

Penetration testing services

A penetration test is an information security assessment which simulates an attack against an organization's IT assets. It examines IT systems for any weakness that our client can address before they are exploited by an attacker to disrupt the confidentiality, availability or integrity of the network, application, and associated data.

We follow a discover-investigate-exploit process during penetration testing. Responsible exploitation of vulnerabilities allows us to quantitatively determine the business risk associated with all identified security problems in the network infrastructure or application. This risk is determined by the perceived value of the information protected by compromised systems, as well as the value of the compromised systems themselves.

Risk based assessment

We use a risk-based approach to penetration testing in order to prioritize the identified vulnerabilities from high risk to low risk. Identified vulnerabilities are assigned a risk by estimating the business impact of successful exploitation of the vulnerability. The tools and techniques used mirror as closely as possible real life 'hacker' behaviour.

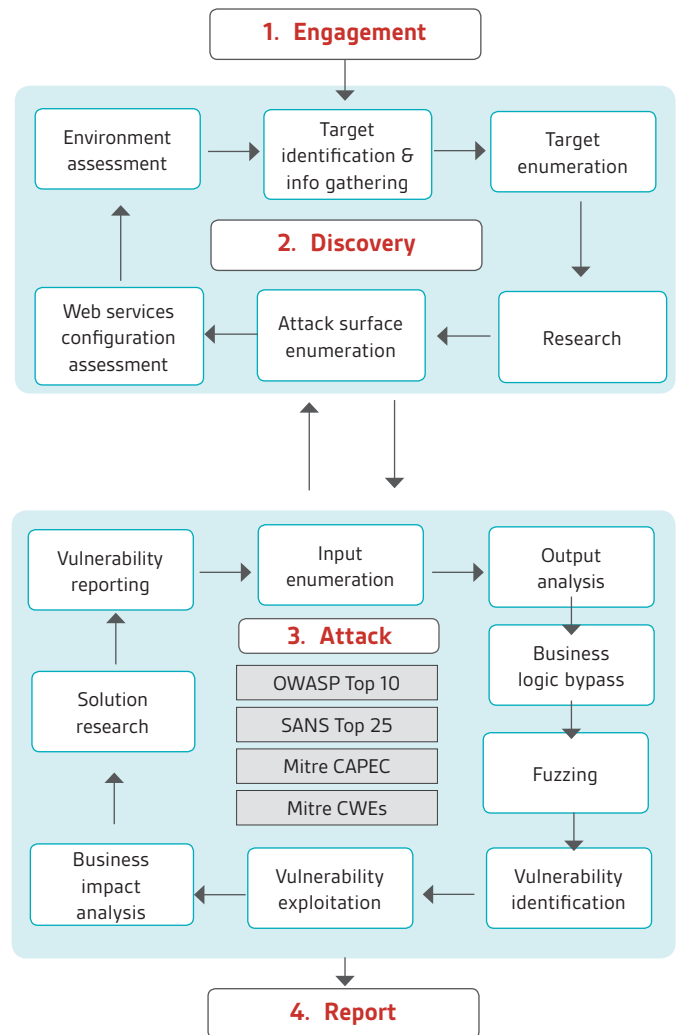
Penetration techniques

We perform all penetration testing using a carefully selected set of industry recognized tools and techniques (e.g. OSSTMM NIST, SP800-115, OWASP Top Ten).

Our experienced consultants are trained to use an exhaustive set of tools to perform and imitate the mind of an attacker.

Any identified security issue will be presented to the system owner, together with an assessment of the impact, a proposal for mitigation or a technical solution.

We are a CREST and NCSC CHECK accredited penetration testing provider, demonstrating that we deliver to the highest levels of security testing standards.



To find out more

Call US: **+1 800 862 4977**
Visit: **bsigroup.com/cyber-us**



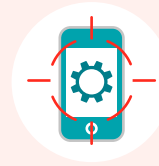
...making excellence a habit.™

Our Penetration Testing services



Infrastructure Testing

Internal and external infrastructure testing of servers, workstations, domains, virtual environments, network devices and network segregation controls



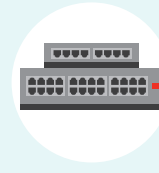
Application testing

Assessment of various applications including web applications, web services, binary application (thick client) and mainframe



Build review

Server build review service of all operating systems including Windows, Linux and Solaris, and AIX as well as common components, such as database and web servers. We also regularly conduct build reviews on end-user devices, such as workstations and laptops to mimic malicious internal users or stolen devices



Network device reviews

Network device review service includes assessing the running configuration, firmware version and firewall rulesets of devices from a large number of major manufacturers including Cisco, Checkpoint, HP, Juniper, Palo Alto, Brocade, SonicWall and Fortigate



Mobile applications and devices

Extensive mobile application penetration testing service of all of the common platforms, including Android, Apple, Windows Phone and BlackBerry applications. Also we provide an assessment to review the configuration lock-down of mobile devices and the mobile device management (MDM)



Wireless penetration testing

Wireless network testing and configuration review service assesses the level of security of wireless network. The service includes wireless access point reviews, WLAN controller and client device reviews, site surveys and rogue access point sweeps



Cloud and Virtualization testing

Build review and infrastructure testing of Cloud or virtual environments, on both commercial and restricted networks. Our experience includes key products such as VMware, Hyper-V as well as cloud service providers such as Amazon AWS, Azure and Google Cloud Platform



Secure code review

Examination of an application's source code from both manual and automated perspectives to rectify any flaws overlooked in the initial development phase, improving both the overall quality of software and the developer's skills.

We offer this service in a wide range of languages, including C#, Java, Python and PHP amongst others.



SCADA and ICS testing

Comprehensive review of your SCADA/ ICS system. This assessment can take on many forms, including reviews of relevant policies and procedures, architecture review, physical security assessment, infrastructure penetration testing, segregation testing and build review exercises



Stolen laptop review

Assessment of whether the laptop can be compromised via boot methods, encryption bypassing and any information that can be used to further attack the company