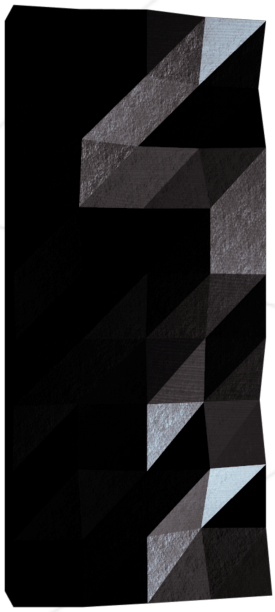

Immersion Cybersecurity (CTF)

Day 02: Gecko - Cell 11

Summary: On this cell, you will need to explore the purpose and functioning of hashes, as well as methods to crack them

Version: 1.0

Contents

Chapter I

Introduction

What this cell will help you understand:

- How to comprehend and identify ciphers, along with methods of concealing data.

Chapter II

General instructions

Unless explicitely specified, the following rules will apply every cell of this Immersion.

- This subject is the one and only trustworthy source. Don't trust any rumors.
- Be careful about the access rights of your files and folders.
- Your assignments will be evaluated by your Immersion peers.
- All shell assignments must run using /bin/bash.
- You must not leave in your turn-in your remote repository any files other than the ones explicitly requested by the exercise.
- You have a question? Ask your left neighbor. Otherwise, try your luck with your right neighbor.
- Every technical answer you might need is available in the man pages or on the Internet.
- Remember to use the Discord server dedicated to your Immersion.
- You must read the examples thoroughly. They can reveal requirements that are not obvious in the assignment's description.

Chapter III

Common Instructions

- The use of automated tools is forbidden unless specified in the subject.
- If no other format is specified, the flag format will be 42SP{this_is_a_test_flag}.
- Peer evaluations will assess your understanding of how to solve each challenge, so you must be able to clearly explain everything you did, and your peers must be able to understand your explanation.
- Exercises within this project follow a strict order, and you will not be able to proceed to further exercises if you have not completed the previous ones (e.g., You can't do cell01 without completing cell00).

Chapter IV

Cell 11

	Exercise : 11
Cell 11	
Turn-in directory : `gecko-cell11/`	
Files to turn in : `flag.txt`	
Forbidden functions : `None`	

All the previously discovered data appears to have limited utility, except for delivering 'flag.txt.' However, this new file holds more promise. Its name is 'ssh_password.txt,' and the contents of this file may contain an SSH key, which could grant you access to a server via SSH. Your mission is to uncover the true content of this data and attempt to use it to access an SSH server.

Marvin suggests that the SSH server is likely running on the same IP as our target, 10.51.1.198, and you should make an attempt to connect to it using 'ctf' as user.

Your ultimate goal is to discover the content of 'flag.txt,' indicated as 42SP{X}, where X represents the flag.

`John the Ripper.`

`Not all word lists will work; sometimes you need to create your own with the information you have.`

Chapter V

Submission and peer-evaluation

- Create a new 'gecko-cell11' folder and navigate to it. Place your 'flag.txt' file inside the folder and then push it.

Please note that during your evaluation, anything that is not present in the folder for the cell will not be checked.