

Penetration test activity

1. Information gathering : mencari informasi mengenai target

* Network Mapping: melakukan port scanning untuk melihat port yg terbuka
* Vulnerability scanning: menggunakan automatic scanning pda modul yg aktif bisa passive dan active scanning.
* Penetration: pengujian secara manual dari modul yang ada mengacu ke API Security milik OWASP.
* Enumerating: melakukan enumerasi lebih dalam apabila berhasil mengambil alih sistem dengan privilege terendah
* Compromise: mencoba melakukan eskalasi lebih tinggi apabila berhasil melakukan enumerasi di tahap sebelumnya.

2. Application Logic: jenis pengujian untuk menguji logika dari aplikasi. Contoh apabila ada fitur upload gambar maka kita akan check apakah dapat menerima ekstensi diluar gambar. Karena memang untuk melihat logic dari aplikasi dalam menerima request dari sisi client apakah dapat di proses dengan baik dan apabila ada request yang dimanipulasi apakah dapat di proses dan menimbulkan kerentanan tertentu atau tidak.

3. Input Handling : Ini jenis pengujian umum yg sering dilakukan contoh injeksi script untuk menguji XSS, SQL Injection, dan jenis injeksi lain yg memang mencoba mengirimkan request tertentu.