enterprise WLAN & Segmentation

Components and network separation.



4

Mobile Security

Android and iOS models, assessment areas, controls.



5

WLAN Attack Classes

Conceptual view with defensive indicators.



CEH v13 treats wireless and mobile platforms as dedicated areas.

802.11 Fundamentals

Access points & stations



The AP provides the network; stations are the client devices.

SSID & BSSID



Network name and the access point's identifier.

Channels



The radio frequencies a WLAN uses.

Association & authentication



How a station joins the network.



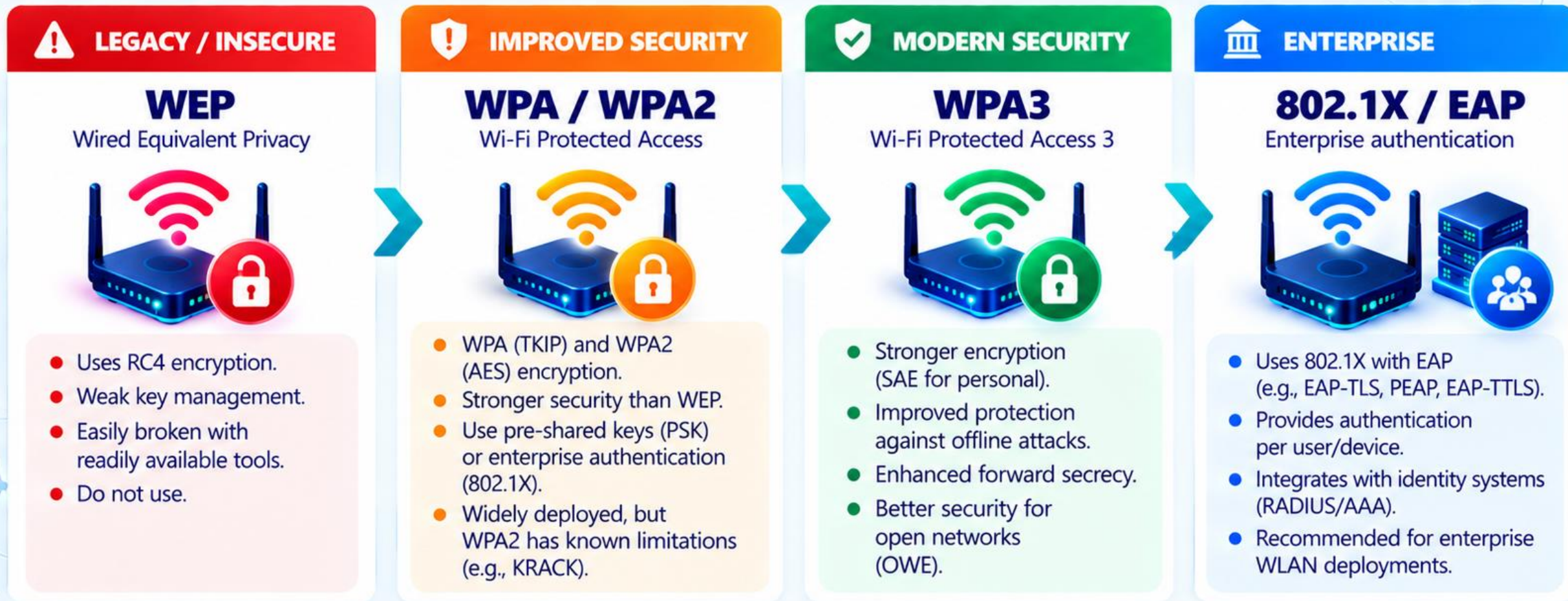
Management frames and client behavior can expose operational metadata even when payloads are encrypted.



Encrypted payloads still leave operational traces.



From WEP to WPA3



Legacy encryption is a finding, not a feature.

Enterprise WLAN Components & Segmentation

Components



AP / controller

Access points and centralized management (controller).



RADIUS / AAA

Authentication, authorization and accounting.



Certificates

For secure 802.1X/EAP authentication.



Identity provider

e.g., Active Directory, Azure AD, LDAP, etc.



