Internet Security TCP/IP 2 24.03.

UDP / TCP
1) 2)

1) connectionless, unreliable

IP may drops a packet, this problem is not fixed by UDP

IP checksum gilt nur für header, data kann korrupt sein

UDP: Port abstraction

zB für streaming - weniger overhead

32 bit UDP header auf folie

Spoofing & hijacking same as IP, Port must be known

UDP Storm DOS attack

Echo service UDP port 7

chargen service port 19 (Character generation)

Echo chargen loops man soll keinen Garbage Packages replien wenn man UDP services programmiert

UDP Portscan Wenn kein Service läuft bekommt man einen ICMP reply - port unreachable

Scanner: nmap ...

2) no loss, duplication etc. for TCP

virtual circuit with src ip + port dest ip + port
socket

checksum on whole data, acknowledgements

ordering at end host - reassembly

TCP segment (packet)

sequence number, acknowledgement number

Position of packet in data stream

Welches packet von ds nächstes will

TCP window: Packet wird nur akzeptiert wenn packet innerhalb ACK + window ist!

TCP flags SIN, ACK, FIN, RST wichtig

TCP options - Erweiterungen

Window size scaling - 16 bit zu 32 bit vergrößert

Three way handshake

TCP data exchange

ACK is delayed Man wartet 200 ms

FIN flag set (eine ist fertig mit Daten zu senden) kann aber noch ACK senden

TCP scanning (zB mit telnet etc., browser)

SYN scanning - no logging

Man kann zB nur SYN schicken, wenn man ACK bekommt ist Port offen!, Man schickt dann zB Reset

geht auch mit FIN packet (hängt mehr von Implementierung ab)

OS fingerprint scanning jede Implementierung ist anders

Fenster Größe, Reihenfolge d Options

Man kann auch mehrdeutige Pakete schicken und Reaktion abwarten.

nmap kann auch bissel OS fingerprinten

TCP spoofing - schwieriger

Initial sequence number guessing - oder mitschneiden

| schwierig

2^{32} Möglichkeiten

| nur wenn man auf selben Link ist

Manche Implementierungen haben keine randomness

TCP Hijacking - Connection übernehmen

Schwierig wenn man nicht im gleichen Netz ist

Correct ACK number must be known!

(client port muss man auch wissen - schwierig

muss nur im Fenster sein

| nur 16 bit → up to 64k

je größer window size desto leichter (mit extensions z.B.)

TCP DOS attacks

SYN flooding Solution: drop oldest half open connection

mindestens implementiert ← Syn cookies - keinen State speichern

aber nicht aktiviert - bei Attacken aktivieren

Process table attack: theoretisch maximal n neue Prozesse für connection