Is Human Element Still Relevant In The Age of Automated Pentests?

By Bhavya Mishra · 17-07-2025

Introduction

* In the world of cybersecurity, knowing your vulnerabilities before being exploited is key, and that’s where penetration testing comes in. We can understand the application of penetration testing with the analogy of buying a house. When we are buying something as big and important as a house, we make sure to check for any potential issues or hidden problems with the house. For that, we consult specialists for meticulously identifying whether our house purchase is feasible or not. In a similar manner, when a company establishes a network, application or a website they too need to know about any potential risks that can affect their operations. For this they consult the cybersecurity specialists which deploy the strategy of penetration tests. Penetration tests are like a fire drill, the mock test conducted in the pentests help to discover some weak points from where potential security threats can arise. This checking can be done by both manual pen tests and automated pentests. With the rise in the complexities of the new age technologies, a shift from the manual tests to the automated systems is seen.
* Do you wonder if we can find every security flaw with just a push of a button? The reality is much more complex. Through this blog you will understand the concept of penetration tests and how automated systems are transforming the field of cybersecurity. Automated systems are used in cybersecurity to handle large volumes of data and for their ease of completing complex tasks. Instead of deploying a skilled professional to undergo the meticulous task of probing the company's defenses to track down the vulnerabilities, automated pentests work on the repetitive tasks with far more efficiency. Considering the rising computational costs alongside the increasing complexities of networks and websites, automated systems emerge as a much needed solution. But this raises a crucial question: are automated systems capable of replacing the manual approach altogether or is the need of the human touch still felt in the high-stakes world of cybersecurity? Or perhaps a combined effort of both is optimal? Let’s embark on the journey to know more together.

Contents

* [1. The Automated Edge: The Final Frontier In Finding Every Flaw?](#_956k9fyubr15)
* [2. The Human Factor: Asset or The Most Significant Vulnerability](#_7ma8ajxvcfoa)
* [3. The Best of Both Worlds: Forging A Hybrid Future in Pentesting](#_byn42vz1t57n)
* [Conclusion](#_g498lvlz7agd)

## 1. The Automated Edge: The Final Frontier In Finding Every Flaw?

An automated system is a combination of hardware and software designed to work with minimal human interventions. They are used to perform repetitive or dangerous tasks to save time and achieve efficient results. A classic example of the automated system is the automated thermostats installed in smart homes that adjust the room temperatures according to a basic schedule or motion sensors. The traditional penetration testing couldn’t keep pace with today’s complex web applications, APIs and infrastructure. This prompted a necessary shift from the older methods.

* Automated tools are efficient in conducting complex scanning tasks in just a fraction of the time that a specialised pentester would require.
* The cost effective nature of automated tools positioned them as a compelling alternative to an entire team of specialists.
* No matter the level of expertise, a chance of human error persists. Using an automated tool ensures the following of the established procedures meticulously.
* At the end of the process, the report generated by the system is very helpful in tackling all the vulnerabilities, as they provide a clear and concise road map.

### **Automated penetration testing process:**

* The process of both humanised and automated approaches are very similar. Both start with defining the scope or aim of the pen test. For this, the system gathers all the necessary information it can get.
* Then the system employs a variety of scanners like vulnerability scanners which initially identify the weak points and analyse their potential impact. The various scans ensure that the faults of the entire system are properly assessed. The automated systems gain essential information to easily detect the known vulnerabilities.
* After the identification of weak points, the system mimics a real world hacker attack to further identify the extent of the weak point and essentially generate a detailed outline of how vast a vulnerability can be exploited.



### **The Power and Pit falls: The Reality of Automation Security**

While the automated system is a helpful tool, it isn’t a perfect one.

* Automated systems generally flag the harmless vulnerabilities too, which can result in wastage of time for tackling them.
* The automated systems lack contextual understanding. Let’s say a medical company uses the automated system, then the scanner won’t specifically search for vulnerabilities in the context of the company. Every approach of the pentest is a black box approach with the automated systems.
* The complex vulnerabilities are difficult for the automated systems to verify. The broad complex vulnerabilities require the work of a specialised pentester.

