ESCUELA SUPERIOR POLITECNICA DEL LITORAL

FACULTAD DE INGENIERIA EN ELECTRICIDAD Y COMPUTACIÓN
AUDITORÍA INFORMÁTICA Y SEGURIDAD
EXÁMEN MEJORAMIENTO
Febrero 2011
PROFESOR: ING. ALFONSO ARANDA

Desarrollar los 4 escenarios presentados, aplicando lo aprendido en clases:

1) **Una entidad Financiera desarrolló, un complemento para los navegadores, que alerte cuando una página web es posiblemente un phishing. Lo interesante de su funcionamiento es que no usa una base de datos externa para detectar las páginas falsas sino un algoritmo de comparación de patrones (obtenido de las páginas reales a proteger) , con ello supliría la deficiencia que tienen los complementos tradicionales para detectar phishing de día cero o no registrados aún en la base de datos.**

   Un mes después del éxito de la solución resulta que los clientes nuevamente están siendo engañados con páginas falsas, aún teniendo el complemento instalado. Asumiendo que el complemento funciona correctamente en el análisis de patrones y tiene un margen de error de 0% , mencione y explique cuáles serían las posibles métodos(externos o internos al PC del cliente) que se estarían usando para saltarse el control del complemento QUE HACE BIEN SU TRABAJO.

2) **Una Pequeña empresa acaba de sacar a producción un portal web de pedidos en línea de regalos románticos, resulta que el primer día le ingresa un pedido por 1'000.000, del tipo de productos 5 que son cajas de bombones decorados, con facturación a nombre de: GOLOSOS S.A. RUC: 10103456789XXXX y Dirección: Pelotillehue y Conchinchina 666. El recién llegado (dos días) politécnico, encargado de los sistemas, revisa el sitio web y encuentra que cuando en el formulario uno ingresa letras en el campo de cantidad de pedidos el aplicativo responde con un error "SQL ERROR PROCEDURE pedidos ON TABLE PEDIDOS.cantidad".**
   ¿Cuáles son los pasos que debe seguir el politécnico recién llegado para encontrar la causa raiz, cual es el posible método que usaron para ingresar el pedido en mención? y ¿Cuál sería el plan de acción a seguir para solucionar el problema y que esto no vuelva a ocurrir?.

3) **Resulta que usted es el nuevo administrador de sistemas de una compañía la que está a punto de montar su portal de compras en línea. Llegando el día, después de una hora que el portal entra en producción resulta que recibe un ataque de DDOS. Mencione mínimo 10 pasos a seguir para solventar dicha situación.**

4) **La compañía donde usted trabaja está buscando obtener la certificación ISO 27001:2005, resulta que en la auditoría de Fase 1 (documental), el auditor le menciona que no va a poder continuar a la Fase 2 puesto que ha encontrado una falla medular en el sistema y a su juicio los controles seleccionados no minimizan el riesgo sobre los activos. Usted está sorprendido por este comentario y le pide por favor una reunión para explicarle paso a paso y a detalle todo el sistema. ¿Qué procedimientos les mostraría al auditor, explique?**