MALNATI, MARCOS MIGUEL

System administrator

+54 11 5886 6751
marcos@soporte.net.ar
soporte.net.ar
Argentina, Buenos Aires, Ciudad Autónoma de Buenos Aires, Almagro

Con más de 11 años de experiencia en IT. En los últimos 6 años estuve como administrador de sistemas, enfocándome principalmente en sistemas operativos basados en GNU/LINUX, y haciendo uso de herramientas open source para distintos proyectos o implementaciones. Cuando estuve en ciberseguridad, aprendí a usar distribuciones como Kali y Parrotsec, realizando tareas de pentest y análisis de vulnerabilidades, usando herramientas como Apache Jmeter para stress test entre otras. Siempre tratando de probar nuevas herramientas y mantenerme al día con las nuevas tecnologías.

EXPERINCIA LABORAL

Responsable de seguridad informática y sysadmin

Ministerio de Modernización, Dirección de procesamiento de datos | 06/18 – actual

Mis tareas consisten en administrar las siguientes tecnologías:

- Administración de servidores GNU/LINUX basado en Red Hat 7
- Análisis de vulnerabilidades y pentesting
- Alta y renovación de certificados para sitios web
- Validación de los sistemas a través de certificado cliente (mediante haproxy)
- Creación de ambiente de pentest, stress test y análisis de vulnerabilidades
- Administración de equipos BIG-IP F5 (principalmente LTM, pero también manejo DNS)
- Manejo de ambientes en docker, y uso de portainer

Administrador de infraestructura

Subsecretaría de protección de infraestructuras críticas de información y ciberseguridad | 06/16 – 06/18

Encargado de administrar los servidores del área, los servicios y la seguridad. También implementar servicios para la red interna. Hardening de servidores, scripting básico para automatización de tareas en cron, prueba de herramientas de monitoreo de servicios. Entre las tecnologías que manejé, están las siguientes:

- Windows (2008 R2 y 2012)
- Linux (Debian 8)
- DNS (Bind)
- HAproxy
- Teampass
- VirtualBox
- Apache Server
- Nginx
- GLPI
- FOG
- Firewalls (Shorewall, pFsense)
- Squid proxy
- CUPS
- VMware vSphere 6
- Administración de servidor SAMBA
- Administración básica de switches Cisco Catalyst 2960 Plus Series
- Manejo de ambientes en docker, y uso de portainer
- Zabbix
- Pandora FMS
- Nagios

Ciberseguridad:

Además de administrar los servidores, estoy en la parte de GAP (gestión de análisis preventivo) realizando escaneo de vulnerabilidades a sitios web, pentesting, stress test a servidores web, base de datos, informes con recomendaciones para mejorar la estabilidad y seguridad de los mismos y análisis preventivos. Entre las herramientas y distribuciones que uso, se encuentran las siguientes:

- Kali Linux
- Parrotsec
- Acunetix
- Apache Jmeter
- Wireshark
- tcpdump
- Netsparker

Administrador de infraestructura

Subsecretaría de protección de infraestructuras críticas de información y ciberseguridad | 08/15 – 12/15

Luego de trabajar en el CERT como operador, pasé al área de infraestructura, y me desempeñé en la administración de los servidores y la red interna, así como también aportando en el GAP (gestión de análisis preventivo).

- Operador del CERT, carga de incidentes y reporte de vulnerabilidades a entidades privadas y públicas.
- Responsable de Soporte técnico / Infraestructura
- Encargado del mantenimiento de las estaciones de trabajo del departamento
- Troubleshooting básico sobre problemas de uso cotidiano
- Instalación de programas básicos (Windows 10, Office 2013)

Soporte técnico

Universidad Torcuato Di Tella | 06/12 – 07/15

- Manejo del servidor de impresiones bajo plataforma Windows Server 2008
- Pcounter (contador de impresiones)
- Consola de AD (creación de usuarios, reseteo de contraseña, permisos sobre carpetas)
- Consola de administración de Google, creación de casillas, listas de distribución, calendarios, Google Drive
- Instalación de programas básicos (Windows 10, Office 2013)
- Atención a usuarios, tanto telefónicamente como on site
- Administración de impresoras

Soporte técnico

Exolgan S. A | 05/09 – 03/12

Mis responsabilidades principales eran atención a usuarios finales y resolución de incidentes de manera remota o presencial. Entre mis tareas se encontraban las siguientes:

- Manejo básico de consola Linux
- Armado, reparación y mantenimiento de PC a medida
- Redes de datos y telefonía, reparación
- Configuración y mantenimiento impresoras
- Administración de Active Directory de Windows Server 2003 / 2008 R2
- Manejo de consola de Antivirus McAfee Orchestrator, manejo de Consola Trend Micro Appliance
- Instalación y configuración de ACU Manager y Digicard Sistemas, instalación y configuración de biométricos NEC AcuSmart
- Instalación y mantenimientos de sistema CCTV Bosch, instalación de Boch Vidos Lite Client, Achive Player
- Manejo de Herramientas Microsoft Office, StarOffice y OpenOffice
- Configuración de Psion Teklogix 7535G2, 8525G2 y WorkAbout PRO
- Sistema informático MARIA AFIP, MPX System, Aranda Service Desk

Soporte técnico telefónico a productos Linksys

Next S. A | 06/07 – 12/09

- Cableado de redes
- Configuración de Routers Linksys
- Instalación de adaptadores cableados y wireless para PCs
- Administración remota, Access Restrictions, Print Servers
- Access Point, Cámaras IP
- Bridge inalámbricos, repetidores Wi-Fi, VPN (IPSec), VoIP (SIP)

PROYECTOS

Soluciones informáticas

Soporte técnico a pymes y particulares

Creé ésta empresa para brindar servicios a particulares y pymes. Éstos van desde arreglos de computadoras de escritorio, hasta hacer una evaluación de vulnerabilidades, escaneos de vulnerabilidades, y brindar seguimiento en el proceso de mejora contínua.

ESTUDIOS

(RHCSA) (EX200)
Actualmente realizando el curso de Red Hat System Administrator, para Red Hat Certified System Administrator

Teoría y práctica de la investigación del cibercrimen
Organizado por la Dirección General de Capacitación y Escuela del Ministerio Público Fiscal de la Nación durante mayo de 2017

Facultad de Ingeniería del Ejército – Grl Div Manuel N. Savio
Formación en Ciberdefensa, dictado por el Dr. Alejandro Corletti (04/09/2017 a 08/09/2017)

National Nuclear Security Administration
Gestión de Riesgos Cibernéticos en la Seguridad Nuclear Internacional dictado por personal de la NNSA (19/03/2018 a 24/03/2018)

INAP
Administración GNU/Linux I y II (03/2018 a 06/2018)

Escuela educación técnica N°2
Técnico electrónico, Producción de bienes y servicios (2002)

HABILIDADES

Técnicas

GNU/Linux
SAMBA
Apache Server
Apache Jmeter
Scripting bash
HAproxy
tcpdump
Kali Linux
Parrotsec
Acunetix
Docker

Profesional

Trabajo en equipo
Proactivo
Capacidad de comunicación
Capacidad de Análisis e investigación

IDIOMAS

Español (Nativo)
Inglés (intermedio)
Italiano (en curso)