Les attaques par force brute ou brute force en anglais permettent de trouver le nom d'utilisateur ou un mot de passe en recherchant toutes les combinaisons possibles. Pour ce faire les pirates utilisent souvent des logiciels spécialisés pour effectuer l'attaque. Ces attaques sont longues à faire car tester toutes les combinaisons possibles de chaines de caractère est long. Pour simplifier cette tâche les pirates utilisent souvent des dictionnaires. Un dictionnaire pour les attaques par force brute est un ou plusieurs fichiers qui contiennent des chaines de caractères diverses et variées pour éviter à la machine de rechercher toutes les combinaisons possibles et donc gagner du temps. En plus des dictionnaires, les pirates utilisent aussi des algorithmes qui permettent de mettre certaines lettres en majuscules ou des caractères spéciaux à certains endroits. Il y a aussi des attaques par force brute inversée, ça consiste à utiliser un mot de passe qui a fuité par exemple et ensuite rechercher tous les noms d'utilisateur qui pourraient utiliser ce mot de passe, cela est pratique quand un pirate veut revendre des comptes car plus il a de comptes à vendre, plus il se fera d'argent donc s'il trouve plusieurs comptes avec le même mot de passe il pourra revendre plus de comptes. Beaucoup de pirates peuvent trouver un mot de passe en moins d'une seconde grâce aux dictionnaires. S'ils n'avaient pas eu de dictionnaire cela aurait pris plusieurs années. Des outils automatisés sont également disponibles pour vous aider à lutter contre les attaques par force brute (Brutus, Medusa, THC Hydra, Ncrack, John the Ripper, Aircrack-ng et Rainbow, par exemple). Ces outils agissent contre de nombreux protocoles informatiques (FTP, MySQL, SMPT et Telnet par exemple) et permet à des pirates de craquer des modems sans fil, d'identifier des mots de passe faibles, de déchiffrer les mots de passe en stockage chiffré, de traduire des mots en leet speack (« don'thackme » [nemepiratepas] devient « d0n7H4cKm3 », par exemple), d'exécuter toutes les combinaisons de caractères possibles et d'opérer des attaques par dictionnaire. Les protocoles cités précédemment sont des protocoles qui ne sont pas ou très peu sécurisé donc les mots de passes peuvent se trouver facilement.