Automated Penetration Testing

Identify vulnerabilities in your systems and improve security posture to avoid attacks.

Automated Penetration Testing for Digital Businesses

The adoption of digital and cloud technologies has significantly increased the attack surface for businesses. With this phenomenon, businesses want to ramp up their security measures. One way to do that is by identifying weaknesses in the IT infrastructure.

Attackers prey on vulnerabilities because it makes their job easier. Hence, businesses must see their attack surface and security posture from the attacker's standpoint. Penetration testing is an effective way to do so.

Penetration testing involves simulating attacks on your infrastructure, including networks, systems, and applications, to identify vulnerabilities within the system. However, manual testing alone may prove inadequate for expanding businesses or those managing large, complex, and dynamic infrastructure.

Automation offers a solution, streamlining the testing process and enhancing effectiveness.

Penetration Testing, when automated, becomes less time-consuming, scalable, accurate, and covers infrastructure better. Automated Penetration Testing helps businesses detect vulnerabilities faster, gauge the impact of vulnerabilities, adhere to compliance requirements, save costs, and take a proactive approach to cyber security.

With the use of technologies like Artificial Intelligence (AI) for scanning, and automation for streamlining the end-to-end testing process, businesses reduce their time and effort in remediating the vulnerabilities. This enables businesses to mitigate security risks before bad actors can exploit them. Automated Penetration Testing minimizes the impact of security incidents on the business.

When should you choose Automated Penetration Testing?

Consider Automated Penetration Testing when you want:

Proactive vulnerability detection: Identify and address security vulnerabilities within the network, systems, and applications to reduce the risk of data breaches and unauthorized access.

Faster and efficient testing: Streamline the testing process, saving valuable time and resources compared to manual methods. Conduct comprehensive assessments more frequently and efficiently to ensure continuous security monitoring without extensive manpower requirements.

To meet compliance requirements: Meet regulatory compliance standards such as GDPR, NIS2, HIPAA, PCI DSS, and others. By regularly testing the security infrastructure, you can ensure compliance with industry regulations and avoid costly penalties for non-compliance.

Comprehensive coverage: Offer comprehensive testing coverage across various attack surfaces, including network infrastructure, web applications, and endpoints. Identify vulnerabilities across the entire IT environment, reducing blind spots and enhancing overall security posture.

Scalability: Tailor testing parameters to your specific requirements. Whether it's scheduling tests, defining testing scopes, or selecting target systems, you have the flexibility to customize the testing approach to suit your unique needs.

Capabilities of Automated Penetration Testing

▸ **Advanced scanning:** Faster and precise
▸ **Automated reporting:** Actionable insights
▸ **Continuous monitoring:** Real-time detection, response
▸ **Integration with existing security:** Minimal disruption
▸ **Customizable testing parameters:** Meet unique needs

··T··Systems·

Let's power
higher performance

How we can help you get started

After understanding your business objectives, we'll target one or more systems for penetration testing. This could be network security, web application, cloud security, device security, and more.

Stages of our testing:

Reconnaissance
Automated tools gather information about the target network, systems, applications, entry points, and vulnerabilities.

Scanning
Scanners are systematically deployed to probe the target environment for open ports, services, and vulnerabilities.

Enumeration
Automated tools compute system details, such as user accounts, resources on the network, configurations, etc. to further refine the scope of potential exploits.

Post-Exploitation
Gathering further information, escalating privileges, and maintaining access to compromised systems.

Reporting
Detailed report of findings from the testing. This detailed report includes the severity of identified issues, recommendations for remediation, and prioritization of actions to address vulnerabilities effectively.

Benefit from T-Systems Automated Penetration Testing

- **Avoid severe attacks:** Through the identification of vulnerabilities, your business enhances overall security, thereby reducing risks and protecting sensitive information.

- **Cost savings:** By streamlining testing processes, you can reduce manpower needs, saving time and resources for continuous monitoring.

- **Regulatory compliance:** By meeting standards like GDPR, NIS2, and other regulations, you avoid penalties and maintain trust with stakeholders.

- **Improved incident response:** By providing insights into vulnerabilities, you enable prompt remediation to minimize security risks.

- **Reputation protection:** By demonstrating a commitment to cyber security, you enhance trust and credibility, protecting brand integrity.

Why T-Systems?

- We have a team of security professionals with experience and certifications from Offensive Security Certified Professionals (OSCP), Global Information Assurance Certification (GIAC), and more.

- We offer detailed reports with recommendations and insights. Also, get an executive report for a high-level summary.

- We follow industry best practices and frameworks such as MITRE ATT&CK to stay updated with the latest threats and techniques.

- You get options to choose one or more types of testing: Black Box, Grey Box, & White Box Testing.

- Our teams use advanced tools to suit your environment and diverse testing scenarios.

- We use adverse simulation capabilities for scenarios such as weak credential exploits, endpoint security tests, active directory testing, data exfiltration, ransomware simulation, etc.

- Your business operations are unaffected due to testing.

- We also offer comprehensive security consulting to further map your security journey.

Find security gaps in the infrastructure today. Choose from our packages to meet your unique business needs.

Start a conversation with us today.

Expert Contact
Andreas Pecka
Head of International Expert
Sales & Pre-Sales
Cyber Security
a.pecka@t-systems.com

Contact us
www.t-systems.com/contact
cyber.security@t-systems.com

Published by
T-Systems International GmbH
Hahnstrasse 43d
60528 Frankfurt am Main
Germany

T··Systems

Let's power
higher performance