Commandes gdb-gef utiles au reverse-engineering

Voici un récapitulatif non exhaustif de commandes gdb-gef utiles à maîtriser :

- **catch**
    - Tout particulièrement `catch syscall`, pour arrêter automatiquement après un appel système. Exemple :
        - `catch syscall read`
- **disassemble**
    - Soyez à l'aise avec des commandes comme :
        - `disassemble $pc-5, +20` (désassembler 20 octets à partir de l'adresse actuelle - 5)
        - `disassemble /r $rbx+0x30, +5` (désassembler 5 octets à l'adresse RBX + 0x30)
- **search-pattern**
    - Très utile pour chercher des chaînes de caractères ou toute autre valeur dans le code. Exemple pour chercher l'instruction `int 0x80` (opcode 0xcd 0x80) :
        - `search-pattern cd80 big`
- **set**
    - Permet, entre autres, de réécrire des registres durant l'exécution pour tester des hypothèses. Exemple :
        - `set $rbx=0xbbbb`
- **vmmap**
    - Permet de visualiser les segments mémoire utilisés par le binaire et leurs permissions.
- **process-status**
    - Affiche l'état actuel du processus en cours d'exécution, y compris les informations sur les processus parents et enfants, les fichiers ouverts et les connexions réseau.
- **p (print)**
    - `p/d 0xffff` (affiche en décimal)
    - `p/x $rax` (affiche en hexadécimal)
- **x (examine)**
    - `x/1s $rax` (affiche 1 chaîne à l'adresse $rax)
    - `x/8x $rax` (montre 8 octets en hexadécimal à $rax)
    - `x/3i 0x40101c` (désassemble 3 instructions à l'adresse 0x40101c)
    - `x/10xg $rsp` : montre 10 valeurs géantes (valeur 64 bits) en format hexadécimal
- **dereference**
    - Montre et déréférence les prochaines adresses, ainsi que les valeurs pointées, sur une taille arbitraire. Exemple :
        - `dereference –length 20 $pc`

- **hexdump**
  - Dump en hexadecimal a partir d’une adresse
- **scan stack libc**
  - cherche dans la stack les pointeurs vers des zones de la libc (exemple d’utilisation, lire le help)
- **xinfo <PTR>**
  - infos completes sur la page memoire dans laquelle se situe un pointeur.
- **xfiles**
  - liste toutes les sections chargees par le binaire
- **si, ni**
  - aller a la prochaine instruction (**ni** pour ne pas entrer dans un call)
- **break**, **name-break**
  - interrompre l’execution lorsque RIP pointe sur une adresse specifique
- **finish**
  - arreter l’execution a la sortie de la fonction actuelle
- **patch**
  - permet de patcher un ou plusieurs octet a une adresse arbitraire.
- **gef**
  - **cette commande affiche l’aide globale pour toutes les commandes de gef.**
- **help <command>**
  - **affiche l’aide detaillee pour une commande.**