The Cost of Pen Testing a Web Application

Abstract

With increasing cyber threats and breaches, every organization needs to be alert in order to safeguard their assets. To implement the most proactive approach, most organizations today opt for 'Penetration Testing', more popularly known as pen testing. While there is an increasing demand for this exploitative type of testing, there is a considerable amount of confusion in the industry regarding the differences between vulnerability assessment and pen testing. Hence, there exists an ambiguity around its pricing as well. A structured approach to understand the dynamics related to pen testing will help companies decide when and what kind of pen testing to opt for, and at what price.

Refocusing on Pen Testing

Cyber criminals and hackers employ a number of sophisticated tools and network attacks to penetrate enterprise systems. Since web applications can be the easiest target, it is essential to perform pen tests for it. This kind of testing is expected to go beyond the realms of traditional vulnerability assessment, and locate potential issues. While vulnerability assessment simply identifies and reports noted vulnerabilities, pen testing attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Although pen testing now gets its due importance, its specific applications and additional benefits are yet to be realized.

Since there is no uniform package for pen testing, quotations vary from US $1000–5000 per application. This variance in cost is alarming, and the reason is the absence of any structured approach for estimation.

Outlining the Estimation Framework

Cost is one of the key deciding factors for any enterprise before it signs up for a security solution. Our estimation model is based on three factors:

1. What is the motive?

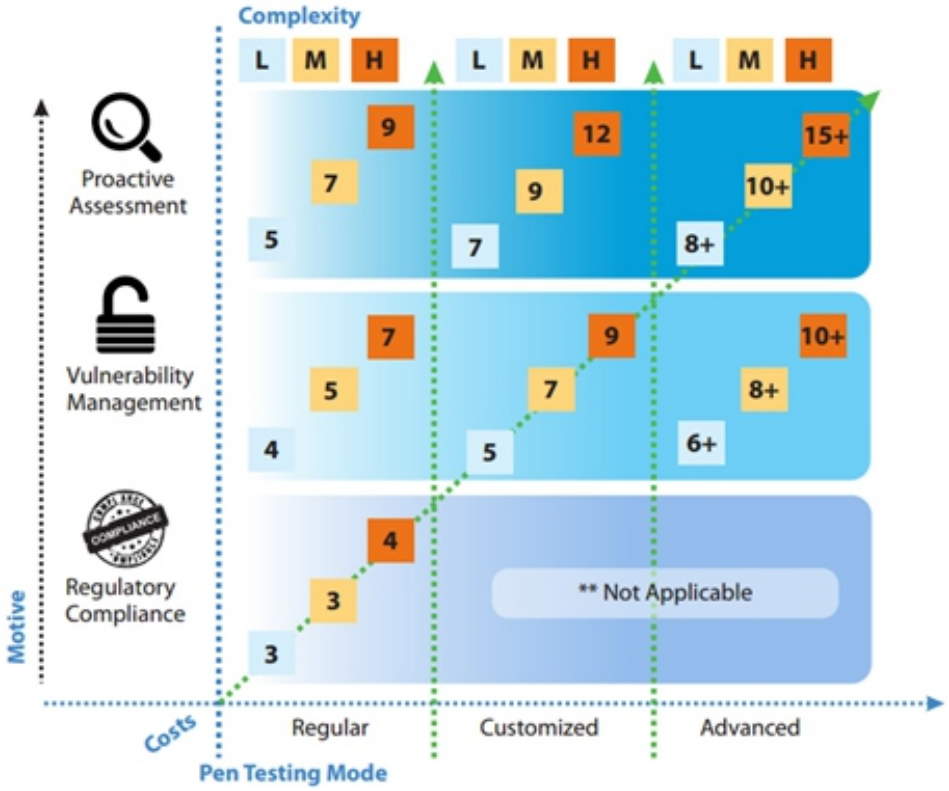
   An organization may face three types of motives: regulatory compliance, vulnerability management, and proactive assessment.

2. What is the application complexity?

   Web applications can be classified based on three levels of complexity: high, medium, and low.

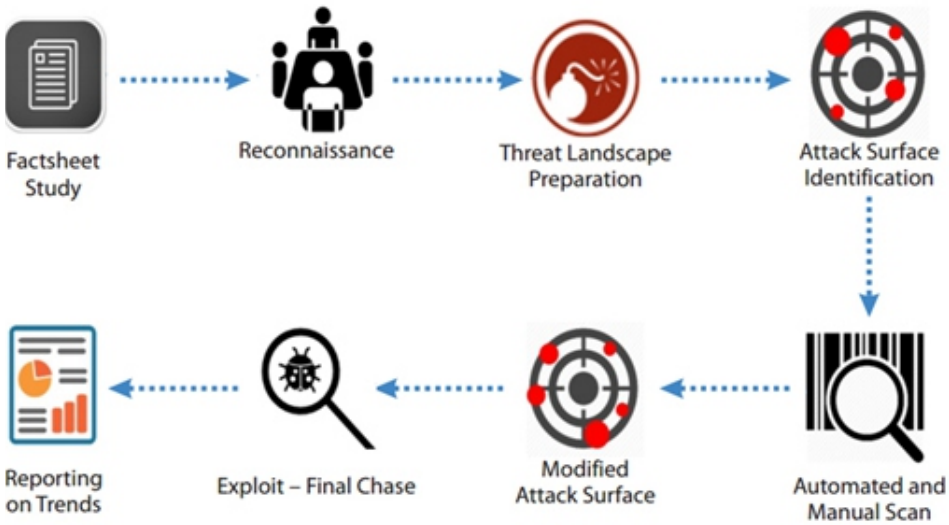
3. What type of pen test should be undertaken?

