

UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FCFM

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS



Universidad Autónoma de Nuevo León
Facultad de Ciencias Físico Matemáticas

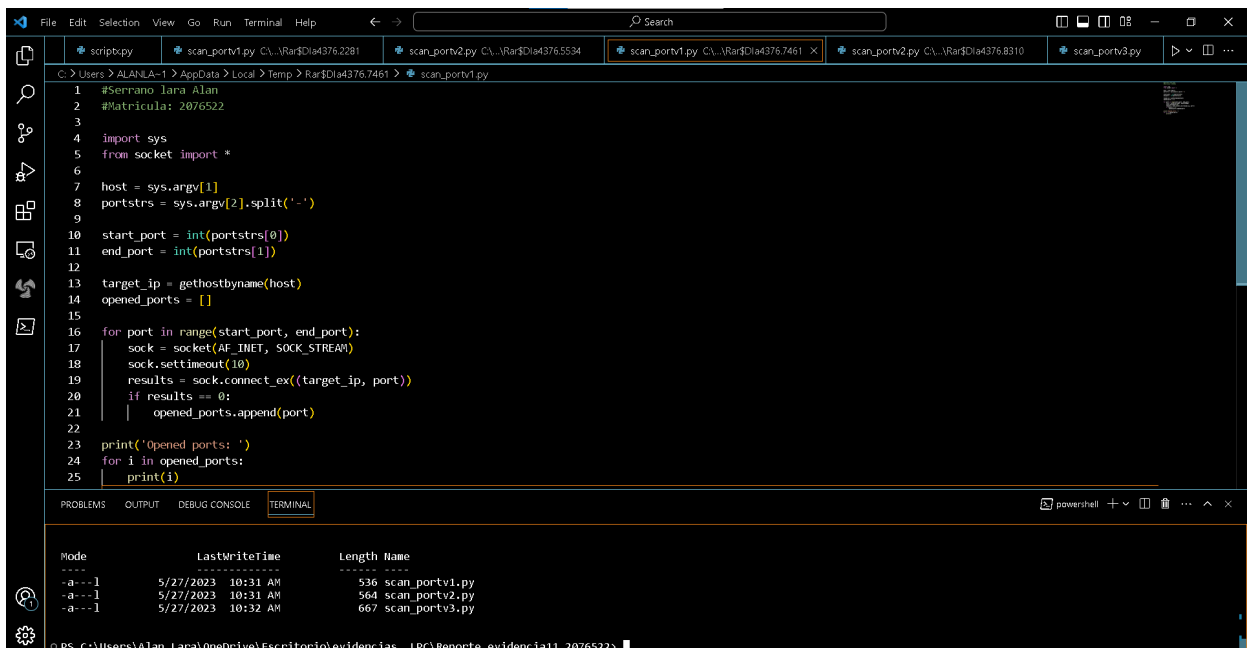
Licenciatura en Seguridad en Tecnologías de Información

Escáner de puertos | práctica 11
Catedrático Lic. Gerardo Bernal Carranza

Serrano Lara Alan David

2076522

Evidencias



```
1 #Serrano Lara Alan
2 #Matricula: 2076522
3
4 import sys
5 from socket import *
6
7 host = sys.argv[1]
8 portstrs = sys.argv[2].split('-')
9
10 start_port = int(portstrs[0])
11 end_port = int(portstrs[1])
12
13 target_ip = gethostbyname(host)
14 opened_ports = []
15
16 for port in range(start_port, end_port):
17     sock = socket(AF_INET, SOCK_STREAM)
18     sock.settimeout(10)
19     results = sock.connect_ex((target_ip, port))
20     if results == 0:
21         opened_ports.append(port)
22
23 print('Opened ports: ')
24 for i in opened_ports:
25     print(i)
```

