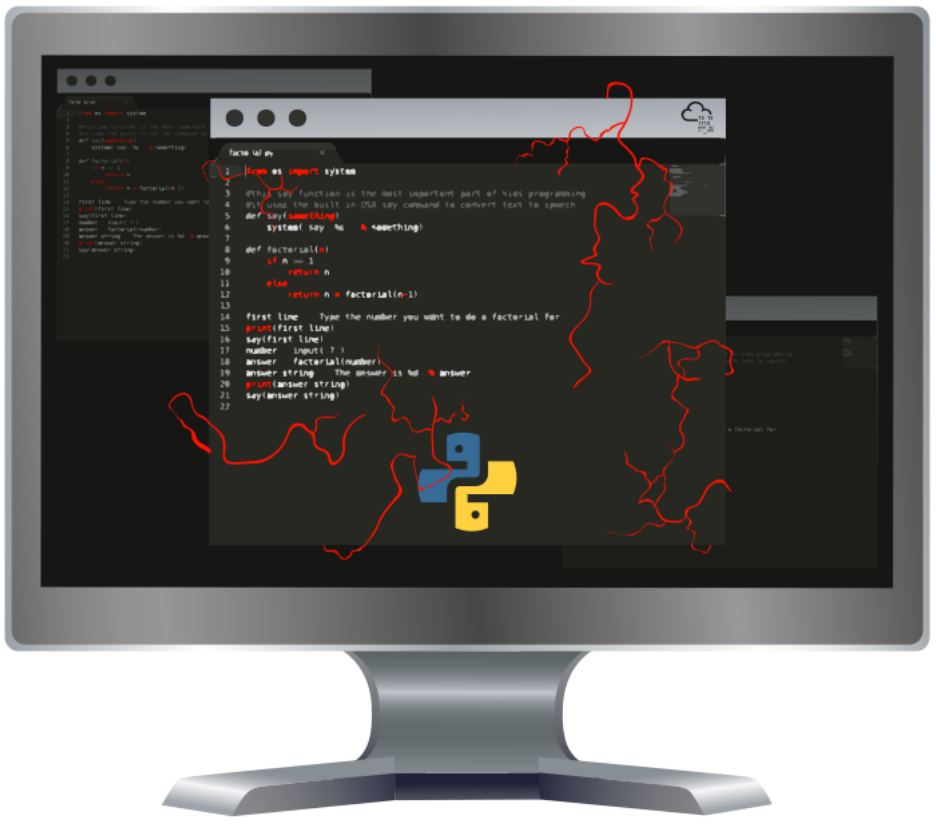


Python for Pentesters

Start AttackBox | Show Split View | Cloud Details | Awards | Help

Python is probably the most widely used and most convenient scripting language in cybersecurity. This room covers real examples of Python scripts including hash cracking, key logging, enumeration and scanning.

Chart | Scoreboard | Discuss | Writeups | More

Difficulty: Easy

Active Machine Information

Title	IP Address	Expires	
Py4PT2	10.10.96.99	1h 41m 29s	? Add 1 hour Terminate

41%

Task 1 Introduction

Task 2 Subdomain Enumeration

Task 3 Directory Enumeration

As it is often pointed out, reconnaissance is one of the most critical steps to the success of a penetration testing engagement. Once subdomains have been discovered, the next step would be to find directories.

The following code will build a simple directory enumeration tool.

```
import requests
import sys

sub_list = open("wordlist.txt").read()
directories = sub_list.splitlines()

for dir in directories:
    dir_enum = f"http://{sys.argv[1]}/{dir}.html"
    r = requests.get(dir_enum)
    if r.status_code==404:
        pass
    else:
        print("Valid directory:" ,dir_enum)
```

At first glance, you will certainly notice the similarities with the subdomain enumeration script. This script takes an approach based on a for loop and passes all "404" responses.

```
┌──(root💀TryHackMe)-[/home/alper/Desktop/Py4PT]
└─# python3 direnum.py 192.168.1.6
Valid directory:  http://192.168.1.6/index.html
```

Make sure you have downloaded the wordlist file from Task 2 before proceeding with the following questions. The wordlist was also added to the AttackBox and is located in the following path /usr/share/wordlists/PythonForPentesters/wordlist2.txt

Answer the questions below

How many directories can your script identify on the target system? (extensions are .html)

4 Correct Answer

What is the location of the login page?

private.html Correct Answer

Where did you find a cryptic hash?

apollo.html Correct Answer

Where are the usernames located?

surfer.html Correct Answer

What is the password assigned to Rabbit?

