Seguridades de software

Examen Final.

"Como estudiante de ESPOL me comprometo a combatir la mediocridad y a actuar con honestidad; por eso no copio ni dejo copiar"

Firma de compromiso del estudiante

100	Firma de aceptación

Profesor: Gustavo Cali, M.Sc.

Estudiante: _____ Fecha: ___ / Febrero / 2018

1. **Responda Verdadero o Falso según corresponda. (30 pts.)**

   A. El objetivo de la seguridad informática es proteger activos valiosos. ( )
   B. Una amenaza es una debilidad en el Sistema. ( )
   C. Malware es un programa cuya función es dañar un sistema o causar un mal funcionamiento. ( )
   D. hacking ético es la acción de efectuar pruebas de intrusión controladas sobre sistemas informáticos . ( )
   E. ARP Spoofing es Suplantación de identidad por falsificación de tabla ARP. ( )
   F. Phishing se utiliza para estafar y obtener información confidencial usando ingeniería social. ( )
   G. Hacking manual hace uso de un software de explotación desarrollado por un tercero.( )
   H. Payloads son programas que se ejecutan remotamente en un host víctima luego de que un exploit es exitoso. ( )
   I. Payloads Bind abren el puerto en mi máquina, para que la maquina victima/objetivo se conecte a mi máquina. ( )
   J. En un ataque basado en Diccionario se prueba todas las combinaciones posibles de claves. ( )

2. **Seleccione la opción(es) correctas según corresponda. (30 pts.).**

Ejemplos de ingeniería social:

1. Envío de correos electrónicos falsos con adjuntos maliciosos
2. Llamadas al personal del cliente fingiendo ser un técnico del proveedor de Internet
3. Visitas a las instalaciones de la empresa pretendiendo ser un cliente para colocar un capturador de teclado (keylogger)

Reconocimiento pasivo es:

1. Buscar en el periódico por anuncios de ofertas de empleo en el departamento de sistemas de la empresa X
2. Consultas de directorios en Internet.
3. Búsquedas en redes sociales.
4. Llamadas al personal para obtener información confidencial.

Reconocimiento activo es:

1. Barridos de ping para determinar los equipos públicos activos dentro de un rango de IP's.
2. Conexión a un puerto de un aplicativo para obtener un banner y tratar de determinar la versión.
3. Recuperación de información desde la basura.
4. Hacer un mapeo de red para determinar la existencia de un firewall o router de borde.

3. Escriba las fases del hacking/cracker y del hacking ético (20 pts.).

4. Escribir 4 tipos de Hackers y su definición. (20 pts.).