# Summary of Hands-On Cybersecurity Lab: Metasploitable 2 & Kali Linux

Over the course of this lab exercise, I successfully set up and configured two virtual machines — Kali Linux as the attacker and Metasploitable 2 as the vulnerable target. Using these environments, I performed a simulated penetration test focused on gaining unauthorized access, extracting sensitive information, and understanding defense mechanisms.  
  
Key activities included:  
  
- Configuring internal networks in VirtualBox to enable communication between VMs.  
- Downloading, extracting, and properly loading ISO and VM files for Kali Linux and Metasploitable.  
- Conducting reconnaissance and network scanning to identify running services.  
- Extracting password hashes from the Metasploitable system’s shadow file.  
- Using John the Ripper with common wordlists to crack user passwords.  
- Connecting to the FTP server on Metasploitable with cracked credentials.  
- Uploading and transferring files using netcat to facilitate data exfiltration.  
- Troubleshooting challenges with VM network settings, command-line navigation, and password cracking limitations.  
- Practicing operational security by clearing command histories, logs, and removing uploaded files in cleanup steps.  
  
Challenges encountered:  
  
- Initial confusion over network adapter types and how to configure VirtualBox internal networks.  
- Dealing with missing or compressed ISO files requiring extraction and proper VM import.  
- Navigating and understanding password cracking outputs and errors.  
- Handling network connectivity issues between VMs and firewall rules blocking traffic.  
- Learning to use CLI tools like netcat and John effectively, including syntax and flags.  
  
Key learnings:  
  
- The importance of setting up accurate and isolated lab environments to safely test exploits.  
- How to extract and leverage password hashes and the role of wordlists in cracking.  
- The significance of FTP service vulnerabilities and how credential reuse can be exploited.  
- Practical skills in transferring files and maintaining operational security.  
- Understanding that root access represents full control, shifting focus from escalation to persistence and lateral movement.  
- How to document findings professionally for reporting and future reference.  
  
This hands-on experience greatly enhanced my understanding of attack methodologies, defensive countermeasures, and the overall penetration testing process, preparing me for more advanced cybersecurity challenges.