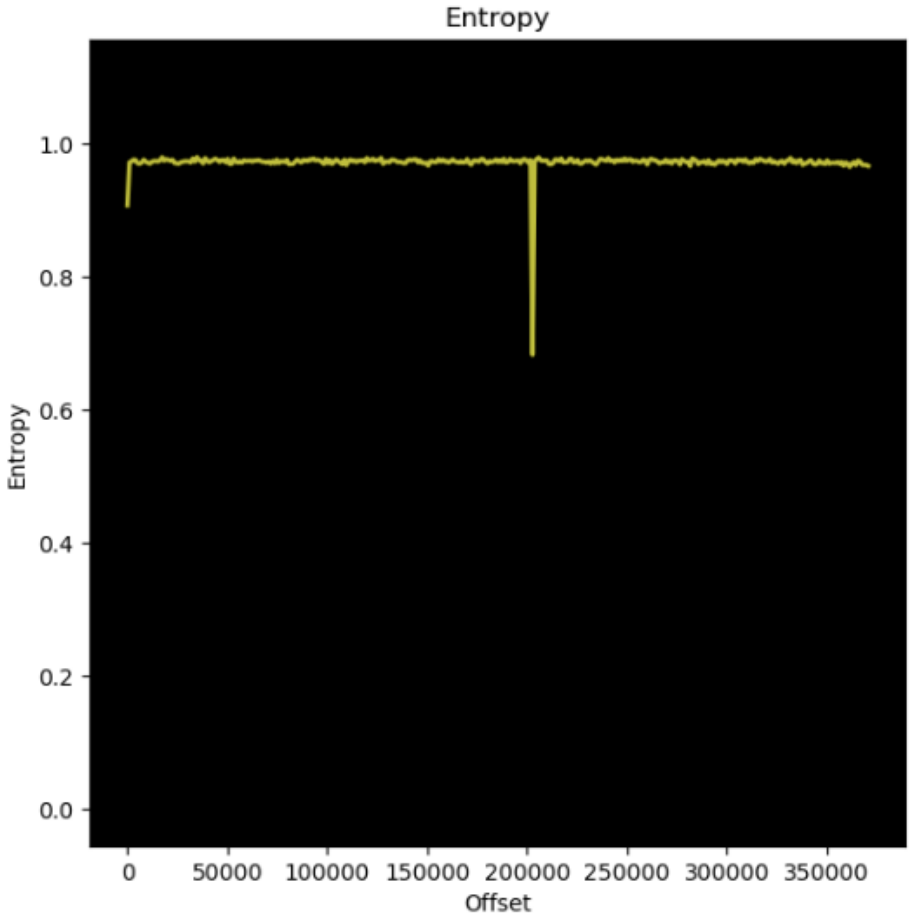
Review Test Submission: Parcial 2

User	GIAN LUCA PECILE
Course	(20221Q) 72.44 - Criptografía y Seguridad - Comisión: S
Test	Parcial 2
Started	6/23/22 4:03 PM
Submitted	6/23/22 5:32 PM
Status	Completed
Attempt Score	95 out of 100 points
Time Elapsed	1 hour, 29 minutes out of 1 hour and 30 minutes
Results Displayed	All Answers, Submitted Answers, Correct Answers, Feedback, Incorrectly Answered Questions

Question 1

10 out of 10 points

La siguiente imagen es el resultado de un análisis sobre una imagen adjunta en un mail sospechoso. En el eje X se presenta el offset en bytes desde el principio del archivo y el eje Y la entropía sobre ese byte. ¿Qué puede decir sobre el archivo? Fundamente por qué el sistema pudo detectarlo como sospechoso. ¿Qué representa la Entropía ?



Selected Answer:

En la imagen adjunta se puede ver el gráfico de la entropía de la imagen. Si esta fuera una imagen completamente blanca sin ningún tipo de mensaje escondido la entropía daría 0 ya que se sabe que el resultado es siempre igual para cada pixel y no hay incertezas, que es lo que mide el concepto de la entropía. Similar a como hicimos en el TPE de estenografía, se puede ver que se hace un análisis con algún programa que genera un gráfico de entropía (por ejemplo binwalk utilizando el parámetro -E) donde por el extraño pico que ocurre en el offset ~200000 podemos suponer que se está ocultando algo. Se podría hacer un analisis con un hex editor para ver si es un mensaje de texto plano incrustado en el archivo o si es algo más delicado realizado con método como LSB1, LSB4 o alguna de sus versiones mejoradas pero a su vez no parece estar encriptado lo que se oculta. Este método de esconder mensajes no sería detectado por el sistema ya que en definitiva se está pasando un archivo adjunto que posee escondido otro archivo y el sistema no se encarga de analizar los contenidos. Hay casos donde gmail detalla que dentro de un zip no puede garantizar que los contenidos no sean confiables por este mismo motivo.

Correct Answer: [None]

Response Feedback: [None Given]

Question 2

10 out of 10 points

Se encuentra en una página de “filas virtuales” para poder comprar entradas a un recital. Viendo que está en la posición N°86 y los tickets se agotan, decide ver si puede apurar el trámite. En eso, se da cuenta que el servicio web utiliza una librería de javascript que corre en el browser para realizar el mecanismo de fila. ¿Es correcto esto? En caso de que no lo sea, ¿Qué tipo de vulnerabilidad sería? ¿Podría abusarse para saltearse la fila?

