Segundo Ejercicio del proceso selectivo de ingreso en la escala de Gestión, especialidad informática, de la Universidad de Cádiz mediante turno de promoción interna (16 de mayo de 2022)

Supuesto práctico 1

Se pretende actualizar los equipos de puestos de trabajo disponibles en un aula informática de la Facultad de Ciencias que dispone de 30 puestos para alumnos y un puesto para el profesor. La cantidad estimada disponible por cada equipo microinformático completo es de 800 a 900 euros.

Los programas para la docencia que se van a usar desde esta nueva aula informática son MATLAB, SPSS, ASPEN, QGIS, Octave, R-UCA, Maxima, Scientific Notebook.

Responda razonadamente las siguientes cuestiones:

1.- Sistemas o herramientas que utilizaría para la gestión de las imágenes locales de los equipos del aula informática.

2.- Posibles soluciones para poner a disposición de los alumnos el software relacionado anteriormente, desde los equipos del aula informática.

3.- Propuesta de posibles equipos microinformáticos a adquirir, conforme a la disponibilidad económica indicada, indicando las características hardware de los equipos.

4.- Alternativas que le puede dar al docente en el aula informática para que no tenga que llevar un pendrive con su material docente.

5.- Propuesta de medios audiovisuales para la mesa del profesor para el desarrollo de su docencia en el aula informática.

Supuesto práctico 2

La universidad de Cádiz dispone de un CPD situado en el campus de Cádiz y un mini CPD en cada uno de los campus restantes. Se disponen de 2 aulas informáticas por campus, cada aula dispone de un ordenador para el profesorado y 24 ordenadores para el alumnado.

Se desea implantar el sistema OpenGnsys para la clonación de equipos de las aulas.

a) ¿Qué tipo componentes hardware o servidores serían necesarios?

b) ¿Qué componentes software de OpenGnsys se precisan y cuáles serían sus funciones?

c) ¿Dónde ubicaría/instalaría cada uno de los componentes hardware y software?

d) El servicio de comunicaciones de la Universidad de Cádiz ha asignado el siguiente direccionamiento para las redes de aulas de cada uno de los Campus:

	RED de Aulas	**Router/Gateway**	**DNS**	**Mascara de Red**	**Broadcast**
Cádiz	10.161.0.0/16	10.161.1.1	10.161.1.3		
Puerto Real	10.162.0.0/16	10.162.1.1	10.162.1.3		
Jerez	10.163.0.0/16	10.163.1.1	10.163.1.3		
Algeciras	10.164.0.0/16	10.164.1.1	10.164.1.3		

d.1 Que mascara de red y dirección de broadcast le correspondería a cada campus.

d.2 Defina un esquema de direccionamiento IP para las aulas de informática de cada uno de los campus. Razone ese esquema.

d.3 Defina un esquema de nombres para los equipos de las aulas de informática de cada uno de los campos. Razone ese esquema.

e) ¿Qué configuraciones debe realizar en las BIOS de los equipos para que el equipo pueda ser gestionado por OpenGnsys?

f) ¿Qué datos del equipo del aula se debe dar de alta en la consola web para que el equipo pueda ser gestionado con OpenGnsys?

g) ¿Qué direcciones IP le asignaría a cada uno de los componentes software de OpenGnsys?

h) Defina una nomenclatura de nombres para las imágenes que se creen con OpenGnsys que facilite la gestión, utilización y actualización de dichas imágenes, teniendo en cuenta que el nombre de la imagen no debe ser mayor de 50 caracteres y no se puede usar como separador el signo **-** .

i) Describa un protocolo con los pasos a seguir para la creación de una imagen con OpenGnsys

Supuesto práctico 3

Hemos recibido un anuncio en el que nos avisan de que se ha descubierto una vulnerabilidad en el protocolo de acceso a escritorio remoto de Windows (RDP) que afecta a los SO Windows, tanto clientes como de servidor. La característica más relevante de esta vulnerabilidad es que, sin necesidad de la intervención del usuario, y simplemente enviando una petición al servicio RDP debidamente formada, permite ganar el acceso total a la máquina objetivo y, desde ahí, realizar la actividad maliciosa correspondiente y continuar propagándose.

Se ha detectado que se ha desarrollado un exploit y que ya están circulando varios virus que aprovechan esta vulnerabilidad, utilizando dicho exploit. Afortunadamente, los fabricantes de antivirus han estado rápidos y ya los tienen "fichados" en su última versión de ficheros de firmas y, además, han desarrollado un agente que actúa en el equipo de forma proactiva deteniendo la ejecución de procesos que realicen actividades sospechosas.

Microsoft acaba de publicar el correspondiente parche de seguridad, pero éste no contempla a los Sistemas operativos que están fuera de soporte: Windows 7 y anteriores (en equipos de usuarios) y Windows Server 2008 y anteriores (en servidores).

Además de las capacidades de infección automáticas (mediante RDP) se ha detectado una campaña de phishing para robo de contraseñas de usuarios, con el objetivo de entrar en las máquinas con los correspondientes permisos de administrador y ejecutar un código malicioso que aprovecha esta vulnerabilidad y se propaga por la red de la institución.

El Responsable de Seguridad de la universidad es novato en estas lides y está muy preocupado con este tema; así que te manda un correo en el que pasa una referencia de la vulnerabilidad (CVE-2019-0708). La información básica que aparece en el enlace (https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2019-0708) es la siguiente:

Vulnerabilidad en Remote Desktop Services Remote Code Execution Vulnerability (CVE-2019-0708)

Tipo: Utilización después de liberación
Gravedad: Alta
Fecha publicación : 16/05/2019
Última modificación: 03/06/2021

Descripción

Existe una vulnerabilidad de ejecución remota de código en Remote Desktop Services, anteriormente conocido como Terminal Services, cuando un atacante no autenticado se conecta al sistema de destino mediante RDP y envía peticiones especialmente diseñadas, conocida como 'Remote Desktop Services Remote Code Execution Vulnerability'.

