Information Security Testing or

The Art of Breaking Stuff To Improve It

Alexandre Dulaunoy

January 11, 2013

Definition

- Information security assessment is the process of determining the effectiveness of security measures to reach specific security objectives.
  - The assessment is usually performed using different techniques of *testing*, *examination* or *interviewing*.
  - *Testing*: actively assess components under specified conditions to see if they deviate from their baseline.
  - *Examination*: reviewing, studying or analyzing components to understand how they work and if they deviate from their intended objectives.
  - *Interviewing*: conducting discussion with people or groups of people involved in the components to be assessed.

Testing? Examination? Interviewing?

- Security assessment is usually a balanced approach using testing, examination and interviewing.
- There are many security testing techniques and procedure like "OSSTMM 3 - The Open Source Security Testing Methodology Manual", NIST SP 800-53A.
- Compare available tests with the components to be analyzed or the objectives. Do the tests fit? What is the information available for the assessment?

Penetration Testing

- Penetration testing is a subpart of *testing* including service identification and trying to make real-world attacks against a specify set of components.
- There are risks to perform "penetration testing" and they must be understood in advance.
- Penetration testing is not only a technical matter but may also include non-technical tests (e.g. social engineering).
- Black-box versus white-box pentesting.

Penetration Testing Approaches

- Often described linearly: planning → discovery → attack → reporting and mitigation.
- Usually it's more a circular approach where new attacks generate new discoveries than can lead to other attacks.
- Penetration testing is usually relying on anomalies than can lead to unexpected behavior of the components.
- Working in a small team is usually more efficient by the collaboration of the discoveries and step to be performed to lead to privilege escalation.
- Penetration testing is not full proof and offers usually a limited view.

Penetration Testing Tools

- Tools can be used in penetration testing to ease the work but are usually used in conjunction to custom software or manual solution.
- Discovery can usually be done with active tools (e.g. nmap, Nessus/OpenVAS,. . .) or active tools.
- Attack can be performed using tools like Metasploit or/and Social-Engineer Toolkit (SET).
- Fuzzing is specific kind of testing often used as starting point to find new vulnerabilities.

Bibliography

- NIST 800-115 - Technical Guide To Information Security Testing and Assessment
- Know Your Enemy, The Honeynet project - various, (second edition) Addison Wesley, ISBN 0-321-16646-9
- Computer Security, Art and Science, Matt Bishop, Addison Wesley, ISBN 0-201-44099-7

Q and A

- Thanks for listening.
- adulau@foo.be