

# INFORME DE RESULTADOS

RETO PYTHON - TEAM CHALLENGE - SPRINT 1 - CIBERSEGURIDAD

Elaborado por:	Fecha de creación:
Víctor Manuel Martínez Barberá	03/06/2024

En relación al reto practico indicado, se han practicado las instrucciones recibidas en los archivos en pdf habiendo obtenido un resultado satisfactorio, como se puede observar en las siguientes capturas:

**1** •— Una vez configurada la imagen .ova del reto, se abrió en el Virtual Vox esta maquina, aperturando además mi Kali Linux, ejecutando el comando ip a, con el cual se muestra información detallada sobre las interfaces de red de tu sistema Linux, tanto las físicas como las virtuales, usándose para verifacas si tus interfaces están bien configuradas, con las IPs esperadas. También se puede usar esta información para hacer nuestro scripts.

```
y ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1c:12:50 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 474sec preferred_lft 474sec
    inet6 fe80::a00:27ff:fe1c:1250/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Extraemos que nuestra interface de red es eth0.

**2 •-** Ejecutamos el comando `arp-scan -I eth0 -l`, con el cual realizamos un mapeo de la red buscando los dispositivos que están conectados a la red `eth0`, sus IPs , para ellos envía solicitudes ARP (protocolo de resolución de direcciones) a todas las direcciones de mi red, esperando respuesta de las mismas. Este comando es muy útil en ciberseguridad para mapear la red en busca de intrusiones no autorizadas.

```
> sudo arp-scan -I eth0 -l
[sudo] password for vicevil:
Interface: eth0, type: EN10MB, MAC: 08:00:27:1c:12:50, IPv4: 10.0.2.4
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1      52:54:00:12:35:00      (Unknown: locally administered)
10.0.2.2      52:54:00:12:35:00      (Unknown: locally administered)
10.0.2.3      08:00:27:45:d5:c5      (Unknown)
10.0.2.15     08:00:27:c3:3a:68      (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.039 seconds (125.55 hosts/sec). 4 responded
```

En el resultado observamos 4 direcciones IPs (10.0.2.1, 10.0.2.2 y 10.0.2.3), siendo éstas utilizadas por VirtualBox para facilitar la comunicación entre el sistema anfitrión y el sistema invitado, por lo que la IP donde realizar la conexión segura.

**3 •-** Se procede a establecer la conexión segura, tunelizada y cifrada simétricamente mediante clave pública entre el sistema anfitrión y la maquina `Reto_python`, siendo utilizado en ciberseguridad, para automatizar de tareas periódicas repetitivas en servidores remotos mediante scripts.

```
> ssh user1@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:HkyjvIvLqRiz0qjlfLrfHaHUmKRRKMcRhYtkxwu6N9Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
user1@10.0.2.15's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Se pueden aplicar 275 actualizaciones de forma inmediata.
67 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

*** System restart required ***
Last login: Wed May  8 23:24:38 2024 from 10.0.2.4
user1@ubuntu-VirtualBox:~$
```

Aquí ya estaríamos conectados, por lo que podríamos ejecutar comandos, transferir archivos, instalar programas y realizar otras tareas de forma segura ( los administradores de sistemas se conectan así, y además consume menos recursos que el TeamViewer).

**4** •— finalmente hacemos la comprobación si realmente están conectados, creando un archivo `estoy_dentro.txt` desde la maquina anfitrión, siendo las misma positiva:

```
user1@ubuntu-VirtualBox:~$ ls
Descargas Documentos Escritorio Imágenes Música Plantillas Público snap Videos
user1@ubuntu-VirtualBox:~$ touch estoy_dentro.txt
user1@ubuntu-VirtualBox:~$ ls
Descargas Documentos Escritorio estoy_dentro.txt Imágenes Música Plantillas Público snap Videos
user1@ubuntu-VirtualBox:~$
```