Selected Answer: Es una gran vulnerabilidad esto y se encuentra basada en un caso real que se ha explotado dicha vulnerabilidad para un recital famoso argentino.
Lo que se está haciendo en este caso es confiar en el cliente y este puede realizar cambios al servidor si lo desea, esto es la base de un ataque de tipo CSRF que se puede abusar para saltear lugares en la fila alterando el archivo del cliente tal como sucedió en el caso real previamente mencionado.

Correct [None]

Answer:

Response Feedback: [None Given]

Question 3

10 out of 10 points

Un ex-compañero graduado le comenta sobre su startup de un producto embebido. Luego de detallar los aspectos técnicos, le explica como anécdota que tuvo que aprender a deshabilitar controles de canary y de ejecución de stack y heap para el binario final por unas funcionalidades extras que requería. ¿Podría esto ser un problema? En caso de que sí, explicar por qué. En caso de que no, justificar por qué no.

Selected Answer: Esto puede ser un problema grave, dichas restricciones existen para proteger al usuario y no para generar trabas. Nuestro ex-compañero graduado debería tener cuidado ya que se pueden explotar vulnerabilidades relacionadas al stack y heap como la de tipo "buffer overflow".

Correct Answer: [None]

Response Feedback: [None Given]

Question 4

10 out of 10 points

Para un trabajo práctico de la universidad, con su grupo concuerdan realizar un “hosteador de CVs”. La idea es que una persona suba su CV como un archivo HTML y su servicio simplemente hostearía el archivo, garantizando su disponibilidad y ofreciendo que esté bajo el nombre de dominio que usted elija. ¿Ve algún problema de seguridad en la idea? Argumente su respuesta.

Selected Answer: Hay un gran problema de seguridad con la idea de confiar tanto en que cada uno suba un archivo HTML que no sea malicioso, se realiza un salto de fe en creer que todo usaurio usaría su archivo puramente para "hostear su CV". En un archivo HTML se puede contener código Javascript donde, por ejemplo, se puede realizar un ataque de tipo XSS persistente que cuando cada usario ingresa a ese dominio, este se ve afectado por el ataque.

Correct Answer: Es una muy mala idea desde el punto de vista de seguridad porque un usuario podría subir un HTML con código malicioso y nosotros los estaríamos hosteando para que cualquier persona que entre, lo active. Habría que *mínimo* sanitizar la entrada y aún así, revisar todos los links que utilice.

Response Feedback: [None Given]

Question 5

10 out of 10 points

Su prima comenta que quiere empezar un kiosco. Por lo que consulta si le puede hacer un presupuesto del equipo necesario para funcionar. Usted que cursa Criptografía y Seguridad le muestra un presupuesto de 1K USD. Cuando su prima le pregunta por qué tanto, le contesta que es lo necesario para evitar que un atacante externo robe datos confidenciales o realice interrupción del servicio. ¿Cree que es correcto el nivel de protección? En caso de que no, ¿Qué etapa del diseño cree que se realizó mal?

Selected Answer: El presupuesto tan alto con ese nivel de protección para el equipo de un kiosco es muy costoso teniendo en cuenta lo que se desea proteger, no se realizan muchas ataques de seguridad informática donde se roban datos o se desea interrumpir el servicio de kioscos entonces esto se tiene que tener en cuenta al momento de desarrollar un servicio.
Uno de los principios de diseño que se realizó es el psicológico donde no se debe complicar el sistema más de lo que se debería con el motivo de ser más seguro, sacrificando la usabilidad del mismo en el proceso ya que nadie querría comprar en un kiosco que haga verificar la identidad (como caso extremo).

Correct Answer: Se realizó un mal Threat Modelling, en donde se plantea qué tipo de atacante va a ser el más común para amenazar mi modelo de negocios. En el caso de un quiosco, no me preocupa que me hackee la NSA sino que me roben la mercadería. En caso de que no funcione el sistema, siempre puedo cobrar en efectivo

Response Feedback: [None Given]

Question 6

7 out of 10 points

Suponiendo el software del controlador de las barras de grafito de la central nuclear de Chernobyl, ¿Se puede asegurar que un sistema cómo este es seguro mediante algún mecanismo?

Selected Answer: Es díficil asegurar que un sistema es seguro pero hay herramientas que permiten detectar vulnerabilidades en el sistema como en el caso de pen testing que se podría contratar un equipo o individuo para realizar pruebas y que estos brinden las vulnerabilidades encontradas con el fin de auditarlas, corregirlas y mejorar la seguridad del sistema.

Correct Answer: [None]

Response Feedback: En este caso dada la criticidad del sistema se pueden considerar métodos formales.

Question 7

10 out of 10 points

Describir cómo se podría implementar un esquema básico de autenticación en una aplicación web basada en HTTPS, y como implementar un esquema para evitar un ataque basado en CSRF.

