

Lab 0 - Kali and Metasploitable (Environment Setup)

Lab preparation

1. Install VirtualBox, VMware, or UTM.
2. Install the following virtual machines.
 - Kali Linux
 - Metasploitable 2 (from Rapid7)



Basic commands in Kali Linux

3. Run the following commands and give a short description of what each one does.
 - `ls -a`
 - `ls /etc/`
 - `lsusb`
 - `cd`
 - `cd -`
 - `cd ..`
 - `cd /`
 - `cd /usr/bin/ or usr/bin`
 - `mv myFile aDir/`
 - `mv aDir/myFile .`
 - `mv aDir myDir`
 - `cp myFile subDir/`
 - `cp -r myDir/ elsewhere/`
 - `mkdir photos`
 - `mkdir -p photos/2025/vacation`
 - `pwd`
 - `find myfile*`
 - `find -name *myfile*.ogg`
 - `find /home/ -name myfile`
 - `find . -name "*.c"`
 - `grep -n mytexte myfile`
 - `cat -n myFile`
 - `sudo apt-get update`
 - `sudo apt-get upgrade`
 - `sudo apt-get install packet1 packet2`
 - `sudo apt-get --purge remove packet3`
 - `rmdir Dir_1`
 - `exit`
 - `who`
4. Write and run a Bash script `lab0_.sh` that collects a small system report (reconnaissance) and saves it to `/tmp/lab0-report-<yourname>-YYYYMMDD-HHMMSS.txt`. The script should:
 - Check it is running on Linux and exit with a message if not.
 - Print a header with student name, hostname, and timestamp.
 - Collect and append to the report: `uname -a` (kernel info).
 - `whoami` and user list (`cut` from `/etc/passwd` for human users).
 - IP addresses (`ip -brief addr` or `ip a` fallback).