# Experiment 1

- **Rats Tool:-**

  **Install Command:-**

  1. sudo git clone https://github.com/andrew-d/rough-auditing-tool-for-security
  2. cd rough-auditing-tool-for-security/
  3. sudo ./configure
  4. sudo make
  5. sudo make install

  **Execute Command:-**

  1. rats filename
     Example: rats ocr.py, rats palin.c, etc

- **FlawFinder:-**

  **Install Command:-**

  1. sudo apt-get install python-pip (If not installed).
  2. sudo pip install flawfinder

  **Execute Command:-**

  1. Flawfinder filename
     Example: flawfinder ocr.py, flawfinder bufferoverflow.c

# Experiment 2

- **Nessus:-**

  **Installation:-**

  1. Visit (“https://www.tenable.com/downloads/nessus”) website and download compatible nessus 8.7.2 for your ubuntu(It's in .deb file).
  2. Open Terminal and goto Download directory(cd downloads).
  3. sudo dpkg -i Nessus*.deb
  4. Start Nessus Scanner by typing /etc/init.d/nessusd start.
  5. Then Open browser and visit (“https://localhost:8834”).
  6. Click on Nessus Essentials and get the activation code and complete the process.
  7. Now sit back and relax, it will take more than 2 hour to initialize the process.

- **Nikto:-**

  **Installation:-**

  1. sudo apt-get install nikto

  **Execution:-**

  1. sudo nikto -h https://www.google.com

## Experiment 3

- **Httrack:-**

  **Installation:-**

  1. sudo apt-get install httrack

  **Execution:-**

  1. sudo httrack "https://www.w3schools.com/" -O "https://www.w3schools.com/"

## Experiment 4

- **Wapiti:-**

  **Installation:-**

  1. Download wapiti 3.0.2.
  2. Extract using “sudo unzip wapiti3-3.0.2.zip”
  3. cd wapiti3-3.0.2
  4. sudo apt-get install python3-venv libxml2 libxml2-dev libz-dev libxslt1-dev python3-dev
  5. sudo python3 -m venv wapiti_venv
  6. . wapiti_venv/bin/activate
  7. sudo python setup.py install
  8. Wapiti -h (For help).

  **Execution:-**

  1. wapiti -u http://testphp.vulnweb.com/

- **Beef:-**

  **Installation:-**

  1. sudo apt-get install ruby ruby-dev
  2. sudo apt-get install git
  3. git clone https://github.com/beefproject/beef
  4. cd beef
  5. ./install
  6. sudo ./install

  **Execution:- (“https://www.youtube.com/watch?v=sB9whT_QILA”)**

  1. ./beef
  2. Change default password from config.ymal
  3. Open browser and go to http://127.0.0.1:3000/ui/authentication
  4. Enter username and password.
  5. And visit above given link for execution.

## Experiment 5

- **SqlMap:-**

  **Installation:-**

  1. sudo apt-get install sqlmap

  **Execution:-**

  1. sqlmap -u http://testphp.vulweb.com/listproducts.php?cat=1 --dbs
  2. sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart –tables
  3. sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T products –columns
  4. sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T products -C name --dump

## Experiment 6

- **Metasploit:-(“https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers”)**

  **Installation:-**

  1. curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \
     chmod 755 msfinstall && \
     ./msfinstall

  **Execution:-**

  1. msfconsole
  2. https://www.tutorialspoint.com/metasploit/metasploit_brute_force_attacks.htm

## Experiment 9

- **“https://www.youtube.com/watch?v=ycH4Cprtcow”**

## Experiment 11

- **DD:-**
  1. sudo dd if=/dev/sda1 of=dhruv bs=65536 conv=noerror,sync
- **DC3DD:-**
  1. sudo apt-get install dc3dd
  2. sudo dc3dd if=/dev/sda1 of=/mnt/sdb.dd hash=md5
- **Debugfs:-**
  1. Visit the link https://www.tecmint.com/debugfs-command-show-file-creation-time-in-linux/

# Experiment 12

- **FTKImager:-(“**https://www.cybrary.it/0p3n/using-ftk-imager-cli-challenging-new-disks-technologies**”)**

  **Installation:-**

  1. curl -o ftk.tar.gz https://ad-zip.s3.amazonaws.com/ftkimager.3.1.1_ubuntu64.tar.gz
  2. tar zxvf ftk.tar.gz
  3. sudo mv ftkimager /usr/local/bin
  4. cd /usr/local/bin

  **Execution:-**

  1. sudo ./ftkimager /dev/sda1 /home/viraj/ --e01 --compress 9 --case-number 1700345498 --evidence-number ITEM001 --description "This crime happened today " --examiner "Viraj" --notes "Cases and Notes"

- **Autopsy:- (karna maaat abhi)**

  **Installation:-**

  1. Download “https://github.com/sleuthkit/autopsy/releases/download/autopsy-4.13.0/autopsy-4.13.0.zip”
  2. Download “https://github.com/sleuthkit/sleuthkit/releases/download/sleuthkit-4.7.0/sleuthkit-java_4.7.0-1_amd64.deb”
  3. sudo apt-get install testdisk
  4. Download .deb file for java8 jre package “https://www.azul.com/downloads/zulu-community/?&version=java-8-lts&os=&os=ubuntu&architecture=x86-64-bit&package=jre”
  5. Download “https://www.azul.com/downloads/zulu-community/?&version=java-8-lts&os=&os=ubuntu&architecture=x86-64-bit&package=jdk-fx&show-old-builds=true”
  6.