TEMARIO

PFSENSE

DURACIÓN DEL CURSO

40 HRS

Informes: Telf. (01) 640-5805 | Av. Arenales N° 1912 Of. 805 - Lince

AULATEC

FORMACIÓN Y DESARROLLO PROFESIONAL EN T.I.

CAPÍTULO 1 : FIREWALL PFSENSE OPENSOURCE

- Introducción a PfSense
- Instalación y puesta a punto de PfSense
- Requisitos de hardware
- Funcionamiento y manejo de PfSense
- Configuración básica de PfSense
- Configuración de firewall
    - Administración vía web
    - Configuración de interfaces LAN, WAN, VLAN
    - Filtro de paquetes
    - Redirección de puertos
    - Reglas de bloqueo, rechazo y aceptación
    - NAT / PAT
    - Configuración de DMZ
- Servicios básicos incluidos
    - DHCP
    - DNS
    - SNMP
    - Portal Captivo
- Carga de extensiones adicionales
- Balanceo de carga MultiWAN
- Delimitar el ancho de banda en las descargas traffic-shapper
- Gráfica de consumo de internet (entradas y salidas)
- Servidor proxy manual y transparente: Squid
    - Bloqueo por categorías de páginas web: Squidguard
- Clientes Road Warrior
- Servidores
    - OpenVPN
    - IPSEC
    - PPTP
    - L2TP

CAPÍTULO 2 : MOD SECURITY

- Conceptos de servicios y aplicaciones Web
- Módulos de seguridad en Apache
    - Mod_security y Mod_evasive
- Módulo de mod_security
- Características
- Funcionamiento
- Instalación y configuración básica
- Descarga y configuración de reglas
- Prueba funcional

CAPÍTULO 3 : HACKING ETICO

- Introducción al Hacking ético
- Reconocimiento y descubrimiento de servicios
- Google Hacking e Interrogación DNS
- Comandos de búsqueda y recopilación de información
- Escaneo de red redes y enumeración de servicios con NMAP
- Hacking sobre sistemas operativos
- Ataques de password cracking a servicios
- Creación de diccionarios personalizados
- Cracking de contraseñas en Linux
- Metasploit para explotación de vulnerabilidades a sistemas Windows y Linux
- Análisis de vulnerabilidades con Nessus a nivel de Plataforma y aplicaciones.
- Interpretación de reportes de Nessus y búsqueda de vectores
- Hacking sobre aplicaciones Web
- Introducción a vulnerabilidades web
- Ataques a servidores Web con SQL Inyección manual
- Desarrollando e identificando XSS reflejado y almacenado
- Explotando XSS para robo de sesiones en aplicaciones web
- Ataques de Local File Inclusion (LFI) y Remote File Inclusion (RFI)
- Desarrollando ataques Cross Site Request Forgery – XSRF
- Generando shell reverso vía formularios de UPLOAD vulnerables