**Student Name:** **Weight: \_\_\_\_\_\_\_\_\_\_**

**Student ID:** **Marks: \_\_\_\_\_\_\_\_\_\_**

Lab 8: SNORT/RECON-NG

## *Please attach screenshots for each step. Mention your team member’s name.*

SSH-KEYS

* Create SSH keys for your user in kali/parrot and login in remotely from second machine.

SNORT

* Set up a metasploitable and capture the following tasks in your snort: Please attach screenshots of your rules, verification of rules, perform each task in your testing machine and alerts captured in the snort console(each time).
  + Set up a snort rule for accessing any http traffic in the network.
    - Fire up a metasploitable and try accessing its webserver from your testing machine.
  + Set up a snort rule for capturing ftp traffic in the network.
    - Fire up a metasploitable and try accessing its ftpserver from your testing machine.
  + Set up a snort rule for accessing any ssh traffic in the network.
    - Fire up a metasploitable and try accessing its sshserver from your testing machine.

RECON-NG

* Target : <http://testphp.vulnweb.com>
* What kind of information do you gather using the module: discover/info\_disclosure/interesting\_files.
* Were you able to find any vulnerability using the module: recon/domain-vulnerabilities/xssed.
* Target : <http://testfire.net>
* What kind of information does this module capture on your target: /recon/domains-hosts/hackertarget
* Create a html report using the module reporting/html