Python

Seguridad

Rogelio Ferreira Escutia

Profesor / Investigador
Tecnológico Nacional de México
Campus Morelia

Análisis

Análisis de conexión

- **Comando “ping” de consola:**

```python
# Librería para llamar al Sistema Operativo
import os

# Definir servidor a revisar
hostname = "www.itmorelia.edu.mx"

# Llamada a la consola
respuesta = os.system("ping -c 1 " + hostname)

# Verificando la respuesta
if respuesta == 0:
  print (hostname + ": está en fucionamiento!")
else:
  print (hostname + ": No funciona!")
```

```
PING denebvirtual.itmorelia.edu.mx (200.33.171.77): 56 data bytes
64 bytes from 200.33.171.77: icmp_seq=0 ttl=60 time=21.399 ms

--- denebvirtual.itmorelia.edu.mx ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 21.399/21.399/21.399/0.000 ms
www.itmorelia.edu.mx: está en fucionamiento!
```

"Pinging servers in Python", https://stackoverflow.com/questions/2953462/pinging-servers-in-python, febrero 2020

Detectar computadoras activas

- **Comando “nmap” de consola:**

```
# Librería para llamar a la consola
import os

# Seleccionar segmento de red
red = "192.168.0.0/24"

# Rastrear red
os.system("nmap -sP " + red)
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-25 21:22 CST
Nmap scan report for 192.168.0.1
Host is up (0.0039s latency).
Nmap scan report for 192.168.0.4
Host is up (0.0074s latency).
Nmap scan report for 192.168.0.6
Host is up (0.0012s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 1.46 seconds
```

"NMAP: 5 ejemplos de cómo utilizar este potente escáner de red", https://esgeeks.com/nmap-5-ejemplos-de-uso/, febrero 2020

Detectar puertos abiertos

- **Comando “nmap” de consola:**

```
# Librería para llamar a la consola
import os

# Seleccionar una computadora
computadora = "192.168.0.6"

# Detectar puertos abiertos
os.system("nmap -sT " + computadora)
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-25 21:29 CST
Nmap scan report for 192.168.0.6
Host is up (0.0012s latency).
Not shown: 502 filtered ports, 497 closed ports
PORT      STATE SERVICE
49167/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.99 seconds
```

"NMAP: 5 ejemplos de cómo utilizar este potente escáner de red", https://esgeeks.com/nmap-5-ejemplos-de-uso/, febrero 2020

Detectar sistema operativo

- **Comando “nmap” de consola:**

```
# Librería para llamar a la consola
import os

# Seleccionar una computadora
computadora = "192.168.0.6"

# Detectar sistema operativo
os.system("nmap -O " + computadora)
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-25 21:40 CST
Nmap scan report for 192.168.0.6
Host is up (0.00014s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
49167/tcp open  unknown
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=2/25%OT=49167%CT=1%CU=32495%PV=Y%DS=0%DC=L%G=Y%TM=5E55
OS:E8DB%P=x86_64-apple-darwin17.7.0)SEQ(SP=106%GCD=1%ISR=108%TI=Z%CI=RD%II=
OS:RI%TS=A)OPS(O1=M3FD8NW6NNT11SLL%O2=M3FD8NW6NNT11SLL%O3=M3FD8NW6NNT11%O4=
OS:M3FD8NW6NNT11SLL%O5=M3FD8NW6NNT11SLL%O6=M3FD8NNT11SLL)WIN(W1=FFFF%W2=FFF
OS:F%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M3FD8NW6SLL
OS:%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=
OS:Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=40%W=0%S=Z%A=S+%F=AR%O=%
OS:RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=40%W=0
OS:%S=Z%A=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK
OS:=Z%RUCK=0%RUD=G)IE(R=Y%DFI=S%T=40%CD=S)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.87 seconds
```

"NMAP: 5 ejemplos de cómo utilizar este potente escáner de red", https://esgeeks.com/nmap-5-ejemplos-de-uso/, febrero 2020

Pentesting

Conexión ftp:

- **Usando usuario “anonymous”:**

```
from ftplib import FTP
host = "192.168.1.69"
usuario = "anonymous"
clave = ""

try:
    conexion = FTP(host)
    conexion.login(usuario, clave)
    print("\nConexión establecida!!!\n")
except IOError:
    print("\nFalló la conexión!\n")
```

```
MacBook-Pro-de-Rogelio-2:seguridad rogelioferreiraescutia$ python3 python_seguridad_ftp.py

Conexión establecida!!!

MacBook-Pro-de-Rogelio-2:seguridad rogelioferreiraescutia$
```

Rogelio Ferreira Escutia

Profesor / Investigador
Tecnológico Nacional de México
Campus Morelia

rogelio.fe@morelia.tecnm.mx

rogeplus@gmail.com

xumarhu.net

@rogeplus

https://www.youtube.com/channel/UC0on88n3LwTKxJb8T09sGjg

rogelioferreiraescutia