Penetration Testing

autodata

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

What is a Pen Test?

Penetration or 'pen' testing involves an external cybersecurity consultant ethically attempting to identify and exploit existing vulnerabilities to fully understand how your organisation's defences would hold up during an actual attack.

Vulnerabilities could easily be used by a malicious attacker to either disable infrastructure or steal sensitive, valuable or secret information.

Common vulnerabilities include poor configurations, inadequate patching policies and inappropriate trust relationships.

There are three stages to a pen test that build upon each other to ensure a properly scoped and delivered service:

1. **Discovery**
2. **Assessment**
3. **Exploitation**

Penetration testing is more important than ever for organisations to ensure their critical data protection efforts are effective.

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 any 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.

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 etc) 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.

1. **Discovery:** Use automated and manual tools to scan and locate devices and services within the agreed target IP address ranges. This creates a list of potential targets for further assessment and identifies all devices and active services across the agreed scope to highlight potential vulnerabilities.

- TCP and UDP Port Scanning: NMap is generally used for this test
- Service Identification: employing various techniques (such as RAS, VPN, Telnet, SSH, R-services, SNMP, TFTP, NFS, Active Directory services, HTTP, HTTPS, MSSQL) to identify the type and version of all active services
- Network Mapping: with tools such as NMap/Trace Routing/IP fingerprinting
- User Enumeration: wherever services are available to complete this process
- Security Devices: assessing routers, switches and firewalls to ensure all these devices are configured and secured correctly

Once completed, manual checks are implemented to further investigate all findings and establish open attack vectors through known vulnerabilities.

256-260 Old Street, London, UK, EC1V 9DD
t. +44 (0) 207 749 7949 | e. salesteam@autodata.co.uk | www.autodata.co.uk

1. Discovery Stage

The process of 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.

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

2. Assessment Stage

This phase takes the information identified through Discovery and applies 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.

Internal Infrastructure Assessment (cont'd)

2. **Assessment:** Implement a detailed manual testing approach to investigate:

- Host Device & Service Configuration: poorly configured and/or inadequate processes can inadvertently open attack vectors via running services which allows company systems to be accessed and compromised
- Patching: poor patching strategy and implementation leaves systems open to attack via vulnerable running services
- Clear Text Protocols: FTP, Telnet and older legacy services do not encrypt data or credentials are an easy way for attackers to gain unauthorised access to your data. All these services will be reviewed and tested.

3. **Exploitation:** Attempt to exploit all identified and validated vulnerabilities.

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.

1. **Discovery:** As per the Internal Assessment, undertake the following tests. Once completed, implement manual checks to investigate the findings and establish open attack vectors through known vulnerabilities across:

- TCP and UDP Port Scanning
- Service Identification
- Network Mapping
- User Enumeration
- Security Devices

2. **Assessment:** The following processes are again undertaken:

- Host Device & Service Configuration
- Patching
- Clear Text Protocols

3. **Exploitation:** Attempt to exploit all identified and validated vulnerabilities.

Reporting

The resulting Report provides detail and context around the vulnerabilities identified, their impacts and the likelihood of a breach of an asset, along with recommendations for effective security counter-measures.

256-260 Old Street, London, UK, EC1V 9DD
t. +44 (0) 207 749 7949 | e. salesteam@autodata.co.uk | www.autodata.co.uk

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, CITYSPRINT

How regularly should you perform a 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 penetration-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 infrastructure and understand the motivations behind the penetration testing by helping organisations focus on determining what is needed.

What information does the organization want to protect?
Is it seeking to gain certifications or meet specific compliance standards?

It is necessary to work with testing providers to clearly define goals and understand what it is they do and how they do it. This alignment must be always be present for penetration testing to be effective.

Secondly, external penetration testers are trained to think and act as if they were a real-world malicious attackers, poking holes in information security and finding vulnerabilities their clients will not. They are up to speed on the misconfigurations in the latest software and operating systems that might let someone sneak in, as well as the common mistakes made when setting up hardware such as switches and servers.

If an information security consultant can gain access to your critical data assets, then so can a hacker. The recommendations that come from penetration testing can remediate the areas where existing measures have fallen short.

Autodata's penetration-testing teams hold some of the top certifications in the industry including **CREST STAR** and Offensive Security's **OSCP** and **OSWP** designations. They are members of the Council of Registered Ethical Security Testers (CREST) which has put in place specific and stringent standards regarding the delivery of penetration testing and incident response services; CHECK, whose members are approved by the National Cyber Security Centre (NCSC) to provide penetration testing for the UK government and other public sector bodies; and TigerScheme, an additional commercial certification scheme for technical security specialists.

256-260 Old Street, London, UK, EC1V 9DD
t. +44 (0) 207 749 7949 | e. salesteam@autodata.co.uk | www.autodata.co.uk