

Trabajo práctico 4: Capa de Transporte - Sockets TCP y UDP - Puertos

En este trabajo práctico buscamos poder comunicar computadoras mediante sockets TCP y UDP. Además de conocer y comprender el uso y utilidad de herramientas de escaneo de puertos.

Actividad 1:

Esta actividad nos pide hacer un chat basado en UDP, será el archivo “actividad1-UDP.py”.

¿Cómo ejecutarlo?

Asegurarse de tener el archivo descargado y estar en su carpeta de origen, además se debe contar con python instalado. Finalmente ejecutar el siguiente comando

```
python3 actividad1-UDP.py
```

Si todo funcionó correctamente, se pedirá el nombre de usuario y la ip de Broadcast, si no conoce la ip de Broadcast, en Linux se puede obtener ejecutando el siguiente comando

```
ip a
```

y buscar las siguientes líneas:

```
2: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether b4:b5:b6:c8:d7:43 brd ff:ff:ff:ff:ff:ff
    inet 10.65.4.232/24 brd 10.65.4.255 scope global dynamic noprefixroute wlp2s0
        valid_lft 86256sec preferred_lft 86256sec
    inet6 fe80::5d74:f33d:abac:9099/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Imagen 1: Algunas líneas resultado de 'ip a'

En este caso la ip de broadcast es '10.65.4.255', esta se encuentra en la tercera línea.

Luego de esto ya se realizó la conexión, por lo que podrá comunicarse con cualquier cliente conectado.

¿Cómo funciona?

Su funcionamiento se basa en la creación de dos hilos, uno el cual recibirá mensajes, y otro que los enviará. Primeramente se crea un socket y se asocia a la IP '0.0.0.0' con el fin de que funcione tanto para conectarse con programas en la misma máquina o externos a esta. Luego simplemente empiezan a funcionar ambos hilos, el de enviar avisara a todos los conectados que se unió un nuevo cliente, y estará esperando entradas de texto permanentemente que serán enviadas al resto, y el de recibir estará comprobando el buffer todo el tiempo para poder extraer los mensajes que lleguen y mostrarlos por pantalla. En el caso de que se envíe un mensaje 'exit' el programa enviará este mensaje para avisar del

abandono del cliente, y también el hilo de recibir dejará de funcionar, dando así finalizado el programa

Actividad 2:

Esta actividad nos pide hacer un chat basado en TCP, estará conformado por los archivos 'actividad2-ClienteTCP.py' y 'actividad2-ServerTCP.py'.

¿Cómo ejecutarlo?

Asegurarse de tener los archivos descargados y estar en su carpeta de origen, además se debe contar con python instalado. Finalmente ejecutar el siguiente comando para empezar a correr el servidor:

```
python3 actividad2-ServerTCP.py
```

Seguir las instrucciones del programa para poder Luego desde otra consola o otra maquina en la red local ejecutar el siguiente comando:

