happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

A Hybrid Model for Penetration Testing: Leveraging the Benefits of both Automated and Manual Testing

Happiest People . Happiest Customers

Contents

Introduction

Everyone remembers Sony Pictures Entertainment's nightmare in late 2014. Attackers hacked terabytes of data after deleting the original copies from Sony computers. Recent estimates indicate that the incident has already cost Sony USD 15 million, and still counting.

With the burgeoning usage of networking technologies, data breaches have become common today. A recent study

conducted by the Ponemon Institute reported that the average cost of data breach to a company was USD 3.5 million in 2014, 15% more than the previous year. The high cost of data loss, business outage, and disruption in business processes, as well as the escalating costs of recovery from security breaches make it vital for organizations to have strong security measures in place.

One such widely implemented and effective precautionary measure is Penetration Testing (or pen testing as it is popularly called). The objective of a pen test is to determine if an application/network/infrastructure can withstand an intrusion attempt—it involves simulating an attack on your system, with the pen tester seeking to deliberately exploit exposed vulnerabilities. The pen test, thus, provides specific information on the flaws in an application or system, pointing to the data that could be compromised and the resulting business impact. This exercise enables you to explore multiple attack vectors on the same target. Pen testing works on the premise that hackers have a deeper knowledge of network vulnerabilities than the organization that runs the networks. And the pen tester seeks to replicate these 'attacks' and exploit your vulnerabilities.

Pen tests are conducted with knowledge of the organization, and a variety of tools and techniques are used to bypass security controls, pinpoint technical flaws in coding, and identify business logic vulnerabilities. The concluding step is the reporting and remediation of issues discovered during the test.

Automated Testing or Manual Intervention?

When it comes to penetration testing, there are any number of automated tools available in the marketplace—both the high-priced sophisticated lot, and their inexpensive counterparts that are just about adequate. However, the ideal pen test is more than just a series of automated tests ticked off on a checklist. The effective pen test goes beyond the technical to test business logic vulnerabilities as well. It studies the vulnerability of your entire system and not just isolated, discrete functionalities. In short, the ideal pen test is one that uses automated tools, but is led by human intelligence and insight. Automated tools for penetration testing are efficient and consistent, but complementing them with manual testing ensures complete coverage.

Comparing the Two

Combining the two offers comprehensive coverage, both breadth (automated) and depth (manual)

Automated tools can identify simple and well-known forms of the common technical vulnerabilities.

The more complex vulnerabilities, those related to application logic or security functionality design require manual intervention. Identifying and analyzing business logic vulnerabilities, for instance, require a skilled manual tester who can understand the logical flow. Consider this example—an application might direct the user from point A to point B to point C, where point B is a security validation check. A manual review of the application, however, might show that it is possible to go directly from point A to point C, bypassing the security validation entirely.

Combining automated and manual testing increases staff productivity. For example, if you assume a single security professional makes $100,000 per year and is spending 25% of his time on creating exploits and running manual pen tests, this represents an annual cost of $25,000. This cost can be reduced by automating the test and then supporting it with human intervention where required.

In addition, a tool typically tends to focus on a particular area of vulnerability or individual flaw, necessitating multiple pen testing tools. With manual testing, you can not only examine specific flaw categories, but also identify specific application vulnerabilities within the scoped domains. Further, automated testing tools cover certain vulnerability types and not all. According to the MITRE Corporation , automated tools cover only 45% of the known vulnerability types. Hence, the remaining 55% requires manual intervention

In addition, a tool typically tends to focus on a particular area of vulnerability or individual flaw, necessitating multiple pen testing tools. With manual testing, you can not only examine specific flaw categories, but also identify specific application vulnerabilities within the scoped domains. Further, automated testing tools cover certain vulnerability types and not all. According to the MITRE Corporation , automated tools cover only 45% of the known vulnerability types. Hence, the remaining 55% requires manual intervention.

Manual intervention reduces the false positives generated in automated testing results

Automated tests generally result in a high number of false positives. This then demands manual verification for false alarms, since false positives can lead to wasted effort in remediation. Ideally, an automatic tool can perform the bulk of the assessment, followed by human evaluation of the results in order to reduce the number of false positives.

Manual testing is 'safe' testing

Automated testing tools can only perform the regimen of tests designed. It normally does not take into account data damage, data loss, impact on application or other resultant scenarios. Context-dependent testing is possible only with manual intervention, where a tester studies the application in the context of its functionality and its interdependencies to obtain precise results. Any disruption to business processes resulting from a pen test can be controlled and rectified by manual testers.

