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 43m 00s

? | Add 1 hour | Terminate

41%

Task 1 ✓ Introduction

Python can be the most powerful tool in your arsenal as it can be used to build almost any of the other penetration testing tools. The scope of this module does not allow us to go into too many details on Python. Still, we will cover several key areas that will be useful during engagements and help you better understand Python.

▶ Start Machine

Please complete the "Python Basics" room before proceeding, as this room will not go over the basic usage and programming features of the Python language.

We are not learning to become a developer; our objective is to become a penetration tester. This room will give you pointers on which you can build and improve. Examples are given on a "one of each" basis, and no code should be considered as "the only and correct way" to reach a solution. Our goal is then to build quick and effective tools that will help us in our daily tasks.

Throughout this room, you will see how to:

- Use Python to enumerate the target's subdomain
- Build a simple keylogger
- Scan the network to find target systems
- Scan any target to find the open ports
- Download files from the internet
- Crack hashes

Any code you will find in this section can be compiled using simple tools such as PyInstaller and sent to the target system.

Notice: A wordlist that will be useful to complete tasks related to the target system associated with this room can be found attached to the next task. The wordlist was also added to the AttackBox and is located in the following path /usr/share/wordlists/PythonForPentesters/wordlist2.txt

To access the machine you start on this task, you need to either:

- Use OpenVPN - Go to the access page and connect to our network via OpenVPN. This is important to do before you can access the machine.
- Use AttackBox - (Recommended) Start the AttackBox (blue button at the top of the page) and write your Python scripts through the browser.

Answer the questions below

What other tool can be used to convert Python scripts to Windows executables?

py2exe | Correct Answer | Hint

Start the machine on this task

No answer needed | Question Done

Task 2 ✓ Subdomain Enumeration

Task 3 ✓ Directory Enumeration