Presentacion

Nombre: Bradigson

Matricula: 2018-6114

Profesor: Huascar Frias Vilorio

Trabajo: TAREA DE LA UNIDAD NO. 1

Dar respuesta a las siguientes preguntas:

1. Clasificación de los virus informáticos ?

Virus mutantes.Un virus mutante cambia con cada nueva infección, para hacer esto seutilizan diferentes técnicas, algunos encriptan el código ejecutable del virus y son capaces decambiar la clave de encripción, de esta manera se pueden lograr una gran diversidad devariantes.

Virus de boot y de programas.Son muy escasos, son los virus que son capaces de infectar tanto el boot como los programas.

Virus de programas.Un virus de programa introduce su código al comienzo de losprogramas que infecta, de esta manera cada vez que sea ejecutado el virus toma el controldel equipo. Casi todos los virus de programas quedan residentes en memoria.

2. Defina: Cracker y hacker ?

Los términos ***hacker*** **y** ***cracker*** **tienen significados diferentes**, ya que, mientras que el primero alude a la persona capaz de introducirse en sistemas informáticos ajenos, el segundo se refiere a quien lo hace con fines ilícitos. En las noticias es frecuente encontrar frases como «El grupo hacker que hizo posible el caos de la semana pasada "prepara algo peor"» o «Unos 'hackers' extorsionan a Disney con la filtración de *Piratas del Caribe: La venganza de Salazar*».

Aunque en el uso general es frecuente asociar la palabra *hacker* a 'pirata informático' y, por tanto, a quien usa sus conocimientos con fines ilegales, en el ámbito de la informática se diferencia claramente entre *hacker* y *cracker*.

Así lo recogen los principales diccionarios de inglés y algunos de español como el de María Moliner, que indica que **un *hacker* es una 'persona con sólidos conocimientos informáticos capaz de introducirse sin autorización en sistemas ajenos** para manipularlos, obtener información, etc., o simplemente por diversión'.

La palabra ***cracker***, en cambio, se aplica a quien, además de ser capaz de entrar en sistemas ajenos, **lo hace con fines delictivos**, como señala el diccionario de Oxford.

Así, en los ejemplos anteriores, y teniendo en cuenta el tipo de actividad que se les atribuye, habría sido preferible escribir «El grupo *cracker* que hizo posible el caos de la semana pasada "prepara algo peor"» y

«Unos *crackers* extorsionan a Disney con la filtración de *Piratas del Caribe: La venganza de Salazar*».
Un uso adecuado de ambos términos es el que figura en el siguiente ejemplo: «Las empresas necesitarán 825 000 *hackers* para frenar a los *crackers* en 2025».

3. Mencione 5 medidas preventivas para proteger los equipos informáticos ?

1. Actualizaciones regulares.
2. Proteje tu **equipo** con programas antivirus.
3. Atención a fuentes **de** datos desconocidas! .
4. Precaución con archivos desconocidos en Internet.
5. Cuidado al instalar un software nuevo. .

4. Qué política de seguridad usted implementaría en una empresa para minimizar los riesgos de los virus informáticos. ?

1. Controles de acceso a los datos más estrictos
2. Realizar copias de seguridad
3. Utilizar contraseñas seguras
4. Proteger el correo electrónico
5. Contratar un software integral de seguridad
6. Utilizar software DLP
7. Trabajar en la nube
8. Involucrar a toda la empresa en la seguridad
9. Monitorización continua y respuesta inmediata

5. Defina:

a) Firewall

Un **firewall**, también llamado cortafuegos, es un sistema cuya función es prevenir y proteger a nuestra red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso. Permite el tráfico entrante y saliente que hay entre redes u ordenadores de una misma red.

b) Phising

Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de **phishing** que es la más común.

c) Cookie

El anglicismo cookie, usado también galleta o galleta informática, es un término que hace referencia a una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador.

d) Captcha

Un **CAPTCHA** (Completely Automated Public Turing test to tell Computers and Humans Apart: test de Turing público y automático para distinguir a los ordenadores de los humanos) es un tipo de medida de seguridad conocido como autenticación pregunta-respuesta.

e) Spyware

El **Spyware**, también denominado spybot, es un programa malicioso espía. Se trata de un malware, un tipo de software utilizado para recopilar información de un ordenador o dispositivo informático y transmitir la información a una entidad externa sin el permiso del dueño del ordenador.