Python for CTF

Introduction to Python librairies for CTFs

DaVinciCode

30/09/2021

whoami

- Clovis
- A4 IOS
- President of DaVinciCode

Python for CTFs

- High Interpreted language level language created in 1991
- Most used programming language today
- Version 3

The python command line tool

The python command line tool

```
joytide@debian:~$ python3
Python 3.7.3 (default, Jan 22 2021, 20:04:44)
[GCC 8.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 2+2
4
```

The python command

The python command

```
$ python3 -V
Python 3.7.3
```

```
# python3 -c command
$ python3 -c "print(2+2)"
4
```

```
# python3 -m module
$ python3 -m venv
```

Python Package manager: pip

Python Package manager

```
$ pip3 install lib
$ pip3 list
$ pip3 -r requirements.txt
```

Virtual environments

Virtual environments

```
$ pip3 list
$ python3 -m venv my_venv
$ pip3 list
```

Overview of python's capacities

Overview of python's capacities

Python cheatsheet

- Lists, functions, exceptions, dictionaries, args, classes, etc.
- JSON, regex, scapy, requests...

Python for CTF

Cryptography, network, pwn, misc.

Misc

Regex

```
import re
re.findall(r'(?::\/\/)(.*)(?:\.)','https://dvc.tf')
# ["dvc"]
```

JSON

```
import json
dictionary ={"name": "Python_For_CTF", "type": "Masterclass", "month": 9,"awe
with open("masterclass.json", "w") as outfile:
  json.dump(dictionary, outfile, indent = 4)
```

Requests

Installing request

```
$ pip3 install requests
```

Requests

Basic request to an html page

```python
import requests
resp = requests.get("https://dvc.tf/")
print(resp.status_code,"\n", resp.text)
```

Scapy

Packet manipulation library: capture, forge, decode, scan...

Installing Scapy

```
pip3 install --pre scapy
```

Scapy

Usage

```python
from scapy.all import *
import base64

capture = rdpcap('frames.pcapng') # pcap file

output = open('output.bin','wb') # save dumped data to output.bin

for packet in capture:
  if IP in packet and packet[IP].src == '172.16.139.128' and TCP in packet:
     output.write(packet[TCP].payload)
```

Pwntools

PWNTOOLS

Installing pwntools

```
pip3 install pwntools
```

Pwntools

Without pwntools

```
nc pwn-2021.duc.tf 31905
```

With pwntools

```
from pwn import *
r = remote('pwn-2021.duc.tf', 31905)
```

Even SSH!

```
s=ssh(host='domain.com' ,user='joytide' ,password='123',port=22)
```

Pwntools

Example

```
from pwn import *
r = remote('pwn-2021.duc.tf', 31905)
print(r.recvline().decode('utf-8'))

r.sendline()
print(r.recvline().decode('utf-8'))
print(r.recvline().decode('utf-8'))
r.sendline("2")
r.interactive()
```

Going further

https://docs.pwntools.com/en/stable/

The Checksec command

```
pwn checksec
```

Utils

```
xor(b'abc', b'aaa')
```

Going further

https://docs.pwntools.com/en/stable/

Assembly and binary manipulation

```
disasm(b'\xb8\x0b\x00\x00\x00')
# '   0:   b8 0b 00 00 00          mov    eax, 0xb'
```

```
e = ELF('/bin/cat')
```

PWN: Rop, format strings, shellcodes...