Malnati Marcos Miguel

**Objetivo**

Lograr desempeñarme en el área de IT y seguridad informática, aplicando mis conocimientos, y a su vez poder adquirir mayor experiencia en tareas relacionadas a la administración de la infraestructura y la seguridad de servidores, políticas de seguridad y herramientas libres.

**Experiencia**

06/18 – actual **MINISTERIO DE MODERNIZACIÓN, DIRECCION DE PROCESAMIENTO DE DATOS (GDE)**

*Responsable de seguridad informática/sysadmin*

* Administración de servidores basado en Red Hat
* Análisis de vulnerabilidades y pentesting
* Alta y renovación de certificados
* 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

Referencia:

Director, Diego Fumero.

Teléfono de contacto: 15-7099-8540

06/16 – 06/18 **MINISTERIO DE MODERNIZACIÓN, SUBSECRETARÍA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD**

*Administrador de infraestructura*

Estoy 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.

* Windows (2008 R2 y 2012)
* Linux (Debian)
* 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
* 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 (conjunto de herramientas para pentest, escaneo de vulnerabilidades, etc, basado en Debian)
* Parrotsec (similar a Kali Linux, pero con algunas otras herramientas. También basado en Debian)
* Acunetix (software escáner de vulnerabilidades)
* Apache Jmeter (stress test)
* Wireshark (analizador de protocolos y tráfico)
* tcpdump
* Netsparker (escáner de seguridad de aplicaciones web)

**Cursos**

* 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.
* Formación en Ciberdefensa dictado en la Escuela Superior Técnica - Facultad de Ingeniería del Ejército, Universidad de la Defensa. Dictado por el Dr. Alejandro Corletti (04/09/2017 a 08/09/2017)
* Gestión de Riesgos Cibernéticos en la Seguridad Nuclear Internacional dictado por personal de la NNSA (National Nuclear Security Administration) (19/03/2018 a 24/03/2018)
* Administración GNU/Linux I y II en INAP

08/15 – 12/15 **JEFATURA DE GABINETE DE MINISTROS, SUBSECRETARÍA DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN Y CIBERSEGURIDAD**

*Administrador de infraestructura*

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

Luego de trabajar en el CERT, 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).

06/12 – 07/15 **UNIVERSIDAD TORCUATO DI TELLA**

*Soporte técnico*

* 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
* Atención a usuarios, tanto telefónicamente como on site
* Administración de impresoras
* Conocimientos básicos en sistemas Bejerman y SIGEDU

05/09 – 03/12 **EXOLGAN S. A**

*Soporte técnico/Admin Wintel Jr*

* 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
* Instalación, configuración de sistemas: Acronis Enterprise Server, Oracle Developer 6i y Database 9i, Navis Express Terminal Operating System, Navis Sparcs Terminal
* Operating System, Navis Condor Express y Condor Works, Baplie Viewer Ship Editor
* Sistema informático MARIA AFIP, MPX System, Aranda Service Desk

06/07 – 12/09 **NEXT S. A**

*Soporte técnico telefónico de productos Linksys*

* Cableado de redes
* Configuración de Router 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)

*Estudios*

2002 **ESCUELA EDUCACIÓN TÉCNICA N°2**

*Técnico electrónico, Producción de bienes y servicios*

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