

Caretower Penetration Testing

In the digital age, it's a serious matter when intruders bypass your defences and access sensitive data; a compromise impacts the business and its reputation. Caretower's Information Assurance Services are designed to give our customers a comprehensive overview of potential threats, vulnerabilities and weaknesses in their network.



Caretower have a team of leading experts ready to provide Internal Audits and Security Assessments. Our Penetration Test Team have vast expertise in performing vulnerability assessments and penetration testing for both internal and external facing end points. The main objective of this service is to assist organisations analyse and identify threats to information assets to help prevent infiltration and attacks as well as ensure a remediation plan is put in place to mitigate risk.

Our Penetration Test Team believe in results validation and report correctness. Not only will the Penetration Test Team express their opinions, they will also provide a detailed vulnerability report and remediation plan which will greatly help decision makers and systems administrators to prioritise areas of concern. This advisory service ensures the client understands the risks and vulnerabilities that they may be exposed to.

A penetration testing package consists of two key testing procedures:

Vulnerability Assessment: This procedure is mainly conducted by semi-automated tools, these tools scan for known vulnerabilities most common and prevalent in end point devices. We use a minimum of two scan engines to reduce false positives from our results.

Penetration Testing: This term refers to the process conducted by the Penetration Test Team who undertake testing procedures on internal and external end points as per guidelines. Ethics and standards such as NIST and OWASP are used as a framework to conduct vulnerability assessments and exploit weaknesses in security. The Penetration Test Team detects and exploits vulnerabilities from the perspective of a malicious outsider and/or insider, respectively.

Accreditations and Membership

As one of Europe's leading I.T. Security Specialists, We are committed to providing a high standard of Penetration Testing and as such have achieved numerous accreditations and memberships of professional organisations including the following:



The key benefits of Caretower's Penetration Testing Service:

- Secure your network's critical infrastructure
- Prevent data leakage and viruses
- See what the intruders can do
- Meet regulatory requirements
- Prevent ID theft
- Avoid network downtime
- Stop website hacks
- Protect your company image and brand
- Reduce operational risk
- Protect and retain your customers



What We Do

Penetration Testing Methods:

- Black Box or Zero Knowledge Test
- Grey Box or Partial Knowledge Test
- White Box or Full Knowledge Test

Caretower consultants will provide quality reports that will reflect accuracy and objectivity. The output from these reports will help guide management and technical personnel through a remediation plan based on risk and impact of the vulnerability. We use a clear traffic light system to highlight critical, high, medium and low risk vulnerabilities.

The report will be divided into three main sections:

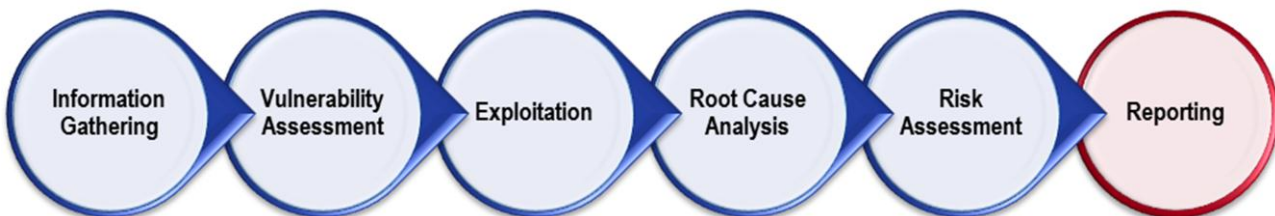
- Executive Summary:**
 - Number of critical, high, medium and low risk vulnerabilities
 - Overview of affected systems
 - Principal security concerns
- Technical Summary:**
 - Technical summary of vulnerabilities and affected systems
 - Prioritised by severity and risk
 - Overview of issue and fix
- Test Results:**
 - Detailed information on vulnerable systems and exploit
 - Remediation action required
 - Reference links

Caretower's security risk intelligence approach to information assurance follows 5 steps:

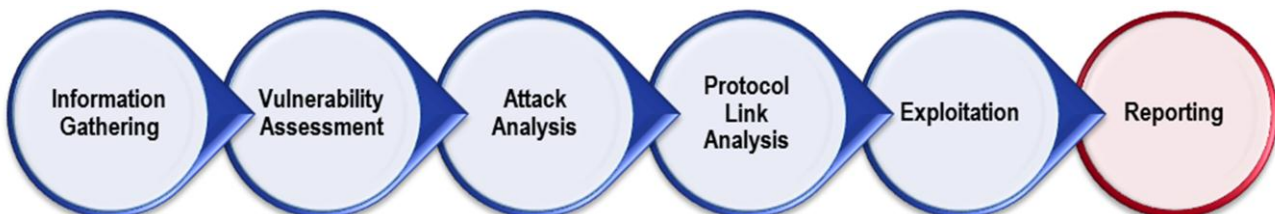
- **Discovery:** Identify business critical assets and vulnerabilities
- **Risk Detection:** Verify and prioritise vulnerabilities based on the exploitability and overall risk score
- **Testing & Validation:** Identify gaps in security controls
- **Remediation & Mitigation:** Prioritise efforts based on acceptable risks
- **Actionable reporting:** Actionable management and operations

How we do it:

Caretower's External Penetration Test: Conducted remotely on external or public facing networks or applications in order to identify vulnerabilities that are visible to outsiders at large.



Caretower's Internal Penetration Test: Conducted on the internal network to identify vulnerabilities that are visible to insiders, contractors or partners with potential malicious intent.



Penetration Testing Services

Additional Services*

- Application Testing
- Web Application Testing
- Wireless Security Testing
- Social Engineering
- Remote Access (VPN) Security Testing
- Gold Image Build Assessment
- Mobile Security Testing
- Social Media Testing
- Bespoke Testing

We offer a multitude of tests to suit client's needs. This table outlines the methods used in our external and internal penetration tests.

Infrastructure Penetration Testing Services				
Vulnerability Assessment (External & Internal)	PCI ASV Scan	Basic	Standard	Advanced*
Compliance Scanning	✓	✓	✓	✓
Report and Remediation Plan	✓	✓	✓	✓
Multi Engine Scanning		✓	✓	✓
False Positive Removal		✓	✓	✓
Footprinting (External)				
DNS Queries		✓	✓	✓
Zone Transfers		✓	✓	✓
Traceroutes		✓	✓	✓
Ping Sweeps		✓	✓	✓
Organisation IP Allocations		✓	✓	✓
Internet Search Engines		✓	✓	✓
Webserver Analysis & Review		✓	✓	✓
Enumeration & Assessment (External/Internal)				
OS Detection			✓	✓
Service Detection			✓	✓
Automated Port Scan			✓	✓
Automated Vulnerability			✓	✓
Automated Scan Assessment			✓	✓
False Positive Detection			✓	✓
Manual Scan & Vulnerability determination			✓	✓
"Low Hanging Fruit" Exploitation (only with customer consent)			✓	✓
Password Sniffing			✓	✓
Exploitation (only with customer consent) (External/Internal)*				
Denial of Service				✓
Buffer Overflow				✓
SQL Injection				✓
Memory Corruption				✓
Brute Force Password Cracking				✓
Cross Site Scripting				✓
Fuzzing				✓
Other attacks may include aspects of web application				✓
Pivoting				✓
DNS and ARP poisoning				✓
DNS Zone Transfer				✓

*Note: These services are intrusive tests that may cause system or service downtime.