📁 LPIC-2 / 🔒 Tema 212 - La seguridad del sistema - Ejercicios

*Nota: Estos ejercicios implican configurar redes virtuales, firewall y certificados. Realízalos **SIEMPRE en un entorno de VM de prueba aislado** con al menos dos VMs (una servidor OpenVPN, una cliente OpenVPN) en una red host-only, además de acceso a internet para el servidor (simulando una conexión externa). La gestión de certificados es fundamental. Necesitarás privilegios de superusuario (`sudo`).*

Ejercicio 12.5.1: Instalando OpenVPN y easy-rsa

- **Objetivo:** Instalar el software necesario en el servidor y el cliente.
- **Requisitos:** Acceso a la línea de comandos. Privilegios de superusuario (`sudo`). Conexión a internet. **VM de prueba (servidor y cliente).**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal en la VM servidora y en la VM cliente.
    2. **Instala OpenVPN en ambos:** `sudo apt update && sudo apt install openvpn` (Debian/Ubuntu) o `sudo dnf install openvpn` (Red Hat/CentOS/Fedora).
    3. **Instala easy-rsa (generalmente solo en el servidor, donde se gestionará la CA):** `sudo apt install easy-rsa` (Debian/Ubuntu) o `sudo dnf install easy-rsa` (Red Hat/CentOS/Fedora).

Ejercicio 12.5.2: (Conceptual) Generando Certificados y Claves con easy-rsa

- **Objetivo:** Entender los pasos para crear los archivos necesarios para la autenticación SSL/TLS.
- *Requisitos:* easy-rsa instalado. Acceso a la línea de comandos. **VM de prueba (servidor).**
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal en la VM servidora.
    2. **Copia los scripts easy-rsa a un directorio de trabajo seguro (requiere sudo):** `sudo cp -r /usr/share/easy-rsa /etc/openvpn/easy-rsa`. Es buena práctica hacer esto fuera del directorio de configuración principal si planeas modificar scripts. Alternativamente, trabaja directamente en `/usr/share/easy-rsa` (pero tus archivos generados estarán allí).
    3. **Cambia al directorio de trabajo easy-rsa:** `cd /etc/openvpn/easy-rsa`.
    4. **Edita el archivo `vars`:** `vi vars`. Modifica las variables de entorno para tu CA (KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, KEY_EMAIL, KEY_OU, y quizás KEY_NAME). Define el tamaño de la clave (ej: `export KEY_SIZE=4096`).
    5. **Carga las variables de entorno:** `source ./vars`.
    6. **Limpia el entorno (si has ejecutado antes):** `./clean-all`.
    7. **Inicializa la CA:** `./build-ca`. Te pedirá información; la mayoría se puede dejar por defecto si configuraste `vars`. Se generará `keys/ca.crt` y `keys/ca.key`.

8. **Genera la solicitud de certificado y clave del servidor:** `./build-key-server server`. Usa "server" como nombre común (Common Name - CN). Se generarán `keys/server.csr` y `keys/server.key`. Te pedirá firmarla; responde "y".
9. **Genera la solicitud de certificado y clave para cada cliente:** `./build-key client1`. Usa "client1" como nombre común (CN). **El CN de cada cliente debe ser único.** Se generarán `keys/client1.csr` y `keys/client1.key`. Te pedirá firmarla. Repite para cada cliente (client2, client3...).
10. **Genera los parámetros Diffie-Hellman:** `./build-dh`. Esto puede llevar tiempo. Se generará `keys/dh*.pem`.
11. **(Opcional) Genera una clave TLS-Auth:** `openvpn --genkey --secret keys/ta.key`.
12. **Copia los archivos necesarios a un directorio seguro en el servidor:** `ca.crt`, `server.crt`, `server.key`, `dh*.pem` (y `ta.key` si se usa) a un directorio como `/etc/openvpn/certs/`.