Automated testing offers speed and efficiency

However, standalone manual testing is not exhaustive enough to uncover all vulnerabilities, especially where you require hundreds of iterations to identify patterns. Some smart measures and tools can improve a manual tester's efficiency, for example, by enabling the automation of a series of steps that, if undertaken manually, would be long-drawn and impractical. Or short code snippets could be run to test iterating logic or conditions.

Automated testing is more predictable and consistent because it does not depend on skill of tester

Automated testing results produces consistent results over time. There is close to zero discrepancy between two or more executions of the same test. It is fairly predictable. Manual tests, on the other hand, may be erroneous and are only as good as the expertise of the tester.

Tools are updated faster than human knowledge and skill

Remember that a manual tester is only as good as his skill and expertise. Unless he constantly updates himself with knowledge of new threats, his testing will not be exhaustive and complete. In this, he can be ably assisted by sophisticated automated tools that are regularly updated to combat new threats. Automatic tools are patched regularly with new technologies, techniques, or additional functionalities.

While these updates do depend on the vendors, a pen tester learning new techniques and feeding the test methodology back to the system can compensate for the wait time. In this way, one kind of testing can constantly make up for and support the other.

Manual and Automated Testing at a Glance

Parameters	Manual testing	Automated testing
Testing process	Labor-intensive and time consuming	Fast, easy and efficient
Coverage	Depth	Breadth
Safe testing	Contextual and hence safe	Context independent and unaware
Training	Invest in training to learn techniques and skills	Easy to use
Logging/Auditing	Slow and cumbersome	Automatic tracking and management
Determining ROI	Often difficult to measure the productivity and efficiency of a manual tester	Easy measurement and comparison of automated testing results

Conclusion: Not Automated OR Manual, but Automated AND Manual

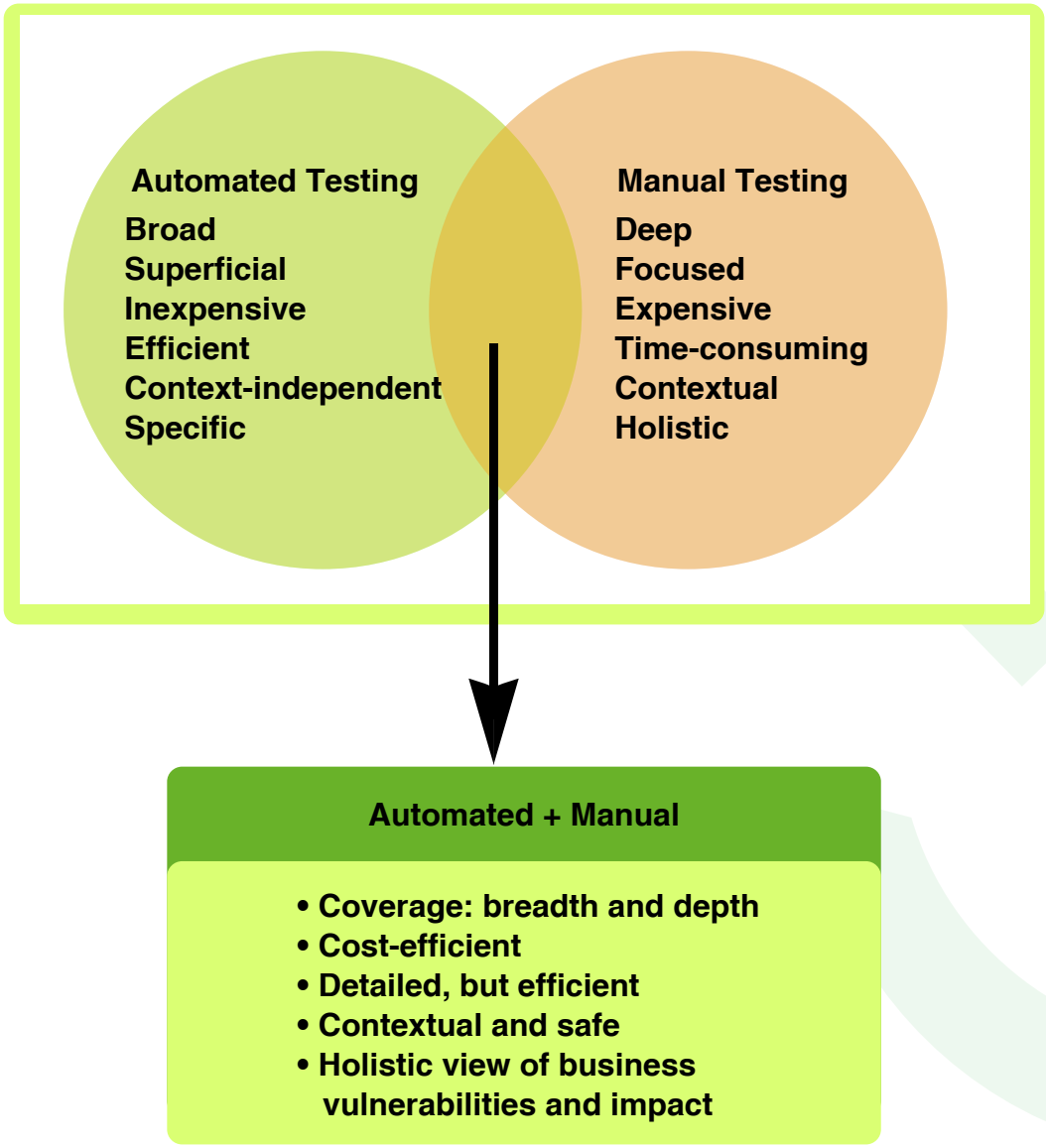
Banking industry is going through a phase of commoditization. In today's scenario, differentiated and delightful customer experience has become more important than just providing financial services. To grab a bigger piece of the cake, banking industry has to understand the unstated needs of the customer the way airlines understands the preferences of the frequent flyers or the retailers understand the likes/dislikes of their customers, without even taking direct feedback of the customer.

