Penetration Test Workshop (CSE3157)

Introduction to Penetration Testing

Dr. Rourab Paul

Computer Science Department, SOA University

What pen test?

Penetration testing, or pentesting is not to be confused with testing ballpoint or fountain pens

Room, timetable, teacher

- Teacher
  - Rourab Paul
    - Computer Science Department
    - Web: https://rourab.com/leclist.php?sub=ptw&year=2024-2025&sec=24
    - Email: rourabpaul@soa.ac.in
    - Skype: rourabpaul

- Room and Timetable
  - 16:00 – 18:00 Monday, C204
  - 10:00 – 13:00 Wednesday, C204
  - 08:00 – 11:00 Friday, C204

Evaluation Procedure

- Mid Sem 30 marks (Weight 15)
- Attendance 5 marks
- Assignment+Quiz+mini Project =20 Marks
- End Sem 60 Marks

Purpose

- On a pentest (as opposed to a vulnerability assessment), the testers not only discover vulnerabilities that could be used by attackers but also exploit vulnerabilities, where possible, to assess what attackers might gain after a successful exploitation.

Stage: 1 of the Penetration Test

- Pre-engagement phase, which involves talking to the client about their goals for the pentest, mapping out the scope (the extent and parameters of the test), and so on. When the pentester and the client agree about scope, reporting format, and other topics, the actual testing begins.

Stage: 2 of the Penetration Test

- In the information gathering phase, the pentester searches for publicly available information about the client and identifies potential ways to connect to its systems. In the threat-modeling phase, the tester uses this information to determine the value of each finding and the impact to the client if the finding permitted an attacker to break into a system. This evaluation allows the pentester to develop an action plan and methods of attack.

Stage: 3 of the Penetration Test

- vulnerability analysis. In this phase, the pentester attempts to discover vulnerabilities in the systems that can be taken advantage of in the exploitation phase. A successful exploit might lead to a post-exploitation phase, where the result of the exploitation is leveraged to find additional information, sensitive data, access to other systems, and so on.

Final Stage of the Penetration Test

Finally, in the reporting phase, the pentester summarizes the findings for both executives and technical practitioners.

For more information on pentesting

http://www.pentest-standard.org/

Vulnerability Assessment VS Pen Test

1. Scan systems using automated tools like Nessus, OpenVAS, or Qualys.
2. Generate a report of identified vulnerabilities.
3. Assess the severity based on predefined criteria (e.g., CVSS scores).

1. Reconnaissance to gather information about the target.
2. Exploit vulnerabilities identified in the target system.
3. Attempt privilege escalation, data exfiltration, or system compromise.
4. Report findings, including proof-of-concept exploits and remediation steps.

Type of Pen test

Black Box: No prior knowledge of the system.

White Box: Full knowledge of the system.

Gray Box: Partial knowledge of the system.

Benefits of Pen test

- Protects against **data breaches** and **financial loss.**
- Helps meet **compliance** and **regulatory requirements.**
- Enhances trust with stakeholders.

Thank You