TCP, UDP eta Three Way Handsakea

Abatailak eta Desabantailak protokoloen artean

TCP (Transmisioa Kontrolatzeko Protokoloa):

Abantailak: 1.**Fidagarritasuna:** TCPk datuen entrega ordenatua eta fidagarria bermatzen du. Transmisioan paketeak galtzen badira, TCP arduratzen da paketeak transmititzeaz. 2.**Fluxu-kontrola:** TCPk fluxu-kontroleko mekanismoak inplementatzen ditu sarean pilaketa saihesteko eta hartzaileak datuak erritmo egokian prozesatu ahal izatea ziurtatzeko. 3.**Aitortzea eta ematea:** Aitortza-mekanismoak ematen ditu, igorleak jakin dezan zer datu jaso diren behar bezala eta galdutakoak eman ahal izan ditzan.

Desabantailak: 1.**Gainkarga handiagoa:** TCPk protokolo-gainkarga handiagoa du UDPrekin alderatuta, konexioak, fluxu-kontrola eta emankizunak ezarri eta mantentzeko beharragatik. 2.**Latentzia handiagoa:** Fluxua entregatu eta kontrolatzeko berme-mekanismoak direla eta, TCPk nolabaiteko latentzia sar dezake datuen transmisioan.

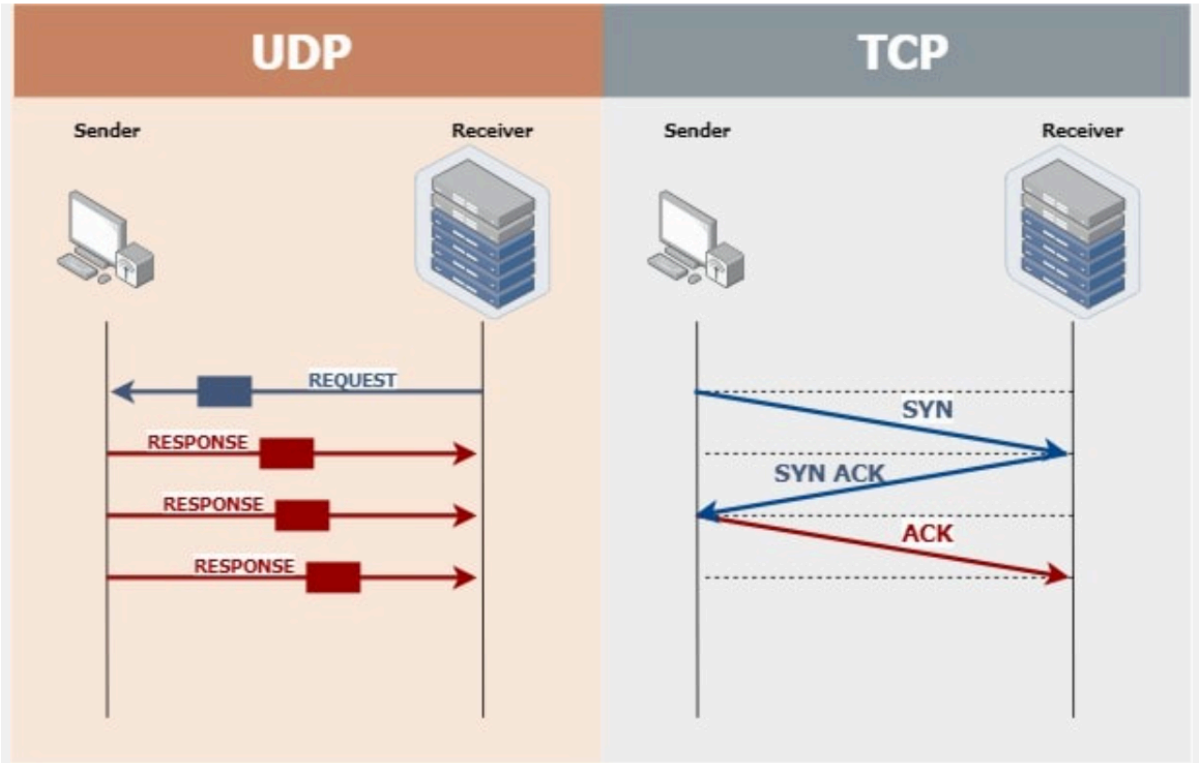
UDP (User Datagram Protocol):

Abantailak: 1.**Gainkarga txikiagoa:** UDPk protokolo-gainkarga txikiagoa du, ez baitu konexiorik ezarri edo mantendu behar, eta ez du fluxu-kontrolik edo emanaldirik inplementatzen. 2.**Latentzia txikiagoa:** TCP mekanismo gehigarriak ez dituenez, UDPk latentzia txikiagoa eskain dezake datuen transmisioan. 3.**Datuak denbora errealean transmititzea:** Egokia da datuak denbora errealean azkar transmititzea eskatzen duten aplikazioetarako, hala nola audio- eta bideo-transmisioetarako.

