M4. TAREA 1 – SCAPY

CELSO GIMENO CORBELLA

Objetivo

El objetivo de esta tarea es generar en Python, usando la librería Scapy, un script para llevar a cabo un escáner ARP Ping o ARP Scan.

Desarrollo

Se ha creado el siguiente script:

```
┌──(root㉿9eefa5ec7e18)-[/home/M4T1]
└─# cat arp_ping.py
from scapy.all import *
ipdst = '172.17.0.0/30'
arp = ARP(pdst=ipdst)
ether = Ether(dst=ETHER_BROADCAST)
paquete = ether / arp
resultado = srp(paquete,timeout=1,verbose=False)
print("Equipos encontrados:")
for enviado, recivido in resultado[0]:
        print("Ip: {0}".format(recivido.psrc))
print("Ejecucion terminada")
```

Lo primero que se hace es determinar el rango de direcciones IP que se quiere analizar en formato CIDR. En caso de querer analizar individualmente, se puede introducir solamente la IP. Esta variable es la que tiene que cambiar el usuario manualmente.

Acto seguido se crea el paquete, indicando el rango de direcciones IP y la dirección broadcast, para que llegue a toda la red.

Una vez enviado el paquete, se muestra por pantalla aquellas direcciones IP de los equipos encontrados.

En el siguiente ejemplo, se crea un entorno en Docker con dos contenedores. El contenedor atacante tendrá la IP 172.17.0.3 y el contenedor objetivo la IP 172.17.0.2. Hay que tener en cuenta que existe un tercer contenedor con la IP 172.17.0.1, se trata del puente de red de Docker. Con el script anterior, se deben de encontrar el contenedor objetivo y el puente de red:

```
┌──(root㉿9eefa5ec7e18)-[/home/M4T1]
└─# python3 arp_ping.py
Equipos encontrados:
Ip: 172.17.0.1
Ip: 172.17.0.2
Ejecucion terminada
```