Universidad Diego Portales
Criptografía y seguridad en redes

NOT informe
2025-2

I. Reglas del juego

- Todos los alumnos **deberán seguir el template de laboratorio** proporcionado por los ayudantes, en el cual se especifica el orden y contenido que debe tener la entrega final.
- Los alumnos **tendrán 1 semana** desde que inicia el laboratorio presencial para **subir a canvas el informe final** de la experiencia. Debe ser entregado **antes de las 8:30 AM** en canvas.
- **No habrá más plazo**; en caso de atraso o no entrega, **se evaluará con la nota mínima**.
- **No se sumarán puntos** en caso de que el alumno **solo proporcione imágenes y ningún tipo de explicación** y/o contexto, a pesar de que la actividad esté resuelta.
- Todos los alumnos **deberán proporcionar un enlace a su repositorio de GitHub** (en forma de comentario en la entrega), en el cual deben estar **disponibles todas las imágenes, capturas de pantalla y códigos utilizados en el informe**. Cualquier tipo de **copia será sancionada** y notificada a los organismos correspondientes. En caso de no estar, **será penalizado con un descuento de 5 décimas**.
- Todos los repositorios de GitHub deben ser **PÚBLICOS**. Caso de que no sea público se considerará como no entregado.
- Una vez que las notas han sido publicadas en canvas, el alumno tendrá **1 semana** para solicitar una **nueva corrección** indicando, como comentario en canvas y en copia a los ayudantes, que solicita recorrección.
- Para optimizar la revisión, aquellos que no utilicen o no respeten la plantilla proporcionada **recibirán un descuento de 10 décimas**.
- Finalmente, cualquier alumno que incurra en los errores que se expondrán no obtendrán el puntaje completo.

II. Not informe

En esta sección, se tratarán errores comunes y malas prácticas al momento de realizar el informe de laboratorio.

Cualquier persona que tenga algo de lo que se detallará o no cumpla con las restricciones que están en las siguientes páginas recibirá una penalización de 5 décimas.

Not Informe Laboratorio

Deben proporcionar sus datos correctamente

Sección X

Alumno X
e-mail: alumno.contacto@mail.udp.cl

Marzo de 2024

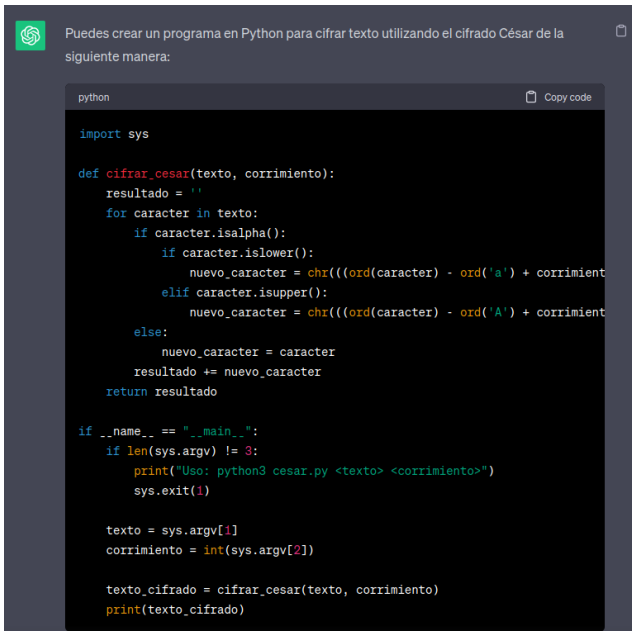
Índice

El template ya viene con las secciones preparadas, **NUNCA** eliminen o agreguen una sección. Si no las responden deben dejarla en blanco para no retrasar la revisión. (Siempre nos vamos a dar cuenta si eliminan o agregan algo)

1. Desarrollo de Actividades

1.1. Actividad 1

Deben respetar las secciones definidas, por algo existen. Cada imágen debe ir en su sección



NO usar imágenes diminutas

Figura 1: Generación de chatGPT de un programa en python que hace el cifrado César

