UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR IT-SICHERHEIT

Praktikum 7

Reverse Engineering: Dynamische Analyse

Zu bearbeiten bis zum 20. Juni 2023

Cybersecurity im Sommersemester 2023

Jan Wichelmann, Anja Köhl

Einführung

Das Unternehmen *Immature Technical Solutions* (ITS) braucht weiterhin Ihre Hilfe. Neben der datenverschlüsselnden Software hat der unbekannte Gegner (EVE?) auf den Firmenservern auch noch verschiedene binäre Bomben hinterlassen, die durch gezielte Eingriffe die Hardware unbrauchbar machen sollen.

Die binären Bomben bestehen aus mehreren Modulen. Jedes Modul kann entschärft werden, indem Sie die richtige Zeichenfolge eingeben. Wird eine falsche Zeichenfolge eingegeben, explodiert die Bombe. ITS bittet Sie, für eine Bombe so viele Module wie möglich unschädlich zu machen und EVEs Plan zu vereiteln.

Zum Glück hat ITS recht robuste Hardware gekauft, die einigen Explosionen standhält – aber auch diese Hardware hat ihre Grenzen, es gilt also größte Vorsicht!

Aufgabe 1 Eine binäre Bombe vom Server laden

Sie können über den gewohnten Weg mithilfe des CTF-Systems auf den Praktikumsserver zugreifen. Auf der Übersichtsseite sehen Sie einige Zugangsdaten sowie den aktuellen Status der einzelnen Module. Sie haben nun zwei Möglichkeiten zur Bearbeitung der Aufgaben:

- Sie loggen sich über SSH auf dem zum Praktikum gehörenden Linux-Server ein. Die zur Bearbeitung nötigen Tools sind alle bereits vorinstalliert. Sie finden die ausführbare Bombe in Ihrem Homeverzeichnis.
- Sie laden die Bombe über den vorgegebenen SCP-Befehl herunter. Beachten Sie hierzu folgendes:
  - Die Bombe ist ausschließlich für die Systeme von ITS ausgelegt und daher auch nur für deren Hardware schädlich; sie stellt keine Gefahr für Ihr lokales System da, die Nutzung einer virtuellen Maschine ist hier also ausnahmsweise nicht notwendig.
  - EVE hat mit so etwas natürlich gerechnet und sich eine Gegenmaßnahme überlegt. Die Inspiration kam hier aus der (für derartige Tricks bekannten) Spieleindustrie: Die Bombe hat Online-Zwang!

    Irgendwo in den undurchdringlichen Netzwerken von ITS hat EVE es fertiggebracht, einen manipulationssicheren Command&Control-Server anzulegen, der die eingegebenen Zeichenketten nochmals überprüft und gegebenenfalls selbstständig eine Explosion auslöst. Es muss ständig eine Netzwerkverbindung vorliegen, da die Bombe ohne den Server nicht funktioniert.
  - Für die korrekte Funktion der Bombe müssen auf Ihrem System unter anderem die folgenden Pakete installiert sein:
    * `libcurl4`
    * `libncurses5`

Weiterhin sollte das Terminalfenster groß genug sein, um das Hauptmenü korrekt darstellen zu können. Vergrößern Sie Ihr Terminalfenster gegebenenfalls, wenn Sie Darstellungsfehler bemerken. Wenn die Bombe abstürzen sollte oder Sie die Ausführung über den Debugger beenden, kann es passieren, dass das Terminal in einem inkonsistenten Zustand verbleibt. Sie können dies reparieren, indem Sie entweder die Bombe nochmals ausführen und regulär beenden, oder, falls dies nicht möglich ist, den folgenden Befehl eingeben:

```
reset^J
```

Das entspricht der Eingabe der Zeichenkette `reset` und anschließend der Tastenkombination `Strg+J`.

Aufgabe 2 Entschärfung der Bombe

Um ITS zu helfen, müssen Sie so viele Module der Bombe zu entschärfen wie möglich, mindestens jedoch die folgenden vier:

- Modul 0, ◀ 30 / 6
- Modul 1, ◀ 30 / 6
- Modul 2, ◀ 40 / 8
- Modul 5. ◀ 40 / 8

Die verbleibenden Module sind:

- Modul 4, ◁ 50 / 10
- Modul 3, ◁ 50 / 10
- Modul 7, ◁ 60 / 12
- Modul 8, ◁ 70 / 14
- Modul 6, ◁ 70 / 14
- Modul 9. ◁ 70 / 14

Während die Modulreihenfolge in der Bombe offensichtlich von EVE anders vorgegeben ist, scheint die Reihenfolge bei der Entschärfung keine Rolle zu spielen. Ein Praktikant war daher so freundlich, die Module nach (vermeintlicher) Schwierigkeit zu sortieren. Natürlich möchte ITS Sie für Ihre Arbeit honorieren, daher liefert die Entschärfung jedes Moduls eine gewisse Punktzahl.

Da die Hardware wie schon erwähnt recht robust ist, haben Sie pro Modul außerdem eine Explosion „frei“; jede weitere Explosion führt jedoch zu Punktabzug.

Sie können für die Entschärfung der Bombe diverse Tools verwenden. Schauen Sie sich dazu die Hinweise am Ende dieses Dokuments für einige Tipps und Ideen an.

