Introduction à l'exploitation binaire (pwning)

Guillaume Pillot aka salt

Club de sécurité de l'université Laval

02 Octobre 2024

Qui suis-je ?

- Guillaume Pillot aka salt sur Discord
- Testeur d'intrusion depuis 6 ans
- Ancien étudiant de l'université Laval
- Responsable du club de hacking de l'université de 2015 à 2016
- Passionné de sécurité informatique
- Participe régulièrement au compétition de hacking (CTF)
- Conçois des challenges pour le hackfest depuis 2020
- Sites web :
  https://guillaume-pillot.ca
  http://clubsecuriteinformatique.ift.ulaval.ca/
  https://www.salt-hacking-blog.com/
  https://desencyclopedie.org/wiki/Linux

Prérequis

- Base en Python
- Base en réseau
- Base en ligne de commande Linux
- NB : Je recommande d'installer tous les tools de la présentation dans une VM Linux comme Kali Linux

Pwntools

- Pwntools est un framework écrit en Python utilisé dans les CTFs ou pour le développement d'exploit
- https://docs.pwntools.com/en/stable/

Premier challenge

- nc 159.203.46.23 1234
- Aide : Lien

Prérequis

- Base en C
- Base en assembleur

Ghidra

- Ghidra est un désasembleur développé par la NSA
- Le tool est gratuit et très complet
- Ghidra génère du pseudo code en C
- https://ghidra-sre.org/

Deuxième challenge

- nc 159.203.46.23 2222
- Télécharger le binaire

Prérequis

- Base en assembleur
- Binaire/hexadécimal

gdb-peda

- gdb est un vieux tool mais un très bon tool de débogage sur Linux
- gdb-peda est une extension très utile que je recommande
- https://github.com/longld/peda

Troisième challenge

- nc 159.203.46.23 3333
- Télécharger le binaire

En quoi cela consiste ?

- Un programme vulnérable permet à un attaquant d'écraser les données de la pile du programme
- Cela arrive avec l'utilisation de fonction vulnérable comme gets() ou un mauvais usage des pointeurs (par exemple une instruction qui écrase le null byte à la fin d'une chaîne de caractère)
- Avec un bufferoverflow il est souvent possible d'overwrite l'adresse de retour de la fonction du programme
- Si on met une adresse valide dans l'adresse de retour, il est possible de détourner le flux d'exécution du programme
- En règle général, l'attaquent essaye de redirigé le programme vers un shellcode pour exécuter des commandes sur le serveur comme /bin/sh par exemple

En quoi cela consiste ?

- nc 159.203.46.23 4445
- Télécharger le binaire

- Hacking : The Art of Exploitation
- RPI SEC MBE
- OSED
- x64/ARM/MIPS/OSEE/heap overflow