CYBERNOVA

CIBERSEGURIDAD

Tecnicas de evasion
Tunelizacion

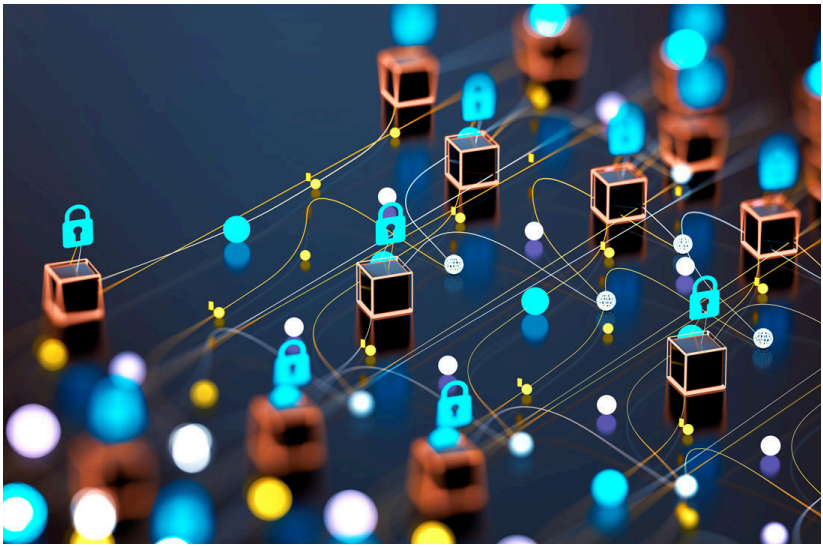
Ing. Marvin G. Soto

CYBERNOVA
CIBERSEGURIDAD

Tabla de Contenidos

INTRODUCCION

Tunelizacion



Otro método de evacion es la creación de túneles. Al encapsular el tráfico dentro de protocolos legítimos, podemos ocultar nuestras actividades y evadir la inspección, ofuscando el tráfico dentro de esos protocolos legítimos que las tecnologías de protección perimetral permiten, como HTTP, DNS, VPN o ICMP.

Para citar un ejemplo, al usar DNS tunneling para enviar datos dentro de consultas DNS o usar SSH tunneling para encapsular tráfico dentro de conexiones cifradas.

Herramientas

Algunas herramientas comunes son: dnscat para DNS tunneling y Stunnel para túneles SSL/TLS.

Con estas herramientas podemos evadir firewalls comerciales y de nube, especialmente cuando se usa en combinación con certificados SSL para disfrazar el tráfico como HTTPS.

Se puede usar VPN, SSH tunneling o técnicas de Domain Fronting para ocultar el tráfico. Muy útil contra firewalls de capa 4 y algunos NGFW.

Limitaciones

Esta técnica es muy efectiva contra firewalls que solo inspeccionan puertos y no el contenido profundo del paquete (inspección de capa 7).

Los firewalls de ultima generación (NGFW) con inspección profunda de paquetes (DPI), pueden detectar patrones anómalos en túneles cifrados.

PRIMER EJERCICIO

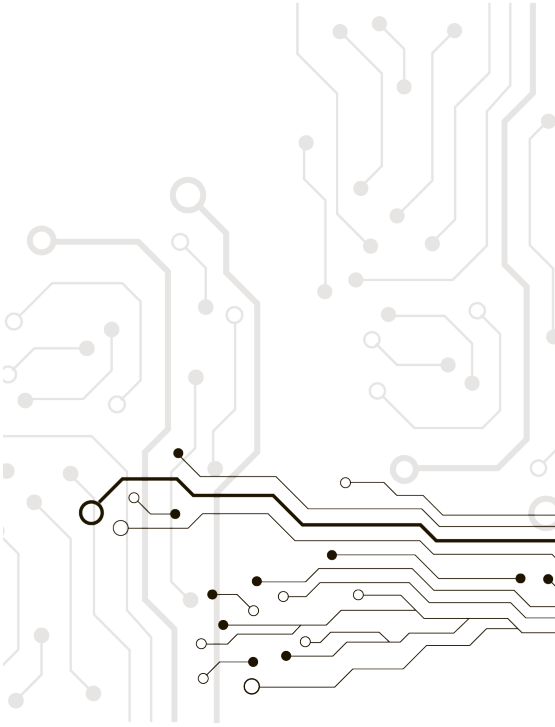
Crear un túnel DNS para evadir firewall

Objetivo

Encapsular tráfico dentro de consultas DNS para evadir firewalls que permiten solo tráfico DNS estándar.

Requerimientos

- Servidor Linux con IP pública (VPS) para actuar como servidor DNS tunelizado.
- Cliente Linux en laboratorio.
- Control sobre un dominio y sus registros DNS.
- Herramienta iodine (túnel DNS).