Ejercicio 12.5.3: (Conceptual) Configurando el Archivo del Servidor OpenVPN

- **Objetivo:** Crear un archivo de configuración básico para el servidor.
- *Requisitos:* Certificados y claves generados y copiados a `/etc/openvpn/certs/`. Privilegios de superusuario (`sudo`). **VM de prueba (servidor).**
- **Desarrollo Paso a Paso (Conceptual):**
  1. Abre una terminal en la VM servidora.
  2. **Crea un archivo de configuración (requiere sudo):** Ejecuta `sudo vi /etc/openvpn/server.conf`.
  3. **Pega la configuración básica (adapta las rutas y la subred VPN):**

```
port 1194
proto udp # O tcp
dev tun

ca certs/ca.crt # Rutas relativas a /etc/openvpn/
cert certs/server.crt
key certs/server.key
dh certs/dhparams.pem

server 10.8.0.0 255.255.255.0 # Red virtual VPN
ifconfig-pool-linear

push "redirect-gateway def1 bypass-dns" # Opcional: enviar todo el
trafico por la VPN
# push "route 192.168.1.0 255.255.255.0" # Opcional: enviar ruta a
red privada LAN

keepalive 10 120
cipher AES-256-CBC
auth SHA256

user nobody
group nogroup # O groupadd nogroup si no existe
```

```
persist-key
persist-tun

status /var/log/openvpn-status.log
log /var/log/openvpn.log
verb 3

# Si usaste tls-auth
# tls-auth certs/ta.key 0
```

4. **Guarda y sal.**
5. **Crea el directorio de logs si no existe y dale permisos (requiere sudo):** `sudo mkdir /var/log/openvpn && sudo chown nobody:nogroup /var/log/openvpn`.

Ejercicio 12.5.4: Gestión del Servicio del Servidor OpenVPN (Modo Instancia)

- **Objetivo:** Habilitar e iniciar el servicio OpenVPN con una configuración específica.
- **Requisitos:** Archivo `server.conf` creado en `/etc/openvpn/`. Privilegios de superusuario (`sudo`). **VM de prueba (servidor).**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal en la VM servidora.
    2. **Habilita la instancia del servicio:** Ejecuta `sudo systemctl enable openvpn@server.service`.
    3. **Inicia la instancia del servicio:** Ejecuta `sudo systemctl start openvpn@server.service`.
    4. **Verifica el estado:** `systemctl status openvpn@server.service`. Busca mensajes de éxito al levantar la interfaz tun/tap y escuchar en el puerto.
    5. **Verifica la interfaz virtual:** Ejecuta `ip addr show tun0`. Debería tener una IP de la red virtual VPN (ej: 10.8.0.1).
    6. **Revisa los logs de OpenVPN:** Ejecuta `sudo less /var/log/openvpn.log`.

Ejercicio 12.5.5: Configurando Firewall, Reenvío y NAT en el Servidor

- **Objetivo:** Permitir el tráfico de la VPN y el enrutamiento/NAT hacia otras redes.
- **Requisitos:** Servicio OpenVPN corriendo. Privilegios de superusuario (`sudo`). Herramienta de firewall configurada. **VM de prueba (servidor).**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal en la VM servidora.
    2. **Verifica que el reenvío de IP está habilitado:** `sysctl net.ipv4.ip_forward`. Habilítalo si es necesario (Ej. 12.1.1).
    3. **Permite tráfico entrante al puerto OpenVPN en el firewall** (Ej. 12.3.2, pero para puerto 1194 UDP/TCP o el que configuraste).

4. **Permite tráfico enrutado (FORWARD) desde la interfaz tun0 a otras interfaces** (y viceversa, dependiendo de tu política de firewall). Si la política FORWARD por defecto es DROP, necesitas reglas explícitas (Ej. 12.1.4).
    - **Con `iptables`:** `sudo iptables -A FORWARD -i tun0 -j ACCEPT`, `sudo iptables -A FORWARD -o tun0 -j ACCEPT`. Guarda reglas.
    - **Con `firewalld`:** Configurar el reenvío entre zonas (ej: zona `trusted` para `tun0` y zona `public` para la interfaz a Internet).
5. **Configura NAT (Masquerading) si los clientes necesitan acceder a Internet o a redes detrás del servidor vía NAT:**
    - **Con `iptables`:** `sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o <interfaz_publica> -j MASQUERADE`. Guarda reglas. (Reemplaza `10.8.0.0/24` por tu red virtual VPN y `<interfaz_publica>` por la interfaz de salida a Internet del servidor).
    - **Con `firewalld`:** Añade la interfaz `tun0` a una zona y habilita masquerading en la zona de salida (ej: `sudo firewall-cmd --zone=external --add-masquerade --permanent`, `sudo firewall-cmd --zone=trusted --add-interface=tun0 --permanent`, `sudo firewall-cmd --reload`).

