Internet Security 10.03.2010

Dumpster Diving: Looking for useful info in ppl. trash

OSI Modell:

siehe Folien

Session & Presentation Layer sind in Layer 7 abgegangen

→ only five layers left

Exchange layers f.e. Wireless Link instead of optical

IP ↔ IPV6 and still using TCP

IPV4 4 bytes / IP adr.

Unterteilung # Netbits & hostbits
define a Class

Subnet mask to split into subnets
Subnet mask XOR IP address → # subnet id bits
& host id bits

127. something always local machine
Reserved adresses - non routables
192. 168. ...

Japan IPV6 used

IP: connectionless - unreliable
Datagram - Header (still destination) - contains - payload

TTL in header: how old is the packet; dec by 1 when forwarded - when 0 discarded

f.e. TTL = 1 : Router sets TTL = ∅ → sends ICMP
TTL = 2 : to provider

IP options :
source route option f.e. specify all hops where packets must go!

IP encapsulation into ethernet

Hub only connects - forwards info to all channels
switch only sends to correct channel

Fragmentation : Set fragment bit ID specifies # of packet — the source will put it together

Some networks do not allow fragmentation - just drop packets and send ICMP

POD : siehe Folien

TCP overwrite

Fragmentierte Pakete ... 2. Paket überschreibt 1. Paket, z.B. Destination address

Network Sniffing z.B bei einem Hub möglich

Confuse a switch with Mac spoofing / flooding

Detect sniffers : suspicious DNS lookups
check if interface is in promiscuous mode

Use Latency to detect sniffers
Sending invalid packets to a sniffer → if a reply comes it's a sniffer