ATIS - Software Reverse Engineering

Prof. Dr. Christian Dietrich
dietrich@internet-sicherheit.de

3 Lab: Disassembly Part 2

Aufgabe

Das Ziel dieser Praktikumsaufgabe besteht darin, die Semantik aus der Disassembly eines Binärcode-Ausschnitts zu ermitteln. Dazu sollen Sie die Disassembly verstehen, die Sie in der vorherigen Praktikumsaufgabe erarbeitet haben und ein Ergebnis zu gegebenen Eingaben berechnen.

Es handelt sich bei dem gegebenen Code um eine Funktion, die die `cdecl`-Aufrufkonvention nutzt, ein Byte-Array zurückgibt und folgende Signatur besitzt:

```
1 _BYTE *  __cdecl func(BYTE *arg0, signed int arg1)
```

Die Funktion, die in Instruktion 9 (`call 0x10003f3c`) aufgerufen wird, allokiert (Heap-)Speicher. Sie erwartet ein Argument (die Größe des zu allokierenden Speicherbereichs), nutzt ebenfalls die `cdecl`-Aufrufkonvention und gibt einen Pointer auf den allokierten Speicher zurück:

```
1 LPVOID __cdecl MyAlloc(SIZE_T dwBytes)
```

Den Code der Funktion `MyAlloc()` benötigen Sie für das Verständnis nicht.

In der zu untersuchenden Funktion wird Speicher an der Adresse 0x100071B4 referenziert. Der folgende Hexdump zeigt den Inhalt beginnend an der referenzierten Speicheradresse:

```
100071B4  53 09 5A 7C 63 08 26 43  1A 33 23 1D 3C 39 00 00  S.Z|c.&C.3#.<9..
100071C4  18 6C 28 12 06 64 15 71  34 57 4F 71 06 7A 3F 0E  .l(..d.q4WOq.z?.
100071D4  50 3A 08 27 76 5F 00 00  00 61 36 0B 02 78 4F 6D  P:.'v_...a6..xOm
100071E4  7E 5F 4F 00 1C 65 3F 4F  51 26 42 2F 76 00 00 00  ~_O..e?OQ&B/v...
100071F4  06 7B 36 11 0C 66 08 27  76 5F 00 00 16 71 2A 1D  .{6..f.'v_...q*.
10007204  0D 6C 63 2D 6C 5A 51 72  52 54 36 67 2E 2F 17 7A  .lc-lZQrRT6g./.z
10007214  4F 2D 7D 40 74 00 00 00  10 7B 3F 1D 17 6D 76 31  O-}@t....{?..mv1
10007224  75 50 46 6E 4F 6E 00 00  38 6C 23 1E 07 57 43 35  uPFnOn..8l#..WC5
```

Um das abzuliefernde Ergebnis zu ermitteln, nehmen Sie an, dass die zu untersuchende Funktion mit folgenden 2 Argumenten aufgerufen wird:

a. Das erste Argument (arg0) ist ein Byte-Array, das sich ergibt, wenn folgender String hexadezimal dekodiert wird: `02 38 30 35 0A 6A 63 02 74 7C 53 51 6C 7F 1F 3E 3F 45 04 44 4B`

b. Das zweite Argument (arg1) ist 21.

Eingaben

- Datei mit dem Namen `binarycode1`
- Speicheradresse 0x100030d1; an diese Adresse wird der Code aus der Datei `binarycode1` gemapped

Abzuliefernde Ergebnisse

Ermitteln Sie den Inhalt des Speicherbereichs, der in der Funktion allokiert und als Return value zurueckgegeben wird. Es handelt sich um ein Byte-Array, daher sollten Sie das Ergebnis als hexadezimal-kodierte Zeichenkette einreichen.

Hinweise

- Es wird empfohlen, die Disassembly Schritt fuer Schritt durchzugehen und jede Instruktion zu annotieren.
- Wenn Sie die Instruktionen nachvollzogen haben, beginnen Sie Schritt fuer Schritt, die Eingaben zu verarbeiten.