Endpoint posture controls

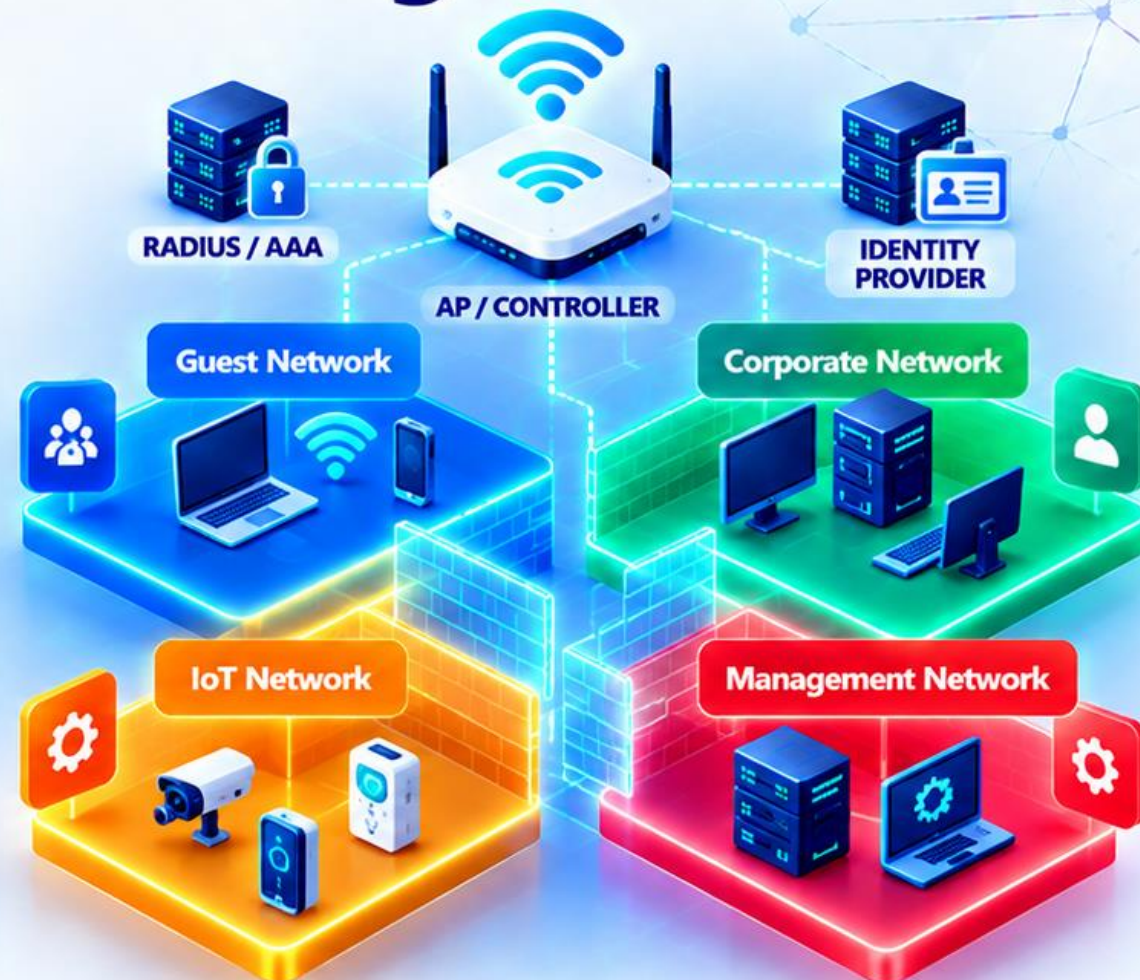
Device health checks and compliance before access.

Segmentation



Guest, corporate, IoT and management networks should not share unnecessary trust.

- ✓ Separate network segments (VLANs/subnets).
- ✓ Restrict access between segments.
- ✓ Allow only required services and traffic.



Separate networks so one weak zone cannot reach the rest.

Mobile Security Domains

Operating system



Android and iOS have different architecture, sandboxing and security controls.

Application sandboxing



Apps run in isolated environments with limited access to system resources.

Permissions



Controlled access to sensitive data, hardware and platform features.

Secure boot



Verifies system integrity and prevents unauthorized software from loading.

Key storage



Uses secure hardware (e.g., Keychain, Keystore, TPM/TEE) to protect cryptographic keys.

Encryption



Device, app and data encryption protect information at rest and in transit.

MDM / UEM



Centralized device management, policy enforcement and compliance controls.

Network security



Secure connectivity (VPN, TLS), certificate validation and protection against rogue networks.



Android and iOS use different security models; testing must account for OS version and device-management state.



Know the platform before you assess the app.



Mobile Assessment Areas & Enterprise Controls

Common assessment areas



Excessive permissions

Apps request more permissions than required.



Insecure storage

Sensitive data stored without encryption or proper protection.



Weak authentication

Weak or missing authentication mechanisms.



Insecure transport

Data transmitted without proper encryption.



Outdated OS and apps

Known vulnerabilities in older versions.



Exposed debug interfaces

Debugging enabled or unnecessary interfaces exposed.

Enterprise controls



Device enrollment

Register devices with MDM/UEM before access.



Policy enforcement

Enforce security policies and compliance settings.



Certificate-based access

Use certificates for Wi-Fi, VPN and enterprise apps.



Remote wipe

Ability to remotely wipe lost or stolen devices.



Application allowlisting

Allow only approved and trusted applications.



Threat detection

Monitor for malware, risky behavior and policy violations.



Every weakness found should map to a control that closes it.

WLAN Attack Classes — Know and Detect

Rogue / evil-twin AP



Impersonates legitimate wireless infrastructure to attract clients.

Deauthentication / disruption



Abuses management behavior to interrupt connectivity.

Weak-credential attacks



Target weak pre-shared keys or identity credentials.

Legacy encryption attacks



Weaknesses in obsolete protocols such as WEP.

Misconfiguration attacks



Weak isolation, insecure management interfaces, exposed services.



Safe lab: use a dedicated AP or virtual WLAN with a test SSID and test devices. Do not test public, neighbor, campus, office or hotel Wi-Fi without written authorization.



Understand the attack class and its defensive indicators — never test networks you do not own.

