Datasheet

Viettel X-Data service
(Red Teaming Service)

viettel security

Overview

In the booming era of technology and digital engineering, cyber security has become the common concern for almost organizations and service providers, etc. Therefore, the stronger investment in information security of organizations and businesses is essential to ensure business performance and minimize risks of data loss, service interruption or influence on reputation on the market.

So how to know if businesses and organizations are adequately equipped with information security solutions, network system has been planned in accordance with its functions and duties, security levels or not?

Currently, businesses and organizations often use Information security Inspection and Audit Service or known as Penetration Testing Service - Pentest or use product tools to review, audit security levels of information system based on detection security vulnerabilities, severity and exploitation and penetration into objects with security vulnerability in a short-term.

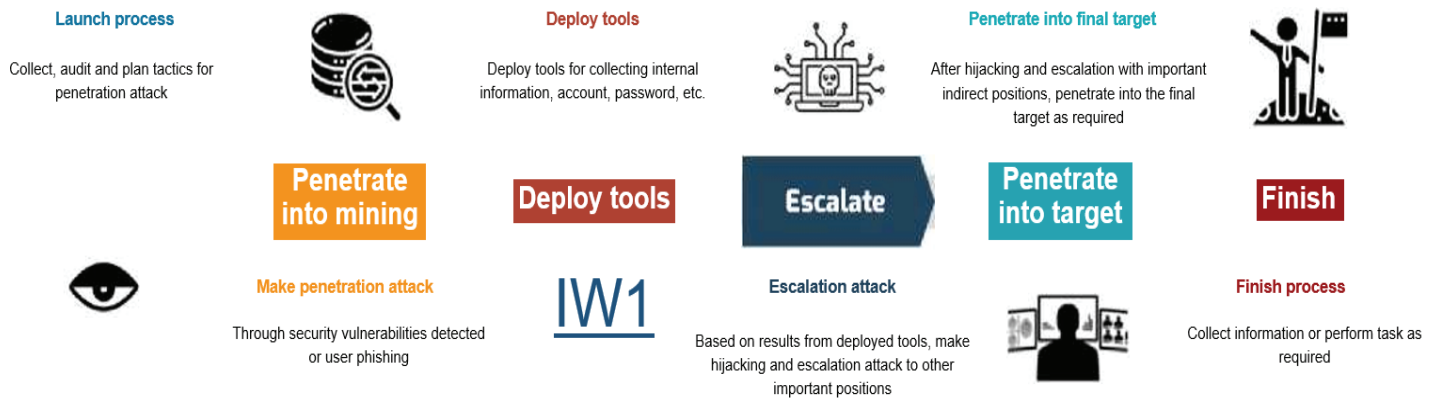
However, implementation of Pentest service or use of such tools is limited:

- Objects of audit are often fixed, meanwhile information system is always a linked, interconnected and influential chain. Therefore, the audit of information security in limited scope may omit some cases that can cause escalation attacks, in-depth penetration into critical components of the system such as Active Directory, Database Server, etc.
- The level of discrete risk for each IT infrastructure is only audited but the actual severity to production and business of an organization. In some cases, the system with medium errors may be more vulnerable to steal data than the one with serious vulnerability but low attack capacity. Simultaneously, the ability to detect and handle incidents and issues on information security have not been audited.

Viettel X-Data (Red Teaming Service)

Viettel X-Data Service (test of targeted data exploiting) is designed to provide businesses with more specific view about level of influence on production and business from outstanding Information security issues.

Instead of auditing and testing of previously localized objects, we focus on the most important X position the client targets, within the agreed upon time, without limiting the scope and implementation method, X-Data will help clients audit the overall detection and processing of Information security system, through a kill-chain exploited from outside, escalated via each different system and at X position, how your business will be affected when being attacked, hijacked or stolen data.



