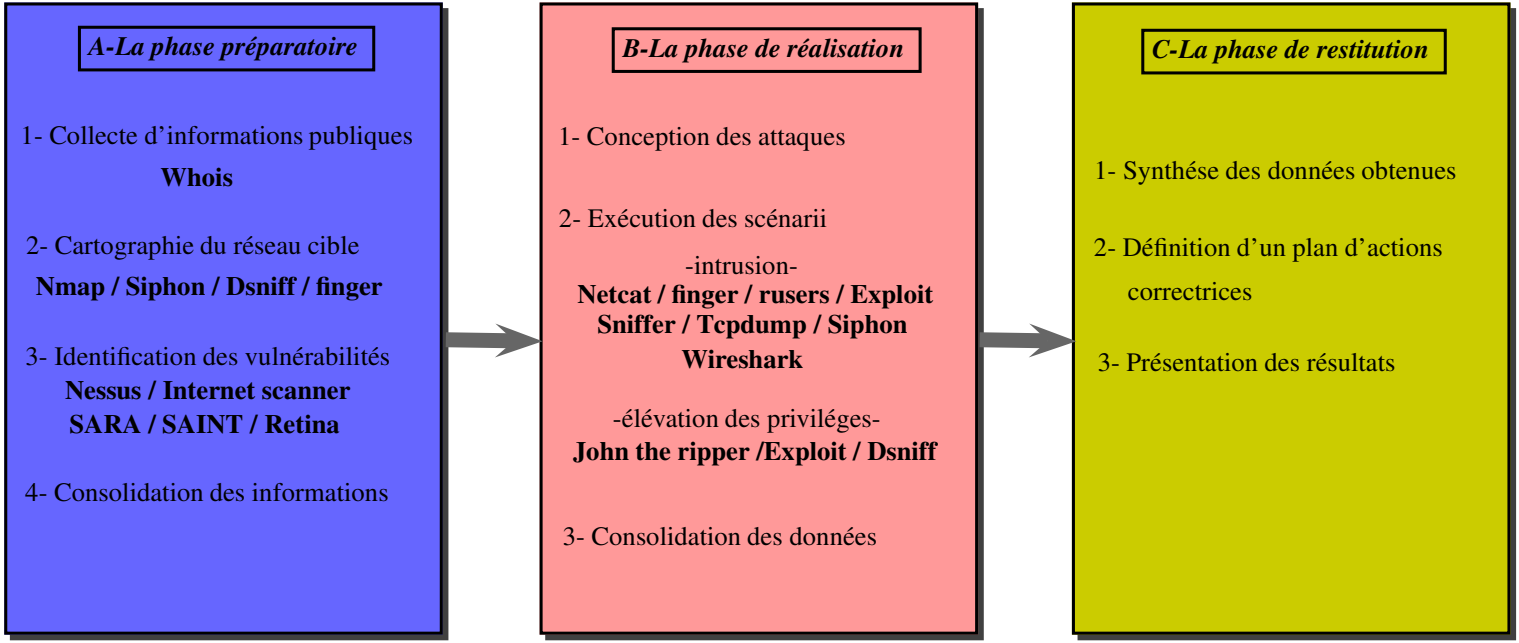
A-La phase préparatoire
1- Collecte d'informations publiques
Whois
2- Cartographie du réseau cible
Nmap / Siphon / Dsniff / finger
3- Identification des vulnérabilités
Nessus / Internet scanner
SARA / SAINT / Retina
4- Consolidation des informations
B-La phase de réalisation
1- Conception des attaques
2- Exécution des scénarii
-intrusion-
Netcat / finger / rusers / Exploit
Sniffer / Tcpdump / Siphon
Wireshark
-élévation des priviléges-
John the ripper /Exploit / Dsniff
3- Consolidation des données
C-La phase de restitution
1- Synthése des données obtenues
2- Définition d'un plan d'actions correctrices
3- Présentation des résultats