   The three recommended modes of pen testing are: advanced, customized, and regular.



Consolidating Estimation Framework Elements. (The numbers within squares are the tentative timeframes in 8-hour business days for a pen test in that category.)

The Pen Test Methodology



The Typical Flow of a Pen Test

A pen test remains a manually intensive exercise, thriving mostly on findings accrued from previously carried out assessments. It is generally performed by experienced resources who have a grip on the domain and technology of the app in question.

- The factsheet is created and then analyzed. It lays out strengths, limitations, and information pertaining to an asset or a group of assets, along with a slew of instructions to help analysts focus on a specific aspect of their assessment methodology. As the factsheet is prepared based on the CoEs experience, and not just previous tests, it is also referred to as a 'strategist's note'.
- Reconnaissance involves knowing as much as possible about the application from public sources. It includes studying how similar apps have fared in terms of vulnerabilities from the same database. With reconnaissance, the assessment team led by the strategist, draws up a threat landscape to attach appropriately identified soft zones of the app.
- The threat landscape is then further reduced to an attack surface where the actual assessment will be undertaken.
- These inputs are carried into the automated and manual vulnerability assessment scan to look for all the known yet critical vulnerabilities afflicting the system.
- The attack surface is then modified again, based on the automatic and manual mode findings.
- Then begins the final chase for suspected vulnerabilities and relevant cases are exploited to bring the issue to the forefront, wherever necessary.
- Finally, a report captures all the preceding points, findings, and trends to develop the final pen testing report.

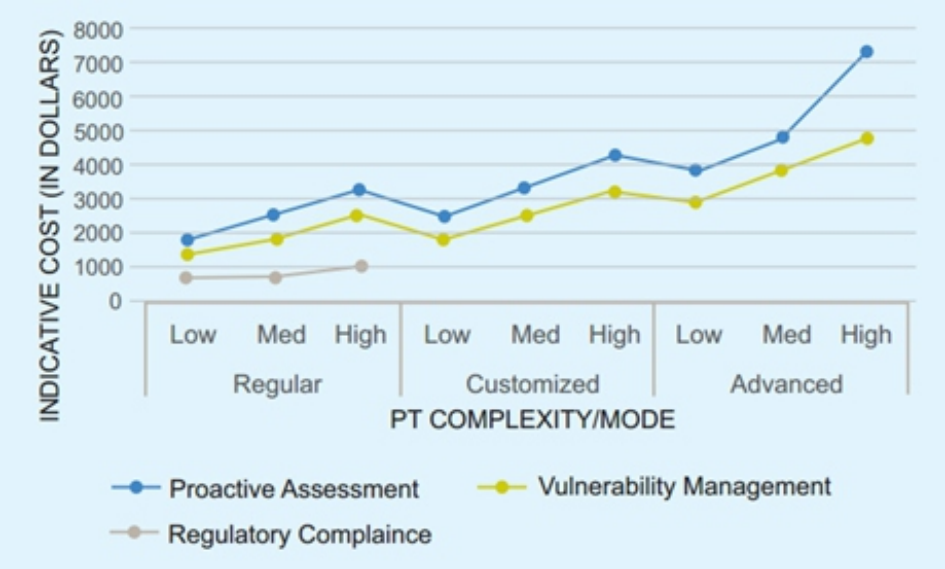
Building the Pen Testing Team

Contrary to the conventional notion, pen testing is not an individual exercise. It is best performed by a team of 2–3 people with varying degrees of experience per application, depending upon its complexity. The team should broadly comprise of:

- **A Strategist:** He is the most experienced hand of the pen test team who dictates the course of the assessment. The strategist also consults the back-end CoE and abuse cases best suited to a specific situation.
- **An Analyst:** This executive should be good with Open Source tools, malicious scripts, and breaching through validation controls.
- **An Ethical Hacker:** This is an optional function. The ethical hacker plays the ideal foil to the rest in the team in going after unimaginable leads.

Drafting the Pen Testing Cost Chart

A pen test is a very difficult assignment to complete. However, in most cases it is carried out with a deadline in mind. The advanced mode of pen testing is a continuously evolving exercise and thrives on run-time correlations made on emerging vulnerabilities that the team can come up with. The indicative cost chart for various modes of pen testing with diverse motives is based on industry experience, however, the costs do not include commercial licensing fees, and in the event these are in use they will surely increase the overall cost depending upon the tool selected.



The Indicative Pen Testing Cost Chart

Conclusion

A pen test should be best considered as an investment and not merely an expense head. When it is completed within a comprehensive vulnerability management program, it offers the promise of fortifying the application better as opposed to a traditional vulnerability assessment. While pen testing may seem a daunting exercise with the possibility of delays to deployment or disruption of data integrity, it does assure a better tomorrow for the organization. All sensitive applications should ideally undergo pen testing at least twice a year. Another important benefit accrued from pen testing is that it gives the organization real experience in dealing with an actual intrusion. The organization may indeed have all the important standards, best practices, and policies in place. However, until they actually have to deal with an attacker, they may not be certain as to how they should proceed. Pen testing brings in the state of preparedness for such unforeseen events.

About The Authors

Srimant Acharya

Srimant Acharya heads the Center of Excellence or Enterprise Vulnerability Management within the Enterprise Security and Risk Management (ESRM) business unit at TCS. With 15 years' experience in the software industry, and 6 years in the security domain, he describes himself as a developer by heart and security analyst by profession.

Contact

Visit TCS' Enterprise Security and Risk Management services unit page for more information

Email: Global.esrm@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Experience certainty. IT Services
Business Solutions
Consulting

TCS Design Services | M | 12 | 16