



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

41%

- Task 1 ☒ Introduction
- Task 2 ☒ Subdomain Enumeration
- Task 3 ☒ Directory Enumeration
- 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

Based on what we have covered in this room, here are a few suggestions about how you could expand these tools or start building your own using Python:

- Use DNS requests to enumerate potential subdomains
- Build the keylogger to send the capture keystrokes to a server you built using Python
- Grab the banner of services running on open ports
- Crawl the target website to download .js library files included
- Try to build a Windows executable for each and see if they work as stand-alone applications on a Windows target
- Implement threading in enumeration and brute-forcing scripts to make them run faster

Answer the questions below

Read the above.

No answer needed

Completed

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.