Penetration Testing

autodata

Ensuring your security controls stand up to an ethical hacker mimicking real-life attack techniques and tactics

CREST

CHECK
IT Health Check Service

What is a Pen Test?

Penetration (aka pen) testing is more important than ever to ensure that your critical data-protection efforts are effective.

Pen testing involves an external cybersecurity consultant attempting to "ethically hack" your system to identify then aim to exploit existing vulnerabilities in order to show how well your organisational defences would hold up against a real attack.

Vulnerabilities can easily be used by a malicious attacker to disable infrastructure or steal sensitive, valuable or secret information. Some of the most common vulnerabilities include poor configuration, inadequate patching policies and inappropriate trust relationships.

There are three stages that build upon each other to ensure a properly scoped and delivered pen test (see overleaf)...

Your IT systems hold data which is critical to your organisation. You may believe your system is secure, using assured solutions and appropriate security procedures, but are you sure it has been correctly configured and does not have vulnerabilities?

Autodata offers a number of security assessments services to help you understand which threats and vulnerabilities pose the most risks to your organisation due to infrastructure gaps, people, environmental issues or third-party exposure. All organisations should regularly conduct both internal and external assessments on their infrastructure, networks and applications.

External Infrastructure Assessment

The **External Infrastructure Assessment** is performed **outside** the organisation, mimicking a hacker attempting to gain access to sensitive information by targeting your public-facing profile and architecture. Testers attempt to access a target node, gain identity credentials and then deny and disrupt the service.

The objective is to test your current security posture and the state of your internet-facing systems in response to what an attacker might initially implement prior to launching an external attack.

Prior to testing we investigate your current internet profile using non-invasive techniques such as domain-based discovery, open-source vulnerability checks and bouncing email messages to determine the location of mail servers.

Internal Infrastructure Assessment

The **Internal Infrastructure Assessment** is performed **inside** the organisation, mimicking a disgruntled employee or other individual that has successfully gained access to sensitive information. Testers attempt to gain extra identity privileges and defeat auditing, detection and other security mechanisms such as access control.

The objective is to identify which internal infrastructure elements (email, databases, systems) are vulnerable to attack, enabling you to understand the potential impact posed by individuals existing inside your internal network.

All IP address ranges for the assessment are required prior to the start of testing and all devices deemed in scope are enumerated to ascertain that they are responsive and alive.

bsi ISO/IEC 27001 Information Security Management CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

256-260 Old Street, London, EC1V 9DD
t. +44 (0) 20 7749 7949 | e. sales@autodata.co.uk

Penetration Testing

1. Discovery Stage

Identifying known and potential vulnerabilities and/or unpatched or misconfigured systems.

Many tools and techniques are used for this process depending on the environment, infrastructure, application and assessment type.

This stage provides the attack surface of the infrastructure or application, allowing a tester to target weak areas first and ensure coverage is as complete as possible.

2. Assessment Stage

Taking the information identified in the Discovery Stage and applying manual effort to validate findings and investigate further areas of interest, such as confirming that encryption conforms to current best practices or that application cookies are secured and resist tampering.

3. Exploitation Stage

Once a vulnerability has been identified and validated, the final stage is to attempt to exploit it. This is conducted in accordance with predetermined rules of engagement.

This stage comprises manual attempts to exploit all vulnerabilities identified within your infrastructure, escalating privileges, gaining control of the network, and stealing sensitive data.

The real value of a penetration test is delivered in this stage and reveals what it would be possible for a real-world attacker to achieve.

Web Application Pen Testing

External facing web applications used by businesses are by their very nature available to all via the public Internet. Their complexity and availability have made them an ideal target for attackers and there have been many publicised data breaches that have been caused by insecure web applications.

Protecting these applications from new threats is a constant challenge, especially for developers who may not be security aware and typically working toward a performance deadline. Web Application Penetration Testing is therefore now a critical part of your security strategy to ensure your public facing applications are free from security risks. As a result, various regulatory bodies now mandate that Web Application Testing be performed regularly within your infrastructure.

Web applications can use a variety of technologies and development frameworks, so the exact technical approach to each application may vary, however our testers follow the OWASP Web Application testing methodology as closely as possible examining certain fundamental areas including: Public Information, Authentication, Authorisation, Session Management, Input Validation/Sanitisation, Business Logic and Web Server Configuration.

