

INTERNAL PENETRATION TESTING

SECCOM
GLOBAL
SERVICES



20
22

INTRODUCTION

Internal Penetration Test

An Internal Penetration Test is performed by a highly skilled Seccom Global security consultant who is onsite within your corporate network or securely connected to your network via a secure VPN over the internet.

This type of assessment looks for security issues and vulnerabilities on the inside of your corporate network with the same physical access as a member of staff or other types of employee who has access to the organisation.

This assessment provides a very comprehensive view of the configuration of your corporate network devices and servers from a security viewpoint of an insider, connected to your network.



**Penetration Testing
can be performed
Internally within
your corporate
network or securely
over the Internet**

SOLUTION OVERVIEW

What Are the Risks?

- Most large fraud operations and industrial espionage attacks are performed from inside an organisation.
- These attacks may be carried out by a contractor who has their contract cancelled, by a disgruntled employee or by a remote attacker who has gained access to your internal network.
- The closer an attacker is to their target, the more control they have over the environment. This is why internal attacks can be so devastating and costly
- Various forms of compliance exist that mandate regular Penetration Testing as a required standard and the risks of not doing anything are widely publicised.

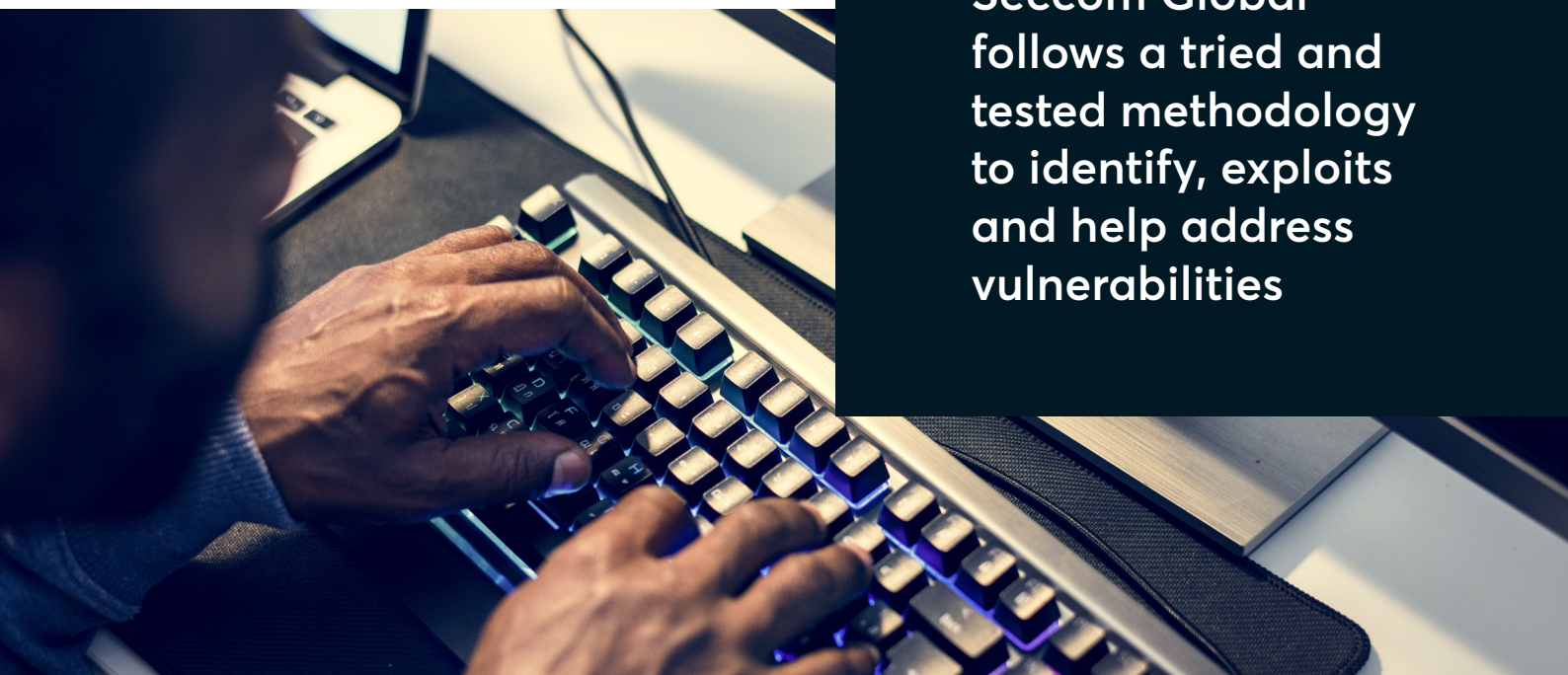
How Seccom Can Help?

- Identify security gaps by understanding how an internal attacker could compromise your internal network.
- Gain real insight into the potential damage and business risk an attacker could inflict.
- A comprehensive report outlining the security posture of your internal network, including high impact recommendations.
- Enhanced protection of your business intelligence, data and IT systems, brand and reputation.

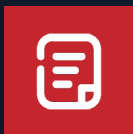
Best Practice recommends that each organisation perform an Internal Penetration Test as part of their regular Security Program in order to ensure the security of their internal network defenses.



**Seccom Global
follows a tried and
tested methodology
to identify, exploits
and help address
vulnerabilities**

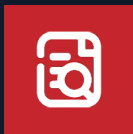


OUR APPROACH TO PENETRATION TESTING



SCOPING

Seccom Global's network and infrastructure testing experts work with you to define any network and asset in scope and devise an appropriate assessment strategy.



ACTIVE SCANNING AND VULNERABILITY ANALYSIS

Using a combination of manual and automated tools, our testers identify security weaknesses and develop a strategy to exploit them.



EXPLOITATION

To obtain initial access to your network, our experienced network penetration testers exploit all identified vulnerabilities, but in a safe way that avoids damage and disruption.



REPORTING

Once a network assessment is complete, our testers document key findings and supply prioritised remediation guidance to help address any identified exposures.



FAQS

FREQUENTLY ASKED QUESTIONS ABOUT INTERNAL PEN TESTING

What vulnerabilities are detected by our network penetration testing service

- Insecure configuration parameters
- Ineffective firewall rules
- Unpatched systems
- Software flaws
- Weak encryption protocols
- Inadequate security controls

Can an internal pen test be performed remotely?

In many scenarios, internal penetration tests can be performed remotely via a secure VPN connection. If your organisation's network is segmented, you may need help to decide upon the best physical location for internal pen testing to be conducted.

What is the difference between internal pen testing and external pen testing?

An internal pen test is performed within an organisation's network, looking for vulnerabilities from the inside. An external pen test is conducted remotely, with an ethical hacker searching for security vulnerabilities in internet-facing assets such as web, mail and FTP servers.

Australia
Philippines
India
Singapore

WWW.SECCOMGLOBAL.COM

