

Challenge - Meli - 18/04/2024

Dev challenge_port - Documentos Google

Instalando Python / Pip / Scapy

Acesse o terminal e digite os comandos

- 1 - python3 get-pip.py
- 2 - curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py
- 3 - python3 get-pip.py
- 4 - pip install scapy

```

2.1/2.1 MB 10.1 MB/s eta 0:00:00
Downloading setuptools-69.5.1-py3-none-any.whl (894 kB)
894.6/894.6 kB 8.5 MB/s eta 0:00:00
Downloading wheel-0.43.0-py3-none-any.whl (65 kB)
65.8/65.8 kB 4.4 MB/s eta 0:00:00
Installing collected packages: wheel, setuptools, pip
  Attempting uninstall: pip
    Found existing installation: pip 24.0
    Uninstalling pip-24.0:
      Successfully uninstalled pip-24.0
Successfully installed pip-24.0 setuptools-69.5.1 wheel-0.43.0
helisonlouredo@MacBook-Pro-de-Helison ~ % pip --version
pip 24.0 from /Library/Frameworks/Python.framework/Versions/3.12/lib/python3.12/site-packages/pip (p
ython 3.12)
helisonlouredo@MacBook-Pro-de-Helison ~ % pip install scapy
Collecting scapy
  Downloading scapy-2.5.0.tar.gz (1.3 MB)
    1.3/1.3 MB 5.8 MB/s eta 0:00:00
    Preparing metadata (setup.py) ... done
Building wheels for collected packages: scapy
  Building wheel for scapy (setup.py) ... done
    Created wheel for scapy: filename=scapy-2.5.0-py2.py3-none-any.whl size=1444327 sha256=cb67d390929
d1d5794ab5f4c679d80866d553f952e1c56e9935d19fb14ef6e0f
    Stored in directory: /Users/helisonlouredo/Library/Caches/pip/wheels/8a/5e/7c/6f92df559dadf49d0e31
cecd5b104fc8c38a7c67fde16b029
Successfully built scapy
Installing collected packages: scapy
Successfully installed scapy-2.5.0
```

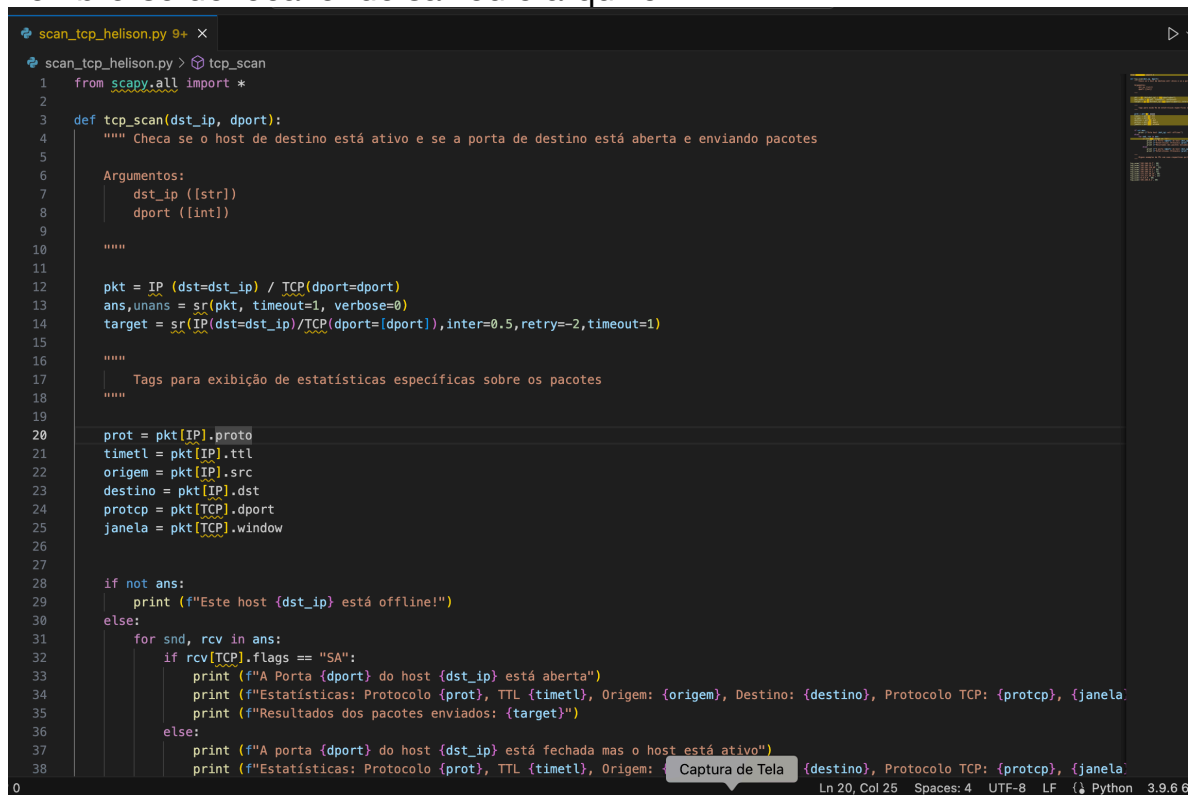
Para confirmar as instalações de cada aplicação basta digitar os comandos abaixo:

