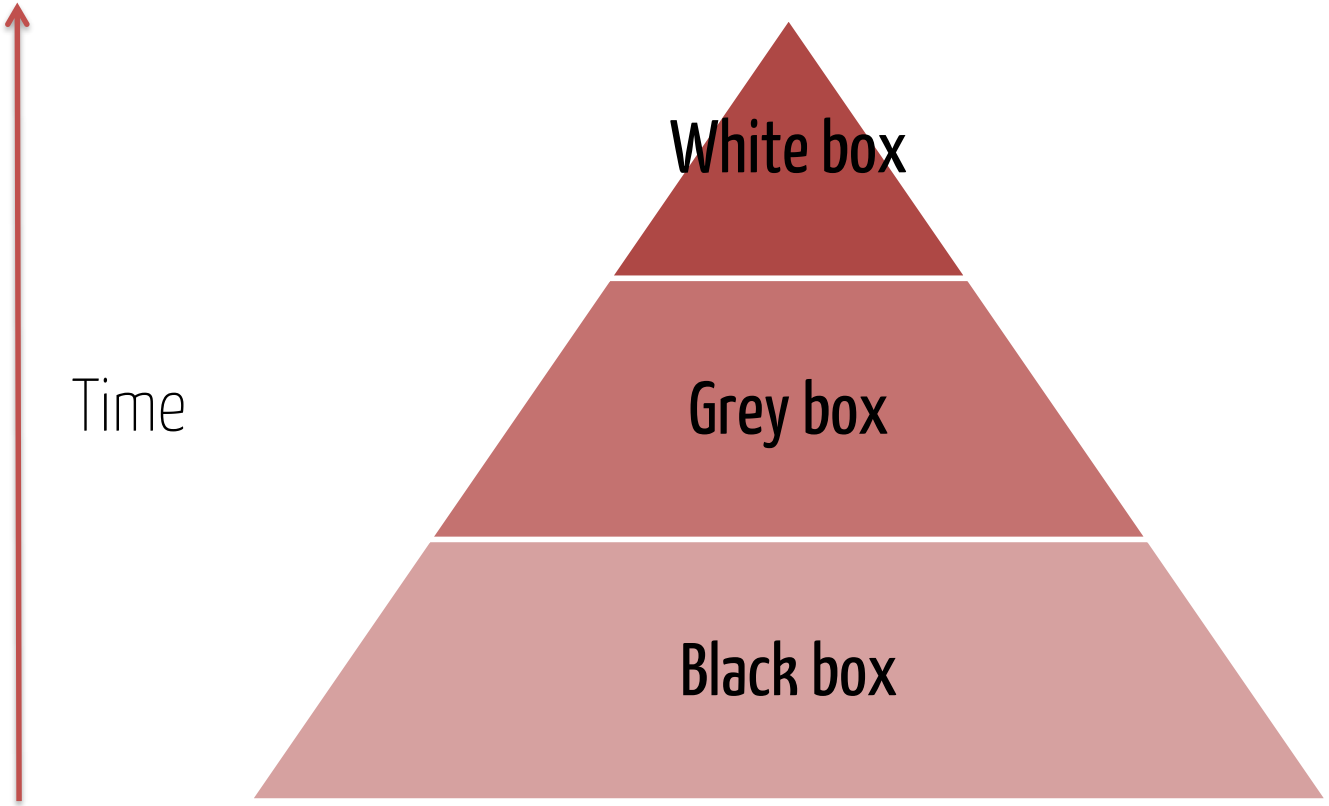
INTRODUCTION TO PEN TESTING

Introduction to
Penetration Testing

SECURITY ASSESSMENT

- Vulnerability assessment
  - A thorough evaluation of a system to assess the current security posture and to identify all possible weaknesses.
- Penetration test
  - A penetration test simulates an actual attack to test and validate the security controls that are in place.
  - The only aim of a penetration test is to compromise a system and assess the impact.
  - A penetration test may or may not cover all possible weaknesses.

TYPES OF TESTING



TYPES OF TESTING

Black Box Penetration Testing

- The tester is not furnished with any information.
- Information is gathered during the information gathering phase.
- Mimics actual attacks.
- The goal of this methodology is to simulate actual attacks by a malicious attacker.
- IDS / IPS might block attacks.
- Takes longer to complete.

TYPES OF TESTING

White Box Penetration Testing

- The tester is provided with information & sometimes access to the servers / source code.
- Login credentials are also sometimes provided.
- Most of the time, the tester's IP address is whitelisted on the IDS / IPS.
- Works well when there is a time constraint.
- This testing methodology is used to simulate an inside attacker who has some knowledge of the systems and possibly even credentials.
- Actual attacks are not always performed. Completion time is faster than black box testing.

TYPES OF TESTING

Grey Box Penetration Testing

- Is a combination of white box and black box testing.
- Limited information is provided to the tester.
- The aim of this methodology is to provide the speed of a white box test with the attack mindset of an external attacker.

DEVISING A PENTEST

- Kick off meeting
  - Discuss the objective of the penetration test.
  - Discuss on the scope and parties involved.
  - Discuss the timing and period of testing.
  - Discuss the final form of how the results are presented.
- Legal documents
  - Sign the letter of engagement.
  - Sign the Non-Disclosure agreement.

DEVISING A PENTEST

- Preparation
  - Identify which methodology to use.
  - Prepare the required checklist.
  - Update tools and scripts.
- Perform penetration test
  - Penetration testing life cycle.
  - Verifying findings.
  - Clean up

DEVISING A PENTEST

- Analysis & reporting
  - Assess the impact to the business based on the findings.
  - Assess probability of attack.
  - Compile evidence and findings for reporting.
- Remediation & revalidation
  - Customer remediates security flaws.
  - Penetration tester revalidates the finding(s).

LIMITS OF PENTESTING

- The business must first recognize what it is they are looking for before hiring a penetration tester, else it would be a waste of time and money.
- The test will only focus on the agreed scope.
- The test will be limited to the agreed time frame.
- The quality of the test depends on access to quality testers.
- Limitations to the methods involved highly hinders the result of the penetration test.
- A penetration test will not ensure your are safe from attacks.
- Penetration testing will only identify the risk. It is up to the business to remediate.