UNIVERSIDAD UTE

FACULTAD DE CIENCIAS DE LA INGENIERÍA

CARRERA DE INGENIERÍA INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN

EXAMEN DE SUFICIENCIA DE SEGURIDAD DE REDES

NOVIEMBRE 2020

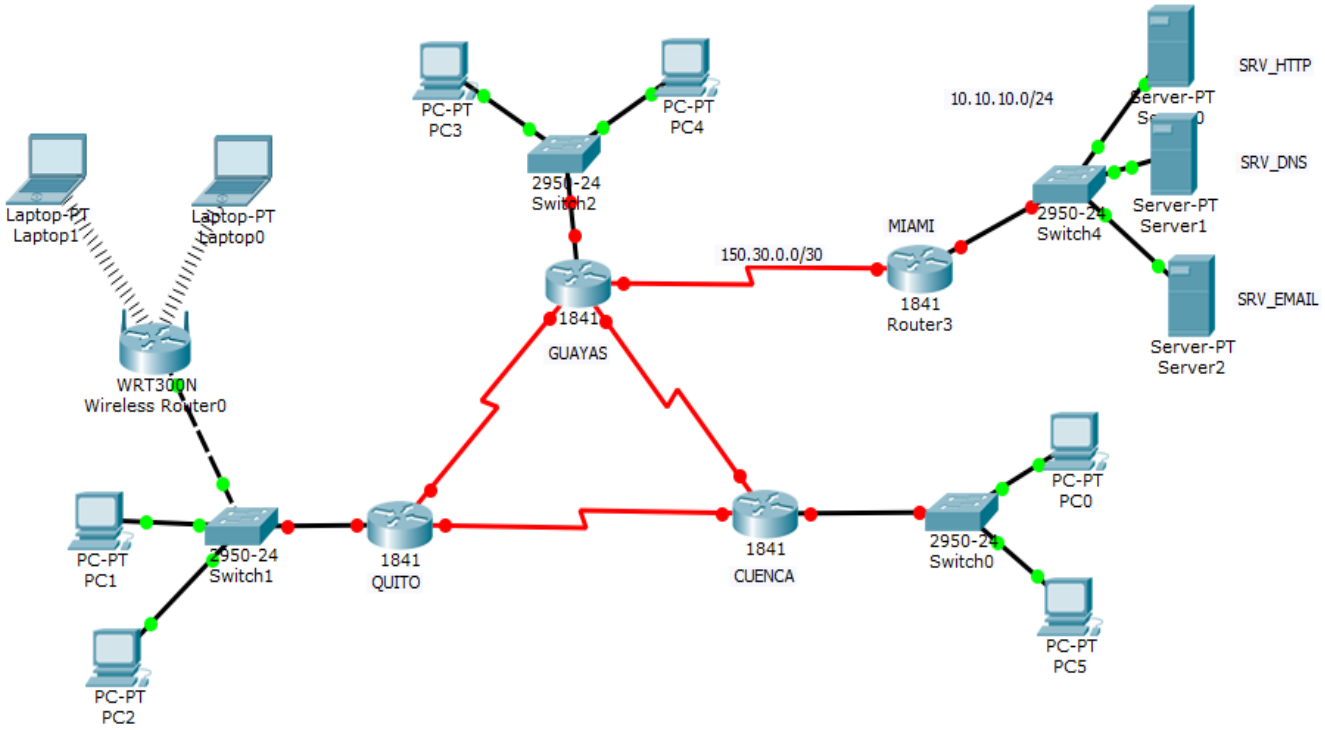
QUITO –ECUADOR

CASO PRÁCTICO

La red de la empresa **CONSULTAR**, cuya topología de red se indica en la figura, ha sufrido ataques de DoS, DNS Spoofing y otros. El gerente de sistemas de la empresa ha contratado los servicios de un especialista en seguridad de redes para que realice un análisis de las vulnerabilidades existentes en la red y realice el rediseño de esta, de manera que se garantice la confidencialidad, integridad y disponibilidad de la información de la empresa. La empresa maneja la IP privada clase C: 192.168.10.0/24 y tiene asignado el 50 como número de sistema autónomo.

El rediseño de la red de la empresa a nivel nacional, contempla:

1. Diseñar el esquema de direccionamiento IP de la red, a través de la división de la IP: 192.168.10.0 /24 en varias subredes, una por cada red LAN y una para todos los enlaces WAN de la red, a través de VLSM.
2. Configurar la red WAN de la empresa utilizando el protocolo de enrutamiento EIGRP.
3. Por estrategia de seguridad, el gerente de sistemas ha acordado contratar los servicios de hosting con la empresa TELNET ubicada en la ciudad de MIAMI, a través de una ruta estática desde el Router de Guayas, para lo cual se utilizará la IP pública 150.30.0.0/30. Aquí se alojarán los servidores de DNS, HTTP y CORREO, los mismos que serán configurados con la IP: 10.10.10.0/24.
4. Configurar en cada dispositivo de borde las contraseñas cifradas para el acceso: modo usuario (consola), modo privilegiado (administrador) y acceso remoto seguro SSH, utilizando claves de longitud de 10.
5. El informe de auditoría de los ataques indica que el Servidor de EMAIL recibe pings de diversas direcciones IPv4 en un ataque por denegación de servicio distribuido (DDoS), por lo que se debe minimizar este tipo de ataque a través de una ACL.
6. El informe también indica que un usuario móvil de la red inalámbrica de Quito actualiza repetidamente su página web, lo que ocasiona ataques por denegación de servicio (DoS) contra el Servidor WEB, por lo que es necesario también bloquear este tipo de ataques.
7. Configurar seguridad a nivel de puertos en los Switch de las sucursales de modo que permita solo un usuario por puerto para prevenir ataques de ARP Spoofing.
8. Configurar la seguridad en la red inalámbrica de la sucursal de Quito con WPA y sin broadcast de SSID
9. Todos los usuarios podrán accesar al portal de la empresa con la URL www.consultar.com, así como manejar correo internos entre los usuarios.
10. Probar toda la conectividad de la red.



Bolivar Jácome C
Docente