LOUSYRABBO Correct Answer

Task 4 ✔ Network Scanner

Task 5 ○ Port Scanner

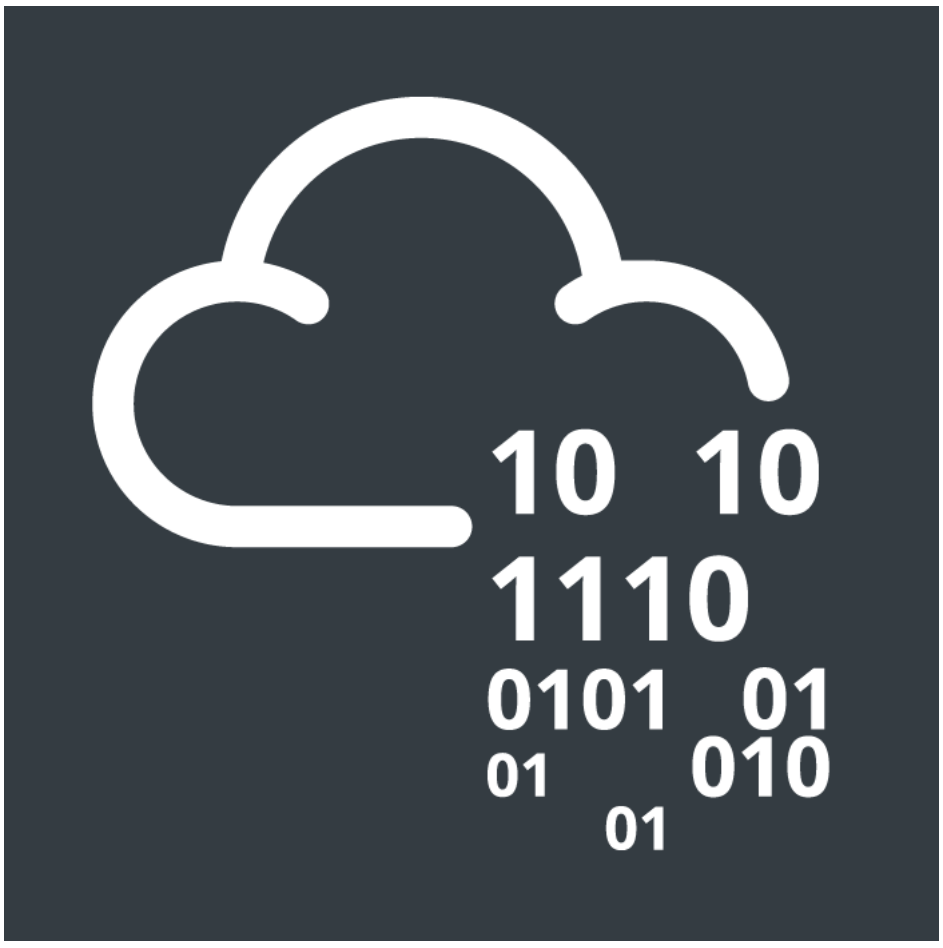
Task 6 ○ File Downloader

Task 7 ○ Hash Cracker

Task 8 ○ Keyloggers

Task 9 ○ SSH Brute Forcing

Task 10 ○ Extra challenges

Created by 

tryhackme

Only subscribers can deploy virtual machines in this room! Go to your profile page to subscribe (if you have not already). 20121 users are in here and this room is 594 days old.