TP ESPECIAL

Objetivo

El objetivo del TP Especial es que cada grupo implemente un sistema de red específico y muestre su funcionamiento en el laboratorio frente al resto de los alumnos junto con una exposición oral del tema tratado.

Temas

Cada grupo deberá elegir e implementar solo uno de los TP siguientes, sin poder repetir el tema entre grupos.

Puntos a desarrollar

Cada grupo deberá implementar, demostrar y explicar, sin excepción, cada uno de los puntos que se especifican a continuación dentro del tema que haya elegido o le haya sido designado por la cátedra.

Tema 1 - Streaming

a) Configurar un servidor de streaming de Audio y Video.
b) Pruebas con al menos dos fuentes simultáneas en vivo y diferidas.
c) Informar cantidad de clientes conectados y consumo de ancho de banda individual y total.
d) Explicación de codecs utilizados y utilización de ancho de banda de cada uno.
e) Mostrar protocolos utilizados (ej: RTP y RTSP)

Tema 2 – WAF (Web Aplication Firewall)

a) Configurar un servidor con HAProxy que funcione como proxy reverso para recibir las peticiones para al menos 2 servidores con web server.
b) Configurar un servidor con ModSecurity que reciba las redirecciones del HAProxy y chequee la seguridad de las mismas
c) Configurar diferentes reglas de waf para al menos dos servidores web.
d) Probar al menos 3 ataques para mostrar la respuesta del waf, configurar un página default de respuesta ante detección de anomalía.

Tema 3 – Metasploit Framework

a) Una PC con Windows con aplicaciones y servicios instalados
b) Metasploit en PC con Linux.
c) Mostrar al menos 4 exploits diferentes en aplicaciones y sistemas operativos.
d) Mostrar diferentes módulos y niveles de acceso logrados.

TP ESPECIAL

Tema 4 - OpenVas

a) Instalación y Configuración.
b) Mostrar scaneo remoto con o sin login.
c) Mostrar el indicador de cambios en base a los ultimos escaneos.
d) Mostrar detección de parches no aplicados y aplicar solución.
e) Mostrar detección de servicios en puerto no conocidos (ej SSH en port 2222)
f) Mostrar escaneos previos para no demorar la presentación.

Tema 5 – OpenStack

a) Crear una nube con OpenSatck con al menos 3 nodos (servidores fisicos) diferentes. De los cuales uno será exclusivamente “Compute Node” y otro “Storage Node”
b) Mostrar la creación, copia, modificación y eliminación de “Proyectos”, “Instancias”, “Servicios” y “Sabores”. Explicar la relación y configuración de cada uno de ellos.
c) Configurar diferentes perfiles de usuarios y mostrar la asignación de cuotas.
d) Crear una aplicación clásica de sitio web con base de datos.

Tema 6 – Zabbix (Sistema de monitoreo y alertas)

a) Crear una red virtual o real a monitorear de al menos 4 hosts.
b) Configurar el monitoreo de al menos dos características de hardware de un servidor.
c) Configurar el monitoreo de un servicio web, usando pasos secuenciales dentro de la navegación de sitio.
d) Configurar alertas por tiempos de respuestas en un sitio web.
e) Configurar monitoreo de al menos 2 servicios (SMTP, POP3,etc)
f) Configurar alarmas con distintos niveles según el tiempo de caída de servicio a distintos administradores u operadores.

Tema 7 – OPNSense (Router y firewall)

a) Se deben crear dos escenarios, uno en modo transparente (bridge) y otro en modo gateway.
b) Crear y aplicar políticas de QoS de al menos 3 servicios(ej. http, ftp, p2p)
c) Crear y aplicar políticas por aplicación, skype, emule, msn.
d) Crear y aplicar políticas por tipo de tráfico, streaming, chat.

e) Configurar ancho de banda máximo y garantizado. Saturación del enlace para las pruebas.

Tema 8: OpenVPN

- Se deben crear tres tipos de VPN (Cliente-Sitio, Sitio-a-Sitio, Multisitio)
- Para la conexión Cliente-Sitio
  - El cliente debe pasar a través de un equipo que realiza NAT.
  - El cliente debe obtener una IP por DHCP de la red interna del sitio.
  - Probar la conexión directa por NAT y a través de un web Proxy
- Para la conexión Sitio-Sitio
  - Ambos equipos deben tener conectarse mediante direcciones “públicas” e interconectar sus redes internas. Los host de ambas redes deben tener distancia de un salto entre ellos.
  - Para la conexión multisitio debe interconectar al menos 3 sitios por VPN, los cuales deberán cumplir la topología "full mesh", es decir, que desde cualquier equipo de la red se puede llegar a cualquier otro equipo.

Tema 9: ELK

- Implementar ElasticSearch, Logstash y Kibana en un servidor para generar alertas y métricas al recibir información de servidores.
- Usar como pruebas al menos 4 tipos servidores diferentes que contengan: Servidor Linux, Servidor Windows, servidor web, servidor de base de datos.
- Mostrar las ventajas y desventajas de la utilización o no de agente en los servidores que envían información.
- Recolectar información de tipo “Events” de Windows, syslog de Linux con y sin agente.
- Mostrar al menos las siguientes alertas:
  - Un usuario hace login desde una dirección IP no habitual.
  - Un servicio se encuentra caído o no responde hace x segundos.
  - Evento de firewall generado por un ataque.
- Mostrar al menos 3 reportes de kibana con estadísticas de una semana de actividad.

Tema 10 – Serverless

- Utilizar un servicio Serveless (Amazon Lambda, Azure Functions o Google Cloud Functions) para que al insertar una imagen a un contenedor (S3, Azure Storage o Google Cloud Storage), se genere la imagen en un tamaño diferente.
- Hacer un script que suba muchas imágenes simultáneamente al contenedor, y mostrar cómo se generan las imágenes redimensionadas.
- Mostrar el gráfico de CloudWatch (o similar) cuando se hacer el redimensionamiento de las imágenes.
- Explicar cómo escala el sistema anterior.

TP ESPECIAL

- Explicar cómo funciona y las ventajas de usar un servicio Serverless frente a un servidor común.
- Hacer otro caso que muestre de forma simple el funcionamiento de Serverless.

Consideraciones especiales

- El tipo de diseño y la forma de implementación serán discutidos entre el grupo y la cátedra durante las clases de laboratorio o teóricas, dejando la posibilidad de modificar éste enunciado escrito, previo acuerdo entre el docente y los integrantes del grupo.
- Para la evaluación se tendrá en cuenta no sólo la implementación sino también la exposición oral y el documento para repetir la implementación (how-to)
- Todos los integrantes del grupo debe estar presenten en la presentación y ser oradores.
- Cualquier aclaración oral a cargo de la cátedra con respecto al enunciado del TP tiene la misma validez que el enunciado escrito.

Material a entregar

Cada grupo deberá enviar por mail a la dirección de correo redes-catedra@googlegroups.com el día de la entrega:

- Presentación PPT que se utilizará en la exposición
- Documento explicativo (how-to) de cómo se realiza la implementación.

Fechas de entrega, demostración y exposición oral

- El plazo máximo de entrega del TP es el **7 de junio a las 14:00hs** vía correo electrónico.
- Las presentaciones se realizarán los días 7 y 14 de Junio en el laboratorio de Informática, según orden aleatorio.