```
python3 actividad2-ClienteTCP.py
```

Deberá ingresar su usuario y la ip a la cual quiere conectarse (debe asegurarse que el server está escuchando conexiones), esta debe ser la de la máquina en la que se encuentra el servidor, esta se ve también en la Imagen 1, justo a la izquierda de la ip de Broadcast.

Finalmente ya se encuentra conectado y se podrá comunicar el servidor con el cliente y viceversa.

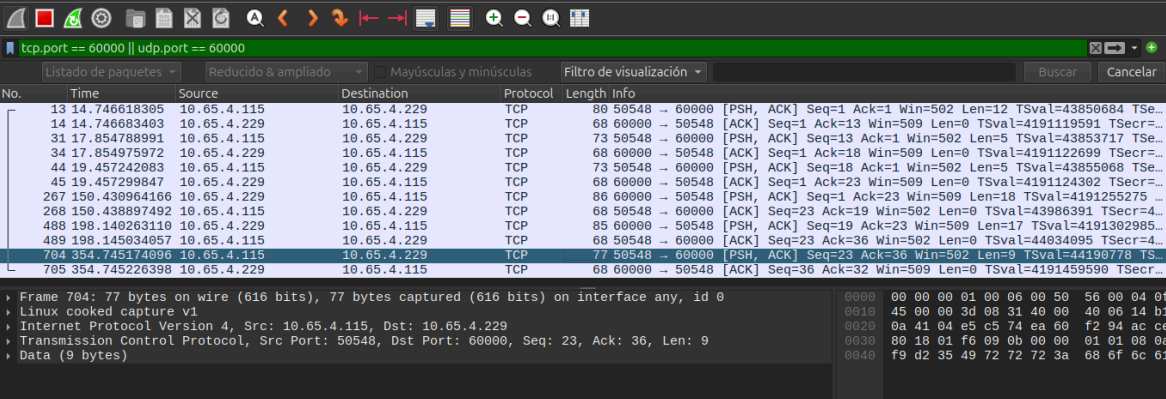
¿Cómo funciona?

La idea es que cada proceso (server y cliente) tendrá dos hilos, uno para recibir mensajes y otro para enviarlos, en la parte server se dará la opción de buscar una conexión o salir, si se busca una conexión quedará permanentemente buscando hasta que se establezca una. Una vez que se establezca la conexión se iniciaran los hilos de recepción y emisión de mensajes. Una vez que se establezca la conexión, no se podrá apagar el proceso servidor. Cuando el cliente abandone el chat, se pedirá presionar enter para continuar, ya que estará frenado esperando un mensaje. Y se vuelve al principio. Respecto al cliente, se pedirá un usuario y la ip del servidor, en el caso que exista un error al conectar se volverá a pedir, en caso de que la conexión sea exitosa empezaran ambos hilos mencionados anteriormente hasta que se envíe un exit.

Actividad 3:

Renzo Dávila,
Ramiro Martinez

Redes de las Computadoras



No.	Time	Source	Destination	Protocol	Length	Info
13	14.746618395	10.65.4.115	10.65.4.229	TCP	80	59548 → 60000 [PSH, ACK] Seq=1 Ack=1 Win=502 Len=12 TSval=43850684 TSecr=...
14	14.746683463	10.65.4.229	10.65.4.115	TCP	68	60000 → 59548 [ACK] Seq=1 Ack=13 Win=509 Len=0 TSval=419119591 TSecr=...
31	17.854788991	10.65.4.115	10.65.4.229	TCP	73	59548 → 60000 [PSH, ACK] Seq=13 Ack=1 Win=502 Len=5 TSval=43853717 TSecr=...
34	17.854975972	10.65.4.229	10.65.4.115	TCP	68	60000 → 59548 [ACK] Seq=1 Ack=18 Win=509 Len=0 TSval=4191122699 TSecr=...
44	19.457242083	10.65.4.115	10.65.4.229	TCP	73	59548 → 60000 [PSH, ACK] Seq=18 Ack=1 Win=502 Len=5 TSval=43855068 TSecr=...
