

Overview

In the Industry 4.0 era development, cities are increasingly dynamic and the growth of information technology (IT) systems is involved in modern life.

Therefore, IT is popularly applied in organizations and businesses to serve for the “dynamics” and it has become an integral part of such organizations and businesses to meet instant information access.

That is the reason why security of IT systems is becoming more and more essential and playing a prerequisite role in information security for organizations and businesses.

Necessity of Penetration Testing

IT systems always exist security weaknesses that can be exploited by hackers. Therefore, organizations should beat hackers to the punch, particularly, find out and overcome weaknesses in its IT systems before attacks by hackers.

However, because the periodic audit of an organization’s IT system is very complicated and requires high objectivity, organizations intended to use Penetration Testing by external providers.

Penetration Testing, also known as Pentest, is a form of testing whether clients’ IT systems can be attacked by playing as hackers and simulating test attacks on clients’ systems. The main objectives of Pentest service are:

- Identify security vulnerabilities in the system.
- Give recommendations and remedies for vulnerabilities detected during pentest.
- Check out the organization’s information security policies.
- Test and evaluate users’ awareness when cyber attacks take place in the organization.

Typically, information on security weaknesses identified and exploited by pentest will be collected and provided to organizations to support organizations in planning strategies and priorities for increasing security for IT system of such organizations.

Viettel Penetration Testing service

Implementation method

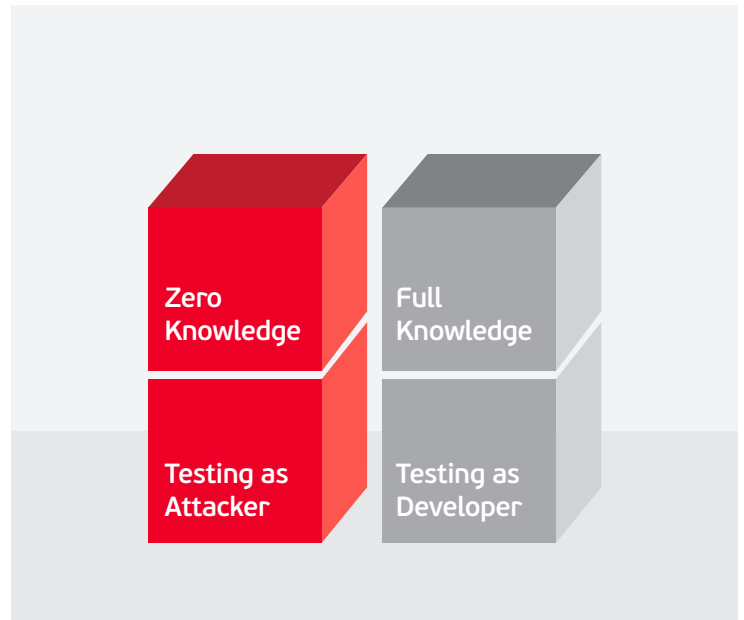
VCS provides 2 Pentest types of BLACKBOX and WHITEBOX



• **BLACKBOX PENTEST:** Refers to information security audit method by accessing to clients’ IT system from the Internet: Provision of internal data is not required, Audit as hacker, finding vulnerabilities only without impact on client’s system.










