LABB 4

VINCENT PALMA
IOT20

# IPsec

IPsec står för Internet Protocol Security och den består av flera protokoll som ska kunna ge tjänsterna som gör att mottagaren enbart förstår vad som tas emot,
garanti på att data inte alterneras på vägen, signering av data med verifiering
och bearbetningen av datagrammet sker endast en gång så att den inte repeteras.

Strongswan är det som ger oss IPsec funktionen och det installerar vi samt ställer in det så att den inte startar automatiskt
**sudo apt install strongswan libcharon-extra-plugins**
**sudo systemctl disable —now strongswan-starter**

Då vpn tunneln inte är aktiv så behöver vi mata in
**sudo systemctl restart ipsec i terminalen och det**
ser till att ipsec funktionen drar igång (uppkopplingen mellan de två datorerna via en tunnel blir aktiv).

**sudo systemctl status ipsec**
visar mig statusen på uppkopplingen.

**curl ipinfo.io/ip**
kontrollerar nuvarande publika ip address

sudo cp ca-cert.pem /etc/ipsec.d/cacerts/
ser till att vi kopierar ce-cert.pem filen dit strongswan hittar den.

15. Kolla IP-adressen nu (svaret kan ta en stund):
    curl ipinfo.io/ip
    a) Har du fått ut samma IP-adress som du fick tidigare? Eller har du fått något felmeddelande?

    Fick först meddelandet "Could not resolve host: ipinfo.io.
    men med att lägga in nameserver 8.8.8.8 i /etc/resolv.conf så fick jag det att fungera. (Google sensei)
    Källa: https://bobcares.com/blog/curl-6-could-not-resolve-host-ubuntu/

    a) Vilken IP-adress då?
        När kommandot fungerarde så fick jag ett nytt ip nummer och det blev 13.48.248.81.
    b) Förklara innebörden av den här IP-adressen.
        Oklar fråga, men resultatet av de kommandon vi har matat in tidigare samt ändrad ipsec.conf fil har vi nu en tunnel från min dator till denna nya ip (vpn).

16.
    a) Hur många Security Associations har du?

```
Security Associations (1 up, 0 connecting):
```

    b) Hur många Security Parameter Index har du?

```
ikev2-rw[1]: IKEv2 SPIs: e5565c4aab584d2f_i* 45b6d52473dff5e1_r, EAP reauthentication in 2 hours
```

    2St skulle jag säga

```
SPIs: c07297d3_i cf8652bb_o
```

    En SPI är på 32bitar.

    c) Vilken kryptoalgoritm (cipher) har den valt för ESP och i vilket läge (cipher mode) körs den?
        AES_CBC Advanced Encryption Standard , Cipher Blocker Chaining
    d) Hur lång nyckel (antal bitar) har den valt för kryptoalgoritmen i ESP?
        256bit
    e) Vilken hashalgoritm används för HMAC i ESP?
        SHA2

CHAP står för challenge handshake authentication protocol och MSCHAP är microsofts version av protokollet. Vad den gör är att en certifierad klient kan koppla upp sig till servern med en handshake. Som en VIP får tillgång till en plats men inte andra. Den används som en autenticieringsmetod via PPTP (Point to Point Tunneling Protocol).Det börjar med en EAP (Extensible Authentication Protocol) session mellan klienten och server och vid uppkoppling väljs vilken metod som ska användas och vid detta tillfälle blir det MSCHAPv2 (*microsoft.com*).

## WIRESHARK DATA

### SOURCE SPI


### DESTINATION SPI


SPI i hex