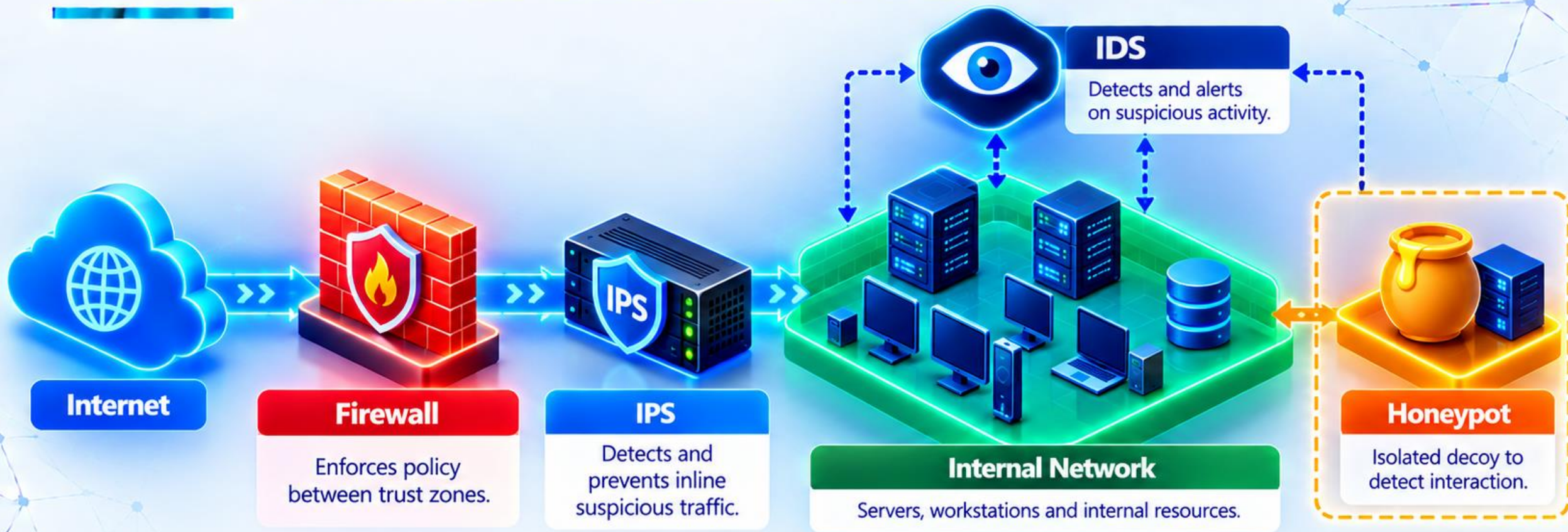
IDS, IPS, Firewalls and Honeypots

Control	Primary Role	Typical Visibility	Limitation
 IDS	Detect and alert on suspicious activity.	Network/host events, signatures, anomalies.	Detection does not necessarily block traffic.
 IPS	Detect and actively prevent suspicious traffic.	Inline network activity and policy violations.	False positives can disrupt legitimate traffic.
 Firewall	Enforce traffic policy between trust zones.	Connections, ports, protocols, identities depending on platform.	Cannot replace endpoint, application or identity security.
 Honeypot	Create monitored decoy assets to detect interaction.	Connection attempts and attacker behavior.	Must be isolated so it cannot become a pivot.



No single control is enough — each has a role and a limit.

Where Each Control Fits



Firewalls enforce, IPS prevents, IDS alerts, honeypots watch.

Lab 8: Detection and Logging Concepts

IDS



Alerts on suspicious activity; it does not necessarily block.

IPS



Prevents suspicious traffic; false positives can disrupt legitimate traffic.

Firewall



Enforces policy but cannot replace endpoint, application or identity security.

Honeypot



Logs connection attempts; keep it isolated.



Student question:

Which control would alert you? Which would block?
Which would only record?



Logging is what turns an event into evidence.

SECTION 9

Vulnerability Assessment

What weaknesses are present — and how serious are they?

1



Audit vs VA vs Pentest

Three activities, three questions.

2



Nessus Lab Workflow

Seven steps from target to retest.

3



Findings & Validation

Severity, false positives, remediation.



A vulnerability assessment is broad; a penetration test is deep.

Security Audit vs Vulnerability Assessment vs Penetration Test

Activity	Primary Question	Output	Typical Depth
 Security audit	Are controls/policies implemented and evidenced?	Compliance/control findings.	Control and evidence focused.
 Vulnerability assessment	What weaknesses are present?	Vulnerability inventory and risk prioritization.	Broad discovery; limited validation.
 Penetration test	Can weaknesses be chained to produce real impact?	Validated attack paths, evidence and remediation.	Deep, controlled validation.



Same goal — better security — three different questions.

Nessus Lab Workflow

**AUTHORIZED LAB ONLY**

Scan → validate → fix → retest.

Findings, Validation and Tools

Group by severity



Organize results by severity and affected service.

Validate manually



Scanners report possibilities; confirm a sample before reporting.

Record false positives



Document them with remediation recommendations.

Tools



Nessus Essentials



OpenVAS/
Greenbone

Nessus Essentials where eligible · OpenVAS/ Greenbone.



A scanner reports possibilities — validation turns them into findings.

Penetration Testing

Controlled testing that shows whether weaknesses lead to real impact.

1



Types of Penetration Testing

By knowledge, position and technology.

2



The Penetration-Testing Roadmap

Eight phases from authorization to retest.

3



Rules of Engagement & Safety

Least disruption, cleanup, reporting.



Penetration testing is authorized, scoped and controlled.

Types of Penetration Testing

By knowledge



Black box

Limited information, approximating an external attacker.



