

Hands-On Activity 1: Structured Penetration Test

This interactive worksheet is designed for students to type their answers directly into the PDF. It follows a controlled penetration testing methodology using the existing virtual lab: Kali Linux, Metasploitable, and Windows 11.

How students should use this PDF

Click inside the white boxes to type. Tick the checkboxes to confirm understanding or completion. Save a copy of the PDF before submitting it. If a browser does not save typed answers correctly, download the file and open it in Adobe Acrobat Reader or another PDF reader that supports forms.

Lab Setup

- Kali Linux - attacker machine
- Metasploitable - intentionally vulnerable Linux target
- Windows 11 - secondary target and comparison system
- All machines must remain on an isolated internal or host-only network

Student Details

Student name:

Date:

Class / group:

Lab machine:

Activity Overview

- ☐ Define scope and rules of engagement
- ☐ Perform reconnaissance
- ☐ Conduct scanning
- ☐ Compare Metasploitable and Windows 11
- ☐ Evaluate risk without causing damage
- ☐ Produce a professional mini-report

Task 1: Complete the Rules of Engagement

Before starting the technical work, students must confirm the boundaries of the lab. This helps keep the activity safe, legal, and professional.

Objective - briefly explain what this lab is trying to achieve

In Scope

Only the approved virtual lab systems are in scope. Complete the IP addresses after reconnaissance if they are not known yet.

In Scope Systems

System	Role	IP Address
Kali Linux	Attacker machine	Not required
Metasploitable	Vulnerable target	
Windows 11	Comparison target	

Allowed Activities

- ☐ Identify live hosts inside the lab network
- ☐ Scan lab machines for open ports and services
- ☐ Record screenshots and notes as evidence
- ☐ Compare the security posture of the two target systems

Out of Scope - Not Allowed

- ☐ Denial of Service attacks
- ☐ Password brute force attacks
- ☐ Exploits that modify, delete, or damage data
- ☐ Persistence, backdoors, or maintaining access
- ☐ Testing real websites, public IP addresses, school systems, or personal devices

Task 1 Continued: Evidence and Confirmation

Evidence Handling

- ☐ Screenshots and notes will be stored locally
- ☐ Evidence will only be used for this academic lab
- ☐ Findings will not be shared outside class without permission

Why Rules of Engagement matter - write one or two sentences

Student Confirmation

- ☐ I understand which systems I am allowed to test
- ☐ I understand which actions are not allowed
- ☐ I will only test inside the approved lab environment
- ☐ I will record findings responsibly and avoid causing harm

Student name / signature:

Date:

Teacher note

Students confirm Task 1 by ticking each box and typing their name and date. This is not a legal contract, but it helps them practise professional testing habits.

Task 2: Set Network Mode to Host-Only

The most important safety step is network isolation. All three virtual machines must communicate with each other, but not with the real network.

Host-Only Network Checklist

VM	Powered off	Adapter 1 set to Host-only	Saved settings
Kali	☐	☐	☐
Windows 11	☐	☐	☐
Metasploitable	☐	☐	☐

Host-only network name or subnet used

Task 3: Phase 1 - Reconnaissance from Kali

Use Kali to identify active hosts on the subnet. This step builds awareness of the lab network before scanning services.

Command used for host discovery

Asset Identification Table

System	IP Address	Operating System	Purpose / Notes
Metasploitable			
Windows 11			
Other / Unknown			

Screenshot filename or evidence note

Task 4: Phase 2 - Scanning Metasploitable

Perform service discovery against Metasploitable. Record open ports, services, versions if available, and a brief observation.

Metasploitable scan command used

Metasploitable Scan Results

Port	Service	Version	Observation

Metasploitable screenshot filename or evidence note

Task 4 Continued: Scanning Windows 11

Perform service discovery against Windows 11. Compare the results with Metasploitable and consider why the exposed services may differ.

Windows 11 scan command used

Windows 11 Scan Results

Port	Service	Version	Observation

Windows 11 screenshot filename or evidence note

Task 5: Compare the Two Systems

Use your scan results to answer the questions below. Focus on security posture, not just the number of ports.

1. Which system exposes more services?

2. Which system appears more hardened?

3. Why does Metasploitable show more vulnerabilities?

4. How does a modern OS differ from an intentionally vulnerable one?

Task 6: Risk Evaluation Without Exploitation

Select 2-3 high-risk findings from Metasploitable. Explain the risk and recommend a safer configuration. Do not exploit the findings.

Risk Evaluation - Metasploitable

Finding	Why it is risky	Recommended mitigation

Windows 11 notes - why were fewer services exposed or better protected?

Step 7: Post-Exploitation Reflection

This reflection is about impact awareness. Do not perform post-exploitation activities in this lab.

If an attacker gained access to Metasploitable, what could they do next?

If an attacker gained access to Windows 11, what barriers might stop them?

What should an ethical tester do after demonstrating access?

Expected Professional Response

- | | |
|--|--|
| ☐ Document the evidence | ☐ Report the finding |
| ☐ Recommend remediation | ☐ Stop testing and avoid unnecessary harm |

Step 8: Mini Report Checklist

Use this checklist to make sure your final mini-report includes the required sections.

Report Sections

- ☐ Executive Summary
- ☐ Scope and Rules of Engagement
- ☐ Methodology: reconnaissance, scanning, and risk analysis
- ☐ Findings: Metasploitable
- ☐ Findings: Windows 11
- ☐ Recommendations
- ☐ Limitations

Executive Summary - short draft

Limitations to Mention

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

Final comments or questions