### **The Road Ahead: What will automated pentesting look like tomorrow?**

The rapidly evolving field of automated penetration testing field of automated penetration testing gives way to new possibilities and shows the scope of more technological advancements.

| **Recent Trend/ Technology** | **Advantages** |
| --- | --- |
| AI and Machine learning techniques | With the integration of AI and machine learning techniques, we can modify the system to analyse the potential risks even before the hacking. |
| Security Information and Event Management (SIEM) systems | By the advancement of automated systems, the procedural work could be linked together and thus the entire pen test can run on its own, minimising the role of humans. |
| Contextual Orientation | If the systems are designed to be context oriented, then the potential downsides of automated systems can be rectified. |
| Cloud Based Automation | It is a nice alternative being considered for the ease of integration, cost effectiveness and completion of complex tasks with efficiency. |

## 2. The Human Factor: Asset Or The Most Significant Vulnerability

Human behaviour is a complex but intriguing concept that can make or break the success of cybersecurity measures. While developing a website or network, it is quite general that factors like security are often overshadowed by other factors. This is a cognitive bias which occurs in professionals who consider simple tasks as familiar and ignore potential weak points. Via small assistance to complex judgements, cybersecurity professionals( here referred as pentesters) can implement modifications to rectify all the security threats. The penetration testers are very skilled professionals that are able to identify the fine and often unnoticed weak links as potential security threats.

### **Different Roads Same Goals: A comparison of the automated and human pentest process**

According to the need of the test, specialists describe the various pen tests as namely- application pentests, network pentests and hardware pentests. Although some similarities in the procedural flow of the pentest, both the systems seem to show some significant differences:

* The scope defined to the expert pentester is very detailed and client driven. The contextual knowledge is expressed with utmost clarity and in comparison to the automated system, the scope is more precise.
* The information collection performed by experts is a very detailed one, although a time taking task, the expert ensures to correctly collect all the active as well as passive information possible to identify each and every point of vulnerability.
* For scanning the networks, the pentester utilizes automated tools. For instance, tools like Medusa and Hydra are bots which test various passwords till they crack the correct one. Another widely used automated tool is Nmap which is a port scanner that scans for open ports that a hacker can potentially use. Analysis of these tools are essential and significant helpers of the entire process.However, they do not stop here, they further interpret the scanning results correctly and apply logic and human reasoning to find the complex logical flaws.
* The pentesters are easily able to mimic the hacker’s activity more efficiently than an automated system and therefore it can effectively understand the vastness of a weak point.
* Unlike the automated system, the report of the expert pentester is very detailed and it clearly describes how each problem can affect the business and what can be the further ill effects caused by the hacker’s attacks.

### **Comparative analysis of both the systems:**

| Feature | Automated Pentest | Human(Manual) Pentest |
| --- | --- | --- |
| Methodology | Automated systems have a detailed list of instructions and knowledge that they strictly follow. | The expert pentesters use additional skills such as creativity, logical thinking and intuition to enhance their testing. |
| Speed | The entire process is very fast and highly efficient as the multiple scans of even the complex systems take a very short time. | The scanning speed and the overall process is comparatively more time taking as the expert builds their own testing plan on the basis of gaining knowledge. |
| Creativity | The automated system follows little to no creativity and stick to the confined known knowledge provided to it. | High level of creativity and proficient method to identify unique flaws and weak points that are unknown at the time but can pose a potential grave threat in the future. |
| Variety of Vulnerability Detected | Excels in detection of known vulnerabilities | Can also detect the unknown vulnerabilities, complex business effects and creative attack plans that hackers use. |
| Report Generated | The report is very standard and constrained. | The report is highly contextualized and contains additional information about business impact assessment and possible tailoring advice. |
| Positives | The system has the possibility of generating false positives as they flag the non harmful errors too. | The approach is highly adaptable hence the probability of a false positive is less likely. |

## 3. The Best of Both Worlds: Forging a Hybrid Future in Pentesting

While learning more about both the systems, the confusion of selection between the two is drastically increasing. So, how to make the choice? The correct option is- selecting both. The combined effort of both can cancel out each of their difficulties. The automated systems can work on redundant tasks with record speed but they lack creativity, intuition and contextual understanding all of which can be easily covered by the human system of penetration testing. By the alarming rates of modern cyber threats, the idea of removing the human element entirely from pentests is a dangerous one.

* The Creative Challenge: The automated system does not have expertise to mimic how the human hacker would think to approach a network or website. Think of it as a light switch, which can perform only a constraint set of tasks, that is to turn the light on or off. Similarly, the automated system can only work on the basis of the constraint set of information available to it. Thus the creative ways by which the “human” hacker can breach defenses are not perceived by it. It takes a human brain’s out-of-the box thinking which can uncover the true extent of a hacker’s capability.
* Moreover, to identify the weak points which have the potential to be harmful to the network in the future are often not noticed by the automated system sticking to the known vulnerabilities.
* The filtering of the non essential vulnerabilities are done by human experts as they flag them as threats or harmful errors.

