Managing Penetration Testing: Pentest In Action!

Jyoti Raval
Staff Product Security Engineer
harness

Agenda

- ❏ Introduction
- ❏ What is pentesting?
- ❏ Challenges running pentests?
- ❏ Problems solved by MPT
- ❏ Why MPT?
- ❏ Tool demo live!

WhoAmI

I am Jyoti Raval, working as Staff Product Security Engineer with harness

Responsible for researching on new security trends and help secure product end-to-end

Application security enthusiast

Presented at BlackHat,DefCon, NullCon, InfosecGirls and OWASP.

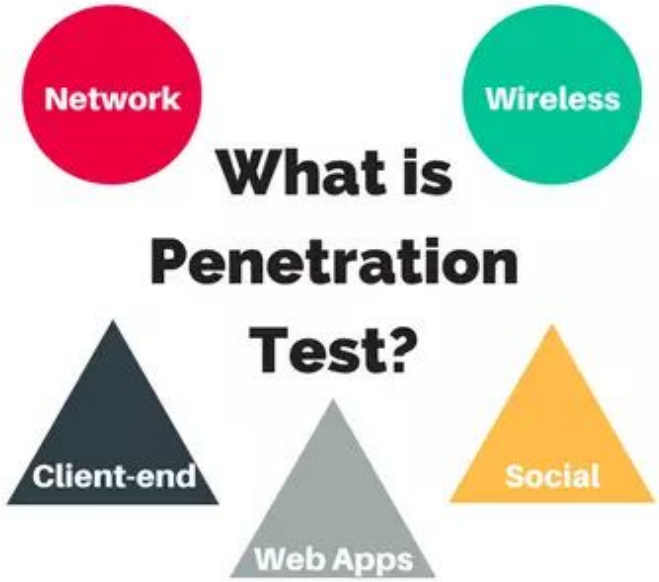
Author of tool - Phishing Simulation Assessment

OWASP Pune chapter leader and goes by jenyraval on github

What is Penetration Testing?

A penetration test, colloquially known as a pen test or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.

The test is performed to identify weaknesses (also referred to as vulnerabilities), including the potential for unauthorized parties to gain access to the system's features and data. [wiki]



Challenges running pentests?

- Lack of holistic view
- Pentest activity knowledge base
- Increasing number of pentests
- Different Dashboards
- Lack of analytics
- Lack of tracking and measuring capabilities
- No Automation
- Collaboration Inefficiency
- Lack of visibility
- Lack of holistic view
- Ad-hoc Processes
- Historical data analysis

Which Problems MPT Solves?

1. Asset database to know all organisation assets that are in pentest process. You can't secure what you are not aware of!
2. Tracking each pentest and activities in real time
3. Pentesting activity knowledge which comprises of what particular let's say application does, or the purpose of hardware that we are testing
4. When next pentester takes over the testing all they have to do is view the asset and associated information which is already there.
5. Time taken for each pentest
6. Issue status
7. Trend analysis of vulnerabilities observed during multiple pentestings

Why MPT?

It also has security pentest analytics which helps us not only track and view everything in single pane of glass but also

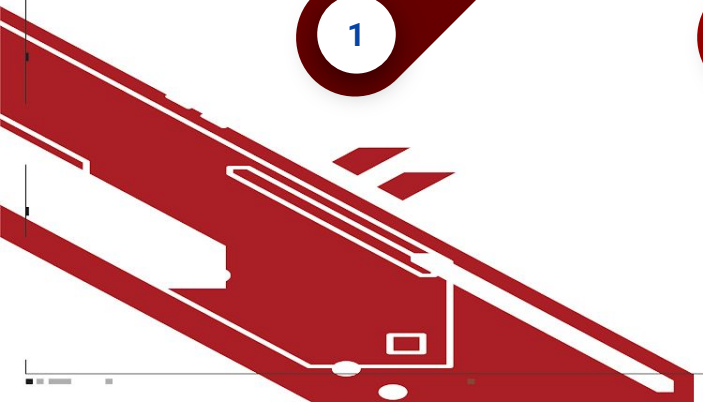
1. Finding improvement areas to boost pen tester productivity
2. Understand the current risk posture
3. Understand recurring issues
4. Average amount of time taken for each pentest v/s asset scope
5. Average high/medium/low fixing time
6. Most number of vulnerabilities fixed in a year

Why MPT? contd..

7. Class of new vulnerabilities reported
8. Developer trends
9. Open findings
10. Critical assessments
11. Asset health
12. Top pentester reported findings
13. Average busy time for each pentester

Tool Demo!

1. Open Source
2. Simple Installation
3. MPT: Pentest In Action running live!!



Lets Connect!

jenyraval@gmail.com

https://github.com/jenyraval/