- python3 --version
- pip --version
- pip3 list | grep scapy

Executando o script via Visual Studio Code

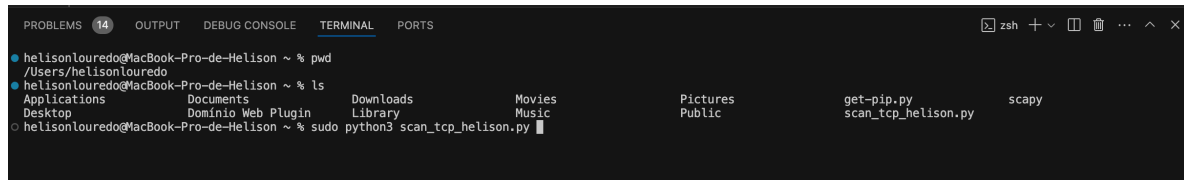
- 1 - Abra o VS Code e o arquivo scan_tcp_helison.py

Lembre-se do local onde salvou o arquivo



```
scan_tcp_helison.py 9+ x
scan_tcp_helison.py > tcp_scan
1 from scapy.all import *
2
3 def tcp_scan(dst_ip, dport):
4     """ Checa se o host de destino está ativo e se a porta de destino está aberta e enviando pacotes
5
6     Argumentos:
7         dst_ip ([str])
8         dport ([int])
9
10    """
11
12    pkt = IP(dst=dst_ip) / TCP(dport=dport)
13    ans,unans = sr(pkt, timeout=1, verbose=0)
14    target = sr(IP(dst=dst_ip)/TCP(dport=dport), inter=0.5, retry=-2, timeout=1)
15
16    """
17    Tags para exibição de estatísticas específicas sobre os pacotes
18    """
19
20    prot = pkt[IP].proto
21    timetl = pkt[IP].ttl
22    origem = pkt[IP].src
23    destino = pkt[IP].dst
24    prottcp = pkt[TCP].dport
25    janela = pkt[TCP].window
26
27
28    if not ans:
29        print(f"Este host {dst_ip} está offline!")
30    else:
31        for snd, rcv in ans:
32            if rcv[TCP].flags == "SA":
33                print(f"A Porta {dport} do host {dst_ip} está aberta")
34                print(f"Estatísticas: Protocolo {prot}, TTL {timetl}, Origem: {origem}, Destino: {destino}, Protocolo TCP: {protcp}, {janela}")
35                print(f"Resultados dos pacotes enviados: {target}")
36            else:
37                print(f"A Porta {dport} do host {dst_ip} está fechada mas o host está ativo")
38                print(f"Estatísticas: Protocolo {prot}, TTL {timetl}, Origem: {origem}, Destino: {destino}, Protocolo TCP: {protcp}, {janela}")
39
40    """
41    Tags para exibição de estatísticas específicas sobre os pacotes
42    """
43
44    return ans,unans, target
45
46 if __name__ == '__main__':
47     dst_ip = input("Digite o IP do host a ser verificado: ")
48     dport = input("Digite a porta a ser verificada: ")
49     ans,unans, target = tcp_scan(dst_ip, dport)
50     print(f"Resultado da verificação: {ans,unans, target}")
```

