**CSE 345/545: Foundations to Computer Security**

**HW 3 (TOTAL OF 150 POINTS)**

**Deadline: December 1, 2020**

**Instructions:**

- Do your Assignment questions individually.
- Make one PDF format file for writing your analysis/results in the format <RollNo>_HW3.pdf
- ***Do not* zip your submissions.**
- State your assumptions (if any) in your question.
- All the Queries, if any can be posted on google classroom.
- **Note: Answer the questions in bullet points. Keep your responses crisp and to the point.**

---

**Part 1**

1. What is "Recoverability" in the context of software security testing? You are the Admin of a chat server hosted on the IIITD network, what is your plan to ensure 'data recoverability'? How do you test the 'recoverability' functionality?

[10 marks]

2.
   a. What is automatic code analysis? List the 4 types of code analysis discussed in class. Given example code for each type.
   b. Install PyCharm or Intellij. Do not install any plugins. In the vanilla version of these IDEs what code analysis types are covered? Fill in the table below with 5 such functionalities.

| **Code Analysis Type** | **Sub-functionality** | **Supported (Yes/No)** |
|---|---|---|
| Control flow analysis | unreachable-code | ... |
| | | |

[10 + 10 = 20 marks]

3. When is regression testing necessary? You are a hacker working for the mobile giant Samsing. The nextgen sPhone will have 'under display fingerprint scanner' for locking and unlocking the phone; while the current version has a 'face recognition' based unlock mechanism. Write the regression test scenarios for the new upgrade. Start with 1) test cases written for unlocking the phone, add 2) tests specific for 'face recognition' based

unlock mechanism. Identify 3) what test cases stay relevant with the new upgrade, and finally 4) describe the regression test plan.

[20 marks]

## Part -2

---

1. Download ‘metaspoiltable.zip’ (attached with the HW on classroom), install VM and bring the system up. (default username: msfadmin and password: msfadmin.)

   Attack Machine: You are free to use Kali linux or Ubuntu as the attacking machine. Kali linux comes with a suite of applications pre-installed. Unless specified you will perform the following exercise on the attacking machine.

   Report format: Your report should contain.

   1. Background of the attack (3 bullet points on why / how / outcome )
   2. Steps followed to perform the attack
   3. Appropriate screenshots for each command / attack
   4. Other deliverables specific to the questions.

   Questions:

   a. Use nmap to identify the OS version of the metaspoiltable system.

   [10 marks]

   b. List the open ports on metaspoiltable system. What commands did you use? What are the ports used for by default? What applications did you find running on the open ports?

   [10 marks]

   c. Metasploitable contains a backdoor on its’ FTP server. Exploit the same and report the following:

      i. What tool(s) did you use?
      ii. What command(s) did you execute?
      iii. What is the outcome of the exploit?

   [10 + 10 + 10 = 30 marks]

   d. Metaspoiltable has Mutillidae running on the VM. Multillidae contains the top-10 vulnerabilities on OWASP.

      i. Exploit the “SQL Injection on blog entry” vulnerability on “add-to-your-blog.php” page.

ii. The database credentials on Multillidae are unencrypted.

   1. Which file contains the credentials?
   2. List all such credentials.
   3. Purge a table.

[20 + (10 + 5 + 15) = 50 marks]