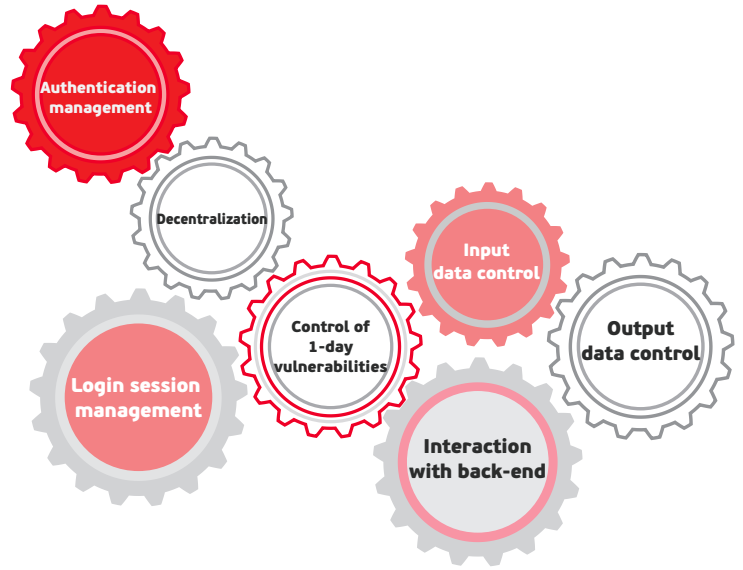
• **WHITEBOX PENTEST:** In contrast to BLACKBOX, client is required to provide information related to internal and external IT system to perform. Testing as a network administrator, audit of potential risks from source code of the system, finding vulnerabilities only without impact on client’s demands, anywhere and anytime, even for essential operations in the field of finance, banking or control of critical systems.



The main services

Based on description of vulnerabilities in the list of Top 10 ranked by OWASP, VCS has developed criteria to identify the vulnerabilities of a web system, including 7 key items:

-  Authentication management: Avoid vulnerabilities that cause account loss.
-  Login session management: Avoid vulnerabilities that hack the control of login.
-  Decentralization: Avoid vulnerabilities that allow unauthorized functions to be performed.
-  Interaction with back-end: Avoid vulnerabilities that cause data loss.
-  Input data control: Keep information security for data that is sent to server.
-  Output data control: Keep information security for users.
-  Control of 1-day vulnerabilities of libraries and framework.






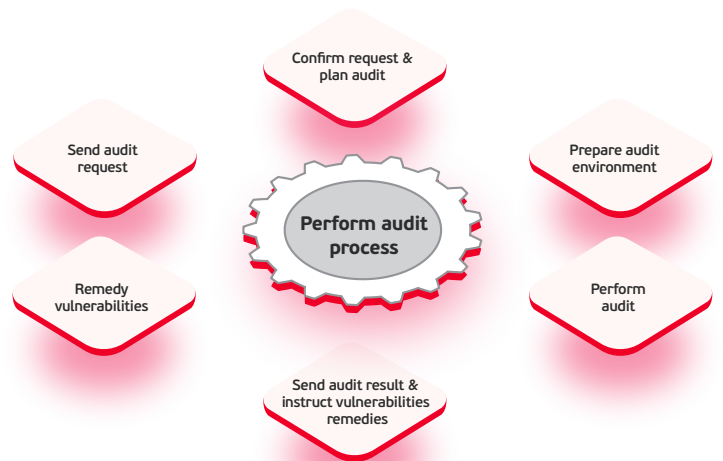
Procedure

Information security audit process is performed with the following steps:

-  Step 1: Client sends audit request
-  Step 2: VCS returns audit plan
-  Step 3: Client prepares audit environment
-  Step 4: VCS performs audit
-  Step 5: VCS sends audit results and remedies guidelines for detected vulnerabilities
-  Step 6: Client takes remedies as guided and sends re-audit request.

The process is complete in the following cases:

-  1. The audit results and assessment of remediation no longer contain errors
-  2. After 2 weeks, clients do not request an audit of corrected errors
-  3. After 2 time auditing remedied errors, the client has not yet completed the remedy



Awards

The Penetration Testing service of Viettel Cybersecurity Company was honored to receive international awards, typically the Gold Winner for “Cyber Security Penetration Testing” certified by Cybersecurity Excellence Awards in 2023 and “Next-gen Penetration Testing” Award 2023 by the Cyber Defense Magazine.

Over the past years, Viettel Cyber Security’s staff and experts have made constant efforts in the process of research and development of the most optimal products to serve for clients’ information security across the country and other clients in the region. During its operations, VCS has researched and owned 50 zero-day vulnerabilities on various application platforms such as: Microsoft, Zimbra, Facebook, Paypal, etc.

Thanks to important results in detecting vulnerabilities of popularly used various applications in the world, VCS has been recognized as an excellent unit in the field of Information Security Audit, Supervision and Assurance.