Mobile Application Pen Testing

Mobile applications are becoming increasingly complex, with larger threat landscapes and more personally identifiable and business critical data being stored. Insecure applications may result in sensitive data being exposed to other applications on the device, with the ability to trigger application components to perform malicious actions amongst other attack vectors.

Mobile Application Penetration Testing can help alleviate risks by identifying vulnerabilities that exist on your mobile applications in both IOS & Android Operating Systems. Applications typically make use of an API to send and retrieve data from the server, so this is a focal point of assessment with our full API methodology being covered.

Our Assessment looks at mobile applications at a storage level by reverse engineering the application package and viewing the database and configuration files to check for misconfigurations or missing core security defences such as root detection, SSL pinning and code obfuscation.

The source code of the application will be analysed to look for misconfigurations, hardcoded credentials or keys. The application level will be analysed for weaknesses such as weak passwords policies, insecure change password functionality and extraction of data from the application.

Services, broadcast receivers and activities will be tested in an attempt to trigger these outside of the normal business logic of the application. This often finds authentication bypasses and the ability to interact with the application and its data in a malicious way.

256-260 Old Street, London, EC1V 9DD
t. +44 (0) 20 7749 7949 | e. sales@autodata.co.uk

Penetration Testing

Whitebox (Authenticated) Testing targets your underlying security with the full knowledge of your IT team, sharing network diagrams, IP addresses, system configurations and access credentials with the testers. This allows for 'role-based' testing, acting as various individuals in or connected to your organisation.

Blackbox (Unauthenticated) Testing mimics a real hacker attempting to gain unauthorised access to obtain and exfiltrate data. It evaluates the underlying technology, people and processes in place to react to attacks. Testers are not given prior knowledge of the organisation or architecture.

Greybox Testing lies between black and white. Testers are provided with some knowledge in certain areas defined in advance to ensure adequate testing coverage and depth whilst controlling time and budget requirements.

Client Testimonial

"The results of our Autodata pen test surprised me in a good way. We'd used another testing supplier two months earlier for the renewal of Cyber Essentials Plus and they had failed to highlight critical and high risks, and most of the medium risks.

I am pleased we have made our perimeter more secure by addressing the areas of weakness exposed by Autodata. I was also pleased to receive the report so swiftly as it had taken the other supplier several weeks."

SIMON PARSONS
DIRECTOR OF IT OPS, CITYSPRINT

How regularly should you Pen Test?

Penetration testing should be viewed holistically as part of your broader information security program.

It should not be thought of as a scheduled, occasional, tactical activity but instead considered as part of a larger lifecycle of critical data-asset protection and an exercise in continuous learning that mitigates risk.

We recommend that our customers perform a pen-testing exercise every six months or less. However it is up to an organisation to identify the milestones that should instigate a retest of its information security.

Most vulnerabilities we expose are due to poor configuration and inadequate patching policy or process. New features can also present new vulnerabilities e.g. a desktop or operating-system refresh, a router that provides guest WiFi access, or a web application enabling employees to remotely access data.

Why is it important to use external Pen Testers?

Firstly, outside experts can recommend the best ways to test your infrastructure and applications, based on what information your organisation wants to protect and whether it is seeking to gain any certifications or meet specific compliance standards.

Secondly, external penetration testers are trained to think and act as if they were real-world malicious attackers, poking holes in information security and finding vulnerabilities their clients simply won't. They are highly knowledgeable of all current software and operating-system vulnerabilities and misconfigurations as well as the common mistakes made when installing, configuring and maintaining hardware.

If a pen-tester can gain access to your critical data assets, then so can a hacker. The recommendations that come from pen testing can remediate the areas where existing cyber security measures have fallen short.

Why Pen Test with Autodata?

- Our services are Check, CREST, Cyber Essentials Plus and ISO accredited
- 50+ testers holding specialist industry qualifications such as CCIE, CISSP and CEH providing a huge pool of knowledge to call upon
- High service level with full project management and daily feedback
- Full visibility of vulnerabilities in real time and efficient reporting via our online portal
- Free retest of up to 5 vulnerabilities within 12 months
- Numerous clients providing positive feedback about our services: See our Autodata Cyber Security Assessment References

256-260 Old Street, London, EC1V 9DD
t. +44 (0) 20 7749 7949 | e. sales@autodata.co.uk