

Problem:

Each activity during penetration test has different goal, therefore organize each activity at least to following categories:

Solution:

Reconnaissance - active nmap, API and passive nslookup, OSINT

Exploit Build, PoC - Java, Python ...

Exploit Run - logs, screenshots, evidences

Report, Evidences - PDF, hash, signature