Forelæsningsnoter

Mikkel Boye Rasmussen

02.03.2023

5-lags modellen recap
TCP - Three way handshake - til at etablere en forbindelse UDP - behøver ikke etablere en forbindelse
application - message - http, ssh, ftp, dhcp, dns, smtp transport - segment - TCP, UDP network - datagram - IPv4, IPv6, ICMP data-link - frame - ARP, bluetooth, MAC, WIFI, ether bits - physical
udp - man broadcaster ved at sende en pakke til 255.255.255
smtp - simple mail transport protocol - anvender TCP
DNS - anvender UDP
DHCP - dynamic host configuration protocol - tildeler IP - man starter med at broadcaste til alle for at få at vide om en DHCP server eksisterer. (DORA - Discover, offer, request, acknowledge).
Agenda full packet capture

- kan hurtigt fylde meget da, evt. hvis man uploader en fil på 4gb vil den også gemme filen i et full packet capture.
tools
netflow

Traffic capturing options
full packet capture - dumping all traffic
session data - only gather info about the traffic
packet strings - dumping application level headers
Full packet capture takes huge amout of space - privacy issues
basically this is what wireshark does for us.In linux we can also use tcpdump for capturing traffic
tcpdump -i eth0 -w dmp.pcap
kan være et gdpr issue.
How to actually collect data hardware taps pros: can be scaled for needs cons: can be very expensive for high speed
mirroring the port on the switch (SPAN) pros: Available if the switch supports it. no downtime cons: can be a problem if collecting more data than the port speed.
tcpdump tcpdump kan give forkert checksum, dette skyldes at tcpdump fanger pakken før checksum er beregnet.