Nombre: Ricardo Alejandro Gómez Pérez

Maestro: Ing. Eduardo Genner Escalante Cruz

Materia: Redes III

Cuatrimestre: 7-.

VPN

Una VPN (Virtual Private Network) es una tecnología de red que se utiliza Para conectar una o más computadoras a una red privada utilizando internet.

protocolos

IPsec: permite mejorar la seguridad a través de algoritmos de cifrado robustos y un sistema de autentificación más exhaustivo.

PPTP/MPPE: tecnología desarrolladora por un consorcio formado por varias empresas PPTP soporta varios protocolos VPN con cifrado de 40 bit y 128 bit.

L2/Ipsec: tecnología capaz de proveer El nivel de protección de Ipsec sobre el Protocolo de túnel L2TP

Firewall

Es la parte de un sistema informático
O una red informática que está diseñada
para bloquear el acceso no
Autorizado, permitiendo al mismo tiempo
Comunicaciones autorizadas.

Los corta fuegos pueden ser implementados
En hardware o software, o en una combinación
De ambos

Los corta fuegos se utilizan con frecuencia para
Evitar que los usuarios de internet no autorizados tengan
Acceso a redes conectadas privadas, especialmente
intranets.

También es frecuente conectar el corta fuegos a una
Tercera red, llamada **zona desmilitarizada** o DMZ
En la que se ubican los servidores de la organización
Que deben permanecer accesibles desde la red
Exterior.

THOR (sigla de The Onion Router

El enrutador cebolla, proyecto cuyo objetivo
principales el desarrollo de una red de
Comunicaciones distribuidas de baja latencia
Y superpuesta sobre internet

el encaminamiento de los mensajes intercambiados
Entre los usuarios no revela su identidad es decir su
Dirección IP.

Para la consecución de estos objetivos se a desarrollado
Un software libre específico

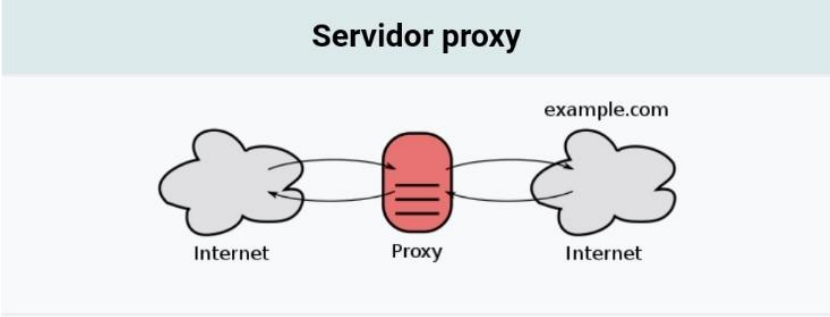
Tor propone el uso de almacenamiento de cebolla de
Forma que los mensajes viajen desde el origen al
Destino a través de una serie de routers especiales
Llamados “routers de cebolla”, (onion routers)

Proxy

Un proxy o un servidor proxy en una red de informática es Un servidor, programa o dispositivo

Ejemplo: si una hipotética maquina **A** solicita un recurso a **C** Lo hará mediante una petición a **B** que a su vez trasladará La petición a **C;** de esta forma **C** no sabrá que la petición Procedió originalmente de **A**.

Esta situación estratégica de punto intermedio le permite Ofrecer diversas funcionalidades: control de acceso, registro de tráfico, restricción a determinados tipos de tráfico, mejora de rendimiento, anonimato de la comunicación, cache web etc.



El proxy puede ser considerada por los usuarios, administradores o Proveedores como legitima o delictiva y su uso es frecuentemente Discutido.

SSL

(secure sockets layer)

Que datos protege el Protocolo **SSL**

Protocolo criptográfico para comunicaciones

Que proporcionan comunicaciones Seguras por una red

Comúnmente internet.

Star sailors leage, circuito de navegación a Vela profesional

SSL, empresa estadounidense fabricante de Satélites

> Información de registro, nombre, dirección, correo electrónico

> datos de identificación dirección, correo electrónico y contraseña

> datos de pago, número de tarjeta de crédito, cuenta bancaria

> formularios de inscripción

> documentos cargados por los clientes

El certificado garantiza que la comunicación no se podrá leer ni Manipular y que la información personal no caerá en las manos Equivocadas.

HTTPS

Acrónimo de hypertext transfer protocol (protocolo de transferencia De hipertexto)

HTTPS, es igual, pero añadiéndole “seguro”
Estos dos se usan para lo mismo, la transferencia de datos.

Si los datos son transferidos mediante HTTP, estos viajan en claro y Son accesibles para cualquier que intercepte la comunicación.

El protocolo HTTPS usan una conexión segura mediante un cifrado SSL y por tanto los datos viajan de un modo seguro de un Lugar a otro.

los datos enviados usando HTTPS están asegurados por el Protocolo TLS (Transport Layer Security) que ofrecen 3 capas De protección fundamentales:
>cifrado
>integridad de los datos
>autenticación

Robo de Identidad

Es la apropiación de la identidad de una persona: hacerse pasar esa persona

El caso más común hoy en día se da cuando un atacante Por medios informáticos o personales, obtienen su información Personal y la utilizan ilegalmente.

El robo de identidad es el delito de más rápido crecimiento En el mundo.

En este transcurso de pocas horas, esta información a veces Se divulga al hacer transacciones en persona, por teléfono Y en línea, al efectuar la compra de productos y servicios.

nadie esta a salvo de este delito ni puede tenerse la corteza de que nunca le ocurrirá.

Lo importante es conocer los métodos existentes para reducir Las probabilidades de que esto ocurra, y saber las medidas a Tomar en caso de que si ocurra.

Ataques de Denegación de Servicios

es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea Inaccesible a los usuarios Legítimos.

Los ataques DoS se generan mediante la saturación de Los puertos con múltiples flujos de información, haciendo Que el servidor se sobre cargue y no pueda seguir Prestando su servicio.

Esta técnica es usada por los *crackers* o piratas Informáticos para dejar fuera de servicio servidores Objetivo.

una ampliación del ataque DoS es llamado ataque de denegación de servicio distribuido, también llamado DDoS el cual se lleva a cabo generando un gran flujo De información desde varios puntos de conexión hacia Un mismo punto de destino.

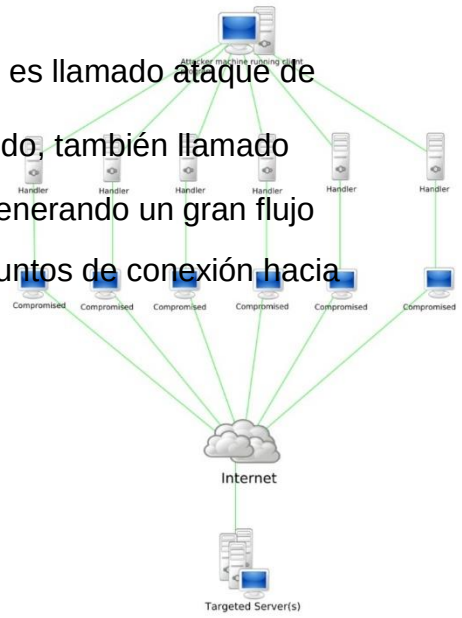


Diagrama de un ataque DDoS usando el software Stacheldraht