Each and every day, new devices / technologies are providing various customer touch points. Every time customers touch a computer or a screen, they are providing an information trail and it's banks' responsibility to understand how they use this trail to move their bottom line upwards. Traditionally, banks spent most of their efforts, time and money on transaction execution, which is nothing but has

become a very basic feature of their overall service. While providing expedient, consistent and precise transaction processing ability is still critical, we believe that banks can learn from how retail-ers see the customers' journey through an Omni-channel lens. Banks now need to rethink the way customers are being valued, may be from the angle of the industries that greatly value customer experience.

A tightly coupled multichannel may provide a share of customer's pocket, but successful implementation of Omni-channel can surely increase the size of the share though competitive advantage and also can help them to retain the same share for a longer period of time.

Millionaires aren't the only ones who want to bank whenever or wherever they want, irrespective of the branch location or the business hours. Customers from all generation, income groups, and countries could make a transaction online one day, and another day, the same transaction through mobile or ATM - or they could start a transaction on any of these channel then continue on another and finish it on different channel. Multichannel gives the flexibility to hop between channel, but not the continuation of the transactions among multiple channels. So, this represent a remarkable challenge for the financial institutions, which are often involved in multiple types of banking such as retails, finance, corporate, mortgage etc...



As the figure above shows, the ideal pen test is one that innovatively combines automated and manual testing techniques, leveraging the benefits of both, and combining together to achieve greater efficiency and accuracy than when individually performed. This is an evolving model assuring coverage of all vulnerability areas, zero false positives, higher efficiency, and accuracy. Ensure that you pen test your systems and applications regularly—new vulnerabilities can creep in at any time, with software updates, evolving threats and new methods of attacks; and you do not want to discover these vulnerabilities when you are under attack!

About the Author

Manoj Rai

Manoj Rai has around 14 years of IT experience in Enterprise Applications, Mobile and Infrastructure security. Has rich and diverse global experience in leading large engagements and building deep technology expertise in security testing domain. Manoj is a Bachelor of Engineering in Computer Science with MBA in Systems and Executive Delivery Program from IIM-Bangalore. A regular speaker on various technical subjects like Ethical Hacking, Mobile security, Secure SDLC and Cloud Security areas in CISO platforms, OWASP, BLUG, NULL etc. Has been a regular blogger and has published white papers on threat management and best practices in various social groups.

Happiest Minds

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

To know more about our offerings. Please write to us at business@happiestminds.com

E-mail: business@happiestminds.com

Visit us: www.happiestminds.com

Follow us on