Exp 9

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ipsec.conf
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ipsec.secrets
```

```
config setup
    charondebug="ike 2, knl 2, cfg 2"

conn right-to-left
    auto=add
    keyexchange=ikev2
    type=tunnel

    left=192.168.217.130
    leftid=192.168.217.130
    leftsubnet=192.168.217.130/32

    right=192.168.217.129
    rightid=192.168.217.129
    rightsubnet=192.168.217.129/32

    ike=aes256-sha256-modp2048
    esp=aes256-sha256
    authby=psk
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ipsec start
Starting strongSwan 6.0.3 IPsec [starter]...
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ipsec up right-to-left
initiating IKE_SA right-to-left[1] to 192.168.217.129
generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_ALG) N(REDIR_SUP) ]
sending packet: from 192.168.217.130[500] to 192.168.217.129[500] (1200 bytes)
retransmit 1 of request with message ID 0
sending packet: from 192.168.217.130[500] to 192.168.217.129[500] (1200 bytes)
retransmit 2 of request with message ID 0
sending packet: from 192.168.217.130[500] to 192.168.217.129[500] (1200 bytes)
retransmit 3 of request with message ID 0
sending packet: from 192.168.217.130[500] to 192.168.217.129[500] (1200 bytes)
retransmit 4 of request with message ID 0
sending packet: from 192.168.217.130[500] to 192.168.217.129[500] (1200 bytes)
retransmit 5 of request with message ID 0
sending packet: from 192.168.217.130[500] to 192.168.217.129[500] (1200 bytes)
^Z
zsh: suspended  sudo ipsec up right-to-left
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.217.129
PING 192.168.217.129 (192.168.217.129) 56(84) bytes of data.
64 bytes from 192.168.217.129: icmp_seq=1 ttl=64 time=0.733 ms
64 bytes from 192.168.217.129: icmp_seq=2 ttl=64 time=0.919 ms
64 bytes from 192.168.217.129: icmp_seq=3 ttl=64 time=0.845 ms
64 bytes from 192.168.217.129: icmp_seq=4 ttl=64 time=1.16 ms
64 bytes from 192.168.217.129: icmp_seq=5 ttl=64 time=0.499 ms
64 bytes from 192.168.217.129: icmp_seq=6 ttl=64 time=0.650 ms
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ipsec.conf
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ipsec.secrets
```

```
config setup
    charondebug="ike 2, knl 2, cfg 2"

conn left-to-right
    auto=add
    keyexchange=ikev2
    type=tunnel

    left=192.168.217.129
    leftid=192.168.217.129
    leftsubnet=192.168.217.129/32

    right=192.168.217.130
    rightid=192.168.217.130
    rightsubnet=192.168.217.130/32

    ike=aes256-sha256-modp2048
    esp=aes256-sha256
    authby=psk
```

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.217.130
PING 192.168.217.130 (192.168.217.130) 56(84) bytes of data.
64 bytes from 192.168.217.130: icmp_seq=1 ttl=64 time=0.772 ms
64 bytes from 192.168.217.130: icmp_seq=2 ttl=64 time=0.724 ms
64 bytes from 192.168.217.130: icmp_seq=3 ttl=64 time=0.806 ms
64 bytes from 192.168.217.130: icmp_seq=4 ttl=64 time=0.754 ms
64 bytes from 192.168.217.130: icmp_seq=5 ttl=64 time=0.808 ms
64 bytes from 192.168.217.130: icmp_seq=6 ttl=64 time=0.559 ms
```

```
┌──(kali㉿kali)-[~]
└─$ sudo tee /etc/ipsec.secrets > /dev/null << 'EOF'
heredoc> 192.168.1.10 192.168.1.20 : PSK "kali123"
EOF
```

```
┌──(kali㉿kali)-[~]
└─$ sudo cp /etc/ipsec.conf
cp: missing destination file operand after '/etc/ipsec.conf'
Try 'cp --help' for more information.

┌──(kali㉿kali)-[~]
└─$ /etc/ipsec.conf
zsh: permission denied: /etc/ipsec.conf
```