Die Bombe ist folgendermaßen konstruiert:

- Im Hauptmenü (`main`-Funktion) kann mit den Pfeiltasten und der Entertaste das zu entschärfende Modul ausgewählt werden. Die Bombe erwartet dann eine Eingabe von Ihnen, die Sie mit der Entertaste absenden können.
- Die `main`-Funktion ruft im Anschluss das entsprechende Bombenmodul auf, welches der Funktion `moduleX` für Modul `X` entspricht.

  ```
  bool moduleX(const char *input)
  {
      // Parse and check input...
  }
  ```

- Im Bombenmodul wird der Eingabestring verarbeitet. Dies geschieht in fast allen Fällen zuerst über die Funktion `read_input`:

  ```
  int read_input(uint32_t moduleId, const char *input, const char *format, ...);
  ```

  Diese verhält sich genauso wie die Standard-C-Funktion `sscanf`, welche einen String in „Wörter“ aufspaltet und diese entsprechend einiger Formatangaben in Variablen schreibt.

- Das Modul führt nun einige Berechnungen auf der Eingabe aus. Wenn diese zum Erfolg führen, wird die Funktion `defused` aufgerufen, und das Modul gilt als entschärft. Im gegenteiligen Fall wird `explode` aufgerufen, und die Bombe explodiert.
- Da EVE daran gelegen ist, dass Sie die Bombe ausführen, um sie zu untersuchen, enthält diese einige Gegenmaßnahmen gegen statische Analyse. Wundern Sie sich daher nicht, wenn `objdump` Ihnen für einige Funktionen keine sinnvolle Disassembly ausgibt.

Hinweise

Es gibt viele Wege eine Bombe zu entschärfen. So könnten Sie sie im Detail untersuchen, ohne sie einmal auszuführen. Eine statische Analyse stellt eine sinnvolle Taktik dar, die aber nicht immer so leicht umzusetzen ist, da es häufig Gegenmaßnahmen dagegen gibt (wie auch in diesem Fall).

Eine andere Herangehensweise ist es, die Bombe mit einem Debugger auszuführen und Schritt für Schritt herauszufinden, welche Berechnungen durchgeführt werden. Diese Informationen können dann dazu benutzt werden, die richtige Eingabe zu bestimmen und die Bombe zu entschärfen. Diese Methode stellt vermutlich die schnellste und einfachste Möglichkeit dar, möglichst viele Module zu entschärfen. Jedoch laufen Sie Gefahr, dass die Bombe explodiert, Sie sollten also mit äußerster Vorsicht vorgehen!

Die Eingabestrings durch Ausprobieren zu bestimmen, stellt keine sinnvolle Strategie dar:

- Sie verlieren Punkte für falsche Eingaben bzw. Explosionen. Die meisten Funktionen lassen sich ohne Serververbindung nicht nutzen, wodurch effiziente Offline-Brute-Force-Angriffe massiv erschwert werden.
- EVE hat nicht spezifiziert, wie lang die Eingabestrings sind oder welche Zeichen sie enthalten. Während eine vollständige Überprüfung aller möglichen Eingaben bei einigen Modulen noch machbar erscheint, gibt es bei anderen erheblich mehr Eingabemöglichkeiten, als Sie in der gegebenen Zeit testen könnten.

Es gibt viele Tools, die speziell dazu entwickelt wurden, Sie beim Bombenentschärfen zu unterstützen. Nachfolgend finden Sie eine (unvollständige) Liste:

GDB

Der GDB (GNU Project Debugger) ist ein Kommandozeilendebugger, der quasi jede Plattform unterstützt. Mit ihm kann man ein Programm disassemblieren, es schrittweise durchlaufen und Speicher- sowie Registerinhalte untersuchen.

Sie finden im Moodle ein kleines Cheat-Sheet mit den wichtigsten Befehlen zur Benutzung von GDB.

Eine nützliche Erweiterung für GDB ist GEF (GDB Enhanced Features)[1]. Diese zeigt unter anderem standardmäßig ein übersichtliches Interface an, dass die Benutzung von GDB erheblich vereinfacht. GEF ist auf dem Praktikumssystem vorinstalliert.

Um die Bombe mit GDB zu analysieren, führen Sie die folgenden Befehle aus:

```
gdb ./bomb
start
```

Letzteres Kommando startet das Programm und bringt Sie in die `main`-Funktion, von wo aus Sie mit Ihrer Analyse fortfahren können. Bitte führen Sie vorher keine anderen Kommandos aus (z.B. Setzen von Breakpoints), da es dort zu Konflikten mit der Sicherheitsmaßnahme gegen statische Analyse kommen kann!

objdump

Dieser Befehl zeigt Informationen an, ohne das Programm auszuführen (statische Analyse). Sie können sich hiermit z.B. die Symboltabelle ausgeben lassen, welche die Namen aller Funktionen und globalen Variablen in der Bombe enthält. Außerdem kann objdump Programme disassemblieren.

Zum Disassemblieren der gesamten Bombe in Intel-Syntax und Speichern des Resultats in einer Datei bietet sich der folgende Befehl an:

```
objdump -d -M intel bomb >bomb.asm
```

Um zusätzlich einen Hexdump aller Inhalte zu erhalten, kann das Flag `-s` benutzt werden. Weitere Parameter finden Sie in der zugehörigen Man-Page (`man objdump`), und in dem integrierten Hilfetext (`objdump --help`).

[1] `https://github.com/hugsy/gef`

strings

Das Tool `strings` zeigt alle druckbaren Strings in einem Programm an.