2 - Abra um novo terminal no menu > Terminal > Novo Terminal



```
helisonlouredo@MacBook-Pro-de-Helison ~ % pwd
/Users/helisonlouredo
helisonlouredo@MacBook-Pro-de-Helison ~ % ls
Applications  Desktop  Downloads  Library  Movies  Music  Pictures  Public  get-pip.py  scan_tcp_helison.py  scapy
helisonlouredo@MacBook-Pro-de-Helison ~ % sudo python3 scan_tcp_helison.py
```

3 - Execute os comandos abaixo:

- # pwd (para verificar o seu local de diretório atual, caso esteja no local errado, usar o próximo comando)
- # cd /Users/helisonlouredo (Referente ao caminho onde está salvo o script)
- # ls (visualizar e listar os arquivos Obs: somente para confirmar que o script está salvo nesse path)

4 - Execute o script com o comando abaixo e digite sua senha:

- # sudo python3 scan_tcp_helison.py

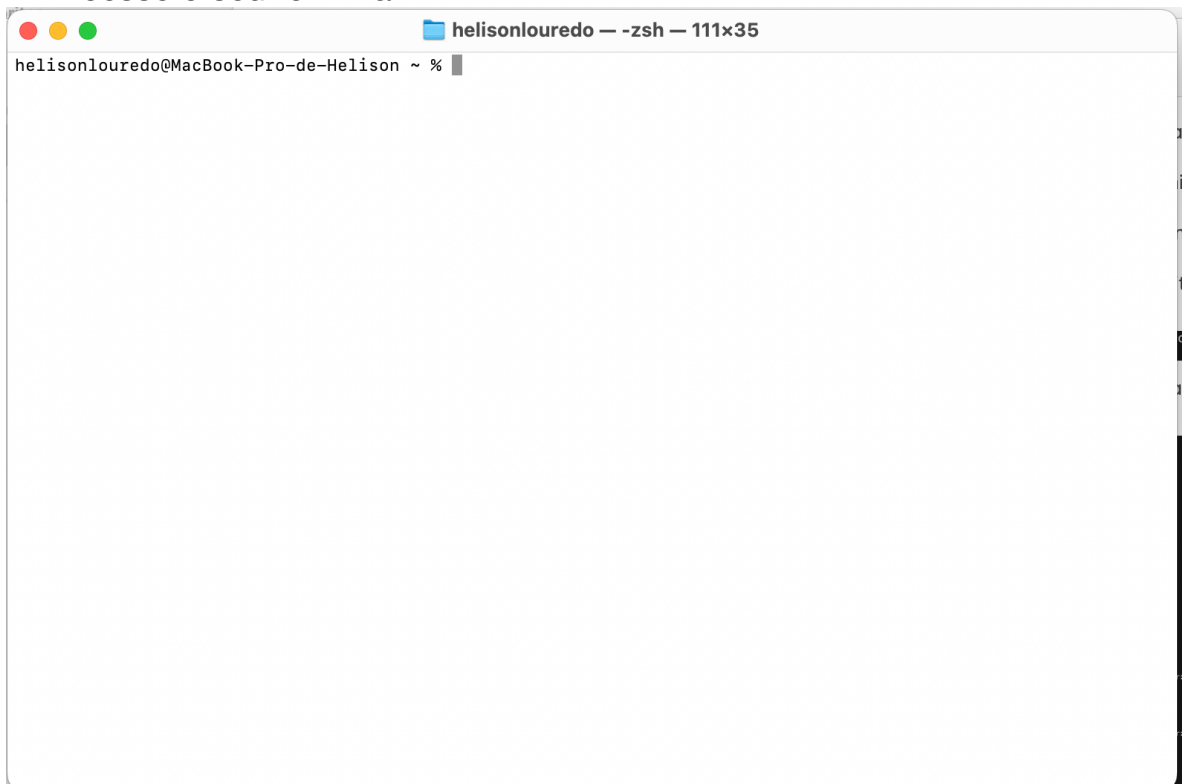
```
helisonlouredo@MacBook-Pro-de-Helison ~ % sudo python3 scan_tcp_helison.py
Password:
```

