

HTTPTunnel

Rubén Ibrahim Zuzuarregui Hidalgo

Conceptos base:

- Tunneling: mecanismo que consiste en enviar un paquete (usualmente cifrado) mediante el encapsulamiento de dicho paquete en un protocolo distinto.
- Port Forwarding: proceso de interceptar tráfico destinado para un IP/puerto y redireccionarlo a un IP/puerto distinto.
- HTTP Tunneling: mecanismo que consiste en encapsular un protocolo (usualmente de la familia TCP/IP) en un método POST o un método GET de HTTP con el objetivo de trasgredir las restricciones de un firewall o un proxy.

Instrucciones:

- La actividad deberá ser realizada en parejas.
- Una computadora tendrá la función de servidor.
- Otra computadora tendrá la función de cliente.

1. Instalar httptunnel en Kali ejecutar el siguiente comando desde la terminal:

```
sudo apt-get install httptunnel
```

2. Iniciar servicio de ssh en el cliente y en el servidor, ejecutar siguiente comando desde la terminal:

```
sudo service ssh start
```

3. Iniciar el servidor, introducir el siguiente comando en consola del servidor:

```
hts -F localhost:22 2139
```

El comando indica que todo el tráfico entrante por el puerto 2139 será mapeado (-F) al puerto 22.

4. Iniciar el cliente, introducir el siguiente comando en consola de cliente:

```
htc -F 8090 <ip de servidor>:2139
```

El comando (-F) indica que toda conexión entrante por el puerto 8090 será direccionado a la ip del servidor, al puerto 2139.

5. Realizar conexión mediante ssh al servidor, introducir siguiente comando en consola de cliente:

```
ssh localhost -p 8090
```

Se debe tener una solicitud de confirmación para conectarse al servidor.