Mode	LastWriteTime	Length	Name
-a---1	5/27/2023 10:31 AM	536	scan_portv1.py
-a---1	5/27/2023 10:31 AM	564	scan_portv2.py
-a---1	5/27/2023 10:32 AM	667	scan_portv3.py

```
Opened ports:
135
139
```

p11

```
192.168.1.251 80 Failed
192.168.1.252 21 Failed
192.168.1.252 22 Failed
192.168.1.252 25 Failed
192.168.1.252 80 Failed
192.168.1.253 21 Failed
192.168.1.253 22 Failed
192.168.1.253 25 Failed
192.168.1.253 80 Failed
192.168.1.254 21 Failed
192.168.1.254 22 Failed
192.168.1.254 25 Failed
192.168.1.254 80 OK
```

```
PS C:\Users\Alan Lara\OneDrive\Escritorio\evidencias - LPC\Reporte_evidencia11_2076522>
PS C:\Users\Alan Lara\OneDrive\Escritorio\evidencias - LPC\Reporte_evidencia11_2076522> .\scan_portv1.py 192.168.1.70 10-80
```

```
Opened Port: 53
```

```
IDLE Shell 3.10.11
File Edit Shell Debug Options Window Help
>>> import nmap
>>> scanner = nmap.PortScanner()
>>> scanner.scan('192.168.1.70' , '1-1024', '-v -sV')
{'nmap': {'command_line': 'nmap -oX - -p 1-1024 -v -sV 192.168.1.70', 'scaninfo':
: {'error': ['NSOCK ERROR [0.4850s] ssl_init_helper(): OpenSSL legacy provider f
ailed to load.\r\n\r\n'], 'tcp': {'method': 'syn', 'services': '1-1024'}}}, 'scan
stats': {'timestr': 'Thu Apr 27 17:58:10 2023', 'elapsed': '13.63', 'uphosts': '
1', 'downhosts': '0', 'totalhosts': '1'}}, 'scan': {'192.168.1.70': {'hostnames'
: [{'name': 'LAPTOP-GSELRQSS.domain.name', 'type': 'PTR'}], 'addresses': {'ipv4'
: '192.168.1.70'}, 'vendor': {}, 'status': {'state': 'up', 'reason': 'localhost-
response'}, 'tcp': {135: {'state': 'open', 'reason': 'syn-ack', 'name': 'msrpc',
'product': 'Microsoft Windows RPC', 'version': '', 'extrainfo': '', 'conf': '10
', 'cpe': 'cpe:/o:microsoft:windows'}, 137: {'state': 'filtered', 'reason': 'no-
response', 'name': 'netbios-ns', 'product': '', 'version': '', 'extrainfo': '',
'conf': '3', 'cpe': ''}, 139: {'state': 'open', 'reason': 'syn-ack', 'name': 'ne
tbios-ssn', 'product': 'Microsoft Windows netbios-ssn', 'version': '', 'extrainf
o': '', 'conf': '10', 'cpe': 'cpe:/o:microsoft:windows'}, 445: {'state': 'open',
'reason': 'syn-ack', 'name': 'microsoft-ds', 'product': '', 'version': '', 'ext
rainfo': '', 'conf': '3', 'cpe': ''}, 902: {'state': 'open', 'reason': 'syn-ack'
, 'name': 'vmware-auth', 'product': 'VMware Authentication Daemon', 'version': '
1.10', 'extrainfo': 'Uses VNC, SOAP', 'conf': '10', 'cpe': ''}, 912: {'state': '
open', 'reason': 'syn-ack', 'name': 'vmware-auth', 'product': 'VMware Authentica
tion Daemon', 'version': '1.0', 'extrainfo': 'Uses VNC, SOAP', 'conf': '10', 'cp
e': ''}}}}
>>> scanner.command_line()
'nmap -oX - -p 1-1024 -v -sV 192.168.1.70'
>>> scanner.all_hosts()
['192.168.1.70']
>>> scanner['192.168.1.70'].state()
'up'
>>> scanner['192.168.1.70'].all_protocols()
['tcp']
>>> scanner['192.168.1.70']['tcp'].keys()
dict_keys([135, 137, 139, 445, 902, 912])
>>> scanner['192.168.1.70'].has_tcp(135)
True
>>> scanner['192.168.1.70'].has_tcp(445)
True
>>> scanner['192.168.1.70']['tcp'][445]
{'state': 'open', 'reason': 'syn-ack', 'name': 'microsoft-ds', 'product': '', 'v
ersion': '', 'extrainfo': '', 'conf': '3', 'cpe': ''}
>>> scanner['192.168.1.70']['tcp'][445][product]
```