45	19.457299847	10.65.4.229	10.65.4.115	TCP	68	60000 → 59548 [ACK] Seq=1 Ack=23 Win=509 Len=0 TSval=4191124302 TSecr=...
267	150.439964166	10.65.4.229	10.65.4.115	TCP	86	60000 → 59548 [PSH, ACK] Seq=1 Ack=23 Win=509 Len=18 TSval=4191255275 TSecr=...
268	150.438897492	10.65.4.115	10.65.4.229	TCP	68	59548 → 60000 [ACK] Seq=23 Ack=19 Win=502 Len=0 TSval=43986391 TSecr=4...
488	198.140263110	10.65.4.229	10.65.4.115	TCP	85	60000 → 59548 [PSH, ACK] Seq=19 Ack=23 Win=509 Len=17 TSval=4191302985 TSecr=...
489	198.145034057	10.65.4.115	10.65.4.229	TCP	68	59548 → 60000 [ACK] Seq=23 Ack=36 Win=502 Len=0 TSval=44034095 TSecr=4...
704	354.745174096	10.65.4.115	10.65.4.229	TCP	77	59548 → 60000 [PSH, ACK] Seq=23 Ack=36 Win=502 Len=9 TSval=44190778 TSecr=...
705	354.745226398	10.65.4.229	10.65.4.115	TCP	68	60000 → 59548 [ACK] Seq=36 Ack=32 Win=509 Len=0 TSval=4191459590 TSecr=...

Frame 704: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface any, id 0

Linux cooked capture v1

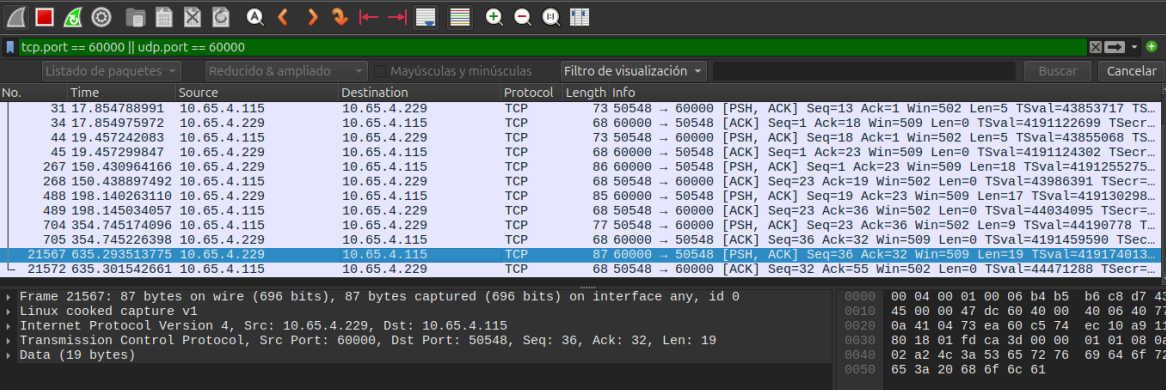
Internet Protocol Version 4, Src: 10.65.4.115, Dst: 10.65.4.229

Transmission Control Protocol, Src Port: 59548, Dst Port: 60000, Seq: 23, Ack: 36, Len: 9

Data (9 bytes)

0000 00 00 00 01 00 06 00 50 56 00 04 0f
0010 45 00 00 3d 08 31 40 00 40 06 14 b1
0020 0a 41 04 e5 c5 74 ea 60 f2 94 ac ce
0030 80 18 01 f6 09 0b 00 00 01 01 08 0a
0040 f9 d2 35 49 72 72 72 3a 68 6f 6c 61

Captura de paquete TCP recibido en el puerto 60000.



No.	Time	Source	Destination	Protocol	Length	Info
31	17.854788991	10.65.4.115	10.65.4.229	TCP	73	59548 → 60000 [PSH, ACK] Seq=13 Ack=1 Win=502 Len=5 TSval=43853717 TS...
34	17.854975972	10.65.4.229	10.65.4.115	TCP	68	60000 → 59548 [ACK] Seq=1 Ack=18 Win=509 Len=0 TSval=4191122699 TSecr=...
44	19.457242083	10.65.4.115	10.65.4.229	TCP	73	59548 → 60000 [PSH, ACK] Seq=18 Ack=1 Win=502 Len=5 TSval=43855068 TS...
45	19.457299847	10.65.4.229	10.65.4.115	TCP	68	60000 → 59548 [ACK] Seq=1 Ack=23 Win=509 Len=0 TSval=4191124302 TSecr=...
267	150.439964166	10.65.4.229	10.65.4.115	TCP	86	60000 → 59548 [PSH, ACK] Seq=1 Ack=23 Win=509 Len=18 TSval=4191255275 TSecr=...
