

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

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 zu analysieren - z. B. durch das Aufdecken von Schwachstellen oder durch Brute-Force - 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 Skript), 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 bisherigen 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.

!! Wichtig

Im Rahmen dieser Aufgaben dürfen Sie AI Assistenten frei einsetzen. Es ist jedoch bei der Abgabe erforderlich explizit darauf hinzuweisen in welcher Weise Sie AI Assistenten eingesetzt haben.

◆ Bemerkung

Im Rahmen des Reverse Engineering kann es immer mal wieder vorkommen, dass Ihnen eine Aufgabe mehr oder weniger liegt. Fokussieren Sie sich deswegen nicht zu sehr auf die Punkte sondern fokussieren Sie sich darauf wo sie glauben am Besten Fortschritte erzielen zu können.

※ Hinweis

Für die Analyse der nativen Binärdateien können Sie gerne Werkzeuge wie Ghidra, Radare2 oder ähnliche verwenden. Ggf. ist der Einsatz von Kali Linux hilfreich. Ghidra kann dort einfach mit `sudo apt install ghidra` installiert werden. Die Binaries wurden alle in einer VM getestet und laufen dort problemlos. Ggf. ist die Emulation (!) von ARM64 oder x86_64 erforderlich.

※ Hinweis

Sollten Sie Probleme haben die nativen Binärdateien auszuführen, dann nutzen Sie ggf. das Tool `file` um herauszufinden, für welche Architektur die entsprechende Binärdatei kompiliert wurde und welche Bibliotheken ggf. fehlen bzw. installiert werden müssen.

(Es gibt zum Beispiel verschiedene Implementationen der C Standardbibliothek. Diese können sich in Details unterscheiden, was dazu führen kann, dass eine Binärdatei nicht ausgeführt werden kann und es dann zu - teilweise sehr verwirrenden - Fehlermeldungen kommt.)

※ Hinweis

Die Analyse von Java Class Dateien kann zum Beispiel über FenFlower (eingebaut in IntelliJ IDEA; als Plug-in für VS Code verfügbar) oder CFR erfolgen.

Bewertung

Aufgabe	Punkte
EncryptMe	8
EncryptMe2	8
Secure24v1	5
Secure24v2	7
EphemeralSafe	12
	Σ 40

!! Wichtig

Es ist lediglich erforderlich 25 Punkte zu holen, um diesen Teil mit 100% Erfolg gewertet zu bekommen.

Überschüssige Punkte können nicht übertragen werden.

Abgaben (Pro Aufgabe)

Die Punkte pro Teilabgabe hängen von der konkreten Aufgabe ab.

Verschlüsselungsalgorithmus

Beschreiben Sie wie die Verschlüsselung funktioniert. Falls mehrere Dinge verschlüsselt sind, dann gilt dies für alle Teile.

Schwachstellenbeschreibung

Beschreiben Sie mit Ihren eigenen Worten die Schwachstelle, die Sie identifiziert/ausgenutzt haben, um die Aufgabe zu lösen.

Lösungswegbeschreibungen

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

Wenn Sie während des Prozesses auf (magische/relevante) Konstanten gestoßen sind, dann sollten Sie diese ebenfalls dokumentieren. Sollten Sie charakteristische Werte berechnet haben, dann müssen diese ebenfalls dokumentiert werden.

Die Lösungswegbeschreibung enthält jedweden Code, den Sie entwickelt haben bzw. haben lassen, um die Aufgabe zu lösen.

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.

Bewertung der Lösung in Hinblick auf Generalisierbarkeit

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 oder ob dies nicht genau abgeschätzt werden kann bzw. ggf. eine Anpassung Ihrer Lösung notwendig ist. Betrachten Sie ggf. nicht nur den aktuellen Zustand sondern auch wie es in der Zukunft aussehen könnte.

EncryptMe [8 Punkte]

0.1. Mit EncryptMe verschlüsselte Datei entschlüsseln

Ziel dieser Aufgabe ist es die Datei zu entschlüsseln. Die Verschlüsselung ist mit der Software `encryptme` durchgeführt worden.

※ Hinweis

Die Software liegt sowohl als ARM als auch als x86_64 Version vor. Beide sind in der Lage die Datei zu entschlüsseln und funktional identisch. Sollten Sie also mit einer der Architekturen vertrauter sein, dann verwenden Sie diese.

EncryptMe2 [8 Punkte]

0.2. Mit EncryptMe2 verschlüsselte Datei entschlüsseln

Ziel dieser Aufgabe ist es die Datei zu entschlüsseln. Die Verschlüsselung ist mit der Software `encryptme2` durchgeführt worden.

※ Hinweis

Die Software liegt sowohl als ARM als auch als x86_64 Version vor. Beide sind in der Lage die Datei zu entschlüsseln und funktional identisch. Sollten Sie also mit einer der Architekturen vertrauter sein, dann verwenden Sie diese.

Secure24v1 [5 Punkte]

Ihnen liegt eine verschlüsselte Datei vor: `Message.odp.encrypted`, die mit dem Programm `Secure24v1` verschlüsselt wurde. Informationen zum verwendeten Passwort liegen nur begrenzt vor. Es ist davon auszugehen, dass das Passwort sicher ist. Es liegt Ihnen aber noch die Datei `key` vor. Weiterhin ist davon auszugehen, dass die verschlüsselte Datei tatsächlich eine OpenOffice/LibreOffice Präsentation ist.

Analysieren Sie die Anwendung, um einen möglichen Ansatzpunkt zu finden, um die Datei erfolgreich zu entschlüsseln.