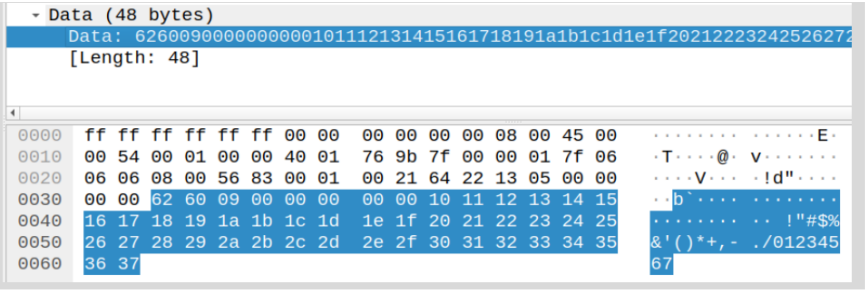
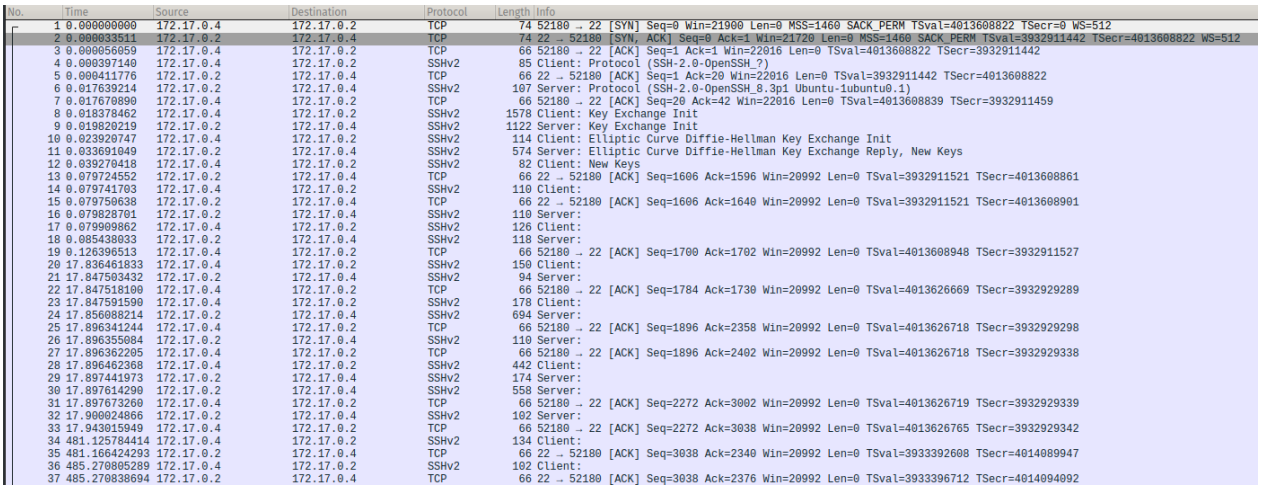


Figura 2: Datos ICMP

Sin embargo, lo más importante aquí es explicar qué es lo que están mostrando y comentar un poco del código, ya sea mencionando su funcionamiento o por qué utilizaron "X"liberías, etc. No es necesario una explicación línea por línea, simplemente información para complementar la imágen y demostrar que el estudiante entiende su funcionamiento.

2. Actividad 2

2.1. Comprobación del tráfico generado por los clientes



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.17.0.4	172.17.0.2	TCP	74	52180 → 22 [SYN] Seq=0 Win=21900 Len=0 MSS=1460 SACK_PERM TSval=4013608822 TSecr=0 WS=512
2	0.000033511	172.17.0.2	172.17.0.4	TCP	74	22 → 52180 [SYN, ACK] Seq=0 Ack=1 Win=21720 Len=0 MSS=1460 SACK_PERM TSval=3932911442 TSecr=4013608822 WS=512
3	0.000056059	172.17.0.4	172.17.0.2	TCP	66	52180 → 22 [ACK] Seq=1 Ack=1 Win=22016 Len=0 TSval=4013608822 TSecr=3932911442
4	0.000397140	172.17.0.4	172.17.0.2	SSHv2	85	Client: Protocol (SSH-2.0-OpenSSH_7)
5	0.000411776	172.17.0.2	172.17.0.4	TCP	66	22 → 52180 [ACK] Seq=1 Ack=20 Win=22016 Len=0 TSval=3932911442 TSecr=4013608822
6	0.017639214	172.17.0.2	172.17.0.4	SSHv2	107	Server: Protocol (SSH-2.0-OpenSSH_8.3p1 Ubuntu-1ubuntu0.1)
7	0.017670890	172.17.0.4	172.17.0.2	TCP	66	52180 → 22 [ACK] Seq=20 Ack=42 Win=22016 Len=0 TSval=4013608839 TSecr=3932911459
8	0.018378462	172.17.0.4	172.17.0.2	SSHv2	1578	Client: Key Exchange Init
9	0.019820219	172.17.0.2	172.17.0.4	SSHv2	1122	Server: Key Exchange Init
10	0.023920747	172.17.0.4	172.17.0.2	SSHv2	114	Client: Elliptic Curve Diffie-Hellman Key Exchange Init
11	0.033691049	172.17.0.2	172.17.0.4	SSHv2	574	Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
12	0.039270418	172.17.0.4	172.17.0.2	SSHv2	82	Client: New Keys
13	0.079724552	172.17.0.2	172.17.0.4	TCP	66	22 → 52180 [ACK] Seq=1606 Ack=1596 Win=20992 Len=0 TSval=3932911521 TSecr=4013608861
14	0.079741703	172.17.0.4	172.17.0.2	SSHv2	110	Client:
15	0.079750638	172.17.0.2	172.17.0.4	TCP	66	22 → 52180 [ACK] Seq=1606 Ack=1640 Win=20992 Len=0 TSval=3932911521 TSecr=4013608901
16	0.079828701	172.17.0.2	172.17.0.4	SSHv2	110	Server:
17	0.079909862	172.17.0.4	172.17.0.2	SSHv2	126	Client:
18	0.085438033	172.17.0.2	172.17.0.4	SSHv2	118	Server:
19	0.126396513	172.17.0.4	172.17.0.2	TCP	66	52180 → 22 [ACK] Seq=1700 Ack=1702 Win=20992 Len=0 TSval=4013608948 TSecr=3932911527
20	17.836461833	172.17.0.4	172.17.0.2	SSHv2	150	Client:
21	17.847503432	172.17.0.2	172.17.0.4	SSHv2	94	Server:
22	17.847518100	172.17.0.4	172.17.0.2	TCP	66	52180 → 22 [ACK] Seq=1784 Ack=1730 Win=20992 Len=0 TSval=4013626669 TSecr=3932929289
23	17.847591590	172.17.0.4	172.17.0.2	SSHv2	178	Client:
24	17.856088214	172.17.0.2	172.17.0.4	SSHv2	694	Server:
25	17.896341244	172.17.0.4	172.17.0.2	TCP	66	52180 → 22 [ACK] Seq=1896 Ack=2358 Win=20992 Len=0 TSval=4013626718 TSecr=3932929298
26	17.896355084	172.17.0.2	172.17.0.4	SSHv2	110	Server:
27	17.896362205	172.17.0.4	172.17.0.2	TCP	66	52180 → 22 [ACK] Seq=1896 Ack=2402 Win=20992 Len=0 TSval=4013626718 TSecr=3932929338
28	17.896462368	172.17.0.4	172.17.0.2	SSHv2	442	Client:
29	17.897441973	172.17.0.2	172.17.0.4	SSHv2	174	Server:
30	17.897614290	172.17.0.2	172.17.0.4	SSHv2	558	Server:
31	17.897673260	172.17.0.4	172.17.0.2	TCP	66	52180 → 22 [ACK] Seq=2272 Ack=3002 Win=20992 Len=0 TSval=4013626719 TSecr=3932929339
32	17.900024866	172.17.0.2	172.17.0.4	SSHv2	102	Server:
33	17.943015949	172.17.0.4	172.17.0.2	TCP	66	52180 → 22 [ACK] Seq=2272 Ack=3038 Win=20992 Len=0 TSval=4013626765 TSecr=3932929342
34	481.125784414	172.17.0.4	172.17.0.2	SSHv2	134	Client:
35	481.166424293	172.17.0.2	172.17.0.4	TCP	66	22 → 52180 [ACK] Seq=3038 Ack=2340 Win=20992 Len=0 TSval=3933392608 TSecr=4014089947
36	485.270805289	172.17.0.4	172.17.0.2	SSHv2	102	Client:
37	485.270838694	172.17.0.2	172.17.0.4	TCP	66	22 → 52180 [ACK] Seq=3038 Ack=2376 Win=20992 Len=0 TSval=3933396712 TSecr=4014094092

