



The Sec-Check approach  
to penetration testing

# Penetration Testing





## **Vulnerability:** Vul'ner|abil'ity, *n.* The quality or state of being vulnerable.

*“Penetration Testing is one of those things you always see as an expense, a ‘tick in the box’ for the auditors while never giving any real value. With Sec-Check, we’ve changed our opinion.”*

**London based law firm**

The UK penetration testing market has seen massive growth in recent years, with a wide range of offerings both in terms of cost and quality. The temptation to buy on cost alone is great, but it's important to understand the differences in testing methodologies, and how this affects the overall return on investment.

So, what makes a good penetration test? One thing is for sure: it's not about security-testing tools. While security-testing tools play an important role within penetration testing, they have serious limitations. Artificial intelligence is exactly that – artificial – and can never provide a true simulation of a skilled attacker. In fact, in recent months, the majority of the most devastating (and previously undiscovered) vulnerabilities discovered by Sec-Check have been found using nothing more than a web browser and a team of skilled testing consultants, and these had been missed by even the most advanced automated scanners.

Further evidence of the limitations of automated testing tools have been documented by independent third parties:

[www.networkcomputing.com/1201/1201f1b1.html](http://www.networkcomputing.com/1201/1201f1b1.html)  
[infosecuritymag.techtarget.com/2003/mar/cover.shtml](http://infosecuritymag.techtarget.com/2003/mar/cover.shtml)

Sec-Tec adopted manual-based testing early on and, in fact, we have based our methodology on manual testing ever since the company's inception in 1999.

## **The main requirements**

We believe a quality penetration test has four main criteria:

- **To be thorough**
- **To be up-to-date**
- **To be informative**
- **To provide value**

## **Thoroughness**

Many organisations claiming to offer security-testing services often employ standard, off-the-shelf vulnerability-testing tools which have serious limitations and provide no real assurance. Sec-Check solves this problem by combining the very best in freeware, commercial and in-house developed tools with a rigid 112-stage manual testing procedure, written by an expert team and overseen by a consultant. Our philosophy on testing has proved so successful that over 65% of the vulnerabilities we document for clients have been missed by the best automated scanners, but discovered in the later manual testing.

A major part of our manual testing procedure is our CAM (Common Attack Methodologies) testing, which allows us to find previously undiscovered vulnerabilities by applying generic attack techniques to bespoke, customised or in-house-developed systems.



**To date, Sec-Check has found previously unknown vulnerabilities in software affecting over 100,000 users globally.**

Sec-Check also includes, as standard, comprehensive testing for both analogue and ISDN Remote Access Servers (RAS). Often an overlooked target, Sec-Check can identify and test over 450 different types of RAS infrastructure.

## Being up-to-date

There are approximately 300 new vulnerabilities being publicly released every month, so a test can only be as good as its last update. Sec-Check is updated on a **daily basis**, with many tests being written in-house. This means we do not have to wait for vendors to release updates, but can react quickly to the ever-changing threat levels that connectivity can produce. We currently track over 24 Internet security feeds.

In the last 12 months, Sec-Tec has added over 2,500 new vulnerabilities to its database, with every one manually catalogued and investigated, with a test written if feasible. With so many vulnerabilities being publicly released, why settle on a service which is only updated on a monthly basis?

We also understand that the configuration of systems may change in-between schedule tests, resulting in the dilemma of whether to change the test schedule or run the risk of being vulnerable until the next scheduled test. To combat this we offer, **at no additional charge**, a comprehensive automated scanning solution which can be used at any time and as frequently as necessary, simply by logging on to our secure web portal and commencing a scan. The results are then instantly available via an encrypted email attachment.

## Information

A penetration test report isn't just about reporting problems. It's about giving solutions. This is why all of our reports are hand-drafted by the tester, concentrating not only on the problems found, but providing the quickest, most efficient route to a fix.

## Value

By providing the optimum combination of automated and manual testing, the savings can be dramatic, whilst providing a higher quality of overall testing:

	Sec-Check	Typical Competitor
Number of individual checks	Over 21,000	Approx 1,250
Total cost	£1,250.00	£1,500.00
<b>Cost per individual check</b>	<b>£0.16</b>	<b>£0.83</b>

Sec-Tec's approach to value penetration testing has always been simple: the most thorough testing for the least cost. Combined with the inclusion of No-Find No-Fee on one-off tests and defacement guarantees on subscriptions, it represents real value:

Competitive Analysis		
Benefit	Sec-Check	Typical Competitor
Number of individual checks	Over 21,000	Approx 1,250
Manually confirmed findings	Yes	No
Remote Access system testing	Yes	No
Performed to international standards	Yes	No
Full manual web application testing	Yes	No
Manual privilege escalation testing	Yes	No
Insured to £1,000,000	Yes	No

## Benefits

- No-Find No-Fee on one-off tests
- Defacement guarantee on subscriptions
- Unlimited interim scans using our secure portal
- Full manual testing of applications
- Remote Access testing as standard
- Standards-based
- All tests overseen by a consultant
- Updated on a daily basis
- Hand-drafted reports

## Brief summary of tests performed as standard

### Automated Testing

#### *Network mapping/discovery*

TCP port scans  
FTP source port scanning  
UDP port scans  
Query of informational services present  
DNS/RIPE transfers  
OS fingerprinting

#### *Vulnerability scanning*

Customised vulnerability scan using freeware and commercial products  
Customised web scan (consisting of over 21,000 individual URLs)

#### *Remote Access testing (RAS testing)*

ISDN enumeration, vulnerability scanning and credential guessing  
Analogue enumeration, vulnerability scanning and credential guessing

### Manual Testing

#### *Verification*

Verification of above results using manual testing and banner grabs  
Public/private vulnerability database searches on discovered applications/OSs

#### *Input validation*

SQL injection tests  
HTML injection tests  
Script injection attacks (XSS)  
General input field modification/validation  
Hidden form field validation/modification  
Directory traversal using ASCII, Hex and 1,2,3 & 4 byte UNICODE encodings

#### *Encryption*

Encryption strength and scope  
Valid server side certificate  
Client side certificate authentication enforced (if applicable)

#### *Client side validation*

Client side validation enforced on server

#### *Session tracking*

Sufficient entropy in session tracking  
Cookie predictability/modification  
Session URL predictability/modification

#### *SMTP specific testing*

Relaying, including malformed From: To: CC: and BCC: fields

#### *FTP specific testing*

Anonymous FTP access  
File read-write tests  
Correct file and directory permissions

### Reporting

Manually drafted report with corrective actions  
Peer review/correction of report

Please note that this list represents a brief summary of tests performed and is in no way a complete list.



**Tel:** +44 (0) 20 8317 7962  
**Fax:** +44 (0) 20 8317 8051  
**Email:** info@sec-tec.co.uk  
**Web:** www.sec-tec.co.uk