Penetration Testing and Its Methodologies

By
Bhashit Pandya
Web Security Researcher

About me!

Hello Friends,
I am an Individual Security Researcher and web app vulnerability researcher!
Now a days working to share knowledge on Web Security and spreading awareness about common securities with Hcon..

“If You Want your system to be fully protected the better way is to turn it off!”

Acknowledgement

The presentation is dedicated to my dad and mom who always supported me and never let me down..
I would also Like to thank **Ashish Mistry** to give me a platform to show my skill's and spread my knowledge with him!

Disclaimer

The Presentation is for ethical and learning purpose. In this talk I will be presenting you about how a penetration testing is been conducted in Companies and Organizations. Here you will Learn about organizations give different methodologies and Manuals to conduct a pentesting session.
Hope you all enjoy and Learn!

What is Penetration Testing?

As per WIKIPEDIA

“A penetration test, occasionally pentest, is a method of evaluating computer and network security by simulating an attack on a computer system or network from external and internal threats.”

Penetration Testing Means testing a system to find out flaws,misconfigs,vulnerabilities all in ethical and systematic manner.

Testing Area's

So there are many testing area's for PenTestinig like

-Response team

-Systems regular Tests

-Human Manipulation

-Network Testing and Analyzing

-Application Auditing, Testing. Etc.

Why Penetration Test(Pentesting)?

How to know whether your network or system is secure or not?
Is any body latching up your personal data or violating your Privacy?
Well for few of you it don't matter a lot but what about the companies having there money logs/transactions or secrete data or any private data regarding customers where it is the duty of Companies to protect there privacy and to fix those vulnerabilities and clean up.

Pentesting Methodology

Penetration Testing Methodologies are the manuals to conduct a security test on a system in a particular manner!

In these manuals may be written by NGO or an individual or Govt. Orgs provides complete guideline to conduct a test.

It includes the following rough criteria:
1) Data collection
2) Vulnerability Assessment
3) Actual Exploit
4) Result analysis and report preparation

Why we need one?

What is the need of Pentest Methodology.
It is very important to know the reason.
There are many reason for this like
-It is use to determine the success of Test.
-Reporting becomes more convenient and precise to the client.
-Pentest can become more easy to conduct.
-Helps to initiate the process ethically and legally.

There are lots of other reason where we need Methodologies.

Orgs creating manuals and guideline

-OSSTMM
-ISSAF
-OWASP
-PTES
-NIST

These are some organizations which develop manuals and guideline as Methodologies.

OSSTMM

Open Source Security Testing Methodology Manual
The OSSTMM is a manual on security testing and analysis created by Pete Herzog and provided by ISECOM.
This is the latest full version of the Open Source Security Testing Methodology Manual. It includes security testing, security analysis, operational security metrics, trust analysis, operational trust metrics, the Möbius Defense, and the essential tactics for testing the security of anything including the cutting edge in technology.
The latest version is 3.

ISSAF

Information Systems Security Assessment Framework(ISSAF)
ISSAF is constantly evolving a framework that can model the internal control requirements for information security supported by the Open Information Systems Security Group (OISSG).
One of the advantages of the ISSAF is that it creates a distinct connection between tasks within a penetration test and PenTest tools

OWASP

Open Web Application Security Project(OWASP)
It is worldwide not-for-profit charitable organization focused on improving the security of software.
It is available under a free and open software license.
The goal is to create a set of commercially workable open standards that are tailored to specific web-based technologies

PTES

Penetration Testing Execution Standard(PTES).
They technical guidelines that help define certain procedures to follow during a penetration test.
They create a baseline structure to initiate and conduct a security test. They have well organized graphs and variety of Methods included in it.

NIST

National Institute of Standards and Technology(NIST).
The document guide to the basic technical aspects of conducting information security assessments. It presents technical testing and examination methods and techniques that an organization might use as part of an assessment, and offers insights to assessors on their execution and the potential impact they may have on systems and networks.

Sites Regarding these Orgs

OSSTMM:
http://www.isecom.org/osstmm/

ISSAF:
http://www.oissg.org/index.php/issaf

OWASP:
https://www.owasp.org/

PTES:
http://www.pentest-standard.org/index.php/Main_Page

NIST:
http://csrc.nist.gov/

Conclusion

These are some of the organizations and non-profitable organization providing manuals and guidelines regarding security Testing and PenTest.
You can refer to these sites while pentesting because these sites provide some very usefull guidelines must read for a pentester or an organization before conducting a testing session!

Any Questions?

You can contact me on Facebook
www.facebook.com/bhashit.pandya

My Email:
bhashitpandya@yahoo.com

Thank You!!!