Our contacts

Richard Peters
Partner | PwC Vietnam
+84 28 3824 0123
richard.peters@pwc.com

Robert Trong Tran
Director | PwC Vietnam
Cyber Security and Privacy Lead
+84 28 3823 0796 Ext. 1007
robert.trong.tran@pwc.com

Our offices

Hanoi:
Floor 16, Keangnam Hanoi Landmark 72
Pham Hung Road, Nam Tu Liem District
Hanoi
Tel: +84 24 3946 2246

Ho Chi Minh City:
Floor 8, Saigon Tower
29 Le Duan Street, District 1
Ho Chi Minh City
Tel: +84 28 3823 0796

pwc

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

©2019 PwC (Vietnam) Ltd. All rights reserved. PwC refers to the Vietnam member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

www.pwc.com/vn

Cyber Security Services

PwC's Approach to Penetration Testing 2018

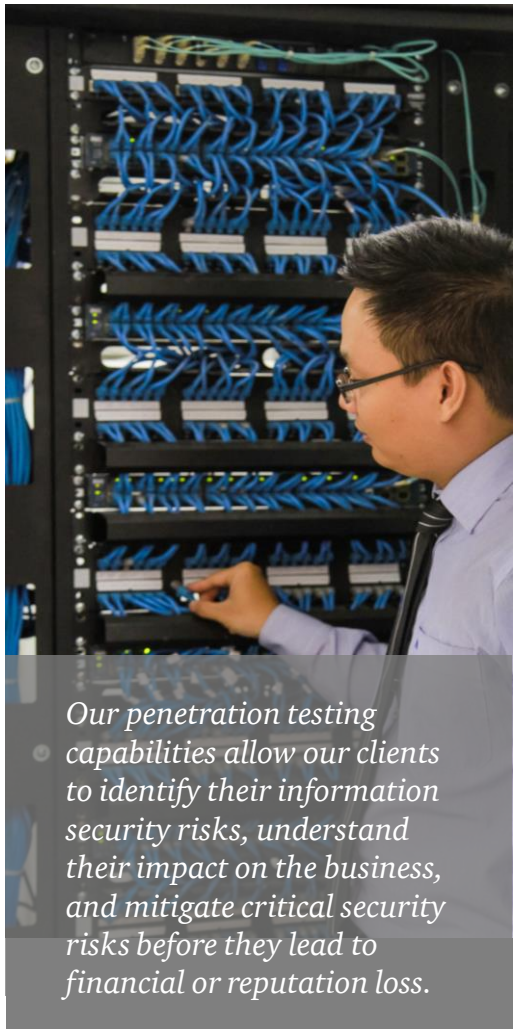
pwc

Why PwC?

We have a highly experienced, global team to address your needs

PwC has been named as a global leader in cyber security by Kennedy, the global leading consulting research and advisory firm. Our commitment to this industry is so well known that new technology vendors regularly come to us to assess their products and help drive them into the marketplace.

Additionally, our security practice is known internationally for its expertise and strong security skills in threat and vulnerability management, cybercrime prevention, response and recovery, strategy and security design, and implementation services. IDC, one of the leading global providers of technology forecasts, insights, and advice, has ranked PwC as an "outperformer" with respect to the depth of its service offerings and growth potential.



Our penetration testing capabilities allow our clients to identify their information security risks, understand their impact on the business, and mitigate critical security risks before they lead to financial or reputation loss.

Realised value

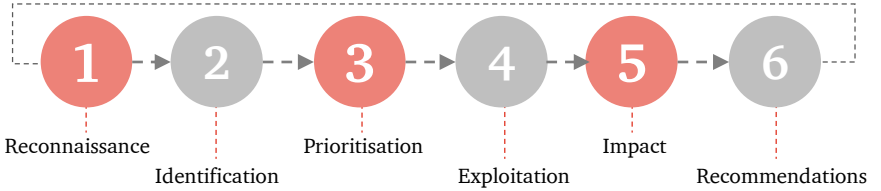
- Help leadership understand security strengths and weaknesses in business language with root cause analysis
- Simulate realistic threats, providing a unique perspective on your security defenses from an attacker's perspective
- Target higher-risk vulnerabilities across the infrastructure in a short timeframe
- Demonstrate results with impact. We clearly illustrate simulated compromises through appropriate evidence and walkthroughs

- Test incident response processes and employee security awareness
- Include flexible and iterative test procedures executed by experienced practitioners to identify non-linear paths of compromise
- Outperform software –our suite of tests provides advantages not provided by an automated vulnerability scanning tool

Our methodology

Our vulnerability assessment methodology consists of iterative processes that emulate the approach of an attacker exploiting vulnerabilities, as well as identifying internal security weaknesses.

Key activities of our approach include both vulnerability scanning and penetration testing that involves the active exploitation of identified vulnerabilities. Our approach incorporates formal approval points throughout the testing lifecycle, specifically to help ensure efficient communication between the testing team and the client.



Our penetration assessment

Level 1

Performing the following tasks:

- Scope and planning
- Reconnaissance (information gathering)
- External/internal automatic scan
- Manual exploitation (limited to critical findings)
- Risk rating
- Reporting and remediation recommendations

Level 2

Network penetration testing:

- Planning
- Reconnaissance
- External/internal automatic scan
- Manual exploitation (limited to critical findings)
- Risk rating
- Reporting and remediation recommendations
- Follow up

Optional:
Source code review, software architecture review

Level 3

Comprehensive assessment

LEVEL1 + LEVEL2 and the following services:

- Network architecture review
- Source code review, software architecture review

Optional:
Compliance review, third parties assessment