Hintergrund

Informationen über den Aufbau von OpenOffice Dateien finden sich zum Beispiel hier:

<http://docs.oasis-open.org/office/v1.0/OpenDocument-v1.0-os.pdf>

Insbesondere Abschnitt 17 enthält Informationen zum Aufbau von entsprechenden Dateien und wie diese erkannt werden können.

Secure24v2 [7 Punkte]

Neben dem Programm `secure24v2` liegen die beiden Dateien: `Text.encrypted` und `key` vor.

In diesem Falle sind keinerlei Informationen über das Passwort bekannt. Beim Inhalt ist davon auszugehen, dass es sich um eine einfache Textdatei handelt. Ziel ist die Entschlüsselung der Datei.

EphemeralSafe [12 Punkte]

Im Rahmen einer forensischen Analyse der Daten einer sichergestellten Festplatte wurde ein neues Program *EphemeralSafe* gefunden. Die Informationen, die Sie im Rahmen einer Recherche finden konnten, besagen, dass das Programm besonders sicher ist und eine Ver-/Entschlüsselung von Daten nur bei bestehender Internetverbindung möglich ist. Als besonderes Feature wird angepriesen, dass verschlüsselte Daten nicht mehr entschlüsselt werden können sobald den Betreibern mitgeteilt wurde, dass der Dateninhaber sich in einer für ihn unpässlichen Situation befindet. Selbstverständlich garantiert der Betreiber, dass er niemals die Daten seiner Nutzer entschlüsseln kann und dass er auch Missbrauch etc. versucht zu entdecken und ggf. pro-aktiv Accounts schließt.

Ihnen wird das Java Programm übergeben sowie eine verschlüsselte Datei und die Information über den mutmaßlichen Lizenzschlüssel des Nutzer.

Aus Logdaten wissen Sie, dass der Server auf folgender Adresse läuft (nur aus dem DHBW Netzwerk bzw. über VPN erreichbar):

141.72.13.52:3000

Von den Ermittlern erhalten Sie weiterhin die Information, dass alle bisher ermittelten Passwort einfach waren.

Ziel dieser Aufgabe ist es die Ihnen zugeordnete Datei zu entschlüsseln. Jeder hat einen passenden Lizenzschlüssel, der zur Nutzung der Software erforderlich ist. Das erste Segment des Lizenzschlüssels ist dem Dateinamen angehängt.

Lizenzschlüssel

ID	Lizenzschlüssel
1	557118900-RRiTTSS_667789900-RRDSSTT_667789900-RRSSSTT_667789900-RRSKSTT
2	132117890-ABDJWWW_134567890-ABDJWWW_123456780-ABDJWWW_123456780-ABDJWWW
3	198054321-ZYXWVUT_098765421-ZYXWVUT_098765321-ZYXWVUT_098765321-ZYXWVUT
4	112663355-AABBCDD_112334455-ABBCCDD_112233455-ABBCCDD_1122334455-AABBCDD
5	662222200-XDXYYZZ_667889900-XDSYZZZ_667889900-XXYPYZZ_667789900-XdXYYZZ
6	557788900-RRiTTSS_667789900-RRDSSTT_667789900-RRSSSTT_667788990-RRSKSTT
7	132467890-ABDJWWW_134567890-ABDJWWW_123456780-ABDJWWW_123456780-ABDJWWW
8	197654321-ZYXWVUT_098765421-ZYXWVUT_098765321-ZYXWVUT_098765321-ZYXWVUT
9	112664455-AABBCDD_112334455-ABBCCDD_112233455-ABBCCDD_1122334455-AABBCDD
10	667458900-XDXYYZZ_667889900-XDSYZZZ_667889900-XXYPYZZ_667789900-XdXYYZZ
11	223346766-EETFFGG_223445566-EEDFFGG_223345566-EQEFGG_223344566-EEGFFGG
12	334400077-HHIGJKK_344556677-HHIDJKK_334456677-HHIJAKK_334455667-HHdIJKK
13	443567788-LLMMNiN_455667788-LDLMNN_445567788-LLMSMNN_445567788-LLGMMNN
14	588877899-OOPGPQQ_556678899-ODOPPQQ_556678899-OOPQPQQ_556677889-OOPPQMQ
15	660988900-RRiSSSTT_667789900-RRDSSTT_667789900-RRSSSTT_667788990-RRSKSTT
16	667788900-RRiTTSS_667789900-RRDSSTT_667789900-RRSSSTT_667788990-RRSKSTT

17	123467890-ABDJWWW_134567890-ABDJWWW_123456780-ABDJWWW_123456780-ABDJWWW
18	097654321-ZYXWVUT_098765421-ZYXWVUT_098765321-ZYXWVUT_098765321-ZYXWVUT
19	112334455-AABBCDD_112334455-ABBCCDD_112233455-ABBCCDD_112234455-AABBCDD
20	667788900-XDXYYZZ_667889900-XDSYYZZ_667889900-XXYPYZZ_667789900-XdXYYZZ
21	223344566-EETFFGG_223445566-EEDFFGG_223345566-EQEFFGG_223344566-EEGFFGG
22	334456677-HHIGJJK_344556677-HHIDJJK_334456677-HHIJAKK_334455667-HHdIJJK
23	445667788-LLMMNiN_455667788-LDLMMNN_445567788-LLMSMNN_445567788-LLGMMNN
24	556677899-OOPGPQQ_556678899-ODOPPQQ_556678899-OOPQPQQ_556677889-OOPPQMQ
25	667788900-RRiSSTT_667789900-RRDSSTT_667789900-RRSSSTT_667788990-RRSKSTT

※ 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.

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.