Pre-engagement Pentest Checklist for Web Applications Assessments

pentestlab.blog/category/general-lab-notes/page/4

February 1, 2015

The success of a penetration test relies 50% on the planning and the information that it has been obtained in advance and the other 50% of the actual deployment of the test. Many times the proposal documents might not contain all the necessary information for the security consultant or the pentester.

As a penetration tester we need to ensure that the requirements of the project are met and there are no delays or any surprises (outside of the actual test) that will impact the assessment and the results.This can happen only with 2 ways:

1. Validation of the information in the proposal
2. Establishment of a communication channel with the client to obtain further information around the pentest

Checklists are always helpful as we don't forget what information is needed. Below is a checklist that is focused on web application assessments and it can assist pentesters especially the newest in the field to ensure that they have all the prerequisites to conduct the project with efficiency and to prevent any failures.

- Determination of the type of pentest (Blackbox, Whitebox)
- Key objectives behind this penetration test
- Location address and contact (if it is an onsite job)
- Validation that the Authorization Letter has been signed
- URL of the web application that is in scope and validation that is accessible
- 2 sets of credentials (normal and admin or a privilege user) and validation that are working
- Determination of the environment (Production or UAT)
- Number of static and dynamic pages
- Testing Boundaries (DoS, Brute force attacks etc.)
- Technologies (PHP, ASP, .NET, IIS, Apache, Operating system etc.)
- Any VPN or port numbers are needed and verify those ahead of time
- Any web services that the site may use.

- Any pages that the client does not want to be tested.
- Any pages that submit emails
- IP address of the tester
- Escalation contact
- 3rd parties that needs to be contacted in advance of the pentest
- Web application firewalls and other IDS in place
- Timeframe of the assessment (dates and hours)
- Diagrams and any kind of documentation
- Validation that a backup has been performed recently on the application
- Other client requirements

P.S

If you think that there is more information that’s needs to be gathered please reply with a comment and I will update the list.