Immersion Cybersecurity (CTF).

Day 00: Tyto - Cell 00

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

Version: 1.0

Contents

Chapter I

Introduction

What this cell will help you understand:

- Learn the basics of OSINT.

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).

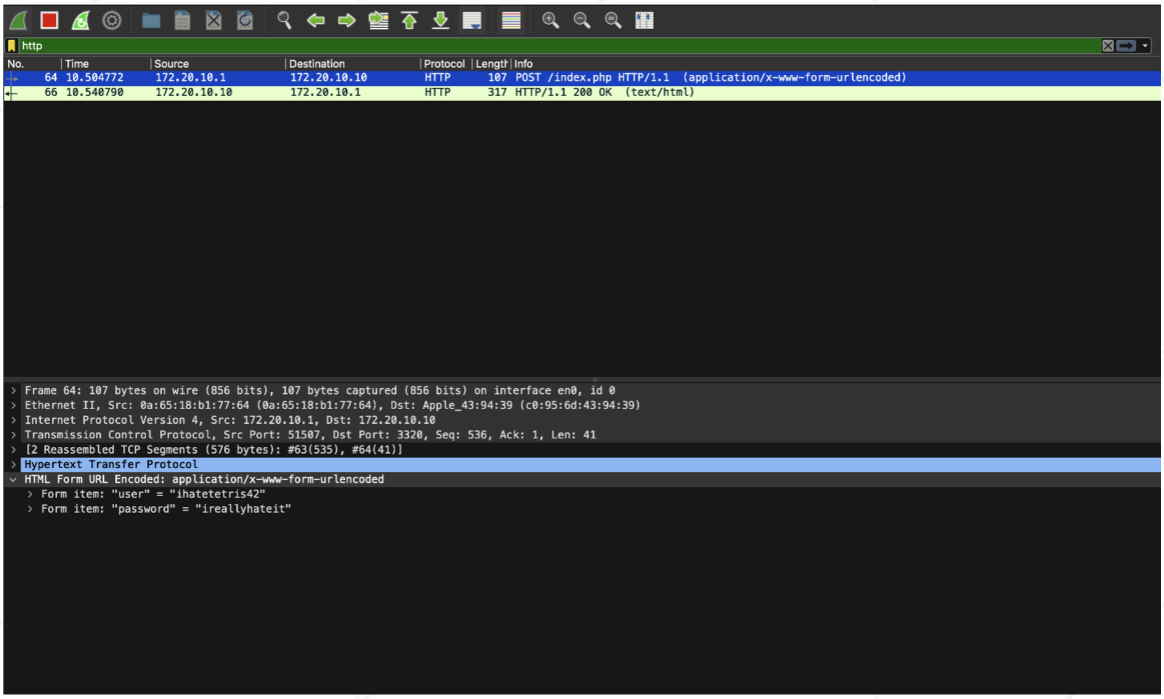
Chapter IV

Cell 00

	Cell: 00
Cell 00	
Turn-in directory : `tyto-cell00/`	
Files to turn in : `flag.txt`	
Recommended tools : `Wireshark`	

You are engaged in an attempt to breach a system, accompanied by a virtual assistant named Marvin. Together, you will endeavor to hack into the system. In this initial phase, your goal is to gather as much information as possible to identify potential vulnerabilities and initiate the process of exploiting software weaknesses effectively.

Marvin has detected packets being exchanged on the network, indicating access to a social media platform. These packets were captured on a privileged network, suggesting that the information shared likely originates from individuals with privileged access. Your task is to analyze these packets using Wireshark and uncover the URL of the social media profile accessed by the user during that time.



```
http

No.     Time        Source        Destination   Protocol Length Info
   64 10.504772   172.20.10.1   172.20.10.10  HTTP      107  POST /index.php HTTP/1.1  (application/x-www-form-urlencoded)
   66 10.540790   172.20.10.10  172.20.10.1   HTTP      317  HTTP/1.1 200 OK  (text/html)

> Frame 64: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface en0, id 0
> Ethernet II, Src: 0a:65:18:b1:77:64 (0a:65:18:b1:77:64), Dst: Apple_43:94:39 (c0:95:6d:43:94:39)
> Internet Protocol Version 4, Src: 172.20.10.1, Dst: 172.20.10.10
> Transmission Control Protocol, Src Port: 51507, Dst Port: 3320, Seq: 536, Ack: 1, Len: 41
> [2 Reassembled TCP Segments (576 bytes): #63(535), #64(41)]
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "user" = "ihatetetris42"
  > Form item: "password" = "ireallyhateit"
```

You must place the URL of the profile in the 'flag.txt' file.

`Check project attachments.`

Chapter V

Submission and peer-evaluation

- Create a new ’tyto-cell00’ 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.