Datasheet

Viettel X-Data service
(Red Teaming Service)

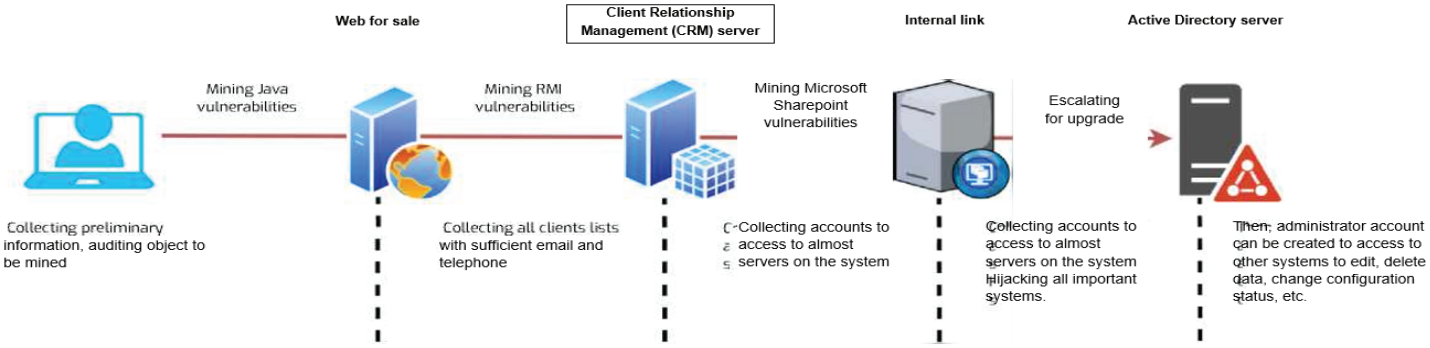
viettel security

Steps of service provision

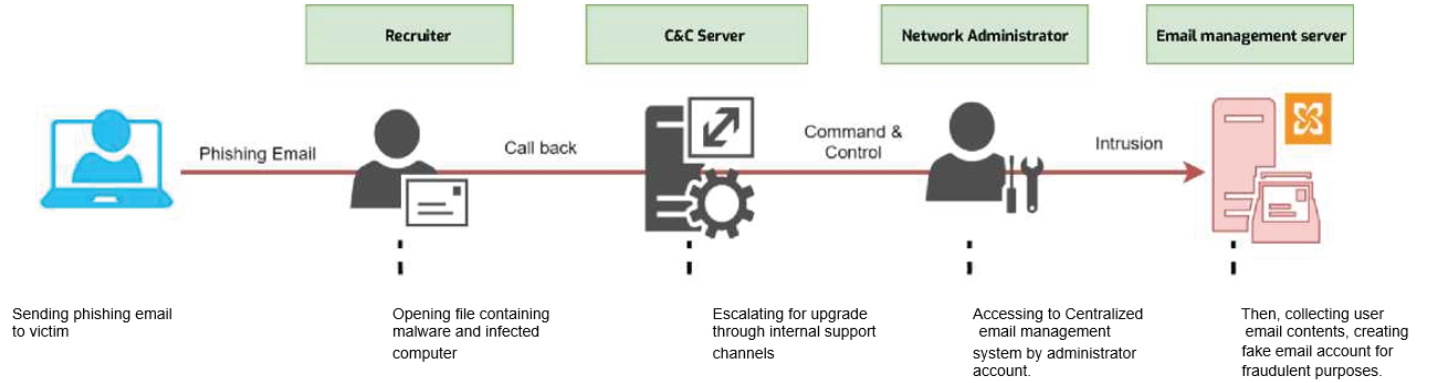
1. Client gives request of important position on the system
   For example: Email system, Active Directory centralized administration system or bank's SWIFT international remittance network, etc.
2. Both parties agree with implementation time
3. Upon the agreed implementation time, VCS send extensive report
4. Stimulate entire real process
5. Analyze risks, effect to an organization or business's operations
6. Finish.

Actual case

Target 01: Hijacking Active Directory centralized administration server, create an account with the highest level of access on the system.



Target 02: Hijacking email management system through phishing email to normal user.



Report

After completing the task, the report provided to the client will include the following information:

1. Attack script, actual action
2. Methods to penetrate into the system through different locations:
   - Outstanding issues on Information security at each penetrated and hijacked location
   - What is the impact when the location is penetrated and the collected information can be stolen?
   - Recommend remedies for each Information security issues at each location.
3. Analyze risks, effects to the system, operations, production and business activities of enterprises (for example: interrupted remittance system; unconnected power grid control server, etc.).
4. Connect attack events, demonstrate actual demo of the entire kill-chain sequence performed.
5. Propose overall preliminary solutions to overcome and improve the information security capacity of the system.