Chapter 01: PyDroid

Rules & Description

Introduction

Welcome to the first Android challenge built around obfuscation, dProtect, and O-MVLL.

The main goal of this challenge is to find the correct login/password that leads to "Access Granted".
To reach this goal, you might have to reverse engineering several layers of protection.

The side goal of this challenge is to evaluate how long a binary protected with open-source solutions can resist against reverse engineering.

Sponsors:

BINARYNINJA

build

build38.com

eShard

The Challenge

This challenge is represented as an Android application running from Android 9 to Android 13. To be as close as possible to modern applications, the challenge can only run on an AArch64 device. In particular, it is on purpose to **NOT** provide the x86/x86-64 version of the challenge.

All the protections used in this challenge are based on open-source and public information.

- The code obfuscation layer is exclusively based on O-MVLL and dProtect.
- The ELF modifications are similar from those described in this presentation: The Poor Man's Obfuscator.[1]
- The RASP checks are based on open-source projects and/or public blog posts.
- The "main" algorithms are known and public.

If you have questions or if some aspects of the challenge are unclear, feel free to reach out by email at this address: ping@obfuscator.re or to join the Discord server: http://discord.obfuscator.re.

The application is not supposed to crash at any point so if you identify a weird behavior, feel also free to reach out.

Practical information

Beginning of the challenge:	19/12/2022
End of the first part:	19/05/2023 I 23:59 (UTC+1)
End of the second part:	19/08/2023 I 23:59 (UTC+1)
URL:	https://romainthomas.fr/challenge-pydroid.apk
SHA-256:	a0b07e97197e2dfe48bb7df65dba4f145d485660ecf4bd0d3ab65b14039ec8d6
Email for the flag:	challenge-pydroid@obfuscator.re

[1] https://cfp.pass-the-salt.org/pts2022/talk/RJCGBC/

Rewards

How Fast Are You?

The first prize will reward the fastest person to find the correct login and password. This person will be able to choose between:

1. A Binary Ninja license.[1]
2. A 1300$/€ cash-prize.

The first person to find the correct login/password will be communicated as soon as the flag is submitted.

How Good Are You?

The second prize will reward the best write-up submitted.[2]

The prize for this section will depend on whether there is a winner for the previous part.
If that's the case, the winner will receive the remaining prize.
Otherwise, if there is no winner for the previous part, the winner will receive both prizes.

The winner for this part of the challenge will be communicated (at most) in the next 2 months following the end of the challenge.

Cash-Prize Notice

The winner of the cash-prize will have to provide all the required informations asked by the sponsors to receive the prize.

The winner could also decide to transform the amount of the prize into a gift card (e.g. Amazon gift card) or to make a donation to an open-source project.

[1] Non-commercial license
[2] With the correct login / password.

Closing Notes

Thank you to Binary Ninja, Build38 and eShard for offering the different prizes and for their trust in this challenge.

I hope you will enjoy this reverse engineering journey,

Romain

Binary Ninja is an interactive disassembler, decompiler, and binary analysis platform for reverse engineers, malware analysts, vulnerability researchers, and software developers.

https://binary.ninja/

Build38 provides mobile app protection solutions that combine AI and the strongest app shielding technology. Recognized in the GARTNER "In-App Protection Market Guide" and the first to combine app-hardening, threat monitoring and reaction.

https://build38.com/

eShard is a leading, independent security expert for in-depth security in ICs, software and IoT devices. The company provides a strong expertise in mobile and embedded software security, hardware fault injection, secure element, Host Card Emulation, whitebox cryptography assessment.

https://eshard.com/

ping@obfuscator.re