

sedian

Seguridad Digital
de Andalucía



Ficha técnica

Configuración segura de
servidores GNU/Linux

Curso presencial 10 horas



© 2019 Junta de Andalucía. Consejería de Economía, Conocimiento, Empresas y Universidad. Este documento y, en su caso, cualquier documento anexo al mismo, contiene información de carácter confidencial exclusivamente dirigida a su destinatario o destinatarios. Queda prohibida su divulgación, copia o distribución a terceros sin la previa autorización escrita de "Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.". Si no es Ud. el destinatario del documento le ruego lo destruya sin hacer copia digital o física, comunicando a "Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A." vía e-mail o fax la recepción del presente documento. Toda declaración de voluntad contenida deberá ser tenida por no producida.

ÍNDICE

1. Datos generales	2
2. Ponente	2
3. Calendario y lugar de celebración	3
4. Objetivos	4
5. Contenido	4
6. Material necesario.	10

1. Datos generales

Título:

Configuración segura de servidores GNU/Linux.

Modalidad:

Presencial.

Duración:

10 horas.

Dirigido a:

Responsables de seguridad TIC y profesionales TIC de la Junta de Andalucía

2. Ponente

Pedro Candel.

Actualmente en CS3 Group Security Services donde es co-fundador.

Ha sido docente en varios Máster de Seguridad en diferentes Universidades como La Salle, UCJC, UCAV, EIG, Ilumno, etc. Especializado en Seguridad Ofensiva, Reversing, Malware, Desarrollo Seguro y Forense.

Ponente habitual en congresos, conferencias, eventos y otras instituciones nacionales e internacionales en materia de ciberseguridad presentando trabajos de investigación en todo el mundo.

Ha trabajado en Deloitte CyberSOC Academy, Buguroo Offensive Security, para el Servicio de Formación y Empleo de la Junta de Comunidades de

Castilla-La Mancha y varias consultoras privadas de Telecomunicaciones y Seguridad TIC formando a cientos de grandes empresas de todo de sectores entre los que destaca el financiero, logístico, farmacéutico, TIC, etc. y formación a Fuerzas y Cuerpos de Seguridad.

También, como auditor de seguridad especializado, ha realizado auditorías de hacking ético para clientes del IBEX35, NASDAQ y todo tipo de empresas privadas.

Miembro del claustro de docentes de IMF. Business School. Andalucía, en el máster semipresencial en ciberseguridad y del claustro de docentes de IMF para el programa Servicio de Formación y Sensibilización. Confianza Digital de Sandetel.

3. Calendario y lugar de celebración

Edición Sevilla: días **25 y 26 de abril** de 2019

Instalaciones IMF Business School Sevilla. PCT Cartuja. Camino de los descubrimientos, 11. Planta baja.

Horario:

09:00 a 14:00.

Edición Granada: días **15 y 16 de mayo** de 2019

Hotel Maciá Real de la Alhambra. Calle Mirador del Genil, 2, 18008 Granada.

Horario:

09:00 a 14:00.

4. Objetivos

- Configurar de manera segura y auditar servidores bajo GNU/Linux.
- Aplicar las políticas de seguridad necesarias de forma automatizada.
- Monitorizar incidencias de seguridad de dichos servidores en tiempo real.

5. Contenido

1.- Seguridad y bastionado de GNU/Linux

1.1.- Configuración de contraseñas

1.2.- Particionado y sistema de archivos

1.3.- Configuración inicial

1.4.- Protección del sistema

1.4.1.- Protección de las particiones

1.4.2.- Configuración segura de la red

1.4.3.- Configuración segura de los parámetros del kernel

1.4.4.- Configuración de TCP-WRAPPERS

1.5.- Limitación de recursos de usuario

1.5.1.- Bloqueo de generación de volcados de memoria

1.5.2.- Límite de los recursos disponibles para cada usuario

1.5.3.- Bloqueo de uso de atajos críticos

1.5.4.- Establecimiento de uso de cuotas de disco

1.6.- Límite de acceso al sistema

1.6.1.- Control de información divulgada por el sistema

1.6.2.- Configuración segura de SSH

1.6.2.1.- Configuración general

1.6.2.2.- Configuración mediante clave pública/privada

1.6.2.3.- Criptografía de curva elíptica

1.6.3.- Módulos PAM de autenticación

1.6.4.- Límites de intento de acceso al sistema

1.6.4.1.- Fail2ban

1.6.5.- Límites de los servicios

1.6.5.1.- Protección con cortafuegos

1.6.5.2.- GUFW

1.6.5.3.- Protección antiDDoS

1.7.- Elementos innecesarios del sistema

1.7.1.- Paquetes no necesarios

1.7.2.- Usuarios innecesarios

1.8.- Permisos y variables de entorno

1.8.1.- Ficheros de configuración

1.8.2.- Directorio de usuarios

1.8.3.- Permisos en ficheros y directorios importantes.