268	150.438897492	10.65.4.115	10.65.4.229	TCP	68	59548 → 60000 [ACK] Seq=23 Ack=19 Win=502 Len=0 TSval=43986391 TSecr=...
488	198.140263110	10.65.4.229	10.65.4.115	TCP	85	60000 → 59548 [PSH, ACK] Seq=19 Ack=23 Win=509 Len=17 TSval=4191302985 TSecr=...
489	198.145034057	10.65.4.115	10.65.4.229	TCP	68	59548 → 60000 [ACK] Seq=23 Ack=36 Win=502 Len=0 TSval=44034095 TSecr=...
704	354.745174096	10.65.4.115	10.65.4.229	TCP	77	59548 → 60000 [PSH, ACK] Seq=23 Ack=36 Win=502 Len=9 TSval=44190778 TS...
705	354.745226398	10.65.4.229	10.65.4.115	TCP	68	60000 → 59548 [ACK] Seq=36 Ack=32 Win=509 Len=0 TSval=4191459590 TSecr=...
21567	635.301542661	10.65.4.115	10.65.4.229	TCP	87	60000 → 59548 [PSH, ACK] Seq=36 Ack=32 Win=502 Len=19 TSval=44174013 TSecr=...
21572	635.301542661	10.65.4.115	10.65.4.229	TCP	68	59548 → 60000 [ACK] Seq=32 Ack=55 Win=502 Len=0 TSval=44471288 TSecr=...

Frame 21567: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface any, id 0

Linux cooked capture v1

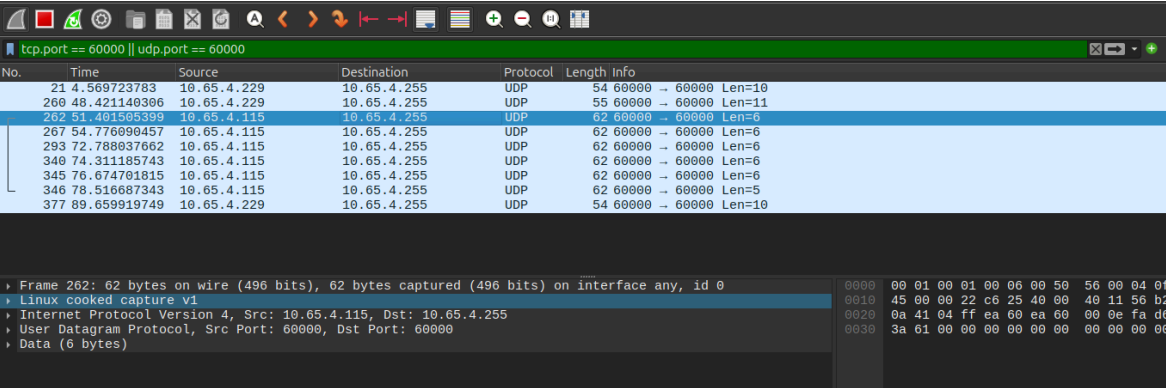
Internet Protocol Version 4, Src: 10.65.4.229, Dst: 10.65.4.115

Transmission Control Protocol, Src Port: 60000, Dst Port: 59548, Seq: 36, Ack: 32, Len: 19

Data (19 bytes)

0000 00 04 00 01 00 06 b4 b5 b6 c8 d7 43
0010 45 00 00 47 dc 60 40 00 40 06 40 77
0020 0a 41 04 73 ea 60 c5 74 ec 10 a9 11
0030 80 18 01 fd ca 3d 00 00 01 01 08 0a
0040 02 a2 4c 3a 53 65 72 76 69 64 6f 72
0050 65 3a 29 68 6f 6c 61

Captura de paquete TCP enviado al usuario conectado (10.65.4.115)



No.	Time	Source	Destination	Protocol	Length	Info
21	4.569723783	10.65.4.229	10.65.4.255	UDP	54	60000 → 60000 Len=10
260	48.421140306	10.65.4.229	10.65.4.255	UDP	55	60000 → 60000 Len=11
262	51.401505339	10.65.4.115	10.65.4.255	UDP	62	60000 → 60000 Len=6
267	54.776990457	10.65.4.115	10.65.4.255	UDP	62	60000 → 60000 Len=6
293	72.788937662	10.65.4.115	10.65.4.255	UDP	62	60000 → 60000 Len=6
340	74.311185743	10.65.4.115	10.65.4.255	UDP	62	60000 → 60000 Len=6
345	76.674701815	10.65.4.115	10.65.4.255	UDP	62	60000 → 60000 Len=6