Figura 3: Tráfico generado por el cliente 1

Si se pide analizar tráfico o demostrar el funcionamiento de algo, debe explicar lo que están mostrando, no basta con poner una captura de pantalla. En este caso, se tienen unas capturas de tráfico en Wireshark, deben explicar qué está sucediendo allí detalladamente para demostrar que entendieron lo que están haciendo. Los paquetes que no corresponden a lo que se le pide, los debe filtrar para que no aparezcan.

También, si el ítem viene con una pregunta específica, jamás pongan una captura genérica pensando que quizás si tengo suerte, esta me la piden.

Adicionalmente, NO seleccionen un paquete si no estarán hablando de él o no es importante. Siempre deben seleccionar lo que se les pide, también puede ser algo adicional que a su juicio sea importante, siempre y cuando tenga la correcta explicación o justificación

3. Actividad 3

NO poner imágenes sin contexto ni explicación.

Si preguntan sobre X captura, debe mostrar X, no debe ser una captura genérica que no muestre claramente lo que se pide.

Figura 4: Gato hackeando la nasa

En la imágen anterior se ve a un gato hackeando la nasa. Por lo que se puede concluir que es peligroso.

¿Que diferencia existe entre el cliente 1 y 2?

Porque son clientes distintos y usan otras tecnologías.

¿Cuál es la diferencia entre sus funciones criptográficas?

No supe verlas, así que no puedo responder :'v

Estas no son respuestas válidas, se debe investigar y proporcionar respuestas sólidas que tengan sustento y sentido con lo que se está preguntando.

La forma correcta de referenciar una imágen es de la siguiente forma:
"*En la Figura X se puede observar...*"
Siempre diciendo a que Figura se refiere. Si no se referencia la imagen, no se sabrá cuando habla de ella. Recuerde que debe explicar lo que se realiza u obtiene en cada imagen para demostrar que sabe lo que se está realizando.

4. ~~I~~mágenes

Las imágenes van en cada sección, jamás se deben poner al final del informe. Nunca deben hablar sobre la imágen número 1 y que dicha imágen esté 2 páginas más abajo.

Figura 5: Perro hackeando el pentágono

Resumen:

Explicar de manera detallada.

Jamás poner imágenes sin contexto ni explicación.

Ser ordenado con las secciones y jamás borrarlas a conveniencia.

Responder lo solicitado

Figura 6: Hamster entrando a la matrix