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 51s	? Add 1 hour Terminate

41%

Task 1 Introduction

Task 2 Subdomain Enumeration

Python gives us an easy way to automate tasks during a penetration test. Any tasks that you have to perform regularly are worth automating. While the automation process comes with a learning curve, the mid and long-term gains are worth it.

Download Task Files

Finding subdomains used by the target organization is an effective way to increase the attack surface and discover more vulnerabilities.

The script will use a list of potential subdomains and prepends them to the domain name provided via a command-line argument.

The script then tries to connect to the subdomains and assumes the ones that accept the connection exist.

```
import requests
import sys

sub_list = open("subdomains.txt").read()
subdoms = sub_list.splitlines()

for sub in subdoms:
    sub_domains = f"http://{sub}.{sys.argv[1]}"

    try:
        requests.get(sub_domains)

    except requests.ConnectionError:
        pass

    else:
        print("Valid domain: ",sub_domains)
```

As you can see, the script will search for a file named "subdomains.txt". The simplest way is to use a wordlist located in the same directory as the Python script, but any wordlist can be used. The wordlist should have possible subdomains listed one per line as shown below:

```
└─# cat subdomains.txt
test
mail
ftp
www
skype
delta1
demo
digital
discover
elasticsearch
enterprise
erp
energy
os
proxy
payment
apps
myapps
marketing
sales
hr
finance
sip
error
20
```

You don't need to download the wordlist attached to this task if you're using the AttackBox as it can be found under: /usr/share/wordlists/PythonForPentesters/wordlist2.txt

Answer the questions below

What other protocol could be used for subdomain enumeration?

DNS — Correct Answer — Hint

What function does Python use to get the input from the command line?

sys.argv — Correct Answer — Hint

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

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.