Aufgaben - Reverse Engineering

W3WI_SE411 - Forschungsseminar Informatik / Advanced Practical IT Security

Dozent: Prof. Dr. Michael Eichberg

Kontakt: michael.eichberg@dhbw-mannheim.de, Raum 149B

Version: 23SEB (**Work in Progress**)

Einführung

Ziel dieser Aufgabe ist es einen ersten Einblick in den Bereich des Software Reverse Engineering zu bekommen. Da es beim Reverse Engineering auch darum gehen kann Schutzsysteme - z. B. durch das Aufdecken von Schwachstellen oder durch Brute-Force - zu umgehen, ist dies auch in diesem Fall Ihre Aufgabe.

Für diese Aufgaben ist es ggf. notwendig (ein bisschen) Code zu schreiben. Für die Abgabe können Sie ggf. Ihren Code in folgenden Sprachen abgeben: Java (ggf. als Script), Python, Scala, C, C++, Rust, JavaScript, TypeScript, Prolog, Bash oder Zsh. Weitere Sprachen sind ggf. nach Rücksprache möglich.

Für die Bewertung gilt: Auch wenn Sie das Ziel nicht erreichen, dann sollten Sie auf jeden Fall eine Beschreibung des Weges und ggf. des bisherigen Codes einreichen.

Es ist im Rahmen des Reverse Engineering fast immer so, dass mehrere Wege zum Ziel führen. Sollte ein Weg nicht erfolgreich sein, dann probieren Sie einen anderen. Das Wichtigste ist Beharrlichkeit!

Es steht ihnen vollkommen frei welchen Weg sie gehen. Im Rahmen dieser Aufgaben dürfen Sie auch AI Assistenten frei einsetzen. Es ist jedoch bei der Abgabe erforderlich explizit darauf hinzuweisen.

!! Wichtig

Sollten Sie das Ziel erreichen, dann führen Sie eine Bewertung Ihrer Lösung durch. Die Bewertung muss besprechen wie wahrscheinlich es ist, dass Sie mit Ihrer Lösung in anderen Fällen - bei Verwendung der selben Software - auch erfolgreich sein werden bzw. welches die begrenzenden Faktoren sind. D. h. es muss klar werden welcher Aufwand in einem vergleichbaren Fall notwendig wäre, um das Ziel zu erreichen.

Bewertung

Aufgabe	Punkte
...	1

!! Wichtig

Es ist lediglich erforderlich XXX Punkte zu holen, um diesen Teil mit 100% Erfolg gewertet zu bekommen.

Überschüssige Punkte können nicht übertragen werden.

Bemerkung

Im Rahmen des Reverse Engineering kann es immer mal wieder vorkommen, dass Ihnen eine Aufgabe mehr oder weniger liegt. Sie sollten deswegen die Punkte erst einmal außen vor lassen.

Abgaben

Lösungswegbeschreibungen

Für jede Aufgabe müssen Sie Ihren Weg genau beschreiben, da dieser essentieller Bestandteil der Prüfung ist.

Nicht-standard Werkzeuge

Entwickeln Sie selber Tools/Skript, dann dokumentieren Sie diese (d. h. den Quellcode).

Laden und kompilieren Sie Skripte aus dem Internet, dann dokumentieren Sie die Quellen und ggf. die Schritte, um das Skript zu nutzen.

EphermalSafe

※ Hinweis

Diese Aufgabe ist ggf. nicht nur eine Reverse Engineering Aufgabe. Es ist ggf. erforderlich den Netzwerkverkehr zu beobachten, um entscheidende Informationen zu erhalten. Alternativen sind auf jeden Fall auch möglich. Sie können davon ausgehen, dass zum Lösen etwas “Scripting” erforderlich ist.

Jede Datei ist mit einem anderen Passwort verschlüsselt und enthält andere Daten.

Zur Ausführung des Codes ist ggf. Java 25 erforderlich.

Sollten Sie UTM unter Mac OS verwenden, um aus einer VM heraus auf den Server an der DHBW zuzugreifen, dann ist es ggf. notwendig die Netzwerkkonfiguration auf “emulated Vlan” bzw. “bridged” umzustellen. Andernfalls können Sie ggf. nicht den Server erreichen.

Um den Netzwerkverkehr zu beobachten können Sie TCPDump oder (empfohlen) Wireshark verwenden. Denken Sie daran, dass Wireshark ggf. mit Administratorrechten (“sudo” unter Linux/Mac) ausgeführt werden muss, um auf alle Schnittstellen zugreifen zu können.