The overall judgement, expertise and experience of a human expert pentester is very essential for the proper conduction of the test. A combined effort of both the systems is the only optimal option to effectively detect security threats.

### **Head-to-head comparison: automated and human hackers for pentests**

An exercise to identify how a human pentester and automated pentester works was conducted by [Fidelis](https://www.cybersecurityintelligence.com/blog/human-vs-machine-attack-response-3288.html) which pointed out some similarities and differences which further explains their differences:-

* Human pentesters approached the problems as a detective, they looked for unstructured and thus searched for vulnerabilities and credentials to hack into the system.
* In contrast, the automated system opted for the structured approach. This is a fast but not a very adaptable approach.
* The similarity in both approaches were the overall procedure, since both attackers looked for the credentials as a weak point.

The activity concluded that we require a combined effort of both. The automated machine is required for a faster and more efficient effect. Additionally, the skilled pentesters are required to meticulously find unique flaws that automated tools can underlook. Hence both systems are not to be considered as competitors, rather they are partners in achieving optimal results.

## Conclusion

### **So what should you choose: Manual or Automated?**

As a person in the security team of the company responsible for the selection of the system, some essential points are there for you to consider:

* Complexity: Complexity of a system or network determines its overall cost. You should consider whether the system environment involves multiple layers and interconnected systems that require a higher amount of effort and time. Hence to reduce its cost, an automated approach is more feasible.
* Scope: When evaluating the scope of the system, one can determine the main requirements and by addressing them you can choose the better system.
* Procedural Knowledge: When you have detailed insights about both the systems, then only you can make a well informed decision.
* Expertise: You should also evaluate the experience level of all the options available to you. Depending upon the work, an apt level of expertise is required, hence valuable decisions such as security should be done after considering the level of expertise and experience of both the human and automated systems.
* Post-Testing Assessment: Consulting reputable cybersecurity firms for advanced guidance is a good step to ensure that you get the work worth your penny. Certain details that we often miss are covered by such firms, such as evaluating the complexity of the post testing assessment report which provides the road map. Thus their expert opinion is generally transparent advice about the prices and optimal choices, catering to your needs.

The ultimate argument comes down to one factor, automated machines are not yet advanced enough to replace the human brain’s creative, logical and intuitive thinking involved in the entire process. The ability to understand business logic and contextual clarity, applying their own anticipation of the threats and creatively uncovering the extent of weak points eventually is lacking from the automated system. My own opinion is that the future of pentest is not about putting both the systems against each other, rather more focused upon building a combined effort. The machines are not added to remove the human element, rather they are included to enhance the overall working of the pentests.

# Short answer section:

1. If you had to plan content for SaaS pentesting products aimed at security engineers, how would you approach different stages of the buyer’s journey?

Answer: For making content of a SaaS pentesting product specially catered to security engineers, I would directly focus on their pain pointers to grab their attention. By offering detailed technical guides and solution oriented case studies, I would direct their attention towards how my product is special in addressing engineering challenges such as API security or CI/CD integration. Maintenance of transparency about the entire cost, providing additional advice and including additional benefits like free trails, are some tiny focal points that would eventually seal the deal.

1. What are some SEO best practices you’d follow when writing an article?

My approach towards writing an article is always to start from the roots, learn and assess everything before framing the article.  
A. By prioritising extensive keyword research, I identify catchy terms to attract the target audience.   
B. By ensuring that my article’s structure(H1,H2 tags) are incorporating my keywords effortlessly, I attain an engaging and informative article.

C. Additional tables, fun notes and visually pleasing images are incorporated in my process to make the article more engaging.

D. Apart from these, I focus on making my content shareable so as to make it more feasible for locating.

1. How would you explain this internship to a mentor or peer two years from now if it turned out to be a turning point in your career?

As a student of Btech, I have learned quite a vast variety of topics, either related to the medical field or the technical field, but with the help of the internship at Astra, I was offered the golden opportunity to deep dive into the core concepts of cybersecurity, an emerging and essential field. The internship helped me in perceiving SaaS pentesting with a content perspective and helped me learn about how the future of cyber security looks like. The internship helped me gain experiences of communicating with my content about such a complex domain. The insights gained about the future, ignited a passion of tech and a curiosity for security, thus truly impacting my career path.