Nombre Completo: **LU:**

Parcial – Seguridad de la Información – 5/6/2019

Elija la opción correcta (2 ptos):

1. ¿Cuál de estas no es una amenaza activa?
A. Keylogger
B. Sniffing
C. Man in the middle
D. DDOS

2. Indique la opción falsa. El software applocker
A. Permite restringir los programas que pueden ser ejecutados en un sistema operativo.
B. Funciona tanto en linux como en windows.
C. Tiene un modo para auditar mediante logs, y otro de aplicación efectiva de restricciones.
D. Se pueden asignar permisos en forma global en el sistema o en forma individual a uno o varios grupos o usuarios.

3. ¿Cuál de las siguientes no es una característica del modelo Clark-Wilson?
A. Es un modelo que hace hincapié en la integridad.
B. Hace foco en las transacciones.
C. Hace foco en la separación de tareas.
D. Hace foco en un modelo multinivel.

4. Indique la opción correcta. En un esquema de PKI, la autoridad de registro es la encargada de:
A. Emitir certificados.
B. Validar la identidad del solicitante de un certificado.
C. Auditar el sistema.
D. Definir las políticas y procedimientos de certificación.

5. Indique la opción correcta. Las herramientas de control de integridad de archivos como tripwire o aide:
A. Firman digitalmente sus archivos de configuración.
B. Detectan el origen de los ataques.
C. Almacenan metadata de los archivos a controlar.
D. Deben estar ejecutándose en forma permanente.

6. El concepto de return to libc está relacionado con:
A. Una forma de saltear restricciones cuando el stack de un proceso no es ejecutable.
B. Un tipo de ataque al cifrado con PFS.
C. Una forma de explotar una vulnerabilidad web de inyección de comandos.
D. Volver a utilizar ciertos lenguajes de programación más performantes.

Desarrolle (identifique todo lo que asume):

1. Describa qué son las linux capabilities.(1 pto)

2. Usando dibujos y unas pocas palabras, ilustre el concepto de botnet. No escriba oraciones ni párrafos.(1pto)

3. En control de acceso, ¿cuál es la dificultad que trae almacenar los permisos mediante listas de capacidades? (1pto)

4. ¿Cuáles son los usos que se les da en seguridad a los números aleatorios? ¿Se debe tener alguna consideración a la hora de generarlos? (1pto)

5. Describa cómo realizaría el robo de sesión a un usuario autenticado en un sitio de apuestas online en la que las cookies de sesión no viajen cifradas por HTTPS, asumiendo que en la aplicación web no se ha descubierto ninguna vulnerabilidad en la implementación del código (ni SQLi, ni XSS). ¿Qué herramientas usaría? ¿Qué requisitos son necesarios para realizar el ataque? (1 pto)

6. Se acercan las elecciones. Se le solicita implementar un sistema que permita a los ciudadanos consultar dónde votan, pero evitando que otro sistema automatizado pueda consultar el padrón electoral en forma completa. Indique consideraciones a tener en cuenta, incluyendo cuestiones de facilidad de uso y privacidad de datos para, por ejemplo, dificultar que un ciudadano curioso averigüe donde vive o donde vota su artista preferido. (1,5 ptos)

7. Mediante el decreto 1265/2016, el Poder Ejecutivo oficializó la creación de la Plataforma de Autenticación Electrónica Central (PAEC), una plataforma de autenticación electrónica para acreditar la identidad del ciudadano a través de un único punto de entrada. La PAEC estará disponible para las entidades y jurisdicciones que componen el Sector Público Nacional. La PAEC verificará la autenticidad de las credenciales electrónicas alegada por personas humanas y jurídicas, pudiendo utilizar diversos proveedores de autenticación. Indique las consideraciones de seguridad a tener en cuenta para implementar esta plataforma, teniendo especialmente en cuenta el proceso de autenticación de los usuarios, la posibilidad de usar más de un proveedor de autenticación, el acceso a diversos sistemas a través de esta plataforma, los procesos de auditoría, y la disponibilidad del servicio. (1,5 ptos)