> La invencibilidad es una cuestión de defensa, la vulnerabilidad es una cuestión de ataque

Configurar el DNS para el tunel

- Crear un subdominio (ejemplo: tunel.midominio.com).
- Configurar registros NS para que apunten a un servidor DNS propio (ejemplo: ns.midominio.com).
- Apuntar ns.midominio.com a la IP pública del VPS.

Instalar iodine en el servidor

Iodine es una herramienta de software libre que permite crear un túnel de datos a través del protocolo DNS (Domain Name System), técnica conocida como DNS tunneling.

Su principal objetivo es facilitar la comunicación entre dos equipos a través de redes que restringen o filtran el tráfico convencional, como ocurre en entornos protegidos por firewalls o portales cautivos que solo permiten resolver nombres de dominio pero bloquean otros protocolos

- `sudo apt-get install gcc make autoconf libz-dev git`
- `git clone https://github.com/yarrick/iodine.git`
- `cd iodine`
- `make && sudo make install`

Ejecutar servidor iodine

Iodine encapsula datos dentro de consultas y respuestas DNS. De esta forma, permite que el tráfico de red pase desapercibido para muchos firewalls que solo inspeccionan el tráfico HTTP, HTTPS o bloquean puertos no convencionales, pero permiten el tráfico DNS para la resolución de nombres.

Ejecutar servidor iodine

Iodine encapsula datos dentro de consultas y respuestas DNS. De esta forma, permite que el tráfico de red pase desapercibido para muchos firewalls que solo inspeccionan el tráfico HTTP, HTTPS o bloquean puertos no convencionales, pero permiten el tráfico DNS para la resolución de nombres.

```
sudo iodined -c -P PASSWORD -n IP_ESTATICA
      172.16.0.1 tunel.midominio.com
```

Explicación:

PASSWORD: Aquí colocamos la contraseña para el túnel.
IP_ESTATICA: Es la IP pública del VPS.
172.16.0.1: Es la IP virtual para la interfaz del túnel.

En el cliente

En el cliente, instalamos iodine y procedemos a conectar

```
sudo iodine -P PASSWORD tunel.midominio.com
```

Esto crea una interfaz de red virtual que encapsula tráfico dentro de DNS.

Verificamos la conexión

- Navegar por internet o acceder a servicios a través del túnel DNS.
- Usar Wireshark para observar que el tráfico está encapsulado en consultas DNS.

SEGUNDO EJERCICIO

Crear un túnel SSH para evadir firewall

Objetivo

Encapsular tráfico TCP dentro de un túnel SSH para evadir firewalls que permiten solo conexiones SSH o HTTPS.

Requerimientos

- Servidor SSH accesible desde cliente (puede ser local o VPS).
- Cliente Windows con PuTTY instalado.

1. **Abrimos el aplicativo PuTTY y cargamos la sesión SSH**
   - Ingresar IP o dominio del servidor SSH.
   - Guardar sesión si se desea.

2. **Configuramos túnel SSH**
   - En el árbol de configuración: Connection > SSH > Tunnels.
   - En "Source port" poner un puerto local (ejemplo: 8080).
   - En "Destination" poner el servicio destino accesible desde el servidor SSH (ejemplo: 127.0.0.1:80 para web local).
   - Click en "Add".

3. **Abrimos conexión SSH**
   - Click en "Open" y autenticarse.
   - Mientras la sesión esté abierta, el puerto local 8080 actuará como proxy hacia el destino.

4. **Usamos el túnel**
   - Abrir navegador y acceder a http://127.0.0.1:8080.
   - El tráfico pasa cifrado dentro del túnel SSH, evadiendo firewalls que bloquean.

TERCER EJERCICIO

Configurar túnel VPN IPSec para evadir fire

Objetivo

Establecer un túnel VPN IPSec site-to-site para encapsular todo el tráfico entre dos redes, evadiendo inspección de firewall.

Requerimientos

- Dos firewalls compatibles con IPSec (Palo Alto, Cisco, Fortinet, Mikrotik, PFSense, etc.)
- Acceso administrativo a ambos dispositivos.

1. **Configurar Fase 1 (IKE)**
   - Definimos los parámetros de autenticación (PSK o certificados).
   - Configuramos los algoritmos de cifrado y hash (ejemplo: AES-128, SHA-256).
   - Establecemos el tiempo de vida y grupo Diffie-Hellman.
2. **Configurar Fase 2 (IPSec)**
   - Definimos los protocolos de encapsulación (ESP).
   - Configuramos los algoritmos de cifrado y autenticación.
   - Establecemos políticas de tráfico que usarán el túnel.
3. **Crear interfaz virtual de túnel**
   - Asociamos a un router virtual o zona de seguridad.
   - Configuramos las rutas estáticas para dirigir tráfico a través del túnel.
4. **Activar y verificar el túnel**
   - Comprobamos que la asociación de seguridad se establece correctamente.
   - Verificamos que el tráfico entre redes pasa cifrado y sin ser bloqueado por firewall.

CYBERNOVA

CIBERSEGURIDAD

Ing. Marvin G. Soto