Ejercicio 12.5.6: Configurando el Archivo del Cliente OpenVPN

- **Objetivo:** Crear el archivo de configuración para el cliente.
- **Requisitos:** Paquete openvpn instalado en la VM cliente. Certificados (`ca.crt`, `client1.crt`, `client1.key` y `ta.key` si se usa) copiados desde el servidor a un directorio en el cliente (ej: `~/openvpn-client/`). **VM de prueba (cliente).**
- **Desarrollo Paso a Paso:**
    1. Abre una terminal en la VM cliente.
    2. **Crea un directorio para los archivos de configuración y certificados (opcional pero recomendado):** `mkdir ~/openvpn-client`.
    3. **Copia los archivos necesarios desde el servidor** (usa `scp` - Revisado 12.3.3) a este directorio: `ca.crt`, el certificado y clave privada de este cliente (ej: `client1.crt`, `client1.key`), y `ta.key` si se usa.
    4. **Establece permisos adecuados en los archivos de clave privada (solo lectura para el propietario):** `chmod 600 ~/openvpn-client/client1.key`.
    5. **Crea el archivo de configuración (ej: client1.conf o client1.ovpn):** Ejecuta `vi ~/openvpn-client/client1.conf`.
    6. **Pega la configuración básica (adapta la IP del servidor y las rutas de archivos):**

```
client
dev tun
proto udp # O tcp, debe coincidir con el servidor

remote <IP_Publica_Servidor_OpenVPN> 1194 # IP y puerto del servidor
```

```
resolv-retry infinite
nobind

persist-key
persist-tun

ca /home/<tu_usuario>/openvpn-client/ca.crt
cert /home/<tu_usuario>/openvpn-client/client1.crt
key /home/<tu_usuario>/openvpn-client/client1.key

remote-cert-tls server

cipher AES-256-CBC # Debe coincidir con el servidor
auth SHA256 # Debe coincidir con el servidor

# Si usaste tls-auth
# tls-auth /home/<tu_usuario>/openvpn-client/ta.key 1

verb 3 # Nivel de log
```

7. **Guarda y sal.**

Ejercicio 12.5.7: (Conceptual) Iniciando el Cliente OpenVPN y Probando Conexión

- **Objetivo:** Conectar el cliente al servidor VPN y verificar que se establece el túnel.
- *Requisitos:* Servidor OpenVPN corriendo y accesible (firewall, IP forwarding, NAT si es necesario). Archivo de configuración cliente con certificados/claves. **VM de prueba (cliente).**
- **Desarrollo Paso a Paso (Conceptual):**
    1. Abre una terminal en la VM cliente.
    2. **Inicia el cliente OpenVPN con el archivo de configuración:** Ejecuta `sudo openvpn --config ~/openvpn-client/client1.conf`. **Ejecútalo en primer plano inicialmente para ver los logs.**
    3. **Observa la salida:** Busca mensajes de log que indiquen que la conexión se está estableciendo, la negociación TLS, la asignación de IP (`ifconfig tun0 ...`), y finalmente "Initialization Sequence Completed".
    4. **Verifica la nueva interfaz virtual:** Abre otra terminal en el cliente. Ejecuta `ip addr show tun0`. Debería tener una IP de la subred virtual VPN (ej: 10.8.0.6).
    5. **Prueba la conexión:** Haz ping a la IP virtual del servidor OpenVPN (ej: 10.8.0.1). Haz ping a un recurso en la red privada detrás del servidor (si configuraste la ruta). Si usaste `redirect-gateway`, haz ping a una dirección de Internet (ej: 8.8.8.8).
    6. **Si la conexión se establece, puedes detener el cliente con Ctrl+C** y luego ejecutarlo como servicio si lo deseas (el nombre del servicio puede variar, busca ejemplos con `openvpn@client1.service` o usa un script de inicio si no hay una unidad systemd genérica).