Pràctica: Escaneig de Ports Oberts entre Dues Màquines Ubuntu en Python

Objectiu de la pràctica:

L'objectiu és escanejar els ports oberts d'una màquina Ubuntu des d'una altra màquina Ubuntu en una xarxa interna a VirtualBox, utilitzant un script de Python.

Pas 1: Configuració de la xarxa a VirtualBox

1. Configuració de la xarxa en mode "Xarxa Interna":

- Obre VirtualBox i selecciona la màquina virtual Ubuntu que serà l'objectiu de l'escaneig.
- Fes clic a Configuració > Xarxa.
- A la pestanya "Adaptador 1", selecciona Xarxa Interna com a mode de xarxa.
- Repeteix aquest pas per a l'altra màquina, assegurant-te que ambdues estan connectades a la mateixa xarxa interna.

2. Configura la xarxa interna a cada màquina:

- Assigna adreces IP fixes a les màquines dins la mateixa subxarxa. Per exemple:
  - Màquina objectiu: 192.168.1.10
  - Màquina d'escaneig: 192.168.1.11

Amb **ip a** podem veure la informació de les interfícies i amb l'ordre:

sudo ip addr add 192.168.1.10/24 dev enp0s3

podem assignar una ip de forma ràpida (es perdrà la configuració si reiniciem la màquina)

Pas 2: Instal·lació de serveis a la màquina objectiu

1. Instal·lació de serveis que deixaran ports oberts a la màquina objectiu:

A la màquina objectiu (IP 192.168.1.10), instal·la els següents serveis per tenir ports oberts:

- SSH:

sudo apt install openssh-server

sudo systemctl start ssh

- Apache (HTTP/HTTPS):

sudo apt install apache2

sudo systemctl start apache2

- FTP:

sudo apt install vsftpd

sudo systemctl start vsftpd

2. Comprovar els serveis actius:

Executa la comanda següent per verificar que els serveis estan actius:

sudo ss -tuln

Hauries de veure els ports 22 (SSH), 80 (HTTP), 443 (HTTPS), i 21 (FTP) com a oberts.

Pas 3: Instal·lació de Nmap i la llibreria `python-nmap` a la màquina d'escaneig

1. Instal·lar Nmap:

sudo apt install nmap

2. Instal·lar la llibreria `python-nmap`:

pip install python-nmap

Pas 4: Creació de l'script Python per a l'escaneig de ports

1. Crea un fitxer Python a la màquina d'escaneig (IP 192.168.1.11), per exemple, `escaneig_ports.py`.

2. Escriu el següent codi dins del fitxer:

```
python
import nmap

# Inicialitzar l'escàner Nmap
nm = nmap.PortScanner()

# IP de la màquina objectiu
ip_objectiu = '192.168.1.10'

# Executar l'escaneig de ports (per exemple, des del port 1 fins al 1024)
print(f"Escanejant els ports oberts de la màquina amb IP: {ip_objectiu}")
nm.scan(ip_objectiu, '1-1024')

# Processar i mostrar els resultats
for protocol in nm[ip_objectiu].all_protocols():
    ports_oberts = nm[ip_objectiu][protocol].keys()
    print(f"Ports oberts ({protocol}):")
    for port in sorted(ports_oberts):
        estat = nm[ip_objectiu][protocol][port]['state']
        print(f" - Port {port}: {estat}")
```

Pas a pas de l'script:

1. Importar la llibreria `nmap`:

```
import nmap
```

Aquesta línia importa la llibreria `nmap` a l'script. `python-nmap` és un "wrapper" que permet controlar Nmap des de Python.

2. Inicialitzar l'escàner Nmap:

```
nm = nmap.PortScanner()
```

Aquí es crea una instància de la classe `PortScanner` que serà utilitzada per executar l'escaneig de ports.

3. Definir la IP de la màquina objectiu:

```
ip_objectiu = '192.168.1.10'
```

Es defineix la IP de la màquina que es vol escanejar. Substitueix `192.168.1.10` per l'adreça IP de la màquina real que estàs escanejant.

4. Executar l'escaneig de ports:

```
nm.scan(ip_objectiu, '1-1024')
```

Aquesta línia executa l'escaneig de ports utilitzant Nmap. La funció `scan()` accepta com a paràmetres:

- `ip_objectiu`: L'adreça IP de la màquina que s'està escanejant.

- `'1-1024'`: El rang de ports que es vol escanejar (del port 1 al 1024 en aquest cas). Pots canviar aquest rang segons les teves necessitats.

5. Mostrar un missatge inicial:

```
print(f"Escanejant els ports oberts de la màquina amb IP: {ip_objectiu}")
```

Aquest missatge informa que s'està escanejant la màquina amb la IP especificada.

6. Processar i mostrar els resultats de l'escaneig:

```
for protocol in nm[ip_objectiu].all_protocols():
```

Aquest bucle recorre tots els protocols trobats durant l'escaneig (com TCP o UDP) per a la màquina escanejada. Utilitza la funció `all_protocols()` per obtenir una llista dels protocols disponibles.

7. Obtenir els ports oberts per a cada protocol:

```
ports_oberts = nm[ip_objectiu][protocol].keys()
```

Aquesta línia obté tots els ports que estan oberts per al protocol actual (per exemple, TCP). Els resultats són retornats com una llista de claus (els números de port).

8. Mostrar els ports oberts:

```
print(f"Ports oberts ({protocol}):")
for port in sorted(ports_oberts):
    estat = nm[ip_objectiu][protocol][port]['state']
    print(f" - Port {port}: {estat}")
```

- `for port in sorted(ports_oberts)`: Es recorre la llista de ports oberts, ordenant-los de menor a major.

- `nm[ip_objectiu][protocol][port]['state']`: Aquesta part del codi obté l'estat del port (normalment serà `open` si el port està obert).

- Finalment, es mostra cada port obert i el seu estat a la consola.

Exemple de sortida esperada:

Escanejant els ports oberts de la màquina amb IP: 192.168.1.10

Ports oberts (tcp):

- Port 22: open

- Port 80: open

- Port 443: open

3. Executa l'script:

Des de la màquina d'escaneig, executa l'script:

python escaneig_ports.py

Pas 5: Resultats esperats

Després d'executar l'script, hauries de veure una sortida semblant a aquesta:

Escanejant els ports oberts de la màquina amb IP: 192.168.1.10

Ports oberts (tcp):

- Port 21: open

- Port 22: open

- Port 80: open

- Port 443: open

Això indica que els ports 21 (FTP), 22 (SSH), 80 (HTTP) i 443 (HTTPS) estan oberts a la màquina objectiu.