Gray box

Partial knowledge or credentials.



White box

Extensive architecture, credentials, code or documentation.

By position



External

Internet-facing attack surface.



Internal

Assumes internal network access or a compromised endpoint.

By technology



Web

Web applications and portals.



API

Application programming interfaces.



Mobile

Mobile applications (iOS/Android).



Wireless

Wireless networks and infrastructure.



Network

Network infrastructure and services.



Cloud

Cloud environments and services.

Scoped by technology or attack surface.



The type of test is defined by what the tester knows and where they start.

The Penetration-Testing Roadmap



Every test starts with authorization and ends with a report.

Rules of Engagement and Safety



Pre-engagement



Authorization, scope, contacts, rules of engagement, testing window and safety constraints.



Controlled exploitation



Use the least disruptive method possible.



Post-exploitation validation



Show what access or exposure is possible — without unnecessary persistence or damage.



Cleanup & reporting



Remove artifacts, restore changes; report evidence, risk, business impact, remediation and retest plan.

RULES OF ENGAGEMENT

- ✓ Authorized
- ✓ Scoped
- ✓ Controlled
- ✓ Safe
- ✓ Documented
- ✓ Cleaned up
- ✓ Reported



Least disruption, clear evidence, full cleanup.

System Hacking & Malware Concepts

Studied through safe simulations in isolated virtual machines.

1

Safe System-Hacking Simulation



Benign tools replace real surveillance utilities.

2

Trojans & Backdoors — Defensive Lab



Persistence inventory and detection.

3

Malware Analysis Workflow



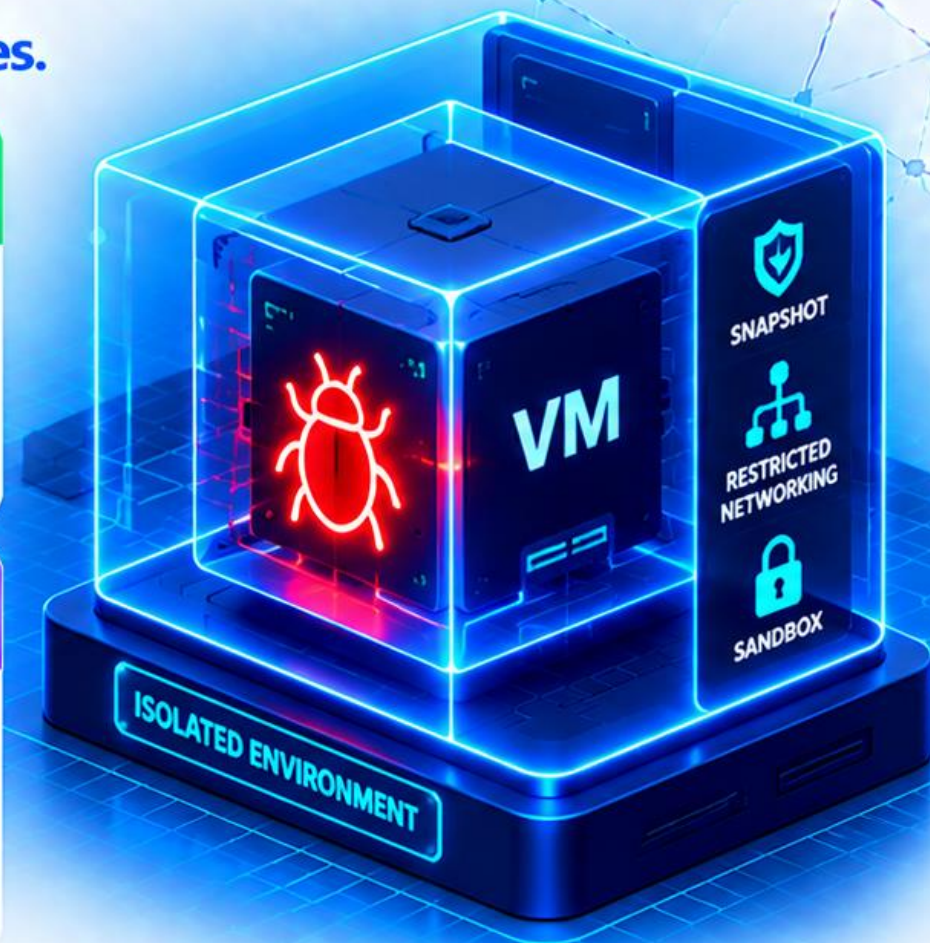
Sandboxing, snapshots and restricted networking.

4

Observation Checklist



What to record during analysis.



Understand the behavior — never deploy it on real users.



System Hacking — Safe Simulation

Do not deploy spyware or remote-access tooling on real users' systems.