Impacto

Vector de acceso: A través de red
Complejidad de Acceso: Baja
Autenticación: No requerida para explotarla
Tipo de impacto: Compromiso total de la integridad del sistema + Compromiso total de la confidencialidad del sistema + Compromiso total de la disponibilidad del sistema

Además, el Responsable de seguridad conoce las medidas de seguridad incluidas en el ENS, pero debido a su poca experiencia no tiene nada claro las acciones concretas que deben realizarse para aplicar esas medidas y así tratar de evitar o, en el peor de los casos, mitigar el efecto que pudiera tener una infección de este tipo. En el mismo correo plantea una serie de cuestiones. Se pide una respuesta breve y razonada a cada una de ellas.

Pregunta 1:

Evaluar la gravedad y posible impacto de un ataque basado en la vulnerabilidad descrita.

Pregunta 2:

¿Cuál es la medida más importante que deberíamos aplicar para evitar que nuestros equipos sean vulnerables? ¿Qué herramientas podemos poner en marcha para automatizar y agilizar en lo posible la solución planteada?

Pregunta 3:

Y, suponiendo que se ha considerado que no es necesario que los equipos en nuestra universidad sean accesibles por el escritorio remoto, ¿qué cambios realizarías en la configuración inicial de los equipos para deshabilitarlo?

Pregunta 4:

¿Qué alternativa/s más segura/s propondrías para que algunos servidores que así lo requieran pudieran ser administrados en remoto?

Pregunta 5:

Pero probablemente hasta que podamos aplicar todo esto pase demasiado tiempo y necesitamos aplicar alguna medida de urgencia para evitar la infección. ¿Podríamos aplicar algo relacionado con la medida "op.exp.6. Protección contra código dañino" reflejada en el Esquema Nacional de Seguridad?

Pregunta 6:

Al responsable de seguridad se le ocurre que también se podría hacer algo en cuanto a "protección de las comunicaciones" para evitar la entrada y la difusión del virus por toda la red de la Universidad; ha hablado con el administrador del nodo de cabecera de red que le ha informado de que están filtrados en el cortafuegos todos los accesos desde el exterior a los "puertos bajos" (inferiores a 1024), salvo los servicios expresamente permitidos. ¿Estaríamos cubiertos con esto de intentos de ataques externos? ¿Habría que hacer algo en la cabecera de red? Y, de cara a minimizar el posible despliegue del virus dentro de la red de la UPCT, ¿qué medida recomiendas?

Pregunta 7:

Finalmente, ¿cuál creéis que es la medida (no necesariamente de índole técnico) más efectiva para minimizar los efectos de la campaña de phishing?

Supuesto práctico 4

En la Universidad de Cádiz se desea llevar un control sobre los proyectos de investigación que se desarrollan. Para ello se decide emplear una base de datos que contenga toda la información sobre los proyectos, departamentos, grupos de investigación y profesores. Esta información se detalla a continuación:

Un departamento se identifica por su nombre (Informática, Ingeniería, …). Tiene una sede situada en un determinado campus, un teléfono de contacto y un Director, que ha de ser un profesor de la UCA.

Dentro de un departamento se crean grupos de investigación. Cada grupo tiene un nombre único dentro del departamento (pero que puede ser el mismo en distintos departamentos) y está asociado a un área de conocimiento (Mecánica de los medios Continuos, Lenguajes y sistemas informáticos, …). Cada grupo tiene un responsable (líder) que ha de ser profesor de la UCA.

Un profesor está identificado por su DNI. De él se necesita conocer el nombre, titulación, años de experiencia en investigación, grupo de investigación en el que desarrolla su labor y proyectos en los que trabaja.

Cada proyecto de investigación tiene un nombre, un código único, un presupuesto, fechas de inicio y terminación y un grupo que lo desarrolla. Por otro lado, puede estar financiado por varios programas. Dentro de cada programa, cada proyecto tiene un número asociado y una cantidad de dinero financiada (Por ejemplo, el proyecto "IAAD – Inteligencia artificial aplicada a la docencia" tiene el número 3113 dentro del programa "Ayudas a la innovación docente" que le financia con 30.000 euros).

Un profesor puede participar en varios proyectos. En cada proyecto se incorpora en una determinada fecha y cesa en otra, teniendo una determinada dedicación (En horas a la semana) durante ese periodo.

a) Para el supuesto semántico del enunciado realizar identificar las entidades con sus atributos, y de las interrelaciones con su tipo de correspondencia, indicando además las cardinalidades mínimas.
b) Trazar la matriz de entidades correspondiente y el esquema E/R asociado al modelo. Describir la simbología utilizada.
c) Obtener el esquema relacional de una base de datos relacional a partir de la semántica descrita en el enunciado. Como pasos del este proceso describir las relaciones básicas, analizar los supuestos semánticos, describir las opciones de borrado y modificación, así como las reglas ECA necesarias.
d) Obtener el mismo esquema relacional a partir del esquema E/R, describiendo la evolución de los conceptos de un esquema al otro. Escribir las instrucciones SQL para crear las tablas de la base de datos relacional asociada.
e) Efectuar en álgebra relacional y en SQL las siguientes consultas:
    a. Profesores que trabajan en el grupo cuyo responsable es el profesor "Juan Pérez"
    b. Programas que financian los proyectos del grupo que dirige ese mismo profesor.