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 40m 03s	? Add 1 hour Terminate

41%

Task 1 Introduction

Task 2 Subdomain Enumeration

Task 3 Directory Enumeration

Task 4 Network Scanner

Task 5 Port Scanner

Task 6 File Downloader

Wget on Linux systems or Certutil on Windows are useful tools to download files.

Python can also be used for the same purpose.

The code:

```
import requests

url = 'https://assets.tryhackme.com/img/THMlogo.png'
r = requests.get(url, allow_redirects=True)
open('THMlogo.png', 'wb').write(r.content)
```

This short piece of code can easily be adapted to retrieve any other type of file, as seen below:

```
import requests

url = 'https://download.sysinternals.com/files/PSTools.zip'
r = requests.get(url, allow_redirects=True)
open('PSTools.zip', 'wb').write(r.content)
```

PSexec allow system administrators to run commands on remote Windows systems. We see that PSexec is also used in cyber attacks as it is usually not detected by antivirus software. You can learn more about PSexec here and read this blogpost about its use by attackers.

Answer the questions below

What is the function used to connect to the target website?

Answer format: ********.*****

Submit

What step of the Unified Cyber Kill Chain can PSexec be used in?

Answer format: ******* ********

Submit

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.