Requested Tool	Concept	Safe Lab Replacement	What to Document
 Actual Spy	Surveillance/ monitoring risk	 Benign process- monitoring or Windows event-log exercise	 Indicators, permissions, detection, remediation
 Alchemy Remote Executor	Remote administration / command execution	 PowerShell Remoting or SSH between two lab VMs	 Authentication, authorization, logs, network controls
 Armor Tool	System-security tooling	 Modern endpoint- hardening or configuration-audit tool	 Configuration baseline and deviations
 F-Secure BlackLight	Rootkit/stealth detection	 Modern endpoint/ rootkit detection in a disposable VM	 Detection artifacts and response steps



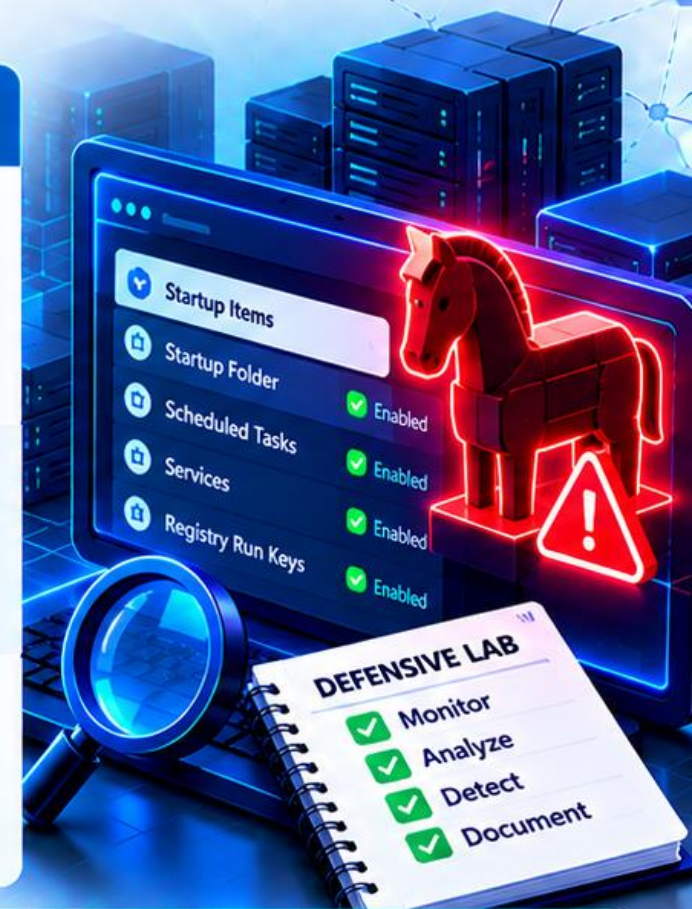
Reproduce the concept safely — document detection and remediation.



Trojans and Backdoors — Defensive Lab

Do not create or deploy real backdoors.

Requested Tool	Concept	Safe Practical	Modern Alternative
 Absolute Startup Manager	Startup/persistence inventory	 Inspect startup locations and scheduled tasks in a disposable VM.	 Autoruns, Task Scheduler, Windows Event Viewer.
 NetWrix Services Monitor	Service monitoring	 Create and monitor benign test service changes in a lab.	 Windows Services, Sysmon, Wazuh.
 StartEd Lite	Startup configuration	 Compare baseline vs modified startup entries.	 Autoruns / native Windows tools.



Persistence leaves traces — defenders learn to find them.



Malware Analysis Workflow



Use disposable VMs, snapshots, restricted networking, and known sample repositories only where legally and safely permitted. **Goal:** understand behavior, indicators of compromise, persistence, network activity and detection.

Legacy Tool	Safe Practical	Modern Alternative
 Anubis Analyzing Unknown Binaries	 Study sandbox reports or analyze benign samples in a controlled environment.	 CAPEv2/Cuckoo-style sandboxes, vendor sandboxes.
 Filterbit	 Use file-analysis/reputation services for non-sensitive test files.	 VirusTotal or enterprise sandboxing, subject to data-sharing policy.
 Sunbelt CWSandbox	 Reproduce historical concepts in a current isolated sandbox.	 CAPEv2/Cuckoo-style systems.
 ThreatExpert	 Study the historical analysis workflow.	 Modern sandbox/EDR telemetry.



Isolate first, observe second, report third.

Malware-Analysis Observation Checklist

1 Process tree



Parent/child relationships.

2 File activity



Creation, modification, deletion.

3 Registry & configuration



Changes and persistence locations.

4 Network



DNS queries and attempted connections.

5 Artifacts



Mutexes, named pipes, services, scheduled tasks.

6 Static metadata



Hash values and file properties.

7 IOCs & detection



Indicators of compromise and recommended detection rules.



Observations become indicators — indicators become detections.

Network Sniffing & Traffic Analysis

Capturing and reading traffic on an authorized lab network.

1



Sniffing & Encryption

What can and cannot be observed.

2



Capture Tools

tcpdump, Wireshark and monitoring tools.

3



Packet-Analysis Objectives

Handshakes, DNS, HTTP, DHCP and anomalies.



Capture only on interfaces you own or are authorized to monitor.



What a Packet Capture Shows



Visible



Source and destination IP addresses and ports.



Protocols and endpoints.



Cleartext metadata.



Reduced by encryption



Encrypted protocols reduce payload visibility.



HTTPS (TLS / SSL)



SSH



VPN



Encryption changes what an observer can see.

Lab: Packet Capture Tools

Legacy Tool	Safe Practical	Modern Alternative
 Colasoft Capsa Network Analyzer	 Capture traffic between lab VMs; identify protocols and endpoints.	 Wireshark, tcpdump
 EffeTech HTTP Sniffer	 Inspect HTTP traffic from a local test web application.	 Wireshark, browser DevTools, mitmproxy in a lab.
 Packet Sniffer	 Capture only on your isolated lab interface.	 Wireshark / tcpdump
 PRTG Network Monitor	 Monitor bandwidth, latency and service availability.	 PRTG, Zabbix, Grafana/Prometheus



```
$ sudo tcpdump -i eth0 -nn -c 100
# Capture only on an authorized lab interface.
# Open the resulting capture in Wireshark for protocol analysis.
```



Capture in the lab, analyze in Wireshark.