5 - A partir daí o script será executado e o resultado será exibido no terminal do VsCode

```
PROBLEMS 14 OUTPUT DEBUG CONSOLE TERMINAL PORTS
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
A porta 80 do host 192.168.15.7 está fechada mas o host está ativo
Estatísticas: Protocolo 6, TTL 64, Origem: 192.168.15.7, Destino: 192.168.15.7, Protocolo TCP: 80, 8192
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
A porta 22 do host 192.168.15.7 está fechada mas o host está ativo
Estatísticas: Protocolo 6, TTL 64, Origem: 192.168.15.7, Destino: 192.168.15.7, Protocolo TCP: 22, 8192
Begin emission:
Finished sending 1 packets.
.....Begin emission:
Finished sending 1 packets.
Begin emission:
Finished sending 1 packets.
.*
Received 14 packets, got 0 answers, remaining 1 packets
Este host 142.251.129.99 está offline!
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
A Porta 80 do host 192.168.15.1 está aberta
Estatísticas: Protocolo 6, TTL 64, Origem: 192.168.15.7, Destino: 192.168.15.1, Protocolo TCP: 80, 8192
Resultados dos pacotes enviados: (<Results: TCP:1 UDP:0 ICMP:0 Other:0>, <Unanswered: TCP:0 UDP:0 ICMP:0 Other:0>)
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
A Porta 22 do host 192.168.15.1 está aberta
Estatísticas: Protocolo 6, TTL 64, Origem: 192.168.15.7, Destino: 192.168.15.1, Protocolo TCP: 22, 8192
Resultados dos pacotes enviados: (<Results: TCP:1 UDP:0 ICMP:0 Other:0>, <Unanswered: TCP:0 UDP:0 ICMP:0 Other:0>)
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
A Porta 80 do host 172.217.30.14 está aberta
Estatísticas: Protocolo 6, TTL 64, Origem: 192.168.15.7, Destino: 172.217.30.14, Protocolo TCP: 80, 8192
Resultados dos pacotes enviados: (<Results: TCP:1 UDP:0 ICMP:0 Other:0>, <Unanswered: TCP:0 UDP:0 ICMP:0 Other:0>)
Begin emission:
Finished sending 1 packets.
Begin emission:
```

Executando o script via Terminal Linux/MacOS

1 - Acesse o seu terminal



2 - Repita os passos 3 e 4 acima, que serão os mesmos utilizados aqui.

```
helisonlouredo@MacBook-Pro-de-Helison ~ % pwd
/Users/helisonlouredo
helisonlouredo@MacBook-Pro-de-Helison ~ % ls
Applications      Downloads          Pictures           scapy
Desktop           Library           Public
Documents         Movies            get-pip.py
Domínio Web Plugin Music             scan_tcp_helison.py
helisonlouredo@MacBook-Pro-de-Helison ~ % sudo python3 scan_tcp_helison.py
Password:
```

3 - A partir daí o script será executado e o resultado será exibido no seu terminal

```
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
A Porta 80 do host 172.217.30.14 está aberta
Estatísticas: Protocolo 6, TTL 64, Origem: 192.168.15.7, Destino: 172.217.30.14, Protocolo TCP: 80, 8192
Resultados dos pacotes enviados: (<Results: TCP:1 UDP:0 ICMP:0 Other:0>, <Unanswered: TCP:0 UDP:0 ICMP:0 Other:
0>)
Begin emission:
Finished sending 1 packets.
.....Begin emission:
Finished sending 1 packets.
.....Begin emission:
Finished sending 1 packets.
.....
Received 35 packets, got 0 answers, remaining 1 packets
Este host 172.217.30.14 está offline!
Begin emission:
Finished sending 1 packets.
.....Begin emission:
Finished sending 1 packets.
.....Begin emission:
Finished sending 1 packets.
.....
Received 41 packets, got 0 answers, remaining 1 packets
Este host 0.0.0.0 está offline!
Begin emission:
Finished sending 1 packets.
.....Begin emission:
Finished sending 1 packets.
.....Begin emission:
Finished sending 1 packets.
.....
Received 23 packets, got 0 answers, remaining 1 packets
Este host 192.168.0.1 está offline!
helisonlouredo@MacBook-Pro-de-Helison ~ %
```