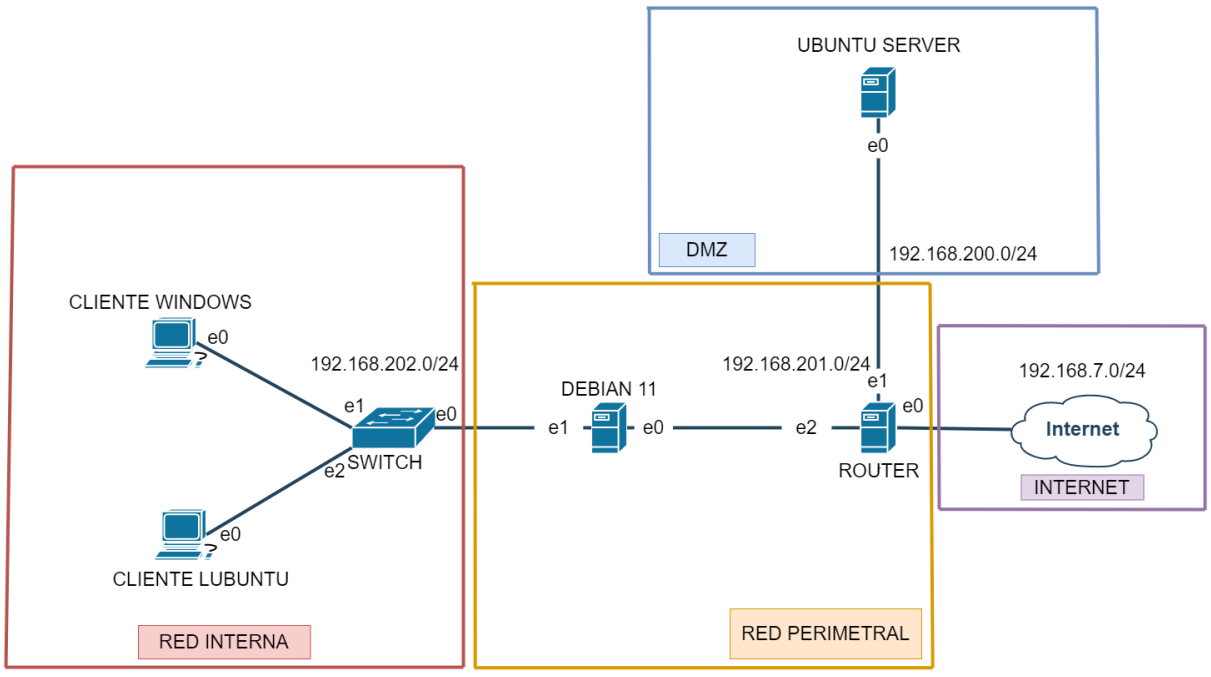
DOCUMENTACIÓN INICIAL

AUTORES

- José María Viúdez Parra
- José Antonio Cervantes Fernández
- Jorge Luis Pérez Martínez
- Karim El Bissari Dakdaki

OBJETIVOS

El proyecto planteado por los miembros del grupo estará formado por un escenario inventado de una empresa ficticia donde se pondrá en práctica los diferentes conceptos de seguridad:



En principio, se tendrán en cuenta las siguientes pautas de seguridad informática:

1. Crear la red interna de la empresa, con su respectiva red perimetral y su zona desmilitarizada. Asimismo, indicaremos el tipo de arquitectura que utilizará dicha empresa.
2. Realizar copias de seguridad de un equipo de la red DMZ en un equipo cliente en determinado momento.
3. Desarrollar scripts de python para llevar a cabo la criptografía y/o detectar las vulnerabilidades de nuestro router.

En segundo lugar, implementaremos una serie de mecanismos de seguridad activa:

4. Evitar que otros usuarios puedan instalar cualquier tipo de aplicación en su equipo.
5. Respecto al router, todavía no sabemos qué software utilizar.
6. Instalar una herramienta de monitorización de la red en la zona DMZ de la empresa.

En tercer lugar, implementaremos técnicas de acceso remoto:

7. Instalar y configurar un servidor de acceso VPN.
8. Instalar y configurar un servidor de autenticación.
9. Comprobar que un usuario situado en el equipo remoto puede acceder a la red empresarial.

Hecho esto, procederemos con la instalación y configuración de cortafuegos.

10. No permitir a los usuarios situados en un equipo de la red DMZ acceder a la zona interna de la red ni a Internet.
11. Permitir a los usuarios situados en un equipo no acceder a Internet y permitir a los usuarios situados en otro equipo sólo realizar http en Internet.
12. No permitir el protocolo ICMP en varios equipos de la red interna (utiliza su cortafuegos personal).

Finalmente, instalaremos y configuraremos los servidores proxy:

13. Permitir en el servidor proxy navegar en Internet sólo un período de tiempo, si estamos autenticados en dicho servidor. Si todo va bien, crearemos una auditoría del uso del servidor y monitorizamos su actividad.

Por otro lado, el proyecto lo desarrollaremos con un software de control de versiones muy conocido, llamado Git:

14. Además, utilizaremos un modelo alternativo de creación de ramas, denominado Gitflow. Asimismo, lo alojaremos con GitHub utilizando Git o bien SourceTree. Este último nos simplifica la forma en que interactúa con sus repositorios de Git.

    A continuación, se muestran los pasos a seguir para crear el entorno de trabajo:

    a. Creamos una carpeta llamada proyectoSeguridad_Grupo3.
    b. Estando dentro de la carpeta creada ejecutamos el comando que se muestra a continuación, dejando la configuración por defecto:

    `$ git flow init`

    c. Enlazamos nuestro repositorio local con un repositorio vacío que nos creamos en GitHub con el mismo nombre:

    `$ git remote add origin`
    https://github.com/JMViiUDEZz/proyectoSeguridad_Grupo3
    `$ git push -u origin master`
    `$ git push -u origin develop`

    d. En Settings > Access, añadimos como colaboradores a mis compañeros.

Tener en cuenta que todos estos temas a tratar podrán cambiarse o modificarse en función del desarrollo del mismo.

TAREAS

Cada uno de los integrantes del grupo ha escogido una máquina para llevar a cabo su configuración. No obstante, la máquina Debian que actúa principalmente como cortafuegos será realizada por dos de ellos. Por lo tanto, la planificación de tareas queda de esta manera:

- **Clientes Windows y Lubuntu:** Jorge Luis Pérez Martínez
- **Servidor Debian:** José María Viúdez Parra
- **Servidor IPFire:** José Antonio Cervantes Fernández
- **Servidor Ubuntu Server:** Karim El Bissari Dakdaki

En primer lugar, se creará una rama feature por cada funcionalidad que partirá de la develop lógicamente.