Packet-Analysis Objectives

TCP HANDSHAKE

- 1 SYN (Client → Server)
- 2 SYN, ACK (Server → Client)
- 3 ACK (Client → Server)

1



Identify

Source and destination IP addresses and ports.

2



Recognize

TCP handshake, DNS, HTTP(S), DHCP and common management traffic.

3



Distinguish

Normal periodic traffic from unusual bursts or unknown destinations.

4



Understand

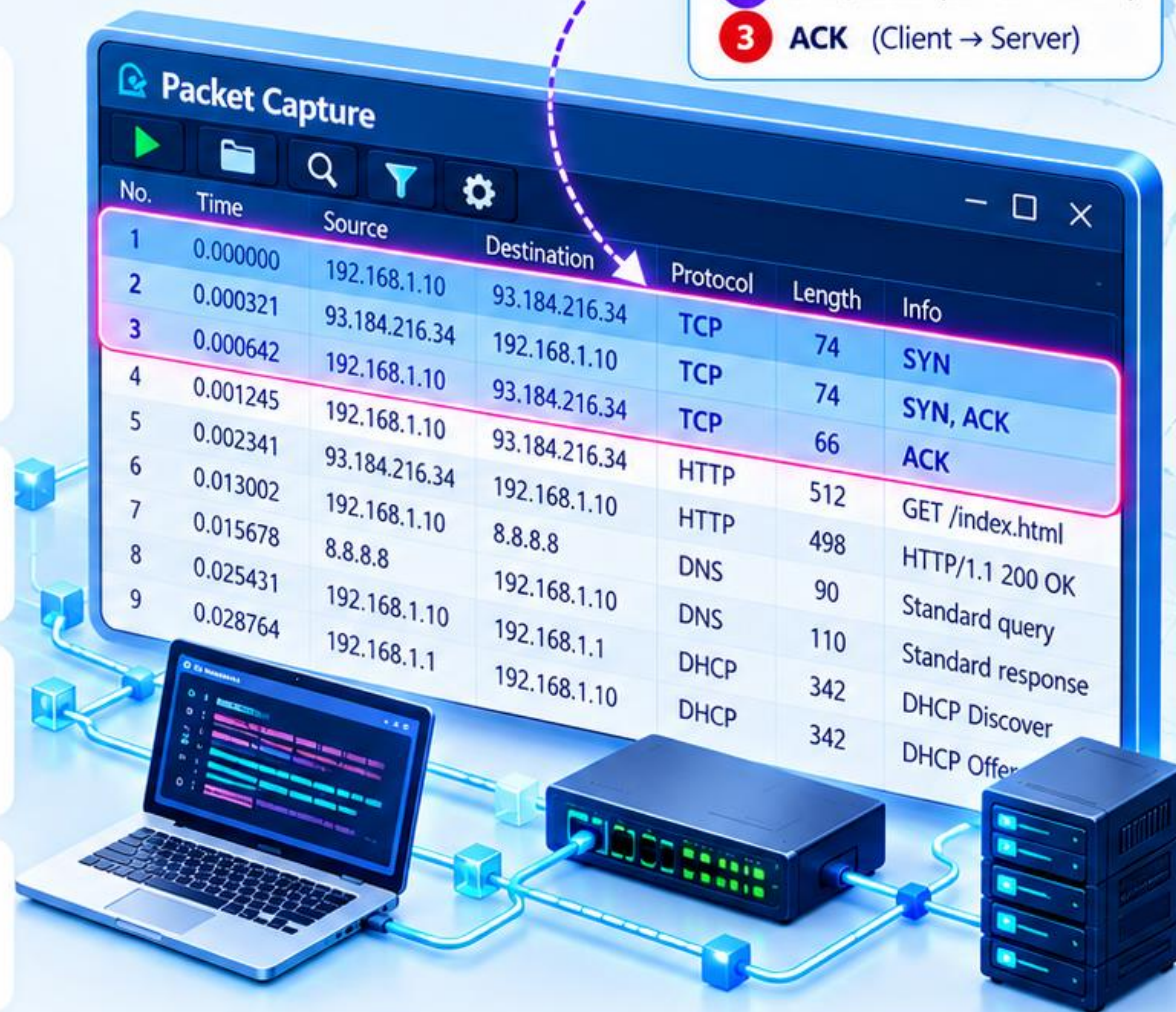
Why encrypted protocols reduce payload visibility.

5



Extract

Defensive indicators without collecting unnecessary sensitive content.



Collect indicators — not other people's data.

SECTION 13

Practical Tools & Labs

Reproducible, safe, evidence-driven practice.

1



Lab Architecture

Attacker VM, target VM,
isolated network.

2



The 10-Lab Sequence

From passive footprinting
to malware analysis.

3



Live Demo Flow

Nmap, dig, tcpdump and Wireshark.

4



Evidence & Reporting

Minimum evidence and finding structure.