Desabantailak: 1.**Ez du entrega bermatzen:** UDPk ez du bermatzen datuak entregatuko direnik, ezta zein ordenatan jasoko diren ere. Transmisioan paketeak gal daitezke. 2.**Fluxu-kontrolik gabe:** Ez dago fluxua kontrolatzeko mekanismorik UDPn, eta horrek esan nahi du datuak ahalik eta abiadura handienean bidaltzen direla, eta horrek auto-pilaketa eragin dezake sarean. 3.**Ez dago ez aintzatespenik ez emanaldirik:** Paketeak galtzen badira, ez dago mekanismo automatikorik horiek transmititzeko, eta erabiltzaileak berreskuratze-mekanismo propioak inplementatu behar ditu, beharrezkoa bada.

Laburbilduz, TCP egokiagoa da fidagarritasuna eta entrega-bermea eskatzen duten aplikazioetarako, eta UDP, berriz, hobea da latentzia kritikoa den eta nolabaiteko datu-galera

onar daitekeen egoeretan. TCP eta UDPren arteko aukeraketa aplikazioaren baldintza espezifikoen araberakoa da.



Portuak eta beren prokoloak

Garrantzitsua da *nmap* tresnarekin atakak eskaneatzeko makina bat zer ataka erabiltzen ari den eta zer protokolorekin erabiltzen ari den jakitea

TCP

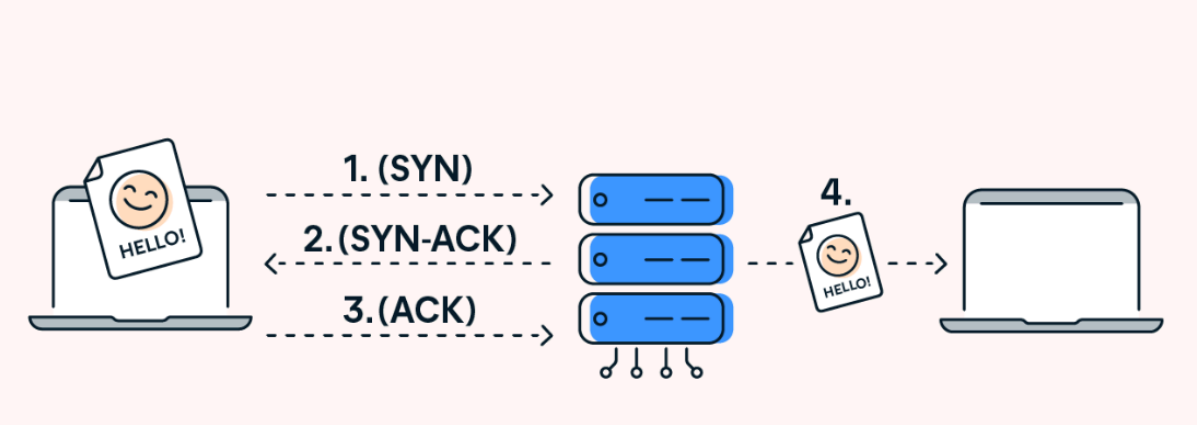
- 21 -> FTP
- 22 -> SSH
- 23 -> (Telnet)
- 25 -> (SMTP)
- 53 -> (DNS)
- 80 -> HTTP
- 443 -> HTTPS
- 110 -> (POP3)
- 139, 445 -> (SMB)
- 4143 -> (IMAP)

UDP

- 53 -> (DNS)
- 69 -> (TFTP)
- 161 -> (SNMP)

Three way handshake

Oharra: Ack dator Acknowledge-etik



Behatu three way handshake Netcat eta Wireshar erabiliz

NetCat tresna erabiliz entzuten dugu. Tresna hori oso erabilgarria da datuak tre por tcp edo udp bidez transmititzeko. Versatila da, eta entzuteko probak egiteko erabil daiteke, orain egingo dugun bezala, baina baita tunelak sortzeko ere, urruneko shell bat irekitzeko, atakak birbidaltzeko eta ssl konexioak egiteko, besteak beste.