2.- Sistema

2.1.- Actualización del sistema

2.1.1.- Online

2.1.2.- Offline

2.2.- Sistema y Servicios

2.3.- Administración de recursos

2.4.- Almacenamiento

2.5.- Sistema de archivos

2.6.- Administración y mantenimiento

2.6.1.- Automatización de tareas

2.6.2.- Logs de sistema

2.6.2.1.- Envío y centralización de logs con syslog-ng y rsyslog

2.6.3.- Control de integridad de hardware

2.6.4.- Control de dispositivos extraíbles

2.6.5.- Copias de seguridad

2.7.- Delegación de administración con sudo

2.7.1.- Configuración

2.7.2.- Auditoría

2.7.3.- Reglas

2.7.4.- Informes

2.7.5.- Integración con syslog-ng

2.8.- HIDS

2.8.1.- OSSEC

2.8.1.1.- Instalación

2.8.1.2.- Configuración

2.8.1.3.- Reglas

2.8.1.4.- Integración con Wazuh

2.9.- NIDS

2.9.1.- Snort

2.9.1.1.- Instalación

2.9.1.2.- Configuración

2.9.1.3.- Reglas

3.- Listas de comprobación de seguridad (CIS Benchmarks)

- 3.1.- CIS Distribution Independent Linux Benchmark v1.1.0
- 3.2.- CIS Debian Linux 9 Benchmark v1.0.0
- 3.3.- CIS SUSE Linux Enterprise 12 Benchmark v2.1.0
- 3.4.- CIS ISC BIND DNS Server 9.9 Benchmark v3.0.1
- 3.5.- CIS Apache Tomcat 7 Benchmark v1.1.0
- 3.6.- CIS Apache Tomcat 8 Benchmark v1.0.1
- 3.7.- CIS NGINX Benchmark v1.0.0
- 3.8.- CIS Apache HTTP Server 2.4 Benchmark v1.4.0
- 3.9.- CIS Oracle MySQL Community Server 5.7 Benchmark v1.0.0
- 3.10.- CIS PostgreSQL 10 Benchmark v1.0.0
- 3.11.- CIS MIT Kerberos 1.10 Benchmark v1.0.0
- 3.12.- CIS Security Metrics v1.1.0
- 3.13.- CIS Security Metrics – Quick Start Guide v1.0.0

4.- Distribución de secretos compartidos

- 4.1.- Shamir Shared Secret
- 4.2.- Distribución de secretos
- 4.3.- Custodios
- 4.4.- Recuperación de secretos

5.- Auditoría de comprobación del bastionado

5.1.- nmap

5.1.1.- Instalación

5.1.2.- Ejecución

5.1.3.- Modos de operación

5.1.4.- Scripts

5.2.- Lynis

5.2.1.- Instalación

5.2.2.- Auditoría

5.2.3.- Corrección de las advertencias de lynis

5.2.4.- Implementación de las sugerencias de lynis

5.2.5.- Personalización de la auditoría de lynis

5.2.6.- Interpretación del "Hardening Index"

5.3.- OpenSCAP

5.3.1.- Instalación

5.3.2.- Guías STIG (SCAP Security Guide)

5.3.3.- Consulta

5.3.4.- Ejecución de la evaluación del SSG

5.3.5.- Generación de informes

5.3.6.- Remediación automatizada con XCCDF

6.- Introducción a la automatización con Puppet.

6.1.- Instalación de un Master-Agent

6.2.- Manifest y Modules

6.3.- Foreman

6. Material necesario

Los asistentes tendrán que tener una máquina virtual con Ubuntu Server Edición 16.04 o inferior (no recomendamos la última versión 18.04 LTS por los cambios que ha sufrido en su distribución).

Ubuntu Server disponible en 64 bits:

<http://releases.ubuntu.com/16.04/ubuntu-16.04.6-server-amd64.iso>

Ubuntu Server disponible en 32 bits:

<http://releases.ubuntu.com/16.04/ubuntu-16.04.6-server-i386.iso>