5



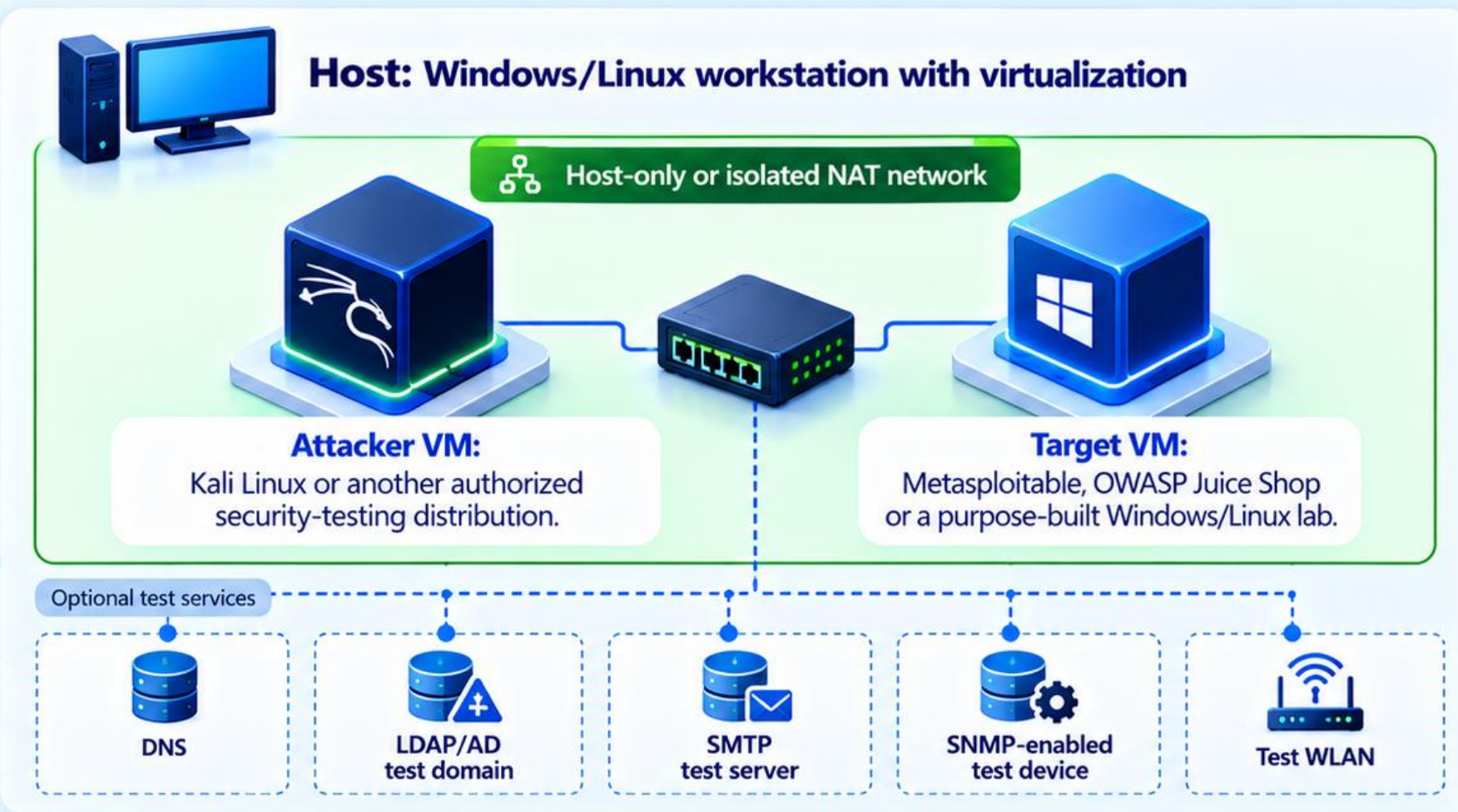
Tool Modernization

Legacy names, modern tools.



If it is not documented, it did not happen.

Recommended Lab Architecture



⚠ Avoid exposing vulnerable VMs directly to the internet.



📅 Keep a dated lab notebook.



Isolation is the safety system of every lab.

Suggested 10-Lab Sequence

1 Lab 1



Passive footprinting
and asset inventory

2 Lab 2



DNS and
traceroute analysis

3 Lab 3



Host discovery and
TCP/UDP scanning

4 Lab 4



Service/version and
OS fingerprinting

5 Lab 5



SNMP/SMB/LDAP/SMTP/
DNS enumeration

6 Lab 6



Vulnerability assessment
with a deliberately
vulnerable VM

7 Lab 7



WLAN architecture
and defensive security
assessment

8 Lab 8



IDS/firewall/honeypot
detection and logging
concepts

9 Lab 9



Packet capture and
protocol analysis

10 Lab 10



Malware/persistence
analysis using a disposable
VM and safe artifacts



Each lab builds on the one before it.

Live Demo Flow

Progressive scanning, then DNS, then traffic capture.

-  **Host discovery**
-  **Ports**
-  **Services & versions**
-  **OS**
-  **DNS records**
-  **Capture → open in Wireshark**

```
# 1. Host discovery
nmap -sn 192.168.56.0/24

# 2. Ports
nmap -sS --top-ports 100 192.168.56.10

# 3. Services & versions
nmap -sV 192.168.56.10

# 4. OS
nmap -O 192.168.56.10

# 5. DNS records
dig example.lab A

# 6. Capture traffic (open in Wireshark)
sudo tcpdump -i eth0 -nn -c 100
```



Isolated lab only — record every command and result.