346	78.516687343	10.65.4.115	10.65.4.255	UDP	62	60000 → 60000 Len=5
377	89.659919749	10.65.4.229	10.65.4.255	UDP	54	60000 → 60000 Len=10

Frame 262: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface any, id 0

Linux cooked capture v1

Internet Protocol Version 4, Src: 10.65.4.115, Dst: 10.65.4.255

User Datagram Protocol, Src Port: 60000, Dst Port: 60000

Data (6 bytes)

0000 00 01 00 01 00 06 00 50 56 00 04 0f
0010 45 00 00 22 c6 25 40 00 40 11 56 b2
0020 0a 41 04 ff ea 60 ea 60 00 0e fa d6
0030 3a 61 00 00 00 00 00 00 00 00 00 00

Captura de paquete UDP recibido en la máquina

No.	Time	Source	Destination	Protocol	Length	Info
21	4.569723783	10.65.4.229	10.65.4.255	UDP	54	60000 → 60000 Len=10
260	48.421140306	10.65.4.229	10.65.4.255	UDP	55	60000 → 60000 Len=11
262	51.401505399	10.65.4.115	10.65.4.255	UDP	62	60000 → 60000 Len=6
267	54.776090457	10.65.4.115	10.65.4.255	UDP	62	60000 → 60000 Len=6
293	72.788837662	10.65.4.115	10.65.4.255	UDP	62	60000 → 60000 Len=6
340	74.311185743	10.65.4.115	10.65.4.255	UDP	62	60000 → 60000 Len=6
345	76.674701815	10.65.4.115	10.65.4.255	UDP	62	60000 → 60000 Len=6
346	78.516687343	10.65.4.115	10.65.4.255	UDP	62	60000 → 60000 Len=5
377	89.659919749	10.65.4.229	10.65.4.255	UDP	54	60000 → 60000 Len=10
3163	198.422242825	10.65.4.229	10.65.4.255	UDP	54	60000 → 60000 Len=10
3164	198.422321440	10.65.4.229	10.65.4.255	UDP	54	60000 → 60000 Len=10

<pre> Frame 3163: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface any, id 0 Linux cooked capture v1 Internet Protocol Version 4, Src: 10.65.4.229, Dst: 10.65.4.255 User Datagram Protocol, Src Port: 60000, Dst Port: 60000 Data (10 bytes) </pre>	<pre> 0000 00 04 00 01 00 06 b4 b5 b6 c8 d7 43 0010 45 00 00 26 39 6a 40 00 40 11 e2 f7 0020 0a 41 04 ff ea 60 ea 00 00 12 ed 9b 0030 6f 3a 65 78 69 74 </pre>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------

Captura de paquete UDP enviado a la ip de Broadcast

Respondiendo a la pregunta, un intruso si podría capturar los datos que se envían en los paquetes, siempre y cuando no estén cifrados.

Actividad 4:

4.2:

