Trabajo Práctico N° 6.3 – Taller de Laboratorio:
"Seguridad Informática"

Objetivos: Que el alumno logre:

- Desarrollar la habilidad práctica para administrar riesgos y planificar líneas de defensa en un ambiente informático.
- Conocer y utilizar herramientas actuales para implementar líneas de defensa de acceso a recursos de SI/TI.

Referencia Temática:

- ***Unidad VI: La Administración de Recursos de SI/TI – Seguridad y Auditoría de SI***
  - Administración del Riesgo: Análisis de Riesgos, Líneas de defensa.
  - Políticas de Seguridad.

Bibliografía de Referencia:.

- ROBSON, Wendy. ***"Decisiones Estratégicas en Sistemas de Información II"***. Tomo 5. Colección Management Estratégico de Sistemas de Información. MP Ediciones. 2ª edición. 1999. Argentina.
- ***"Guía para la Elaboración de Políticas de Seguridad"***. Universidad Nacional de Colombia. 2003.
- Anexos Complementarios sobre ***Seguridad y Auditoría Informática***, provistos por la Cátedra.
- Documentación oficial de cada herramienta.

Consultas extra-áulicas: A coordinar con la Cátedra. 15' por grupo.

Fecha de Exposición PARTE 1: Miércoles 21/10/2020 (30' por grupo)

Modalidad de desarrollo: **Grupal**
- **PARTE 1: En horario extra-áulico, previo al Taller → Subir al CVG.**
- **PARTE 2: En horario extra-áulico, posterior al Taller → Subir al CVG.**

> ***NOTA: Para el desarrollo del Trabajo Práctico y a los efectos de lograr los objetivos de aprendizaje propuestos, se debe respetar el orden de las consignas.***

Consignas:

PARTE 1 → Previo al Taller

1. **Investigar y probar herramientas libres de seguridad de los tipos que se indican a continuación** (a modo de ejemplo se indican algunas herramientas**):**

   a) **Seguridad en el sistema de archivos**: Permisos sobre los dispositivos, archivos, usuarios y grupos. Análisis de logs del sistema (Syslog).
   b) **Escaneador de puertos**: Nmap.
   c) **Control de acceso a los servicios**: /etc/init.d y sus modificadores. SysV-RC-Conf.
   d) **Sistemas seguros de conexión**: SSH.
   e) **Firewalls**: IPTables.
   f) **Sistemas de detección de intrusos (IDS)**: Snort
   g) **Herramientas de backup**: tar, gz, cron.
   h) **Scripts de backup**: Flexbackup, RSync

2. **Analizar las herramientas vistas en la consigna 1, en función de los siguientes criterios:**

   i) Para qué línea de defensa sería útil su implementación?
   ii) A qué elementos del sistema ayuda a proteger?
   iii) De qué amenazas?
   iv) Elaborar conclusiones.

3. **Realizar una presentación de las herramientas asignadas a continuación, con demostración de las pruebas realizadas y el correspondiente análisis** (según pautas de la Consigna 2)**:**

TEMAS	EQUIPOS
a) **Seguridad en el sistema de archivos**: Permisos sobre los dispositivos, archivos, usuarios y grupos. Análisis de logs del sistema (Syslog).	**Equipo C**
b) **Escaneadores de puertos**: Nmap. c) **Control de acceso a los servicios**: /etc/init.d y sus modificadores. SysV-RC-Conf.	**Equipo A**
d) **Sistemas seguros de conexión**: SSH	**Equipo D**
e) **Firewalls**: IPTables. f) **Sistemas de detección de intrusos (IDS):** Snort	**Equipo E**
g) **Herramientas de backup**: tar, gz, cron. h) **Scripts de backup**: Flexbackup, RSync	**Equipo B**

PARTE 2 → Posterior al Taller, en horario extra-áulico

4. **En `/home/usuario/` crear el directorio `admrr` que contenga el archivo `admrr_tp6-3` sobre el cual deberá implementar los siguientes permisos:**

    i) Para el directorio: todos los permisos para el dueño; lectura y ejecución para el grupo y para los otros.
    ii) Para el archivo: todos los permisos para el dueño; lectura y escritura para el grupo; sólo lectura para los otros.
    iii) Si sacamos el permiso de ejecución de "los otros" en el directorio en cuestión ¿qué pasaría si un usuario que no es propietario y que no está en el grupo del directorio quisiera entrar en dicho directorio?

5. **Sabiendo que un sistema informático en entorno GNU/Linux funciona en diferentes niveles de ejecución, y suponiendo que en el "Nivel 3" necesitamos tener los servicios indicados a continuación, detallar la secuencia de pasos a seguir para configurar el sistema en cada caso, e implementar las mismas:**

    i) Servidor **ssh** habilitado y funcionando.
    ii) Servidor web **apache** deshabilitado.
    iii) Servicio **ftp** habilitado y funcionando.
    iv) Servidor de base de datos **mysql** deshabilitado.

6. **Suponiendo que se cuenta con un firewall IPTABLES, ¿cómo habilitaría cada puerto de los servicios anteriores, si la política por defecto es "DROP"?**

7. **Para cada caso indicado a continuación, describir cómo llevar a cabo las configuraciones requeridas para implementar las siguientes restricciones con la herramienta "IPTABLES":**

    i) Denegar el envío de pings desde la red interna 192.168.1.0 hacia las direcciones www.google.com.ar y www.yahoo.com.ar
    ii) Denegar el acceso al puerto 22 (ssh) desde la red interna 192.168.1.0.
    iii) Habilitar el reenvío del puerto 80 al puerto 8080 del equipo con IP 192.168.1.100.

8. **Suponga que tiene indicios para sospechar que está sufriendo una "intrusión" en sus SI:**

    i) Qué herramientas vistas en este Taller utilizaría para detectar tal intrusión? Describa cómo aplicaría cada una.
    ii) Qué controles y medidas implementaría para solucionarlo?
    iii) Qué controles y medidas implementaría para evitar que vuelva a producirse?