



Cybersecurity Discovery Piscine

Tyto 00

by @alrodri2

Summary: In this exercise you will have your first contact with OSINT. The goal is simple, find a social media account with the information provided.

Version: 2.00

Contents

I	About this Cybersecurity Discovery Piscine	2
II	Introduction	3
III	General instructions	4
IV	Exercise 00	5
V	Submission and peer-evaluation	6

Chapter I

About this Cybersecurity Discovery Piscine

Welcome!

Welcome to this Discovery Piscine in cybersecurity, a challenge where you will dive into the basics of offensive cybersecurity while experiencing the unique educational model of 42. Here, you won't find traditional classes or a single correct solution; learning is collaborative, hands-on, and focused on you.

We invite you to explore the code that powers the software you use every day, while developing skills that go beyond the technical: logical thinking, problem-solving, and self-directed learning. Programming isn't about memorizing rules; it's about creatively assembling blocks to solve problems in your own unique way.

During this experience, you'll tackle key topics in cybersecurity:

- Terminal navigation: Learn to operate and navigate a system using basic commands.
- OSINT (Open Source Intelligence): Discover how to gather public information to identify potential threats.
- Web security: Understand common vulnerabilities in websites and how they are exploited.
- Cryptography: Familiarize yourself with the fundamentals of data and communication protection.

Peer learning and evaluation will play a central role in your journey. You'll exchange ideas, discuss solutions, and gain new perspectives by collaborating with your peers. This will not only enrich your learning experience but also help you build connections and develop critical skills for tackling future challenges.

Remember, this experience is as unique as you are: each participant will follow their own path, validate different projects, and face unique challenges. What truly matters is what you learn, from both your successes and your mistakes.

Good luck! We hope you enjoy this journey into the world of cybersecurity and collaborative learning.

Chapter II

Introduction

You've probably heard that "everything on the internet is public," but have you ever wondered just how far that information goes and how you can find it? OSINT (Open Source Intelligence) is the practice of exploring, collecting, and analyzing publicly accessible data to extract valuable insights.

In the digital world, learning to identify patterns, make connections, and analyze open sources will help you understand how information is generated and shared online. Beyond being just a simple Google search, OSINT is a skill that combines creativity, curiosity, and an analytical approach to decipher data and turn it into actionable knowledge.

Social media is a goldmine of information, especially when a user reuses the same "nickname" across multiple platforms. In this exercise, you'll learn to spot patterns, identify related profiles, and connect clues across various social networks.

What you'll learn in this exercise:

- Methods for tracking profiles across multiple platforms.
- Tools and techniques for searching by "nicknames."
- Basic profile analysis to determine authenticity.

Chapter III


General instructions

Unless explicitly specified, the following rules will apply on every cell of this Discovery Piscine.

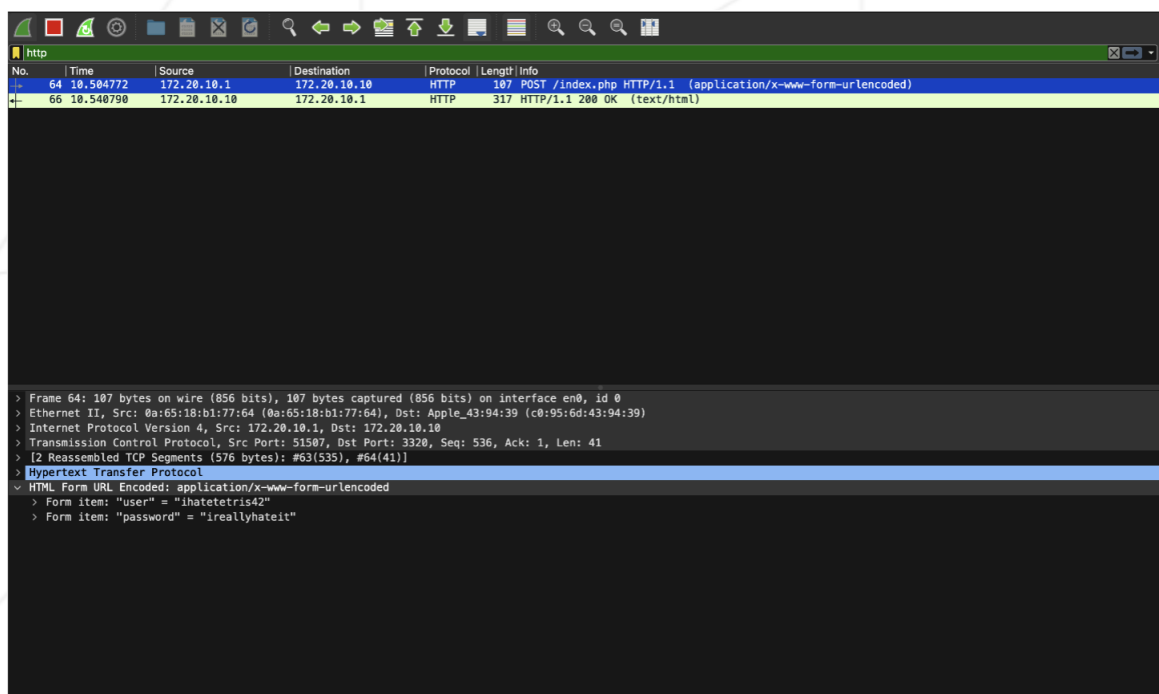
- This subject is the one and only trustable source. Don't trust any rumor.
- The assignments in a subject must be done in the given order. Later assignments won't be rated unless all the previous ones are perfectly executed.
- Be careful about the access rights of your files and folders.
- Your assignments will be evaluated by your Piscine peers.
- All shell assignments must run using `/bin/bash`.
- You must read the examples thoroughly. They can reveal requirements that are not obvious in the assignment's description.
- You have a question? Ask your neighbor on the left. Otherwise, try your luck with your neighbor on the right.
- Every technical answer you might need is available in the `man` or on the Internet.
- Remember to read the documentation and to use Slack!
- By Thor, by Odin! Use your brain!!!

Chapter IV

Exercise 00

	Exercise : 00
Stalker	
Turn-in directory : <i>ex00/</i>	
Files to turn in : flag.txt	
Forbidden functions : None	

The security team of 42 Barcelona has found some suspicious activity from one of the computers and decided to monitor the specific computer and all the traffic that was sent over the network. An interesting packet was found.



Could you give the profile link to what appears to be the social media account used by this suspicious user?

Chapter V

Submission and peer-evaluation

- Your task is to find the real URL used.
- When you have succeeded, you must write it into a `flag.txt` file.
- The `flag.txt` file should be located at `/tyto/ex00`.



Please note that during the evaluation, what we want to verify is that you have understood the exercise. You should be able to explain it and justify the decisions you made.