Selected Answer:

En un esquema de autenticación web se busca verificar que la perosona realmente tiene acceso a la cuenta que desea ingresar, existen distintos mecanismos como funciones de verificación (por ejemplo 2FA, Authkey, token, etc) que tienen como objetivo el reducir que con el simple hurto de una clave se pueda acceder a la cuenta de un usuario. Recientemente Apple anunció -en conjunto con Google, Microsoft y diversas empresas de seguridad- un nuevo sistema llamado passkeys que no involucra el uso de una contraseña sino el uso de claves privadas on device y públicas que se acceden con el hardware biometrico del dispositivo a modo de mejorar la seguridad y teniendo en cuenta el principio de diseño de la simplicidad de los sistemas ya que se usará de modo masivo.
En CSRF el servidor confía en el cliente. Un ejemplo de un ataque podría ser: Se le envia al usuario un mail que tiene como objetivo phishing de sus datos y logra robarlos. El atacante luego accede a la cuenta de banco del cliente donde el banco confía que este es el cliente. Este tipo de ataque se podría evitar con una cookie o datos extra en los pedidos para identificar, autenticar y validar mediante la función de verificación que el cliente es de hecho el asociado a la cuenta.

Correct Answer: [None]

Response Feedback: [None Given]

Question 8

10 out of 10 points

Dado que fue conocida una nueva vulnerabilidad la semana pasada, se emitió un parche de seguridad a aplicar en los equipos. Sin embargo, el jefe de IT le dice que no quiere aplicarlo porque el parche conlleva un reinicio del servidor y por lo tanto, un tiempo muerto de los equipos que constaría mucha plata a la empresa. De 2 argumentos a favor de que se aplique el parche, justificándose con los principios de diseños vistos en clase.

Selected Answer:

Es una mala práctica de seguridad el no actualizar el software ante cualquier vulnerabilidad nueva que sea encontrada y que se realice un parche de la misma ya que se puede explotar la misma en caso que se conozca que el servicio que se ofrece no está actualizado para protegerse de la misma (por ejemplo recientemente el caso de log4j donde al día de hoy hay sitios web que no se encuentran actualizados para proteger dicha vulnerabilidad).
El argumento que da el jefe de IT va en contra de los principios de diseño ya que este cree que ahorrará más dinero el dejar una abertura en el sistema antes que solucionar la misma. Si esta puede ser explotada, es posible que se generen más pérdidas de las que se tendrían si se apagara el servidor para una actualización. Además, se deben tener estadísticas de los horarios con menor tráfico las cuales se pueden utilizar para mitigar la pérdida y los beneficios son mucho mayores.

Correct Answer: [None]

Response Feedback: [None Given]

Question 9

10 out of 10 points

La manera más segura de evitar que un sistema de APIs interna de un Sistema Operativo sea vulnerado es mantener secreta la documentación.

Selected Answer: ✔ False

Answers: True

✔ False

Response Feedback: Eso sería seguridad por ofuscación.

Question 10

8 out of 10 points

La empresa Zeo de criptomonedas implementa un exchange crypto que para poder acceder al portfolio es necesario autenticarse en el sistema. Para el sistema de autenticación, el CSO de Zeo que tiene 5 PhD de la Universidad del Trading, propone un sistema por el cual divide a los usuarios en 3 grupos y les asigna nombres de usuario que empiezan con una letra mayúscula identificatoria para cada caso, U, T, y P. Para la U se permiten sólo claves de acceso que contengan mayúsculas, para la T minúsculas y para la P sólo números. Las claves sólo pueden tener un máximo de 10 caracteres.

a) Utilizando el concepto de entropía, mostrar cómo conocer el nombre de un usuario permite conocer información de la clave, para probar que este esquema super sofisticado es pésimo en relación a la seguridad del proceso de autenticación.

b) El CSO de Zeo es muy capo e insiste en que no es problemática ese flujo de información. Demostrar que en base a esa información adicional sobre las claves,

son más simples de romper.

Selected Answer:

Autenticación:
U -> claves de acceso mayúscula (0-26)
T -> claves de acceso minúsculas (0-26)
P -> claves de acceso números (0-9)

largo de las claves -> máximo 10 caracteres.

Ecuación Entropía: -\sum_{a≤i≤b} (\frac {1} {p} * \log_2 {p})

Se debe ver si las variables se encuentran relacionadas con la ecuación de entropía condicional donde de hecho se va a obtener un valor el cual nos dirá que se encuentran correlacionadas las variables. Por lo tanto se puede decir que hay flujo de información.

En base a que existe un flujo de información, se puede predecir la clave de autenticación debido a que se exclusivamente un conjunto de números o letras que puede ser roto fácilemente con brute force ya que posee como máximo 10 caracteres, haciendo así que el sistema tenga una seguridad pésima.

Correct Answer:

La idea es demostrar que hay una caeida en la entropia condicional cuando se conoce el nombre de usuario y para la segunda parte utilizar la formula de andersson para demostrar que esa información de restricción en los passwords sirve porque hay que probar menos combinaciones.

Response Feedback:

Hay que demostrarlo con números !

Monday, June 27, 2022 9:35:44 AM ART

← OK