Faculty of Computing and Information Technology
University of the Punjab
(Term Spring 25)

CC-403 Information Security Student ID:_____

Class Activity 02

Marks: 70

This activity is about Pen-Testing initial three phases: Reconnaissance & Information gathering, Scanning & Vulnerability Analysis, and Exploitation & gaining initial access. You have to perform this activity on your laptops using your Hacking Lab environment. Due to Ramazan I am making this activity public, so that you can do it on the weekend on your laptops, and give a viva in the coming week to the TAs by showing already performed Proof of Concepts (PoCs) of the below mentioned tasks. TAs of all the sections will announce viva day between 24 Mar to 27 Mar.
Happy Learning to all…

Task 01: **[10]**

- On your Kali Linux machine show as to how you can achieve anonymity using proxy chains, VPNs, and TOR browser. All these must be working on your laptop and you should have a clear understanding of their differences to get full credit. Every student should explore some good links of deep/dark web and share them with the TAs.

Task 02: **[10]**

Show the working of following reconnaissance and information gathering tools on your Kali Linux machine:

- Knockpy
- Netdiscover
- theHarvester
- Sherlock
- Wafw00f
- Discuss and display the best search that you have done using multiple operators of Google Dorking

Task 03: **[20]**

- On your Kali Linux machine install Nessus and perform Vulnerability Analysis on Metasploitable 3 machine in your lab environment
- On your Kali Linux machine install OpenVAS and perform Vulnerability Analysis of the machine hosting your instructor website, or your university website. Please do not go beyond this, as it may cause legal actions if done.

Task 04: **[30]**

- Understand the vulnerable service SMB running on Windows based Metasploitable3 machine and exploit it using EternalBlue **DoublePulsar** attack. Refer to Handout#2.5 [10]
- Understand the vulnerable service **UnrealIRCd** (Internet Relay Chat daemon allows users to connect, communicate and exchange messages in real time) running on port 6667 on M2 and exploit it. [5]
- Understand the vulnerable service **distccd** (a daemon that allows compilation of C programs to be distributed across several machines in a NW) running on port 3632 on M2 and exploit it. [5]
- Understand the vulnerable service **VNC** (Virtual Network Computing, a cross-platform screen sharing system that was created to remotely control another computer) running on port 5900 on M2 and exploit it. [5]
- Understand the vulnerable service **PostgreSQL** (an open- source RDBMS) running on port 5432 on M2 and exploit it. [5]

- **Bonus Task:** Build a portable OS like https://tails.net or https://whonix.org that will allow you to you're your device in a secure, isolated environment leaving no trace on the host machine. Once done try to implement a layered approach by using TOR+VPN+ProxyChains to achieve anonymity. Any student who will practically perform this bonus task will get Full Quiz marks in any of the missed quiz in the entire semester. Or if no quiz is miss, then he/she will get Full Quiz marks in any two of the quizzes having least marks.