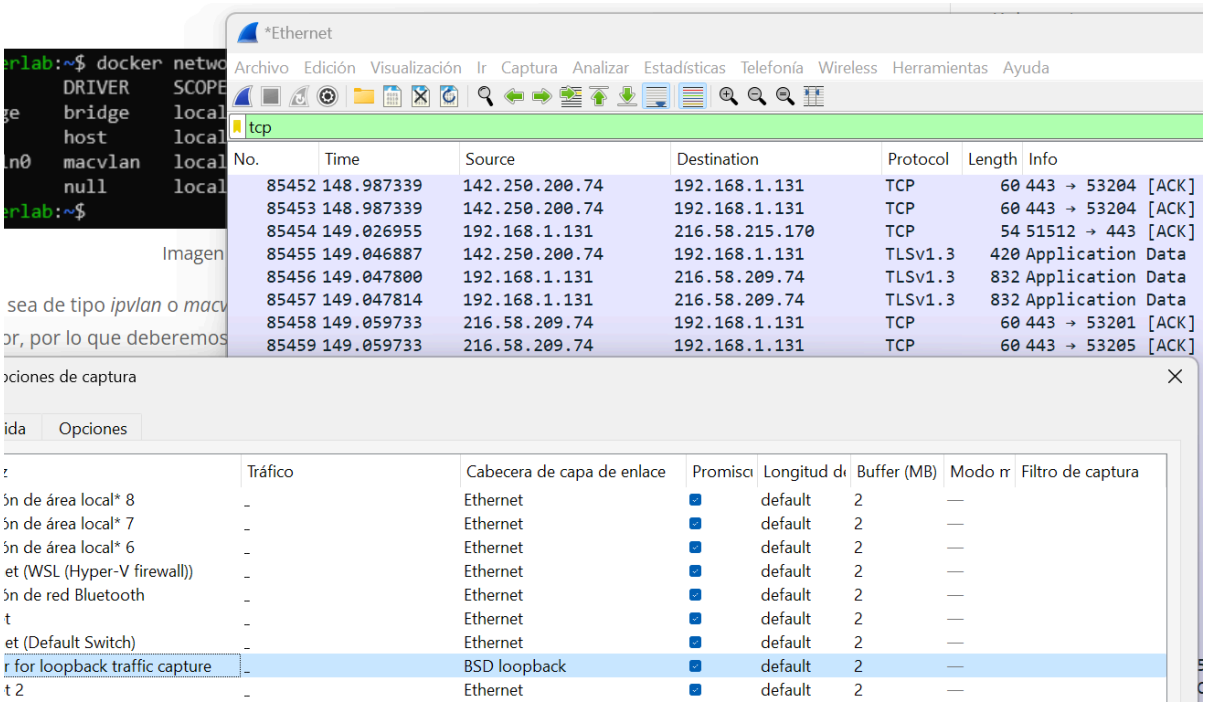
Entzun

```
┌──(root㉿DESKTOP-TNMI2JI)-[~]
└─# nc -nlvp 4646
listening on [any] 4646 ...
connect to [192.168.65.6] from (UNKNOWN) [192.168.65.6] 45170
```

Entzuten ari garen portu honen bidez konektatzen saiatu

```
┌──(root㉿DESKTOP-TNMI2JI)-[~]
└─# nc 192.169.65.6 4646
```

Wireshark -en loopback interfazea atzitu eta tcp bidez iragazi


rlab:~$ docker netwo
DRIVER SCOPE
bridge local
host local
macvlan local
null local
rlab:~$
Imagen
sea de tipo ipvlan o macv
or, por lo que deberemos
*Ethernet
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
tcp
No. Time Source Destination Protocol Length Info
85452 148.987339 142.250.200.74 192.168.1.131 TCP 60 443 → 53204 [ACK]
85453 148.987339 142.250.200.74 192.168.1.131 TCP 60 443 → 53204 [ACK]
85454 149.026955 192.168.1.131 216.58.215.170 TCP 54 51512 → 443 [ACK]
85455 149.046887 142.250.200.74 192.168.1.131 TLSv1.3 420 Application Data
85456 149.047800 192.168.1.131 216.58.209.74 TLSv1.3 832 Application Data
85457 149.047814 192.168.1.131 216.58.209.74 TLSv1.3 832 Application Data
85458 149.059733 216.58.209.74 192.168.1.131 TCP 60 443 → 53201 [ACK]
85459 149.059733 216.58.209.74 192.168.1.131 TCP 60 443 → 53205 [ACK]
ciones de captura
ida Opciones
Tráfico Cabecera de capa de enlace Promisci Longitud d Buffer (MB) Modo m Filtro de captura
ón de área local* 8 Ethernet default 2
ón de área local* 7 Ethernet default 2
ón de área local* 6 Ethernet default 2
et (WSL (Hyper-V firewall)) Ethernet default 2
ón de red Bluetooth Ethernet default 2
t Ethernet default 2
et (Default Switch) Ethernet default 2
r for loopback traffic capture BSD loopback default 2
t 2 Ethernet default 2