Syllabus del Curso de Curso de Sophos Firewall XG 18 con redes virtuales GNS3, Active Directory y Servidores Linux

Introducción
– Introducción a los firewalls.
– Firewalls de red, UTM y NG
– Firewall SophosXG, historia
– Ciclo de Vida de las versiones de SophosXG
– Funcionalidades de SophosXG
– Escenarios de Despliegue

Instalación de Xubuntu 20.04 y GNS3
– Configuración del sistema operativo.
– Configuración de IP Pública
– Configuración de red virtual en netplan
– Acceso remoto rdp
– Instalación de GNS3
– Creación del router virtual

Instalación de Firewall Sophos XG 18
– Creación del router virtual
– Diseño de la red, segmentos de WAN, LAN, DMZ
– Creación de switches en GNS3
– Creación de la máquina virtual SophosXG con Qemu KVM
– Instalación de Sophos XG Home
– Registro de Sophos ID y Key de Sophos XG
– Configuración de la red LAN y WAN
– Configuración de la IP pública
– Configuración de la licencia y sincronización
– Configuración de la DMZ

Instalación del Sistema Operativo de Servidor CentOS 7
– Determinación de requerimientos de hardware

– Estrategia de particionamiento.
– Configuración de Niveles Raid
– Configuración de LVM
– Instalación de CentOS 7
– Configuración de red, Ubicación del Servidor en DMZ

Servidor SSH

– Cliente SSH
– Servidor SSH
– Compartición de Clave compartida en SSH con el VPS

Configuración de Reglas y Políticas de Firewall, NAT

– Reglas de Firewall
– Reglas NAT (SNAT, DNAT y PAT)
– Reglas reflexivas
– NAT de múltiples puertos y servicios
– Gestión de Objetos de Red
– Scheduling

Servidor de Directorio Activo con Windows 2012r2

– Introducción al directorio activo
– Instalación de máquina virtual Windows 2012r2
– Definición del Dominio Windows
– Configuración Inicial del Bosque
– Creación de Unidades Organizativas, Usuarios y Grupos
– Prueba de estaciones windows
– Políticas de grupo (GPO)

Filtrado Web y Filtrado de Aplicaciones, Inspección SSL, Intercepcción SSL.

– Capa de Identidad Layer 8
– Integración de Sophos XG a Active Directory
– Configuración de STAS
– Filtrado Web e Inspección SSL
– Despliegue de certificado SSL por medio de GPO
– Políticas de Filtrado Web para usuarios y grupos de ADS
– Intercepción SSL.
– Filtrado de Aplicaciones
– Reportes y monitores en tiempo real

CentOS 7; Virtualización de servidores con KVM y virt-manager

– Teoría de la virtualización
– Virtualización con KVM y Virtmanager
– Creación de máquina virtual en KVM
– Instalación de máquinas virtuales CentOS 7 y Ubuntu Server LTS
– Configuración de las redes virtuales en modo Nat y Bridge
– Configuración de red y hostname de las máquinas virtuales

Configuración de VPN Móvil y Site2Site (SSL e IPSec)

– Instalación de Sophos XG en una sucursal con Ip dinámica
– VPN SSL
– VPN IpSec
– Configuración de VPN Móvil en Linux y Windows
– Pruebas de Conexión

Configuración de Switch Cisco con VLANs, trunking con SophosXG

– Instalación en GNS3 de Switch Core Cisco con soporte de VLANs
– Reconfiguración de las redes LAN,
– Creación de VLANs para servidores y PCs
– Configuración de Trunk y VLANs con SophosXg y Switch core
– Reconsfiguración de STAS
– Pruebas de capa de identidad, filtrado Web y de Aplicaciones

Configuración de DNS Público y Certificados Letsencrypt

– Resolución de nombres local y en red
– Registro de Dominio Público
– Configuración de DNS Público, registros de DNS en Freenom
– Zonas de Dominio y Registros MX, PTR y SPF
– Certificados Letsencrypt
– Generación de certificado para dominio único y múltiples dominios
– Configuración de certificados Letsencrypt para Sophos XG

Configuración del Servidor Web Apache y Base de Datos

– Acceso al VPS
– Servidor Web con Apache
– Configuración básica
– Configuración de dominios virtuales en Apache
– Configuración de HTTPS
– Configuración de MySQL, permisos, creación y respaldo de base de datos
– Instalación de Certificado Letsencrypt en el VPS

– Instalación de WordPress CMS

Protección de servidor con IPS, DDOS y WAF

– Políticas de IPS
– Protección DOS y DDOS
– Configuración de servidores Web
– Protección WAF para http
– Carga de certificados digitales de dominios https
– Protección WAF para https
– Formulario de autenticación para sitios inseguros

Configuración del Servidor de Correo Zimbra

– Requisitos previos
– Configuración del DNS Bind público y host para Zimbra
– Instalación de Zimbra 8.7.11
– Upgrade de Zimbra
– Publicación de Zimbra con la Ip pública
– Zimbra Webmail.
– Panel de administración.

Instalación de Gateway AntiSpam

– Habilitación de Gateway AntiSpam
– Antispam en modo bridge
– Listas Blancas y Negras
– Políticas de filtrado
– Antispam en modo Gateway
– Cuarentena
– Revisión de Logs

Configuración de WAN Failover

– Configuración de Interfaz de Red Adicional
– Configuración de Ip pública
– Configuración de WAN Failover
– Pruebas Funcionales

Seguridad Inalámbrica y HotSpot

– Configuración de WIFI público
– Configuración de portal cautivo
– Filtrado Web, App y Traffic Shaping del WIFI público

– Creación de cupones de hotspot