# Day 15 – Practice Day (Review & Hands-On)

This document summarizes the review of Days 1–14 from the 30-Day Ethical Hacking Challenge and outlines the Day 15 practice plan. The goal is to consolidate all learned concepts into practical exercises in a safe, isolated lab environment.

## 1. Recap of Days 1–14

* Day 1 – Kali setup & basics: Installation, updates, key tool setup.
* Day 2 – Cyber Kill Chain & Recon: External & internal reconnaissance techniques.
* Day 3 – Google Dorking & DNS Recon: Search filters, DNS lookups, and zone transfers.
* Day 4–8 – Metasploit Foundations: Module types, workflow, shell handling.
* Day 9 – Metasploitable setup: Safe sourcing and isolation.
* Day 10–11 – Service enumeration & exploitation methodology.
* Day 12 – Deeper dive into Metasploit modules and payloads.
* Day 13 – Client vs Server-side exploitation.
* Day 14 – Password Attacks (Online vs Offline) and best practices.

## 2. Day 15 Practice Plan

The practice day consists of a sequence of lab-based exercises to reinforce reconnaissance, exploitation, password cracking, and post-exploitation skills.

1. Part A – Warm-up (30–45 min)

* Confirm scope and legal boundaries.
* Set network to Host-Only mode and verify connectivity.
* Run nmap scans for open ports and services.
* Enumerate HTTP services using WhatWeb and Gobuster.

1. Part B – Scenario 1: Server-Side Exploit (60–75 min)

* Identify a vulnerable service (e.g., vsftpd, Tomcat).
* Use Metasploit to exploit the service and gain a shell.
* Upgrade to a stable session and perform post-exploitation tasks.
* Document findings and take screenshots.

1. Part C – Scenario 2: Web App + Offline Crack (60–75 min)

* Enumerate web application with Gobuster.
* Perform controlled brute-force against the lab login.
* Extract hashes and crack them offline with John/Hashcat.
* Re-use cracked credentials across lab services.

1. Part D – Scenario 3: Client-Side (Optional, 30–45 min)

* Host a benign file locally.
* Access it from the victim browser to understand delivery mechanisms.

1. Part E – Reporting (30 min)

* Document scope, methodology, findings, and remediation suggestions.
* Save all outputs and screenshots in organized folders.

## 3. Quick Reference Commands

* Host discovery: arp-scan -l, ping -c 1
* Port scanning: nmap -p- --min-rate 2000 <IP>
* Service enum: nmap -sV -sC -p <ports> <IP>
* Web enum: whatweb, gobuster dir, nikto
* Metasploit workflow: msfconsole → search → use → set → run
* Password cracking: john --wordlist=rockyou.txt hashes.txt

## 4. Ethics Reminder

All activities should only be performed on systems you own or have explicit written permission to test. Keep all testing in an isolated lab environment and do not target external systems.