SEGURIDAD DE SISTEMAS

TERCER PARCIAL

INSTRUCCIONES

- **Realice un manual utilizando las capturas de pantalla de todo el procedimiento. Desde la etapa de creación de la máquina virtual, instalación, configuración, hasta las pruebas de análisis de vulnerabilidad, ataques, etc. La entrega del manual es en un documento .pdf (DEBEN PODER VERSE TODAS LAS TAREAS NECESARIAS)**
- **El fondo de pantalla de su equipo, portátil, etc, debe ser una imagen en blanco con los nombres de todos los integrantes del grupo.**

PARTE 1 (60%) - DÍA LUNES

NESSUS Y OPENVAS

1.- Utilizará 2 máquinas virtuales, por lo tanto asegúrese que estén en red inicialmente.

Realizar la instalación de NESSUS en una máquina con Linux, a partir de ello realizar pruebas para detectar vulnerabilidades a la PC objetivo:

Realice la instalación OPENVAS o utilice la disponible en KALI y realice el escaneo de vulnerabilidades a la misma PC Objetivo.

- PC OBJETIVO "Metasploitable 2" (Puede descargarla de Internet o usar la que se le facilitará)

De las vulnerabilidades encontradas con las 2 herramientas, elija una por cada PC y analice su significado, característica y la solución.

Por último realice una prueba a la página web de la universidad con ambas herramientas y muestre las vulnerabilidades encontradas.

NMAP

2.- Instale NMAP en una máquina con LINUX o use la Distribución KALI LINUX para responder lo siguiente:

(INDIQUE QUÉ SENTENCIA O COMANDOS UTILIZÓ)

a) En la web www.uatf.edu.bo y www.uajms.edu.bo Que servicios están corriendo? Que versión tienen los servidores (www, ssh,etc)?
b) La IP 216.58.192.100 es un Servidor Web? Justifique porque es o porque no es un servidor Web.
c) Que comando se podría utilizar para realizar una exploración UDP de los puertos inferiores a 1024 de cualquier host.
d) Realice un escaneo hacia la máquina Objetivo de la pregunta anterior: los puertos lógicos abiertos, la versión del sistema operativo.
e) Realice el comando para listar la cantidad de equipos que están conectados al segmento de su red virtual.

Debe entregar la primera parte de este manual este día

PARTE 2 (40%) - DÍA MARTES

1.- Desarrolle una pequeña página web donde estén los nombres de los integrantes (utilice el lenguaje que prefiera) y una base de datos (elija la que prefiera) que almacene el nombre de usuario, contraseña, correo mínimamente. Esta página deberá estar montada en un servidor local para simular un sitio web de una empresa que venda cualquier tipo de producto. Esta web se utilizará para probar y demostrar el funcionamiento de los siguientes tipos de ataques: XSS, SQLInjection.

Primeramente utilice alguna de las herramientas vistas OWASP ZAP, BURP SUITE, para encontrar vulnerabilidades.

A partir de esta información y de estar disponible trate de realizar algún ataque a esta web. (Puede usar cualquier herramienta de KALI LINUX o alguna que prefiera para este propósito)

La página será presentada en la clase y se demostrará cómo funcionan estos ataques primeramente, es decir deberá mostrar el ataque con éxito hacia la página. Luego se deberá demostrar cómo evitar estos mismos ataques en la misma web donde ya no deberá tener efecto con la medida de seguridad que aplicó.

- **1 variantes de XSS**
- **1 variantes de SQL Injection**
- **Otra variante de ataque a páginas web que ud. elija.**

Debe entregar la segunda parte de este manual este día