```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-14 15:39 -03
Nmap scan report for 10.65.4.115
Host is up (0.0053s latency).

PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    open  ssh
23/tcp    closed telnet
24/tcp    closed priv-mail
25/tcp    closed smtp
135/tcp   closed msrpc
139/tcp   closed netbios-ssn
443/tcp   closed https
445/tcp   closed microsoft-ds
3389/tcp  closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds

```

El estado de distintos puertos de la máquina con ip '10.65.4.115'

Como se puede ver el puerto 22 se encuentra abierto, el cual es sobre SSH (secure Shell), el cual los riesgos decaen en una mala configuración, entre los cuales se encuentran ataques con miles de intento de usuario-contraseña, información del servicio SSH corriendo, entre otros.

4.3:

```
- Nikto v2.1.5
-----
+ Target IP: 23.10.210.245
+ Target Hostname: a23-10-210-245.deploy.static.akamai.com
+ Target Port: 80
+ Start Time: 2025-05-14 15:23:43 (GMT-3)
-----
+ Server: AkamaiGHost
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ llnes
+ /crossdomain.xml contains 0 line which should be manually viewed for improper domains or wildcards.
+ "/robots.txt" retrieved but it does not contain any 'disallow' entries (which is odd).
+ /kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
+ /lists/admin/: PHPLIST pre 2.6.4 contains a number of vulnerabilities including remote administrative access, harvesting user
info and more. Default login to admin interface is admin/phplist
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems as described by www.scan-associate
s.net. These could not be tested remotely.
+ /ssdefs/: Sitedeep pre 1.4.2 has 'major' security problems.
+ /sshome/: Sitedeep pre 1.4.2 has 'major' security problems.
+ /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be adm
in/admin
+ /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/p
ass could be admin/admin
+ /scripts/samples/details.idc: See RFP 9901; www.wiretrip.net
+ OSVDB-396: /vti bin/shhtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shhtml.exe/aux.htm -
a DoS was not attempted.
```

Parte del análisis de Nikto, de una ip la cual tiene abierto el puerto 80

La ip analizada es de la empresa Akamai Technologies, la cual se encuentra en Chicago, Estados Unidos

Se le envió la captura a gemini, y se le pidió explicar cada vulnerabilidad y cómo explotarla, este fue el resultado:

El escaneo de Nikto a la IP 23.10.210.245:80 revela:

Falta de encabezado X-Frame-Options: Riesgo de clickjacking.

Possible Explotación: Incrustar la página en un <iframe> malicioso para engañar al usuario.

No se encontraron directorios CGI comunes: Podría haber vulnerabilidades en directorios no estándar.

Possible Explotación: Forzar el escaneo con -C all y luego analizar los scripts encontrados en busca de vulnerabilidades (inyección de comandos, etc.).

/crossdomain.xml vacío: Podría indicar una configuración incorrecta para Flash.

Possible Explotación: Si se pudiera subir un crossdomain.xml malicioso, permitiría a Flash interactuar con el sitio desde dominios no autorizados.

/robots.txt sin directivas 'Disallow': Podría exponer áreas sensibles a rastreadores.

Possible Explotación: Utilizar la información para encontrar rutas no públicas que podrían contener información sensible o vulnerabilidades.

/kboard/ (KBoard Forum 0.3.0 <=): Vulnerabilidades conocidas en archivos PHP (forum_edit_post.php, forum_post.php, forum_reply.php).

Possible Explotación: Investigar el tipo específico de vulnerabilidad (ej. inyección SQL, XSS) para buscar o crear exploits dirigidos a esos archivos.

/lists/admin/ (PHPLIST < 2.6.4): Acceso administrativo remoto y robo de información. ¡Credenciales por defecto: admin/phplist!

Possible Explotación: Intentar iniciar sesión con las credenciales predeterminadas. Investigar las vulnerabilidades de acceso remoto para posibles exploits.

/splashAdmin.php (Cobalt Qube 3): Administración activa; podría tener vulnerabilidades documentadas externamente.

Posible Explotación: Investigar las vulnerabilidades mencionadas en www.scan-associates.net y buscar exploits relacionados.

/ssdefs/, /sshome/ (Siteseed < 1.4.2): Problemas de seguridad "mayores".

Posible Explotación: Investigar los problemas de seguridad específicos de Siteseed pre-1.4.2 para identificar y explotar las vulnerabilidades.

/tiki/, /tiki/tiki-install.php (Tiki 1.7.2 <=): Ver páginas restringidas por "truco URL". ¡Credenciales por defecto: admin/admin! tiki-install.php permite reinstalación.

Posible Explotación: Investigar el "truco de URL" para acceder a páginas restringidas. Intentar iniciar sesión con admin/admin. Si tiki-install.php sigue presente, podría permitir una reinstalación maliciosa.

/scripts/samples/details.idc: Posible vulnerabilidad referenciada externamente.

Posible Explotación: Consultar RFP 9901 y www.wiretrip.net para comprender la vulnerabilidad y buscar posibles formas de explotarla.

/_vti_bin/shtml.exe (FrontPage): Posible denegación de servicio (DoS).

Posible Explotación: Enviar peticiones específicamente crafted a `/_vti_bin/shtml.exe/aux.htm` para intentar sobrecargar el servicio.

4.4:

```
renzo@renzo-IdeaPad-3-15ADA05:~/Escritorio$ nmap -p 80 175.45.176-179.0-255
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-14 15:44 -03
Nmap scan report for mail1.silibank.net.kp (175.45.176.21)
Host is up (0.41s latency).

PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap scan report for 175.45.176.22
Host is up (0.40s latency).

PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap scan report for 175.45.176.68
Host is up (0.41s latency).

PORT      STATE      SERVICE
80/tcp    open      http

Nmap scan report for 175.45.176.69
Host is up (0.42s latency).

PORT      STATE      SERVICE
80/tcp    open      http
```

Consulta de las ip de corea y su análisis del puerto 80

Como resultado de 1024 IPs, se pudo conectar a 20, las cuales 13 tenían abierto el puerto 80