Minimum Evidence for Each Lab

1		Lab topology diagram	6		Screenshots or exported results
2		Target IP/hostname and scope statement	7		Finding interpretation
3		Tool name and version	8		Risk/impact statement
4		Date and time of execution	9		Remediation recommendation
5		Commands or configuration used	10		Retest result and cleanup confirmation



Evidence is what makes a result believable.

Example Finding Structure

Field	Example Content
Title	SNMP service exposes unnecessary management information
Asset	Lab router / 192.168.56.20
Evidence	Controlled SNMP query returned device and interface metadata
Risk	Information disclosure can assist reconnaissance and targeted attack planning
Recommendation	Restrict management access, use SNMPv3, rotate credentials, disable if unnecessary
Retest	Repeat query after hardening and confirm unauthorized access is denied



Evidence → risk → remediation → retest.

Legacy Tools, Modern Replacements



Most useful replacements

- Nmap
- Wireshark/tcpdump
- dig/nslookup
- modern vulnerability scanners
- Wazuh/Sysmon for endpoint telemetry
- a maintained malware-analysis sandbox



Important: a tool appearing in a CEH study list is not a recommendation to deploy it in production. Validate maintenance status, licensing, platform support and security posture before installation.



Legacy Tools

Older tools, may be unmaintained or unsupported.



Modern Replacements

Actively maintained, secure and feature-rich tools.



Prefer actively maintained tools.

Activity: Write Your First Finding

1 Pick a result



Choose one output from today's lab.

2 Fill six fields



Title, Asset, Evidence, Risk, Recommendation, Retest.

3 Label confidence



Verified, inferred or unverified.

4 Peer review



Swap with a partner and check that the evidence supports the claim.



A good finding can be understood and reproduced by someone else.

Key Takeaways

Six ideas to remember.

1 Authorization first



Only test what you own or have explicit permission to test.

2 Passive before active



Collect public information before touching the target.

3 Scan finds, enumeration extracts



Services first, structured information second.

4 Know your controls



IDS alerts, IPS prevents, firewalls enforce, honeypots watch.

5 VA vs pentest



Assessment lists weaknesses; testing proves impact.

6 Evidence to retest



Evidence, risk, remediation, retest — every time.



Ethical hacking is a method, not a mood — scope it, prove it, document it.

CRITICAL THINKING

Discussion Questions

Think beyond the slide.

1



A host does not answer ping.
Is it inactive? Why or why not?

2



One IP address appears to run several services.
What could explain it?

3



Which enumeration protocol would you
restrict first in your lab, and why?

4



How does encryption change what you can see
in a packet capture?

5



When would you recommend a penetration test
instead of a vulnerability assessment?



These questions have no single answer — that is what makes them useful.

QUIZ

Quiz — Part 1

Answer without notes.

1



Which type of reconnaissance can be logged or detected by the target?

5



Why is UDP scanning harder to interpret?

2



What does a CIDR prefix length help you determine?

6



Name two factors that reduce OS-fingerprinting accuracy.

3



Why can a firewall cause a host-discovery false negative?

7



How is enumeration different from scanning?

4



How does a SYN scan differ from a TCP connect scan?

8



Which SNMP version and controls are recommended for defense?



Answers on the key slide.

QUIZ

Quiz — Part 2

9



Which control addresses unauthorized DNS zone-data exposure?

10



Name the WLAN security generations from legacy to current. Which is weakest?

11



What is the difference between an IDS and an IPS?

12



Compare a security audit, a vulnerability assessment and a penetration test.

13



What distinguishes black-box, gray-box and white-box testing?

14



Name the first three phases of the penetration-testing roadmap.

15



Why is malware analyzed in disposable VMs with restricted networking?

16



What can a packet capture still reveal when the payload is encrypted?



Review the revision checklist for any you missed.

Answer Key

- | | | | | | |
|---|---|---|----|---|--|
| 1 |  | Active reconnaissance. | 9 |  | Restrict zone transfers. |
| 2 |  | Network address, usable host space and subnet boundaries. | 10 |  | WEP, WPA/WPA2, WPA3 (plus 802.1X/EAP for enterprise); WEP is weakest. |
| 3 |  | Firewalls may block ICMP, so a live host appears inactive. | 11 |  | IDS detects and alerts; IPS detects and prevents inline. |
| 4 |  | SYN probes TCP state without completing the connection; connect completes it and is more visible in logs. | 12 |  | Audit checks controls; VA lists weaknesses; pentest validates attack paths. |
| 5 |  | Many UDP services do not respond predictably; scans are slower. | 13 |  | Limited information, partial knowledge or credentials, and extensive architecture/code access. |
| 6 |  | Firewalls, virtualization, containers, proxies or NAT. | 14 |  | Pre-engagement, reconnaissance and discovery. |
| 7 |  | Scanning finds services; enumeration extracts users, shares, records and configuration. | 15 |  | To contain behavior and observe it safely using snapshots. |
| 8 |  | SNMPv3 with strong authentication/privacy, ACLs; disable unused SNMP. | 16 |  | IP addresses, ports and other metadata. |



Thank You

Ethical Hacking in Practice



Questions and Discussion

Open the floor — what questions do you have?



Presented By:
Priyank Mistry

