

HANDS-ON ACTIVITY 1: CONDUCTING A STRUCTURED PENETRATION TEST IN YOUR EXISTING LAB

Since Kali Linux, Windows 11, and Metasploitable are already installed in your virtual environment, this activity focuses on applying structured penetration testing methodology directly within your current setup.

This exercise reinforces:

- Ethical and legal boundaries
- Structured testing phases
- Controlled lab practice
- Risk evaluation without unnecessary harm
- Professional documentation

The objective is not exploitation for its own sake, but learning professional methodology and responsible analysis.

LAB SETUP (ALREADY COMPLETED LAST WEEK)

You have:

- **Kali Linux** – Attacker machine
- **Metasploitable** – Intentionally vulnerable Linux target
- **Windows 11** – Secondary target and comparison system

Ensure all machines remain on an isolated internal or host-only network.

ACTIVITY OVERVIEW

You will:

1. Define scope and rules of engagement
2. Perform reconnaissance
3. Conduct scanning
4. Compare two targets (Metasploitable vs Windows 11)
5. Evaluate risk without causing damage
6. Produce a professional mini-report

Task 1: Define Rules Of Engagement

Create a one-page Rules of Engagement document including:

Objective

Identify exposed services and security weaknesses within the lab without disrupting systems.

Scope

- Metasploitable IP address
- Windows 11 IP address
- Internal virtual network only

Out of Scope

- Denial of Service attacks
- Password brute force
- Exploit modules that modify data
- Persistence or backdoors

Evidence Handling

Screenshots and notes stored locally for academic purposes.

Why This Matters

Professional testers must always define legal scope and boundaries before beginning.

Task 2: Set Network Mode to Host-Only

The most important part of your lab is network isolation.

For each VM:

1. Power off the VM.
2. Open VM Settings.
3. Go to Network.
4. Set Adapter 1 to:
 - Attached to: Host-only Adapter
 - Name: VirtualBox Host-Only Network (or equivalent)
5. Save settings.

Do this for:

- Kali
- Windows 11
- Metasploitable

Goal: All three machines must communicate with each other but NOT with your real network.

Task 3: Phase 1 – Reconnaissance from Kali

From Kali: Identify active hosts on the subnet.

1. Identify IP addresses of both Metasploitable and Windows 11.
2. Document them in a small asset table:

Example 1: `sudo nmap -sn 192.168.56.0/24`

Example 2: `sudo netdiscover -r 192.168.56.0/24`

Replace `192.168.56.0/24` with your actual subnet.

This identifies live systems without aggressive scanning.

You should see: Metasploitable and Windows 11. This builds awareness of network footprint.

System	IP Address	OS	Purpose
Metasploitable	192.168.X.X	Linux	Vulnerable test target
Windows 11	192.168.X.X	Windows	Modern secure OS comparison

Learning Goal: You are practicing structured asset identification before scanning.

Task 4: Phase 2 – Scanning

Using Kali, perform service discovery scans against:

- Metasploitable
- Windows 11

Record for each:

- Open ports
- Services
- Service versions (if available)

Create two comparison tables.

Example – Metasploitable

Port	Service	Observation
21	FTP	Outdated version
23	Telnet	Insecure protocol
80	HTTP	Older web server

Example – Windows 11

Port	Service	Observation
135	RPC	Standard Windows service
445	SMB	May require authentication

Take screenshots as evidence.

Task 5: Compare the Two Systems (Critical Thinking Phase)

Answer:

1. Which system exposes more services?
2. Which appears more hardened?
3. Why does Metasploitable show more vulnerabilities?
4. How does a modern OS differ from an intentionally vulnerable one?

Learning Goal: Understand the difference between misconfigured systems and hardened modern systems.

Task 6: Risk Evaluation Without Exploitation

Select 2–3 high-risk findings from Metasploitable.

For each, document:

- Why it is risky
- What an attacker might attempt
- The recommended mitigation

Example:

Finding	Risk	Recommendation
Telnet enabled	Credentials sent in plaintext	Replace with SSH
Anonymous FTP	Unauthorized access risk	Disable or restrict access

For Windows 11:

- Identify why fewer services are exposed.
- Note built-in security features such as firewall protections.

Learning Goal: Shift from “attacking” to “defending” mindset.

Step 7: Post-Exploitation Reflection

Write a short reflection:

If an attacker gained access to:

- Metasploitable – what could they do next?
- Windows 11 – what barriers might stop them?

Then state clearly: What should an ethical tester do after demonstrating access?

Expected answer: Document, report, and recommend remediation, stop.

Step 8: Write the Mini Report

Use this structure:

1. Executive Summary

Summarize:

- What was tested
- Key findings
- Overall risk level comparison

2. Scope and Rules of Engagement

3. Methodology

- Reconnaissance
- Scanning
- Risk analysis

4. Findings

Separate sections:

- Metasploitable
- Windows 11

5. Recommendations

List prioritized fixes.

6. Limitations

Mention:

- Lab-only environment
- Time constraint
- No destructive exploitation
- Some vulnerabilities may not be visible

Expected Learning Outcome

By completing this lab, students will:

- Apply structured penetration testing methodology
- Compare vulnerable and modern systems
- Practice ethical boundaries
- Strengthen analytical thinking
- Develop professional reporting skills
- Transition from attacker curiosity to defender responsibility